

# **GSB Gestion Frais d'installation**


Philippon Alec

Mahamoudou Irache

Sono Nana

Sylla Sakina





Nous avons ici un routeur qui devra tourner sur le système d'exploitation Pfsense, un serveur web tournant sur Debian avec un module web Apache, 2 DNS à installer puis configurer puis un ordinateur tournant sur Windows 10 depuis le réseau GSB.

## Les grandes étapes

### I. Mise en place de l'infrastructure réseau

Nous allons procéder pas-à-pas à l'installation de l'infrastructure, mais aussi à sa configuration très importante pour garantir la meilleure sécurité possible à nos utilisateurs.

### II. Sécurisation des communications

Mise en place de protocole plus sécurisé pour chiffrer les échanges entre le serveur et le client (HTTPS, SFTP, certificat SSL/TLS....)

I. Mise en place de l'infrastructure réseau	4
II. Mise en place du service HTTPS + SSH	58



# I. Mise en place de l'infrastructure réseau

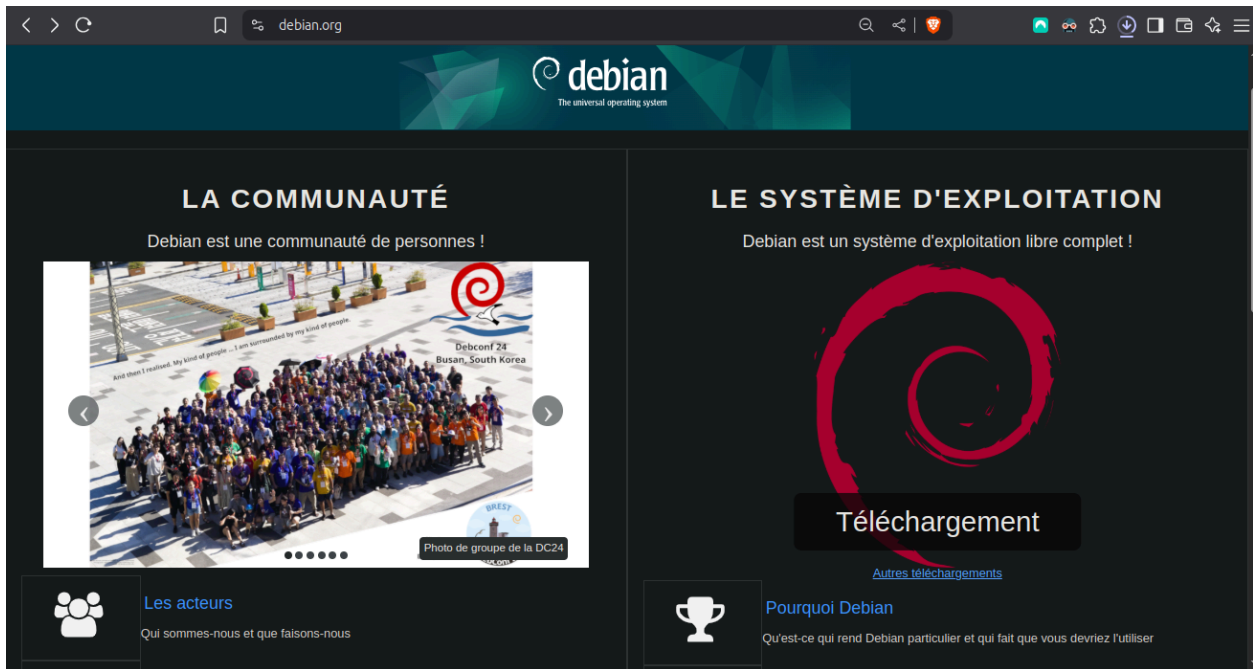
I. Téléchargement puis configuration de Virtualbox et téléchargement de Debian	4
II. Installation de debian	11
III. Configuration de debian	24
IV. Installation & Configuration de Pfsense	33
V. Installation des serveurs DNS	49

## I. Téléchargement puis configuration de Virtualbox et téléchargement de Debian

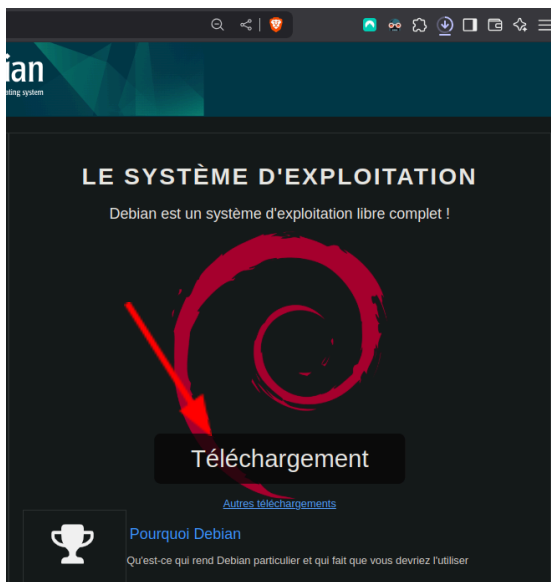
Pour commencer, nous allons commencer cette première partie par le serveur web. Un serveur est un dispositif matériel ou un logiciel qui fournit des services, des ressources ou des données à d'autres dispositifs, appelés clients, sur un réseau. Nous choisissons le système d'exploitation Debian pour notre serveur qui accueillera le site web de GSB ainsi que l'ensemble des modules complémentaires nécessaires à son bon fonctionnement. Pour ce faire, il faut au préalable télécharger l'image ISO du système debian sur le site officiel de debian (debian.org) mais également le logiciel de virtualisation Virtualbox se trouvant sur virtualbox.org. Virtualbox est un logiciel de virtualité de type 2 (Hosted). Pour mieux comprendre le terme de type d'hyperviseur, il en existe 3 différents. Nous avons :

- Le type 1 (Bare-metal) : Il s'exécute directement sur le matériel physique de l'hôte, sans système d'exploitation (OS) intermédiaire. Comme logiciel de ce type nous pouvons citer *VMWare ESXI* ou encore *Microsoft Hyper-V*
- Le type 2 (Hosted) : Celui-ci doit s'exécuter sur un système d'exploitation hôte, permettant de créer et de gérer des machines virtuelles au-dessus de l'OS. *Oracle Virtualbox* ainsi que *VMWare Workstation* sont des logiciels de ce type d'hyperviseur..
- Le type 3 dit Hybrid quant à lui, combine les caractéristiques du type 1 et 2. Comme logiciel de ce type, nous avons *Xen* et *KVM*.

En arrivant sur le site pour télécharger Debian, nous atterrissons sur la page d'accueil :



Pour télécharger l'image iso de Debian, il faut cliquer sur le bouton de téléchargement situé sur la partie droite pour arriver sur la page de téléchargement du système d'exploitation :

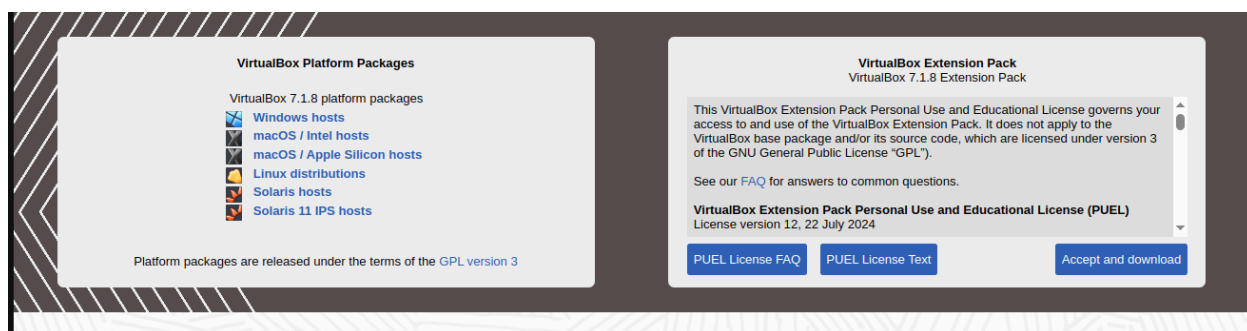


Le bouton “téléchargement” va nous télécharger une image dite "netinstall". Une image iso netinstall est une image disque plus légère mais elle est dépendante d'internet pour s'installer tandis qu'une iso standard est autonome et ne nécessitant pas de connexion internet. Nous choisirons une netinstall pour installer le serveur pour cette documentation mais libre à vous de choisir ce qui est le mieux pour vous en fonction de votre environnement.

Une fois le téléchargement fini, vous devriez avoir un fichier dans votre explorateur de fichiers de ce type :

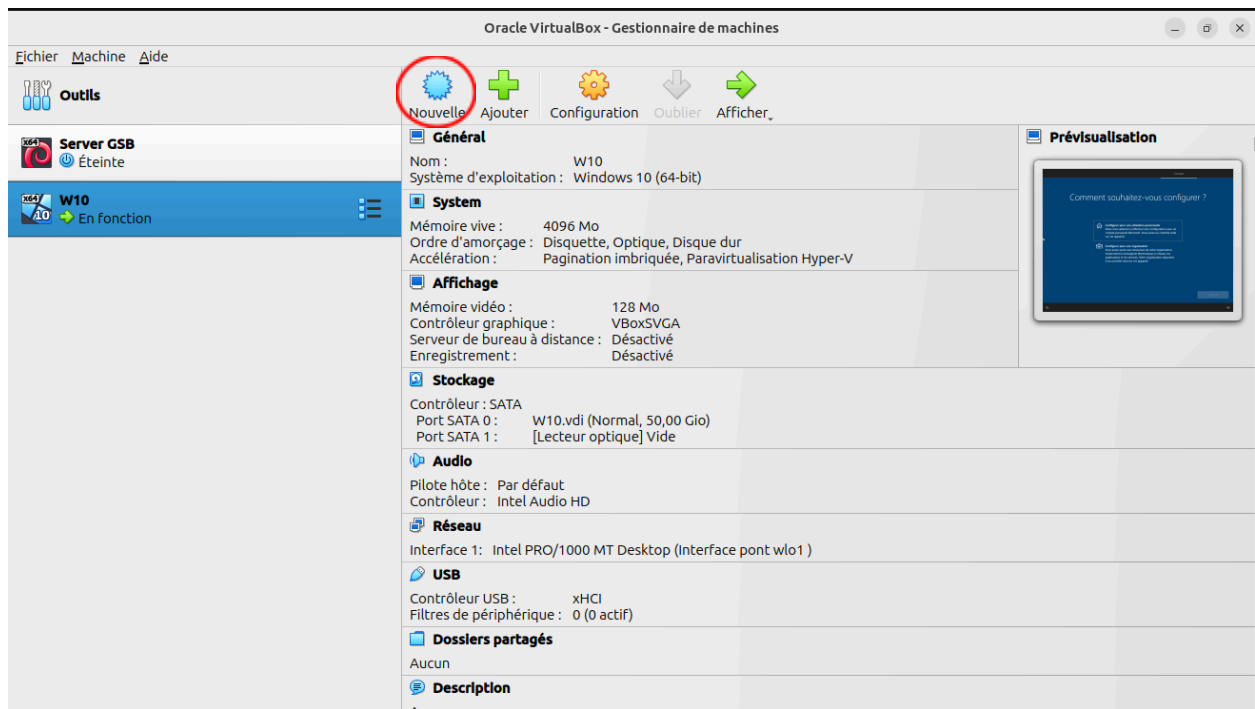


Ceci fait, nous allons nous rendre sur le site de virtualbox pour télécharger le logiciel qui nous permettra de réaliser cette infrastructure. En tapant sur notre navigateur *virtualbox.org* en étant sur le site, cliquer sur la rubrique download pour être redirigé ici :

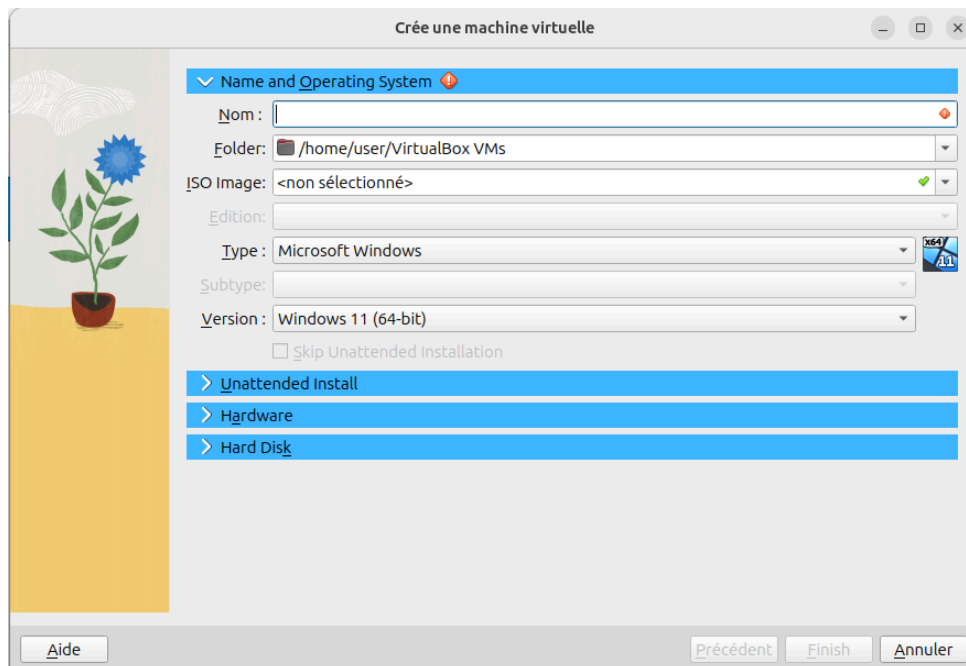


Cliquer en 1er lieu à droite sur l'extension pack de Virtualbox. L'extension pack de VirtualBox ajoute des fonctionnalités avancées comme le support USB 2.0/3.0, l'accès à distance via RDP, l'amélioration des performances graphiques et le chiffrement des disques virtuels.

Ensuite, vous pouvez télécharger le logiciel en faisant attention de prendre **la bonne version adaptée à votre système** car oui virtualbox est disponible sur différents systèmes d'exploitation donc veuillez à faire attention lors du téléchargement de celui-ci. Après ces téléchargements terminés, exécuter Virtualbox pour avoir une fenêtre comme celle-ci :



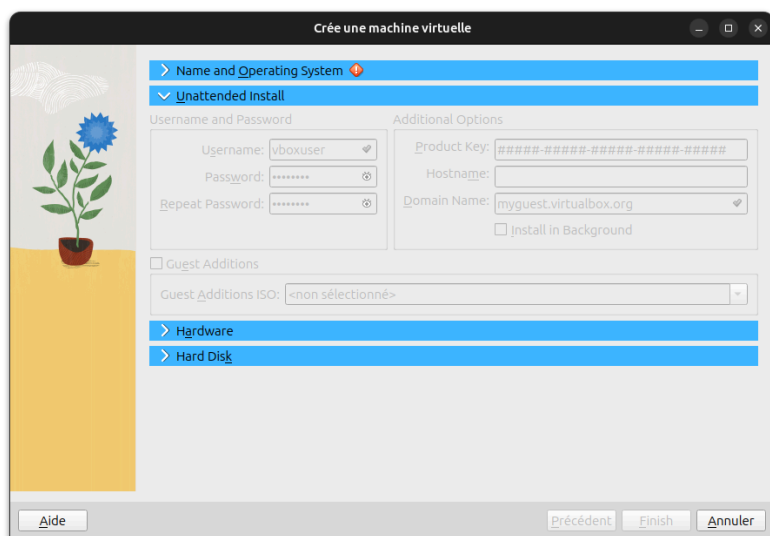
Ceci est la page d'accueil de virtualbox, c'est ici que l'on peut créer nos machines virtuelles, configurer nos machines, les préférences de l'application. Pour ajouter une machine virtuelle, vous devez cliquer sur le bouton représentant un soleil bleu (représenté dans le cercle en rouge sur l'image). Vous devriez avoir une nouvelle fenêtre sur votre écran de ce type :



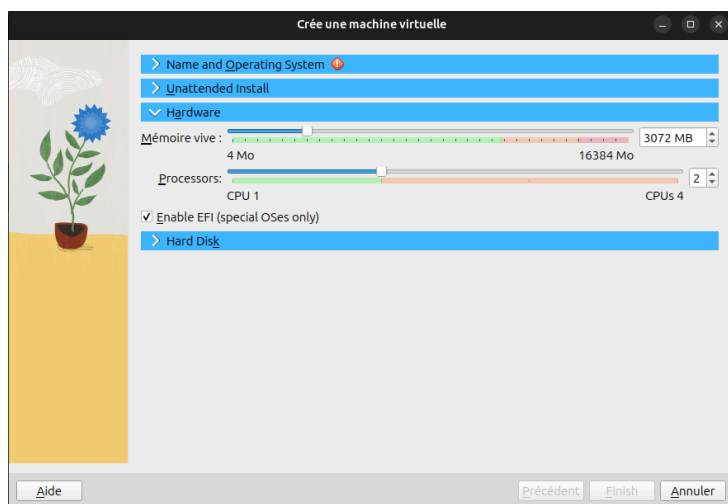
Cette fenêtre sert à configurer notre machine virtuelle en indiquant plusieurs paramètres comme son nom, quelle image disque lui attribuer, la RAM allouée à cette VM... Je vais vous montrer comment paramétrer cela pour notre serveur Debian puis vous pourrez ainsi l'adapter en fonction de vos besoins.

Commençons par la première partie de la configuration de la machine virtuelle en lui donnant un nom. C'est un nom qui va vous permettre de mieux identifier cette machine ainsi que son rôle dans votre quotidien. Vous pouvez mettre le nom qui vous chante. La case suivante est l'emplacement où va se stocker votre machine. Si vous avez un endroit bien spécifique ou si vous voulez les enregistrer vous pouvez le changer ici ou alors le laisser par défaut. A noter que vous pouvez également changer l'emplacement de la VM à l'avenir. ISO image est l'image disque que vous voulez attribuer à votre machine. Dans mon cas, ce sera l'image de Debian mais encore une fois, à personnaliser en fonction de votre choix. Enfin, à la suite de cela, virtualbox arrive à détecter par défaut les dernières rubriques qui sont "Type", "Version". Vous arrivez donc sur une petite case vous demandant si vous souhaitez ou non passer l'installation du système d'exploitation. Cette case est utilisée lors de la création d'une machine virtuelle (VM) pour contrôler le processus d'installation du système d'exploitation invité. Cette étape est facultative, vous pouvez très bien l'activer comme désactiver. Si vous désactivez, alors rendez-vous dans la 3ème rubrique pour paramétrer la suite de notre machine virtuelle. Tandis que si vous activez cette option, alors vous pouvez vous rendre dans la rubrique suivante pour paramétrer quelques informations comme le nom d'utilisateur à attribuer, son mot de passe...

Voici l'endroit où vous devez aller si vous avez activé l'option :

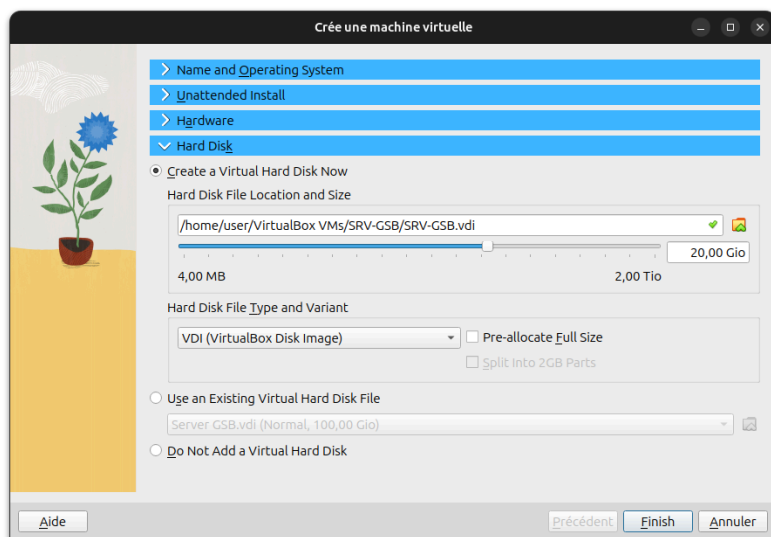


Voici là où vous devez vous rendre si vous désactivez l'option :

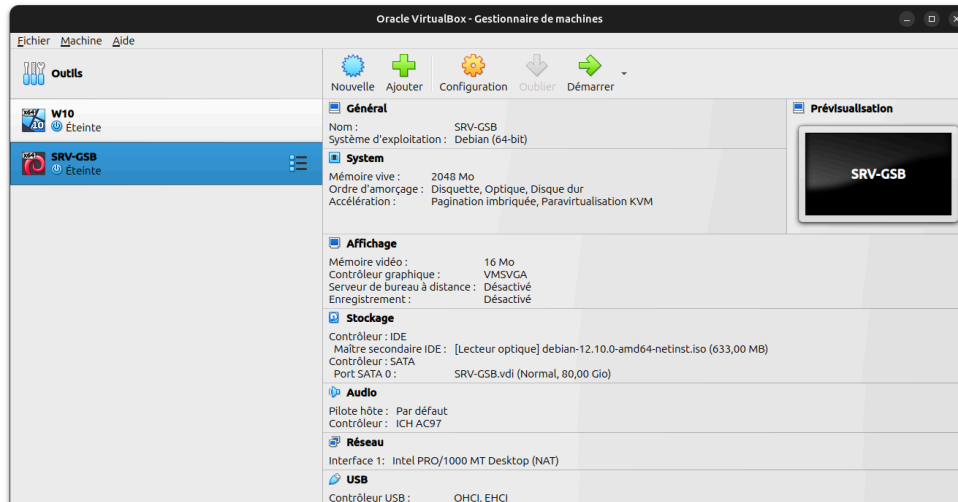


Rassurez-vous, l'endroit où nous nous situons, aussi la suite pour ceux qui ont activé l'option. Dans cette partie, nous pouvons décider de l'allocation de la RAM de notre VM ainsi que du nombre de cœurs. Il faut être précis durant cette étape, car il faut alors anticiper nos besoins en RAM et cœurs de processeur en fonction des tâches que l'on doit effectuer sur cette machine. Retenez juste que plus vous allouez de RAM et de cœur et plus votre VM est performante mais gourmande pour votre système hôte. Alors réfléchissez bien avant d'attribuer une valeur durant cette phase. Je vous conseille également de laisser la case cocher EFI, car de plus en plus de systèmes tournent sur ce mode de micrologiciel.

