KAPALA Paul-Alexis
MASSEI Liam
LIGNIERE Timothée
BTS SIO2
Date de création 21/03/23
Date de maj 15/04/23

DMZ

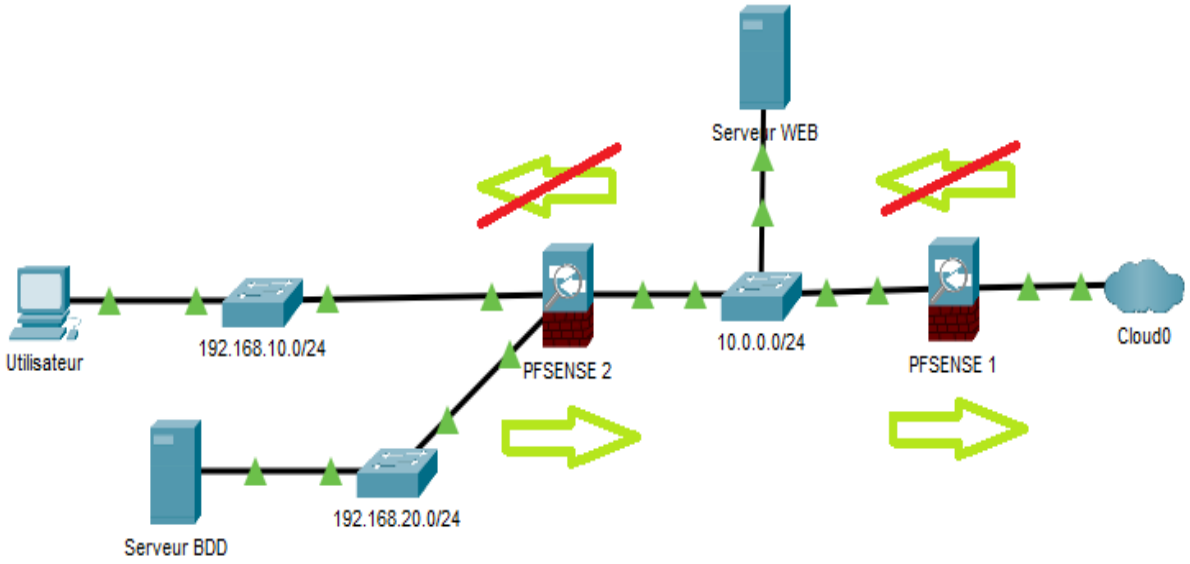
Sommaire

1 - Problématique

Il peut être nécessaire de sécuriser un réseau des menaces extérieures tout en laissant un accès volontaire à un site web et en conservant pour autant la connexion à Internet pour les machines des utilisateurs du réseau. Une solution a été recommandé par l'ANSSI afin de résoudre cette problématique, la DMZ (ou Zone démilitarisée).

Une DMZ a pour but de sécuriser un réseau interne tout en permettant aux machines des utilisateurs d'accéder à Internet, la connexion des utilisateurs passant par deux pare-feu avec des règles légèrement différentes avant de pouvoir être reçu.

2 - Schéma logique de la solution



Le Pfsense 1 refuse toutes les connexions entrantes mis à part celles à destinations du serveur WEB à l'aide d'un reverse proxy ; le Pfsense2 bloque lui aussi toutes les connexions entrantes, mais sans exception.

L'utilisateur et le serveur BDD peuvent donc accéder à Internet, au Serveur Web et communiquer entre eux .

Le Serveur WEB ne peut qu'accéder à Internet.

3 - Notice d’installation

L’installation présentée après se déroule sous Oracle VM.

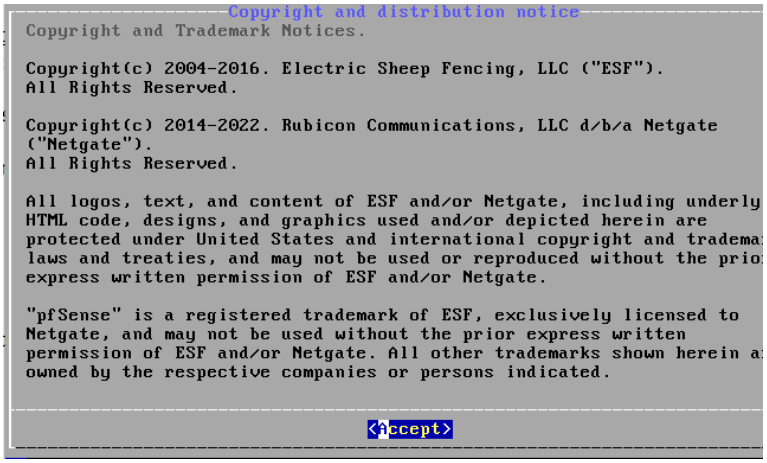
3.1.1 - Installation de Pfsense

L’installation est la même pour les 2 Pfsenses, seul la configuration diffère légèrement.

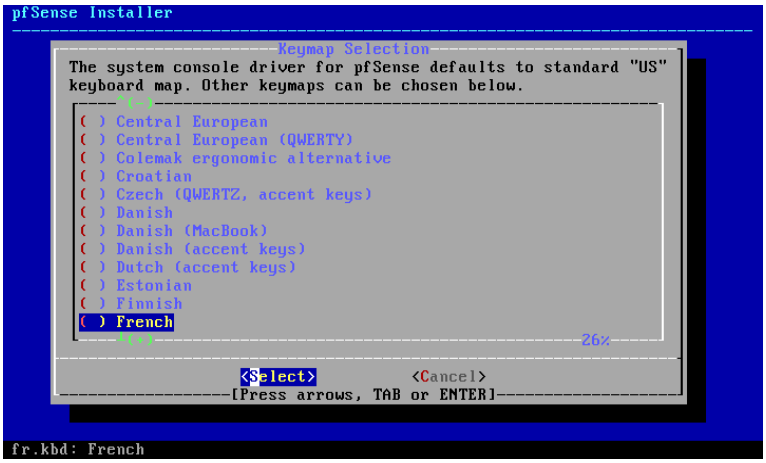
Pfsense n’est pas un logiciel à installer sur une machine déjà existante, il est sa propre machine. Créé donc une machine avec minimum 1 Go de RAM et 1 Go de stockage pour son bon fonctionnement, cela n’est pas un problème si vous lui donnez plus.

Insérez ensuite l’image iso lors de la mise en route de votre machine, il se peut que l’iso de votre pfsense soit incorrect selon votre architecture de processeur

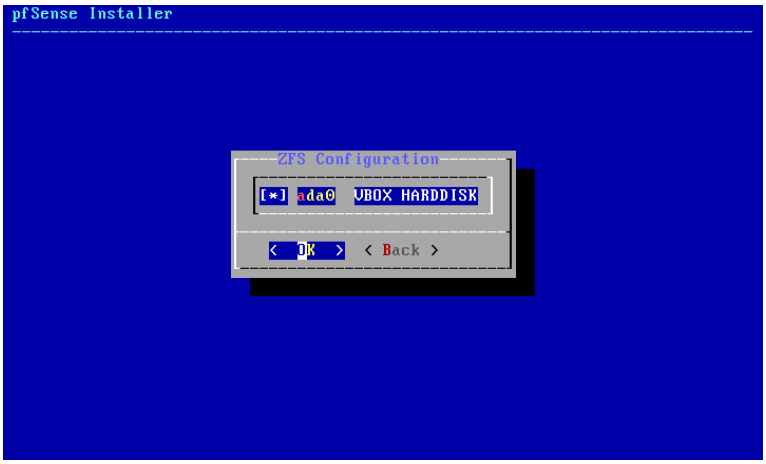
Peu de temps après le lancement, vous aurez cet écran :



Acceptez ceci puis validez l'installation de Pfsense. Vous pourrez ensuite choisir la langue de votre clavier.



