TUTOS-INFO
L'informatique par l'exemple

TUTORIEL

pfsense®
Routeur et pare-feu open source (version 2.7)

MODULE 5

METTRE EN PLACE UNE DMZ AVEC pfSENSE 2.7

SOMMAIRE

EXPERT
DIFFICULTE

1 – QU'EST-CE QU'UNE « DMZ » ?

DMZ signifie « **D**e**M**ilitarized **Z**one » ou « **Z**one **D**é**M**ilitarisée ».

1. **Pourquoi parle-t-on de « zone démilitarisée » ?**

L'expression « Zone démilitarisée » prend sa source avec la Corée. La **zone coréenne démilitarisée**, également désignée par le sigle « DMZ », est une étroite bande de terre servant de zone tampon entre la Corée du Nord et la Corée du Sud, créée le 27 juillet 1953 lors de la signature de l'armistice de P'anmunjŏm.

D'une longueur de 248 km pour environ 4 km de large située de part et d'autre de la frontière entre les deux pays, elle coupe la péninsule suivant approximativement le 38ème parallèle qui formait la ligne de démarcation intercoréenne avant le conflit. La superficie de la zone Coréenne est d'environ 1 000 kilomètres carrés, et est vide d'habitants. La zone est considérée comme un sanctuaire pour la préservation d'espèces naturelles.

2. **Qu'apporte la « zone démilitarisée » dans un réseau informatique ?**

La DMZ est une **zone isolée et séparée du reste du réseau**. Son principal objectif est de **protéger les données et les systèmes internes** d'une entreprise contre les attaques venant de l'extérieur. En effet, les réseaux internes contiennent souvent des données sensibles et confidentielles que les entreprises souhaitent protéger contre les pirates informatiques et autres menaces potentielles.

Le fonctionnement d'une DMZ repose sur une série de **règles de sécurité définies par l'entreprise**. Ces règles permettent de **contrôler le trafic entre le réseau interne, la DMZ et le réseau externe**, garantissant ainsi une **protection optimale des données et des systèmes internes**.

La mise en place d'une DMZ présente plusieurs avantages pour les entreprises et les utilisateurs :

- **Sécurité renforcée :** en isolant les services accessibles depuis l'extérieur dans une zone séparée et protégée, la DMZ contribue à réduire les risques d'attaques et de pénétrations malveillantes.

- **Contrôle accru :** grâce aux règles de sécurité définies par l'entreprise, il est possible de contrôler étroitement le trafic et les communications entre les différents réseaux et d'empêcher tout accès non autorisé aux données sensibles.

- **Flexibilité :** la DMZ offre une certaine souplesse dans la configuration des services et des systèmes accessibles depuis l'extérieur, facilitant ainsi leur gestion et leur maintenance.

- **Performances :** en séparant les services accessibles depuis l'extérieur des ressources internes de l'entreprise, la DMZ permet d'éviter la saturation du réseau et d'améliorer les performances globales du système.

3. **Quels services peut-on héberger dans une DMZ ?**

Voici quelques exemples de services et de systèmes qui peuvent être hébergés dans une DMZ :

- **Serveurs web :** ces serveurs sont utilisés pour héberger les sites internet accessibles par les utilisateurs externes à l'entreprise.

- **Serveurs de messagerie :** ils permettent aux employés de l'entreprise de communiquer avec des personnes extérieures via des mails sécurisés.

- **Serveurs FTP :** ces serveurs offrent un moyen sécurisé d'accéder à des fichiers et des documents depuis l'extérieur de l'entreprise.

- **Serveurs VPN :** ils permettent aux employés en télétravail ou en déplacement de se connecter au réseau interne de l'entreprise via une connexion sécurisée.

4. **<u>Quelles sont les principales étapes de la mise en place d'une DMZ dans un réseau informatique</u> ?**

Pour créer une DMZ, il est nécessaire de suivre plusieurs étapes :

1. **Définir les objectifs :** avant de commencer, il est crucial de déterminer quels services et systèmes seront hébergés dans la DMZ et quel niveau de protection est souhaité.

2. **Configurer un routeur avec un pare-feu :** il est essentiel de configurer correctement les règles de sécurité sur les pare-feu internes et externes pour garantir une protection optimale.

3. **Isoler la DMZ :** la zone démilitarisée doit être isolée du reste du réseau pour éviter tout risque de contamination en cas d'attaque.

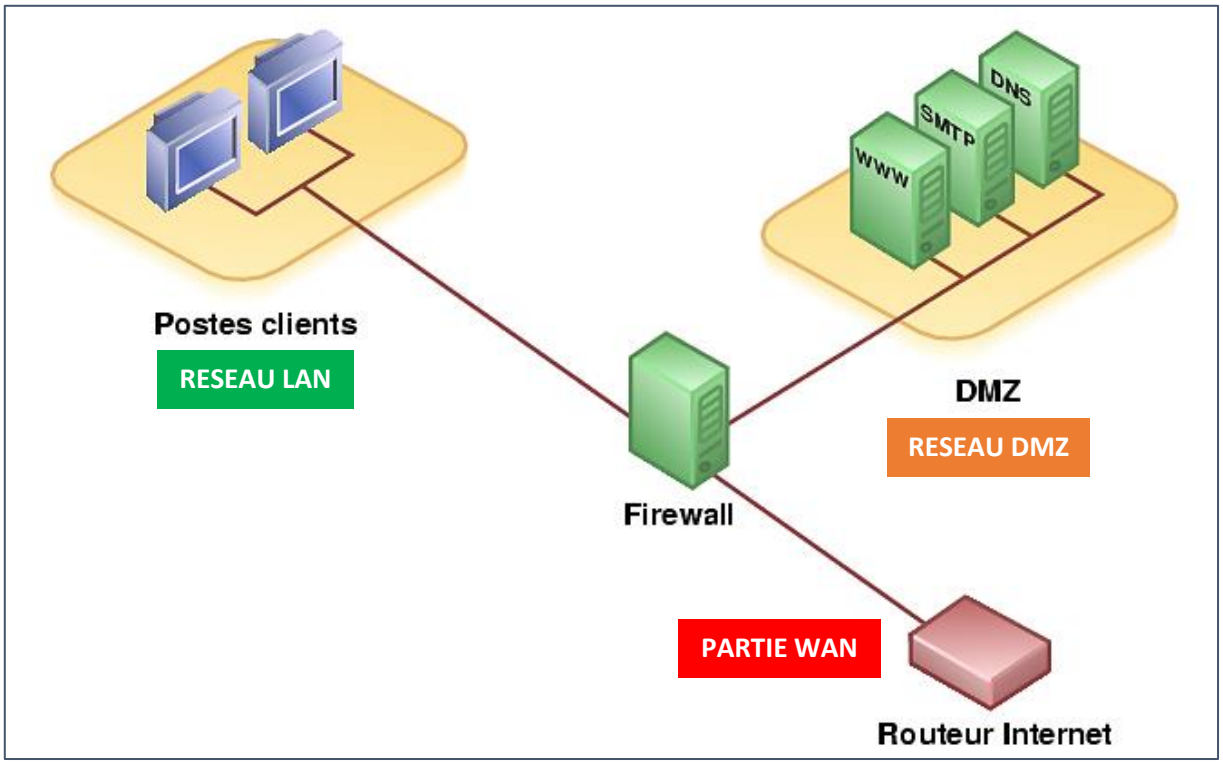
4. **Implémenter les services :** une fois la DMZ configurée, il est temps d'installer les services et les systèmes souhaités.