Enfin, dans la case suivante, vous pourrez créer si vous le souhaitez votre disque dur virtuel en choisissant sa taille ou alors en sélectionnant un déjà existant :



Il ne vous reste plus qu'à cliquer sur "Finish" puis votre machine virtuelle est bien créée, prête à être allumée :



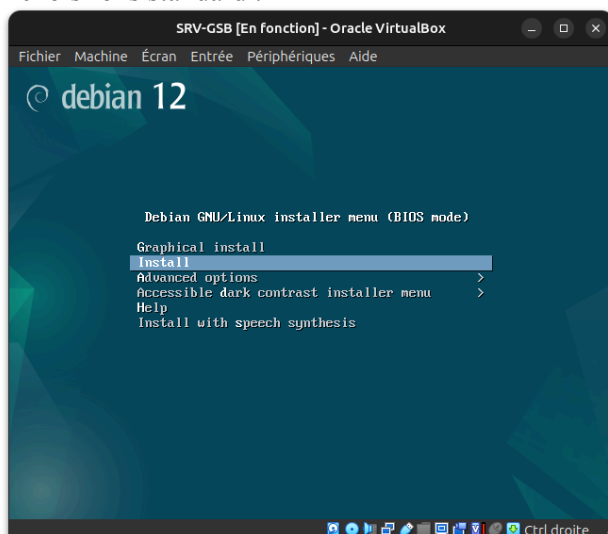
Vous voilà apte à créer autant de machines virtuelles qui vous plaisent en connaissant les paramètres à attribuer en fonction de vos machines à créer. Maintenant, nous allons procéder à l'installation de notre serveur web Debian.

## II. Installation de debian

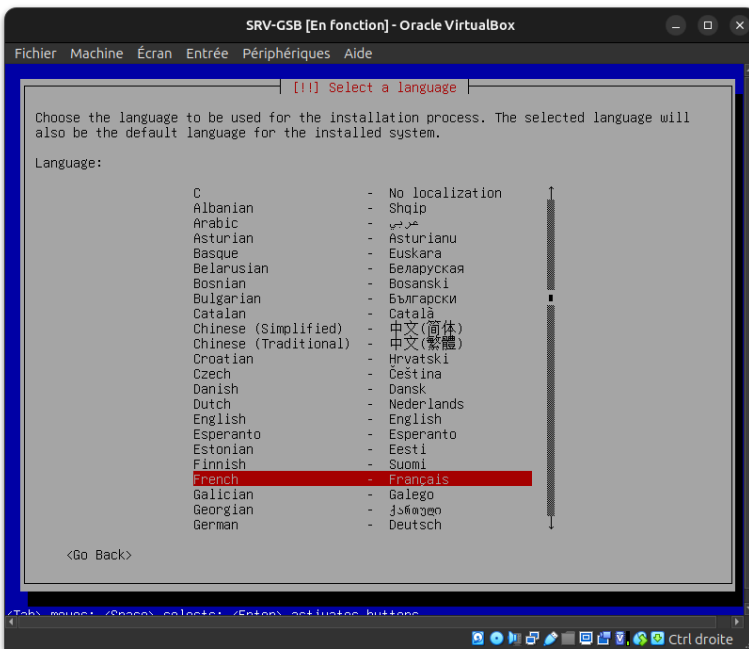
Pour lancer notre VM (virtual machine ou machine virtuelle en français), en la sélectionnant sur le panneau de nos vms dans VirtualBox, il faut lancer le démarrage soit en faisant un clic droit démarrer, soit en cliquant sur la flèche verte :



À la suite du démarrage de la VM, vous allez avoir une fenêtre vous indiquant par quels moyens souhaitez-vous installer Debian, soit avec la version dite graphique, soit avec l'installation standard. Nous choisirons standard :



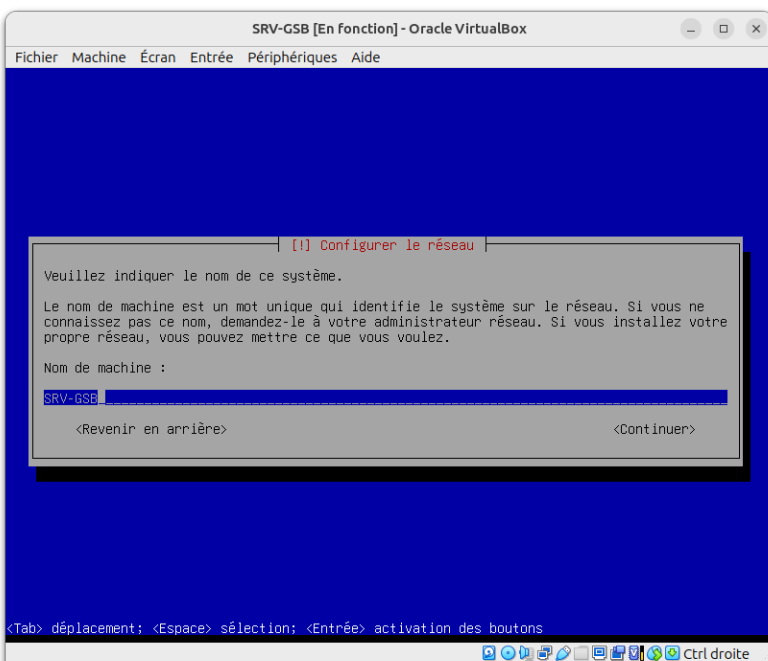
Une fois cliqué sur install, vous allez arriver sur le processus d'installation de Debian qui vous demandera plusieurs informations que l'on va détailler ici pour vous aider à comprendre. En premier lieu, vous allez avoir le choix de la langue du système, à savoir le français pour nous. Pour naviguer dans les menus, cela se fait avec les flèches donc nous allons aller jusqu'à la langue française (French en anglais) puis cliquer sur notre touche Entrer :



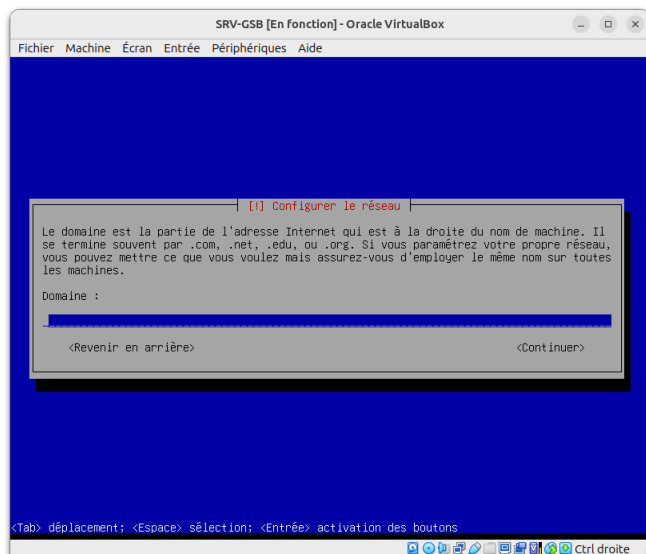
Le fuseau horaire à la langue nous sera alors demandé, par défaut laissé en France mais comme d'habitude, à réadapter en fonction de votre environnement :



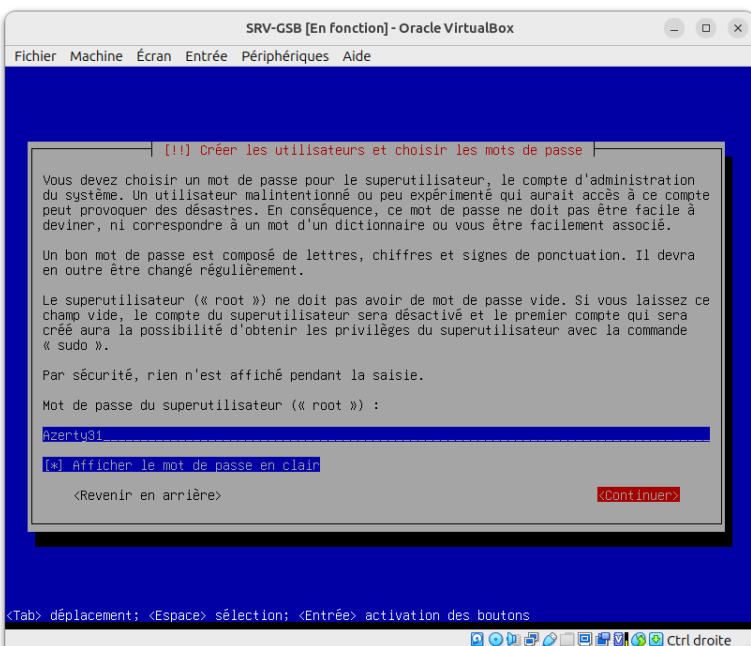
Viens ensuite la configuration de notre clavier. Il existe en effet plusieurs dispositions de clavier en fonction du pays. Nous allons choisir une disposition française pour que notre serveur soit adapté à notre clavier. Par la suite, nous arrivons sur le nom que l'on va donner à notre serveur. Pour notre cas à nous, nous rappellerons notre serveur "SRV-GSB" pour que ce soit plus simple à repérer dans le réseau :



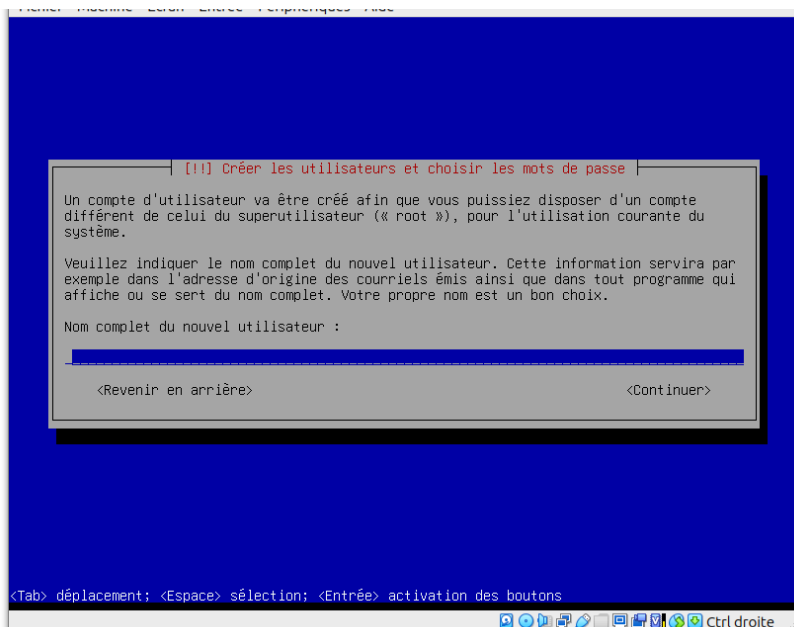
Si vous souhaitez que votre serveur soit rattaché à un nom de domaine de l'entreprise alors c'est dans l'étape suivante que vous allez pouvoir le mettre sinon si vous voulez le mettre plus tard vous pouvez très bien ne rien mettre durant cette étape :



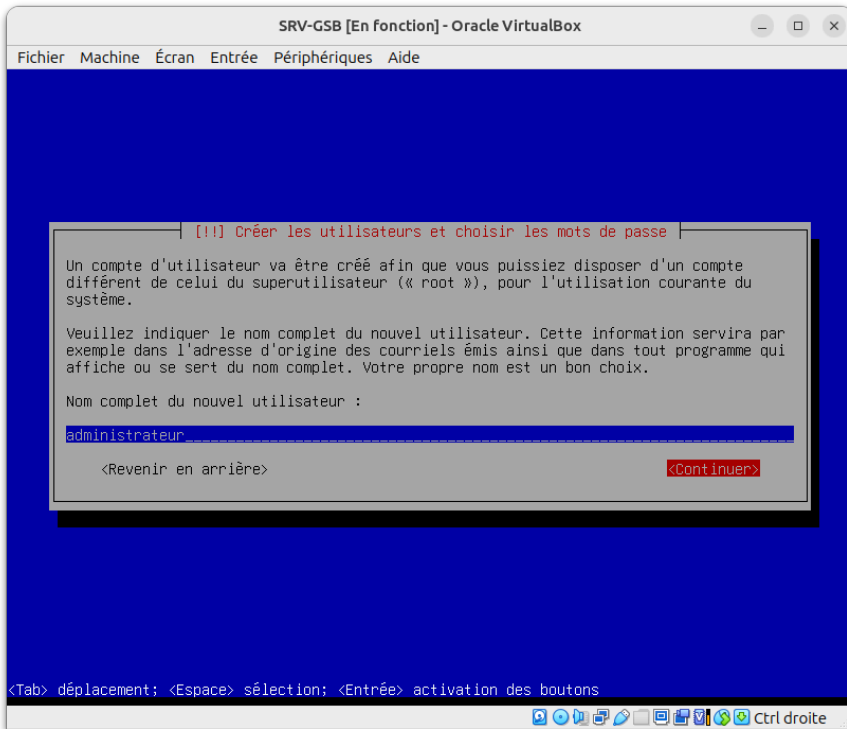
Par la suite, viennent les utilisateurs et nous allons commencer par attribuer un mot de passe au superutilisateur dit root sur Linux. Le root est un compte dédié principalement à l'administration système, il dispose d'un contrôle total sur l'ensemble du système d'exploitation. Le cahier des charges impose que le mot de passe root soit "Azerty31" :



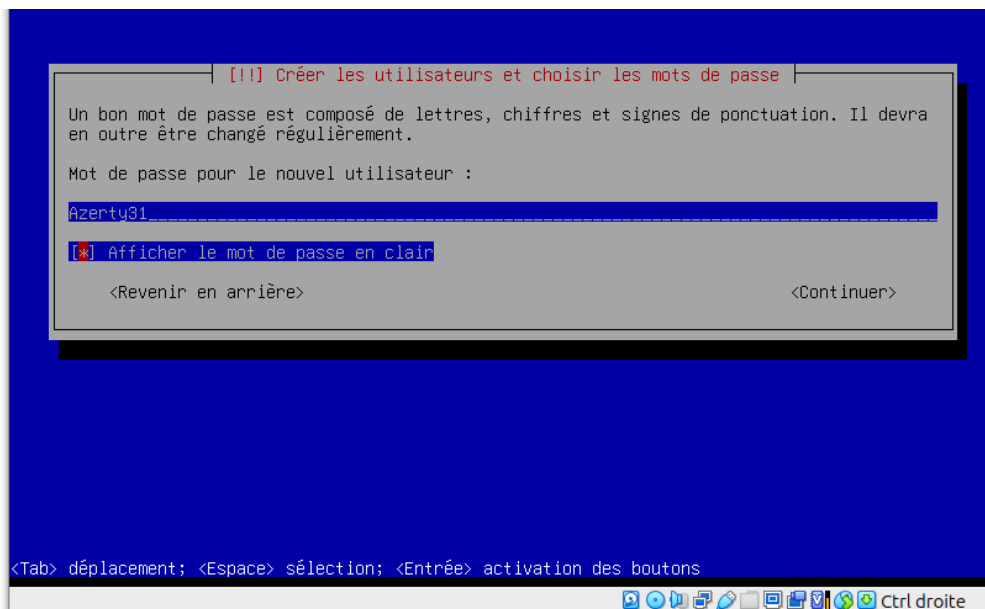
Une seconde fenêtre apparaîtra vous demandera de confirmer le mot de passe root. Vous allez arriver maintenant sur la page de création cette fois-ci du 1er utilisateur. La 1ère fenêtre va indiquer le nom de l'utilisateur (pour notre part Admin) :



Vient ensuite l'identifiant que l'on souhaite appliquer à notre utilisateur. Généralement, cela est la même chose que votre nom d'utilisateur à la différence que celui-ci est écrit en minuscule mais vous pouvez très bien le changer avec un identifiant différent. Pour notre cas cela va être administrateur notre identifiant car admin est déjà réservé par root :



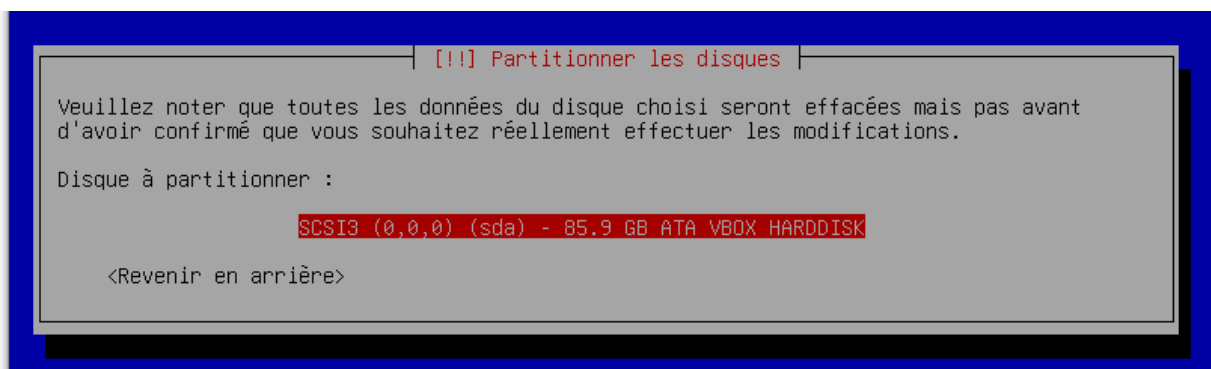
Ensuite, le logiciel d'installation nous demandera le mot de passe de votre utilisateur soit "Azerty31" pour nous :



Comme pour le mot de passe root, le système va nous demander de confirmer le mot de passe avant de poursuivre l'installation. Nous arrivons maintenant dans la rubrique du disque dur. Plus précisément dans le partitionnement du disque dur. Le système nous propose 3 options :

- Partitionnement assisté
- Partitionnement assisté avec un LVM chiffré ou non (Local Volume Management). LVM est un outil qui permet la création et la gestion de volumes logiques sous Linux.
- Partitionnement Manuel

Nous choisirons un partitionnement pour ce cas-là. À noter également que si vous choisissez le partitionnement manuel, je vous conseille de vous aider d'un guide à côté de vous pour mieux comprendre comment fractionner votre disque. Vous allez ensuite sélectionner votre disque dur si vous en avez plusieurs qui va accueillir le système d'exploitation :



Vient ensuite une liste d'options lors de votre partitionnement vous indiquant si vous souhaitez séparer plusieurs fichiers. Ces fichiers sont :

- Tout dans une seule partition (recommandé pour les débutants) : Cette option crée une seule partition pour l'ensemble du système de fichiers. C'est la solution la plus simple et la plus facile à gérer pour les utilisateurs débutants.
- Partition /home séparée : Cette option crée une partition séparée pour le répertoire /home, où se trouvent les fichiers personnels des utilisateurs. Cela permet de séparer les données utilisateur du système de fichiers principal, ce qui peut être utile pour la sauvegarde et la gestion des données.
- Partitions /home, /var et /tmp séparées : Cette option crée des partitions séparées pour les répertoires /home, /var et /tmp. Cela permet une gestion plus fine des ressources et peut améliorer la performance et la sécurité du système.

## Avantages de la Séparation des Partitions dans un Système de Fichiers Linux

Catégorie	Avantage	Description
Gestion des ressources	Isolation des données	En séparant les répertoires comme <code>/home</code> , <code>/var</code> et <code>/tmp</code> , vous pouvez mieux gérer l'espace disque et éviter que des fichiers volumineux dans une partition n'affectent les autres parties du système.
	Performance	Certaines partitions peuvent être montées avec des options spécifiques pour améliorer les performances, comme l'utilisation de systèmes de fichiers différents ou de paramètres de montage spécifiques.
Sécurité	Confinement des données	En isolant les répertoires sensibles comme <code>/tmp</code> (où les fichiers temporaires sont stockés), vous pouvez réduire les risques de sécurité. Par exemple, si <code>/tmp</code> est compromis, les autres parties du système restent intactes.
	Sauvegarde et restauration	La séparation des données utilisateur ( <code>/home</code> ) et des données système ( <code>/</code> ) facilite les opérations de sauvegarde et de restauration. Vous pouvez sauvegarder et restaurer les données utilisateur indépendamment du système d'exploitation.
Maintenance	Mise à jours	Si vous devez réinstaller le système d'exploitation, avoir une partition séparée pour <code>/home</code> permet de conserver les données utilisateur intactes.
	Dépannage	En cas de problème avec le système de fichiers principal, les partitions séparées peuvent être montées et vérifiées indépendamment, facilitant ainsi le dépannage.