Sélectionnez-la avec les flèches puis validez. Puis continué à valider jusqu'à l'écran suivant :

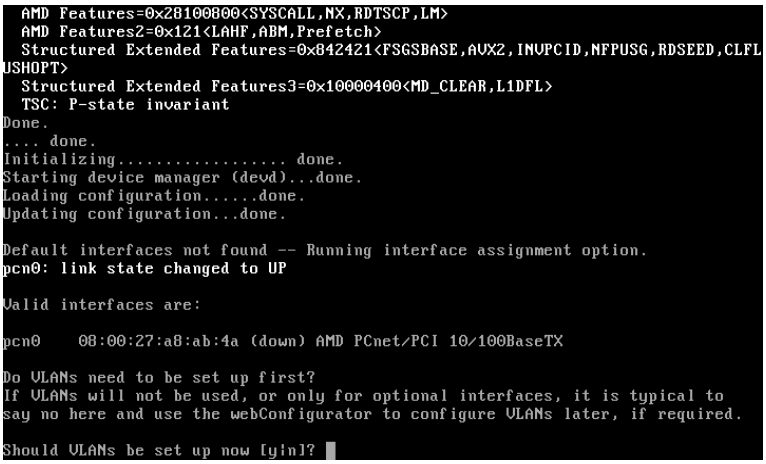


Pour choisir votre disque utilisé la barre espace puis valider. L'installation devrait se lancer après la confirmation de la suppression des données du disque choisit.

Poursuivez jusqu'à cet écran.

Lorsque vous arriverez à cet écran, éjecter de force l'image iso de pfsense afin d'éviter que lors du redémarrage, l'image relance l'installation.

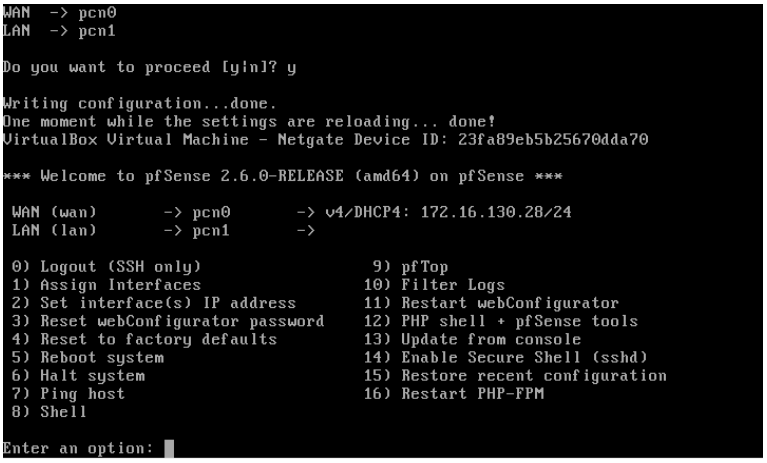
Après cela, redémarrer votre machine. Si tout s'est installé correctement, vous aurez cet écran à la fin du démarrage.



Pfsense va donc vous demander ses premiers paramètres.

Nous n'avons pas besoin des vlans, vous pouvez donc refuser, puis sélectionnez vos interfaces (L'une de vos interfaces doit être de préférence en accès par pont et la deuxième en réseau interne).

Le menu de base de Pfsense apparaîtra suite à cela :

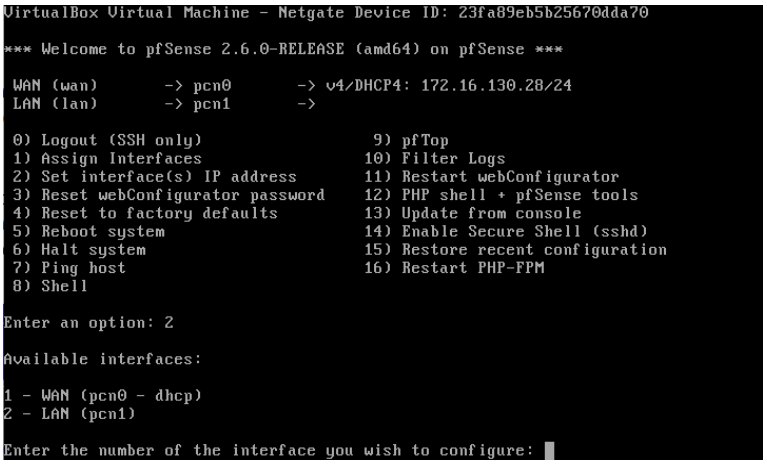


Pfsense est donc désormais installé, la configuration de ce dernier pour initialiser la DMZ se trouve dans la partie suivante . (Vous pouvez cloner cette première machine pour le Pfsense 2 si vous êtes sur une plateforme de virtualisation).

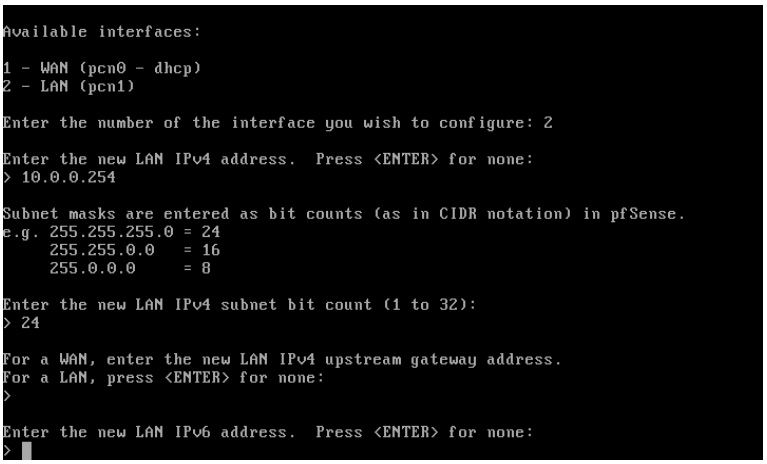
3.1.1 – Configuration basique du Pfsense 1

3.1.1.1 – Configuration passerelle

Pour rajouter une adresse IP à la passerelle du côté du LAN, retourner sur votre Pfsense et entrer l'option 2 :

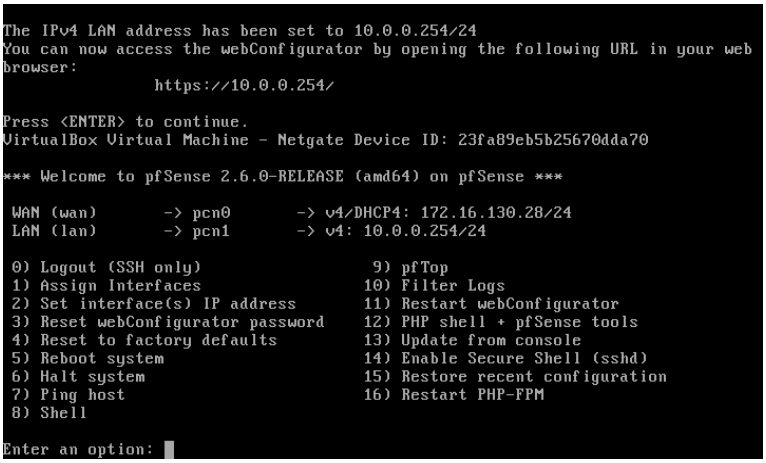


Dans le cas présent, le WAN est déjà géré par le DHCP de notre réseau (Ce n'est pas le cas si vous configurez le pcn0 du Pfsense2). Nous allons donc configurer le LAN et lui assigner l'adresse 10.0.0.254 avec un CIDR de 24 :



Vous pouvez activer le DHCP si vous le voulez, vous n’aurez qu’à remplir l’adresse de début de plage et celle de fin, vous pouvez refuser le reste.