5. **Maintenir et surveiller :** enfin, il est important de surveiller régulièrement l'état de la DMZ et d'effectuer des mises à jour de sécurité pour assurer sa pérennité.

2 – CONFIGURATION D'UNE DMZ AVEC pfSENSE 2.7

La figure ci-dessous représente une architecture DMZ avec un pare-feu à trois interfaces. L'inconvénient est que si cet unique pare-feu est compromis, plus rien n'est contrôlé.

Il est cependant possible d'utiliser deux pares-feux en cascade (ou deux pares-feux redondants) afin d'éliminer ce risque. Il existe aussi des architectures de DMZ où celle-ci est située entre le réseau Internet et le réseau local, séparée de chacun de ces réseaux par un pare-feu.



Ce tutoriel est basé sur la mise en place d'une DMZ **avec un routeur/pare-feu** (pfSENSE).

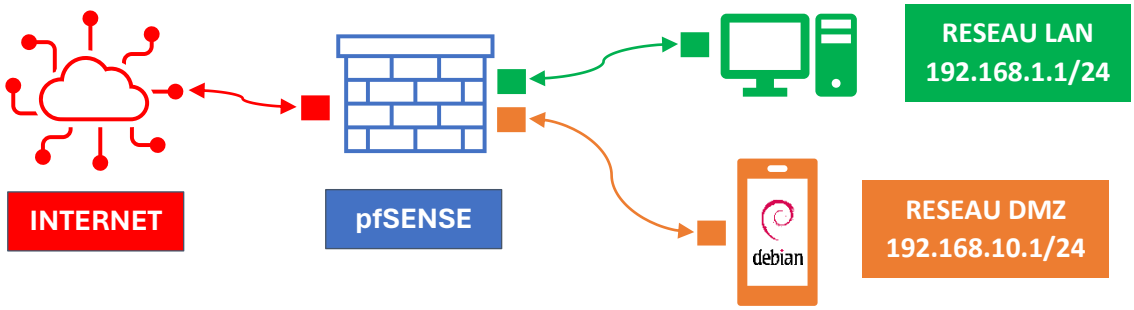
Un point de défaillance unique (**single point of failure ou SPOF** en anglais) est un point d'un système informatique dont le reste du système est dépendant et dont une panne entraîne l'arrêt complet du système. Le point de défaillance unique a comme principale caractéristique de ne pas être protégé (redondant).

Nous étudierons, dans un autre tutoriel la redondance de routeurs pfSENSE afin de supprimer le point de défaillance (**voir tutoriel module 6**).

Prérequis avant d'exécuter ce tutoriel : pour réaliser ce tutoriel, **vous devez avoir réalisé les 3 premiers modules de ces tutoriels** pfSENSE. Votre pfSENSE doit disposer de 3 interfaces :

- 1 interface **WAN (IP publique fournie par notre hébergeur en /32)**
- 1 interface **LAN** (**192.168.1.1/24** dans notre cas ; à adapter selon votre architecture)
- 1 interface **DMZ** (**192.168.10.1/24** dans notre cas ; à adapter selon votre architecture)

L'architecture que nous cherchons à reproduire sera la suivante :

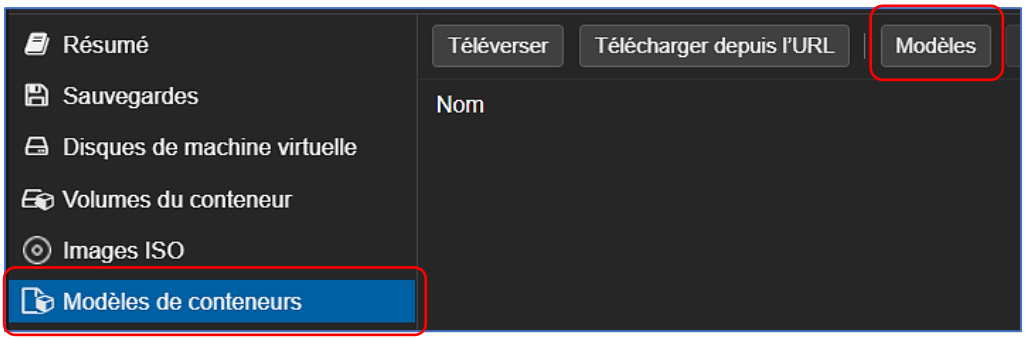


Dans ce tutoriel, **la DMZ hébergera un conteneur Debian** 12 (conteneur LXC Proxmox) dans lequel on installera un serveur web Apache 2.4

1ère étape : téléchargement d'un modèle de conteneur Debian 12 sur Proxmox

Avec Proxmox, nous allons créer un conteneur LXC Debian sur lequel nous installerons le serveur web Apache 2.4
On commence par télécharger le modèle de conteneur Debian ainsi :