Nous allons choisir la 3ème option que nous propose le système, ce qui nous permettra de gérer au mieux les ressources de notre disque dur tout en garantissant une performance accrue, mais aussi une meilleure sécurité. Le système va alors nous proposer un partitionnement en rapport avec l'option choisie précédemment, mais vous pouvez tout à fait revenir en arrière pour le partitionner manuellement ou alors modifier le partitionnement proposé pour qu'il corresponde mieux à vos attentes. Une fois que vos modifications ont été réalisées ou non, vous n'avez plus qu'à cliquer sur la dernière case tout en bas pour confirmer le partitionnement :

```

[!!] Partitionner les disques

Voici la table des partitions et les points de montage actuellement configurés. Vous
pouvez choisir une partition et modifier ses caractéristiques (système de fichiers, point
de montage, etc.), un espace libre pour créer une nouvelle partition ou un périphérique
pour créer sa table des partitions.

Partitionnement assisté
Configurer le RAID avec gestion logicielle
Configurer le gestionnaire de volumes logiques (LVM)
Configurer les volumes chiffrés
Configurer les volumes iSCSI

SCSI3 (0,0,0) (sda) - 85.9 GB ATA VBOX HARDDISK
n° 1 primaire 16.3 GB f ext4 /
n° 5 logique 5.8 GB f ext4 /var
n° 6 logique 1.0 GB f swap swap
n° 7 logique 1.0 GB f ext4 /tmp
n° 8 logique 61.8 GB f ext4 /home

Annuler les modifications des partitions
Terminer le partitionnement et appliquer les changements

<Revenir en arrière>
```

Une seconde fenêtre va apparaître pour confirmer une seconde fois notre partitionnement :

```

[!!] Partitionner les disques

Si vous continuez, les modifications affichées seront écrites sur les disques. Dans le
cas contraire, vous pourrez faire d'autres modifications.

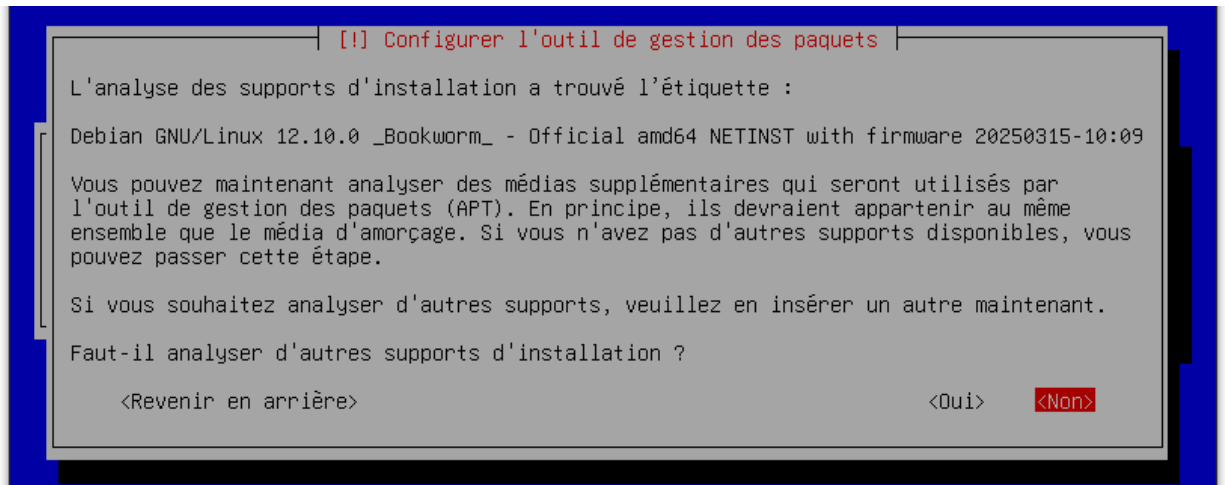
Les tables de partitions des périphériques suivants seront modifiées :
SCSI3 (0,0,0) (sda)

Les partitions suivantes seront formatées :
partition n° 1 sur SCSI3 (0,0,0) (sda) de type ext4
partition n° 5 sur SCSI3 (0,0,0) (sda) de type ext4
partition n° 6 sur SCSI3 (0,0,0) (sda) de type swap
partition n° 7 sur SCSI3 (0,0,0) (sda) de type ext4
partition n° 8 sur SCSI3 (0,0,0) (sda) de type ext4

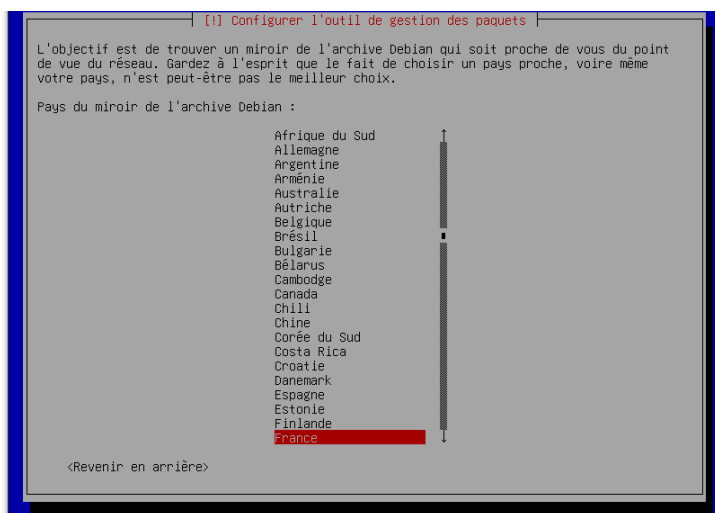
Faut-il appliquer les changements sur les disques ?

<Oui> <Non>
```

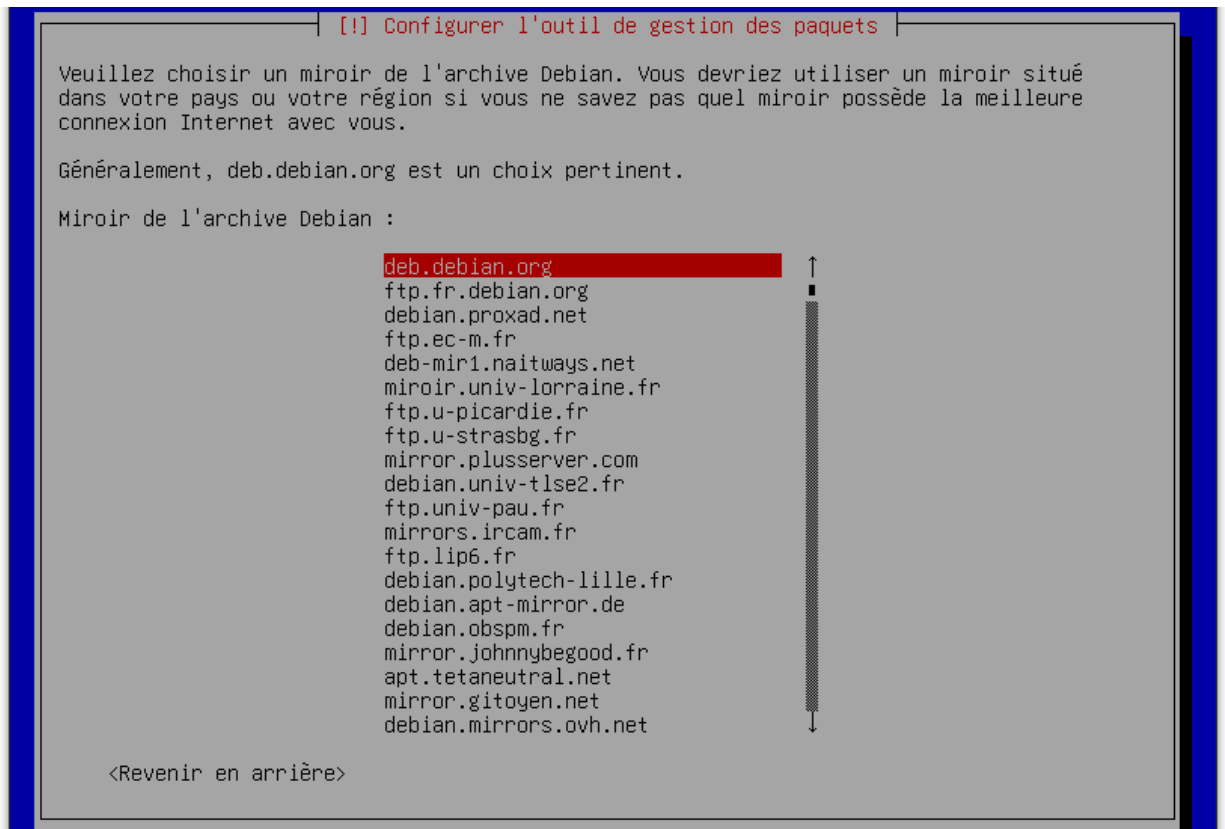
L'installation va alors commencer jusqu'à arriver à la configuration de l'outil de gestion de paquets. C'est un outil essentiel à un système d'exploitation basé sur Linux car il va permettre de faciliter l'installation, la configuration, la mise à jour et la suppression de logiciels ou de bibliothèques sur le système. Il est donc important de le configurer au mieux pour faciliter la maintenance du système par la suite. Alors, arriver sur cette page-ci :



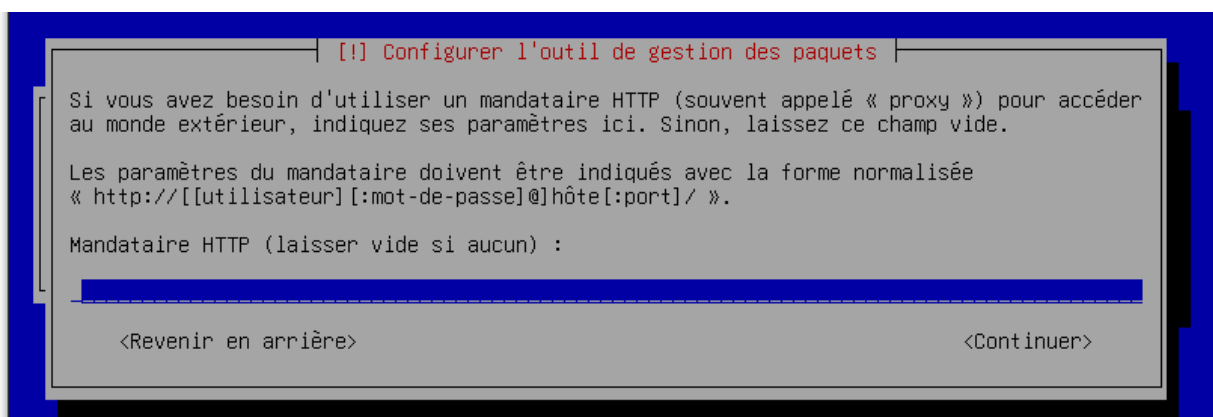
Si vous souhaitez analyser d'autres supports, faites oui pour en sélectionner davantage ou alors faites non pour ignorer cette étape. Vous pouvez très bien les rajouter à la suite de l'installation (cf : page 25). Lorsque vous cliquez sur non, le système va alors vous présenter une liste pour choisir quel dépôt mettre sur votre système. Un dépôt est un lieu de stockage où sont enregistrées un ensemble d'applications prévues pour le système. Sur Debian, il en existe beaucoup. Ils sont triés par pays et dans la zone géographique du pays sélectionné si on veut se rapprocher le plus d'un dépôt proche de chez nous. Pour notre serveur, nous allons choisir les dépôts de Debian France en les sélectionnant dans la liste proposée, mais vous pouvez très bien choisir un dépôt proche de chez vous.:



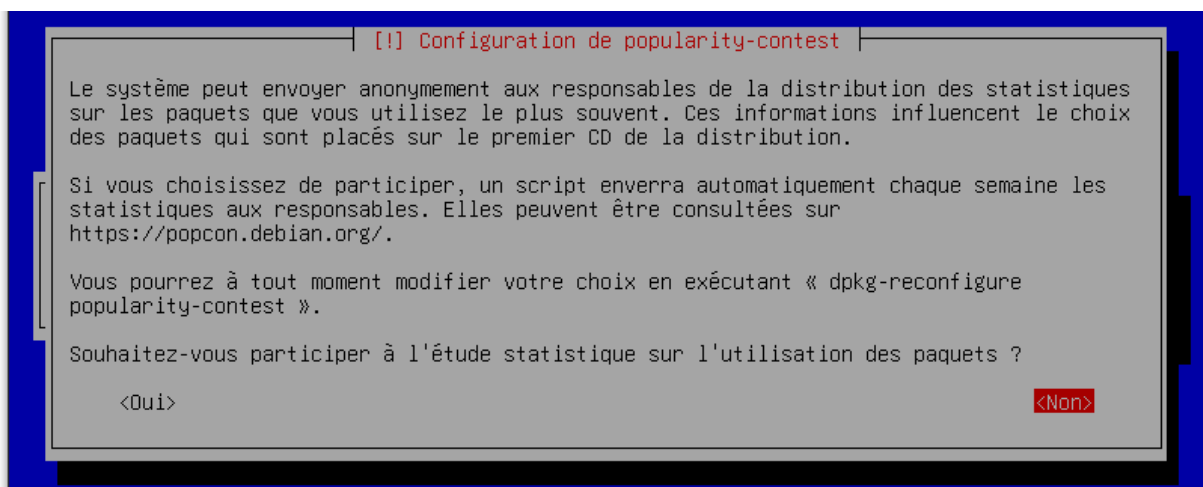
Puis, choisissez le 1er dépôt pour avoir le dépôt *deb.debian.org* pour que le dépôt soit rattaché à votre système :



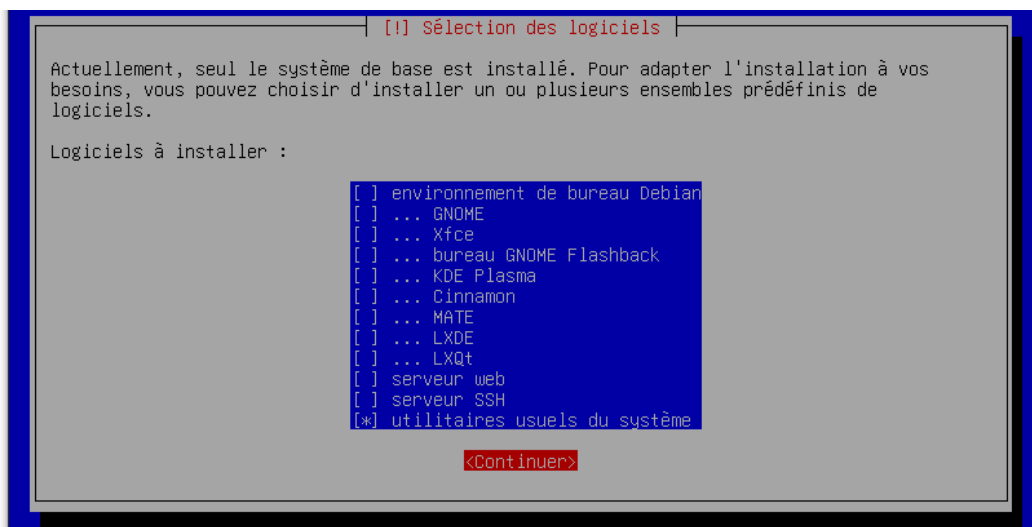
Le système va alors vous demander si, dans le cas où il existe un mandataire (serveur proxy) installé chez vous, de le renseigner et si vous n'en avez aucun, alors vous laissez le champ vide :



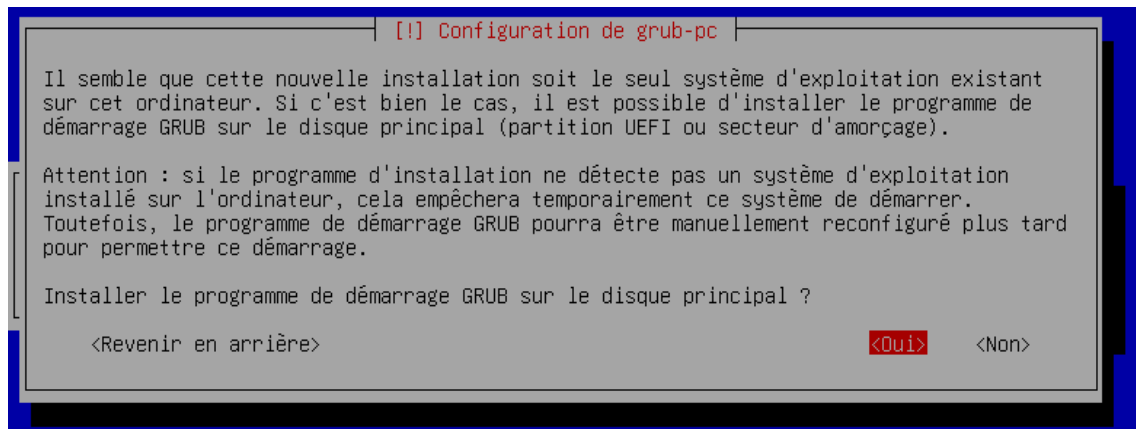
Nous voilà presque à la fin de l'installation de Debian. Le système va alors nous proposer d'envoyer anonymement différentes données au responsable de la distribution. Nous allons mettre non :



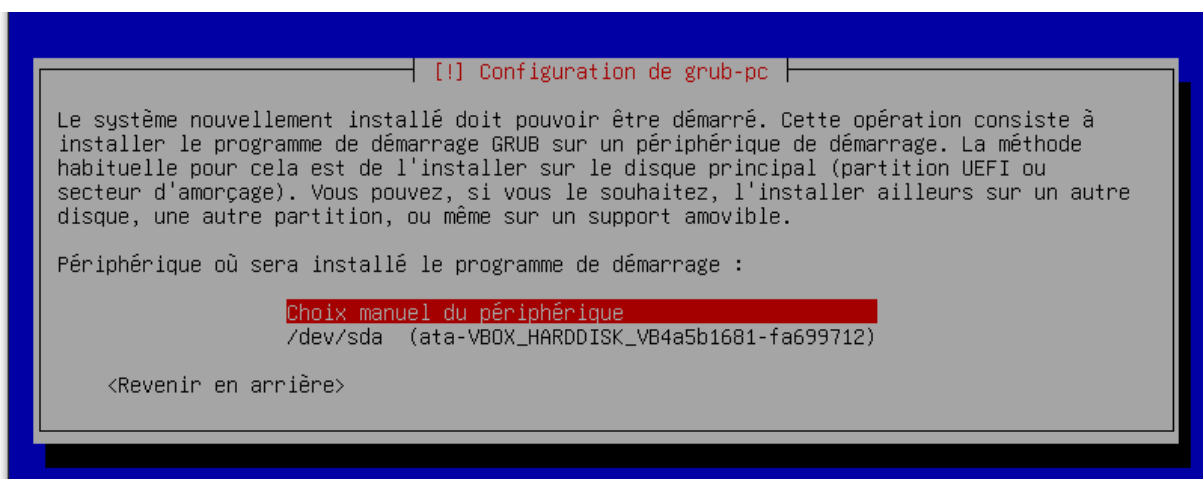
Nous arrivons au choix de l'environnement de bureau de votre système d'exploitation. Il existe 2 modes d'utilisation de Debian, à savoir le mode graphique qui existe avec plusieurs environnements de bureau et le mode core, soit l'ensemble des actions à réaliser se font via une interface shell ( en ligne de commande). Je vous conseille, si vous ne vous y connaissez pas trop dans l'architecture Linux, l'environnement graphique qui sera mieux adapté pour un utilisateur débutant que le mode core. Je vous conseille également de prendre un environnement de bureau assez léger pour votre serveur pour qu'il ne soit pas lourd à faire tourner par votre système. L'environnement XFCE est léger et stable et serait très bien pour un serveur. Sinon, pour ne pas avoir d'environnement de bureau, arriver à cette fenêtre-ci, vous désactivez l'ensemble des options sauf le dernier. Pour les désactiver, naviguez à l'aide des flèches puis tapez sur barre espace pour enlever l'étoile sur les options à activer/désactiver (une étoile sur une option indique qu'elle est active):




Une fois vos options sélectionnées, vous descendez tout en bas à l'aide de la flèche du bas pour arriver sur l'option "Confirmer" puis appuyez sur la touche Entrer de votre clavier. L'installation se poursuivra jusqu'à une fenêtre vous demandant si vous voulez installer le programme de démarrage GRUB. GRUB est un programme de démarrage de micro-ordinateur qui s'exécute après les séquences de contrôle interne et avant le système d'exploitation. Il permet à l'utilisateur de choisir quel système d'exploitation démarrer. Nous allons l'installer en prenant comme disque dur ou l'installer celui où l'on a installé notre système d'exploitation :



Choix du disque dur ou installer GRUB :



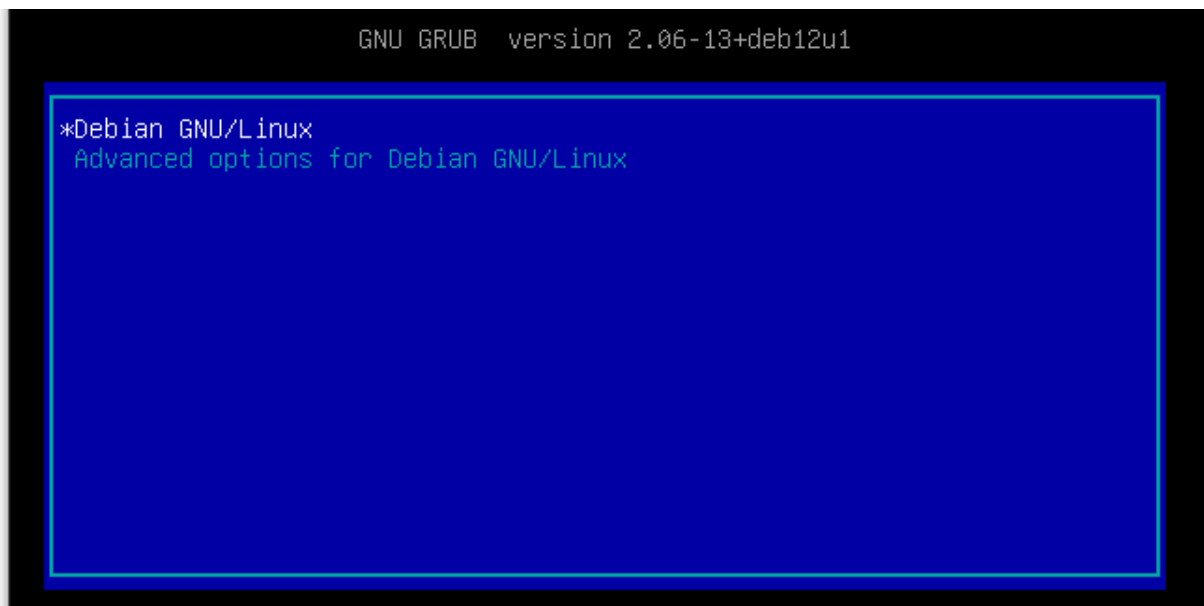


L'installation est maintenant terminée, vous n'avez plus qu'à continuer, puis votre système va redémarrer tout seul. Après le redémarrage, si Virtualbox ne l'a pas déjà fait, vous pouvez enlever le lecteur CD virtuel pour éviter que l'installateur de Debian recommence. Pour ce faire, quand vous êtes sur votre VM, allez sur l'onglet périphériques / lecteur optique puis faites la dernière option proposée indiquant d'exclure le CD virtuel de votre VM.