Une fois cette configuration terminer, vous obtiendrez à peu près cela :



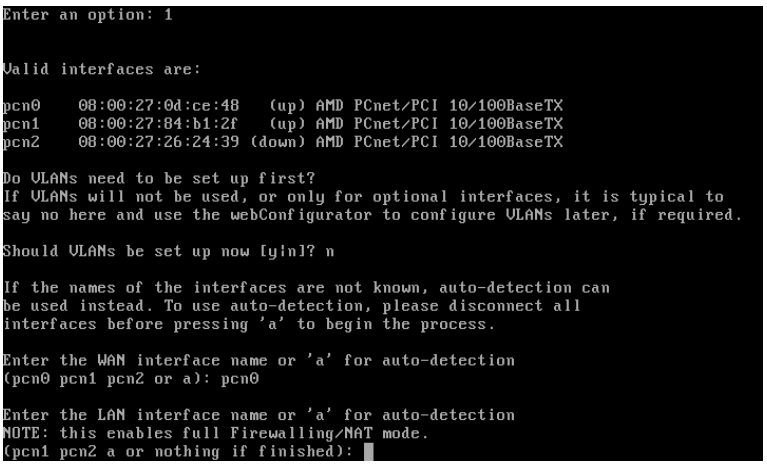
Votre Pfsense est désormais prêt a géré les machines qui seront connectées sur le LAN, afin de ne pas perdre le fil, nous allons désormais configurer le Pfsense2.

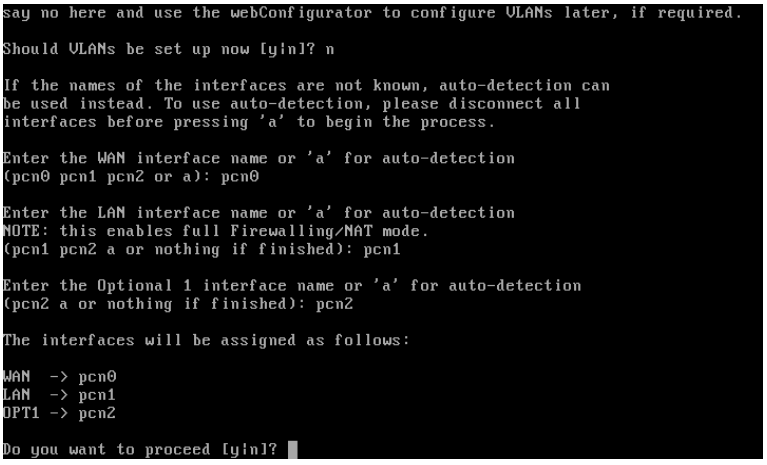
3.2 – Configuration basique du Pfsense 2

Vous pouvez démarrer votre pfsense 2 pour mettre en place les adresses sur chaque passerelle et le pfsense 1 pour vérifier la communication avec l'extérieur.

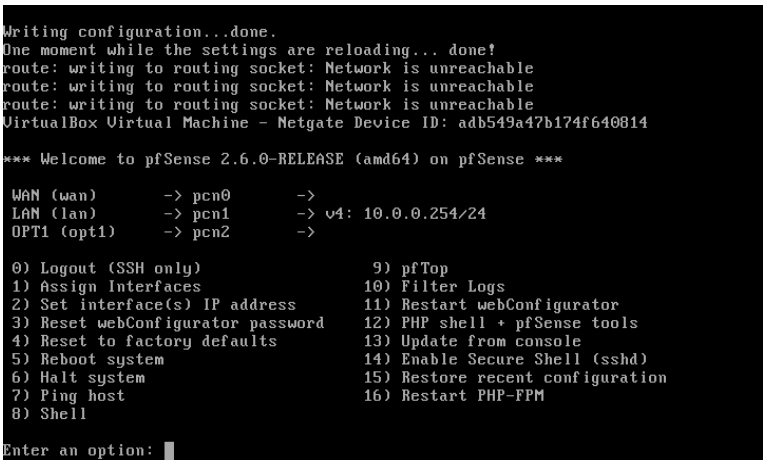
La configuration des passerelles est la même que pour le Pfsense 1, cependant si votre machine a été clonée depuis la première, il peut être nécessaire de lui assigner une nouvelle interface.

Pour cela rentrer l'option 1 puis dites les différents noms de passerelles avec chacune leurs utilités (pcn0=WAN, pcn1=LAN, pcn2=OPT1)



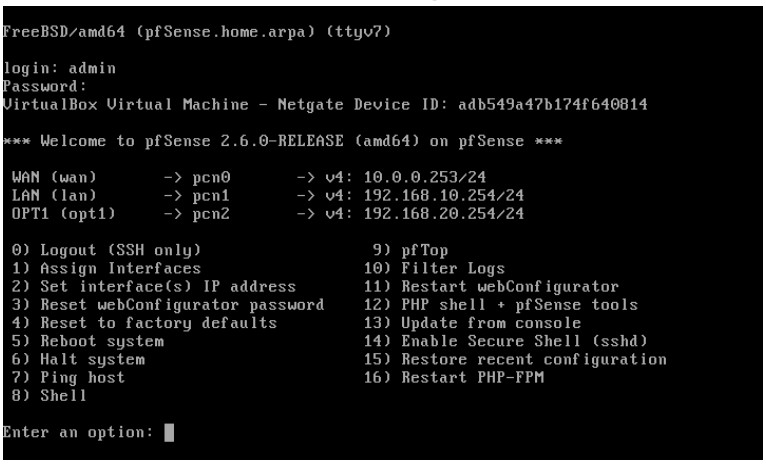


Vous retournerez ensuite sur le menu principal avec cet affichage :



Aucune des adresses n'est donc correcte, pour notre infrastructure pcn0 doit avoir comme adresse 10.0.0.253, pcn1 192.168.10.254 et pcn2 192.168.20.254 tous en CIDR 24 et comme passerelle sur pcn0 10.0.0.254. Pour rappel, ceci est similaire au Pfsense 1.