- Connectez-vous à l'interface de gestion de votre Proxmox
- Cliquez sur « **local** » - « **Modèles de conteneurs** » et « **Modèles** »

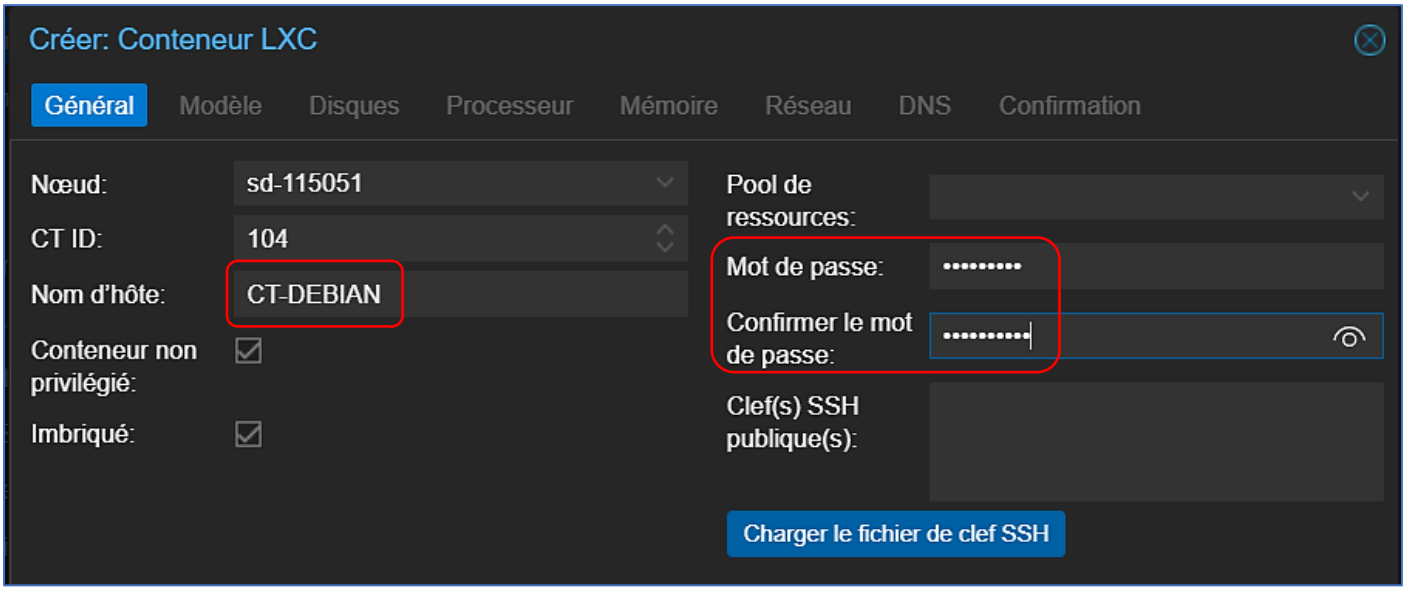


Dans la liste de modèles proposés, on sélectionne le conteneur LXC « **debian-12-standard** » :

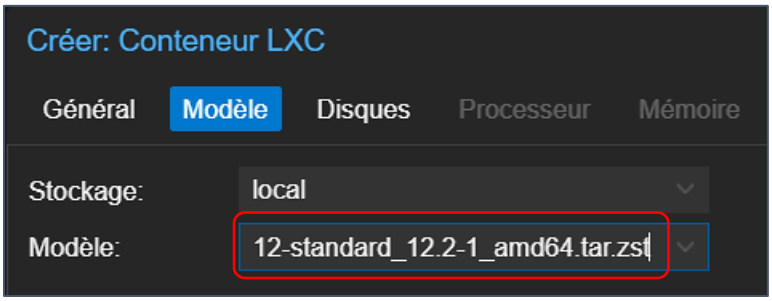
- Cliquez le bouton « **Télécharger** » pour que le modèle soit versé dans votre stockage « local ».

2ème étape : création du conteneur LXC Debian

- Depuis votre interface de gestion Proxmox, cliquez sur « **Créer un conteneur** » (en haut à droite de l'écran)
- Une fenêtre s'affiche ; complétez-la et cliquez le bouton « **Suivant** » :

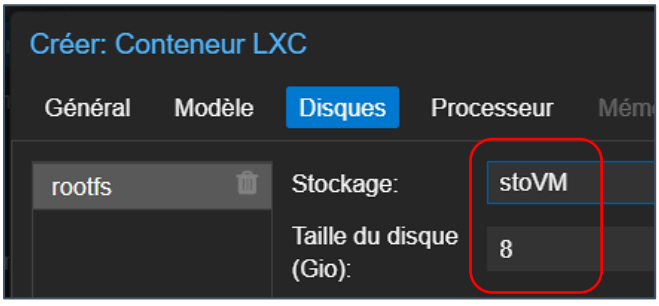


- Sélectionnez le modèle de conteneur précédemment téléchargé et cliquez le bouton « **Suivant** » :



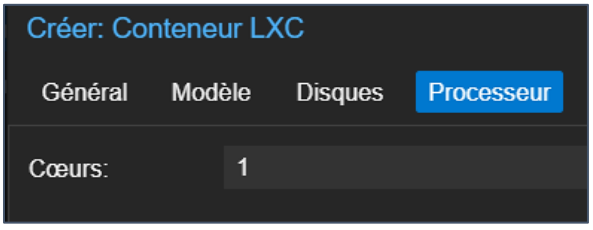
On choisit le modèle de conteneur précédemment téléchargé dans le stockage « local » de Proxmox.