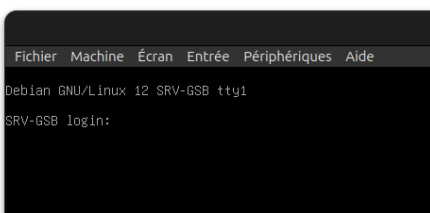
### III. Configuration de debian

Lors de votre 1er démarrage de votre VM, vous allez arriver sur le GRUB installé précédemment vous demandant de choisir sur quel système souhaitez-vous aller. Si ce n'est pas le cas et que votre système ne se lance pas, alors je vous conseille de refaire l'installation de Debian en reprenant les étapes du dessus.

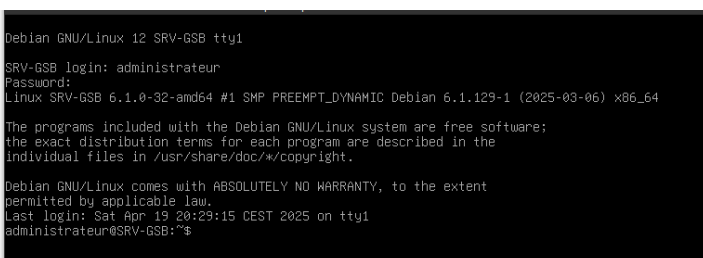
Voici l'écran du GRUB :



Une fois que vous avez cliqué sur *Debian GNU/Linux*, vous arrivez sur une fenêtre de connexion vous demandant de vous authentifier avec l'utilisateur que vous avez créés précédemment ainsi que de son mot de passe :



Une fois votre authentification réussie, vous êtes bien connecté à votre système Debian :



La première étape est de vérifier vos mises à jour. Pour cela, vous devrez vous connecter avec le compte de superutilisateur (root). Pour se connecter avec le compte root, il faut effectuer la commande suivante :

su -

mdp root

Cela va alors nous connecter non plus avec notre utilisateur précédemment configuré, mais avec le superutilisateur disposant de tous les privilèges du système. Ce qui donne ceci en image :

```
SRV-GSB login: administrateur
Password:
Linux SRV-GSB 6.1.0-32-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.129-1 (2025-03-06) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Apr 21 12:24:41 CEST 2025 on tty1
administrateur@SRV-GSB:~$ su -
Mot de passe :
su: Échec de l'authentification
administrateur@SRV-GSB:~$ su -
Mot de passe :
root@SRV-GSB:~#
```

En ce qui concerne la mise à jour des paquets, il faut saisir 2 commandes à savoir :

apt update (Télécharge les paquets qui doivent être mis à jour)

apt upgrade (installe les paquets précédemment téléchargés qui doivent faire une mise à jour)

Vous pouvez les saisir séparément ou alors en faire qu'une seule commande en mettant “&&” à la fin de update :

```
root@SRV-GSB:~# apt update && apt upgrade
Atteint :1 http://deb.debian.org/debian bookworm InRelease
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Tous les paquets sont à jour.
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Calcul de la mise à jour... Fait
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@SRV-GSB:~#
```

Si vous n'arrivez pas à effectuer la mise à jour de vos paquets, cela provient peut-être de vos dépôts mal renseignés. Pour vérifier cela, il faut se rendre dans le fichier de configuration des dépôts pour régler ce problème. Le fichier de configuration se nomme “source.list”. La commande nano sert à éditer un fichier

texte en ligne de commande, ce qui sera pratique pour vérifier le contenu présent dans ce fichier de configuration. La commande Linux à saisir est de ce format : nano /etc/apt/sources.list :

```
GNU nano 7.2 /etc/apt/sources.list
#deb cdrom:[Debian GNU/Linux 12.10.0 _Bookworm_ - Official amd64 NETINST with f
deb http://deb.debian.org/debian/ bookworm main non-free-firmware
deb-src http://deb.debian.org/debian/ bookworm main non-free-firmware
# Line commented out by installer because it failed to verify:
deb http://security.debian.org/debian-security bookworm-security main non-free-
# Line commented out by installer because it failed to verify:
deb-src http://security.debian.org/debian-security bookworm-security main non-f
# bookworm-updates, to get updates before a point release is made;
# see https://www.debian.org/doc/manuals/debian-reference/ch02.en.html#_updates
# Line commented out by installer because it failed to verify:
deb http://deb.debian.org/debian/ bookworm-updates main non-free-firmware
# Line commented out by installer because it failed to verify:
deb-src http://deb.debian.org/debian/ bookworm-updates main non-free-firmware
# This system was installed using small removable media
# (e.g. netinst, live or single CD). The matching "deb cdrom"
# entries were disabled at the end of the installation process.
[ Lecture de 22 lignes ]
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^_ Remplacer  ^U Coller    ^J Justifier ^/ Aller ligne
```

Nous allons maintenant passer à la création des utilisateurs de notre système d'exploitation. En effet, si les développeurs veulent mettre à jour le site web, alors il faut leur donner l'accès dans un premier temps en leur attribuant un identifiant et un mot de passe. Le cahier des charges nous demande de "Autant de compte qu'il y a de membres de l'équipe".

Donc, il faut créer 1 identifiant par développeur et admin réseau. La commande sous Linux pour créer des utilisateurs est la commande adduser suivie du nom d'utilisateur souhaité. Donc en tapant la commande (si possible en superutilisateur soit root en l'appelant avec su - ) vous avez ceci comme réponse :

```

Debian GNU/Linux 11 debian tty1

debian login: root
Password:
Linux debian 5.10.0-34-amd64 #1 SMP Debian 5.10.234-1 (2025-02-24) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Apr 10 15:14:31 CEST 2025 on tty1
root@debian:~# ls /home/
admin irache nana
root@debian:~# adduser deva-1
Ajout de l'utilisateur « deva-1 » ...
Ajout du nouveau groupe « deva-1 » (1007) ...
Ajout du nouvel utilisateur « deva-1 » (1004) avec le groupe « deva-1 » ...
Création du répertoire personnel « /home/deva-1 »...
Copie des fichiers depuis « /etc/skel »...
Nouveau mot de passe : _

```

Le système va alors demander le mot de passe que vous souhaitez mettre à cet utilisateur. Pour nous, ce sera “Azerty31”. Puis le système va alors vous demander plusieurs autres informations qui ne sont pas nécessaires pour le bon fonctionnement de l'utilisateur (n° téléphone, pays...) Appuyez juste sur entrée pour confirmer. Cela voudra dire que vous ne souhaitez rien mettre sur cette case. Vous pouvez utiliser plutôt la commande `useradd` pour éviter ce style d'information, mais vous devrez mettre un nom de passe en utilisateur, la commande `pwd nom d'utilisateur`. Voici la différence entre les 2 sur votre terminal, choisissez ce qui vous convient le mieux :

```

root@debian:~# adduser deva-1
Ajout de l'utilisateur « deva-1 » ...
Ajout du nouveau groupe « deva-1 » (1007) ...
Ajout du nouvel utilisateur « deva-1 » (1004) avec le groupe « deva-1 » ...
Création du répertoire personnel « /home/deva-1 »...
Copie des fichiers depuis « /etc/skel »...
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd: password updated successfully
Changing the user information for deva-1
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Cette information est-elle correcte ? [0/n]
root@debian:~# us
usb-devices  usbhid-dump  usbreset    useradd      userdel      usermod      users
root@debian:~# useradd devb-1
root@debian:~# passwd dev
deva-1  devb-1
root@debian:~# passwd devb-1
Nouveau mot de passe :
Retapez le nouveau mot de passe :
passwd: password updated successfully

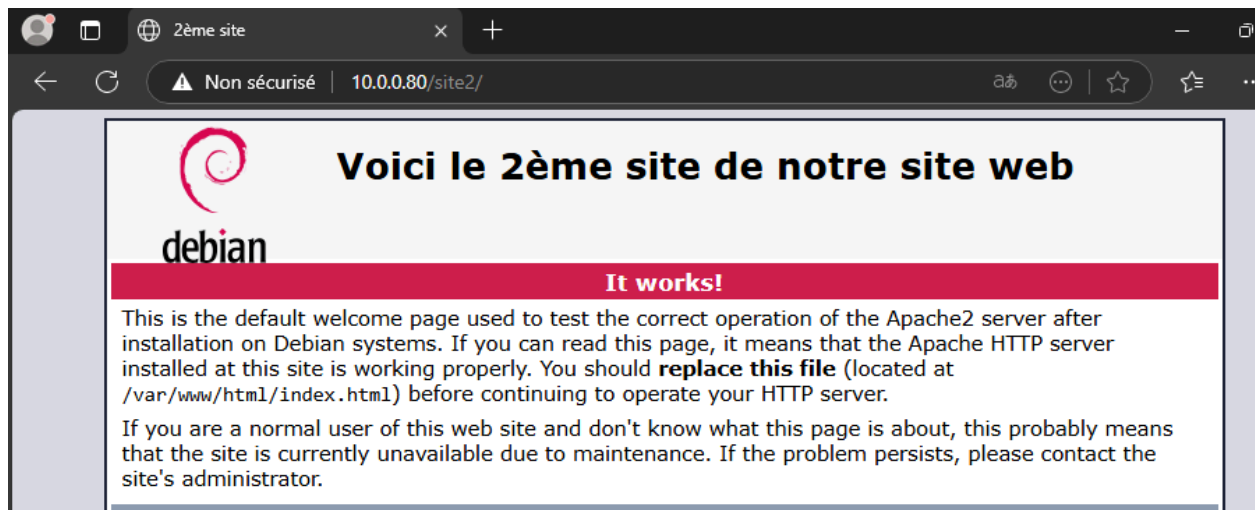
```

Une fois tous les utilisateurs créés, nous allons maintenant passer à l'installation des différents modules de notre serveur web. Pour cela, nous allons installer un LAMP. LAMP est un acronyme qui désigne un ensemble de technologies logicielles utilisées pour créer des sites web et des applications web. LAMP signifie Linux, Apache, MySQL et PHP.

Dans un premier temps, nous installons le module Apache qui permettra à notre serveur d'afficher des pages web. La commande pour l'installer est très simple :

```
apt install apache2 -y
```

Une fois installé, vous pouvez tester votre site web en tapant sur un navigateur l'@IP de votre serveur pour afficher la page par défaut d'apache :



Vous voilà avec Apache qui est installé sur votre serveur, nous allons maintenant passer à l'installation de MariaDB pour accueillir des bases de données. La commande pour l'installer est `apt install mariadb-server` :

```

root@debian:~# apt install mariadb-server
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
Le paquet suivant a été installé automatiquement et n'est plus nécessaire :
 linux-image-5.10.0-8-amd64
Veuillez utiliser « apt autoremove » pour le supprimer.
Les paquets supplémentaires suivants seront installés :
 galera-4 gawk libcgi-fast-perl libcgi-pm-perl libclone-perl libconfig-inifiles-perl
 libdbd-mariadb-perl libdbi-perl libencode-locale-perl libfcgi-bin libfcgi-perl libfcgi01db1
 libhtml-parser-perl libhtml-tagset-perl libhtml-template-perl libhttp-date-perl
 libhttp-message-perl libio-html-perl liblwp-mediatypes-perl libmariadb3 libmpfr6 libsigsegv2
 libsnappy1v5 libterm-readkey-perl libtimedate-perl liburi-perl mariadb-client-10.5
 mariadb-client-core-10.5 mariadb-common mariadb-server-10.5 mariadb-server-core-10.5
 mysql-common psmisc rsync socat
Paquets suggérés :
 gawk-doc libltdb-perl libnet-daemon-perl libsql-statement-perl libdata-dump-perl
 libipc-sharedcache-perl libwww-perl mailx mariadb-test netcat-openbsd
Les NOUVEAUX paquets suivants seront installés :
 galera-4 gawk libcgi-fast-perl libcgi-pm-perl libclone-perl libconfig-inifiles-perl
 libdbd-mariadb-perl libdbi-perl libencode-locale-perl libfcgi-bin libfcgi-perl libfcgi01db1
 libhtml-parser-perl libhtml-tagset-perl libhtml-template-perl libhttp-date-perl
 libhttp-message-perl libio-html-perl liblwp-mediatypes-perl libmariadb3 libmpfr6 libsigsegv2
 libsnappy1v5 libterm-readkey-perl libtimedate-perl liburi-perl mariadb-client-10.5
 mariadb-client-core-10.5 mariadb-common mariadb-server mariadb-server-10.5
 mariadb-server-core-10.5 mysql-common psmisc rsync socat
0 mis à jour, 36 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 20,0 Mo dans les archives.
Après cette opération, 164 Mo d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] O

```

Faites oui pour confirmer l'installation de mariadb sur votre serveur. À la suite de l'installation de mariadb, nous allons configurer la sécurité de notre installation avec la commande mariadb-secure-installation. Ce paquet permet plusieurs choses, notamment de définir un mot de passe pour le compte "root" de MariaDB, d'empêcher les connexions distantes sur votre instance à l'aide du compte "root", d'empêcher les connexions anonymes et de supprimer la base de test. Voici un détail des options réalisées sur cette installation :

```
Switch to unix_socket authentication [Y/n] n
... skipping.

You already have your root account protected, so you can safely answer 'n'.

Change the root password? [Y/n] Y
New password: *****
Re-enter new password: *****
Password updated successfully!
Reloading privilege tables..
... Success!

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] y
... Success!

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] y
... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] y
- Dropping test database...
... Success!
- Removing privileges on test database...
... Success!

Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n] y
Success!
```

Nous pouvons tester la connexion en tapant la commande mariadb -u root -p, en saisissant par la suite le mot de passe root tapé juste avant :

```
root@debian:~# mariadb -uroot -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 38
Server version: 10.5.28-MariaDB-0+deb11u1 Debian 11

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

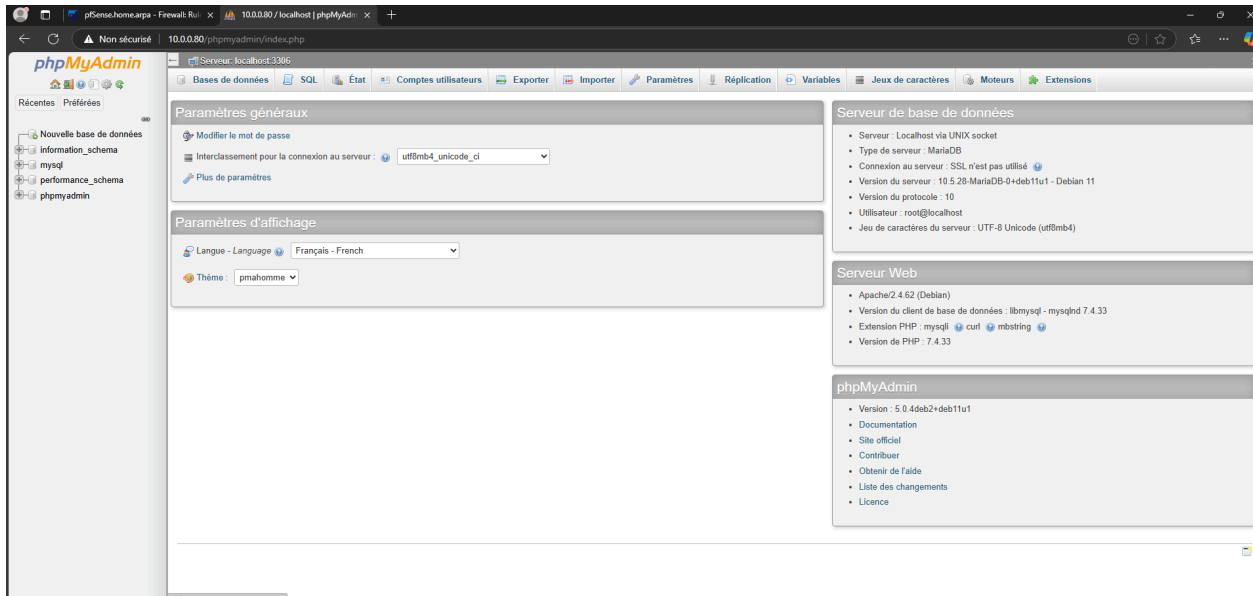
MariaDB [(none)]> _
```

Vous voilà avec mariadb d'installé sur votre serveur, si vous n'êtes pas à l'aise avec la ligne de commande, vous pouvez très bien installer phpmyadmin pour avoir une interface graphique en faisant *apt install phpmyadmin* et taper dans votre navigateur l'*@IP*. Une fois le paquet de phpmyadmin, vous devrez installer par la suite le module php qui va permettre d'avoir l'interface graphique :

```
Paquets suggérés :
  php-pear
Les NOUVEAUX paquets suivants seront installés :
  libapache2-mod-php7.4 php php7.4
0 mis à jour, 3 nouvellement installés, 0 à enlever et 0 non mis à jour.
Il est nécessaire de prendre 1 434 ko dans les archives.
Après cette opération, 4 813 ko d'espace disque supplémentaires seront utilisés.
Souhaitez-vous continuer ? [O/n] O
Réception de :1 http://deb.debian.org/debian-security bullseye-security/main amd64 libapache2-mod-p
b7.4 amd64 7.4.33-1+deb11u8 [1 376 kB]
Réception de :2 http://deb.debian.org/debian-security bullseye-security/main amd64 php7.4 all 7.4.3
-1+deb11u8 [52,1 kB]
Réception de :3 http://deb.debian.org/debian bullseye/main amd64 php all 2:7.4+76 [6 340 B]
1 434 ko réceptionnés en 28s (50,8 ko/s)
Sélection du paquet libapache2-mod-php7.4 précédemment désélectionné.
(Lecture de la base de données... 67516 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de ../libapache2-mod-php7.4_7.4.33-1+deb11u8_amd64.deb ...
Dépaquetage de libapache2-mod-php7.4 (7.4.33-1+deb11u8) ...
Sélection du paquet php7.4 précédemment désélectionné.
Préparation du dépaquetage de ../php7.4_7.4.33-1+deb11u8_all.deb ...
Dépaquetage de php7.4 (7.4.33-1+deb11u8) ...
Sélection du paquet php précédemment désélectionné.
Préparation du dépaquetage de ../php_2%3a7.4+76_all.deb ...
Dépaquetage de php (2:7.4+76) ...
Paramétrage de libapache2-mod-php7.4 (7.4.33-1+deb11u8) ...

Creating config file /etc/php/7.4/apache2/php.ini with new version
Module mpm_event disabled.
Enabling module mpm_prefork.
apache2_switch_mpm Switch to prefork
apache2_invoke: Enable module php7.4
Paramétrage de php7.4 (7.4.33-1+deb11u8) ...
Paramétrage de php (2:7.4+76) ...
Traitement des actions différées (« triggers ») pour libapache2-mod-php7.4 (7.4.33-1+deb11u8) ...
root@debian:~# _
```

Puis en tapant sur votre navigateur internet *@IP* de la machine/phpmyadmin/ vous devriez avoir une fenêtre comme ceci :



Pour gagner du temps, nous allons importer la base de données de gsb directement via phpmyadmin en allant sur la rubrique importer pour arriver sur cette fenêtre :

#### Importation dans le serveur courant

##### Fichier à importer :

Le fichier peut être compressé (gzip, bzip2, zip) ou non.