Vous aurez donc à la fin de votre configuration ceci :

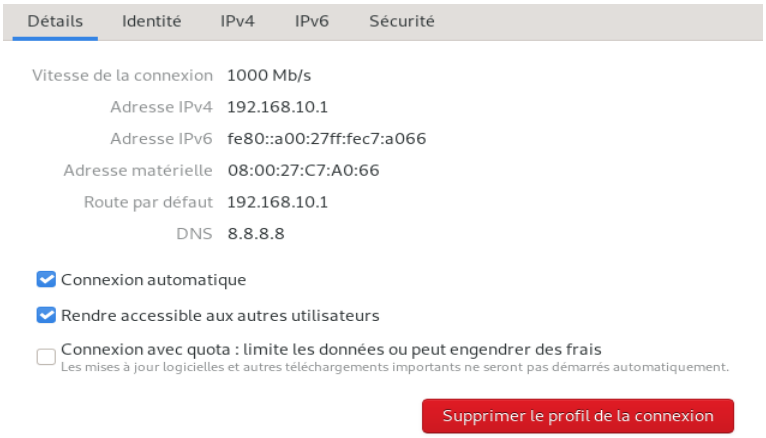


La configuration basique du Pfsense 2 est terminé.

3.3 – Connecter les machines aux Pfsenses

Si vous n’avez pas activé le DHCP de votre Pfsense1, mettez les paramètres suivants pour l’adresse réseau :

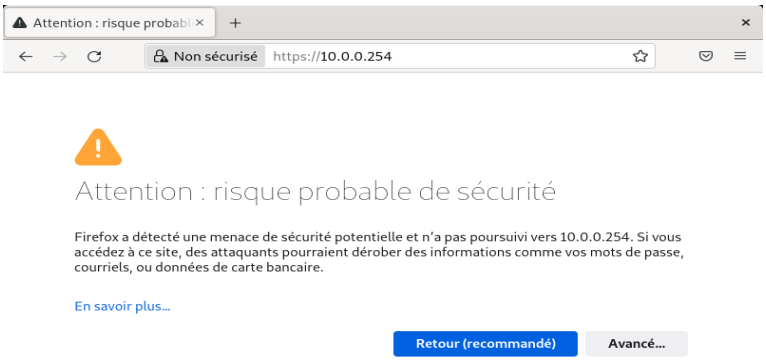
La machine cliente a elle comme configuration ceci :



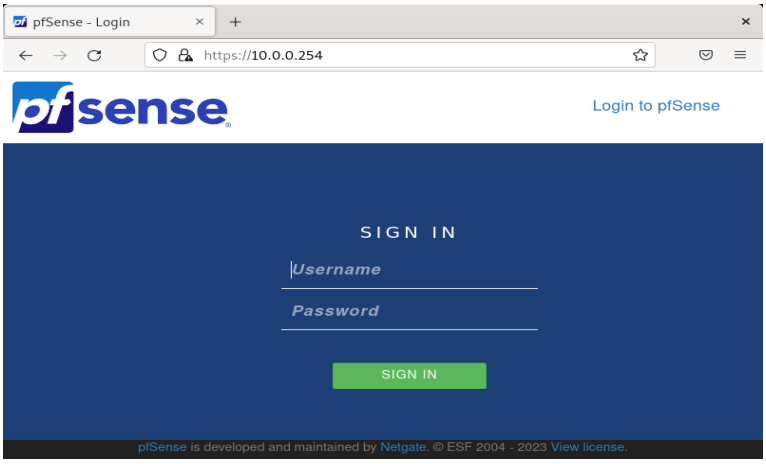
La machine gérant le serveur BDD a pour configuration :

3.4.1 – Configuration poussée du Pfsense 1

Connectez-vous à votre serveur Web puis dans votre navigateur, entrer l'adresse de votre Pfsense 1 du côté de son LAN :



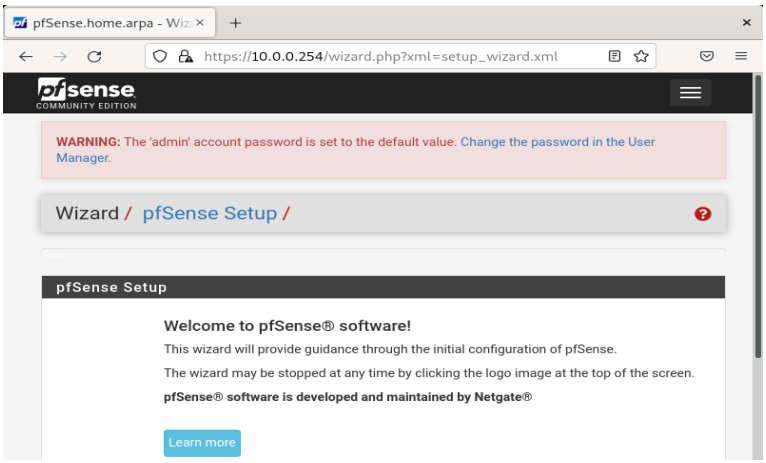
Il est possible que votre navigateur vous mettes en garde comme dans l'image précédente, mais ce n'est rien de grave, cliqué sur « Avancé… » puis « Accepter le risque et poursuivre »



Vous voilà donc sur la page de connexion de votre Pfsense1, le nom d'utilisateur et le mot de passe sont toujours les mêmes lors de la première connexion :

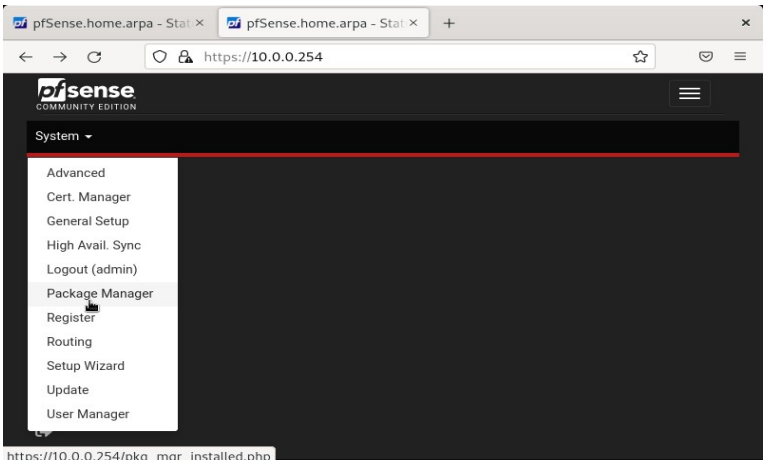
Username = admin

Password = pfsense

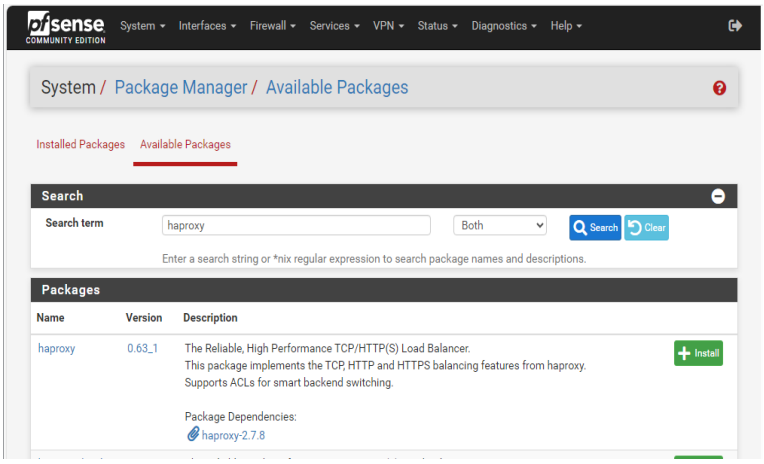


3.4.1.1 – Mise en place du proxy

Pour que le serveur Web soit accessible depuis l'extérieur du pare-feu, nous avons besoin de mettre en place un proxy sur le pfsense 1, pour cela, allez dans « System » puis « Package manager »