- Indiquez l'emplacement de stockage de votre conteneur sur votre hyperviseur (nous avons laissé 8 Go de stockage par défaut et cliquez le bouton « **Suivant** » :



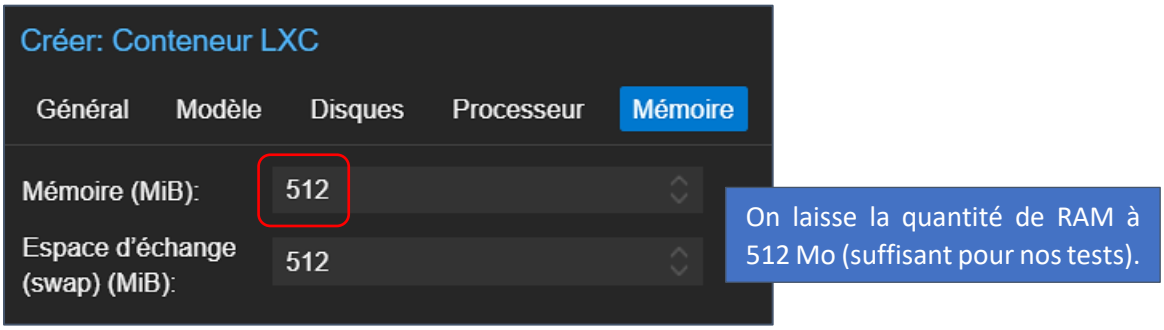
On indique, ici, l'emplacement de stockage du conteneur Debian (« stoVM » pour nous) et on laisse la taille du disque par défaut (8 Go).

- On laisse 1 cœur ici (suffisant) et on clique le bouton « **Suivant** » :



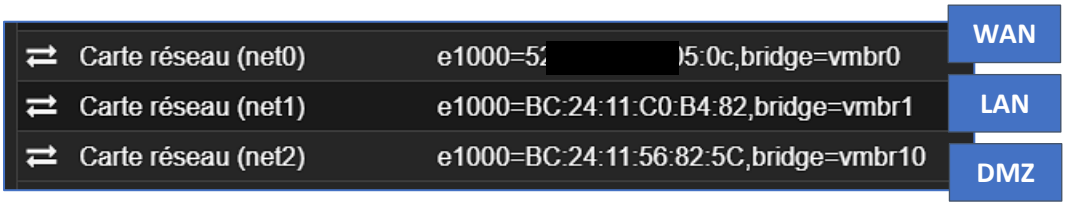
On laisse le paramètre à « 1 cœur » (suffisant pour nos tests).

- On laisse la taille de la RAM sur 512 Mo (suffisant pour ce conteneur) et on clique sur « **Suivant** » :



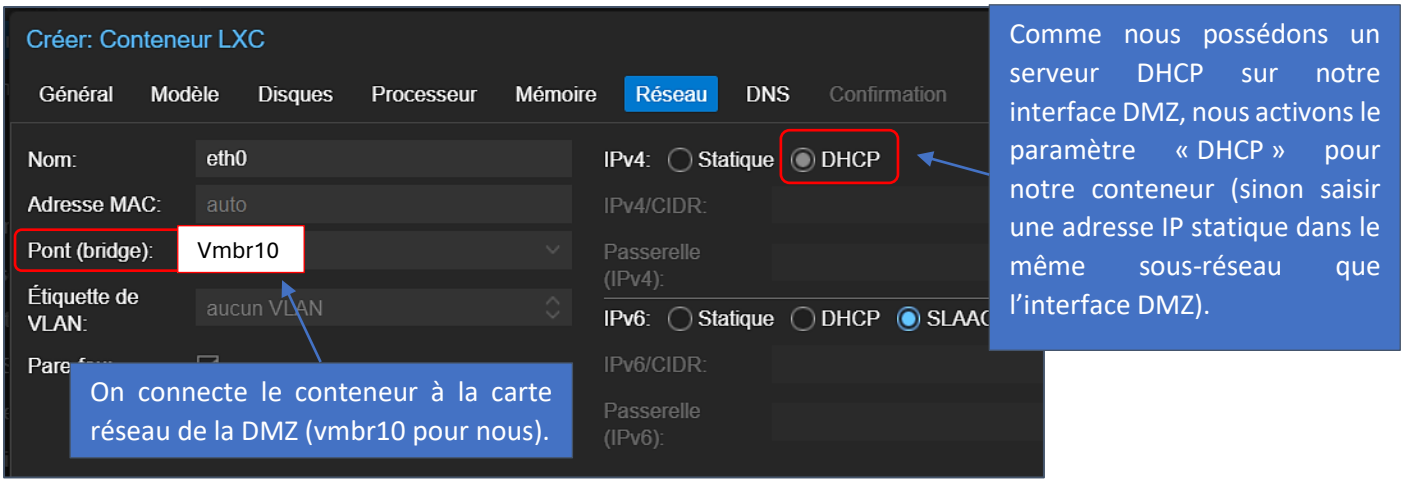
- **Attention, au niveau de la connexion réseau, on sélectionne bien le VMBR correspondant à la DMZ** du pfSENSE.

Rappel : notre routeur pfSENSE est actuellement configuré avec 3 cartes réseau :

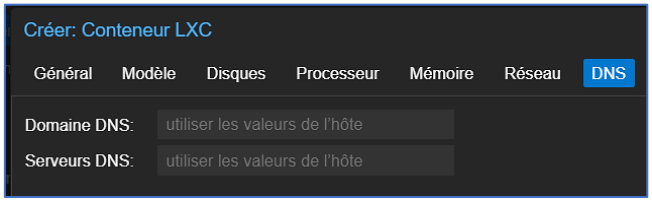


La carte « net0 » est connectée au « vmbr0 » c'est-à-dire la **WAN**
La carte « net1 » est connectée au « vmbr1 » ici, c'est-à-dire le **LAN**
La carte « net2 » est connectée au « vmbr10 » ici, c'est-à-dire la **DMZ**

Nous connectons donc notre conteneur au réseau DMZ soit le « **vmbr9** » pour nous. (à ajuster en fonction de votre propre configuration). En ce qui concerne le paramétrage des IPv4, on stipule ici « **DHCP** » car nous avons un serveur DHCP actif sur la DMZ (sinon il faut saisir une adresse IP valide pour la DMZ). On clique sur « **Suivant** » pour valider les paramètres :



