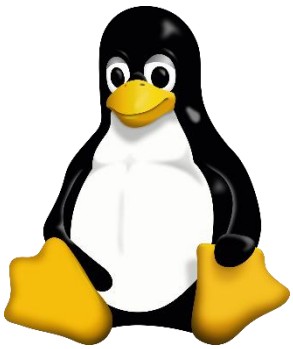
Atelier professionnel 3

M.LEGRAND – 2023/2024

Mise en place d'une infrastructure réseau subdivisé Entre WAN, LAN et DMZ comprenant leurs services associés selon le cahier des charges



Analyse fonctionnelle

Sujet théorique :

Pour mettre en œuvre l'infrastructure réseau décrite, il est essentiel de débuter par l'installation d'une DMZ (Zone Démilitarisée), qui constitue un sous-réseau sécurisé destiné à isoler les services tels que les serveurs web, de messagerie et de fichiers (Nextcloud) du réseau interne principal. Implémentez le protocole CARP (Common Address Redundancy Protocol) sur des dispositifs pfSense afin d'assurer une redondance efficace, garantissant ainsi une disponibilité continue des services même en cas de panne de matériel. Synchronisez les configurations entre les dispositifs pour assurer une cohérence dans la gestion des adresses IP via DHCP (Dynamic Host Configuration Protocol) et la résolution des noms de domaine via DNS (Domain Name System). Configurez le pare-feu IPFire pour sécuriser et réguler le trafic entre le réseau local (LAN), la DMZ et le réseau étendu (WAN), en appliquant des règles de pare-feu rigoureuses et en utilisant des techniques de NAT (Network Address Translation) pour faciliter un accès externe sécurisé aux services. Établissez des serveurs dédiés dans la DMZ pour les services de messagerie et web, en sécurisant les échanges de données à l'aide des protocoles SSL/TLS (Secure Sockets Layer/Transport Layer Security). Documentez exhaustivement toutes les procédures opérationnelles et instaurez un programme de maintenance régulière pour surveiller, analyser et mettre à jour les systèmes, afin d'assurer une gestion optimale et sécurisée de l'infrastructure.

Sujet pratique :

Explication :

Cette section est importante car elle stipule l'ensemble des taches qui vont devoir être réalisée sur l'infrastructure dans l'ordre. Elle découle d'une analyse profonde du sujet et est élaboré de sorte a ce que chaque système et service s'imbrique fonctionnellement avec les systèmes ou services qui suivent. Pour aider à la compréhension, chaque tache correspond à une machine de notre système, une tache est composée de sous-tâches qui correspondent à l'ensemble des actions à effectuer sur chaque machine. Cette démarche a pour but de faciliter la compréhension en évitant le « role-back » (action de revenir en arrière) qui peuvent perdre le lecteur. Les taches découlent donc du nombre de machine présentent sur notre infrastructure, nous décomptons donc 6 taches (en excluant les clients qui ne représentent pas une tache a par-entière) étant : « machine IPfire », « machine PFsense Master », « machine PFsense Slave », « machine Serveur WEB », « machine nextcloud » et « machine serveur de messagerie ». A noter que lors de notre compte rendu il peut être nécessaire d'utiliser une machine cliente pour accéder a certain service ne pouvant être exécutaient que depuis une interface WEB dans ce cas la les machine cliente ne représenteront pas une tâche à part entière.

Tables de matières :

Taches :

Machine IPfire :	Tache 1.0
- Paramétrage de 3 interfaces (Rouge, Vert, Orange)	Tache 1.1
- Création des espaces (DMZ, LAN , WAN)	Tache 1.2
- Mettre en place les systèmes IDS/ IPS	Tache 1.3
- Mettre en place le NAT/ PAT	Tache 1.4
Machine PFsense Master	Tache 2.0
- Paramétrage de 2 interfaces (LAN et CARP)	Tache 2.1
- Activer le service DHCP	Tache 2.2
- Activer et paramétrer le service DNS	Tache 2.3
- Activer CARP	Tache 2.4
- Création IP virtuelle	Tache 2.5
Machine PFsense Slave	Tache 3.0
- Paramétrage de 2 interfaces (LAN et CARP)	Tache 3.1
- Activer CARP	Tache 3.2
- Activer IP virtuel (synchronisation)	Tache 3.3
Serveur WEB	Tache 4.0
- Installation du paquet APACHE 2	Tache 4.1
- Mise en place de la page WEB personnalisée	Tache 4.2
- Mise en place du certificat SSL	Tache 4.3
Serveur Nextcloud	Tache 5.0

- Installation des paquets adéquats Tache 5.1
- Configuration des utilisateurs Tache 5.2

Serveur de messagerie Tache 6.0

- Installation des paquets adéquats Tache 6.1
- Configuration des utilisateurs Tache 6.2

Test Tache 7.0

- Test des services Nextcloud & Pfsense Tache 7.1

Mesure explicative :

Les pares-feux ont en effet des rôles. Le premier rôle est « MASTER », ce qui signifie que ce pare-feu sera le premier à répondre en cas de tentative de communication avec l'adresse IP 172.22.250.1, mais également que toute modification impactant ce pare-feu devra également impacter le pare-feu ayant le rôle « SLAVE ».
Le rôle « SLAVE », quant à lui, est secondaire dans la tentative de communication avec l'adresse IP 172.22.250.1 et ne commence à répondre que si le pare-feu dit MASTER ne peut pas répondre.

La synchronisation via le protocole CARP entre deux pare-feu PFSENSE repose sur la communication régulière entre les nœuds pour surveiller l'état de santé de chacun. Chaque pare-feu est configuré avec une adresse IP virtuelle partagée, et ils se disputent le rôle de maître, responsable de la gestion de cette adresse IP. Les pares-feux échangent des « cœurs » à intervalles réguliers pour détecter les pannes potentielles. En cas de défaillance d'un pare-feu, l'autre prend rapidement le relais et assume le rôle de maître, garantissant ainsi une continuité de service sans interruption perceptible pour les utilisateurs, tout en maintenant la cohérence des connexions réseau.

Lecture.
Tout au long de ce compte rendu, vous trouverez l'ensemble des étapes de mise en place de cet atelier. Cependant, pendant cet atelier, il sera nécessaire de mettre en place des protocoles de test afin de vérifier le bon fonctionnement et la bonne conduite de celui-ci. Pour repérer ces passages de test, ils seront écrits en bleu au lieu du noir traditionnel, suivant le déroulé de l'analyse descendante.

Schéma :

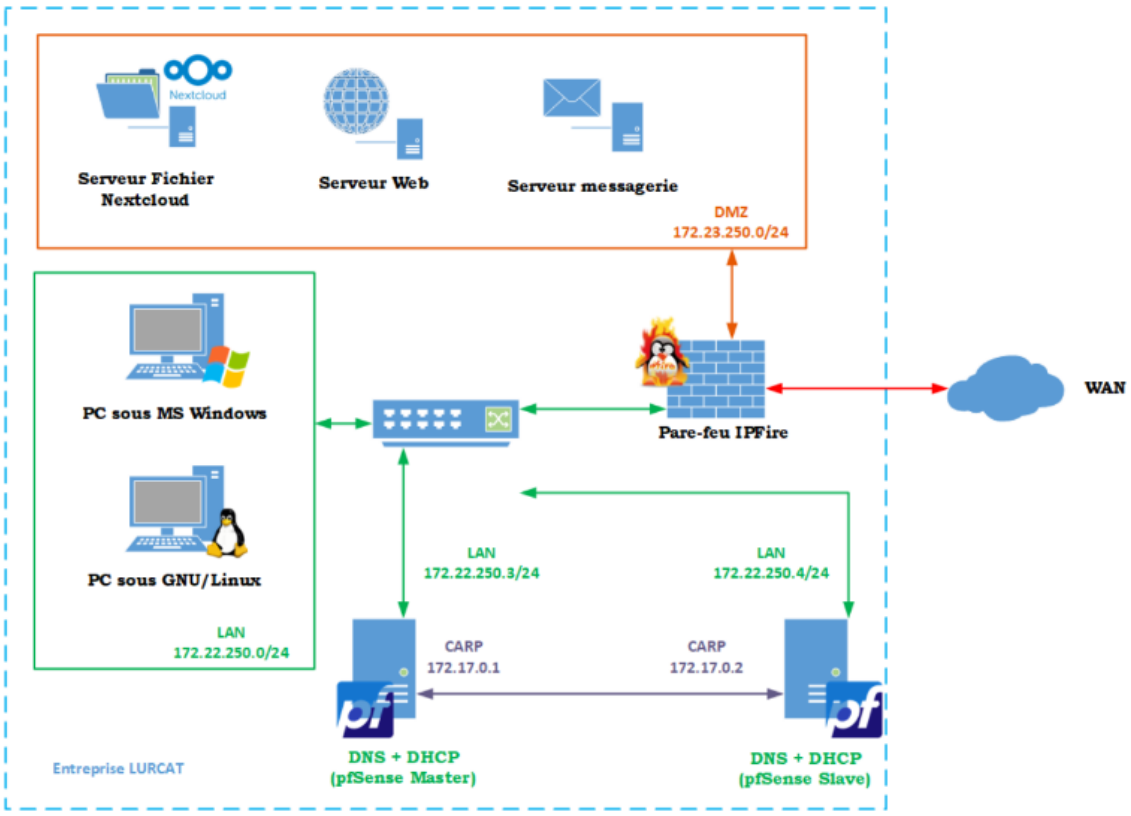


Table des IP

Cette partie répertorie l'ensemble des adresses IP qui vont être utilisées et attribuées aux différentes machines.

Machine IPfire :

Interface WAN → DHCP du au NAT

Interface LAN → 172.22.250.1/24

Interface DMZ → 172.23.250.1/24

Machine PFsense Master

Interface LAN → 172.22.250.3/24

Interface CARP → 172.17.0.1/24

IP virtuelle → 172.22.250.2/24

Machine PFsense Slave

Interface LAN → 172.22.250.4/24

Interface CARP → 172.17.0.2/24

IP virtuelle → 172.22.250.2/24

Serveur WEB

Interface DMZ →172.22.250.10/24

Serveur Nextcloud

Interface DMZ → 172.22.250.11/24

Serveur de messagerie

Interface DMZ → 172.22.250.12/24

Les machines bénéficient du service DHCP du réseau LAN serons au sein de l'étendue :

➔ 172.22.250.150/24 à 172.22.250.200/24

1.0 Machine IPfire

Le but est donc de mettre en place la machine IPFire.

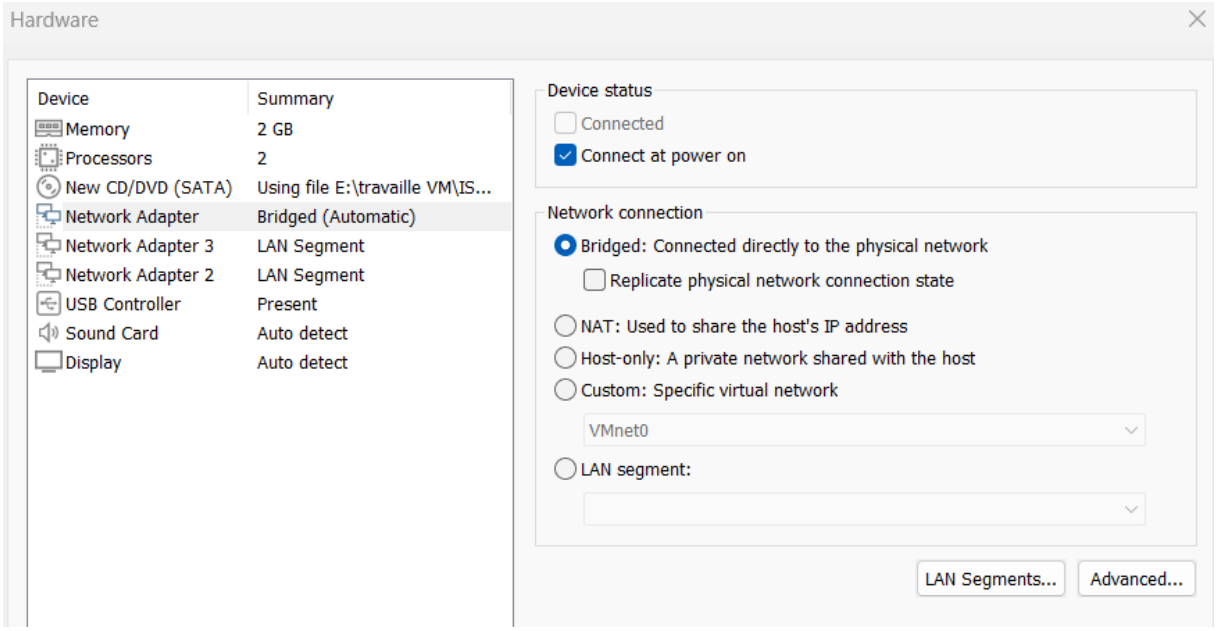
IPFire est un système d'exploitation spécialisé, axé sur la fonctionnalité de pare-feu, conçu pour sécuriser les réseaux informatiques. Basé sur Linux, il est développé pour être sécurisé, flexible et gratuit. IPFire se distingue par sa capacité à s'adapter à divers types d'environnements, allant des petites installations domestiques aux grandes infrastructures d'entreprise.

Le système repose sur une interface web conviviale qui facilite la configuration et la gestion des règles de pare-feu, du NAT (Network Address Translation), des services VPN (Virtual Private Network), ainsi que d'autres fonctionnalités de sécurité comme la détection d'intrusions et le filtrage de contenu.

IPFire peut être configuré pour agir comme un pare-feu de bordure, gérant le trafic entre plusieurs sous-réseaux. Il propose également des fonctions avancées, telles que la gestion de la qualité de service (QoS), permettant de prioriser le trafic réseau. En résumé, IPFire est une solution de pare-feu puissante et personnalisable, souvent choisie pour sa robustesse et sa capacité à renforcer la sécurité des réseaux.

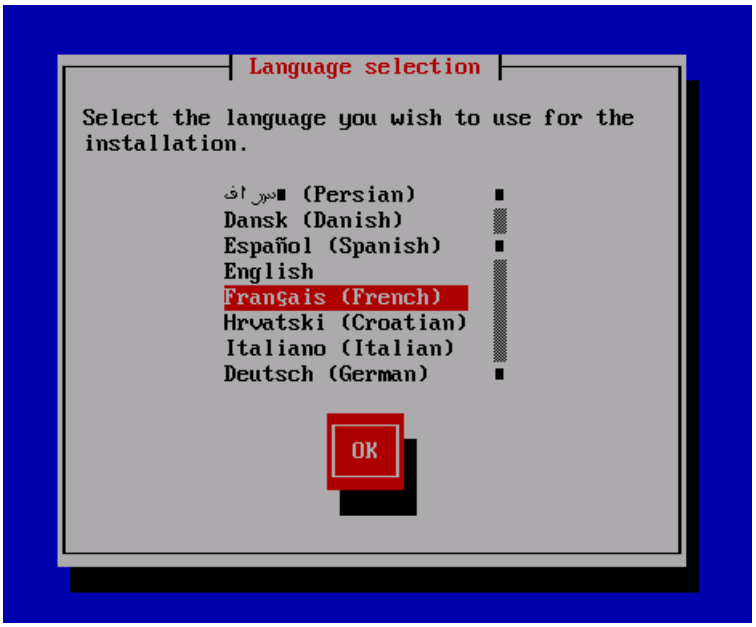
On installe donc l'ISO dans la machine virtuelle, et on s'assure que la VM dispose de trois interfaces réseau : une pour chaque zone (LAN, WAN, DMZ).

Pour cela, on crée deux réseaux internes pour les zones LAN et DMZ, tandis que le réseau WAN sera assuré par le bridge connecté à mon réseau personnel.

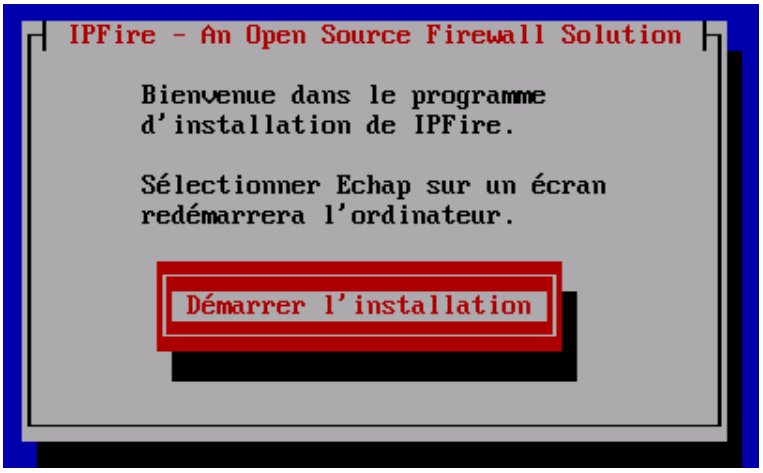


A partir de là nous allons lancer l'initialisation de IPfire

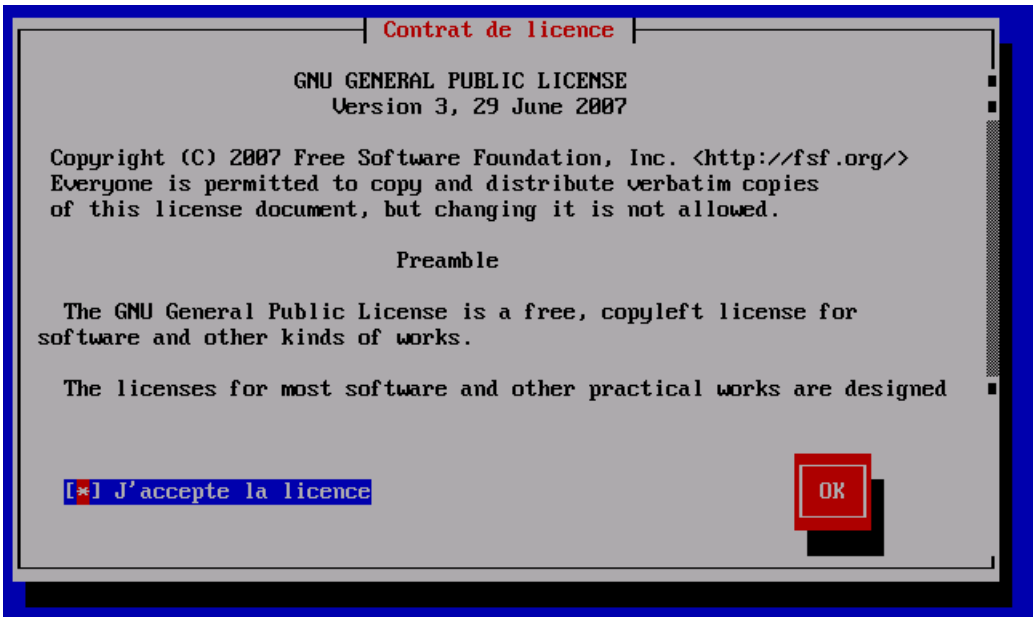
Puis choisir notre langue



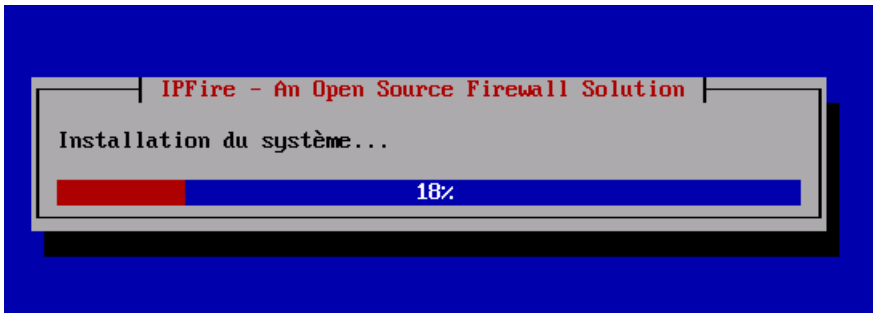
Et démarrer l'installation



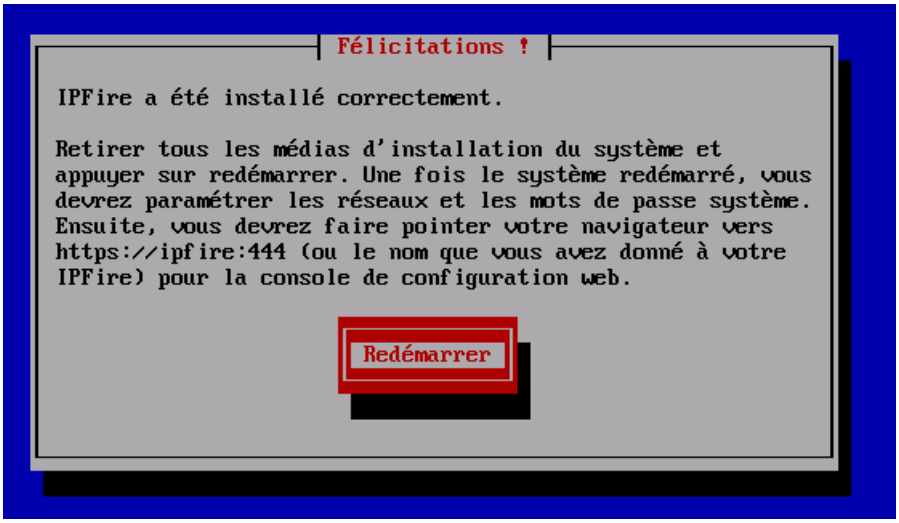
On accepte le contrat de License



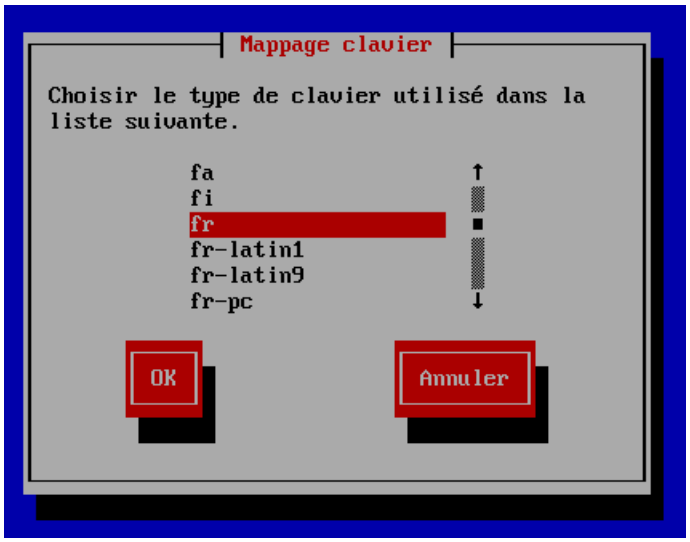
L'installation se lance



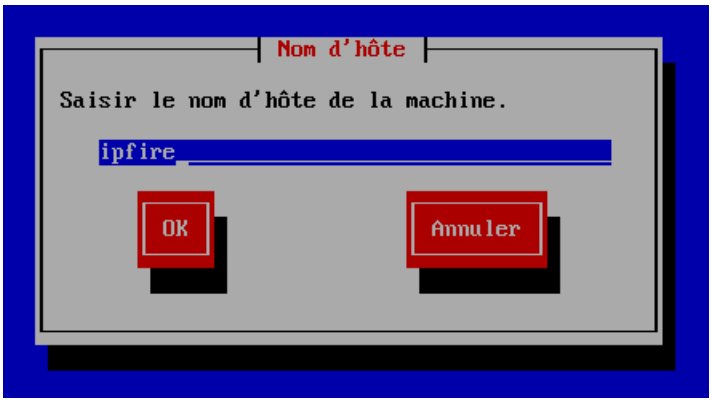
Le système a besoin de redémarrer pour exécuter son rôle correctement



A présent, on nous demande le « mappage clavier » qui correspond à la configuration des touches de notre clavier.



On nous demande ensuite le « nom d'hôte » de la machine qui correspond à nom que portera la machine sur les réseaux. Dans notre cas cela sera : « ipfire »



Le domaine devrait se détecter automatiquement, dans notre cas nous le laissons par default car il n'y a actuellement pas de domaine

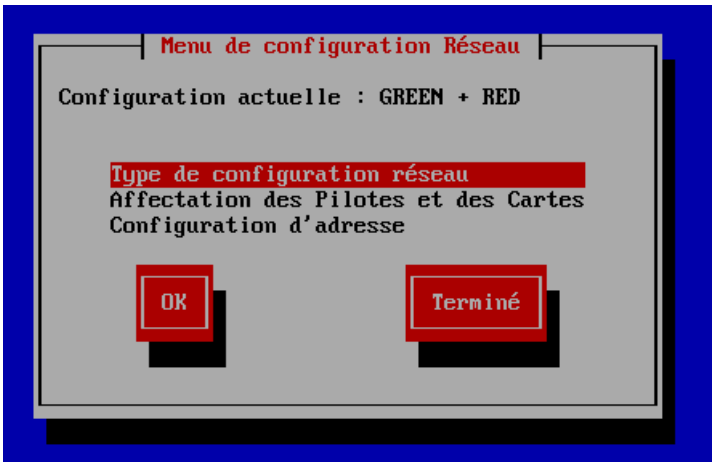
Dans cette section, il nous est demandé de sélectionner un mot de passe pour le système. Je vous conseille un mot de passe robuste car cette machine représente un des poumons de votre sécurité

A présent le système nous demande la configuration réseau de l'ipfire.

IPfire fonctionne avec un système de couleur. Chaque couleur représente un réseau différent :

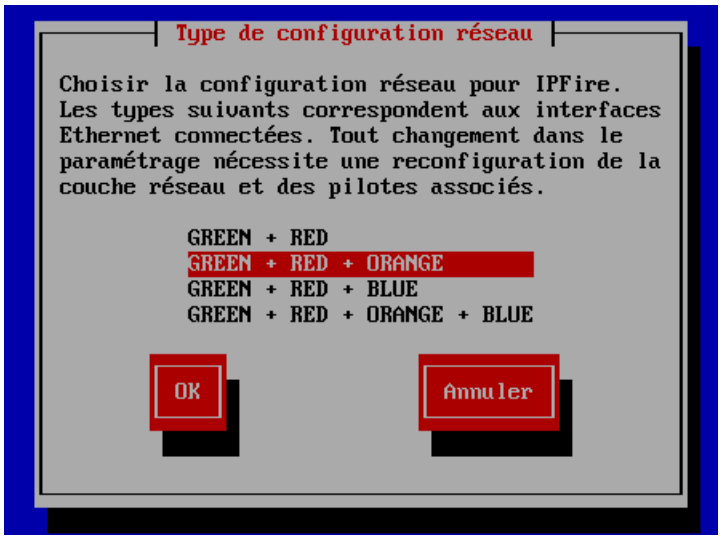
- Rouge pour WAN (réseau étant connecté à internet),
- Vert pour LAN (réseau personnel),
- ORANGE pour DMZ (réseau isolé des autres)
- BLEUE Pour VLAN (que nous ne traiterons pas dans ce compte rendue)

Dans notre cas notre infrastructure est composée d'une DMZ et d'un réseau WAN et LAN donc ce sera la configuration ROUGE+VERT+ORANGE qui sera sélectionnée

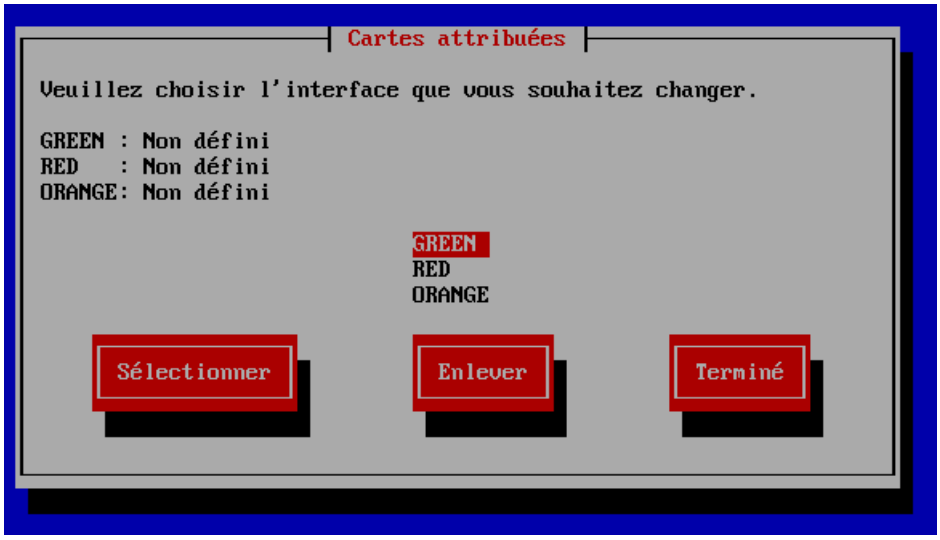


(La configuration par default ne va pas car elle propose VERT+ROUGE)

On sélectionne dont « type de configuration réseau »

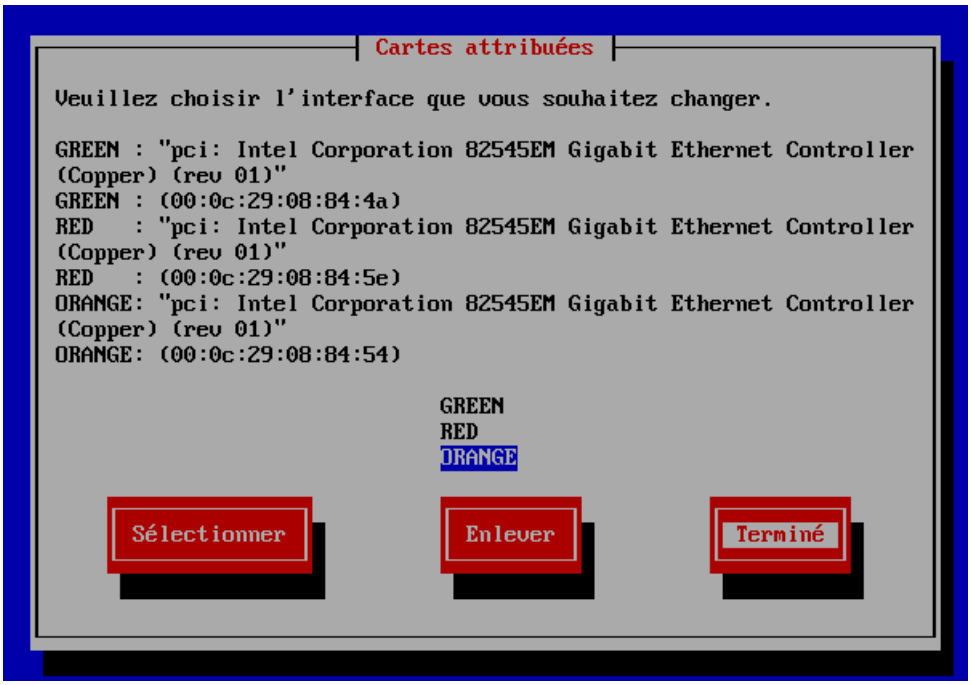


On sélectionne donc l'option "GREEN + RED + ORANGE"

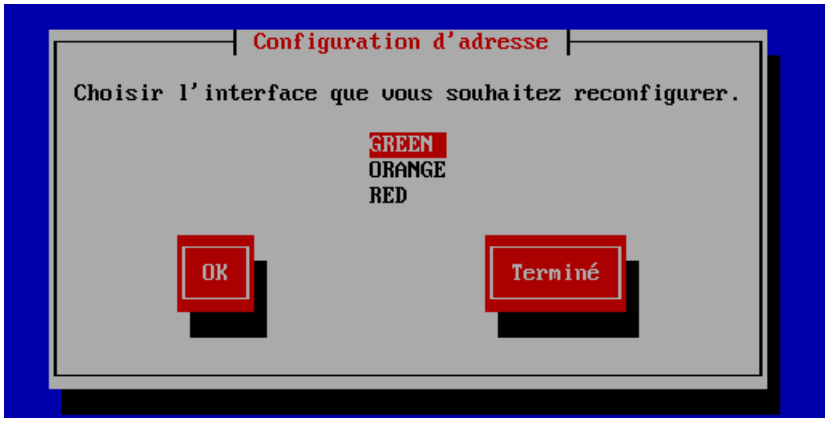


A présent il faut assigner chaque adresse MAC des cartes réseau à chaque couleur

(Pour cette étape il faut vous référencer au carte réseau de chacune de vos interfaces)



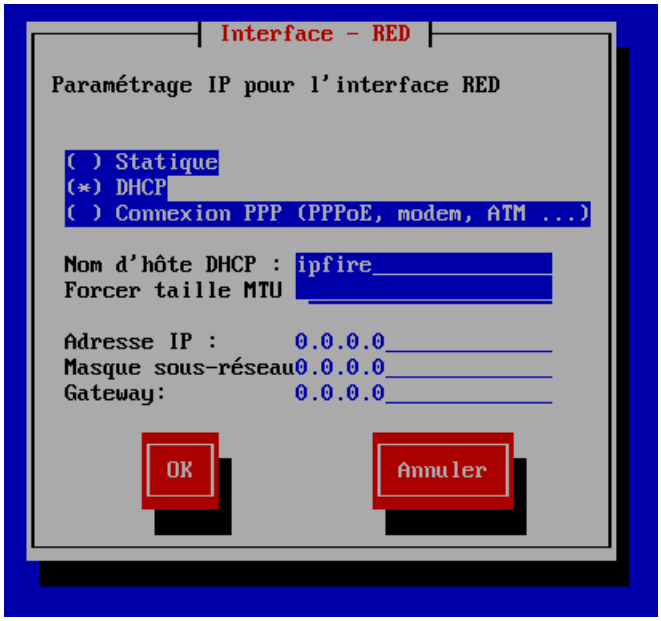
Voici ma configuration pour chaque adresse MAC



On passe maintenant à la configuration IP de chaque interface, On commence par la verte qui selon « la table des IP » devra être 172.22.250.1/24

Puis par l'orange qui sera 172.23.250.1/24

Ensuite, l'interface **RED** (rouge), correspondant à la zone **WAN**, recevra automatiquement une **adresse IP via DHCP**, puisque cette interface est reliée à un **réseau NAT** fourni par l'hôte.