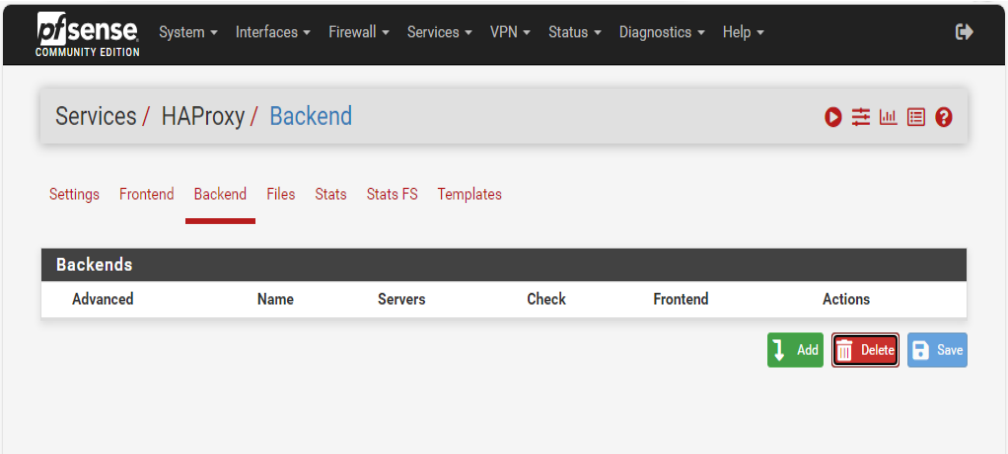


Puis sélectionné « Available Packages » en recherchant « haproxy »

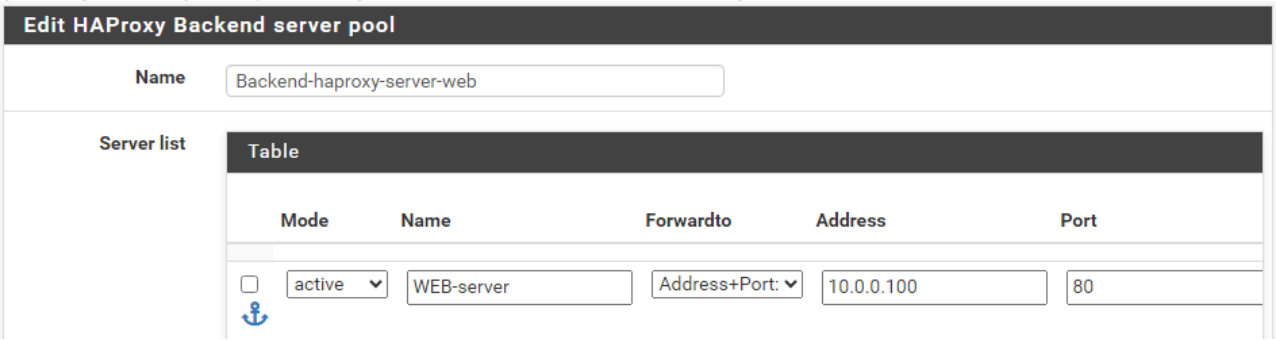


Installez-le et confirmer l'installation

Puis allez dans « Services », « haproxy » et enfin « Backend »:

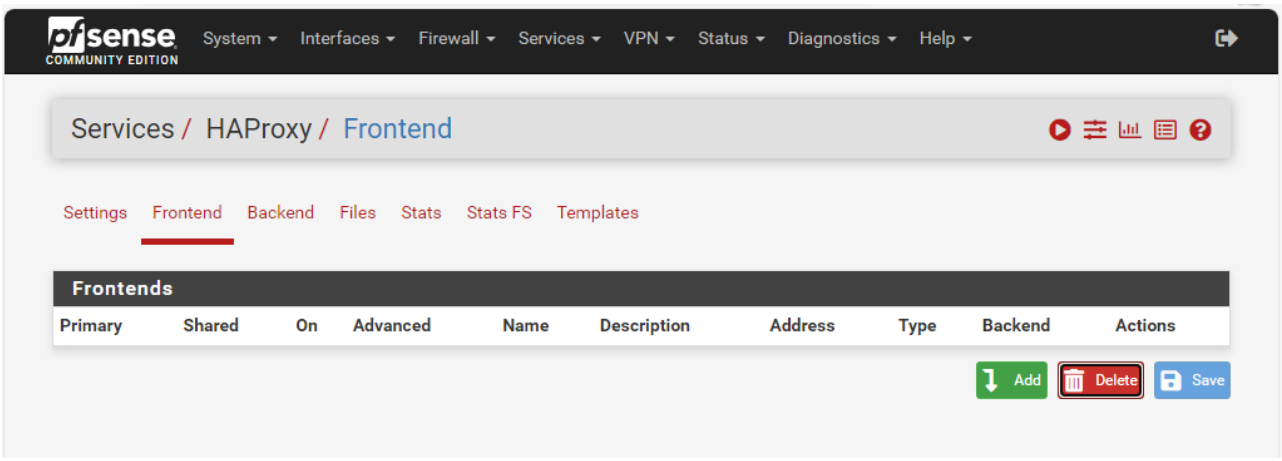


Puis dans « Backend», appuyer sur « add » pour rajouter un serveur web géré par le proxy, remplissez le alors avec les paramètres suivants :

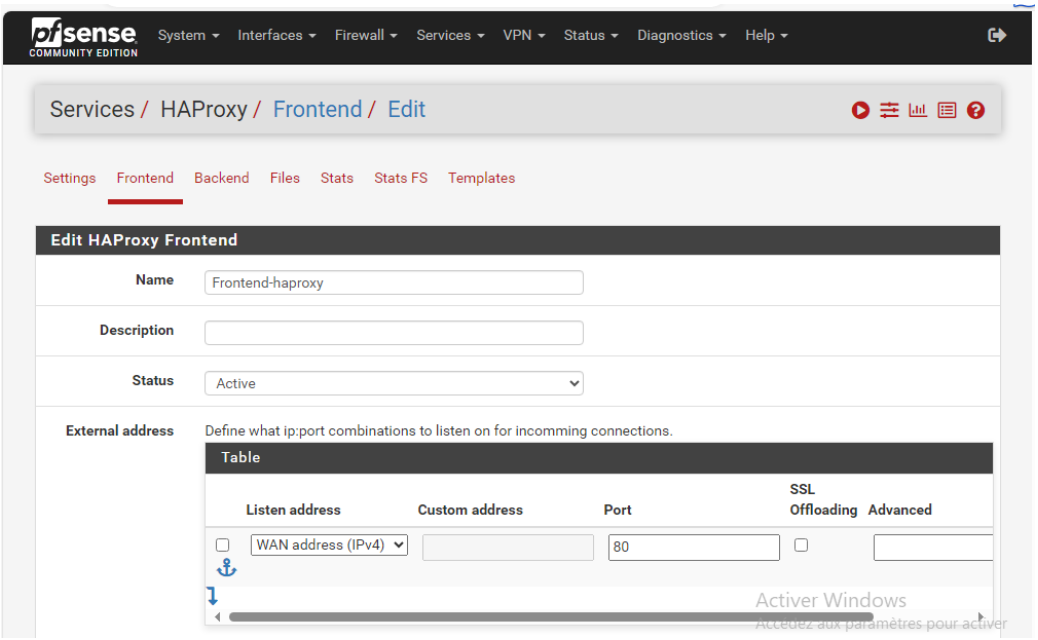


Bien évidemment, remplissez « Address » par celle de votre machine Web. Puis sauvegarder en bas de la page. Appliquer les modifications.