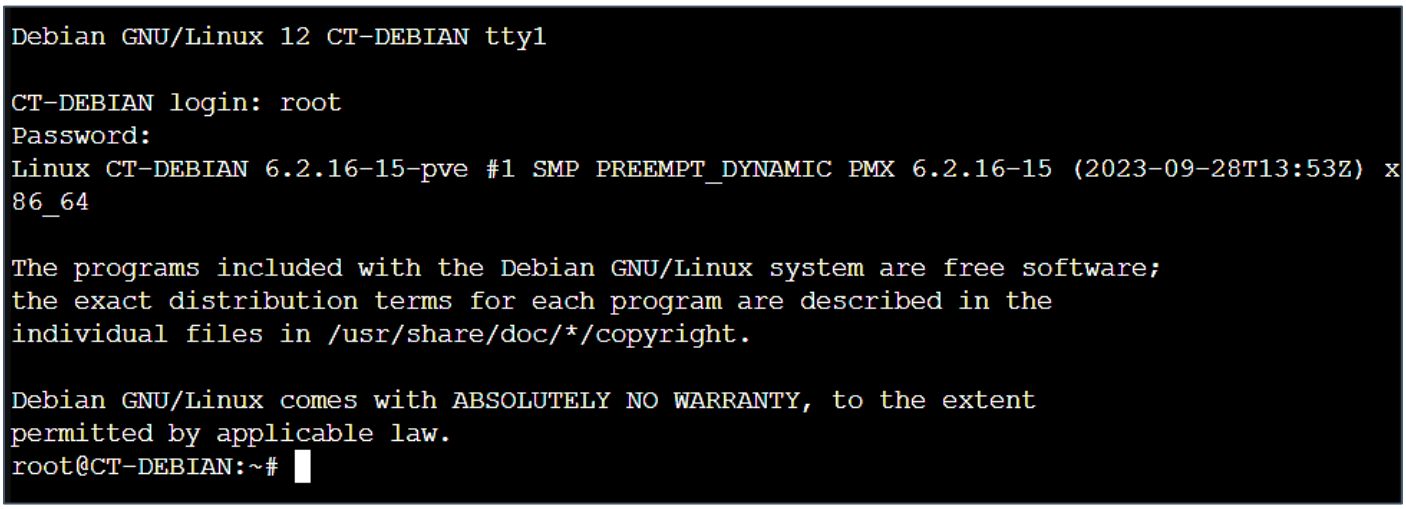
- Ici, on n'indique pas de serveurs DNS car ces derniers sont déjà renseignés dans pfSENSE ; il suffit de cliquer le bouton « **Suivant** » :



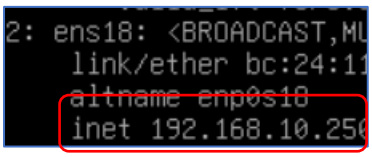
On confirme, dans la dernière étape, la création du conteneur qui ne prend que quelques secondes et le conteneur est généré et prêt à l'emploi.

- Lancez le conteneur en faisant un clic droit dessus et cliquez « **Démarrer** » :

L'accès au conteneur se fait en double-cliquant dessus pour ouvrir la console ; saisissez « **root** » et le mot de passe attribué lors de la création du conteneur :

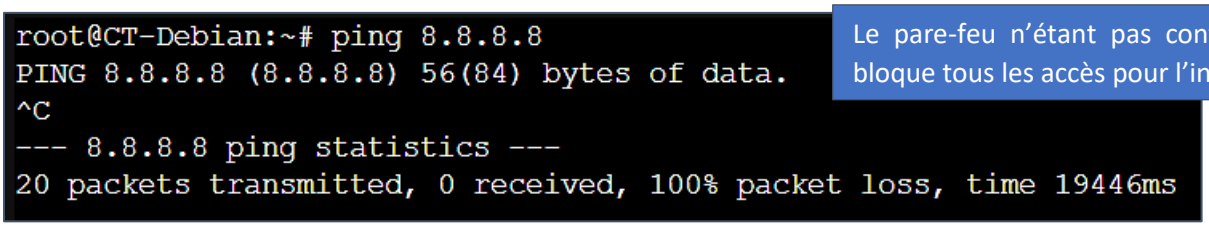


- Vérifiez que votre conteneur a bien obtenu une adresse IP de votre serveur DHCP (en saisissant la commande « **ip a** » et qu'il est bien dans le réseau de votre DMZ (en ce qui nous concerne, le conteneur a bien reçu un adressage IP de type **192.168.10**.xx/24 correspondant au réseau de la DMZ) :



Le serveur DHCP actif sur l'interface a bien attribué une adresse IP au conteneur Debian.

On peut constater que **ce conteneur ne possède pas d'accès à Internet ce qui est normal** puisqu'il est situé « derrière » le **pfSENSE qui bloque, par défaut, les accès entrants/sortants sur l'interface WAN et sur l'interface DMZ**. Si l'on tente les commandes « apt update » ou « ping 8.8.8.8 » on constatera qu'aucun accès à Internet n'est possible. **Il est donc nécessaire de créer des règles dans le pare-feu** de votre pfSENSE :



Le pare-feu n'étant pas configuré, pfSENSE bloque tous les accès pour l'instant !

3ème étape : réservation d'adresse dans le serveur DHCP de la DMZ

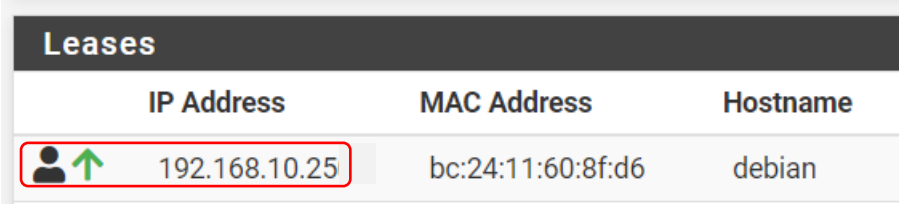
Maintenant que le conteneur Debian est prêt, connectez-vous à votre interface pfSENSE. Une fois connecté, effectuez les manipulations qui suivent.