Le nom du fichier compressé doit se terminer par `.[format].[compression]`. Exemple : `.sql.zip`

Parcourir les fichiers :  Aucun fichier n'a été sélectionné (Taille maximale : 2 048kio)

Il est également possible de glisser-déposer un fichier sur n'importe quelle page.

Jeu de caractères du fichier :

##### Importation partielle :

Permettre l'interruption de l'importation si la limite de temps configurée dans PHP est sur le point d'être atteinte. (Ceci pourrait aider à importer des fichiers volumineux, au détriment du respect des transactions.)

Ignorer ce nombre de requêtes (pour SQL), à partir du début :

##### Autres options :

Activer la vérification des clés étrangères

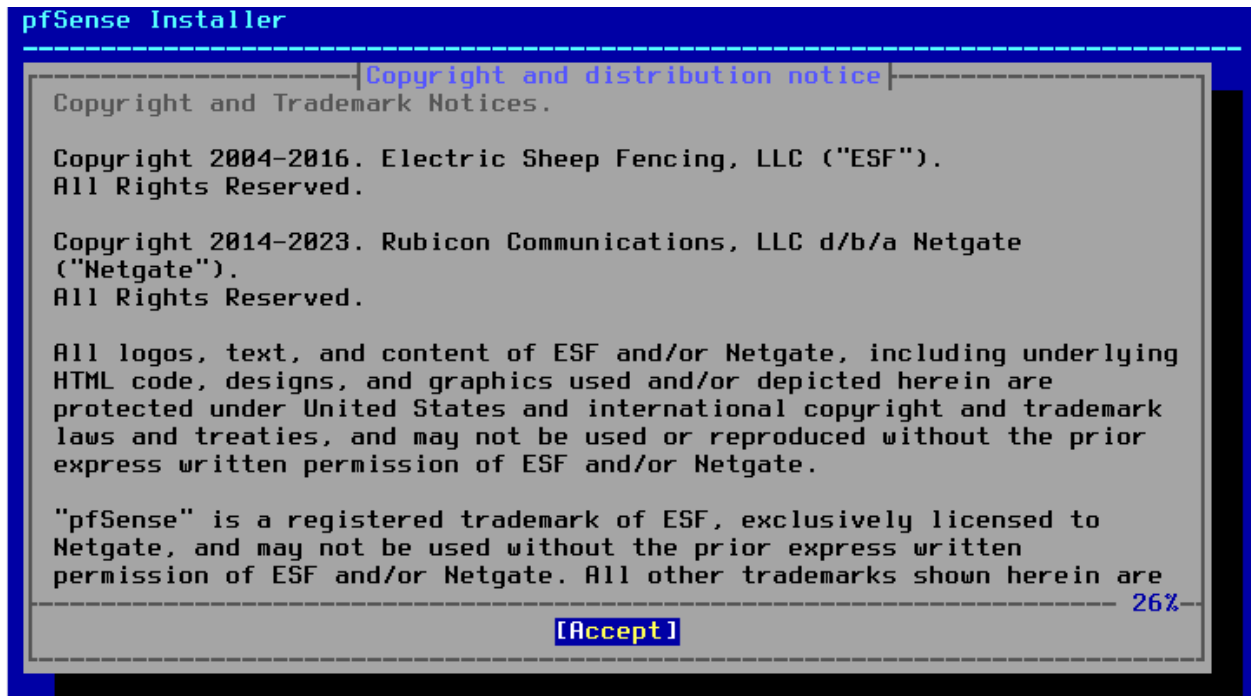
##### Format :

Vous pourrez alors sélectionner le fichier selon le format voulu dans votre SGBD.

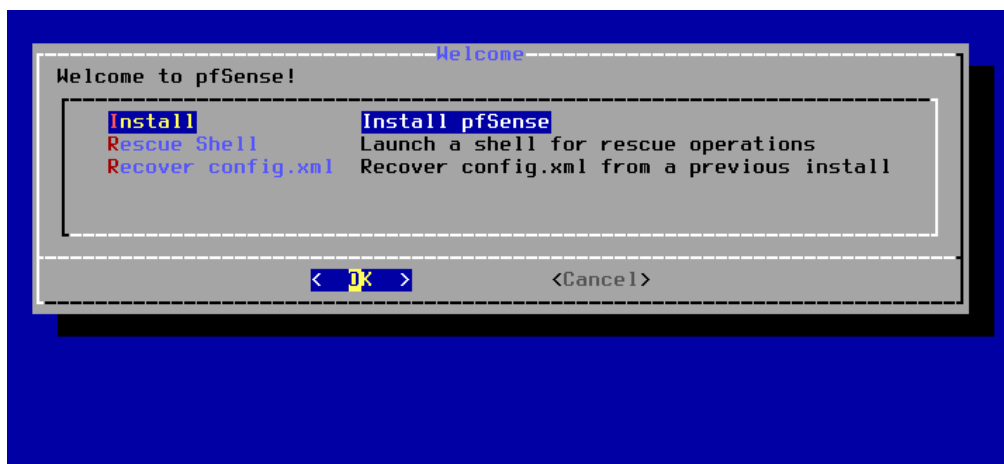
Voilà pour la configuration de notre serveur Debian, pour le SSH, la configuration du SSH se fera plus tard.

## IV. Installation & Configuration de Pfsense

Après avoir créé votre VM, vous allez tomber sur cette fenêtre où va débuter l'installation :



Pour continuer l'installation, la navigation est la même que durant l'installation (flèche et entrer pour confirmer). Nous avons un 1er message qui nous indique les conditions d'utilisation de Pfsense, on accepte celles-ci. Ensuite, le processus d'installation nous propose 3 options. L'option qui nous intéresse est "Install" car elle va permettre de débuter le processus d'installation de pfsense :



Nous voilà arrivés au partitionnement, le processus d'installation va nous offrir 4 possibilités:

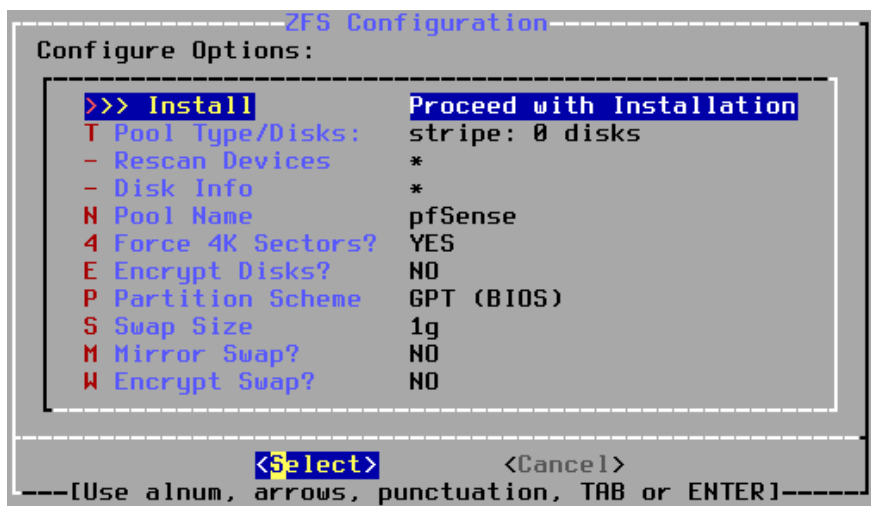
Partitionnement Auto ZFS

Partitionnement Auto UFS

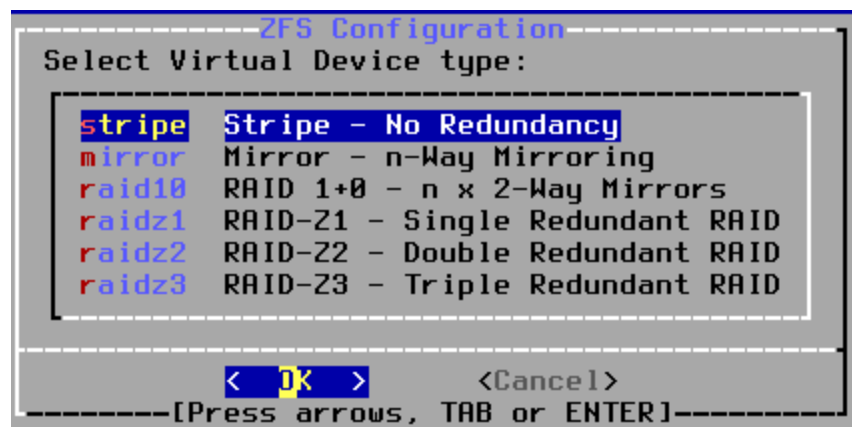
Manuel

Effectuer le partitionnement en ligne de commande

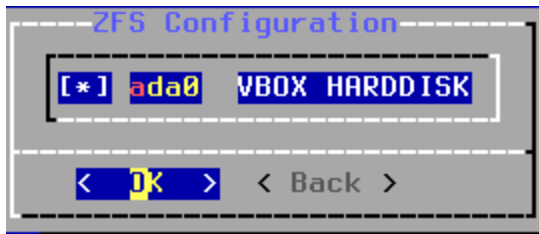
Prenez celle qui vous convient le mieux, nous choisirons un partitionnement ZFS pour notre cas à nous. Ensuite, nous pouvons choisir des options pour la partition comme par exemple chiffrer les partitions, changer la table de partition... Une fois les options finies, cliquez sur entrer quand vous êtes sur install pour débiter l'installation :



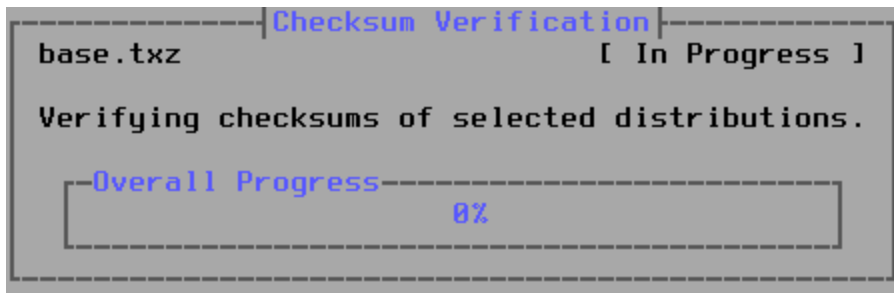
Si vous voulez mettre en place un service de raid ou de mirror, cela se passera sur l'étape suivante. Si vous ne souhaitez pas, cliquez sur entrer en étant sur "stripe":



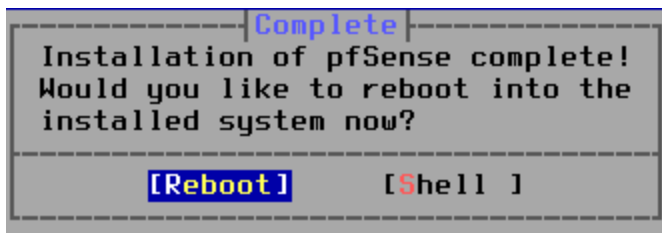
L'étape suivante est le choix du disque dur où pfsense sera installé, vous le sélectionnez en appuyant sur la barre espace une fois au-dessus. S'il est bien sélectionné, alors vous devriez voir une petite étoile sur votre disque dur voulu :



L'installation va alors débuter :



Une fois l'installation finie, vous pourrez redémarrer votre machine en éjectant le lecteur cd virtuel.



Lors du démarrage de pfsense, vous arrivez ici :

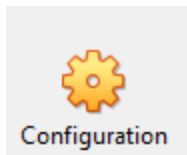
```
KVM Guest - Netgate Device ID: d5ee7d80591189e4aa3c
*** Welcome to pfSense 2.7.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4: 172.16.68.1/16
LAN (lan)      -> em1      -> v4: 192.168.0.1/24
DMZ (opt1)    -> em2      -> v4: 10.0.0.1/24

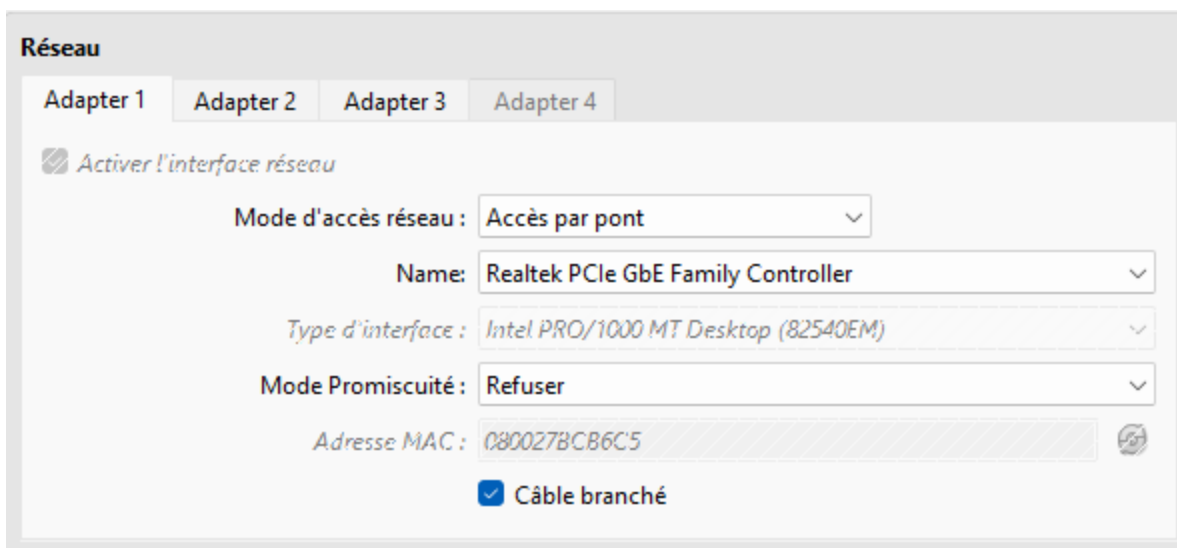
0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable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

Enter an option:
Message from syslogd@pfSense at Apr 30 12:30:37 ...
php-fpm[3981]: /firewall_rules.php: Successful login for user 'admin' from: 192.1
58.0.53 (Local Database)
5
```

Avant de continuer, il faut ajouter des cartes réseaux virtuelles à notre pare-feu pour que l'on puisse simuler au maximum le schéma. Pour ajouter des cartes, retourner sur l'écran d'accueil de virtualbox et cliquer sur l'engrenage orange :



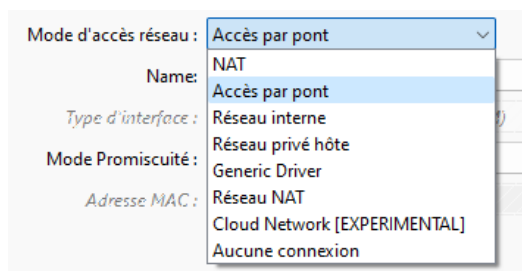
Une fois fait, aller dans la rubrique "Réseau" pour allouer 2 cartes réseaux en plus (Mettez-vous en mode expert de préférence) :



Sachant qu'il nous faut 3 domaines de diffusion par rapport au cinéma, nous allons donc rajouter 3 adaptateurs réseaux. De plus, il va falloir configurer ces cartes en fonction du mode d'accès réseau souhaité. Le découpage va se faire comme ceci :

- 1 interface en accès par pont pour garantir l'accès à internet côté LAN et accès au serveur à distance
- 2 interfaces en réseau interne différents pour illustrer un LAN et une DMZ

Pour changer le mode d'accès, cela se passe sur la carte dans les options déroulantes puis changer le mode d'accès selon ce que vous souhaitez réaliser :



Une fois ceci fait, je vous conseille de redémarrer votre machine pour bien appliquer les modifications effectuées. Dans un premier temps, nous allons assigner les interfaces à nos cartes réseau en faisant la touche 1 de notre clavier :

```
Enter an option: 1

Valid interfaces are:

em0      08:00:27:d6:a5:33   (up) Intel(R) Legacy PRO/1000 MT 82540EM
em1      08:00:27:01:a3:85   (up) Intel(R) Legacy PRO/1000 MT 82540EM
em2      08:00:27:18:9c:4c   (up) Intel(R) Legacy PRO/1000 MT 82540EM

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.
Should VLANs be set up now [y/n]? █
```

Toutes nos interfaces sont bien reconnues par le système, pfsense va alors nous proposer de faire des VLAN, ce qu'on va refuser en faisant "n" puis entrée. Ensuite, pfsense va demander quelle interface va être attribuée pour le côté WAN, vous devez écrire le nom de l'interface que vous souhaitez attribuer à celui-ci :

```
Enter the WAN interface name or 'a' for auto-detection
(em0 em1 em2 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 a or nothing if finished): S █
```

Viens ensuite celle du LAN :

```
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 a or nothing if finished): S █
```

Enfin, la dernière interface que nommera plus tard en DMZ :

```
The interfaces will be assigned as follows:

WAN  -> em0
LAN  -> em1
DMZ1 -> em2

Do you want to proceed [y/n]? S █
```

Une fois que les changements vous conviennent, au moment de la confirmation vous pourrez faire y :

```
Do you want to proceed [y|n]? S
```

Nous allons passer maintenant à l'attribution des adresses IP de nos interfaces. Pour faire cette étape, appuyez sur la touche 2 de votre clavier puis choisissez l'interface où vous souhaitez mettre l'@IP :

```
Available interfaces:
1 - WAN (em0 - static)
2 - LAN (em1 - static)
3 - DMZ (em2 - static)
Enter the number of the interface you wish to configure:
```

Une fois l'interface choisie, pfsense va alors demander des renseignements sur la configuration, comme sur la première demande où on souhaiterait avoir une configuration via DHCP sur cette interface. Si vous mettez non, alors vous devrez saisir l'@IP que vous souhaitez attribuer à l'interface :

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

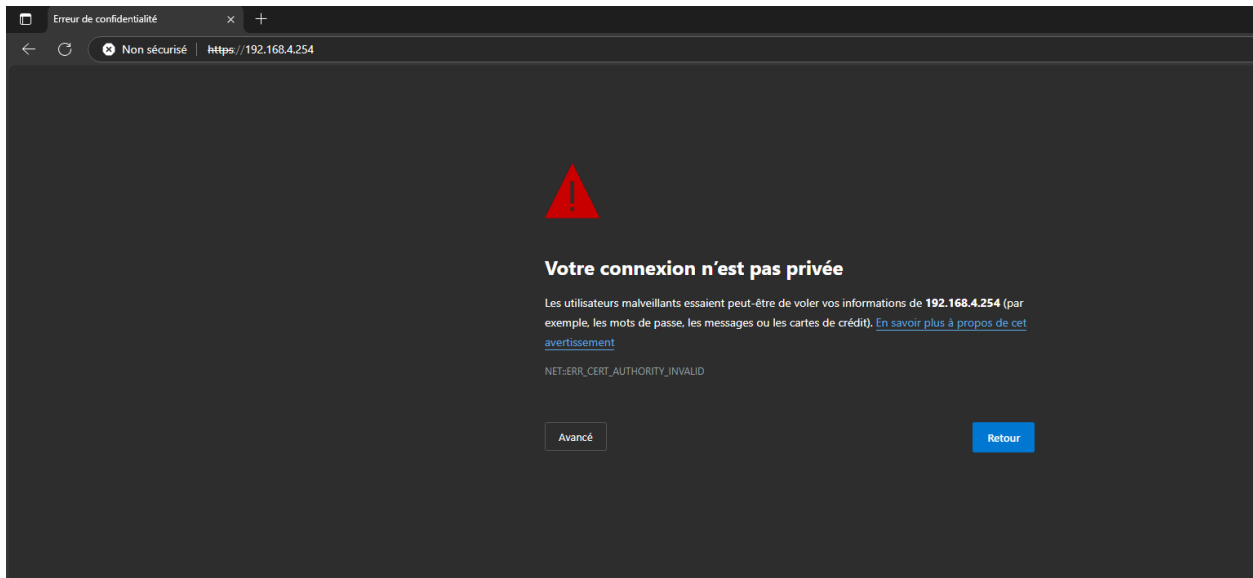
Ensuite, il faudra donner le masque du réseau associé à l'adresse du réseau puis cliquer sur la touche entrer pour arriver sur la page de confirmation nous indiquant que les changements vont être appliqués. Appuyer une nouvelle fois sur la touche entrer pour finir la configuration et revenir au début :

```
For a LAN, press <ENTER> for none:
>
Configure IPv6 address WAN interface via DHCP6? (y/n) n
Enter the new WAN IPv6 address. Press <ENTER> for none:
>
Do you want to enable the DHCP server on WAN? (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 WAN...
Reloading filter...
Reloading routing configuration...
DHCPD...
The IPv4 WAN address has been set to 172.16.68.18/24
You can now access the webConfigurator by opening the following URL in your web
browser:
      https://172.16.68.18/
```