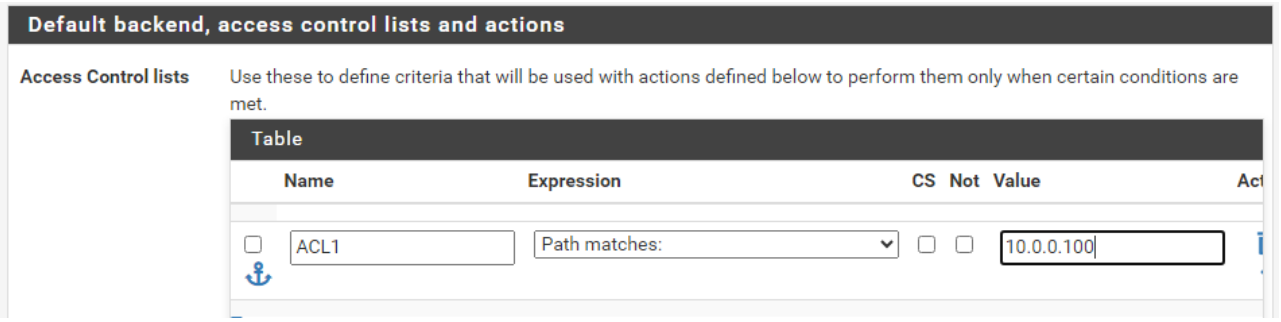
Ensuite, allez dans « Frontend » :



Appuyer sur « Add » pour rajouter une règle :

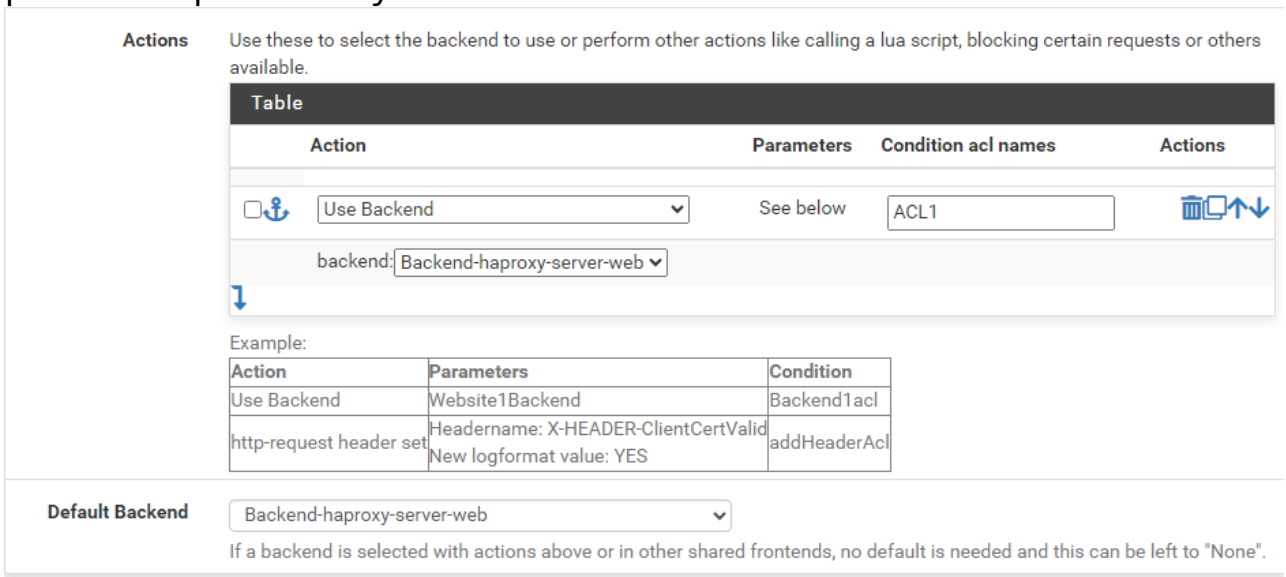


Dans « default backend », nous allons rajouter une règle pour définir qui pourra utiliser le haproxy pour se connecter au serveur WEB :



« Value » doit correspondre à votre adresse de serveur Web dans le cas de « Path matches ».

Puis encore une autre règle dans « Actions » tout en définissant le Backend par default pour renvoyer vers le serveur Web :



Vous avez terminé la configuration de Haproxy. Sauvegarder puis appliquer les changements.

Il faut néanmoins encore créer une règle pour le pare-feu pour autoriser le passage des utilisateurs extérieurs sur le serveur WEB, pour cela, dirigez-vous vers « Firewall » « Rules ».

Créé ensuite une règle avec les paramètres suivants :

```
Action = Pass
Interface = WAN
Address Family = IPv4
Protocol = TCP
Source = any
Destination = single host 10.0.0.100 (L'adresse de votre machine WEB)
Destination Port Range = 80 to 80 (Nous n'avons que le HTTP dans cette configuration)
```

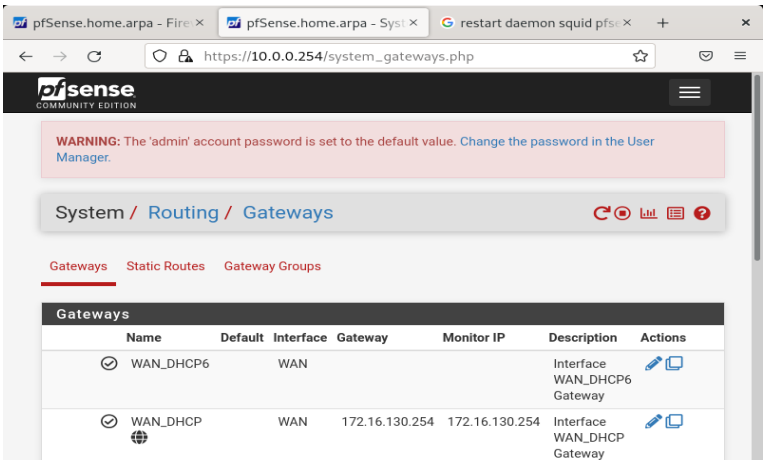
Vous pouvez sauvegarder et essayer de, vous connectez à votre serveur WEB depuis l'extérieur (Attention, il faut que votre machine extérieure ait en passerelle l'adresse WAN du pfsense 1), cependant, nous n'avons pas encore installé le service permettant d'avoir une page web sur la machine en question.

3.4.1.2 – Routage statique du web à la BDD

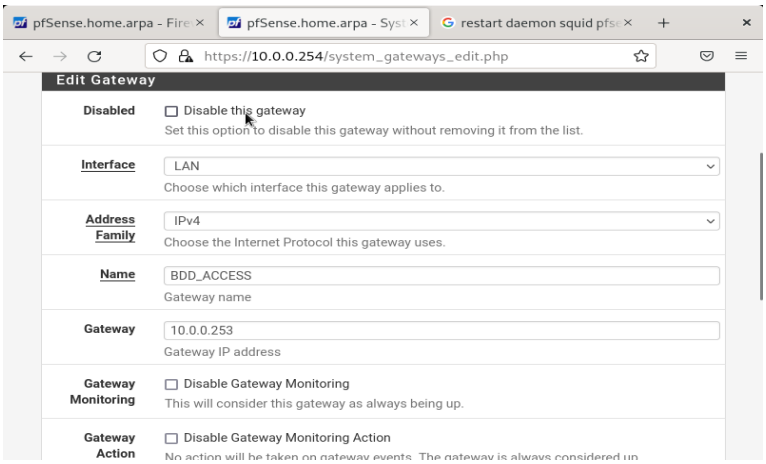
Pour rappel, le serveur web doit pouvoir accéder à notre BDD sans que les utilisateurs externes au Pfsense1 puissent y accéder (la BDD).