En ce qui concerne le conteneur Debian, ce dernier servira de serveur web sur lequel on installera le paquet Apache 2.4. A ce stade, soit nous lui attribuons une adresse IP statique directement en console (modification du fichier /etc/network/interfaces), soit nous réservons l'adresse IP affectée par pfSENSE dans les baux DHCP.

Nous allons opter pour cette 2ème solution pour vous montrer le principe de la réservation d'adresses IP dans pfSENSE.

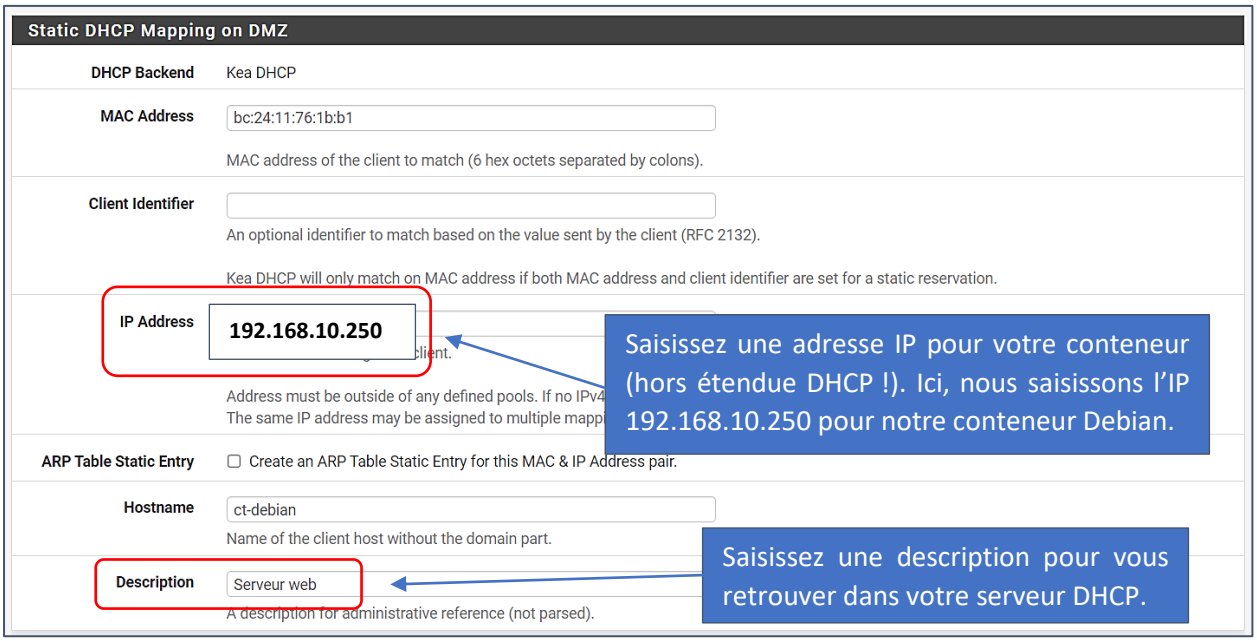
a) Réservation de l'adresse IP de notre conteneur Debian dans le serveur DHCP de pfSENSE

- Connectez-vous à l'interface de gestion de votre pfSENSE
- Cliquez le menu « **Status** » - « **DHCP Leases** » ; les machines ayant reçu des adresses IP sont affichées :

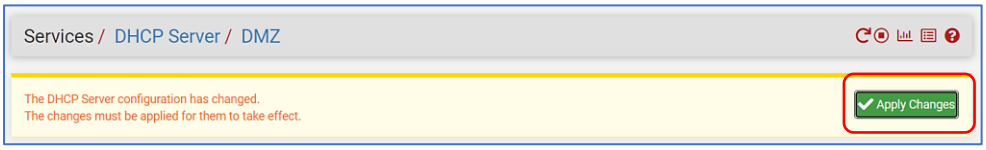


Pour réserver un bail, effectuez les manipulations suivantes :

- Cliquez le premier « **+** » **sur fond blanc** **à droite de la machine** « **CT-DEBIAN** » pour réserver l'IP ; une fenêtre s'affiche ; saisissez l'adresse IP que vous souhaitez réserver (**elle doit être en-dehors de l'étendue** !) et indiquez une description :

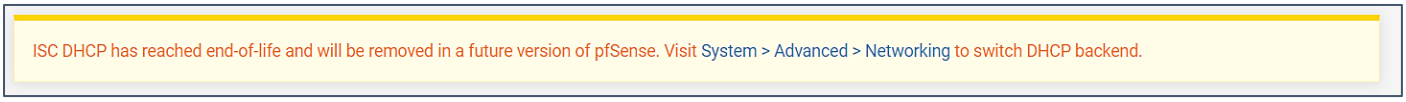


- Cliquez le bouton « **Save** » pour valider les paramètres
- Cliquez le bouton « **Apply changes** » pour valider vos paramètres :

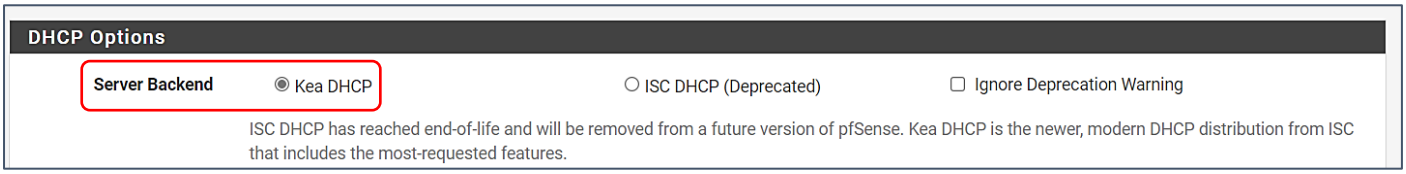


b) *Mettez à jour votre serveur DHCP si vous avez la version « ISC DHCP » (obsolète)*

Si votre serveur DHCP est basé sur la version « ISC DHCP », un message s'affiché dans le haut de la fenêtre et vous indique que la version « ISC DHCP » est obsolète. pfSENSE nous invite à basculer vers une version évoluée du serveur DHCP en cliquant sur le lien « **System > Advanced > Networking** » :



- Sélectionnez « **Kea DHCP** » et cliquez le bouton « **Save** » en bas de la fenêtre pour mettre à jour votre serveur DHCP vers cette version :



Le serveur DHCP de Kea est une conception entièrement nouvelle et remplace avantageusement ISC DHCP qui est implanté depuis une trentaine d'années.