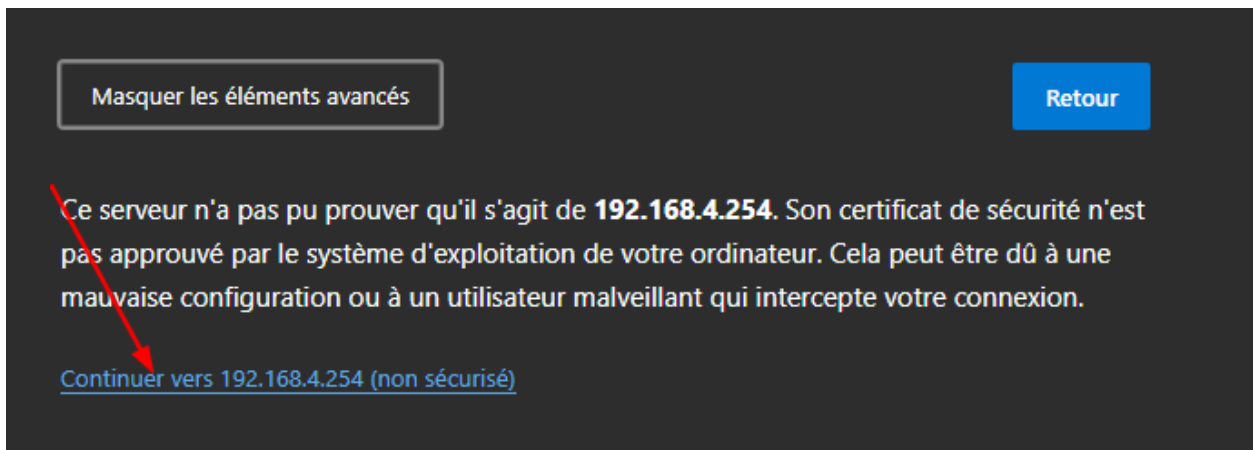
On refait le même procédé pour l'ensemble des interfaces à savoir LAN et DMZ pour avoir un résultat similaire à celui-ci :

```
WAN (wan)      -> em0      -> v4: 172.16.70.254/16
LAN (lan)      -> em1      -> v4: 192.168.4.254/24
DMZ (opt1)     -> em2      -> v4: 10.10.10.254/24
```

Pour la suite de la configuration de Pfsense, cela se passera sur l'interface web côté LAN. Sur un client Windows, situé sur le réseau LAN, dans un navigateur internet il faudra taper l'adresse IP du Pfsense soit 192.168.4.254 pour arriver sur page de connexion :



Si vous avez un message comme celui-ci, il suffira simplement de cliquer sur *Avancé* puis d'accéder à notre interface sur le lien qui sera proposé :



Pour enfin arriver sur la page d'authentification de notre routeur :

**SIGN IN**

Username

---

Password

---

**SIGN IN**

Les identifiants de défaut de Pfsense sont :

login : admin

mdp : pfsense

Une fois authentifié, vous êtes sur la page d'accueil de l'interface web de configuration de Pfsense :

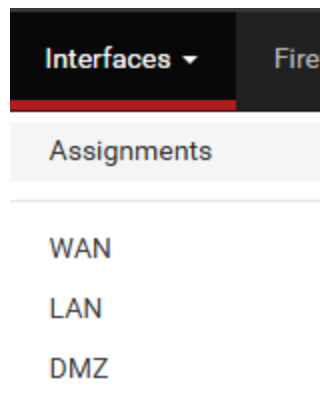
**WARNING:** The 'admin' account password is set to the default value. Change the password in the User Manager.

Status / Dashboard

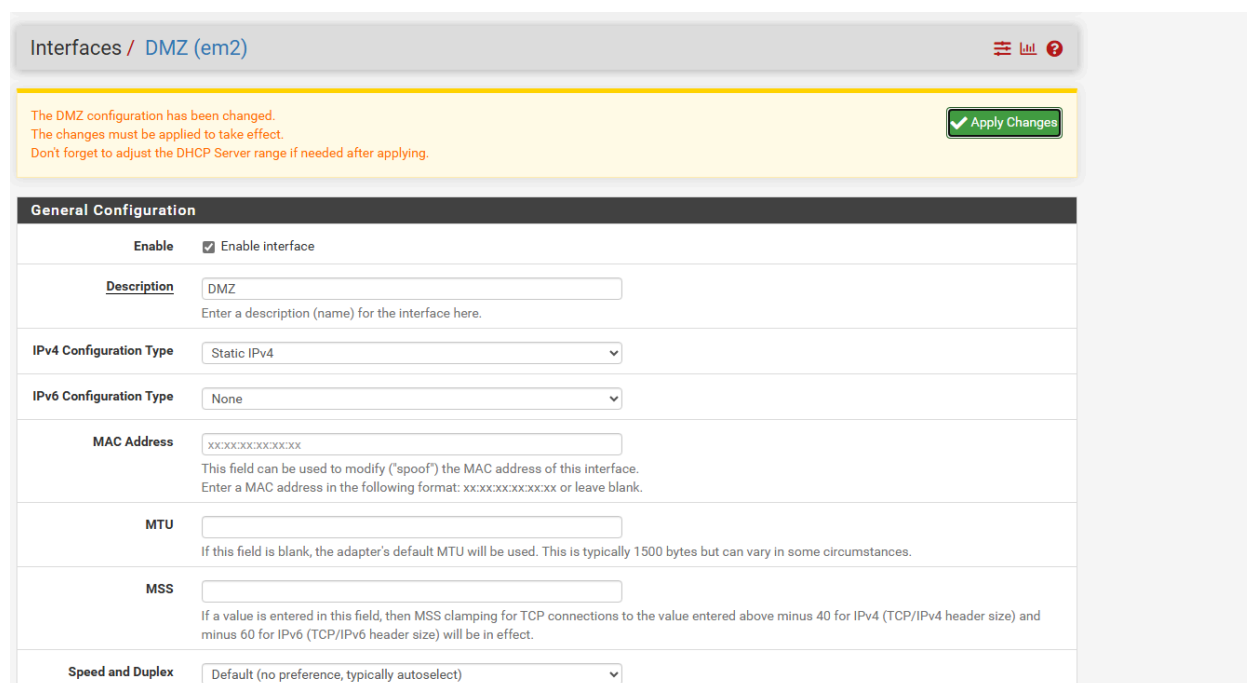
System Information	
Name	pfSense.home.arpa
User	admin@192.168.4.53 (Local Database)
System	KVM Guest Netgate Device ID: ddf351907bf342060b7c
BIOS	Vendor: <b>Innotek GmbH</b> Version: <b>VirtualBox</b> Release Date: <b>Fri Dec 1 2006</b>
Version	<b>2.7.1-RELEASE</b> (amd64) built on Wed Nov 15 17:06:00 UTC 2023 FreeBSD 14.0-CURRENT  Version <b>2.7.2</b> is available Version information updated at Thu May 15 11:50:44 UTC 2025
CPU Type	Intel(R) Core(TM) i5-7500 CPU @ 3.40GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	Inactive
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	00 Hour 44 Minutes 31 Seconds
Current date/time	Thu May 15 12:34:08 UTC 2025
DNS server(s)	+ 127.0.0.1

Netgate Services And Support	
Contract type	Community Support Community Support Only
<b>NETGATE AND pfSense COMMUNITY SUPPORT RESOURCES</b>	
<p>If you purchased your pfSense gateway firewall appliance from Netgate and elected <b>Community Support</b> at the point of sale or installed pfSense on your own hardware, you have access to various community support resources. This includes the <b>NETGATE RESOURCE LIBRARY</b>.</p> <p>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.</p> <ul style="list-style-type: none"> <li>Upgrade Your Support</li> <li>Community Support Resources</li> <li>Netgate Global Support FAQ</li> <li>Official pfSense Training by Netgate</li> <li>Netgate Professional Services</li> <li>Visit Netgate.com</li> </ul>	
<p>If you decide to purchase a Netgate Global TAC Support subscription, you <b>MUST</b> have your <b>Netgate Device ID (NDI)</b> 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 supports <a href="#">here</a>.</p>	

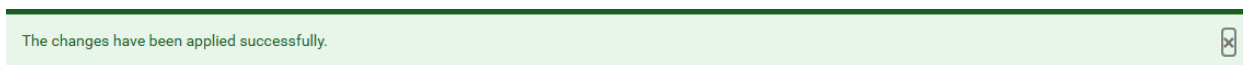
La première configuration que l'on va effectuer est de changer le nom de la 3ème interface qui va s'appeler par défaut opt1. Dans la 2ème rubrique qui se nomme *interface*, vous pourrez alors sélectionner opt1 :



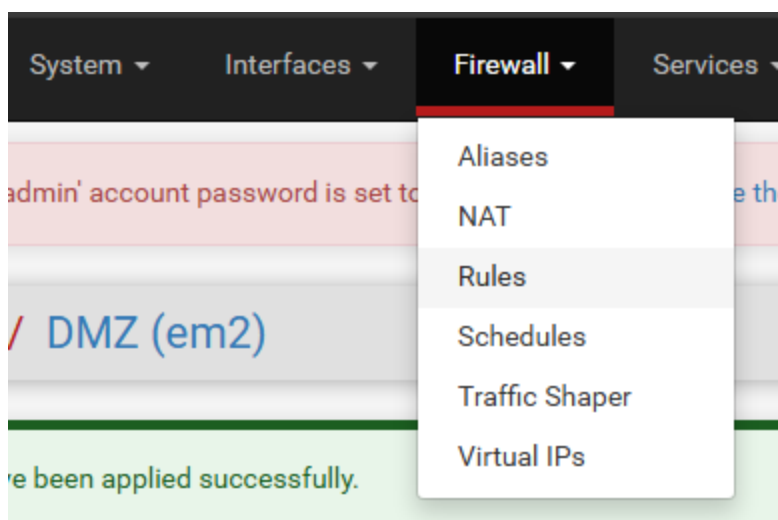
Sélectionner là, puis sur la case *description*, changer le opt1 en DMZ puis descendez tout en bas pour enregistrer les modifications, puis les appliquer à l'interface en cliquant sur *Apply Changes* :



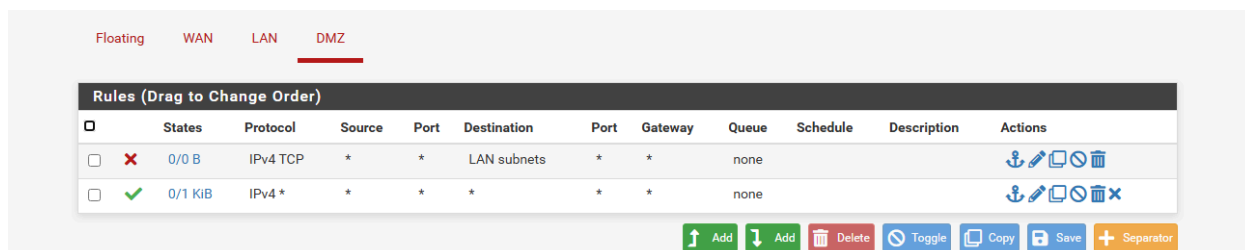
Un message vous confirmera que les changements sont bien appliqués en vert là où était situé le bouton Apply Change :



La seconde étape que l'on va faire est les règles de filtrages qui se situe dans la rubrique Firewall puis Rules :



Dans un premier temps, nous allons nous concentrer sur l'interface DMZ où nous allons créer 2 règles. 1 règle qui autorise l'ensemble du trafic et une autre qui va interdire l'accès au nat depuis la DMZ. donc, en ayant cliqué sur Rules puis sur DMZ, on arrive ici :



On va cliquer sur Add pour ajouter une nouvelle règle, puis nous allons commencer par la règle d'interdiction d'accès au réseau LAN depuis la DMZ. Dans la première case, nous avons le choix de la règle, c'est-à-dire soit on souhaite autoriser ou bloquer. Nous allons bloquer. Ensuite, nous choisirons l'interface où la règle sera appliquée, soit la DMZ. Pour l'onglet Address Family, nous allons mettre IPV4 ainsi que le protocole TCP sur la page suivante, ce qui donne en image sur la première partie de la règle :

**Edit Firewall Rule**

**Action**    
 Choose what to do with packets that match the criteria specified below.   
 Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

**Disabled**  Disable this rule   
 Set this option to disable this rule without removing it from the list.

**Interface**    
 Choose the interface from which packets must come to match this rule.

**Address Family**    
 Select the Internet Protocol version this rule applies to.

**Protocol**    
 Choose which IP protocol this rule should match.

En descendant sur la règle, nous aurons alors plusieurs parties. Dans la partie source, on veut que l'ensemble des trames arrivant à la DMZ à destination de notre LAN soit bloqué donc dans la partie Source, nous mettrons Any pour inclure l'ensemble des propositions de filtrage puis dans l'onglet de destination le réseaux LAN autrement dit le LAN subnets :

**Source**

**Source**  Invert match   /    
   
 The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.

**Destination**

**Destination**  Invert match   /    
**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.

**Extra Options**

**Log**  Log packets that are handled by this rule   
 Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

**Description**    
 A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.


**Advanced Options**

**Rule Information**


<b>Tracking ID</b>	1743689523
<b>Created</b>	4/3/25 14:12:03 by admin@192.168.4.53 (Local Database)
<b>Updated</b>	4/3/25 14:12:03 by admin@192.168.4.53 (Local Database)

Pour enregistrer, descendez tout en bas jusqu'à arriver à un moment sur une icône de sauvegarde


Rule Information	
Tracking ID	1743689523
Created	4/3/25 14:12:03 by admin@19:
Updated	4/3/25 14:12:03 by admin@19:

 Save

Puis appliquer les changements :

The changes have been applied successfully. 

Pour créer une deuxième règle, vous pouvez très bien cliquer sur une seconde fois sur Add ou alors cliquer sur le carré situé sur la règle que vous venez de créer :

 0/0 B IPv4 TCP \* \* LAN subnets \* \* none    

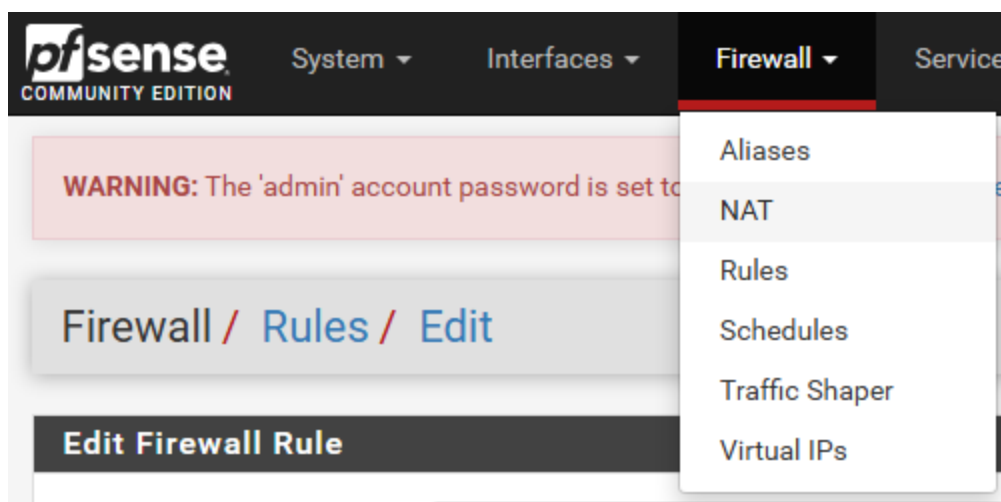
En modifiant les actions de la règle pour autoriser tout le trafic sur l'interface de la DMZ il faudra alors remplacer par exemple le protocole par Any, la source par Any, et destination par Any pour avoir une règle qui laisse passer :

Edit Firewall Rule	
<b>Action</b>	Pass <small>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</small>
<b>Disabled</b>	<input type="checkbox"/> Disable this rule <small>Set this option to disable this rule without removing it from the list.</small>
<b>Interface</b>	DMZ <small>Choose the interface from which packets must come to match this rule.</small>
<b>Address Family</b>	IPv4 <small>Select the Internet Protocol version this rule applies to.</small>
<b>Protocol</b>	Any <small>Choose which IP protocol this rule should match.</small>
<b>Source</b>	
<b>Source</b>	<input type="checkbox"/> Invert match Any Source Address /
<b>Destination</b>	
<b>Destination</b>	<input type="checkbox"/> Invert match Any Destination Address /

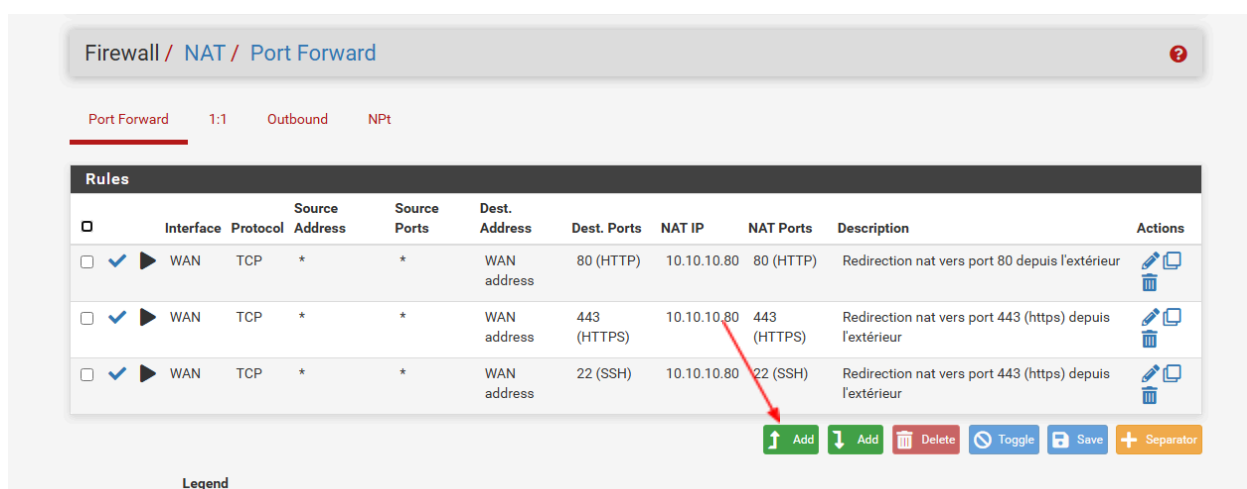
On enregistre une nouvelle fois la règle, puis on applique les changements :

The changes have been applied successfully.

Enfin, la dernière partie consiste à faire la redirection de port ou NAT pour notre serveur que l'on va paramétrer en avance. Pour ça, rendez-vous dans firewall puis dans NAT :



Vous arrivez sur une page vous indiquant les règles qui sont déjà mises en place sur votre PfSense. Pour créer une redirection de port, en cliquant sur le bouton Add, vous arrivez alors sur une configuration d'1 redirection de port :



Nous allons créer la première redirection de port qui sera que lorsque l'on souhaite afficher notre site via le WAN, cela sera automatiquement redirigé sur le port 80 (port par défaut du HTTP) de notre serveur situé sur la DMZ. Donc, sur le choix de l'interface où sera appliquée la règle, ce sera le WAN, l'Address Family sera sur IPV4, le protocole sur TCP, la source sera sur Any si vous souhaitez rediriger toutes les trames sur le port 80 et la destination sera WAN address en port de destination HTTP soit le 80. Pour la redirection, il faut l'effectuer sur notre serveur uniquement donc en saisissant l'adresse IP de notre serveur soit 10.10.10.80 :

Firewall / NAT / Port Forward / Edit ?

### Edit Redirect Entry

**Disabled**  Disable this rule

**No RDR (NOT)**  Disable redirection for traffic matching this rule  
This option is rarely needed. Don't use this without thorough knowledge of the implications.

**Interface** WAN  
Choose which interface this rule applies to. In most cases "WAN" is specified.

**Address Family** IPv4  
Select the Internet Protocol version this rule applies to.

**Protocol** TCP  
Choose which protocol this rule should match. In most cases "TCP" is specified.

**Source** [Display Advanced](#)

**Destination**  Invert match. WAN address /   
Type Address/mask

**Destination port range** HTTP From port Custom HTTP To port Custom  
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

**Redirect target IP** Address or Alias 10.10.10.80  
Type Address

Ainsi que sur son port de redirection, soit le 80, et enfin pour le filtre, mettre pass pour laisser passer la trame :

**Destination port range**  
From port: HTTP, Custom  
To port: HTTP, Custom  
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

**Redirect target IP**  
Address or Alias: 10.10.10.80  
Type: Address  
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4  
In case of IPv6 addresses, it must be from the same "scope", i.e. it is not possible to redirect from link-local addresses scope (fe80:\*) to local scope (::1)

**Redirect target port**  
Port: HTTP, Custom  
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).  
This is usually identical to the "From port" above.