Il faut donc mettre une route statique pour rediriger les requêtes à direction de la BDD.

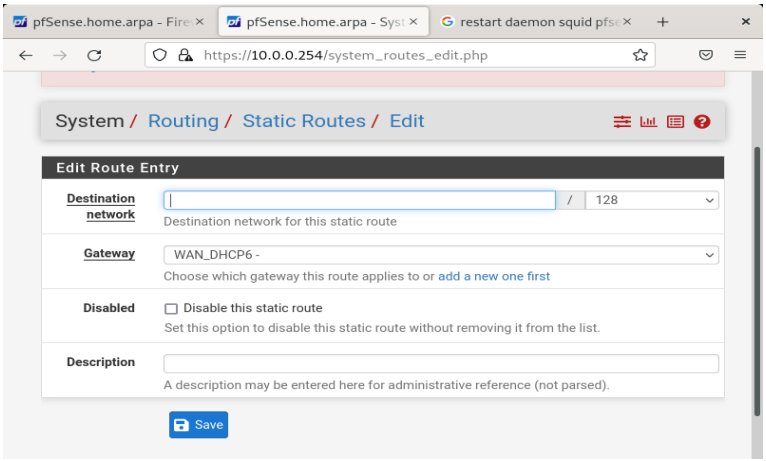
Pour cela, dirigez-vous vers « System », « Routing » et « Gateways »



Descendez pour accéder au bouton « Add » puis créé la passerelle suivante puis sauvegarder



Après cela, allez dans « Static Routes » afin de créé la route statique expliquer précédemment, en appuyant sur « Add »



Nos paramètres de route sont donc :

```
Destination Network = 192.168.20.0 /24
Gateway = BDD_ACCESS
```

Votre pfsense1 est donc terminé en termes de configurations, mis à part si vous désirez y rajouter encore des paramètres, libre à vous.

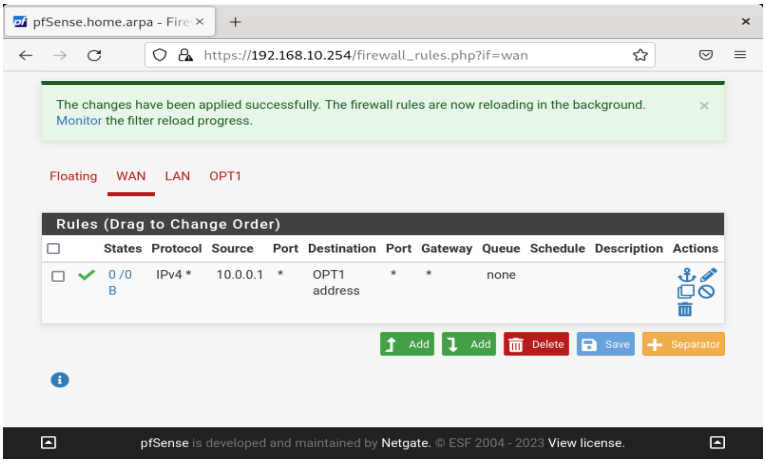
3.4.2 – Configuration poussée du Pfsense 2

Par défaut, la passerelle du Pfsense 2 gérant le LAN où se trouvera notre BDD n'a aucune règle permettant le passage de paquets nécessaires. Hors, les utilisateurs de notre infrastructure et le serveur Web doivent pouvoir y accéder, nous allons donc rajouter une règle.

Allez ensuite dans les règles du WAN puis rajouter une règle avec les paramètres suivants pour que le serveur Web puisse accéder à votre BDD suite au routage précédent :

```
Action = Pass
Interface = WAN
Address Family = IPv4
Source = Single host or alias , <Adresse de votre serveur Web>
Destination = OPT1 address
```

Sauvegarder et appliquer les nouveaux changements.



3.5 – Installer les services sur les serveurs

Au total, nous avons donc dans notre infrastructure, un serveur web et un serveur mariadb.

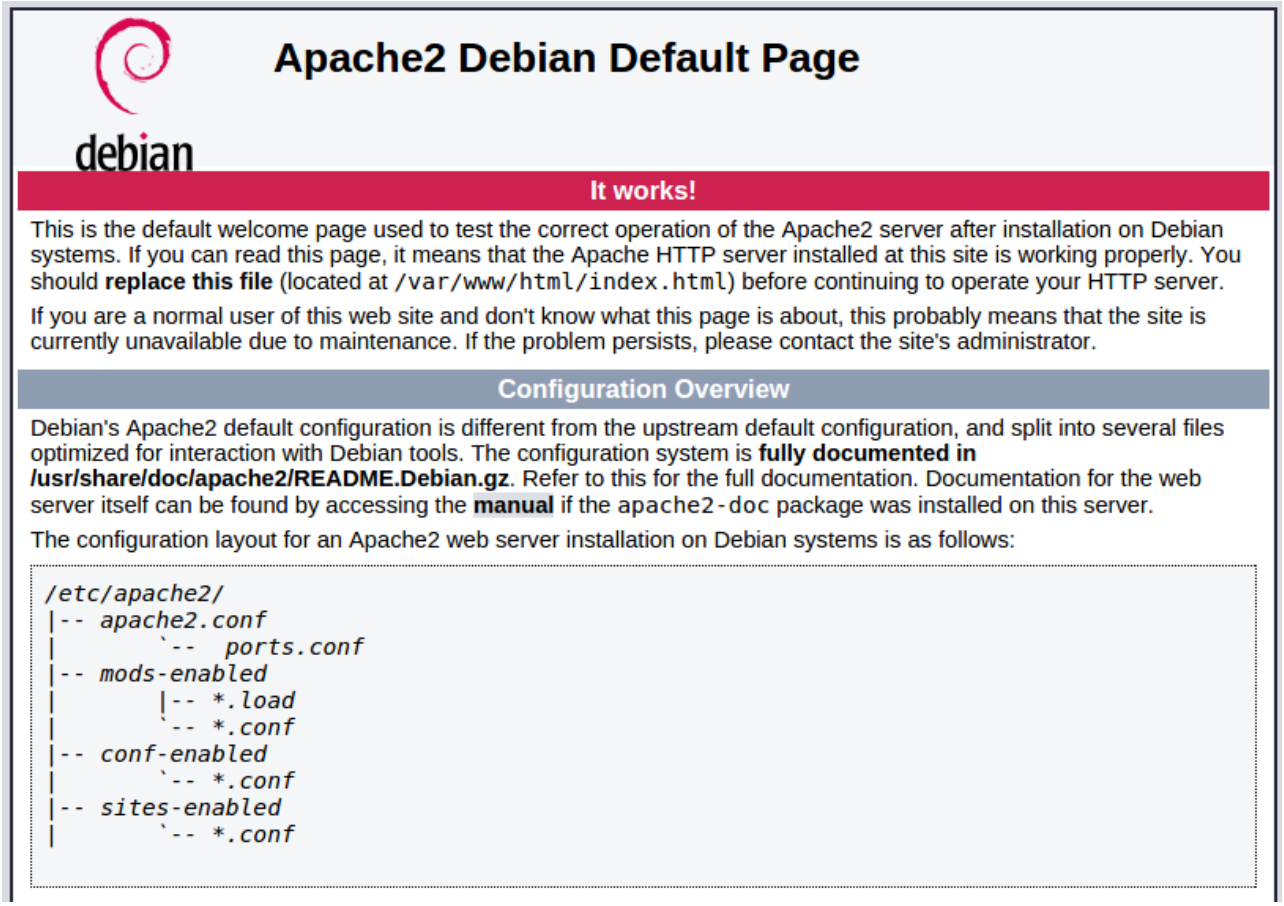
Je considère dans ce tuto que vous avez déjà des machines Linux prêtes à recevoir les différents services.