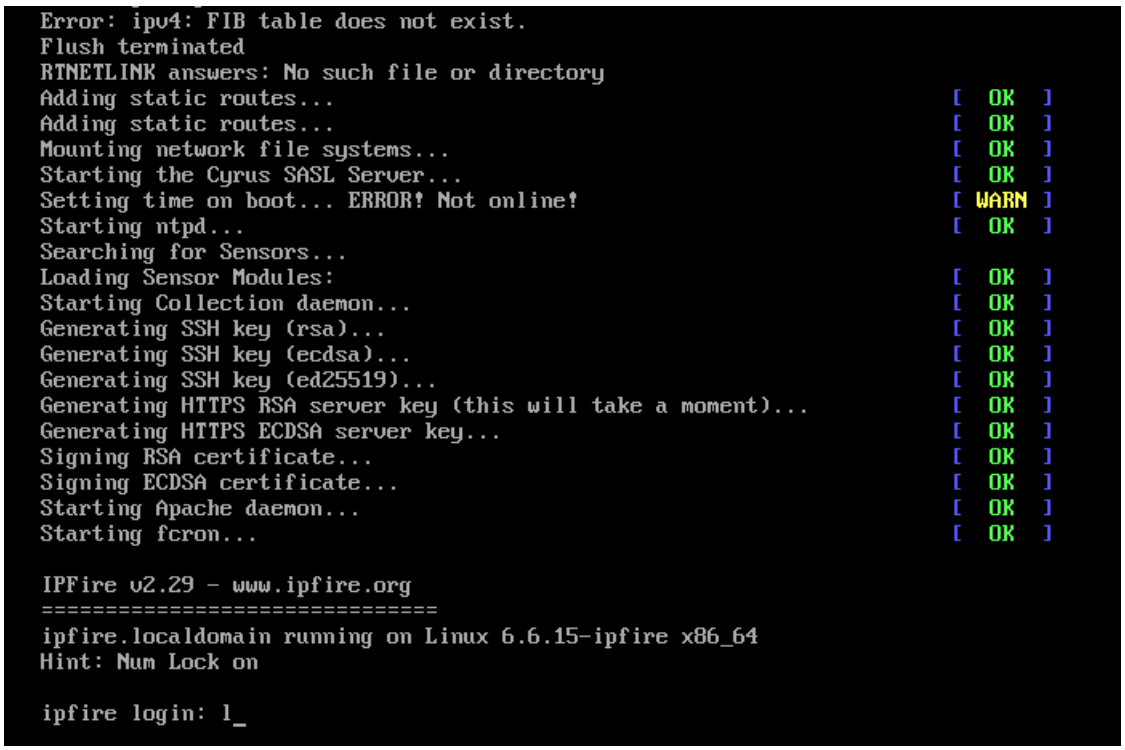


On peut à présent terminer l'initialisation

Puis valider

Les taches 1.1 et 1.2 sont terminées (Paramétrage de 3 interfaces (Rouge, Vert, Orange))

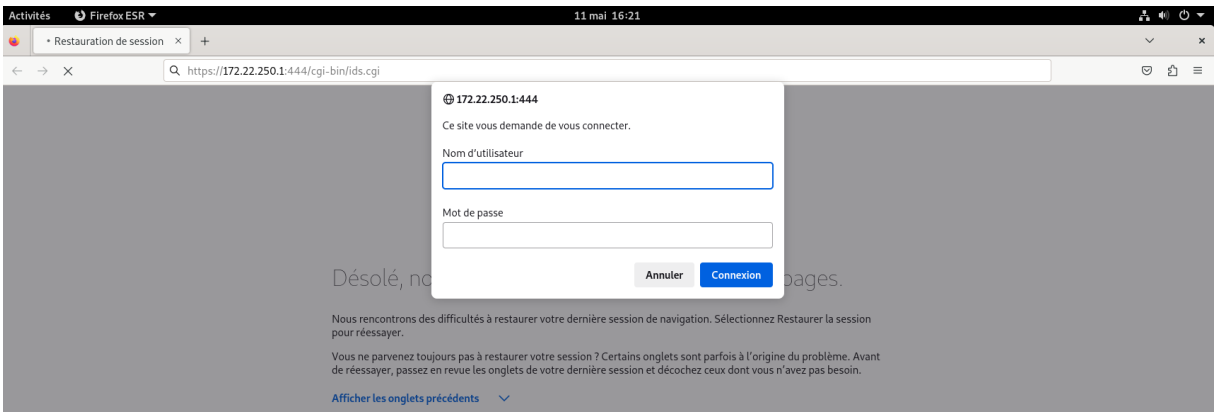
Une fois que l'initialisation est terminée, nous arrivons sur l'interface de base



Nous allons à présent poursuivre la configuration d'**IPFire** depuis son **interface web**.
Pour cela, il est nécessaire d'importer une **machine cliente** dotée d'un **navigateur web** et connectée au **réseau LAN** de l'infrastructure.

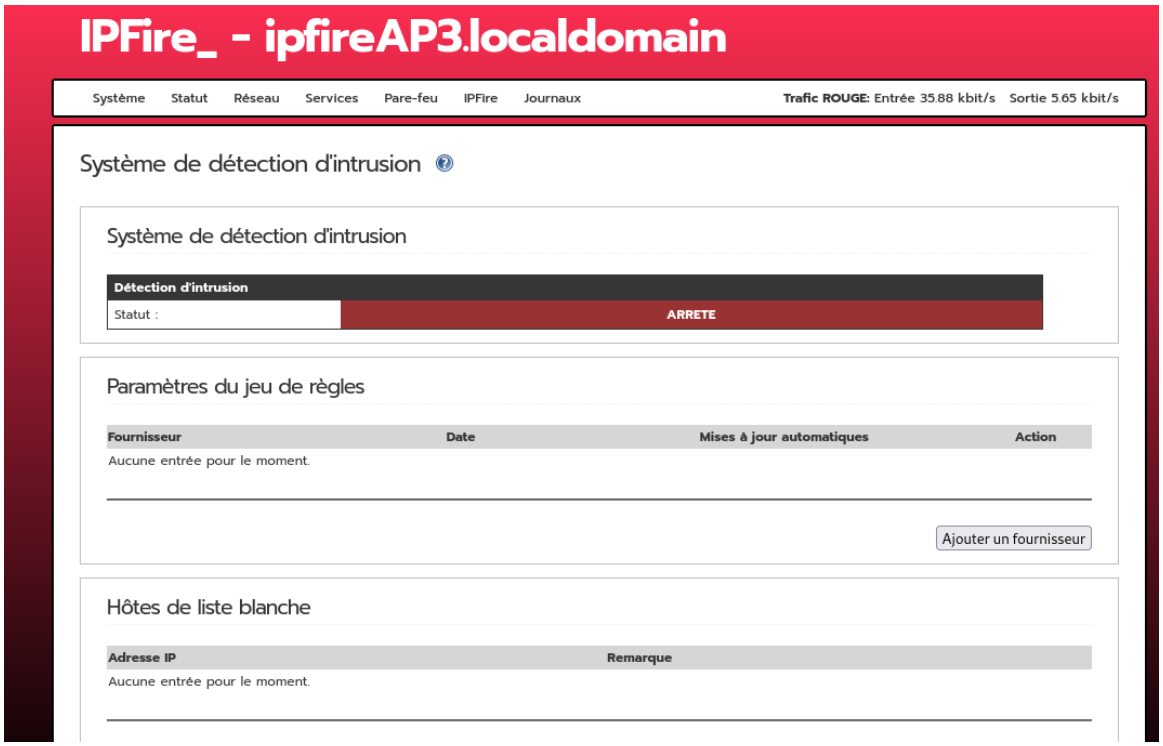
L'adressage IP de cette machine devra être **configuré manuellement**, car aucun service **DHCP** n'est encore actif sur le réseau LAN.

Depuis cette machine, il faudra accéder à l'interface d'IPFire en entrant l'URL suivante dans le navigateur :
https://[adresse IP de l'interface GREEN]:444



La page web vas vous demander à partir de là le nom et mot de passe de l'utilisateur root que nous avons paramétré plus tôt

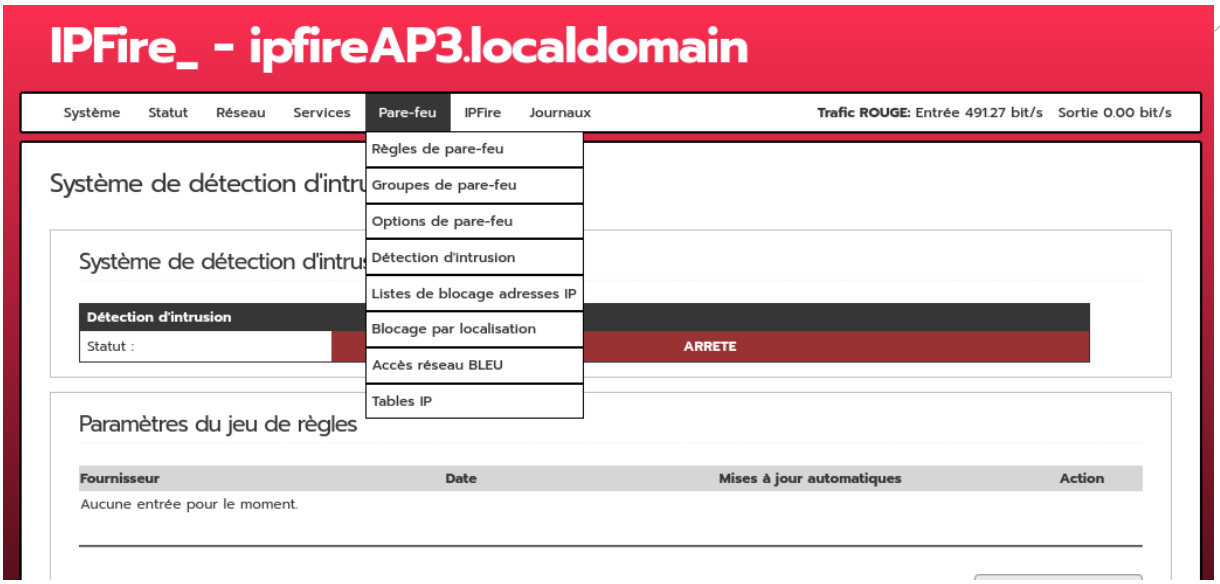
Nous arrivons donc sur la page d'accueil de l'interface WEB de IPfire



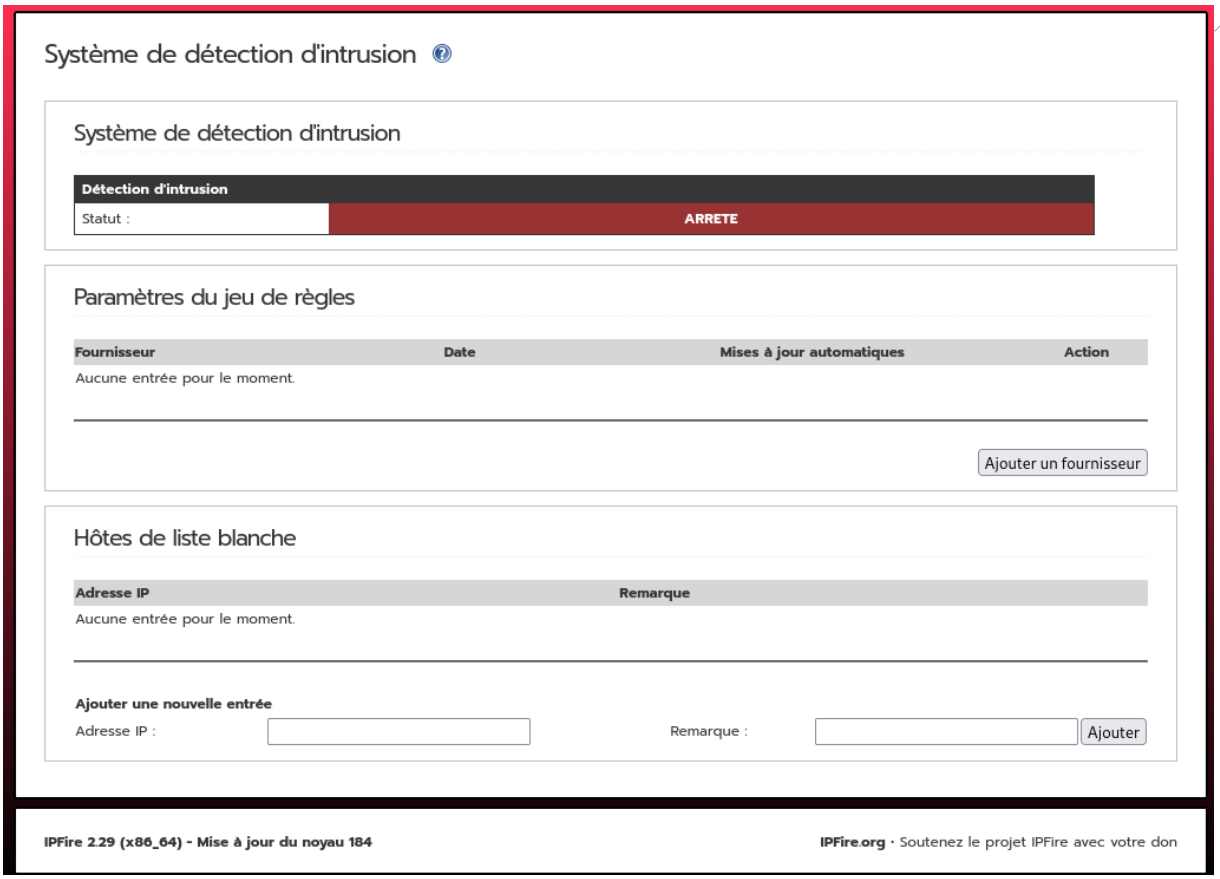
La première chose que nous allons faire sera de mettre en place le système IDS/IPS

Les systèmes IDS (Intrusion Detection System) et IPS (Intrusion Prevention System) sont des composants essentiels pour renforcer la sécurité des réseaux informatiques. Un IDS surveille et analyse le trafic réseau à la recherche de signes d'activités suspectes ou malveillantes, alertant les administrateurs lorsqu'une menace potentielle est détectée. À l'inverse, un IPS étend cette fonctionnalité en prenant des mesures actives pour bloquer ou atténuer ces menaces en temps réel, avant qu'elles n'affectent le réseau. Ensemble, ils offrent une protection robuste en identifiant les comportements anormaux, en utilisant des bases de données de signatures d'attaques, et en implémentant des politiques de sécurité pour prévenir les intrusions et garantir l'intégrité du réseau. Ces systèmes sont vitaux pour maintenir la sécurité et la performance du réseau face aux menaces croissantes et sophistiquées.

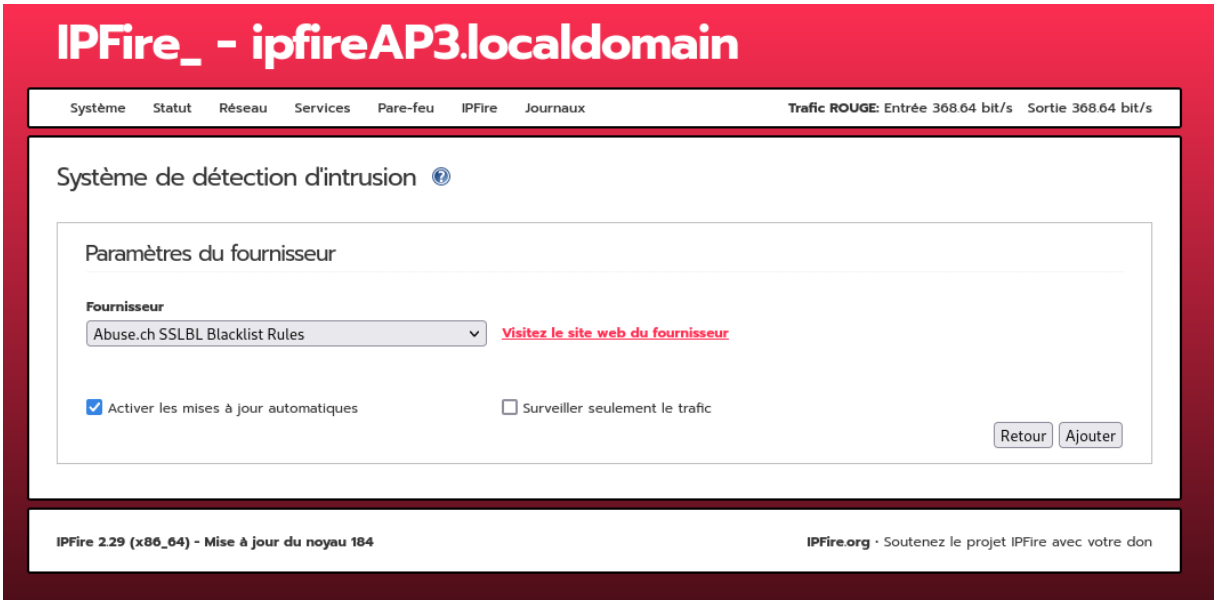
Pour cela, il ne faut pas aller chercher bien loin, et cliquer sur « détection d’intrusion »



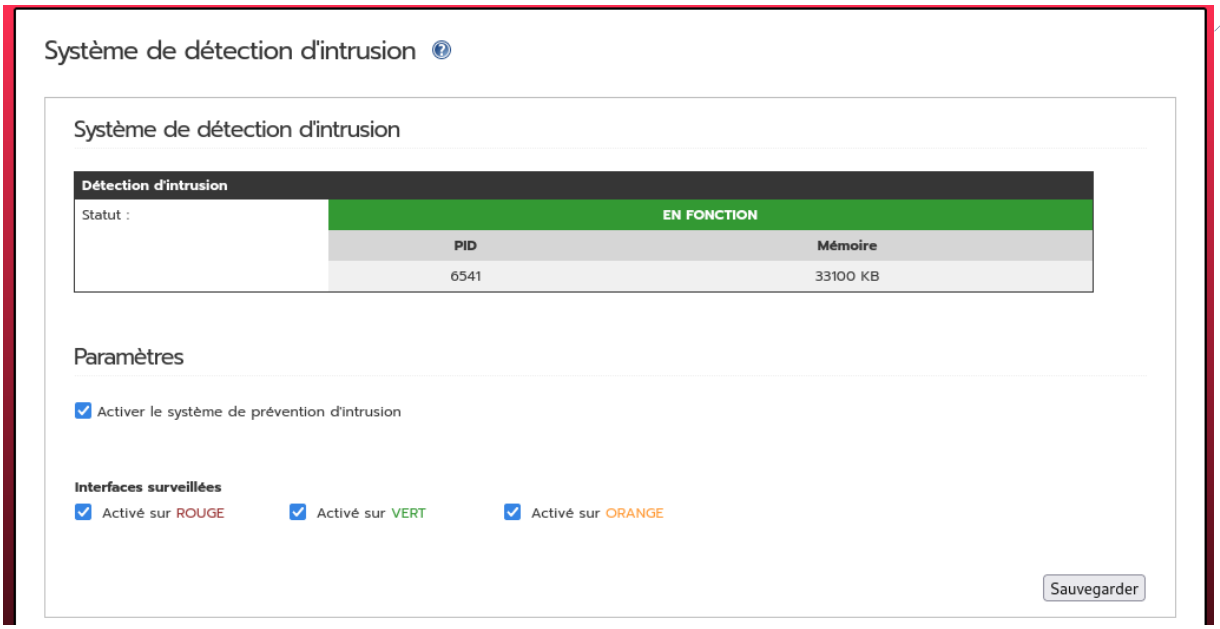
Et vous arrivez sur cette page



Il faut ajouter un fournisseur, on sélectionne donc le fournisseur « Abuse.ch » qui est une liste de facteur qui servent à la détection des intrusions par des attaques connues. Cette liste est constamment mise à jour ce qui assure une veille des failles de sécurité



Puis on clique sur ajouter



Voilà le système IDS/IPS est fonctionnel, on peut le voir grâce à la notion écrit en blanc sur vert « EN fonction »

La tache 1.3 est terminé (Mettre en place les systèmes IDS/ IPS)

Nous allons maintenant mettre en place les règles NAT qui vont nous permettent d'accéder aux services de la DMZ depuis le réseau WAN. Et ce, même si les services n'existent pas encore, nous pouvons anticiper leur adresses IP et leur port d'utilisation

Il y 3 services dans la DMZ :

Serveur WEB →172.23.250.10/24

Serveur Next cloud →172.23.250.11/24

Serveur de messagerie →172.23.250.12/24

Tous ces services sont constitués du même schéma : un serveur WEB avec un applicatif derrière

Pour distinguer chacun de ces services depuis le WAN, nous pouvons utiliser les ports d'utilisations de ces serveurs WEB, tous ces serveurs vont utiliser le protocole HTTPS et nous pouvons choisir manuellement par quel port ils peuvent communiquer donc nous allons attribuer un port de communication du protocole https pour pouvoir distinguer chacun des serveurs à travers le WAN.

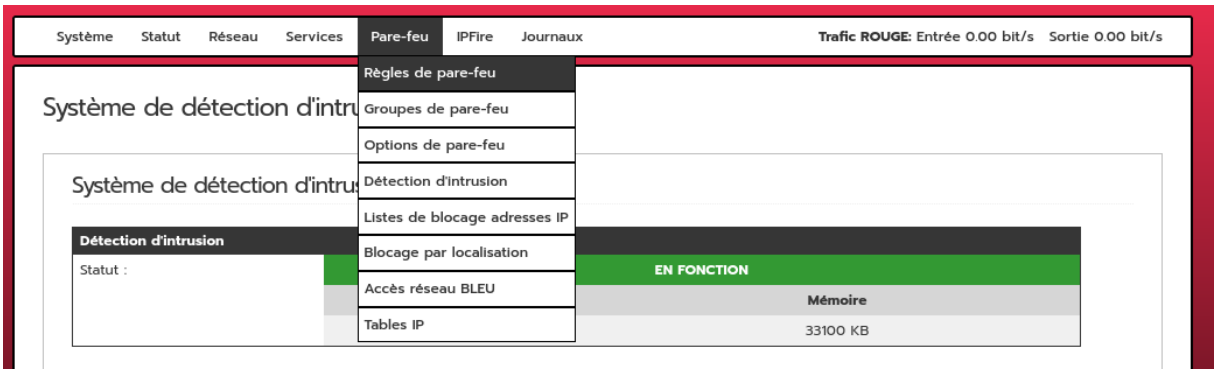
Le serveur WEB utilisera le port 2002

Le serveur Next cloud utilisera le port 2005

Le serveur messagerie utilisera le port 2007

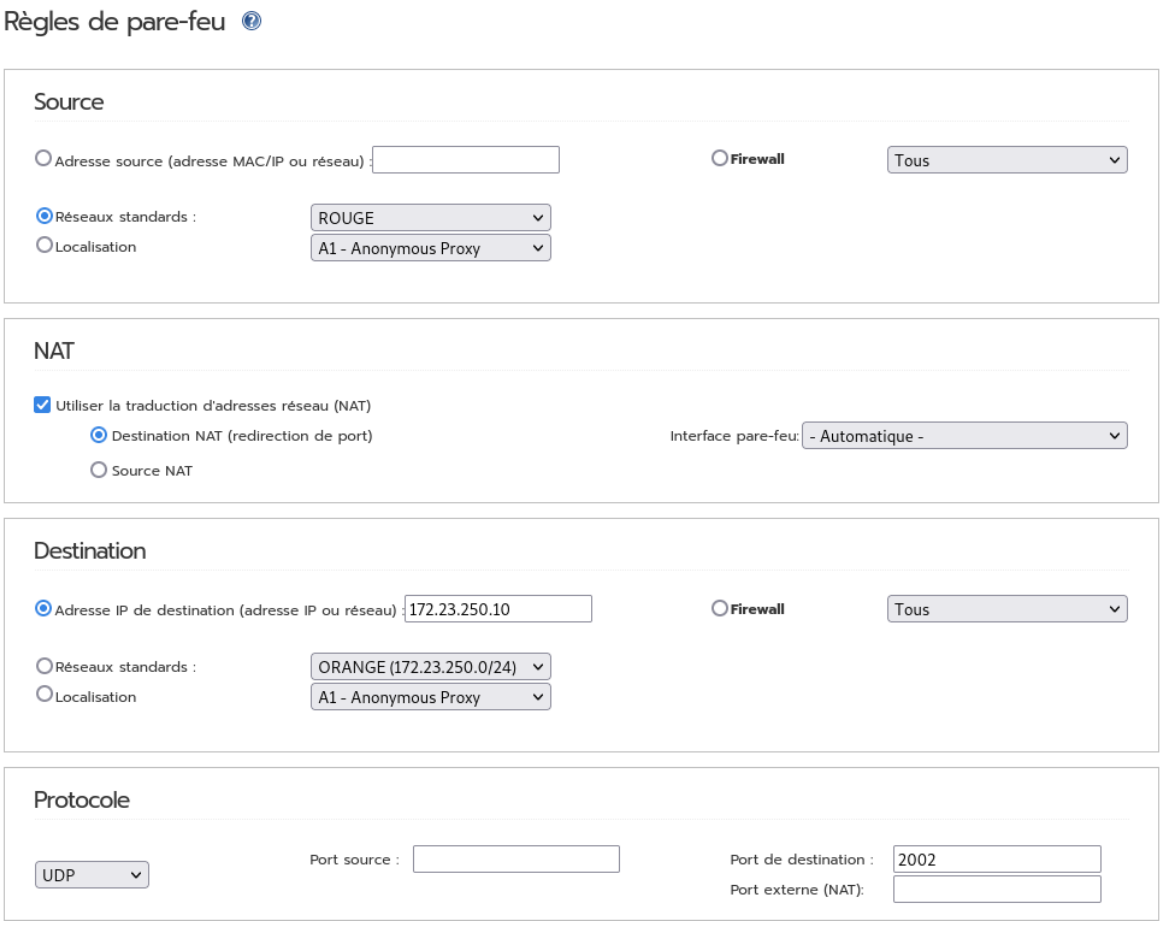
Garce à ces informations, nous sommes en mesure d'établir les règles de NAT pour rendre accessible ces futurs services à travers le WAN

Pour cela on se rend donc dans la section règle de pare-feu



On click ensuit sur « nouvel règle »

Pour la première redirection de port, nous allons commencer par le serveur WEB



Pour cela, on sélectionne la **source**, c'est-à-dire l'**interface** par laquelle la redirection de port doit être effectuée. Dans notre cas, il s'agit de l'interface **WAN**, qui correspond à l'interface **ROUGE**.