**Description**  
Redirection nat vers port 80 depuis l'extérieur  
A description may be entered here for administrative reference (not parsed).

**No XMLRPC Sync**  
 Do not automatically sync to other CARP members  
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

**NAT reflection**  
Use system default

**Filter rule association**  
Pass

**Rule Information**

Created	4/2/25 12:43:44 by admin@192.168.0.53 (Local Database)
Updated	5/15/25 13:43:01 by admin@192.168.4.53 (Local Database)

[Save](#)

On sauvegarde cette première redirection de port puis on l'applique :

The changes have been applied successfully.

on fait de même pour une redirection sur le port 443 pour le https ainsi que sur le port 22 pour la mise en place du SSH et du SFTP, ce qui donne 3 règles :

Port Forward 1:1 Outbound NPt

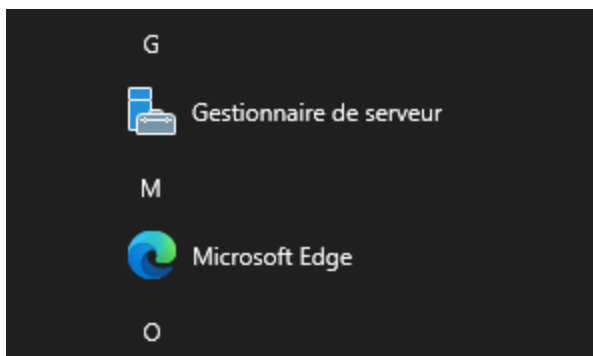
Rules	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	80 (HTTP)	10.10.10.80	443 (HTTPS)	Redirection nat vers port 80 depuis l'extérieur	
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	443 (HTTPS)	10.10.10.80	443 (HTTPS)	Redirection nat vers port 443 (https) depuis l'extérieur	
<input type="checkbox"/>	WAN	TCP	*	*	WAN address	22 (SSH)	10.10.10.80	22 (SSH)	Redirection nat vers port 22 (ssh) depuis l'extérieur	

[Add](#) [Add](#) [Delete](#) [Toggle](#) [Save](#) [Separator](#)

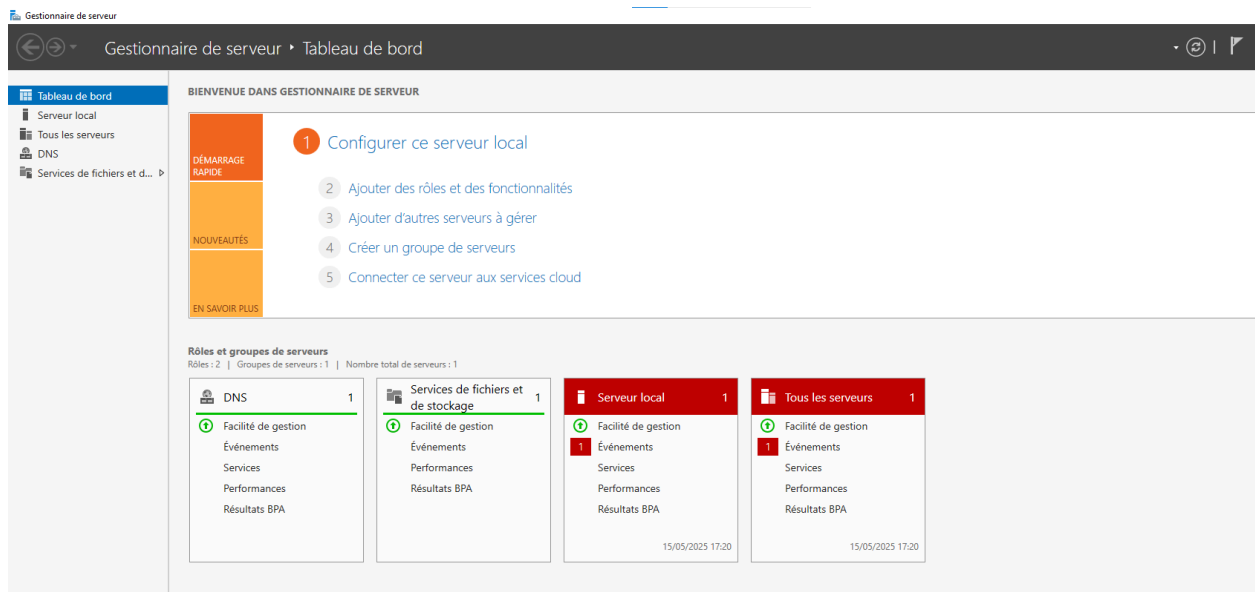
Et nous voilà avec un pfSense configuré prêt pour cette infrastructure .

## V. Installation des serveurs DNS

Un serveur DNS va servir à traduire les noms de domaine en adresses IP pour permettre aux utilisateurs de se connecter à des sites web en utilisant des noms faciles à retenir plutôt que des adresses numériques ou à se connecter à des machines par leurs noms plutôt qu'avec leur adresse IP (DNS sur du LAN). Dans cette infrastructure, nous allons en disposer 2, 1 sur le côté WAN qui jouera le rôle du DNS d'un fournisseur d'accès à internet (FAI), puis le second sur le LAN. Donc, une fois que nos Windows Servers sont installés, la première étape va consister à installer le rôle du DNS. Pour cela, il faut se rendre dans le gestionnaire de serveur en faisant la touche Windows de notre clavier pour le voir :

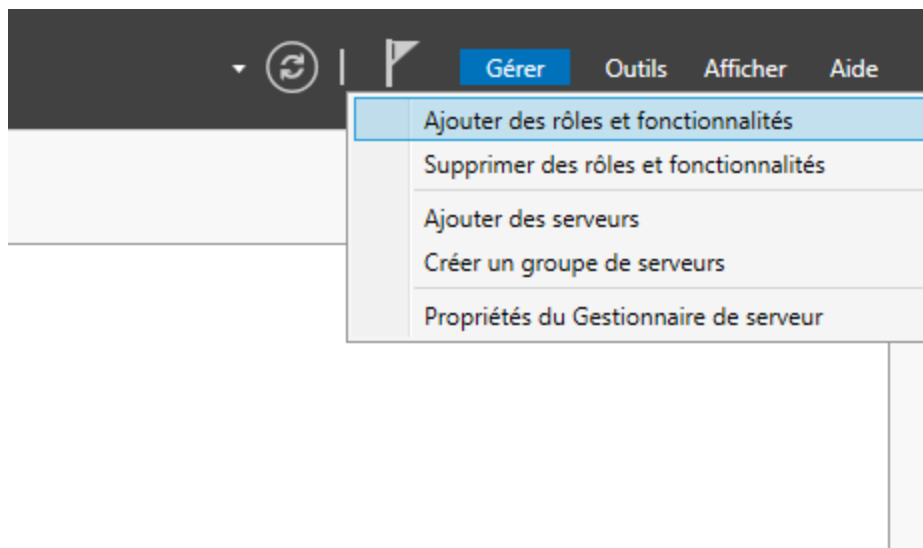


Nous arrivons sur cette page qui est le tableau de bord de notre serveur, là où l'ensemble des rôles installés est répertorié ici :

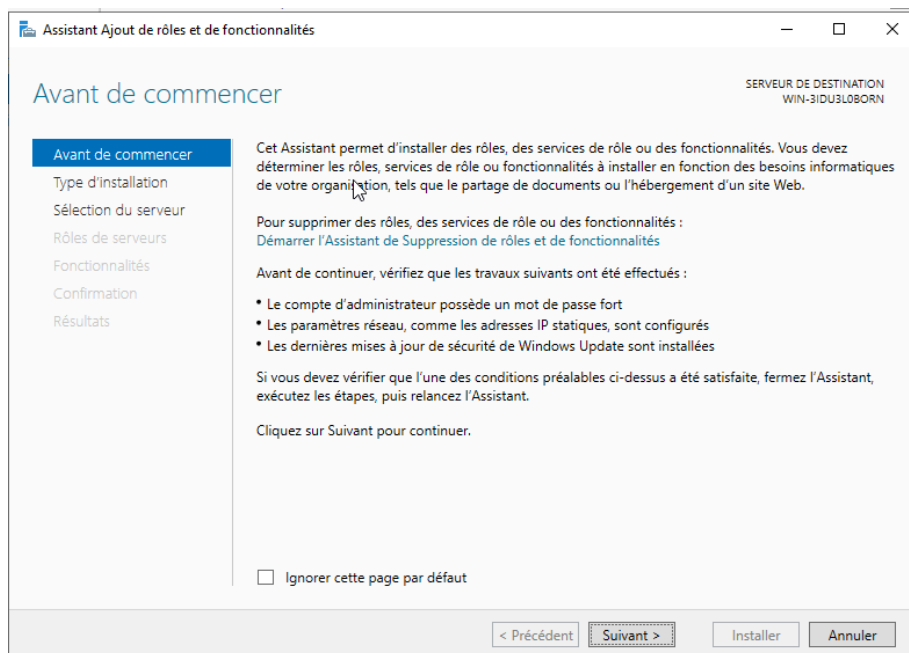


The screenshot displays the Windows Server Manager interface. At the top, there's a navigation bar with 'Gestionnaire de serveur' and 'Tableau de bord'. Below this, a sidebar on the left lists navigation options: 'Tableau de bord', 'Serveur local', 'Tous les serveurs', 'DNS', and 'Services de fichiers et d...'. The main content area is titled 'BIENVENUE DANS GESTIONNAIRE DE SERVEUR' and features a 'DÉMARRAGE RAPIDE' section with a numbered list of tasks: 1. Configurer ce serveur local, 2. Ajouter des rôles et des fonctionnalités, 3. Ajouter d'autres serveurs à gérer, 4. Créer un groupe de serveurs, and 5. Connecter ce serveur aux services cloud. Below this, the 'Rôles et groupes de serveurs' section shows a summary: 'Rôles : 2 | Groupes de serveurs : 1 | Nombre total de serveurs : 1'. Four role cards are displayed: 'DNS' (1), 'Services de fichiers et de stockage' (1), 'Serveur local' (1), and 'Tous les serveurs' (1). Each card lists sub-items like 'Facilité de gestion', 'Événements', 'Services', 'Performances', and 'Résultats BPA'.

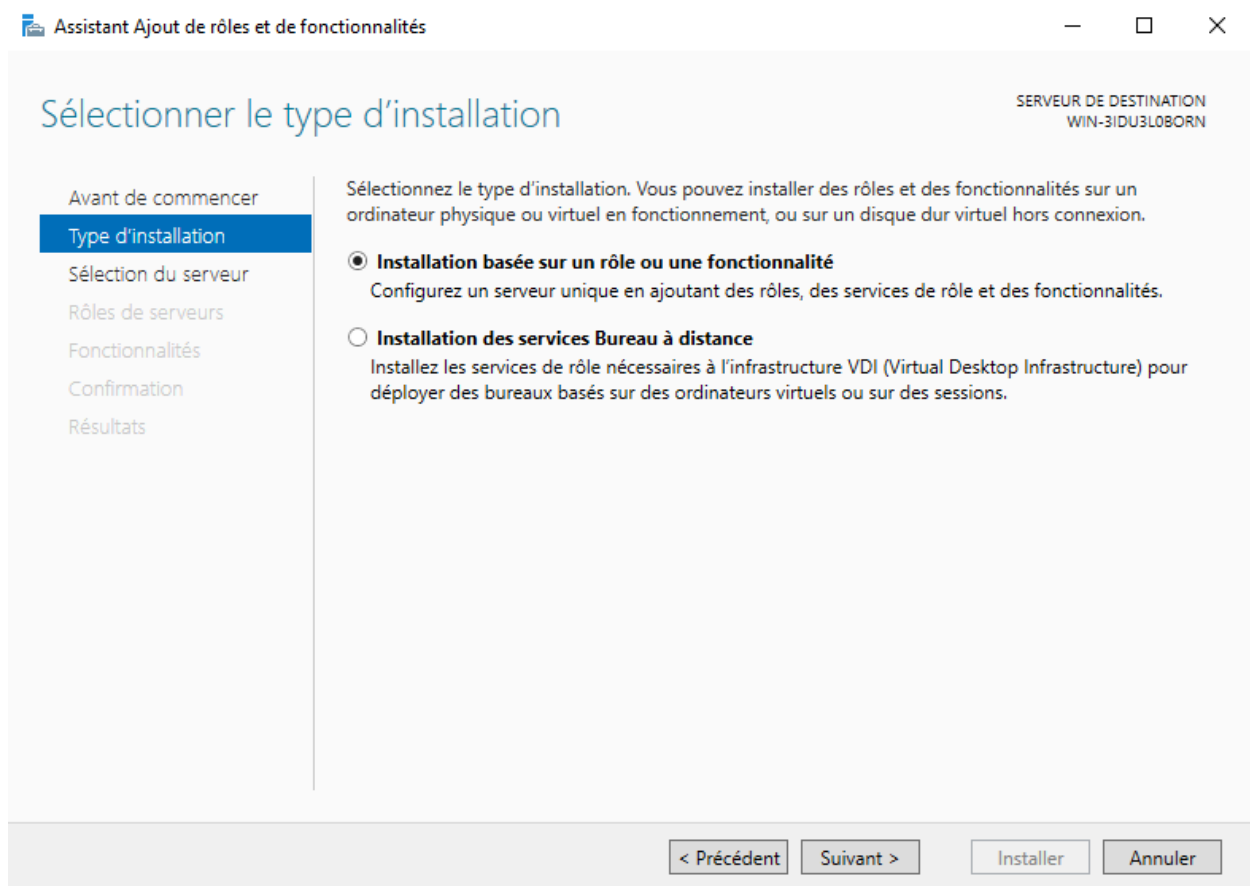
Pour installer le rôle DNS, dans l'onglet gérer puis sur ajouter des rôles et fonctionnalités, nous pourrions installer le rôle de serveur DNS sur notre serveur :



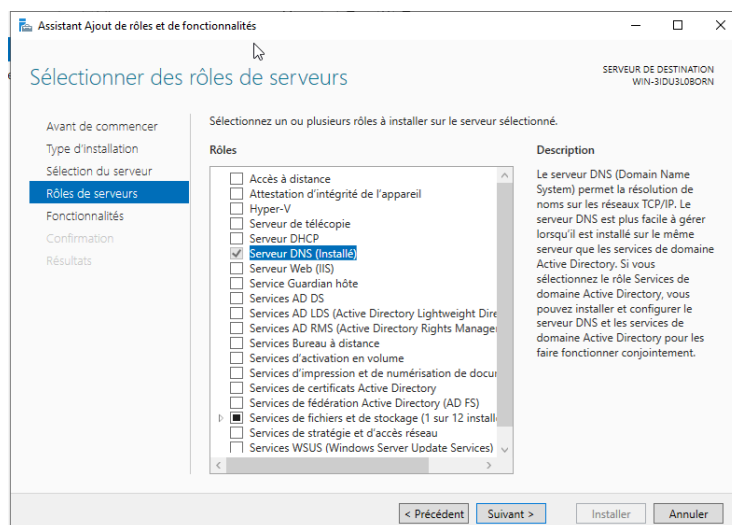
On arrive sur la page d'installation des rôles :



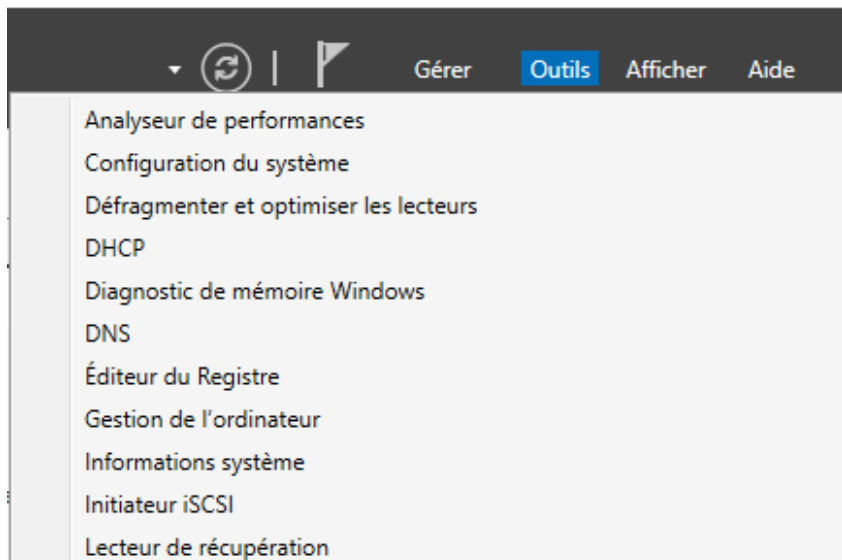
Le processus des installations de rôle va alors nous présenter le fonctionnement dans un premier temps, puis nous demander quelle type d'installation l'on souhaite. Soit on peut faire une installation basée sur un rôle ou une fonctionnalité, ou alors sur un bureau à distance. Nous choisirons la 1ère option :



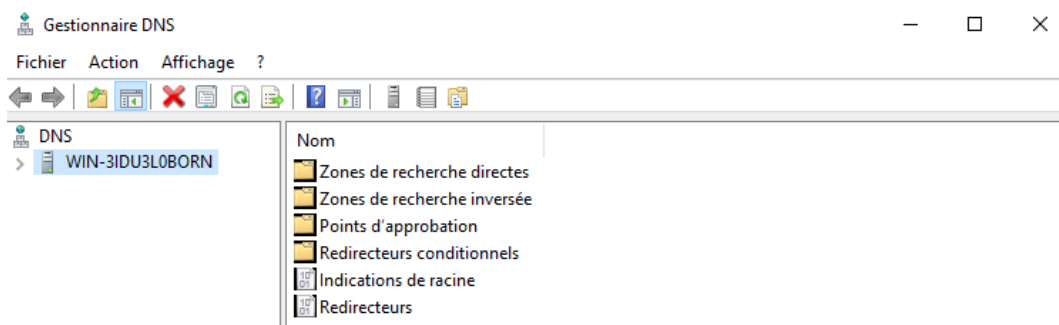
Puis faites une nouvelle fois suivant pour arriver sur les rôles de serveur que vous souhaitez installer :



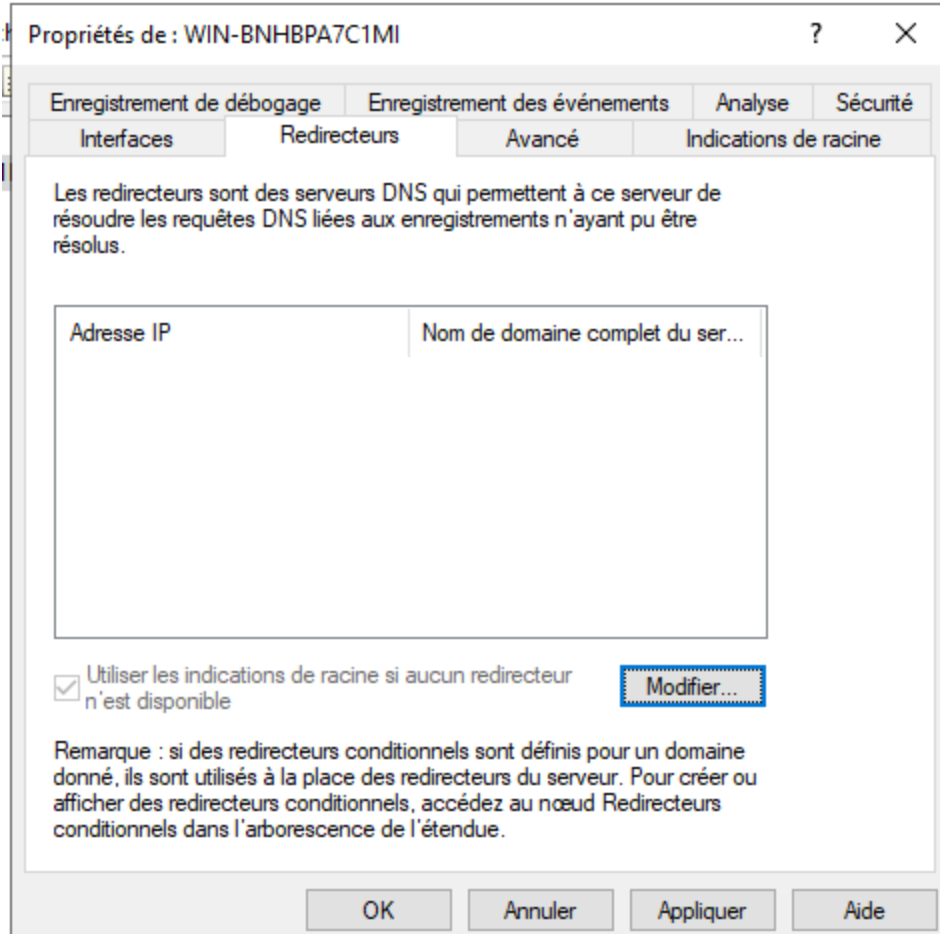
On confirme les messages jusqu'à l'installation du module DNS. Maintenant, lorsque vous cliquez sur l'onglet outils du gestionnaire de serveur, vous allez remarquer la rubrique DNS. Cliquer dessus pour configurer ainsi la redirection DNS :