- De nombreuses fonctionnalités facultatives sont implémentées sous forme de bibliothèques de hooks, et les applications DHCPv4, DHCPv6 et Dynamic DNS sont des packages distincts, de sorte que vous n'avez besoin que d'installer le logiciel que vous prévoyez d'utiliser.

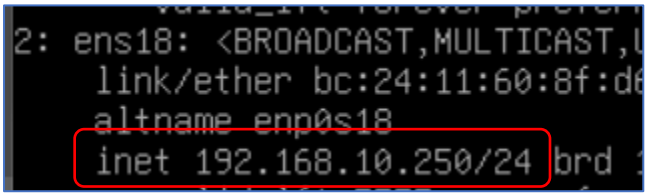
- Kea prend en charge l'intégration dans vos systèmes de gestion existants et la reconfiguration en ligne.

- Les composants qui sont fréquemment modifiés, tels que les réservations d'hôtes et les sous-réseaux, peuvent éventuellement être stockés dans une base de données commune prête à l'emploi, distincte du fichier de configuration principal de Kea, à l'aide de hooks premium.

- Kea prend en charge un mode de haute disponibilité plus simple à la place du basculement DHCP v4 implémenté par ISC DHCP. Le mode Kea HA fonctionne aussi bien pour DHCPv4 que DHCPv6.

- Kea est multithread et offre des performances supérieures celles de l'ISC DHCP sur les ordinateurs modernes.

Relancez votre conteneur en saisissant la commande « **reboot** » et vérifiez que l'adresse IP réservée dans les « Leases DHCP » est bien **192.168.10.250** a bien été appliquée à notre conteneur en saisissant la commande « **ip a** » :



4ème étape : gestion des règles de pare-feu

Maintenant que le conteneur qui recevra votre serveur web Apache possède une adresse IP réservée, on va s'intéresser aux **règles de gestion du pare-feu** à appliquer dans pfSENSE.

Commencez par **établir votre politique de sécurité**.

Par exemple, ici, pour garantir la sécurité de votre LAN, vous voulez :

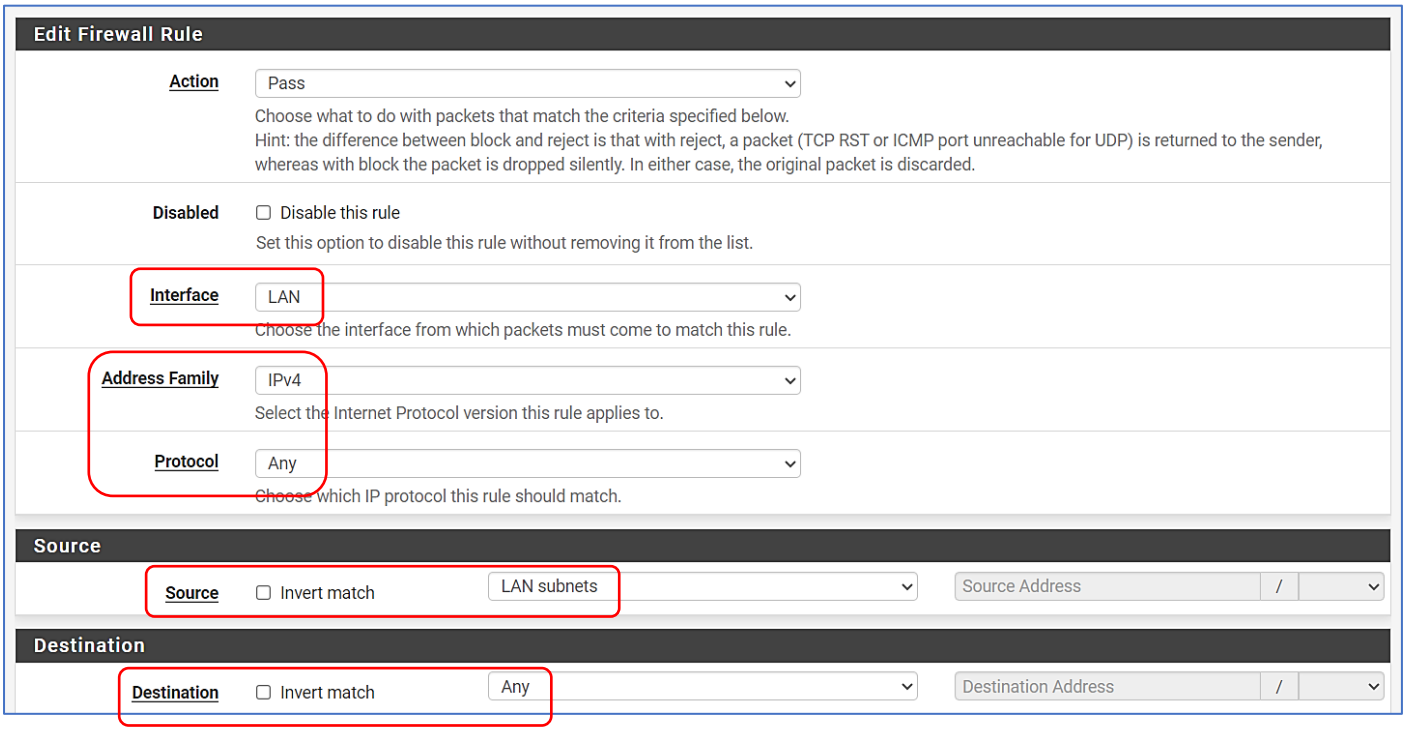
- 1 - que votre LAN puisse naviguer sur le web (en « sortant » via l'interface WAN)
- 2 - que le **réseau de la DMZ**, **n'ait aucun accès vers votre LAN** **mais que le flux entrant soit autorisé**.
- 3 - que votre LAN puisse accéder au serveur web de la DMZ.