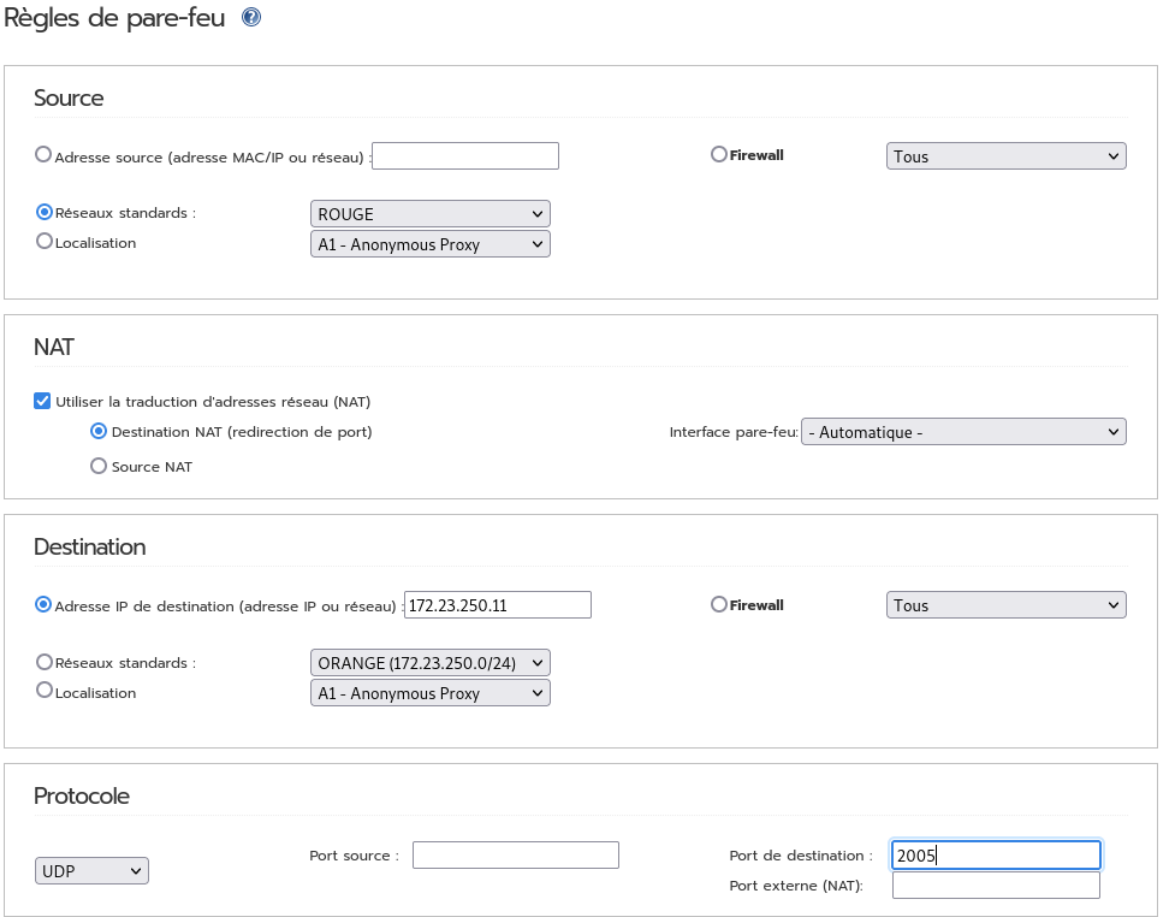
On active ensuite le **NAT** en cochant l'option **« Destination NAT (redirection de port) »**, ce qui signifie que nous souhaitons rediriger un port spécifique vers une machine interne.

Dans la section **Destination**, on renseigne l'adresse IP du **serveur web**, à savoir **172.23.250.10/24**.

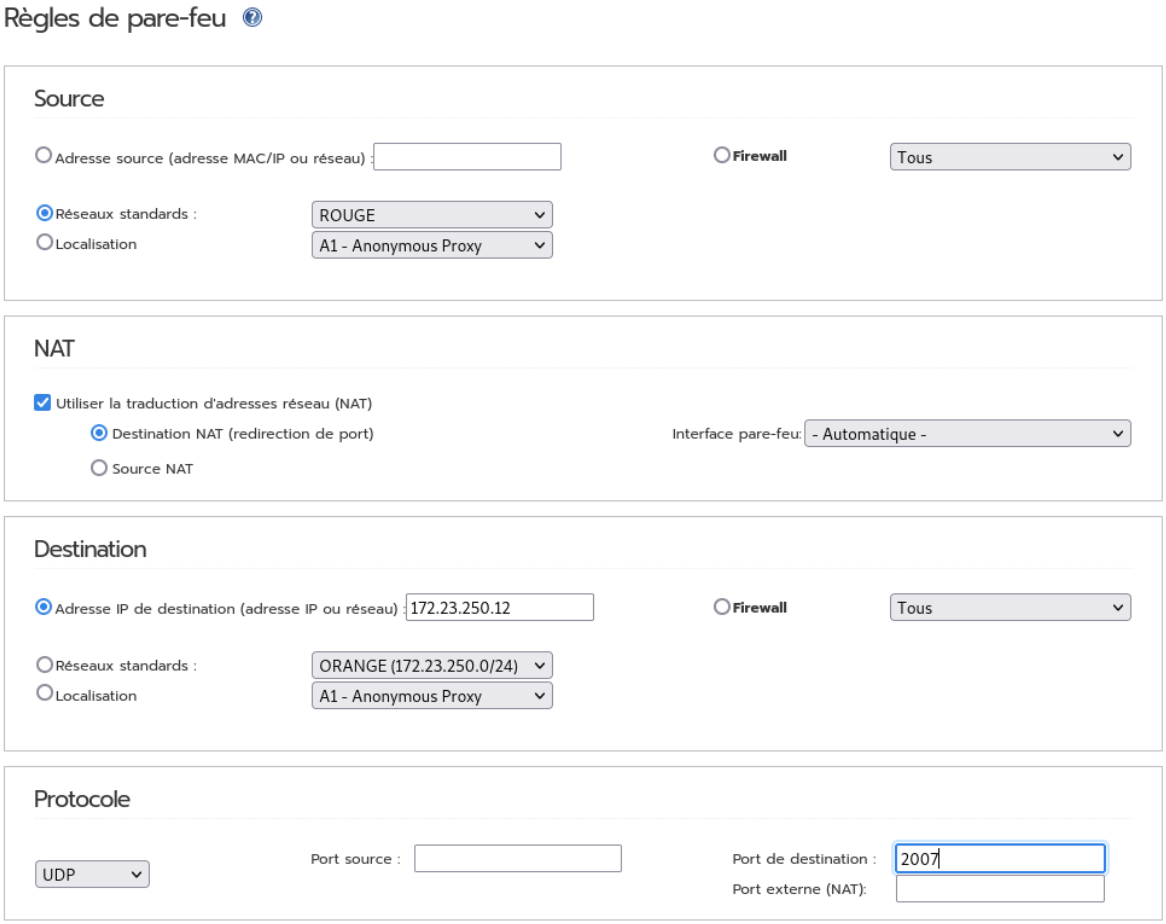
Dans la section **Protocole**, on spécifie le port de destination. Cela permet au service de communiquer via un port bien défini.
Dans notre cas, lorsque qu'un client souhaite accéder au serveur web, il devra impérativement utiliser le **port 2002**.

On répète pour les deux autres serveurs

Pour le serveur **Nextcloud**, situé à l'adresse **172.23.250.11/24**,
on configure une redirection de port en utilisant le **port 2005**.



Puis le serveur de messagerie qui sera en 172.23.250.12/24 et de port 2007



La tache **1.4** est terminé (Mettre en place le NAT/ PAT)

A présent nous allons réaliser les tâches de la section 2.0 (Machine PFsense Master)

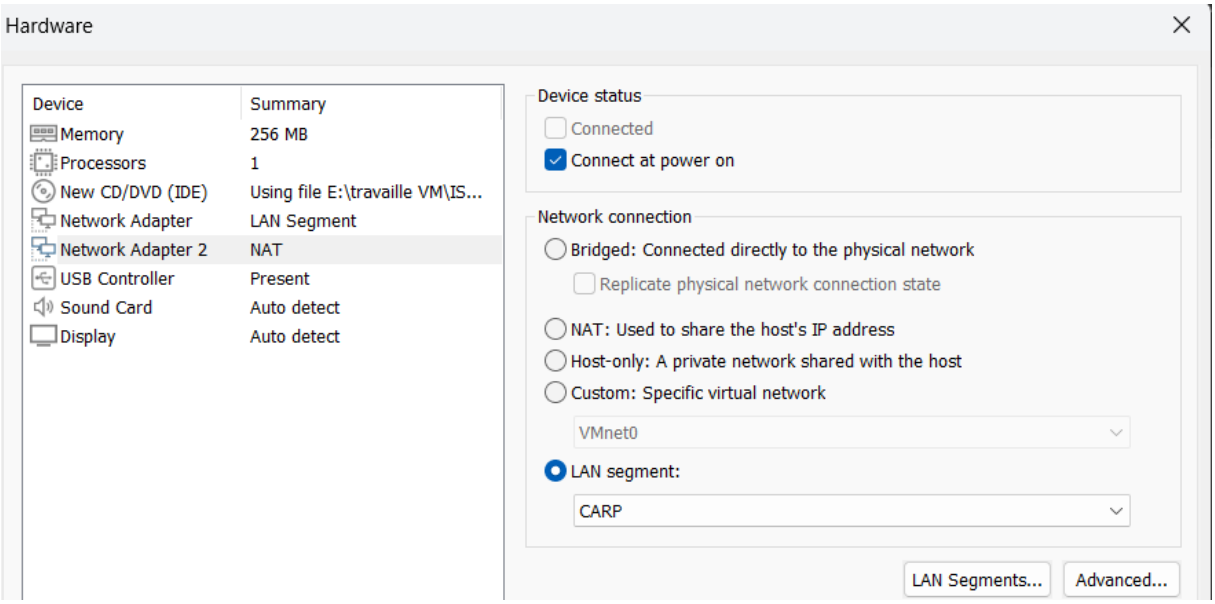
PFSENSE est une distribution **open-source** de pare-feu et de pare-feu basée sur **FreeBSD**, offrant une combinaison puissante de **fonctionnalités de sécurité avancées** et de **routage robuste**.
Sa flexibilité et son extensibilité en font un choix populaire pour les réseaux domestiques, les petites entreprises et les déploiements de taille moyenne.
Elle dispose d'une **interface web conviviale**, facilitant la configuration, et bénéficie d'une **communauté active**, fournissant un soutien continu ainsi que des **plugins additionnels**.
PFSENSE est ainsi une solution complète et personnalisable pour répondre à des besoins spécifiques en matière de sécurité et de routage réseau.

Nous allons commencer logiquement par l'initialisation de la machine **PFSENSE Master**, sur laquelle seront configurés l'ensemble des services, qui seront ensuite **répliqués automatiquement** sur la machine **PFSENSE Slave** via le protocole CARP.

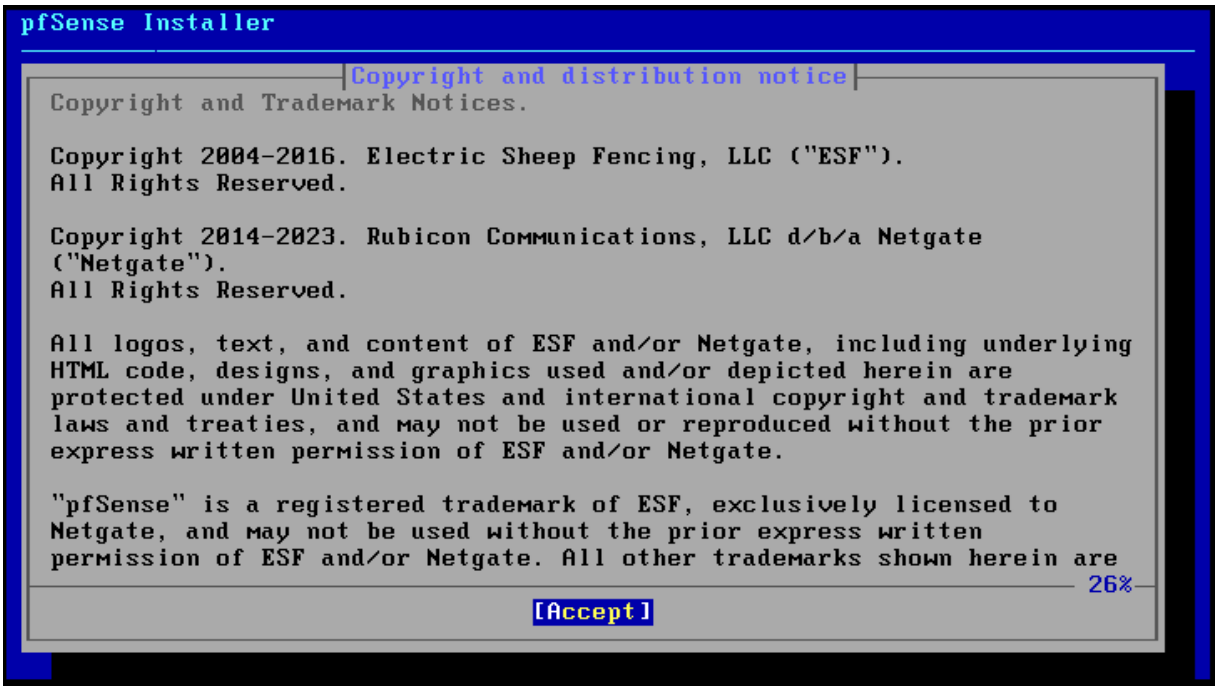
La première étape consiste à **initialiser le système d'exploitation PFSENSE**, juste après avoir créé la **machine virtuelle**.

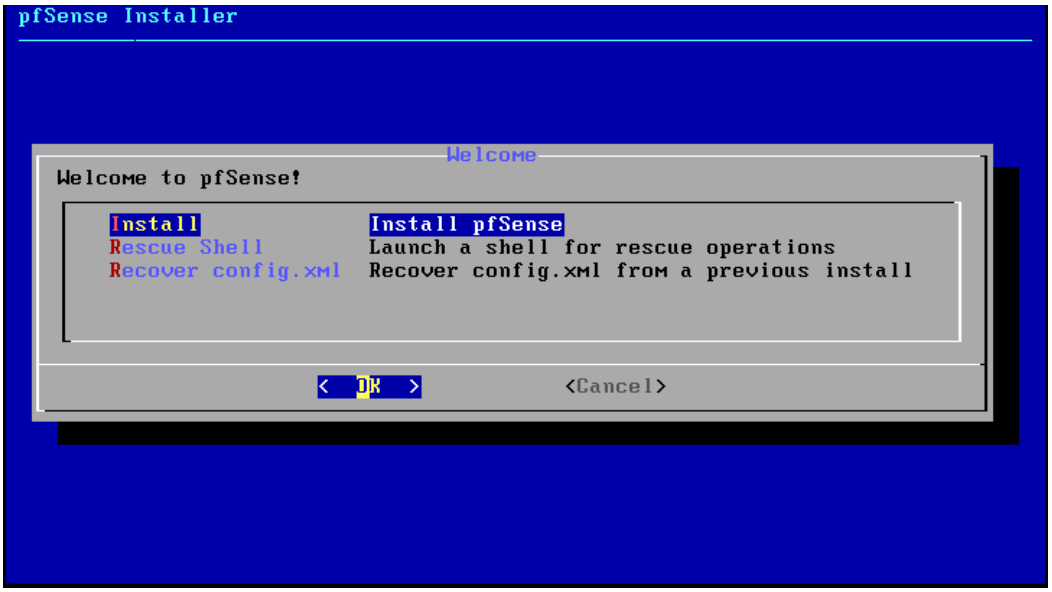
⚠️ Pour rappel, la machine **PFSENSE** doit disposer de **deux interfaces réseau** :

- Une interface pour **communiquer avec le LAN** (et fournir les services **DNS** et **DHCP**).
- Une seconde interface dédiée à la communication **CARP** avec la future machine **PFSENSE Slave**.

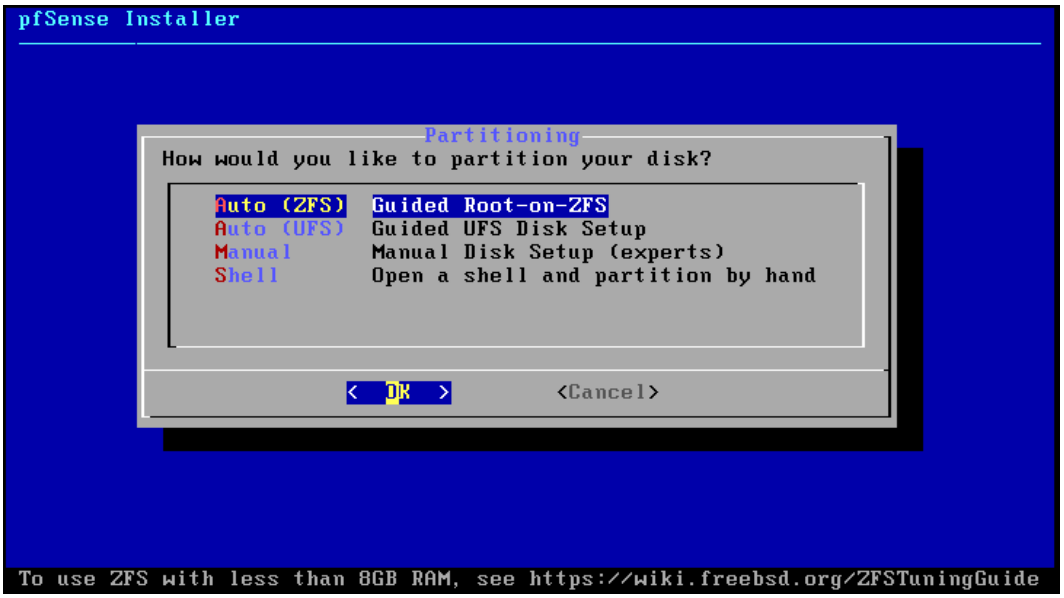


Nous allons maintenant procéder à l'initialisation du pare-feu PFSENSE MASTER

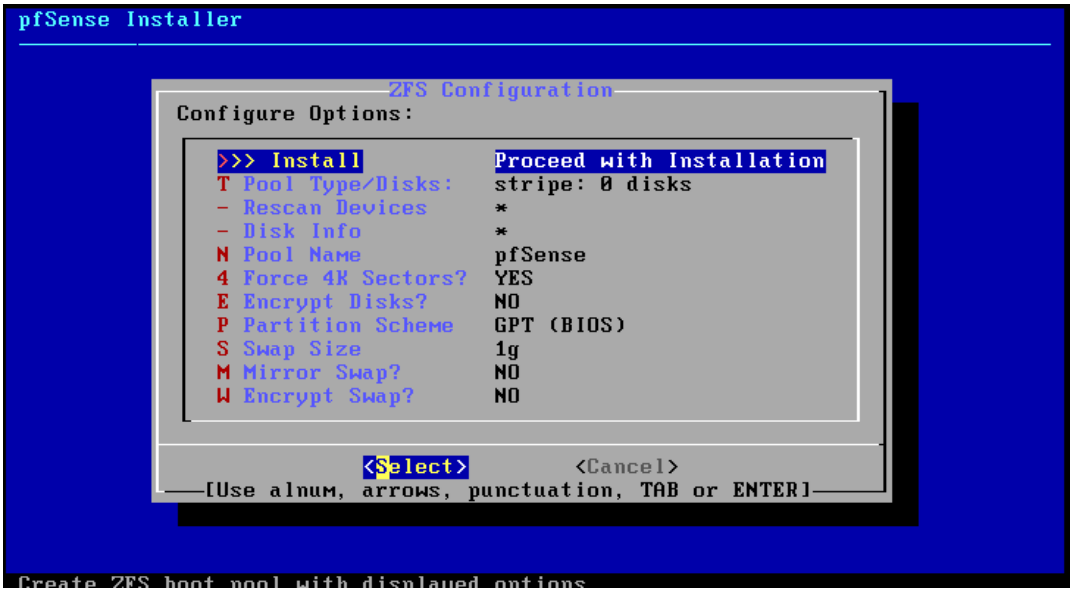


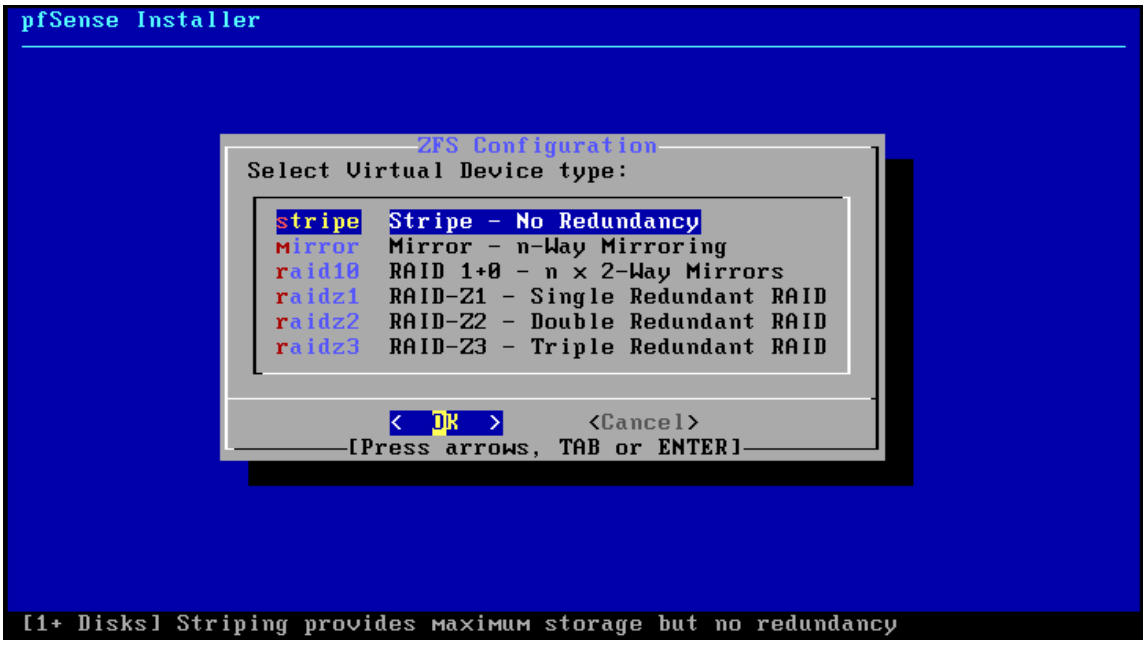


On choisit d'installer le système d'exploitation

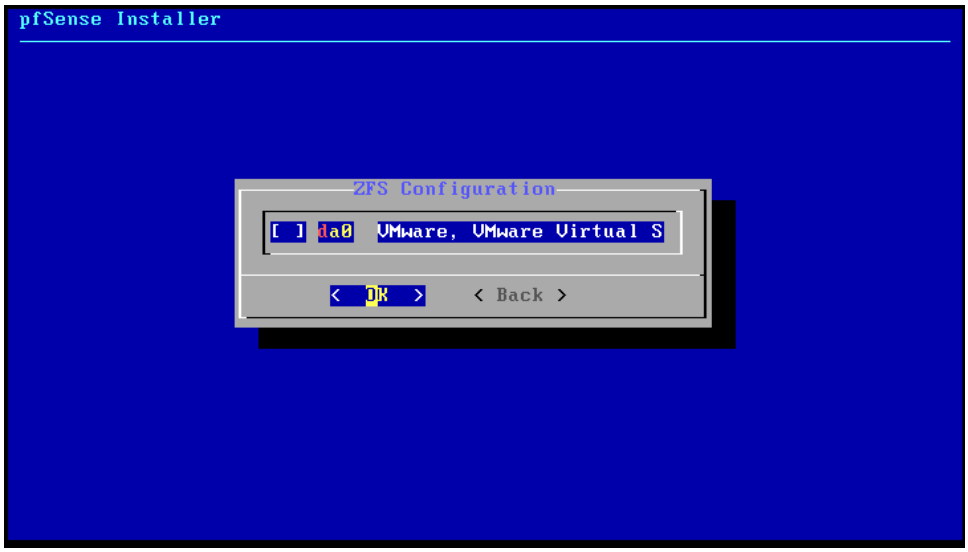


On sélectionne également l'installation guidée du système d'exploitation

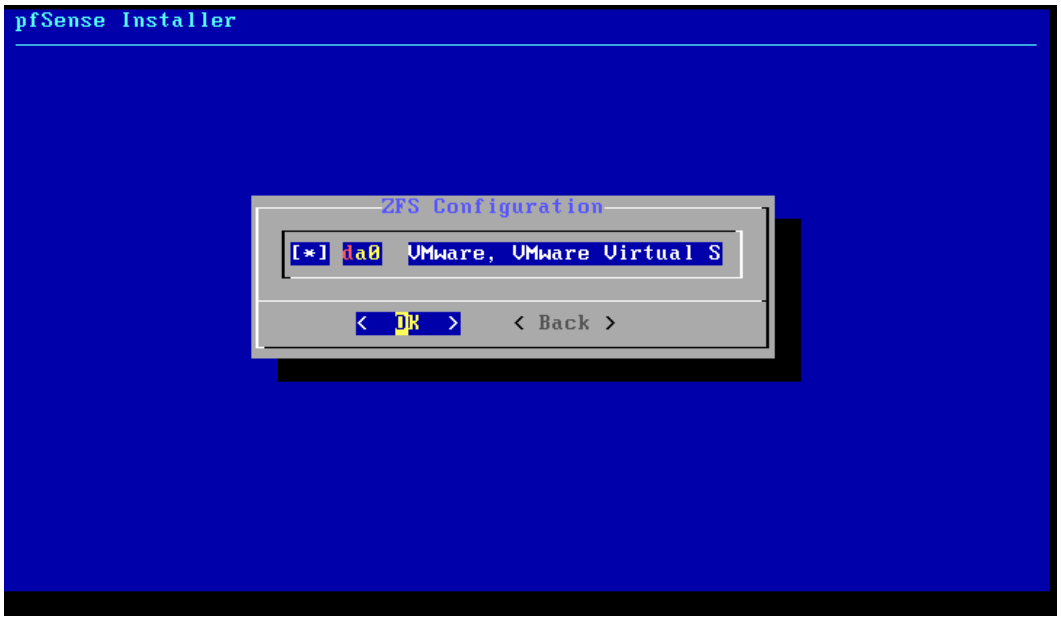




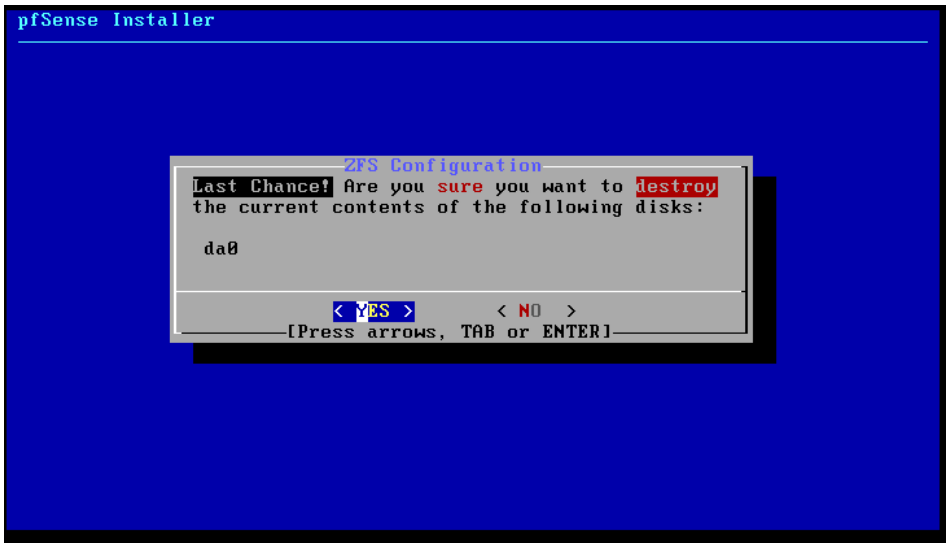
On continue l'installation en sélectionnant toujours le paramètre suggéré



Enfin on sélectionne l'espace de stockage qui sera utilisé pour installer le système d'exploitation, il n'y en a qu'un seul, car nous avons décidé plus tôt de stocker la VM dans un seul disque virtuel

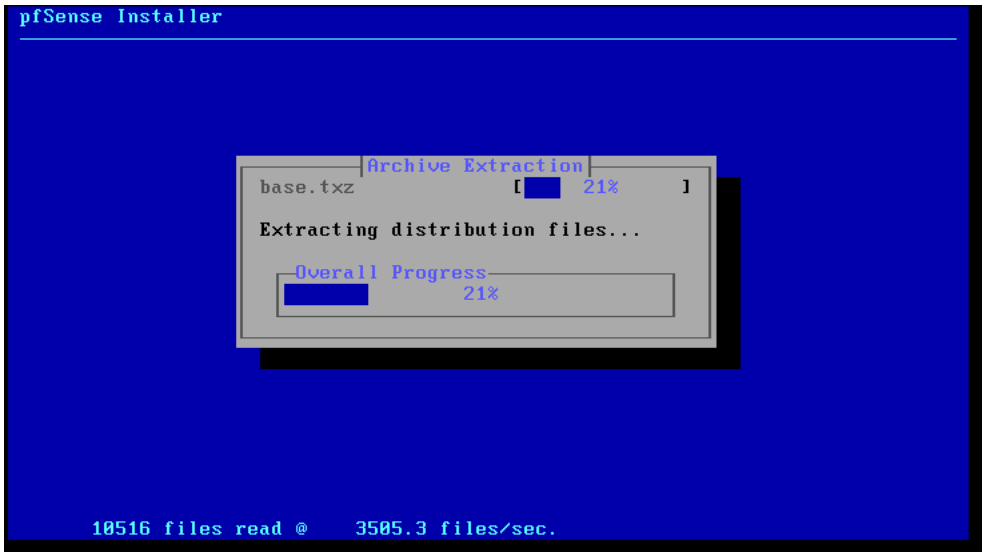


Pour sélectionner l'espace de stockage, il ne faut pas oublier d'appuyer sur la barre d'espace qui est réquisitionné pour la sélection de l'espace de stockage

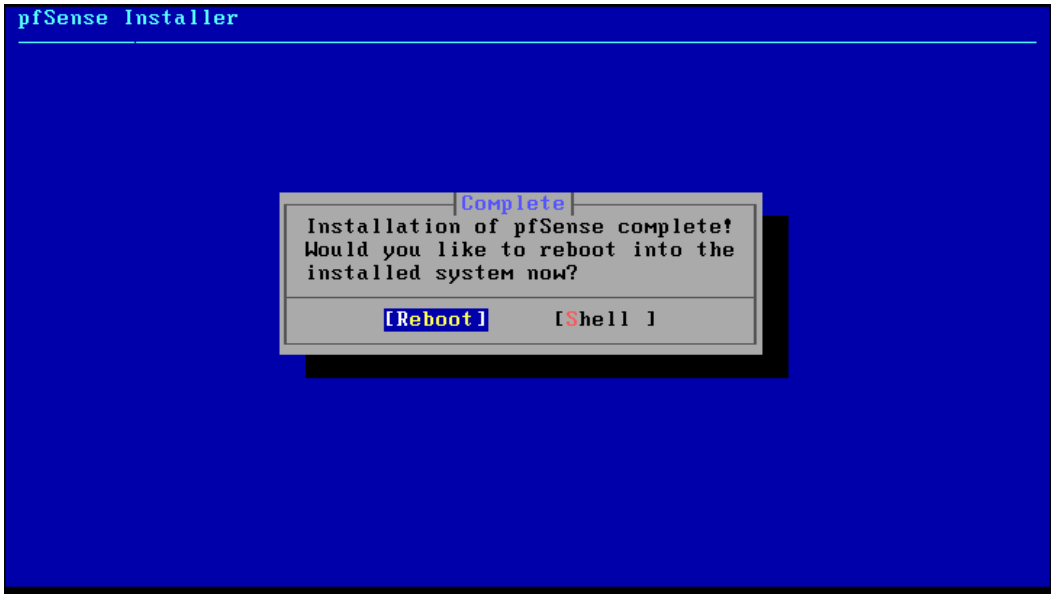


On valide ensuite l'avertissement qui nous explique que l'entièreté des données présentes sur le disque vont être détruites.