Si vous avez réalisé comme décrit précédemment, vous allez être sur une fenêtre de ce style qui est autre que la page de configuration du service DNS :



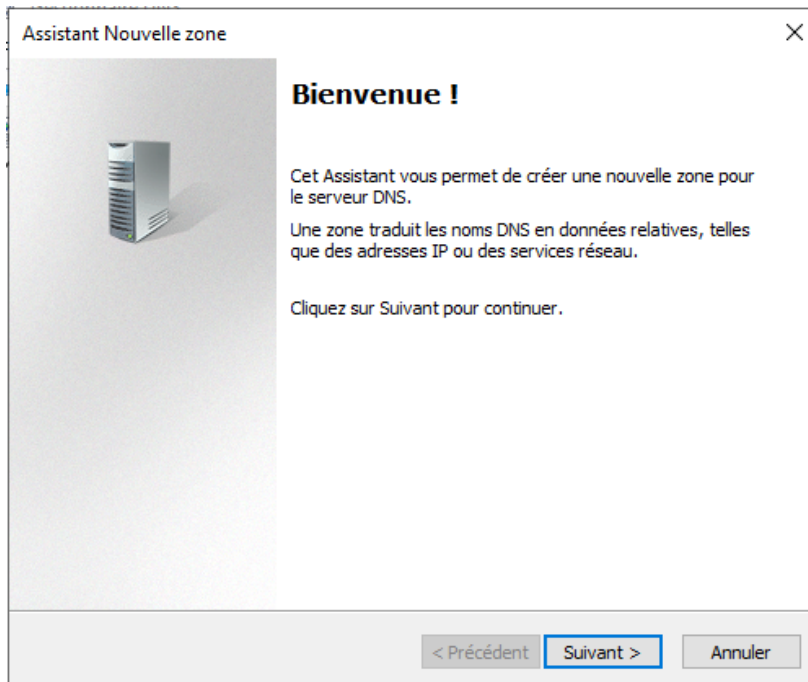
Pour effectuer une redirection, il faudra se rendre dans redirecteur en cliquant sur la partie droite de notre souris pour avoir les propriétés :



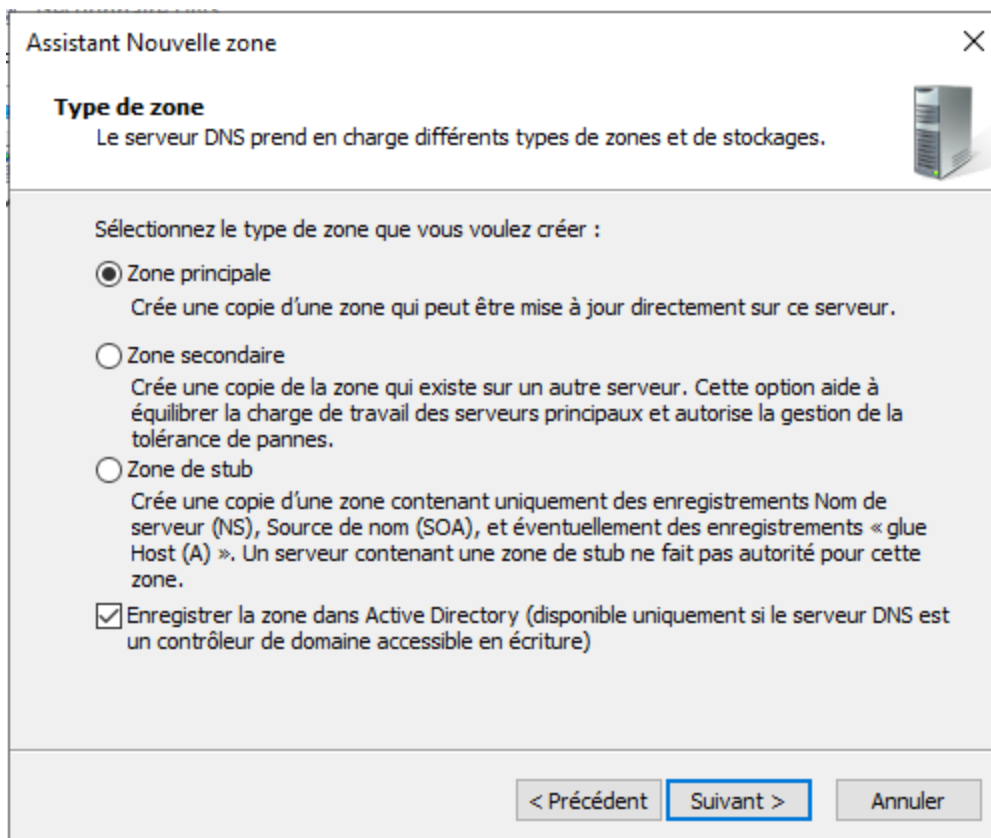
Il vous suffira plus que de rentrer l'adresse IP de votre serveur DNS puis d'appliquer la modification en cliquant sur appliquer (en bas à droite). Pour l'autre service DNS, les étapes sont les mêmes à l'exception du redirecteur qui sera le DNS 172.16.0.100.

Ensuite, pour ce qui concerne l'ajout des noms de domaines, cela est utile car au lieu que l'utilisateur rentre l'adresse IP du serveur web, l'utilisateur pourra taper un nom plus simple qui permettra d'afficher le site web grâce au service de DNS qui se chargera de traduire le nom de domaine par l'adresse IP correspondante au site. Pour cela, toujours dans le gestionnaire du service de DNS, il faut créer une nouvelle zone directe qui se nommera gestionfrais.n°octet.gsb qui fera la traduction de notre adresse IP du serveur web.

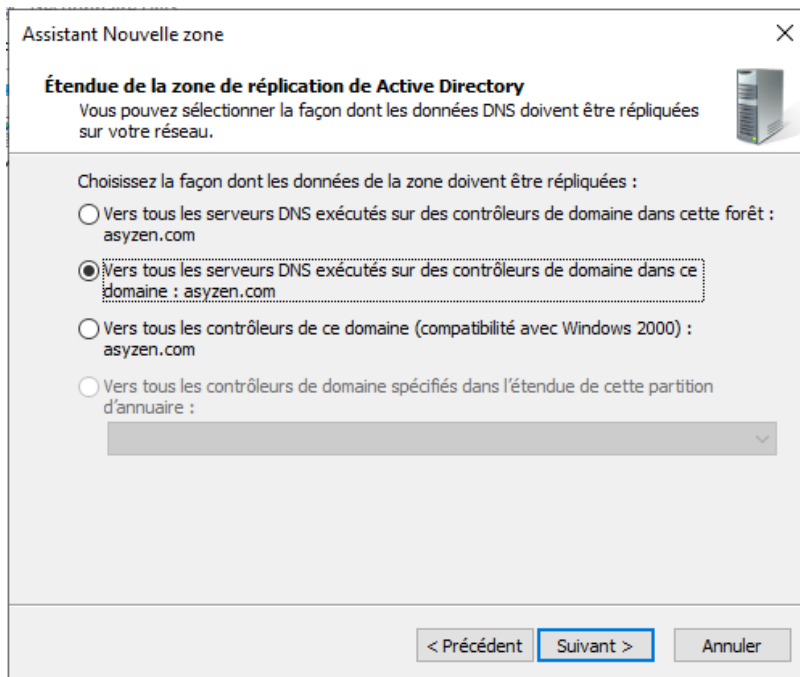
En cliquant sur zone directe, puis clique droit nouvelle zone, on est redirigé vers l'assistant DNS qui nous demandera plusieurs informations :



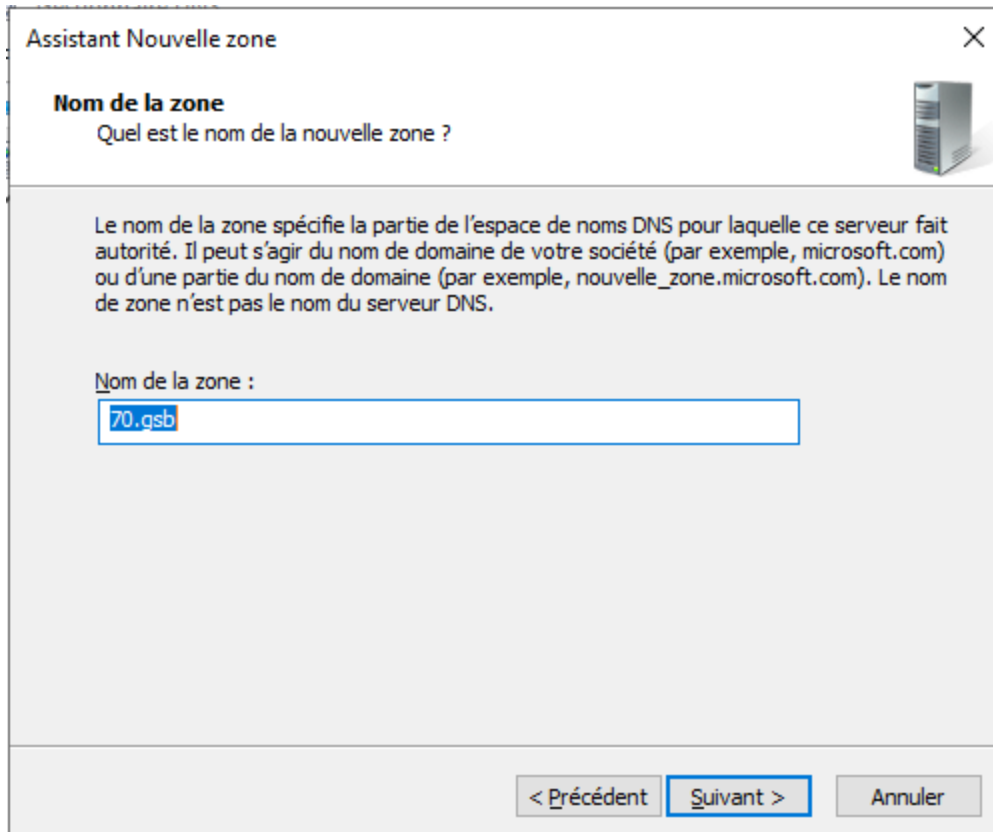
On clique sur suivant, puis on va créer une zone principale :



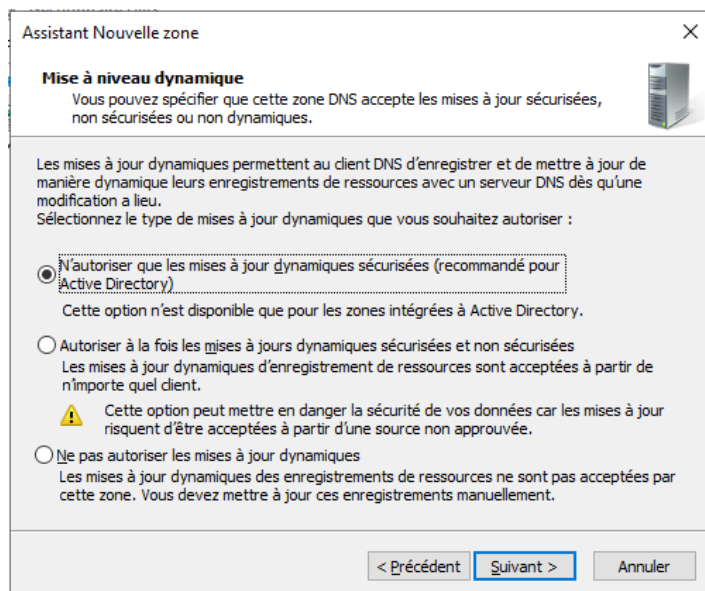
On laisse la case cochée par défaut pour la réplification de notre zone DNS :



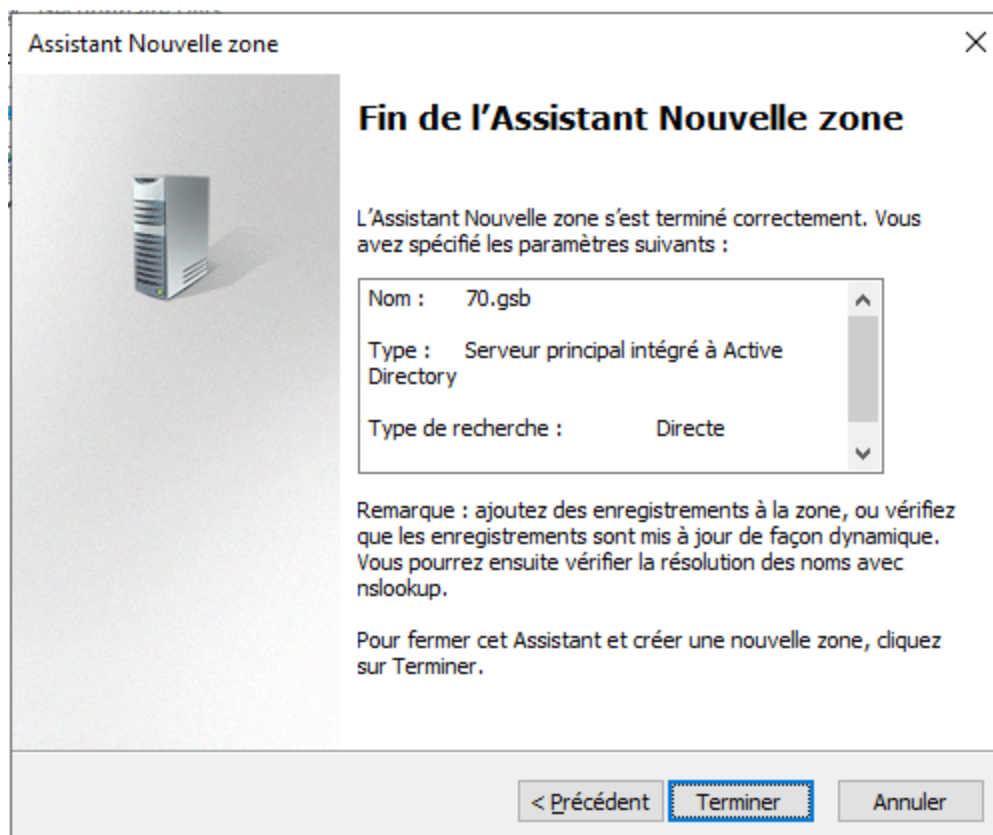
Puis on va lui donner un nom. Le nom sera 70.gsb qui correspondra à mon n°octet.gsb du site :



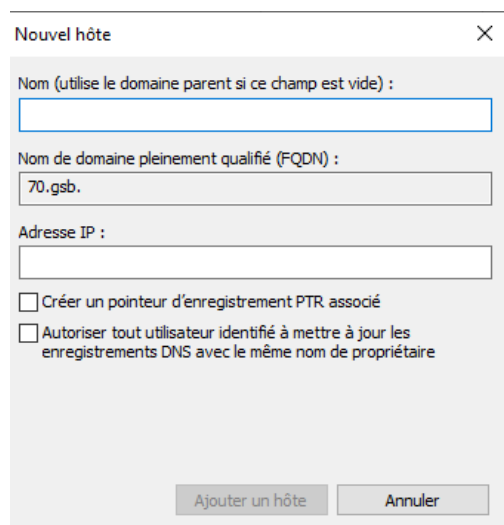
Puis on laisse une seconde fois l'option par défaut de la mise à jour :



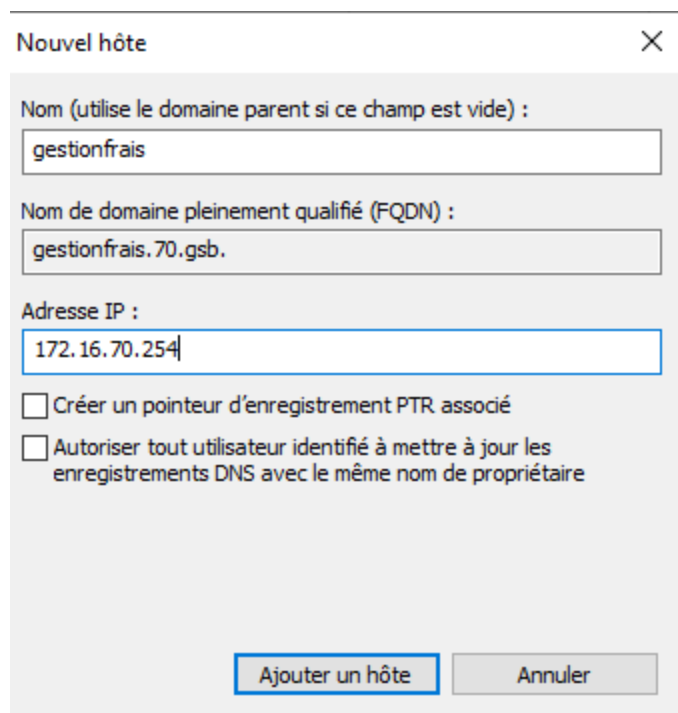
Puis cliquer sur Terminé une fois fini :



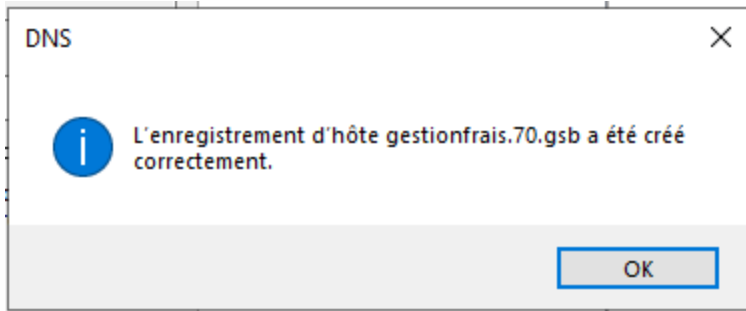
Nous voilà avec notre zone où il faut enregistrer un nouvel hôte. Pour l'enregistrer, double-cliquer sur la zone que l'on vient de créer puis faire un clic droit nouvelle hôte :



Puis, il faut alors saisir plusieurs informations comme le nom de notre hôte qui sera redirigé vers une adresse IP, soit notre serveur web, à savoir pour le nom gestionfrais.70.gsb qui va être traduit par 172.16.70.254 depuis le WAN, puis 10.10.10.80 depuis le LAN, ce qui donne comme exemple pour le WAN :



Une fois fini, cliquer sur ajouter un hôte pour avoir la modification enregistrée sur notre serveur DNS :



## II.Mise en place du service HTTPS + SSH

Pour effectuer un site en https sur Debian, il faut installer OpenSSL en faisant la commande en superutilisateur :

```
apt update
```


```
apt install apache2 openssl
```

Ensuite, il faut créer un certificat SSL auto-signé avec la commande :

```
openssl req -x509 -nodes -days 365 -newkey rsa:2048 \  
-keyout /etc/ssl/private/gestionfrais.key \  
-out /etc/ssl/certs/gestionfrais.crt
```

Maintenant, il ne nous reste plus qu'à mettre dans notre fichier de virtualhost les certificats ainsi qu'indiquer qu'il répondra maintenant uniquement sur le port 443 (HTTPS). Le fichier de virtualhost se trouve dans /etc/apache2/sites-available/gsb.conf :

```
<VirtualHost *:443>  
    ServerName gestionfrais.70.gsb  
  
    DocumentRoot /var/www/html/societyA/GSB/site/  
    DirectoryIndex Choose.html  
  
    SSLEngine on  
    SSLCertificateFile /etc/ssl/certs/gestionfrais.crt  
    SSLCertificateKeyFile /etc/ssl/private/gestionfrais.key  
    <Directory /var/www/gestionfrais>  
        AllowOverride All  
        Require all granted  
    </Directory>
```



```
</VirtualHost>
```

On enregistre le fichier gsb.conf, puis on active SSL avec la commande :

```
a2enmod ssl
```

```
a2ensite gsb.conf
```

on redémarre apache :

```
systemctl reload apache2
```

Pour le ssh :

Création du groupe sftp-users :

```
groupadd sftp-users
```

On crée 2 utilisateur pour les développeurs :

```
useradd -m -G sftp-user -s /usr/sbin/nologin irache
```

```
passwd irache
```

```
useradd -m -G sftp-user -s /usr/sbin/nologin nana
```

```
passwd nana
```

Leurs mot de passe sont Azerty31.

Ensuite, dans le fichier de configuration SSH, il faut créer la configuration suivante pour que les développeurs aient seulement l'accès au répertoire du site et pas aux autres :

```
Match Group sftp-user
```

```
    ChrootDirectory /var/www/html/societyA/GSB/site/
```

```
    ForceCommand internal-sftp
```

```
    X11Forwarding no
```

```
    AllowTcpForwarding no
```

```
    PermitTunnel no
```

Pour que le chroot fonctionne, GSB doit appartenir à root. Donc avec chown on remplace le propriétaire :

```
chown root:root /var/www/html/societyA/GSB
```

On crée le dossier site qui sera là où les développeurs auront l'autorisation de lecture et d'écriture :

```
mkdir /var/www/html/societyA/GSB/site
```

```
chown root:sftp-user /var/www/html/societyA/GSB/site
```

On redémarre SSH avec la commande :

```
systemctl restart ssh
```

Le ssh est maintenant configuré est prêt à l'utilisation.