3.5.1 – Installation du serveur WEB

Sur votre machine de serveur Web, positionnez-vous dans le terminal puis faites la commande suivante

```
sudo apt install apache2
```

Si votre machine est correctement connectée à Internet l'installation devrait se lancer, une fois terminer, rentrez l'adresse IP de la machine dans son navigateur, vous permettant d'accéder à cette page.



L'installation de votre serveur Web est terminé

Lorsque vous essaierez de vous connecter à cette machine pour sa page, n'oubliez pas de changer la passerelle de la machine extérieure à l'adresse de WAN du pfsense 1.

3.5.2 – Installation de la BDD

Sur votre machine BDD, allez sur votre terminal et rentrez la commande suivante :

```
Sudo apt install mariadb-server
```

L'installation devrait se lancer puis se terminer, pour vérifier la bonne installation, lancez la commande suivante

```
mysql_secure_installation
```

Si votre machine vous renvoie un message comme quoi, elle n'existe pas, l'installation est ratée, dans le cas contraire, vous avez terminé. (Nous n'allons pas chercher à configurer mariadb dans ce tuto, juste à s'assurer de sa bonne installation).

4 – Résolution de potentiels problèmes

Il se peut que lors de l'installation de l'infrastructure, différents problèmes peuvent survenir, voici donc une liste des premières choses à vérifier dans ces cas-là.

4.1 – Problème de communications entre machines

1, Essayer de ping la machine en question par son adresse IP (si c'est le serveur WEB, essayez de, vous y connectez par son adresse IP sur le navigateur)

2, Vérifier que le pfsense que vous essayez de contacter est bien allumé

3, Vérifier que les machines sont sur les bons réseaux internes (En cas de VM)

4, Vérifier les interfaces des machines (Est-ce qu'elles ont les bonnes adresses de passerelle à leurs pfsenses respectifs ?)

5, Vérifier les règles de pare-feu, il se peut que vos règles ne concernent soit pas les bons protocoles ou les bons réseaux, aussi, s'il n'y a aucune règle de passage, toutes les requêtes sont arrêtées

6, Vérifier s'il n'y a pas un conflit d'interfaces sur le Pfsense connecté de manière direct à votre machine

4.2 – Problème d'Internet sur les clients

1, Vérifier les problèmes évoqués précédemment

2, Mettez en DNS l'adresse 8.8.8.8

4.3 – Problème de connexion à la page web des Pfsenses

1, Vérifier les problèmes évoqués précédemment

2, Redémarrer le configurateur web avec l'option 11 sur le pfsense en question

3, Réinitialiser le mot de passe du configurateur web (remets le mot de passe à « Pfsense »

4.4 – Aucune des vérifications n’apportent de résultat

1, Refaites les règles des pfsenses, les règles initiales des LAN de pfsense ont parfois tendance à ne pas fonctionner correctement pour aucune raison apparente.

2, Changez vos noms de réseaux internes, les noms en majuscule ont l’air de ne pas fonctionner correctement parfois.

3, Réinstaller la machine défectueuse.

5 - Annexes

Fiche de recette

Vérification de l'opérationnalité de la solution mise en œuvre : *Titre*

Description du test :

1. *Test d'accès du client au serveur base de données*
2. *Test d'accès du client au serveur Web*
3. *Test d'Accès du client à internet*
4. *Test d'accès du serveur Web au serveur base de données*
5. *Test d'accès du serveur Web à internet*
6. *Test de communication du serveur Web avec le client*
7. *Test d'accès du serveur base de données vers internet*
8. *Test d'accès du serveur base de données vers au client*
9. *Test de fonctionnement du reverse proxy*

Résultats Attendus :

1. *Le client peut accéder au serveur base de données*
2. *Le client peut accéder au serveur Web*
3. *Le client peut accéder à internet*
4. *Le serveur Web peut accéder au serveur base de données*
5. *Le serveur Web peut accéder à internet*
6. *Le serveur Web ne peut pas communiquer vers le client*
7. *Le serveur base de données ne peut pas accèder à internet*
8. *Le serveur base de données ne peut pas accèder au client*
9. *Le reverse proxy renvoie sur le serveur Web*

Réception Globale : DMZ **Date: 11/04/2023 Auteurs: Timothée Lignière, Paul-Alexis Kappala, Masseï Liam**

Reçu : ☐

Reçu avec réserve : ☐ ……

Refusé : ☐……

Commentaire :

Recette étape par étape * ******* *(pour chaque étape, vous devez élaborer dans un fichier distinct un scénario détaillé à faire appliquer au « client » venant valider votre solution)*

Réception Etape 1: Accès par MySQLsh du client vers le serveur base de données

Reçu : ☐

Reçu avec réserve : ☐……

Refusé : ☐……

Commentaire :

Réception Etape 2 : *Le client peut ouvrir la page Web du serveur Web en y accédant par explorateur web en 10.0.0.100*

Reçu : ☐

Reçu avec réserve : …☐……

Refusé : …☐……

Commentaire :

Réception Etape 3 : *Ouverture de plusieurs page Web par le client*

Reçu : ☐

Reçu avec réserve : ☐ .....

Refusé : ☐ .....

Commentaire :

Réception Etape 4 : Accès via MySQLsh *du serveur Web vers le serveur base de données*

Reçu : ☐

Reçu avec réserve : ☐ .....

Refusé : ☐ .....

Commentaire :

Réception Etape 5 : *Ping vers 8.8.8.8 depuis le serveur Web*

Reçu : ☐

Reçu avec réserve : ☐ .....

Refusé : ☐ .....

Commentaire :

Réception Etape 6 : *Ping du serveur Web vers le Client*

Reçu : ☐

Reçu avec réserve : ☐ .....

Refusé : ☐ .....

Commentaire :

Réception Etape 7 : Ping vers 8.8.8.8 depuis le serveur base de données

Reçu : ☐

Reçu avec réserve : ☐ .....

Refusé : ☐ .....

Commentaire :

Réception Etape 8 : *Ping vers le client depuis le serveur base de données*

Reçu : ☐

Reçu avec réserve : ☐ .....

Refusé : ☐ .....

Commentaire :

Réception Etape 9 : Connexion par IP avec un explorateur depuis une machine exterieur
Reçu : ☐ Reçu avec réserve : ☐…… Refusé : ☐…… Commentaire :