Dans notre cas cela ne représente pas un problème, car il n'y a pas de donner, car nous venons de créer le disque virtuel



L'installation se lance

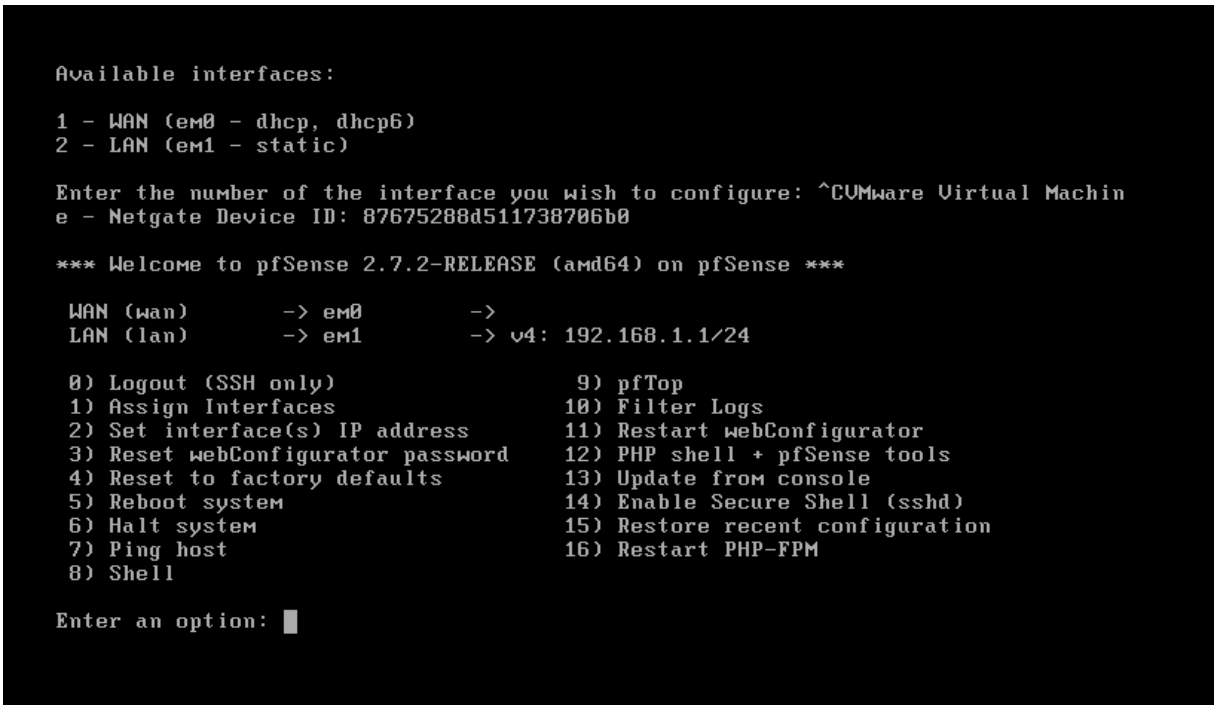


Et on choisit de reboot car cela est généralement conseillé lors de la première exécution de nouveau système d'exploitation

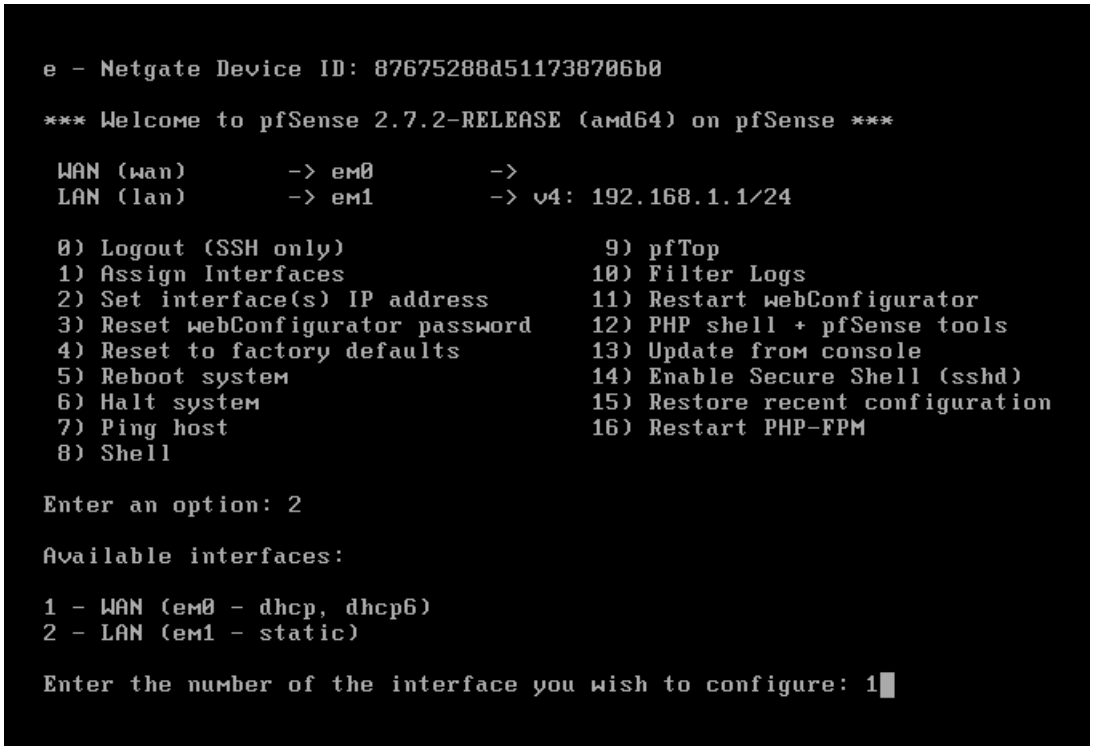
À présent, nous allons **paramétrer les interfaces réseau** de **PFSENSE**.

Pour rappel, selon la **table des adresses IP** :

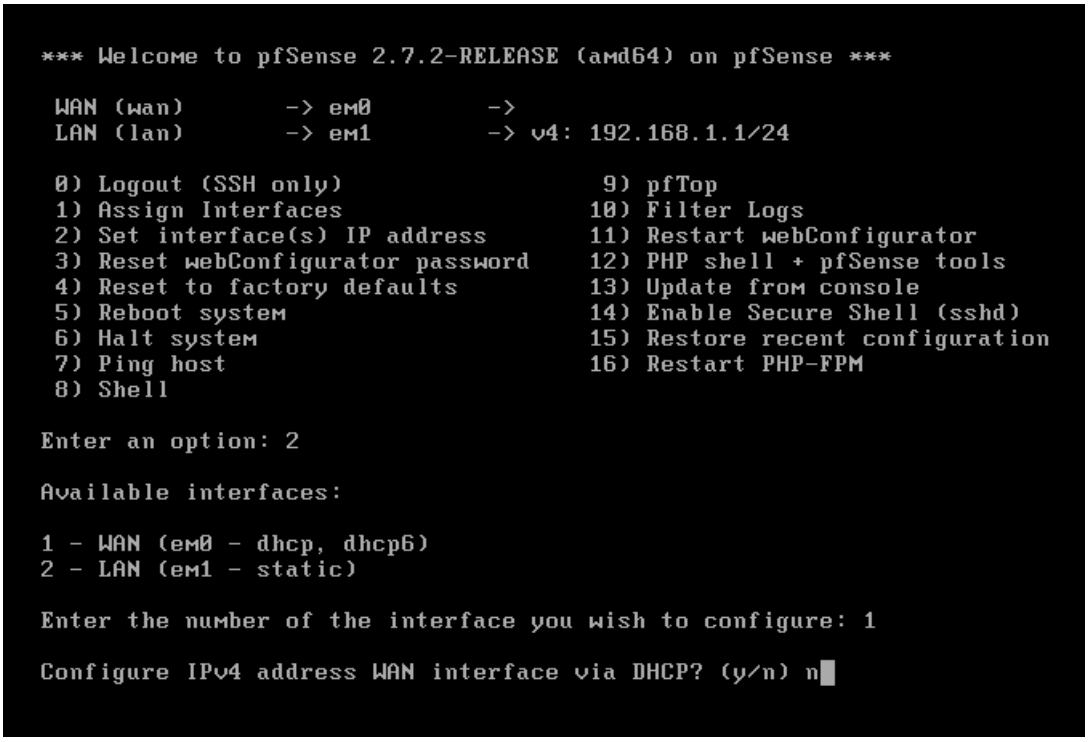
- L'interface **LAN** de la machine **PFSENSE Master** doit être configurée avec l'adresse **172.22.250.3**.
- L'interface dédiée au **protocole CARP** doit être configurée avec l'adresse **172.17.0.1/24**.



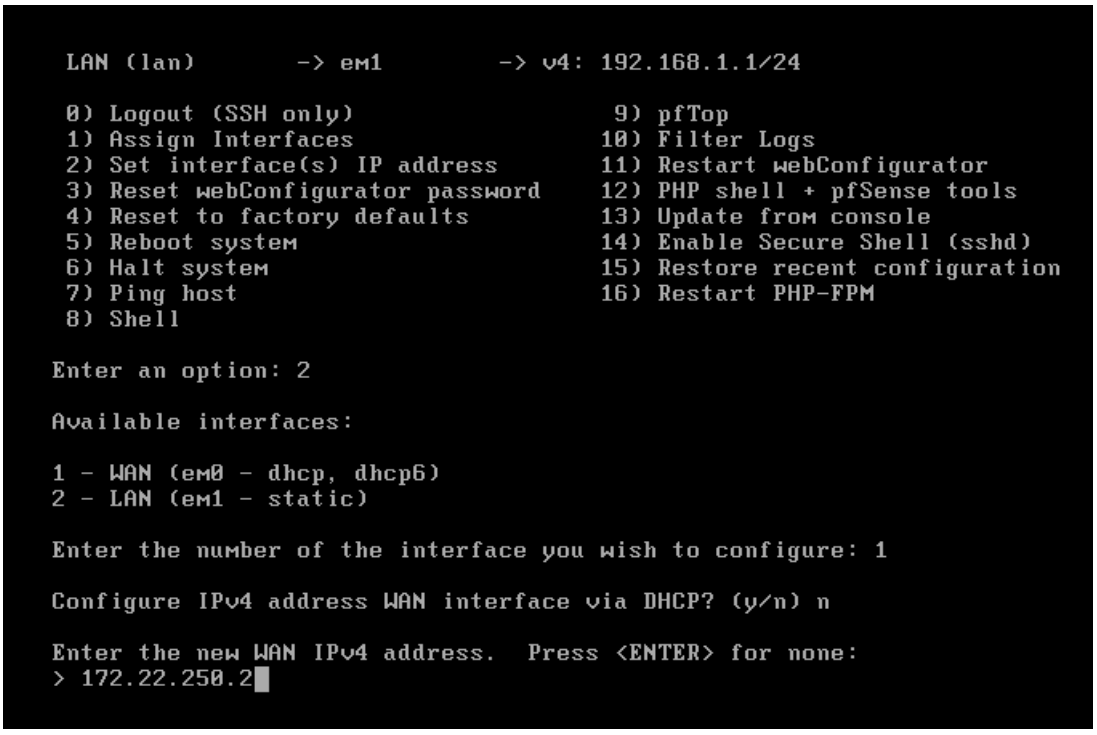
Pour cela on va sélectionner « 2 » pour déclarer nos adresses IP



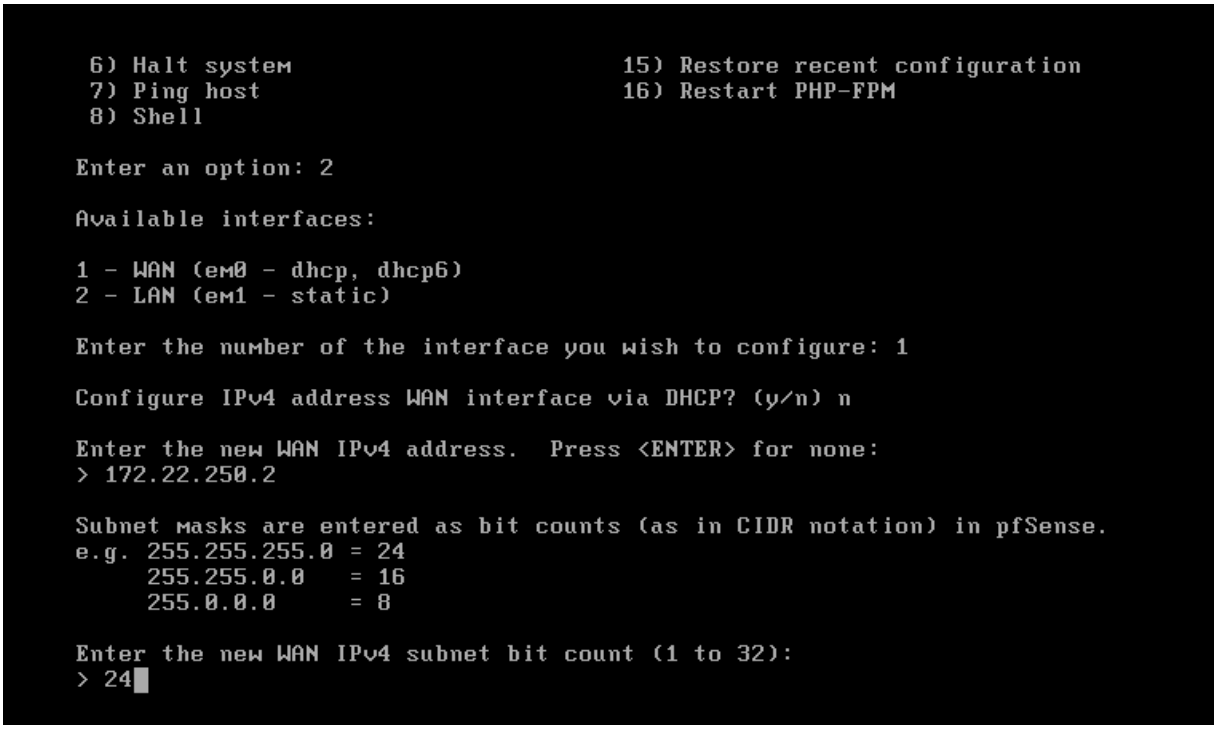
Puis on va sélectionner « n » pour indiquer que l'on ne veut pas configurer l'interface en DHCP



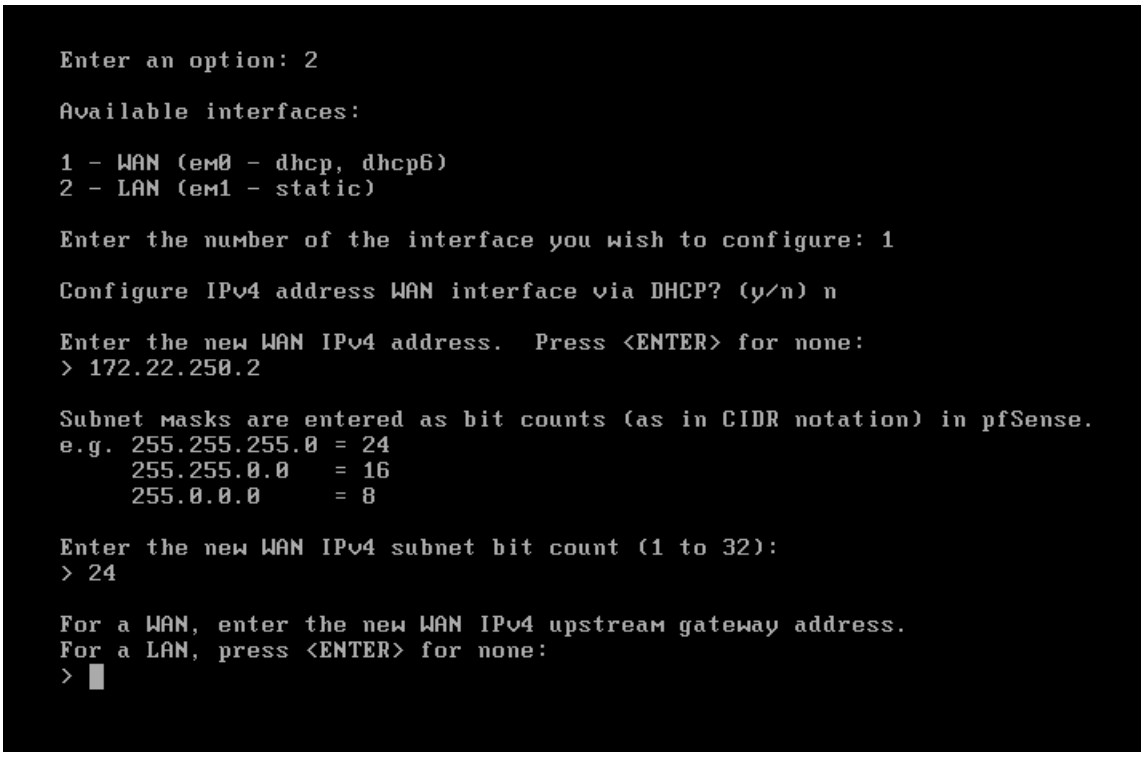
Puis on rentre l'IP 172.22.250.2



Puis on indique le masque en notation CIDR : « 24 »



A cette étape nous allons presser la touche entrée car nous paramètrerons la passerelle après à travers l'interface WEB



De même pour l'utilisation du protocole de communication IPV6

```
2 - LAN (em1 - static)

Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address.  Press <ENTER> for none:
> 172.22.250.2

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
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:
>
```

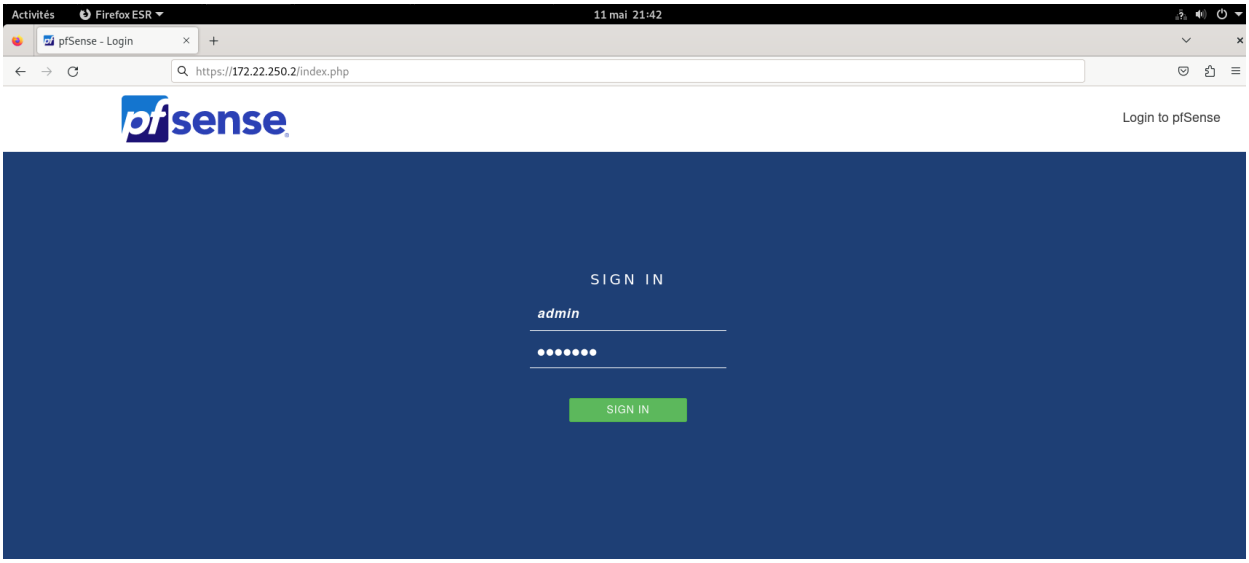
Nous n'allons pour le moment pas activer le protocole DHCP, nous le ferons à travers l'interface WEB

```
Enter the number of the interface you wish to configure: 1

Configure IPv4 address WAN interface via DHCP? (y/n) n

Enter the new WAN IPv4 address.  Press <ENTER> for none:
> 172.22.250.2

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new WAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new WAN IPv4 upstream gateway address.
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
```

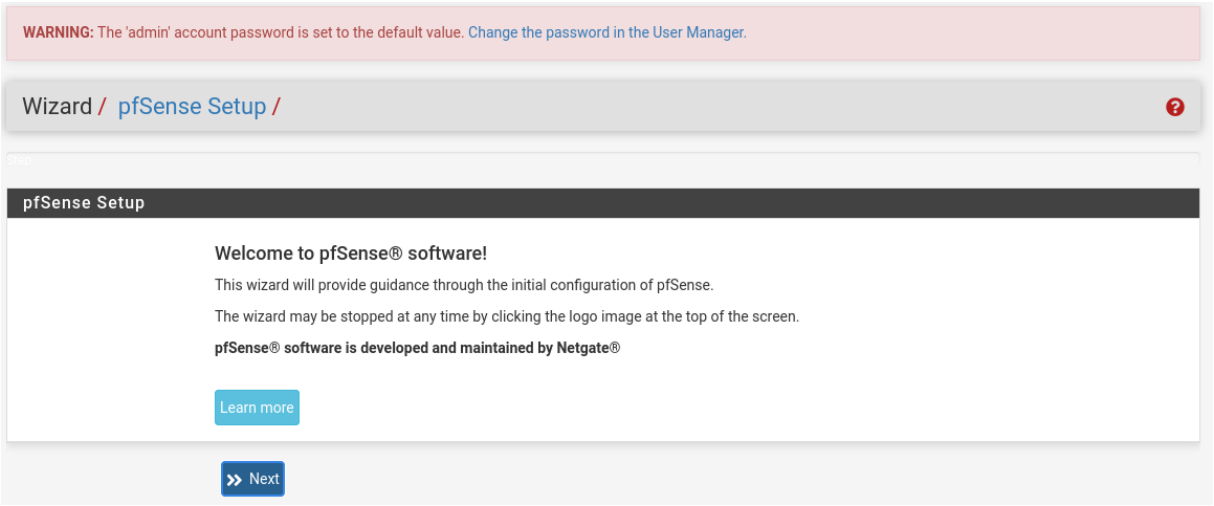
Cette partie est importante car elle nous indique comment accéder à l'interface WEB, plus précisément quelle url indiquer dans le navigateur pour y accéder.

```
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 172.22.250.2/24
You can now access the webConfigurator by opening the following URL in your web
browser:
                https://172.22.250.2/

Press <ENTER> to continue.
```

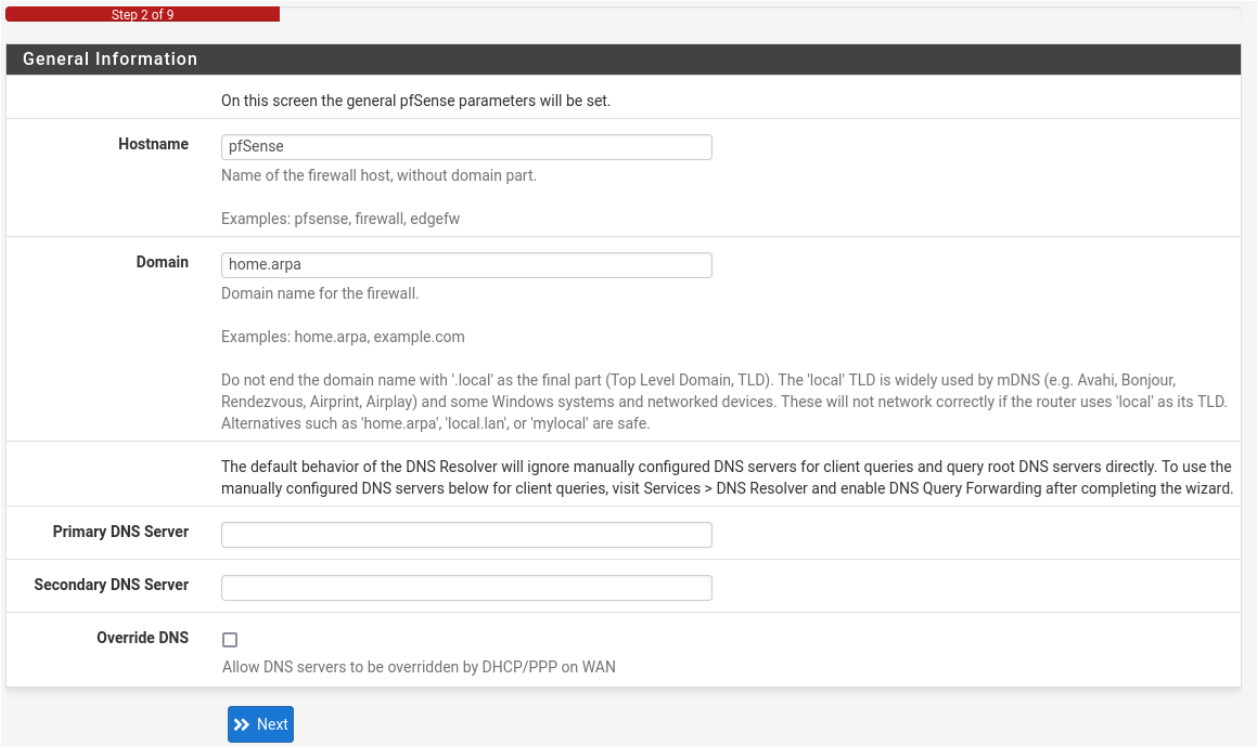
A présent nous pouvons travailler sur l'interface WEB



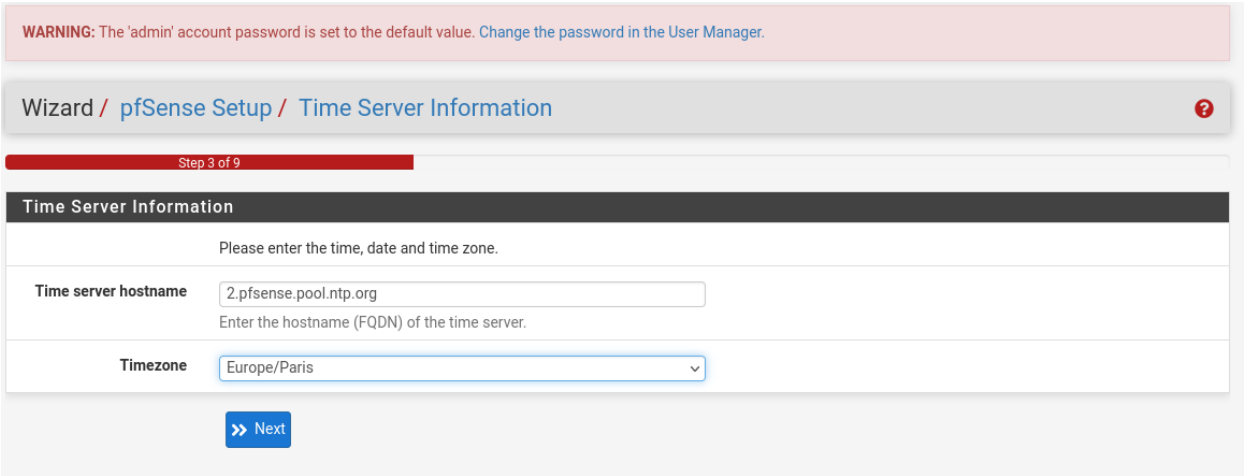
A la suite de notre première connexion, il y a des étapes de configuration



À partir de là il nous est proposé de réaliser l'initiation à pfsense. Nous allons la suivre

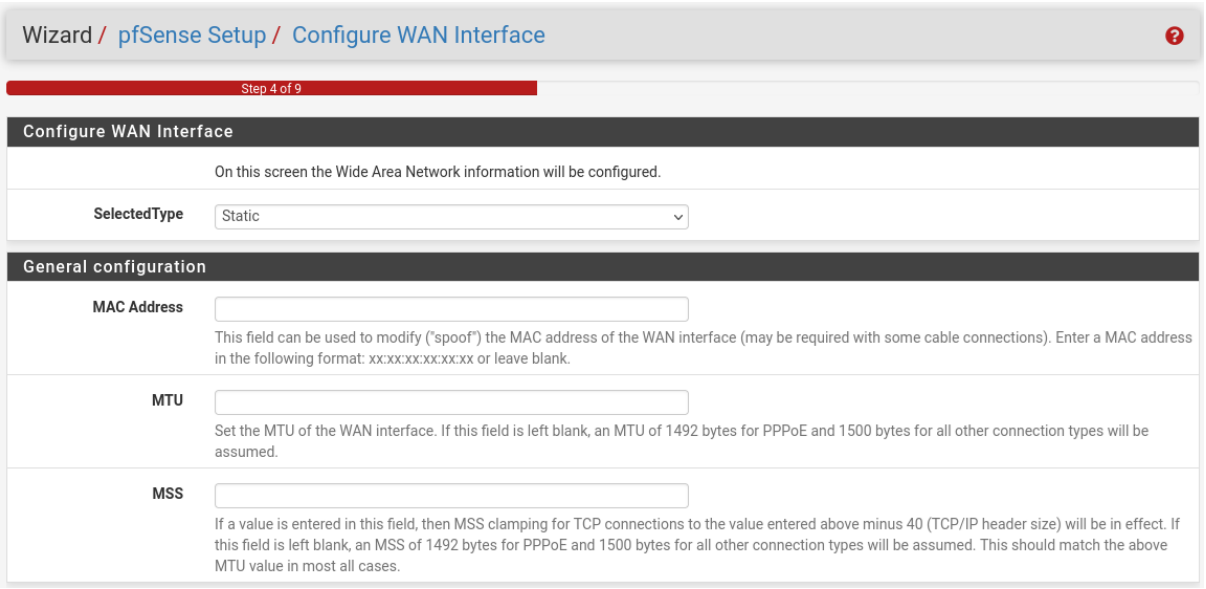


À cette étape nous allons juste décocher la "case Override DNS" qui est une fonction qui permet de remplacer le DNS sur le réseau WAN c'est à dire celui qui a accès à internet par un Service DHCP (nous ne voulons pas le remplacer donc nous allons décocher cette case)

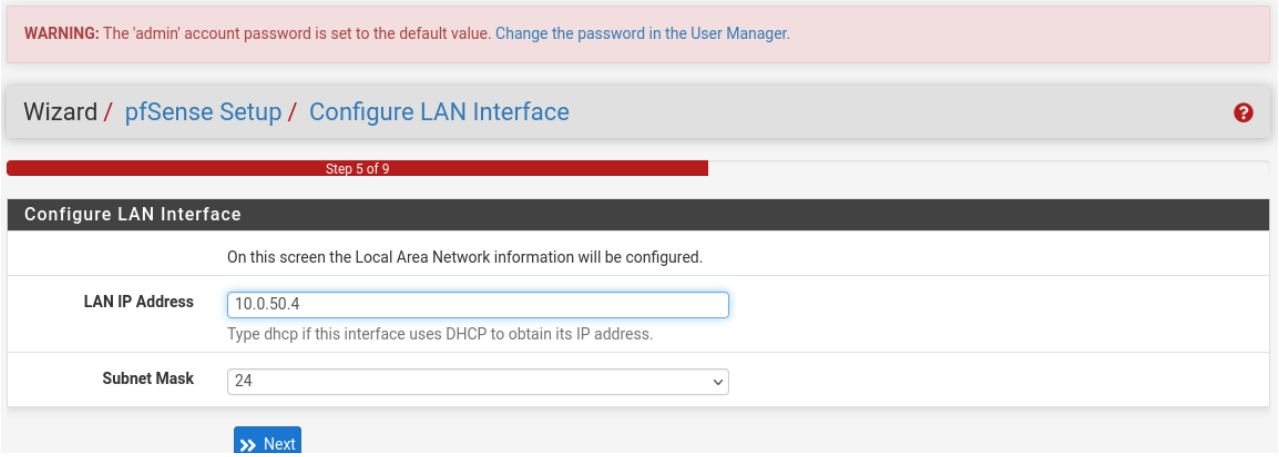


À cette étape, il est important de **changer le fuseau horaire** pour le mettre sur l'heure **française**. Cela peut être utile, notamment pour l'interprétation des messages d'erreur.

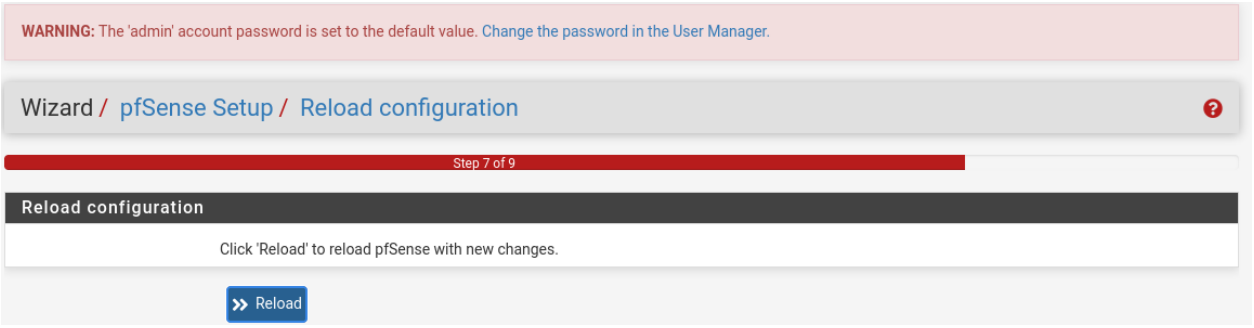
En effet, les messages d'erreur affichent l'heure exacte de leur apparition. Si l'heure n'est pas configurée correctement, il peut être difficile d'identifier quel message d'erreur est survenu en premier.
En configurant le fuseau horaire sur **heure française**, cela facilitera l'identification des messages d'erreur et leur suivi dans les logs.



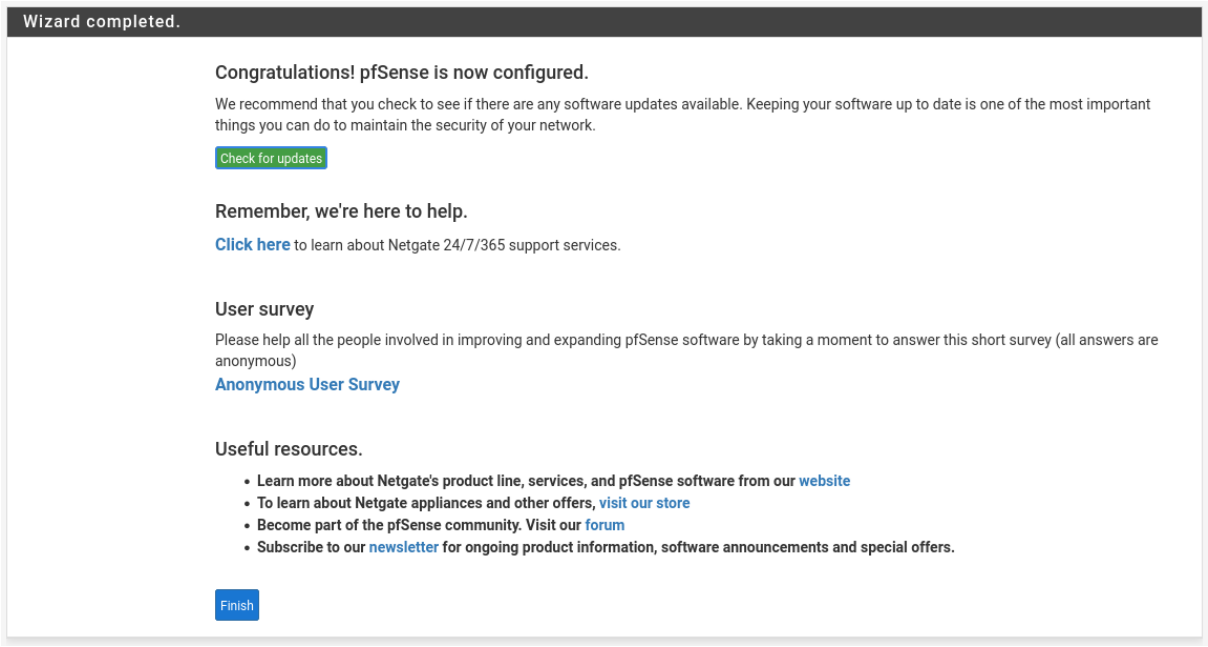
Sur la page suivante, il n'y a rien à signaler, on laisse les paramètres par défauts



Ici le pare-feu nous affiche quel IP et le masque qu'il possède sur son interface LAN. Dans notre cas, tout correspond à ce que nous avons fait auparavant.

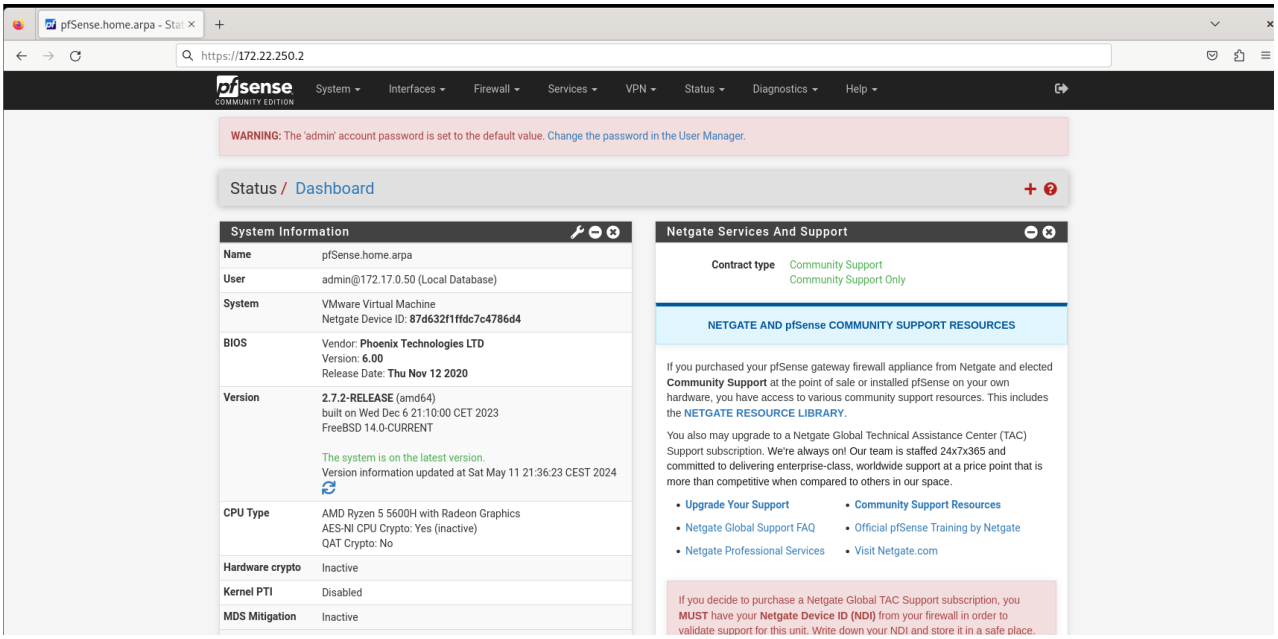


Il suffit maintenant d'appuyer sur "reload" pour charger les quelques paramètres que nous avons modifiés



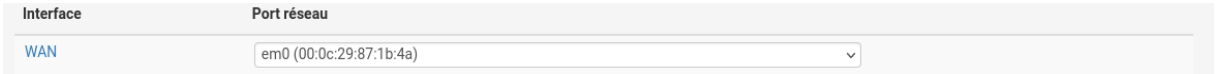
Puis on valide avec le bouton "finish"

Nous arrivons donc sur la page d'accueil de PFsense

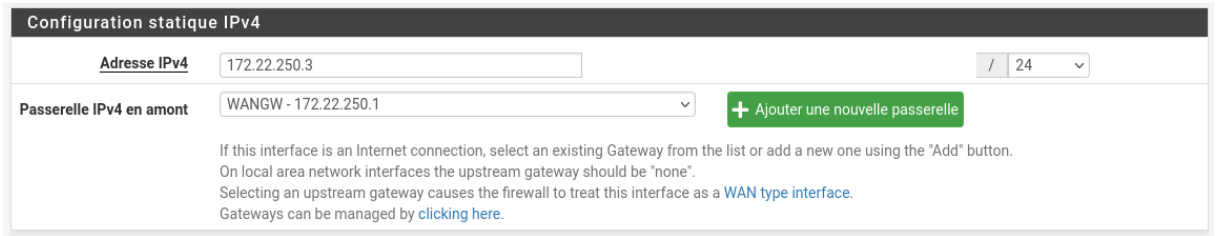


A partir de là nous allons devoir paramétrer la seconde interface CARP qui nous permettra de nous synchroniser avec la machine PFsense Slave Pour cela nous allons nous rendre dans la section « interface »

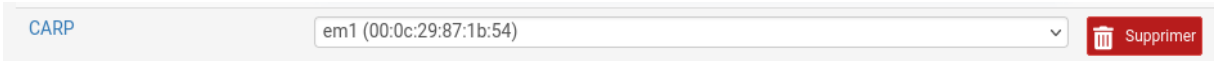
Dans cette section nous allons reparamétrer l'interface que nous avons initialisée précédemment pour notamment activer les services DHCP et passerelle



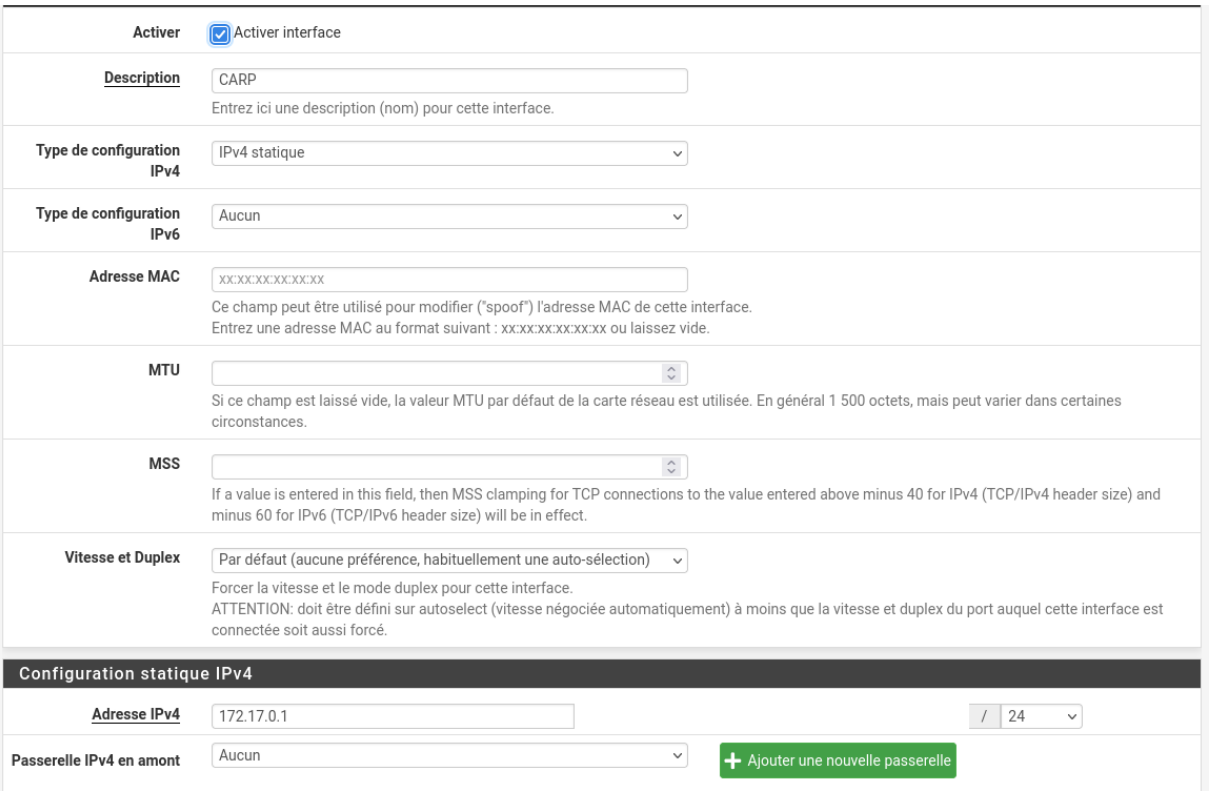
Et dans la section « configuration statique IPv4 » on rentre notre passerelle qui correspond à l'adresse IP de notre pare-feu IPfire en 172.22.250.1/24



Puis nous allons rajouter une interface qui sera utilisais pour synchroniser les machines PFSENSE par le protocole CARP



Pour cela on va commencer par activer l'interface puis par sélectionner une configuration par IPv4 puis finir par rentrer l'adresse IP de notre interface CARP qui est 172.17.0.1



A partir de là, toute ces étapes devront être répété sur la machine PFSENSE SLAVE, c'est à dire :

- Installation du système d'exploitation
- Paramétrage de la première interface
- Première connexion WEB
- Activation de la seconde interface

Ceci en adaptant les adresses IP allouées à cette tache c'est à dire :

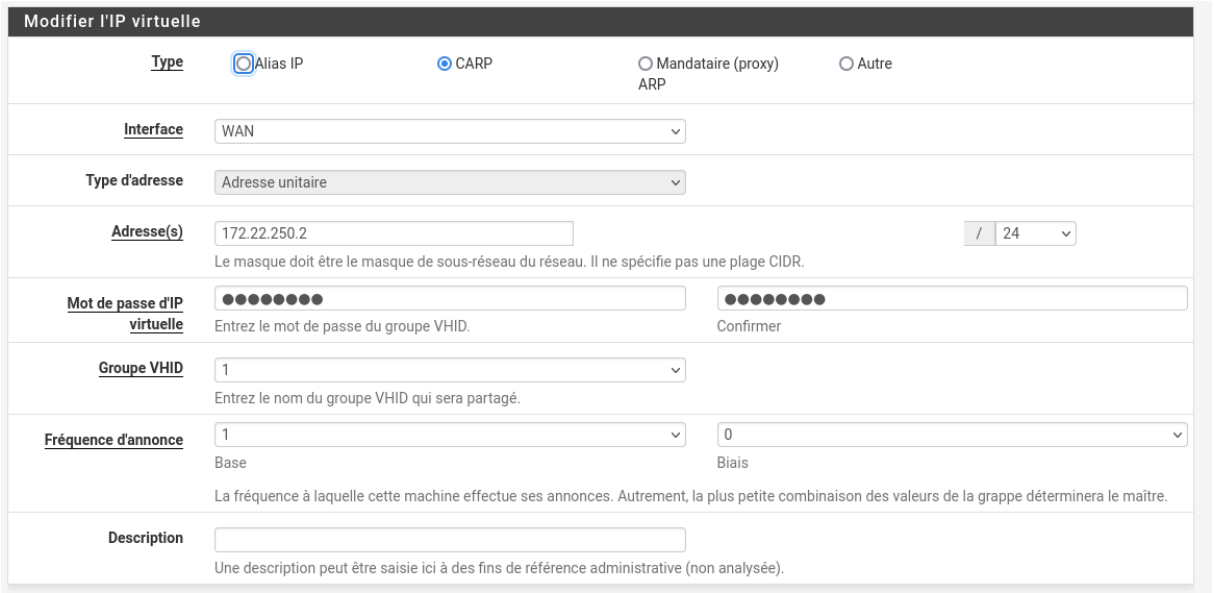
172.22.250.4/24 pour l'interface LAN

172.17.0.2/24 pour l'interface CARP

Les taches 2.1, 2.2 et 3.1 ont été réalisé

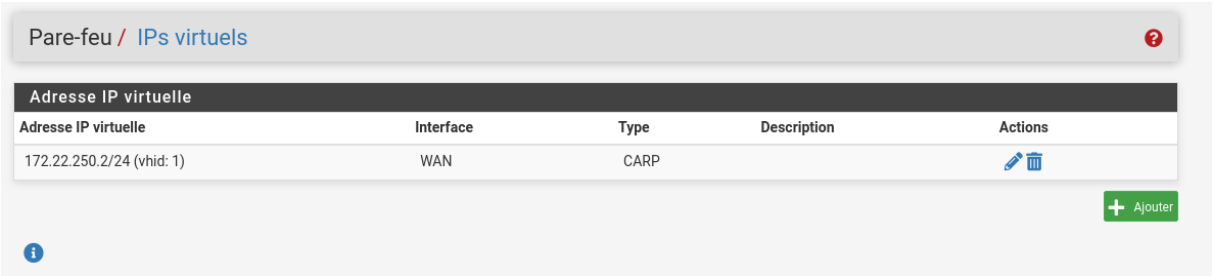
Nous allons maintenant paramétrer le CARP

CARP (Common Address Redundancy Protocol) est un protocole de clustering utilisé dans les réseaux informatiques pour fournir une haute disponibilité et une redondance des adresses IP. Il permet à plusieurs dispositifs réseau, tels que des pares-feux ou des pares-feux, de partager une adresse IP virtuelle, assurant ainsi une continuité de service en cas de panne matérielle ou de maintenance planifiée. Les nœuds CARP communiquent entre eux pour déterminer quel nœud sera le maître et gérera le trafic vers l'adresse IP virtuelle, tandis que les autres nœuds resteront en mode veille, prêts à prendre le relais en cas de défaillance du nœud maître. Cela garantit une haute disponibilité et une redondance des services critiques dans les infrastructures réseau.

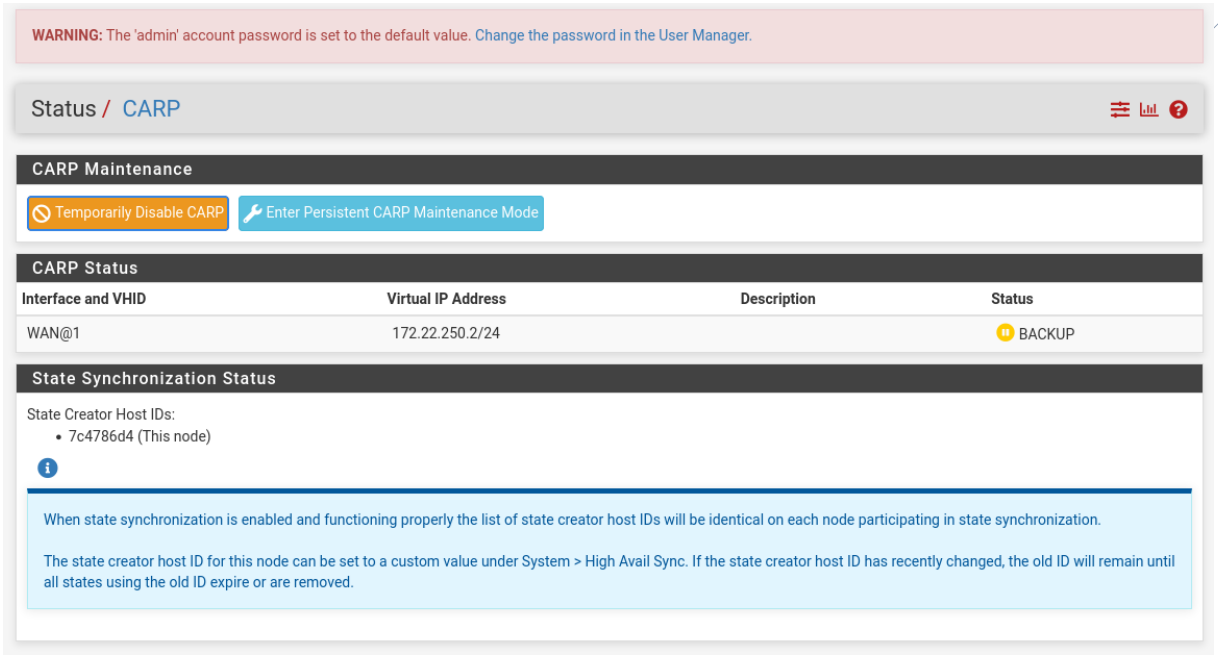


On rend dans « Firewall » « puis Virtual IP » et on rajoute une IP virtuelle

On fait attention au SKEW qui doit être égale 0 sur le maître et a 1 sur le slave

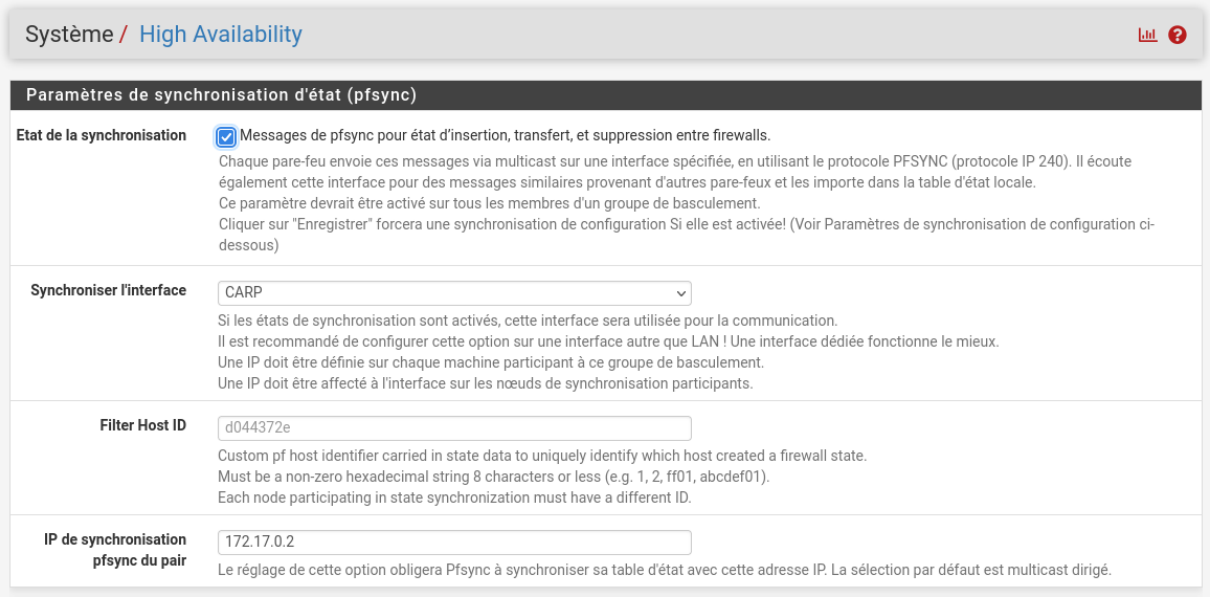


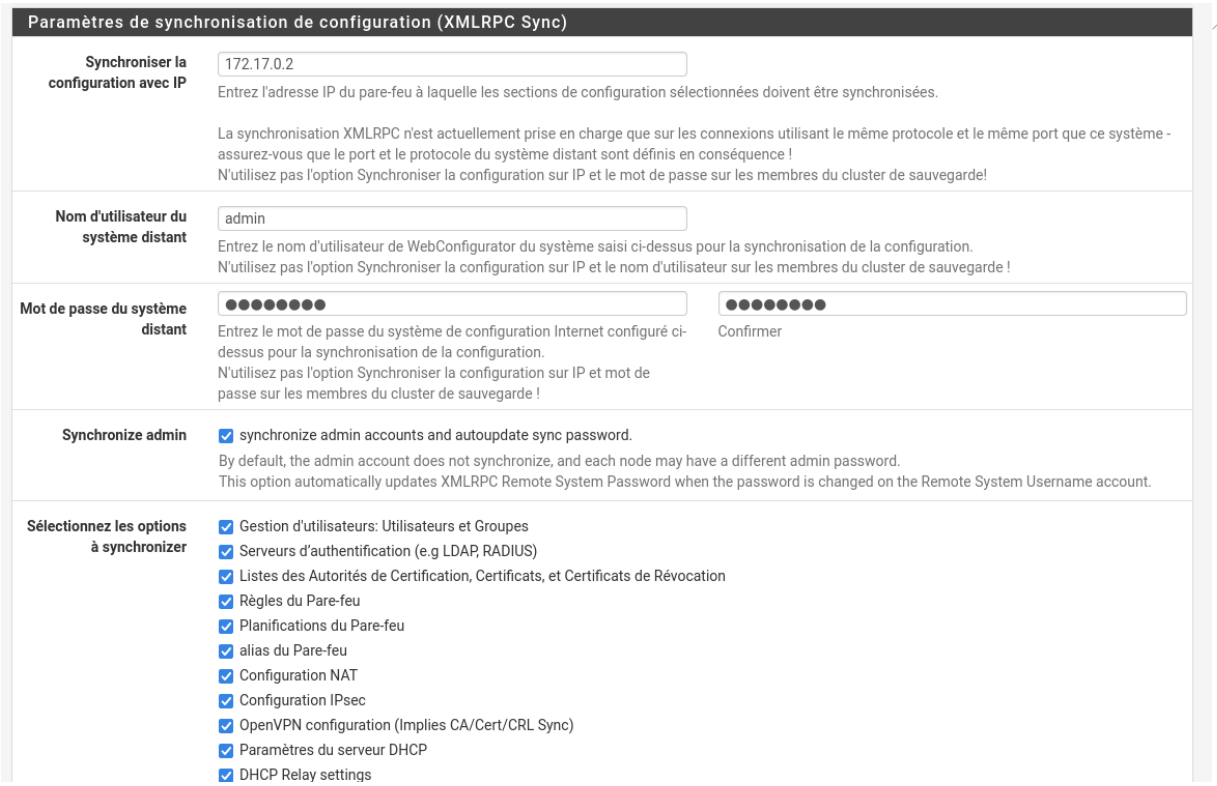
À ce moment-là on peut voir l'état de notre IP virtuel



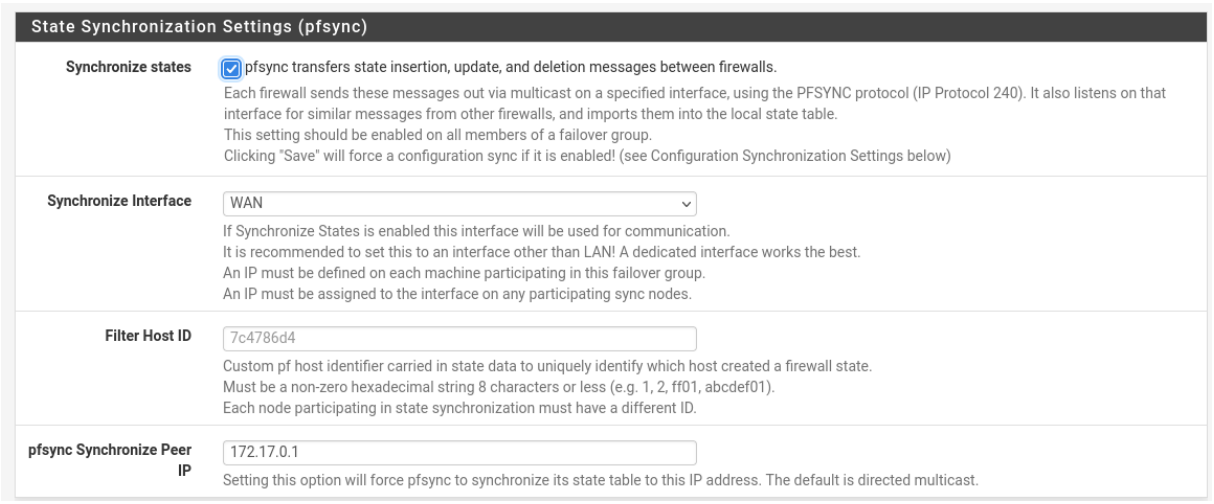
Idem pour le SLAVE

Puis on va paramétrer le CARP sur nos pares-feux :





Les deux photos précédentes sont sur le pare-feu PFSENSE MASTER



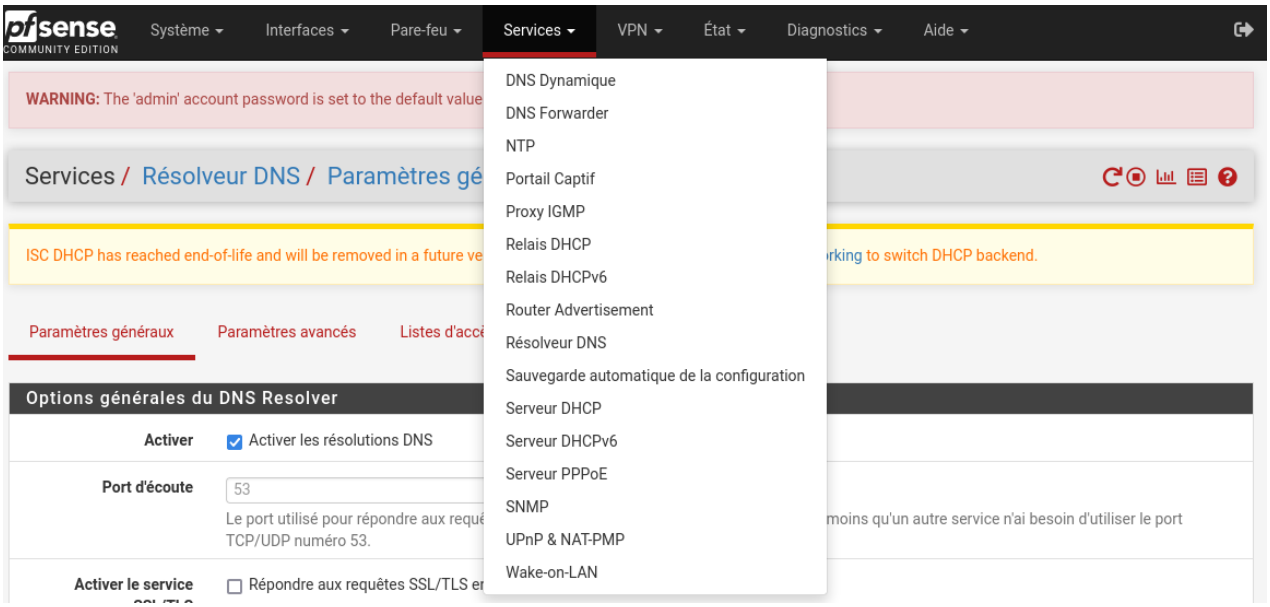
Cette photo est sur le pare-feu PFSENSE SLAVE

Les taches 2.4, 2.5, 3.2 et 3.3 sont terminées

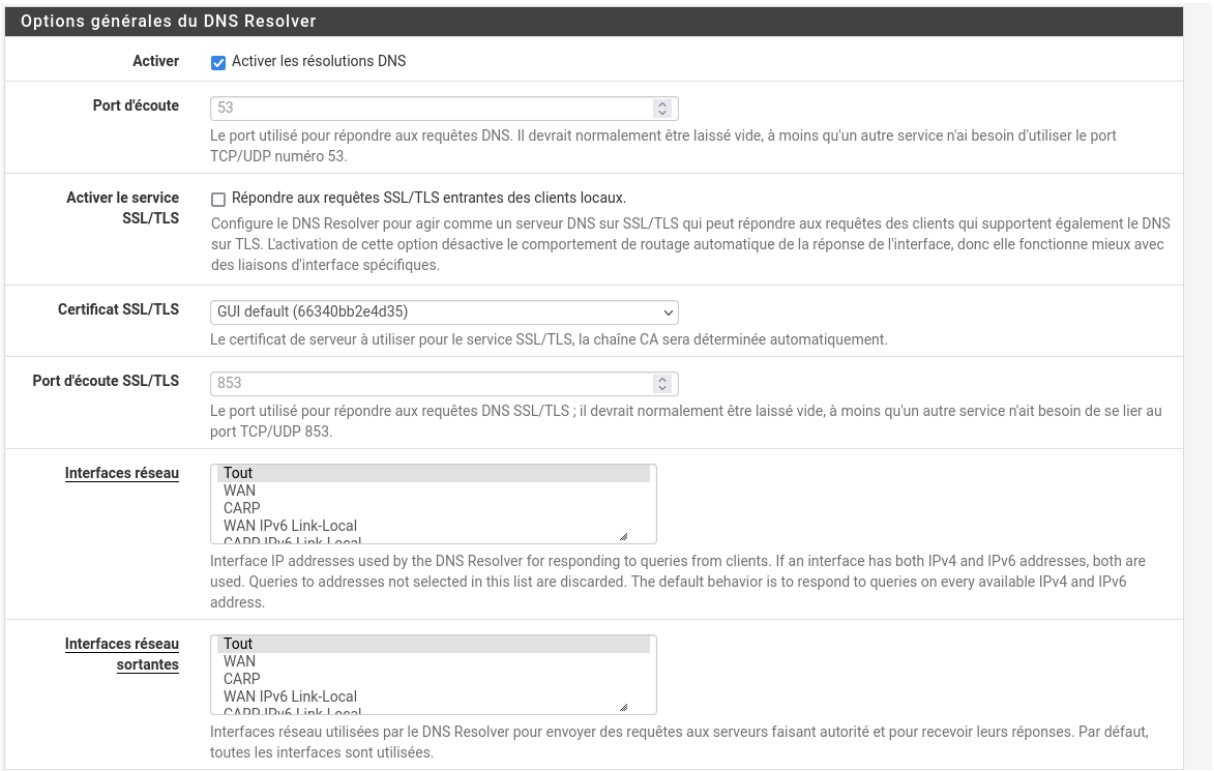
Il ne reste plus qu'à paramétrer le service DNS sur la machine PFSENSE MASTER

Soit l'étape 2.3

Pour activer le service DNS nous allons nous rendre dans la section « résolveur DNS »

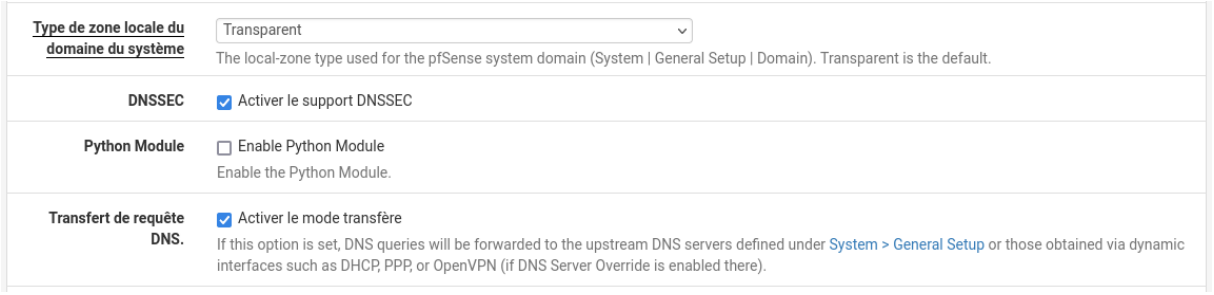


Une fois sur la page de paramétrage, nous allons cocher la case « activer les résolutions DNS »

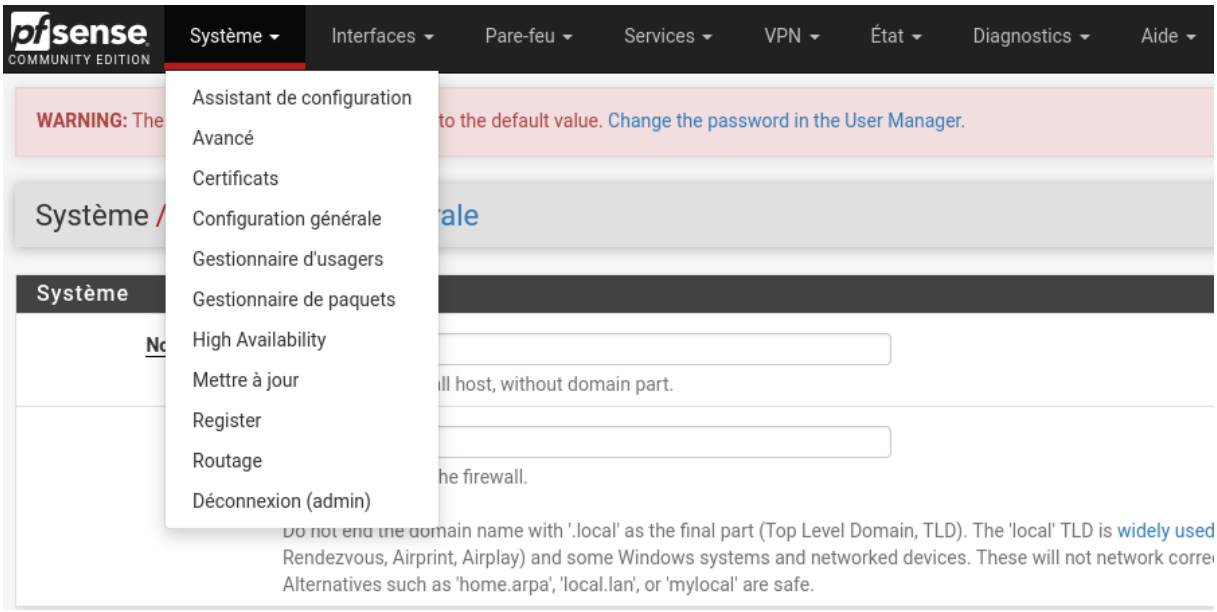


Puis nous allons activer le « support DNSSEC » qui est une norme de communication entre les serveurs DNS pour assurer les transferts d'information sur les domaines

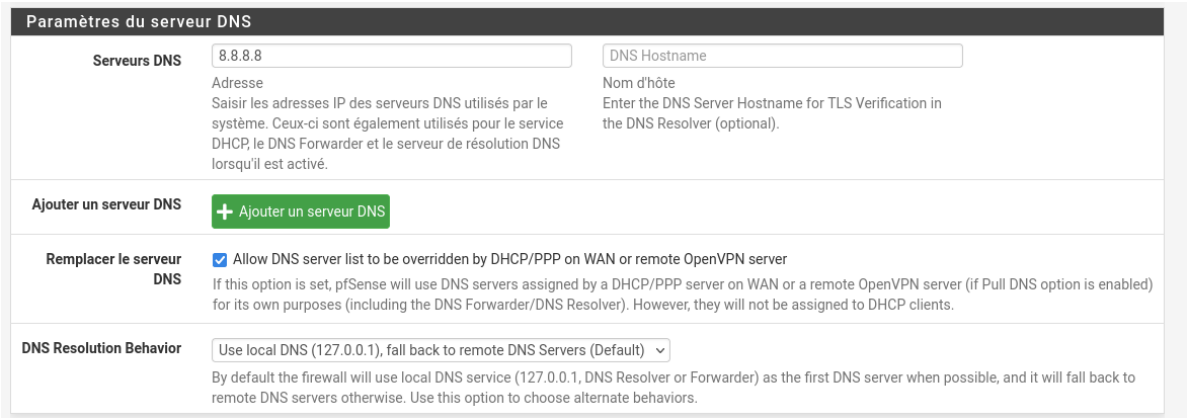
Mais également cocher le « mode transfert » qui une fois activer permet de transférer les requêtes DNS dont notre serveur PFSENSE ne connait pas la résolution a un autre serveur qui aura était choisi à l'avance



Justement pour configurer cet autre serveur DNS qui servira à résoudre les requêtes non-résolue par notre serveur DNS PFSENSE il faut se rendre dans la section « système » puis « configuration générale »



Puis dans la partie « paramètre du serveur DNS »



Il faut renseigner ensuite le serveur DNS qui servira de serveur de transfert, dans notre cas 8.8.8.8

La tache 2.3 est terminé (paramétrage du service DNS)

Nous allons à présent passer a l'installation du serveur WEB au sain de la DMZ

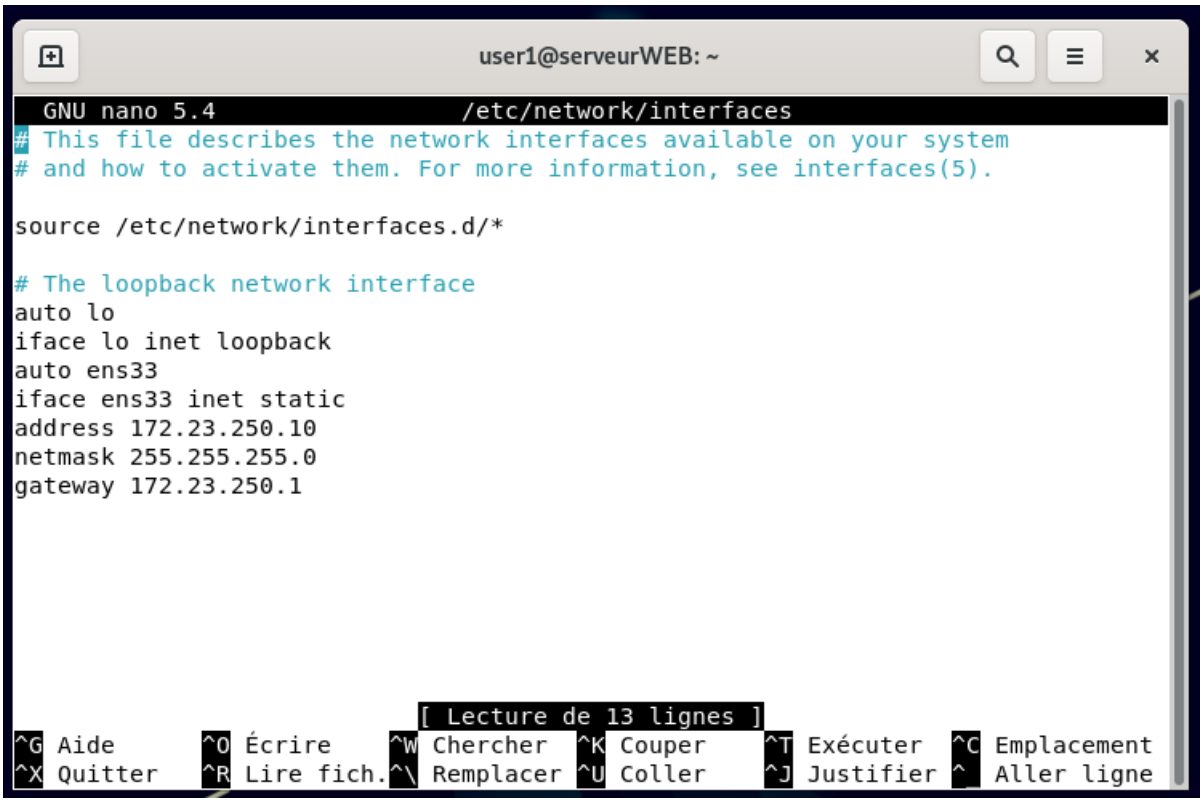
Pour cela nous devons importer une machine Linux qui possède une interface dans la DMZ

La première chose à faire et de paramétrer la carte réseau qui ne peut recevoir de configuration IP par DHCP car elle se trouve dans un réseau DMZ

Pour cela nous allons dans le fichier de configuration : « etc/network/interfaces »

Et on édit les paramètres pour lui donner l'adresse IP 172.23.250.10/24

Et la passerelle 172.23.250.1



Puis nous installons le paquet apache2 (qui est un paquet de serveur WEB)

```
root@serveurWEB:/home/user1# apt install apache2
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
apache2 est déjà la version la plus récente (2.4.59-1~deb11u1).
0 mis à jour, 0 nouvellement installés, 0 à enlever et 64 non mis à jour.
root@serveurWEB:/home/user1#
```

Nous allons a présent faire en sorte que notre page web utilise la norme de communication https ce qui vas passer par l'activation du module ssl

Pour cela on active le module ssl puis la configuration préconfigurée du service apache2

```
root@serveurWEB:~# a2enmod ssl
```

```
root@serveurWEB:~# a2ensite default-ssl
```

Nous allons a présent nous occuper de la modification a effectuer sur la page web pour rappel cette page doit afficher « Bonjour BTS SIO »

Pour cela nous allons modifier la page html hébergé par le service apache2

Nous allons donc éditer avec la commande « nano » le fichier « /var/www/html/index.html »

```
root@serveurWEB:/var/www/html# nano /var/www/html/index.html
```

Puis on supprime toute l'intégralité du document et on le remplace par les quelques caractères suivants

Maintenant en tapant l'adresse IP du serveur WE, cet a dire 172.23.250.10 on peut retrouver notre page avec belle et bien écrit « Bonjour BTS SIO » et on voit que la page utilise bien la certification https garce a la présence du cadenas.

Nous allons maintenant faire en sorte qu'apache (le paquet serveur WEB) utilise et écoute un autre port que celui de base. Apache utilise le port 80 s'il n'utilise pas le protocole http et 443 s'il utilise le protocole https.

Pour le serveur WEB nous avons convenue qu'il utiliserait le port 2002. Cette partie est particulièrement importante car nous avons déjà paramétrais les ports qui seront utilisés par les différents services dans le pare-feu IPfire, notamment au niveau des règles NAT avec la redirection de port.

Nous allons donc éditer le fichier de configuration du virtualhost par-default

```
root@ServeurMessagerie:/etc/apache2/sites-enabled# nano /etc/apache2/sites-enabled/default.conf
```

Et on change la première ligne

```
<VirtualHost *:80>
```

En 2002

```
<VirtualHost *:2002>
```

Puis on redémarre le service

```
root@ServeurMessagerie:/etc/apache2/sites-enabled# systemctl restart apache2
```

Et voilà notre serveur WEB utilise maintenant le port 2002

Les taches 4.1, 4.2, 4.3 on étaient réalisé

Nous allons maintenant nous attaquer à l'installation du serveur Next cloud

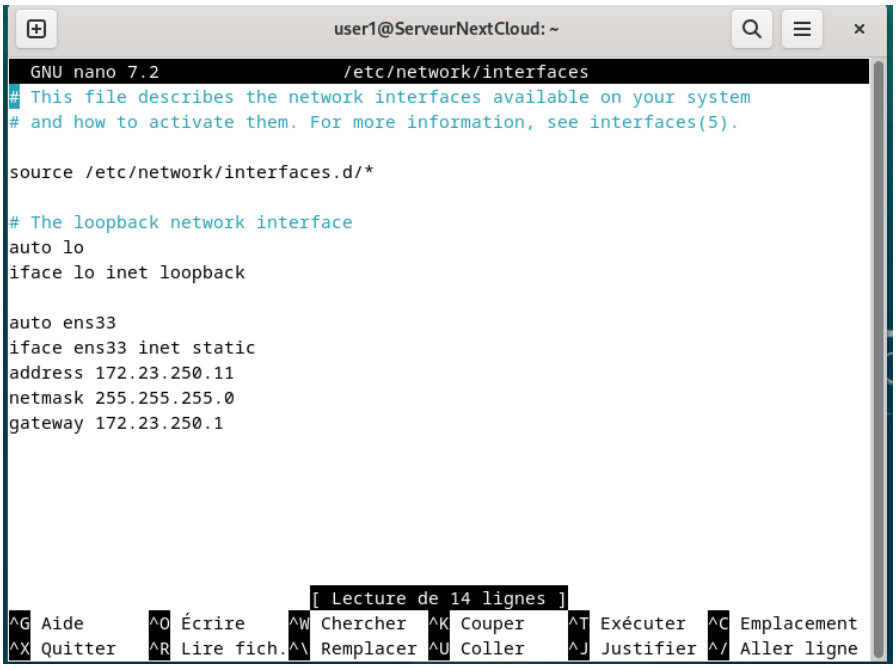
Pour cela nous devons importer une machine Linux qui possède une interface dans la DMZ

La première chose à faire et de paramétrer la carte réseau qui ne peut recevoir de configuration IP par DHCP car elle se trouve dans un réseau DMZ

Pour cela nous allons dans le fichier de configuration : « etc/network/interfaces »

Et on édit les paramètres pour lui donner l'adresse IP 172.23.250.11/24

Et la passerelle 172.23.250.1



Dans un premier temps nous allons installer Apache2, MariaDB Server et PHP 8.1 ainsi qu'un lot d'extensions PHP utiles :

```
root@ServeurNextCloud:/home/user1# apt-get install apache2 mariadb-server php8.1 php8.1-common php
8.1-curl php8.1-gd php8.1-intl php8.1-mbstring php8.1-xmlrpc php8.1-mysql php8.1-xml php8.1-cli ph
p8.1-zip
```

Nous allons aussi installer les paquets "wget" et "unzip" utiles pour télécharger les sources de Nextcloud et décompresser l'archive ZIP.

```
root@ServeurNextCloud:/home/user1# apt-get install wget unzip
```

Toujours sur le serveur Debian, positionnez-vous dans le répertoire "/tmp" pour télécharger la dernière version de Nextcloud avec wget :

```
root@ServeurNextCloud:/home/user1# cd /tmp
root@ServeurNextCloud:/tmp# wget https://download.nextcloud.com/server/releases/latest.zip
```

On décompresse l'archive ZIP téléchargée :

```
root@ServeurNextCloud:/tmp# unzip latest.zip
```

Ce qui donne lieu à un dossier "nextcloud" dans "/tmp" que nous allons déplacer dans son intégralité vers "/var/ww/html/".

```
root@ServeurNextCloud:/tmp# mv nextcloud/ /var/www/html/
```

On se connecte ensuite à la Base de données

```
root@ServeurNextCloud:/tmp# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.6-MariaDB-0+deb12u1 Debian 12

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)]>
```

Après authentification, vous avez accès au prompt MariaDB. Nous devons commencer par créer une base de données que nous appellerons "db23nextcloud".

```
MariaDB [(none)]> CREATE DATABASE db23nextcloud;
```

Puis, on va créer un utilisateur nommé "usr23nextcloud" qui aura le mot de passe "Password14" et qui aura tous les droits sur la base de données "db23nextcloud". Personnalisez ces informations, bien entendu.

```
MariaDB [(none)]> GRANT ALL ON db23nextcloud.* TO 'usr23nextcloud'@'localhost' IDENTIFIED BY 'Password14';
```

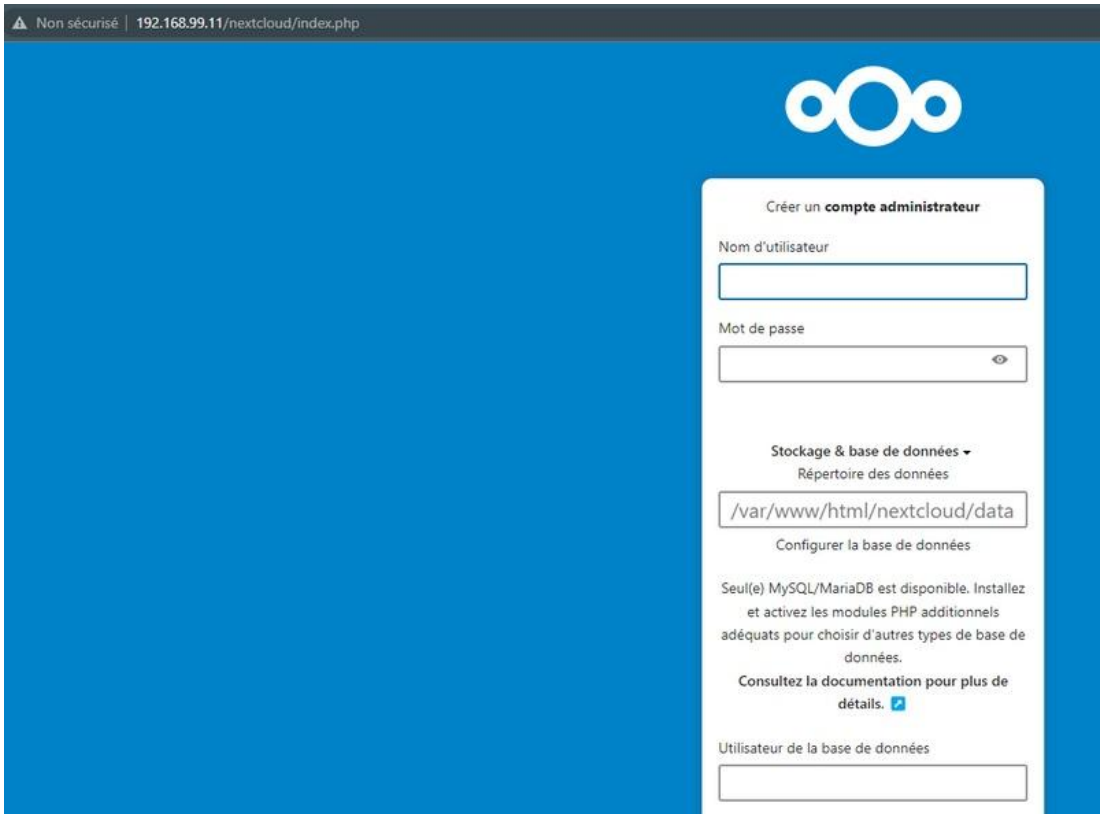
Puis, on se déconnecte de l'instance MariaDB :

```
MariaDB [(none)]> EXIT;
```

Tout est prêt, nous allons pouvoir finaliser l'installation de Nextcloud à l'aide d'un navigateur. Avec votre navigateur préféré, accédez à l'adresse suivante :

http://172.23.250.11/nextcloud/

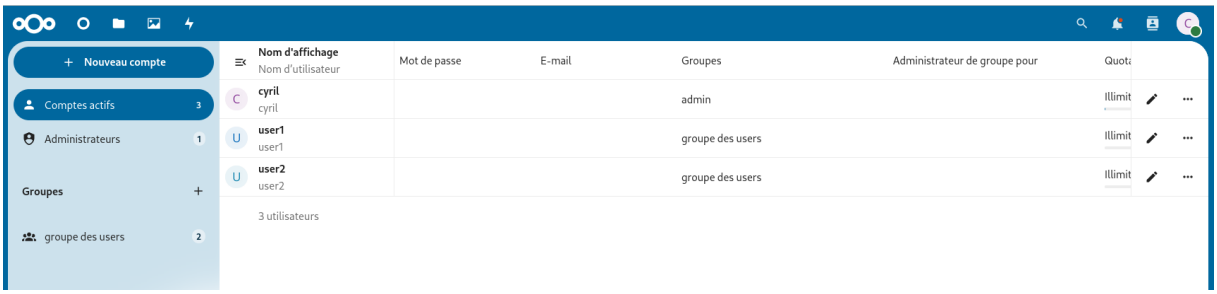
Vous devriez arriver sur une page comme celle ci-dessous. Ici, il va falloir définir un nom d'utilisateur et un mot de passe pour le compte Administrateur principal de Nextcloud.



En bas de cette page, il faut créer votre compte admin en renseignant les informations précédemment utilisé lors de l'installation

Quelques secondes plus tard, l'installation est finalisée,

Nous pouvons accéder à la page admin est inspecter les utilisateurs. A partir de là nous allons ajouter deux utilisateurs : user1 et user2



Nous allons maintenant faire en sorte qu'apache (le paquet serveur WEB) utilise et écoute un autre port que celui de base. Apache utilise le port 80 s'il n'utilise pas le protocole http et 443 s'il utilise le protocole https.

Pour le serveur 2 nextcloud nous avons convenue qu'il utiliserait le port 2005. Cette partie est particulièrement importante car nous avons déjà paramétrais les ports qui seront utilisés par les différents services dans le pare-feu IPfire, notamment au niveau des règles NAT avec la redirection de port.

Nous allons donc éditer le fichier de configuration du virtualhost de nextcloud

```
root@ServeurMessagerie:/etc/apache2/sites-enabled# nano /etc/apache2/sites-enabled/nextcloud.conf
```

Et on change la première ligne

```
<VirtualHost *:80>
```

En 2005

```
<VirtualHost *:2005>
```

Puis on redémarre le service

```
root@ServeurMessagerie:/etc/apache2/sites-enabled# systemctl restart apache2
```

Et voilà notre serveur nextcloud utilise maintenant le port 2005

Nous allons maintenant paramétrer, configurer et installer un serveur de messagerie

La messagerie n'étant pas un système interactif, comme par exemple un service web qui affiche instantanément une page, il faut un service responsable de l'envoi et de la réception/stockage des mails, et un autre responsable de la transmission du mail au destinataire lorsqu'il va se connecter. C'est pourquoi la messagerie utilise plusieurs protocoles, les plus connus étant SMTP et IMAP (ou POP).

Voici pour information un tableau récapitulatif des ports associés aux protocoles des services de messagerie :

Ports par défaut (non chiffré – sans TLS/SSL)		
SMTP	IMAP	POP
25	143	110
Ports sécurisés (chiffré – TLS/SSL)		
SMTP	IMAP	POP
587 (ou 465)	993 (ou 220)	995

Le protocole SMTP sert à échanger des messages entre serveurs de messagerie. Il va permettre l'envoi et la réception de mails quand l'utilisateur n'est pas connecté en stockant les messages dans une boîte mail.

Ensuite, pour récupérer les mails quand on se connecte à sa messagerie via un logiciel de type Outlook ou un webmail comme Gmail, le protocole utilisé sera alors le protocole IMAP (ou POP qui est son ancêtre). C'est lui qui va se connecter au serveur de messagerie où sont stockés les messages et qui pourra ainsi les récupérer.

Pour cette procédure, j'ai choisi d'utiliser le logiciel Postfix, qui va nous permettre de faire du SMTP, couplé à une interface web Postfixadmin pour aider à la gestion des comptes de messagerie sur le domaine. Les utilisateurs seront « virtuels » et stockés en base de données.

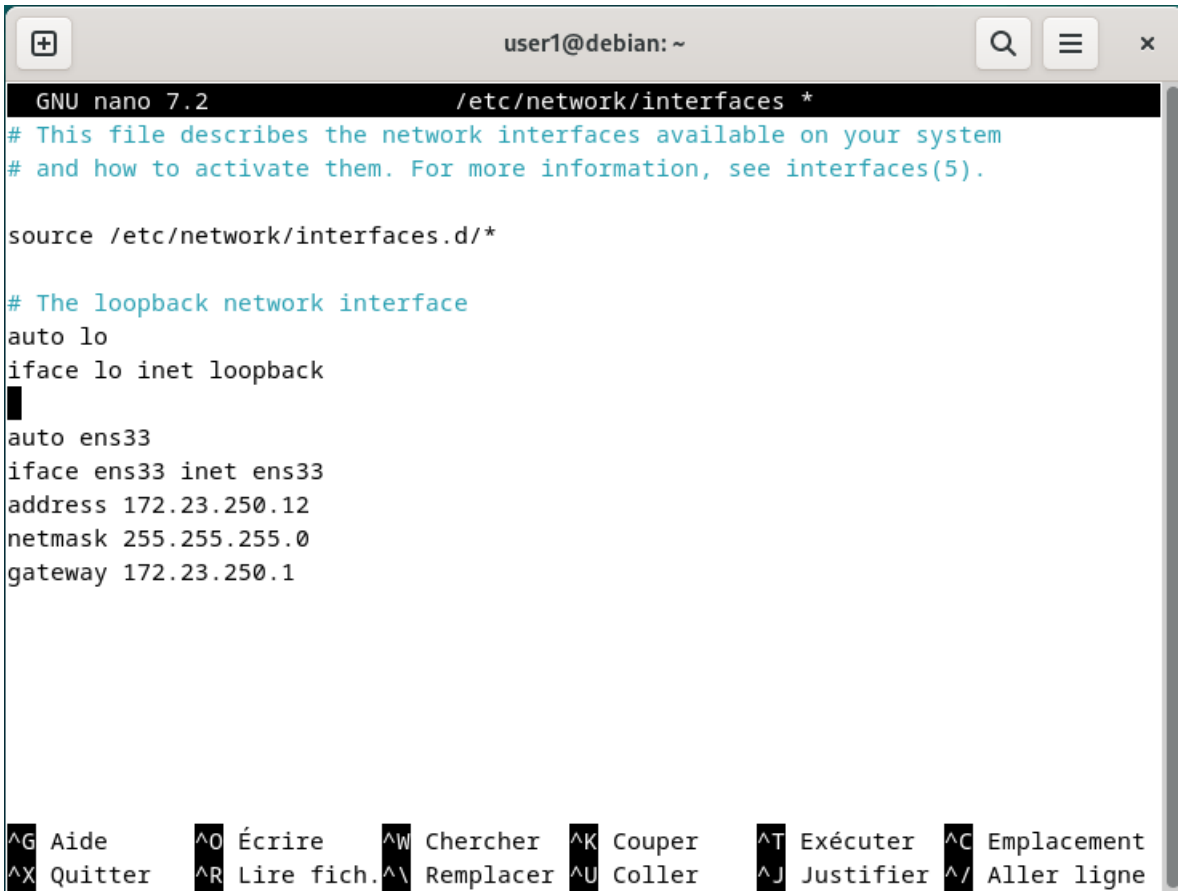
Pour la partie récupération et classement des mails (IMAP), nous allons utiliser le logiciel Dovecot.

Et enfin, pour que les utilisateurs puissent accéder à leur messagerie, nous utiliserons un webmail simple et léger : Rainloop. Un webmail est un serveur web qui permet de lire et envoyer des messages directement via un navigateur plutôt qu'en utilisant une application comme Thunderbird par exemple.

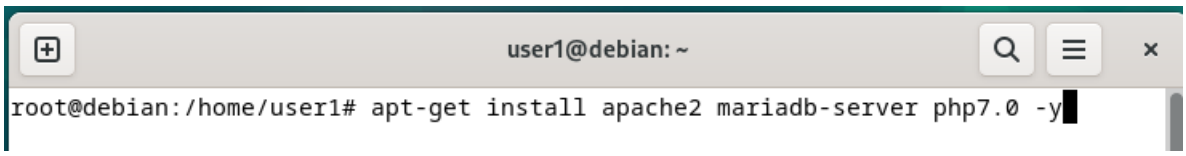
La première chose à faire vas donc d'être d'importer une machine linux et de configurer son interface sur la DMZ. Pour rappel son adresse doit être 172.23.250.12/24 avec comme passerelle 172.23.250.1

Pour cela on édit le fichier « /etc/network/interfaces »

Et on y rentre les informations suivantes

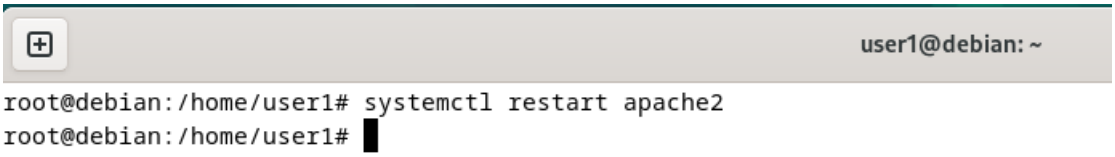


On va installer les services de base de ce qu'on appelle une pile « LAMP » (Linux Apache Mysql PHP) :



On continue par installer toutes les dépendances de php7.0 dont nous allons avoir besoin par la suite et on redémarre le service apache2 pour la prise en compte de ces dépendances :

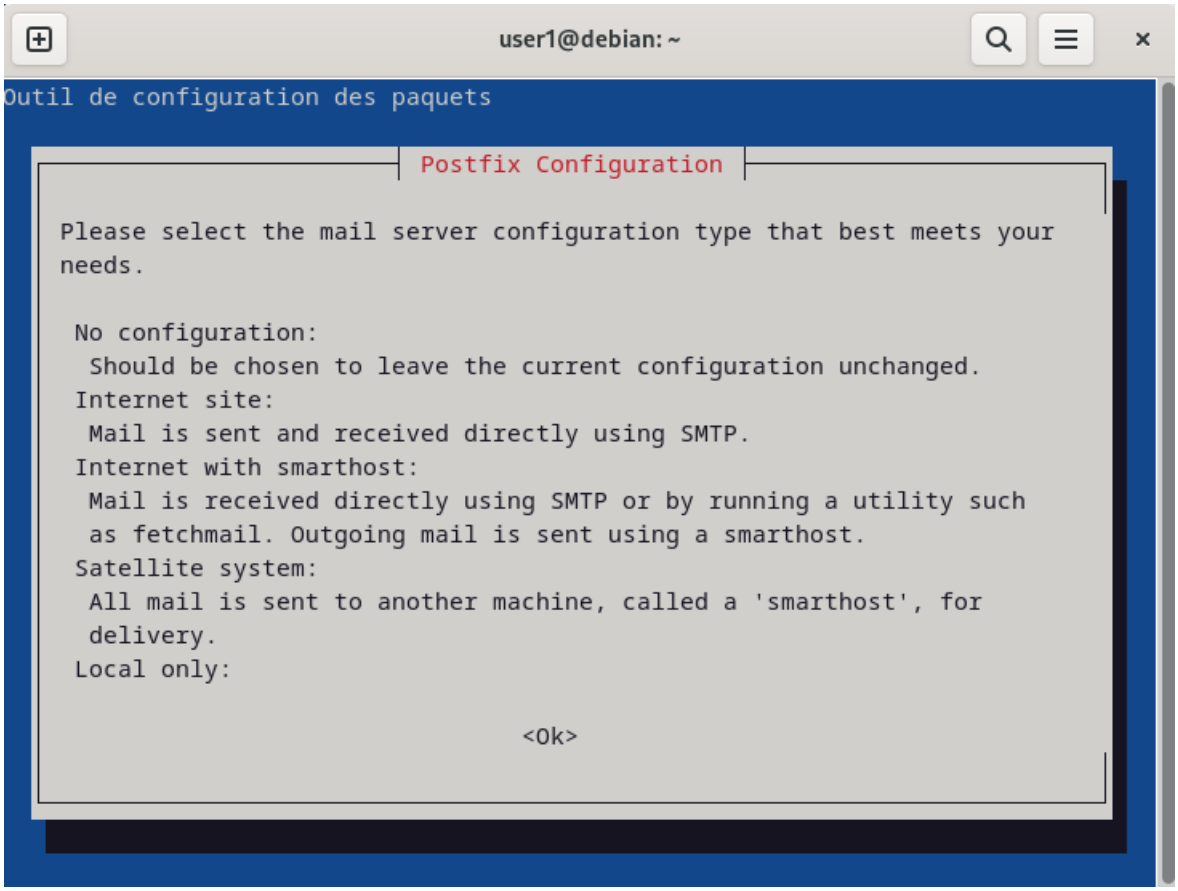
Puis on redémarre apache2



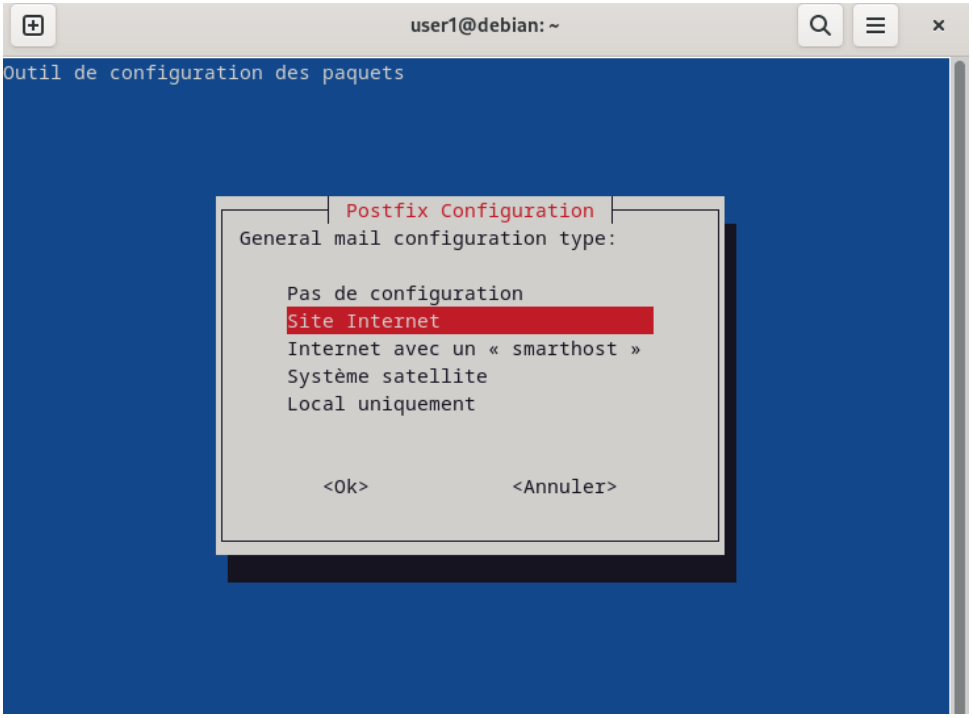
Ensuite on installe POSTFIX

Postfix est un logiciel de serveur de messagerie open source reconnu pour sa fiabilité, sa sécurité et sa facilité de configuration. Sa conception modulaire permet une personnalisation précise et une gestion efficace, tandis que ses fonctionnalités intégrées de sécurité, telles que la protection contre le

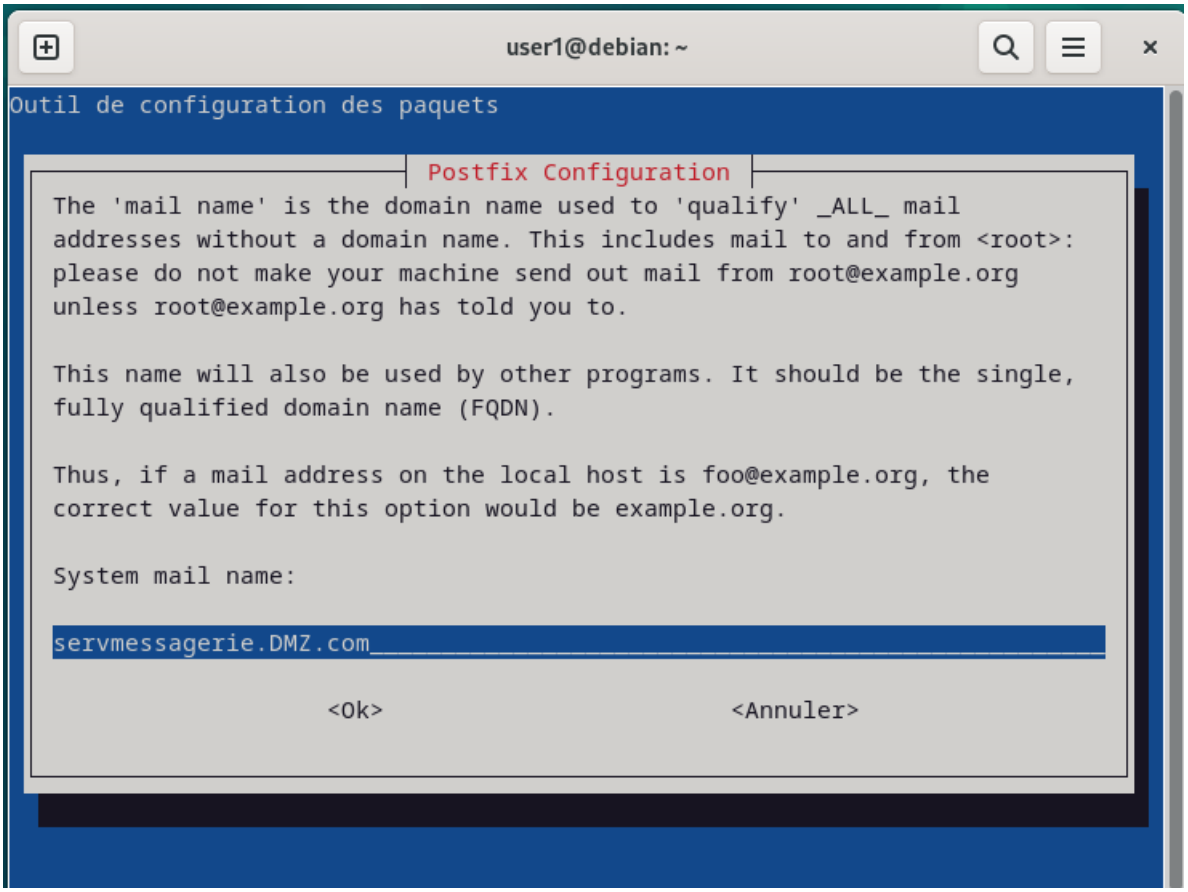
spam et le support TLS, garantissent des communications sûres. Avec une documentation exhaustive et une communauté active, Postfix est un choix populaire pour les administrateurs système cherchant une solution de messagerie robuste et évolutive.



Validez la configuration



Puis sélectionner « Site internet »



Il faudra entrer le nom de votre machine en appliquant le domaine de votre messagerie dans notre cas notre domaine est DMZ.com et notre serveur est « servmessagerie » donc cela donne servmessagerie.DMZ.com. Puis validez

On installe ensuite le paquet DOVECOT

Dovecot est un logiciel serveur de messagerie IMAP (Internet Message Access Protocol) et POP3 (Post Office Protocol) open source largement utilisé dans les environnements de messagerie électronique. Il permet aux utilisateurs d'accéder et de gérer leurs e-mails stockés sur un serveur de messagerie à distance de manière sécurisée et efficace. Dovecot est apprécié pour sa stabilité, sa sécurité et ses performances élevées. Il prend en charge des fonctionnalités avancées telles que le tri des e-mails, la recherche en texte intégral et la synchronisation des boîtes aux lettres, offrant ainsi une expérience utilisateur optimale. De plus, Dovecot est conçu pour être extensible et flexible, permettant aux administrateurs système de le configurer selon les besoins spécifiques de leur infrastructure de messagerie. Avec sa documentation détaillée et une communauté active, Dovecot est un choix populaire pour la mise en place de serveurs de messagerie fiables et évolutifs.

On va également créer sur le serveur un groupe+utilisateur local nommé ici « vmail » qui sera chargé de gérer les emails. Son « home directory » sera défini sur /var/vmail et contiendra par la suite l'ensemble des mails reçus par le serveur.

```
root@debian:~# groupadd -g 5000 vmail~

root@debian:~# useradd -g vmail -u 5001 vmail -d /var/vmail -m
```

Comme exposé en introduction, les comptes de messagerie seront virtuels. Pour administrer ses comptes de façon graphique, nous allons utiliser l'interface web du service Postfix appelée PostfixAdmin.

Avant de procéder à l'installation, nous allons préparer la base de données nécessaires au bon fonctionnement. Avant tout, si ce n'est pas déjà le cas, on va sécuriser mysql en définissant au compte root un mot de passe pour s'y connecter :

```
root@debian:~#
mariadb -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.11.6-MariaDB-0+deb12u1 Debian 12

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)]>
```

On commence par créer une base de données que j'ai appelé ici « postfix » :

```
MariaDB [(none)]> CREATE DATABASE postfix;
Query OK, 1 row affected (0,000 sec)
```

Ensuite, on crée un utilisateur, appelé postfix, et on lui attribue un mot de passe.

```
MariaDB [(none)]> CREATE USER 'postfix'@'localhost' IDENTIFIED BY 'password123';
```

Et ensuite, je donne à mon nouvel utilisateur « postfix », les pleins pouvoirs sur la base de données qui porte son nom.

```
MariaDB [(none)]> GRANT ALL PRIVILEGES ON `postfix` . * TO 'postfix'@'localhost';
Query OK, 0 rows affected (0,001 sec)
```

Pour des raisons de sécurité, nous utiliserons (plus tard dans ce tuto) plutôt un autre utilisateur pour accéder à la base de données « postfix » et qui n'aura que le droit de lecture. Ce compte se nommera « mailuser ». Je le crée et lui donne les droits nécessaires :

```
MariaDB [(none)]> CREATE USER 'mailuser'@'localhost' IDENTIFIED BY 'password321';
```

```
MariaDB [(none)]> GRANT SELECT ON `postfix`.* TO 'mailuser'@'localhost';
Query OK, 0 rows affected (0,000 sec)
```

On peut maintenant quitter la BDD

```
MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0,000 sec)

MariaDB [(none)]> QUIT;
Bye
root@debian:~#
```

On peut installer Postfix-admin

```
root@debian:/srv# wget -O postfixadmin.tgz https://github.com/postfixadmin/postfixadmin/archive/postfixadmin-3.2.
tar.gz
```

Puis on déplace le contenu de l'archive décompressée dans un dossier appelé « postfixadmin ». S'il n'existe pas déjà dans /srv, il sera créé :

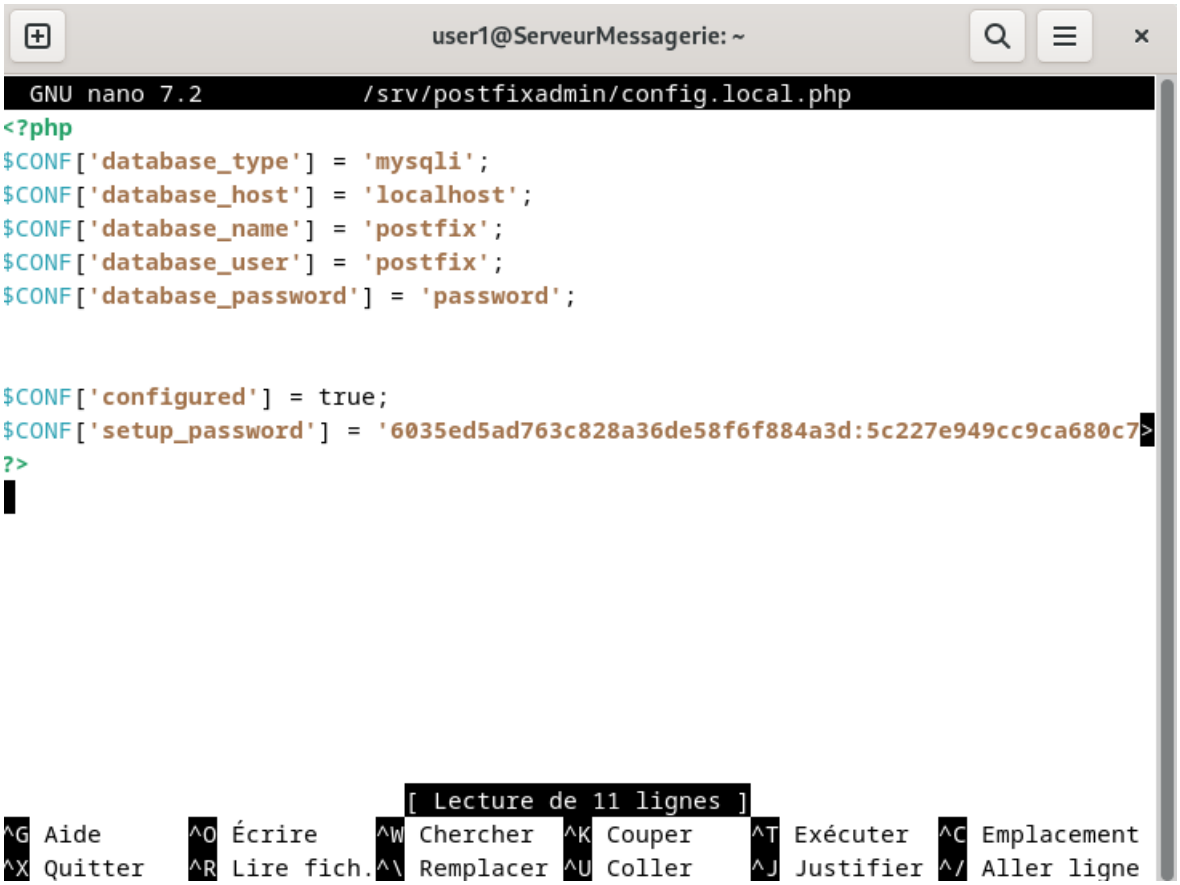
```
root@debian:/srv# mv postfixadmin-postfixadmin-3.2 postfixadmin
```

Créez un lien symbolique de notre dossier postfixadmin dans /var/www/html/postfixadmin :

```
root@debian:/srv# ln -s /srv/postfixadmin/public /var/www/html/postfixadmin
```

Maintenant, on va définir notre configuration. Créez un fichier nommé « config.local.php ».

Insérer dans ce fichier le texte suivant sans oubliez d'adapter selon l'utilisateur que vous avez créé, le mot de passe que vous lui avez attribué et le nom de base de données défini :



Toujours dans notre dossier postfixadmin, créez un dossier nommé « templates_c » et rendez l'utilisateur « www-data » (user spécifique du service web) propriétaire de ce dossier et de tout ce qu'il s'y trouvera. Ce répertoire est nécessaire pour la bonne exécution du setup de Postfixadmin.

```
root@ServeurMessagerie:/home/user1# mkdir -p /srv/postfixadmin/templates_c
root@ServeurMessagerie:/home/user1# chown -R www-data /srv/postfixadmin/templates_c
```

On peut maintenant lancer le setup. Depuis le navigateur internet d'un poste client sur le même réseau, on se rend à l'adresse suivante (en adaptant le nom serveur.domaine bien sûr) :

http://172.23.250.13/postfixadmin/setup.php

postfix.admin

Postfix Admin Setup Checker

Running software:

- PHP version 7.0.33-0+deb9u5
- Apache/2.4.25 (Debian)

Checking for dependencies:

- Magic Quotes: Disabled - OK
- Depends on: presence config.inc.php - OK
- Checking $CONF['configured'] - OK
- Depends on: presence config.local.php - OK
- Depends on: MySQL 4.1 - OK
- Testing database connection (using mysqli) - OK
- Depends on: session - OK
- Depends on: pcre - OK
- Depends on: multibyte string - OK

Une fois que tous les tests sont validés, descendez jusqu'en bas de la page.
Il vous sera demandé de définir un **mot de passe** pour l'installation. Ce mot de passe doit être suffisamment fort pour garantir la sécurité.
Une fois le mot de passe défini, cliquez sur **« Generate »**.

Change setup password

Setup password ●●●●●●●●●●

Setup password (again) ●●●●●●●●●●

Generate password hash

Le mot de passe sera alors crypté.

```
If you want to use the password you entered as setup password, edit config.inc.php or config.local.php and set
$CONF['setup_password'] = '1802f0c625f5376a86713cf7177fcc92:315612d6eaa453708f24821ca18c20f472802b59';
```

Cette ligne est importante car elle permet de **synchroniser la connexion avec la base de données**.
Il faut **copier cette ligne** et la coller dans le fichier **config.local.php** du serveur.

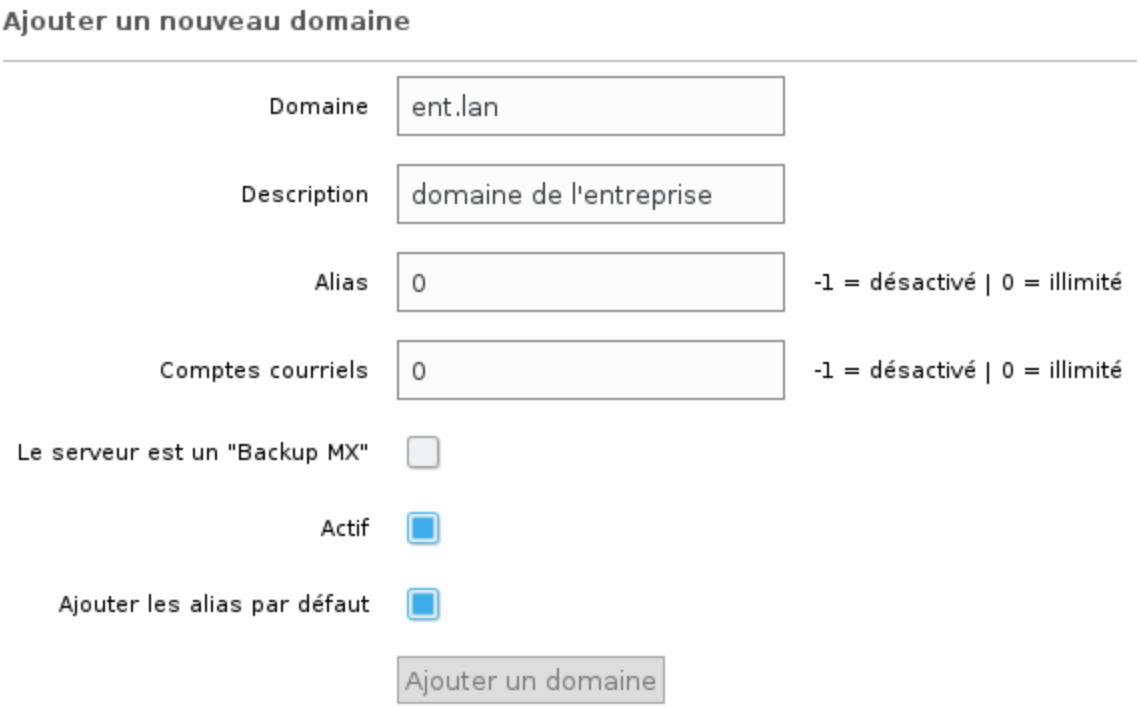
Une fois cela effectué, revenez sur le site et connectez-vous avec votre **compte administrateur**.

Ensuite, vous pouvez vous connecter à l'interface web de **PostfixAdmin** à l'adresse suivante :
http://srv-mail.ent.lan/postfixadmin/login.php

Voici un aperçu de la console d'administration :

Nous allons ajouter notre domaine. Cliquez sur « Liste des domaines » et « Nouveau domaine » dans les onglets en haut de la page :

Ajoutez votre domaine et définir le nombre d'alias et de comptes courriers sur 0 pour pouvoir en créer en illimité.



On peut maintenant créer nos adresses de messagerie. Cliquez sur « Liste des virtuels » et « Ajouter un compte courrier » dans les onglets en haut de la page.

Nous allons maintenant passer à la configuration de postfix

Pour rappel, Postfix est le logiciel de messagerie chargé de la livraison des emails. Il faut lier Postfix à la base de données afin que les utilisateurs puissent échanger des messages.

On va commencer par donner accès au domaine à postfix. Dans /etc/postfix, créez un fichier nommé « mysql-virtual-mailbox-domains.cf » et y insérer le contenu suivant :

```
root@ServeurMessagerie:/etc/postfix# nano /etc/postfix/mysql-virtual-mailbox-domains.cf
```

```
 GNU nano 7.2

user = mailuser
password = password2
hosts = 127.0.0.1
dbname = postfix
query = SELECT 1 FROM domain where domain='%s'
```

Ce fichier va permettre à Postfix, quand il reçoit un mail destiné à user@DMZ.com, de déterminer si notre serveur est bien en charge du domaine DMZ.com. Il faut qu'en exécutant la requête (définie à la ligne "query"), un élément quelconque soit retourné.

Si rien n'est retourné à l'exécution de la requête, cela signifie que le domaine n'est pas présent et que le serveur devra transmettre la demande à un autre serveur de messagerie.

Activez la configuration avec la commande suivante :

```
root@ServeurMessagerie:/etc/postfix# postconf -e virtual_mailbox_domains=mysql:/etc/postfix/mysql-virtual-mailbox-domains.cf
```

Nous allons passer maintenant à la configuration du paquet dovecot

Maintenant qu'on arrive à faire circuler les mails sur notre serveur, et qu'on les arrête quand ils sont pour nous, il faut pouvoir les récupérer pour les mettre dans des dossiers. C'est le rôle de Dovecot.

Dovecot est un serveur de messagerie open source populaire, spécialisé dans les protocoles IMAP (Internet Message Access Protocol) et POP3 (Post Office Protocol version 3), permettant aux utilisateurs d'accéder à leurs e-mails stockés sur un serveur à distance de manière sécurisée et efficace. Il est largement utilisé dans les environnements de messagerie électronique pour sa fiabilité, sa sécurité et ses performances élevées. Dovecot prend en charge diverses fonctionnalités avancées telles que la gestion des boîtes aux lettres, la recherche en texte intégral et la gestion des quotas, tout en offrant une configuration flexible pour répondre aux besoins spécifiques des utilisateurs. Grâce à sa documentation complète et à sa communauté active, Dovecot est un choix populaire pour ceux qui cherchent à mettre en place un serveur de messagerie robuste et évolutif.

On va maintenant indiquer à Dovecot comment se connecter à la base de données. Placez-vous dans le dossier /etc/dovecot.

Modifier le fichier « dovecot-sql.conf.ext ». Tout à la fin de ce fichier, ajouter les 3 lignes suivantes en adaptant avec vos informations

```
driver = mysql
connect = host=127.0.0.1 dbname=postfix user=mailuser password=password2
password_query = SELECT username,domain,password FROM mailbox WHERE username='%u';
```

Modifiez les droits sur le fichier « dovecot.conf » situé dans /etc/dovecot pour que Dovecot soit lancé en tant qu'utilisateur « vmail » :

```
root@ServeurMessagerie:/etc/dovecot#
chgrp vmail /etc/dovecot/dovecot.conf
```

```
root@ServeurMessagerie:/etc/dovecot# chmod g+r /etc/dovecot/dovecot.conf
```

Maintenant qu'on a d'un côté Postfix, qui sait quand un mail passe s'il est pour lui ou s'il doit le transmettre à un autre serveur mails, et Dovecot qui sait où les stocker, il faut donc que Postfix relaie les mails à Dovecot.

Pour cela, ajouter les 2 lignes suivantes à la fin du fichier /etc/postfix/master.cf.

```
mailman   unix  -       n       n       -       -       pipe
  flags=FRX user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py ${nexthop} ${user}

dovecot   unix  -       n       n       -       -       pipe
  flags=DRhu user=vmail:vmail argv=/usr/lib/dovecot/dovecot-lda -f ${sender} -d ${recipient}
```

Et appliquez les modifications que l'on vient d'effectuer avec les 2 commandes suivantes :

```
root@ServeurMessagerie:/etc/dovecot# postconf -e virtual_transport=dovecot
root@ServeurMessagerie:/etc/dovecot# postconf -e dovecot_destination_recipient_limit=1
```

Nous allons pour terminer installer le webmail Rainloop pour que les utilisateurs consultent leurs messages en « graphique »

RainLoop est une application webmail open source légère et conviviale. Conçue pour être facile à installer et à utiliser, elle offre une interface utilisateur moderne et réactive pour accéder et gérer les e-mails à partir de n'importe quel navigateur web. RainLoop prend en charge plusieurs protocoles de messagerie, y compris IMAP et SMTP, ce qui lui permet de se connecter à divers serveurs de messagerie. Ses fonctionnalités comprennent la gestion des dossiers, la recherche d'e-mails, la composition de messages avec une mise en forme riche, et la gestion des contacts. De plus, RainLoop offre des options de personnalisation pour les utilisateurs avancés et peut être intégré à d'autres applications webmail ou services tiers. En raison de sa simplicité d'installation et de son interface utilisateur intuitive, RainLoop est une option populaire pour ceux qui souhaitent fournir une solution webmail efficace à leurs utilisateurs.

On commence par Créer un répertoire « rainloop » dans /var/www /html et on se place à l'intérieur

```
root@ServeurMessagerie:/etc/dovecot# mkdir /var/www/html/rainloop
```

```
root@ServeurMessagerie:/etc/dovecot# cd /var/www/html/rainloop
```

Puis on récupère la dernière version de rainloop en la récupérant sur internet

```
root@ServeurMessagerie:/etc/dovecot# wget -qO- https://repository.rainloop.net/installer.php | php
```

Il faut ensuite Aller dans */etc/apache2/sites-available* et copier le fichier « *000-default.conf* » en le renommant « *rainloop.conf* »:

```
root@ServeurMessagerie:/etc/dovecot# cp 000-default.conf rainloop.conf
```

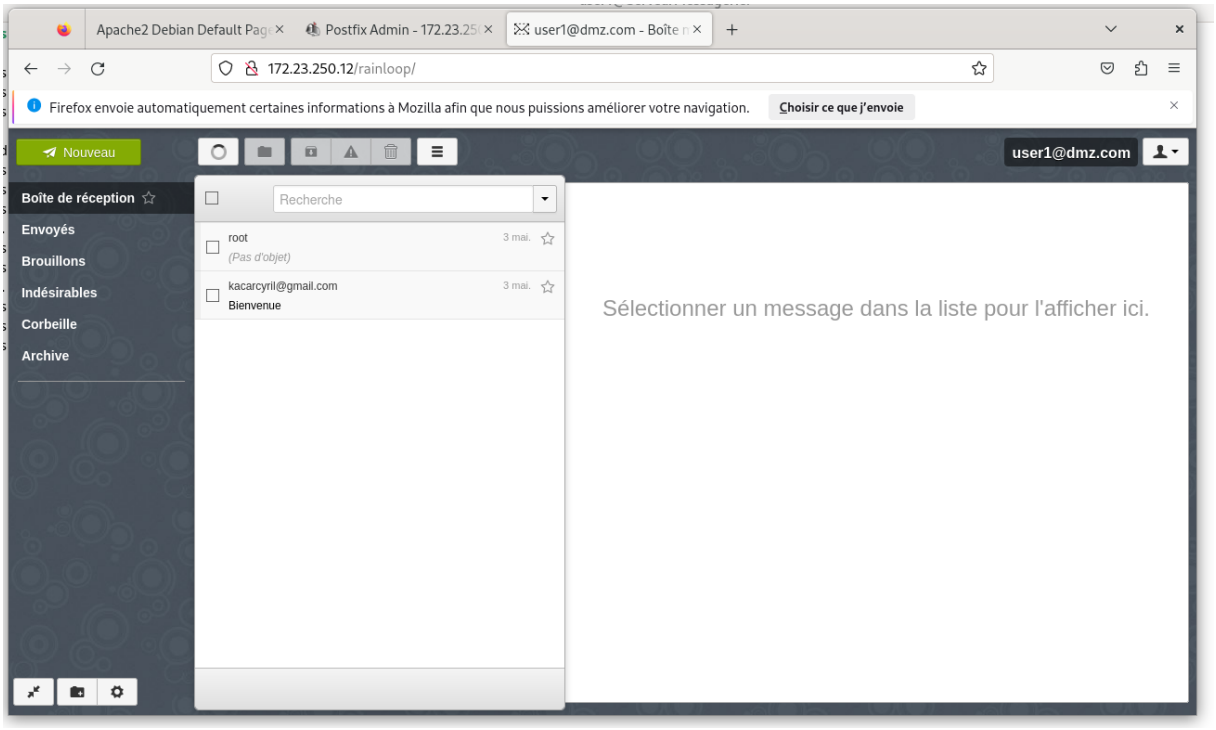
On active ensuite la page web

```
root@ServeurMessagerie:/etc/dovecot# a2ensite rainloop.conf
```

Le serveur de messagerie est maintenant fonctionnel et nous pouvons accéder à l'interface graphique depuis un serveur client

Nous pouvons donc accéder à l'interface de la messagerie en tapant dans l'url

http://172.23.250.12/rainloop/



Et nous voyons que l'utilisateur/ administrateur nous accueille avec un message

Nous allons maintenant faire en sorte qu'apache (le paquet serveur WEB) utilise et écoute un autre port que celui de base. Apache utilise le port 80 s'il n'utilise pas le protocole http et 443 s'il utilise le protocole https.

Pour le serveur de messagerie nous avons convenue qu'il utiliserait le port 2007. Cette partie est particulièrement importante car nous avons déjà paramétrais les ports qui seront utilisés par les différents services dans le pare-feu IPfire, notamment au niveau des règles NAT avec la redirection de port.

Nous allons donc éditer le fichier de configuration du virtualhost de RainLoop

```
root@ServeurMessagerie:/etc/apache2/sites-enabled# nano /etc/apache2/sites-enabled/rainloop.conf
```

Et on change la première ligne

```
<VirtualHost *:80>
```

En 2007

```
<VirtualHost *:2007>
```

Puis on redémarre le service

```
root@ServeurMessagerie:/etc/apache2/sites-enabled# systemctl restart apache2
```

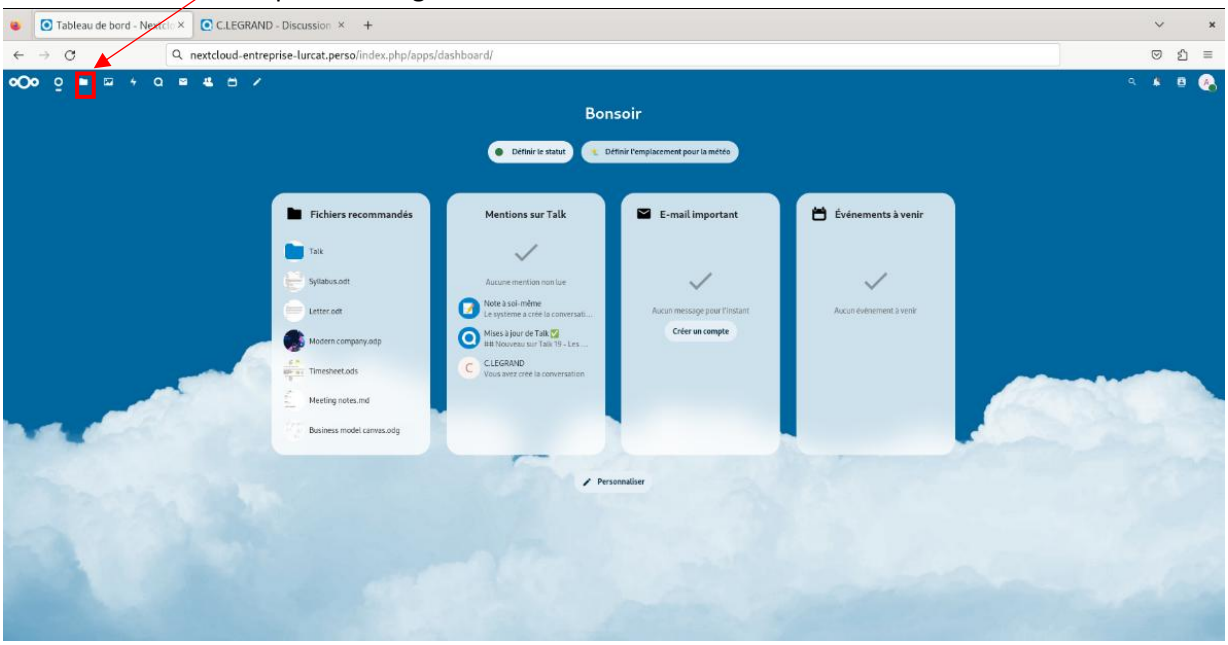
Et voilà notre serveur de messagerie utilise maintenant le port 2007

Les taches 6.0, 6.1 et 6.2 sont terminées

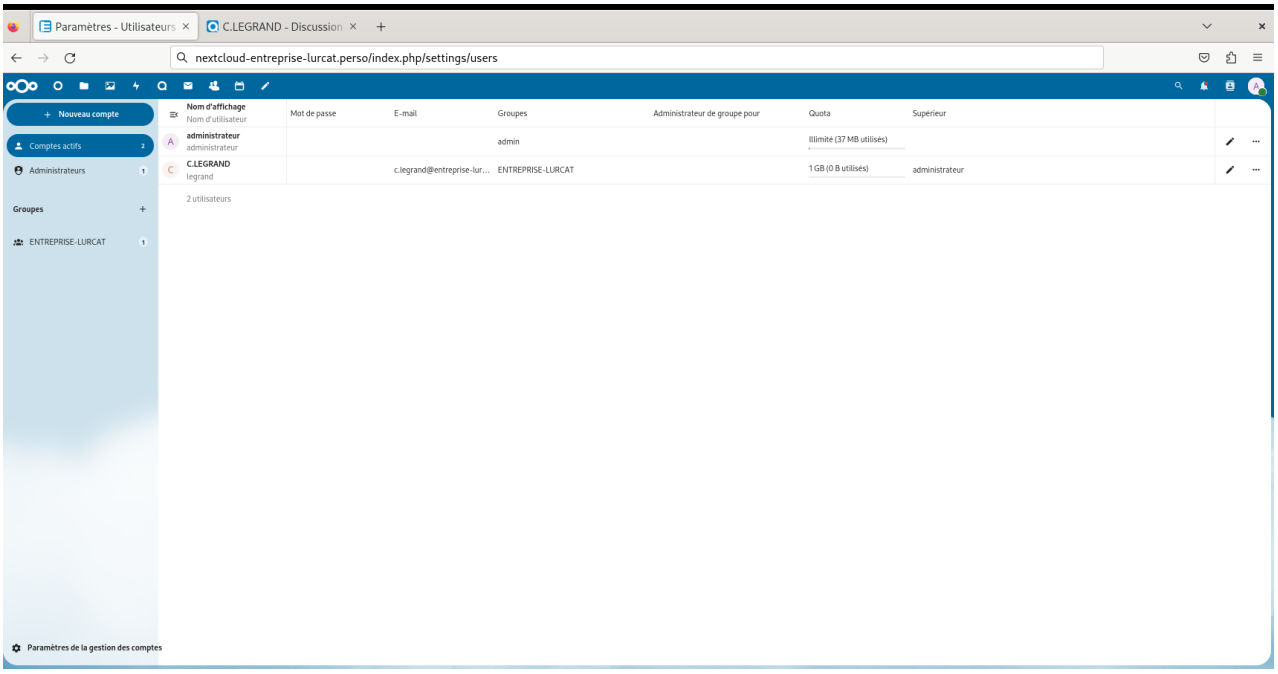
Nous allons passer à la partie test

Test NextCloud :

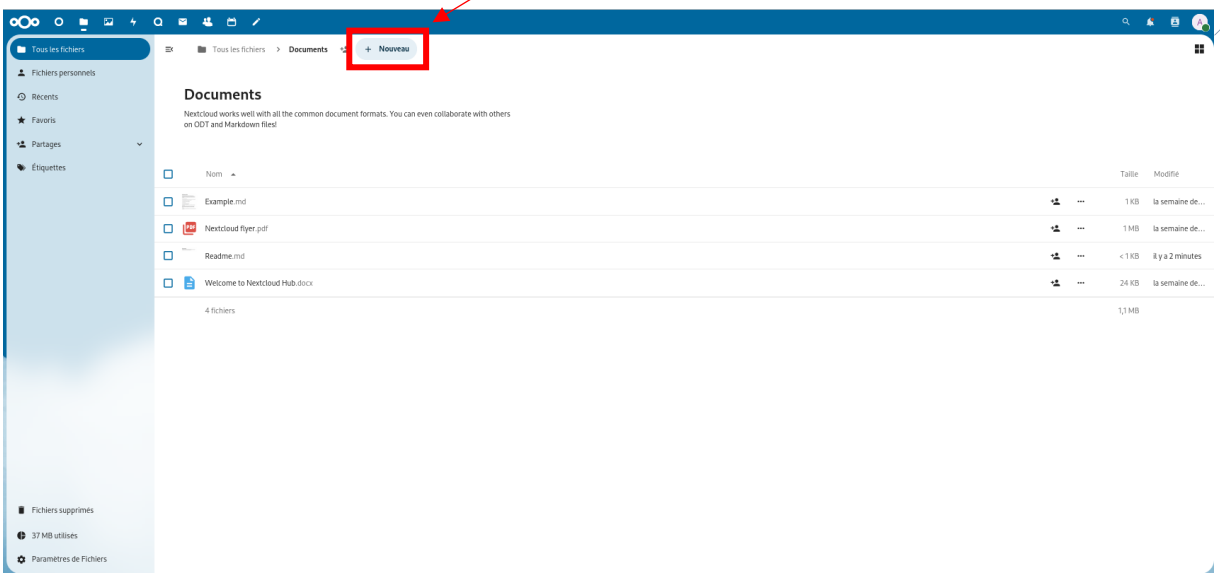
On clique sur le logo fichiers

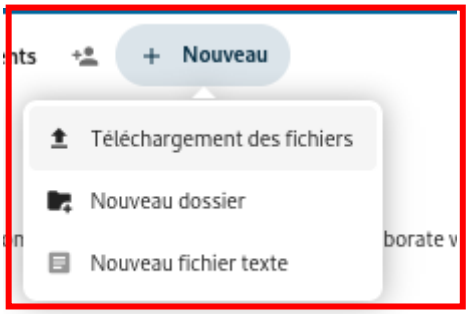


UTILISATEUR C.LEGRAND

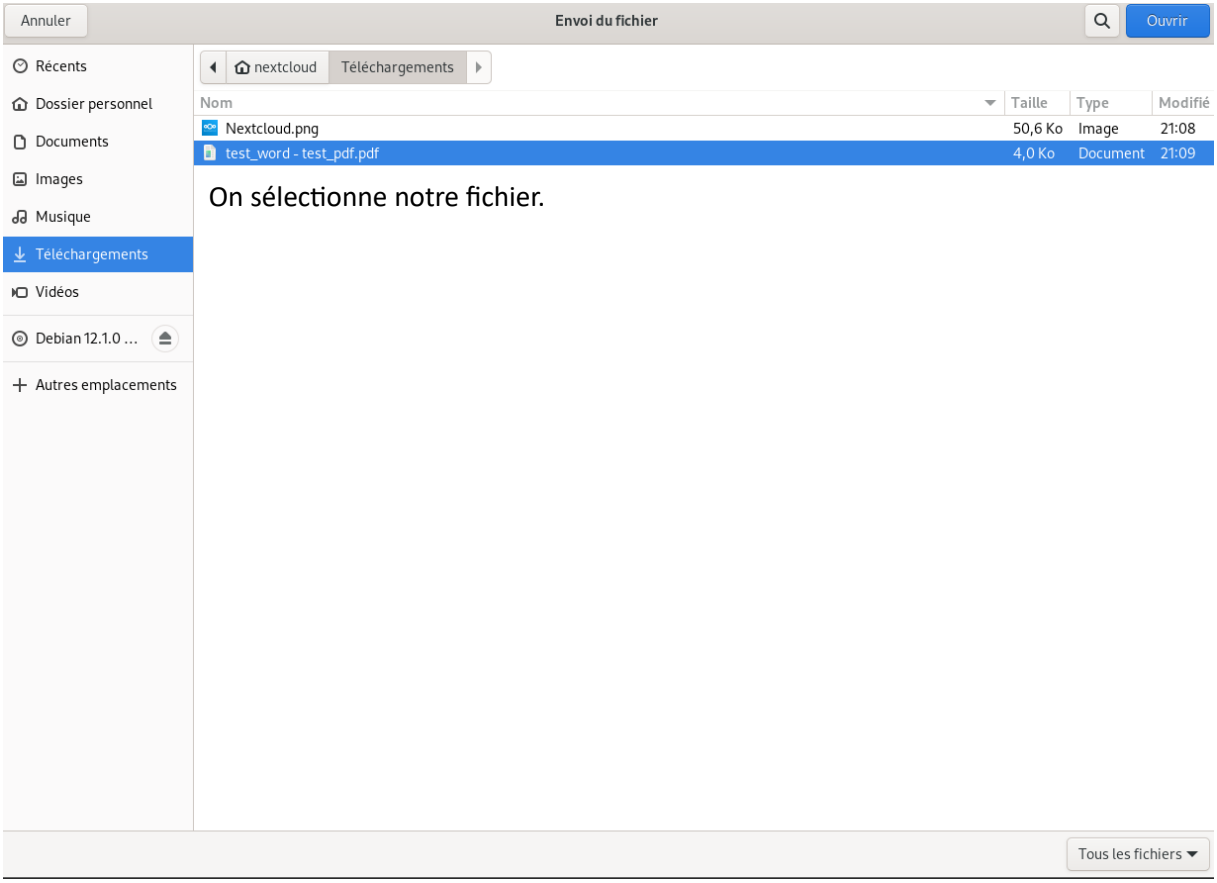


Cliquer sur « + Nouveau »

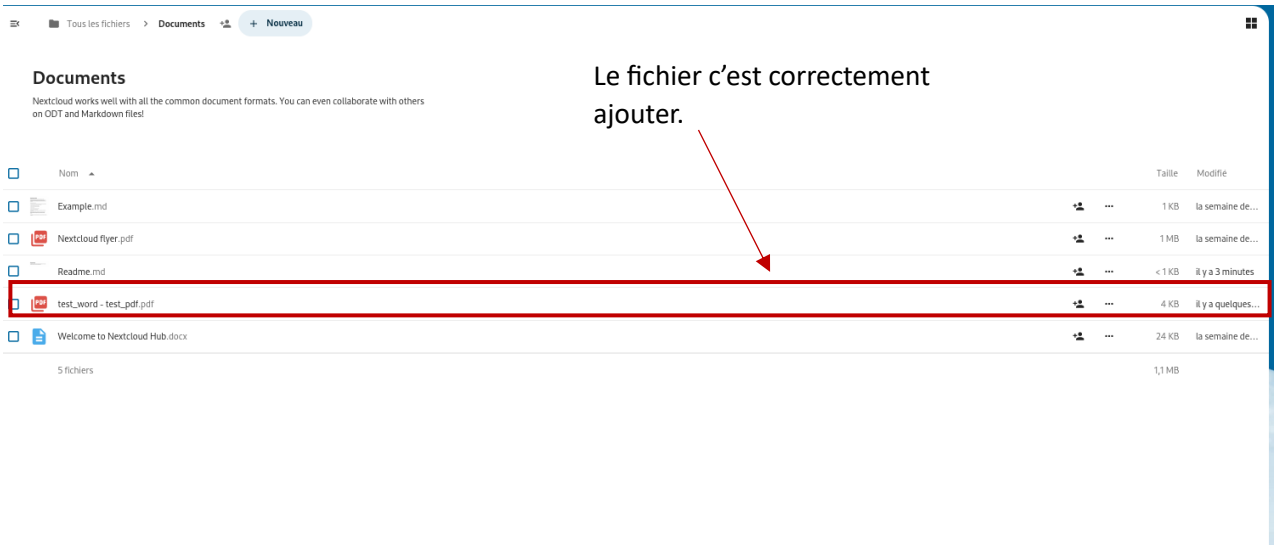




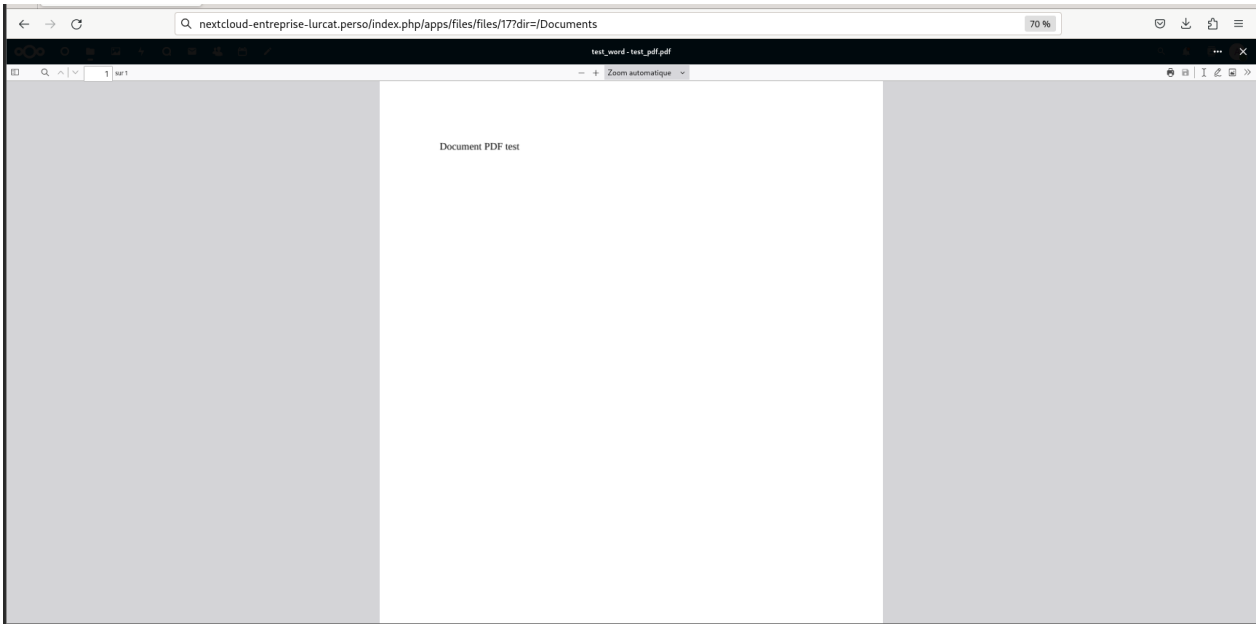
Sélectionner ce que vous souhaitez ajouter, dans notre cas un fichier.



On sélectionne notre fichier.



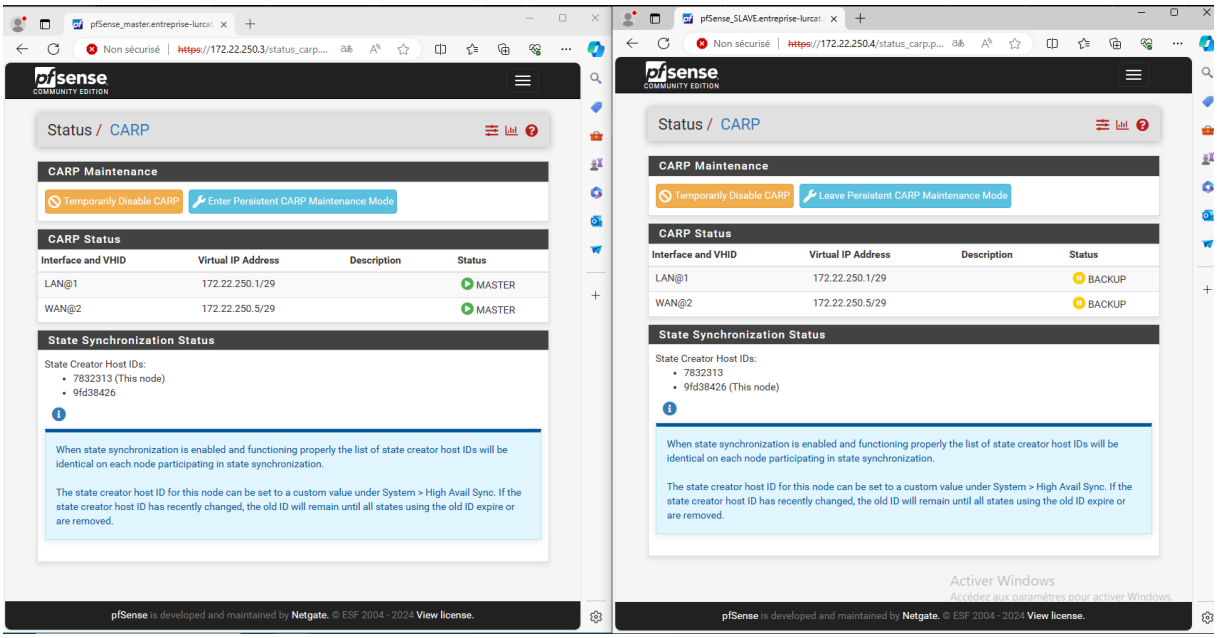
Le fichier c'est correctement ajouter.



On peut cliquer et voir son contenu !

Test de basculement pfSense :

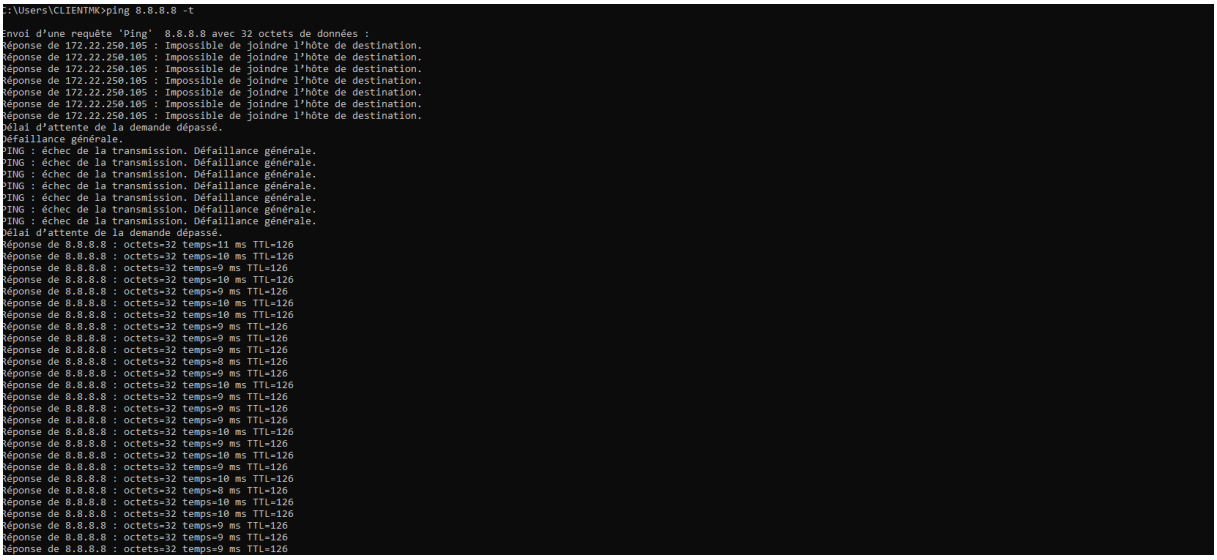
Nous allons commencer par vérifier l'état de la synchronisation entre nos deux servers pfSense Master et pfSense Slave.



En prenant un client du LAN, nous allons pinger la Gateway (ou une IP externe) et éteindre le pfSense Master principal.

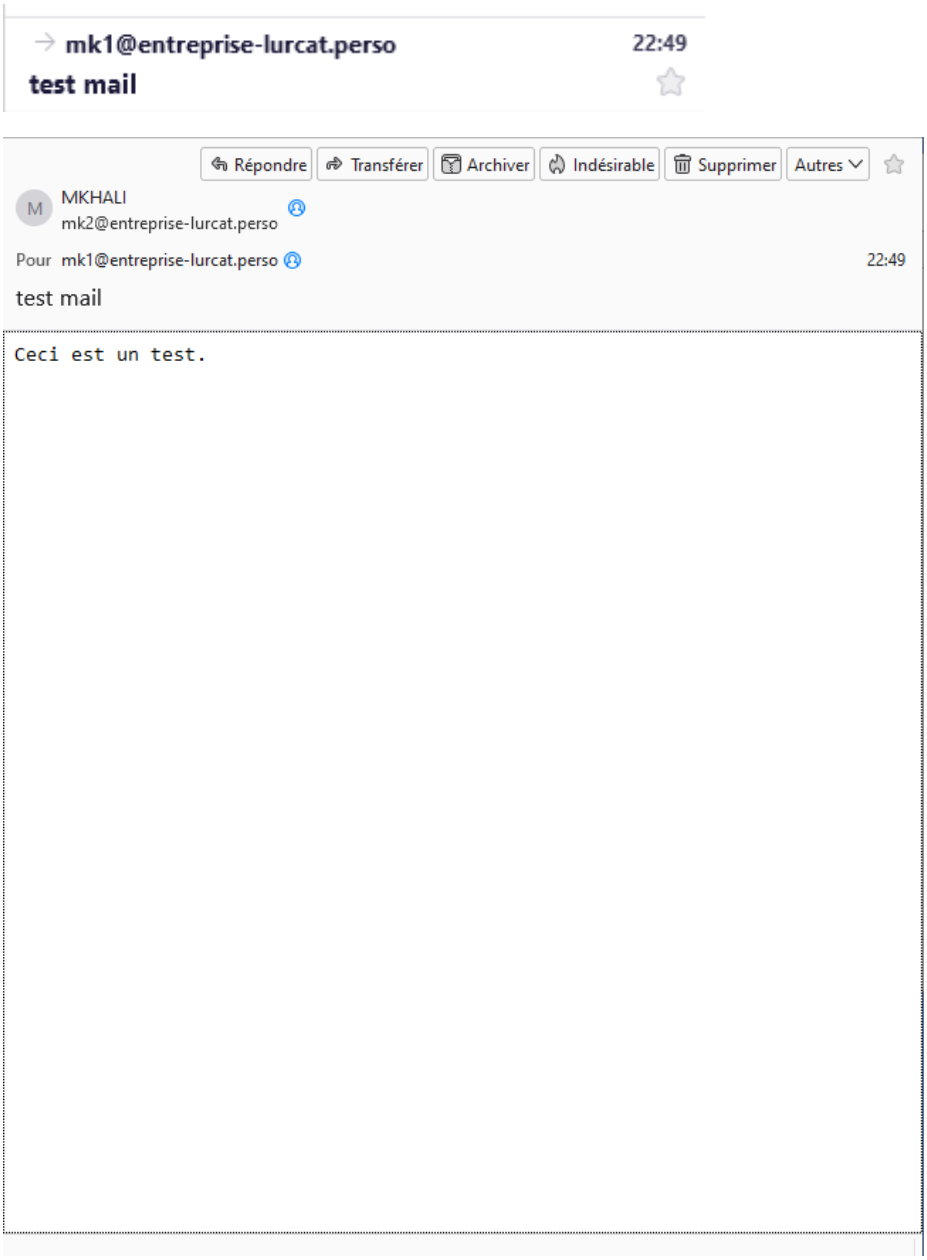
On constate le moment de la bascule avec deux paquets dupliqués (les deux pares-feux répondent à ce moment-là) ou une perte d'un paquet. Il n'y a pas eu d'interruption de service, et le second pare-feu est passé avec le statut MASTER.

Les services rebasculeront sur le pare-feu principal lorsqu'il sera de nouveau opérationnel.



Test de basculement opérationnel (Délais plus long dû au nombreuse machine virtuelle allumé)

Test serveur mail depuis client LAN vers DMZ



Test Serveur WEB :