Mise en place des règles dans le pare-feu pfSENSE :

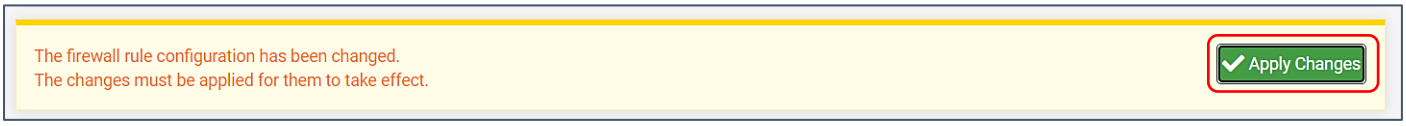
REGLE 1 – AUTORISER LE LAN A NAVIGUER SUR LE WEB VIA L'INTERFACE WAN

Il faut autoriser le trafic sortant du **LAN** vers l'interface **WAN** de la façon suivante :

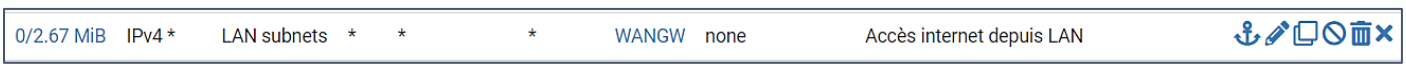
- Connectez-vous à l'interface de gestion de pfSENSE
- Cliquez sur « **Firewall** » - « **Rules** »
- Cliquez sur l'interface « **LAN** »
- Cliquez le bouton « **Add** » et configurez votre règle ainsi :



- Cliquez les boutons « **Save** » et « **Apply Changes** » pour que la règle s'applique :



La règle s'affiche :



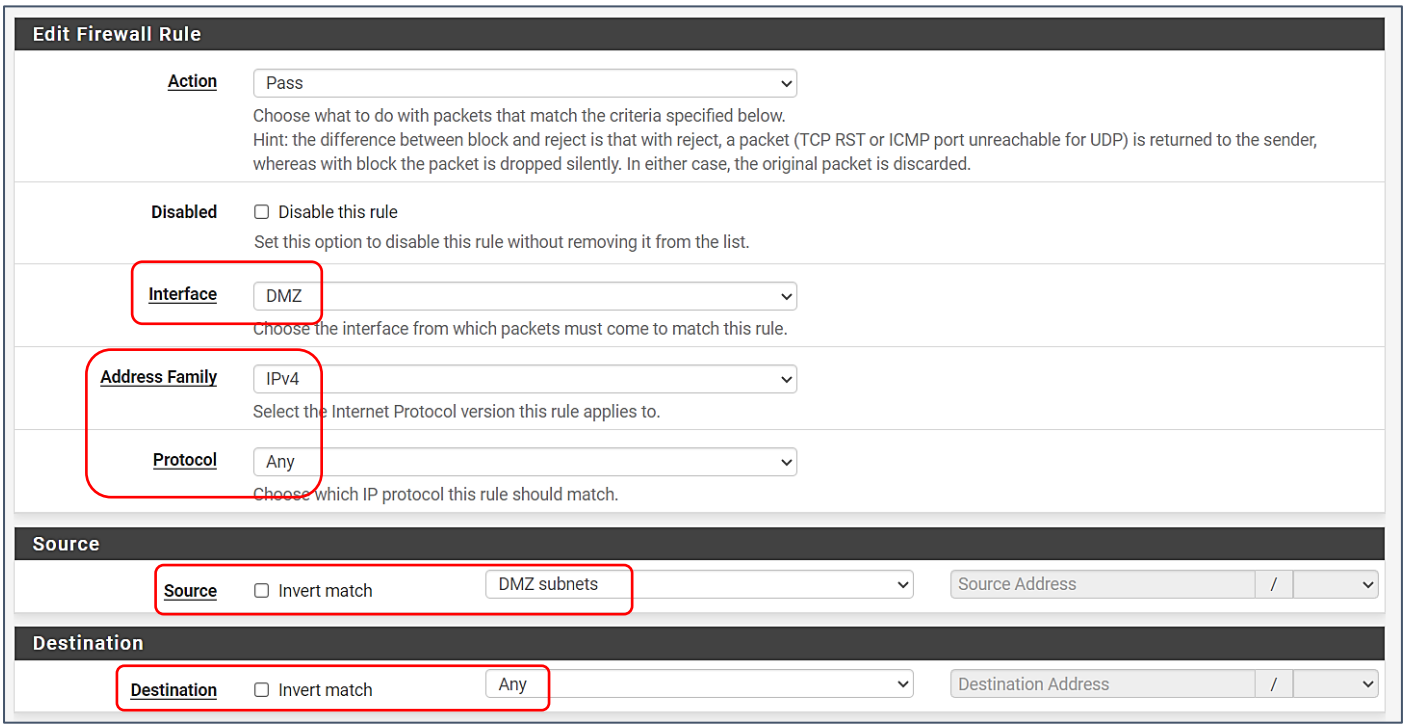
REGLE 2 – AUTORISER LES FLUX SORTANTS DANS LA DMZ

Notre conteneur Debian qui hébergera notre serveur web Apache ne possède pas de connexion au web par défaut.

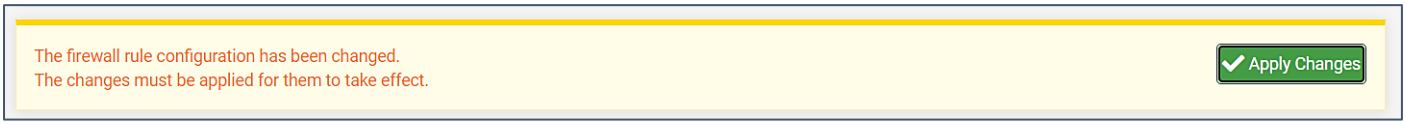
Nous allons, dans un 1er temps, créer une règle dans la DMZ pour autoriser le trafic sortant de la DMZ afin de pouvoir mettre à jour le conteneur et installer le serveur Apache.

Pour cela, effectuez les manipulations suivantes à partir de l'interface de gestion de pfSENSE :

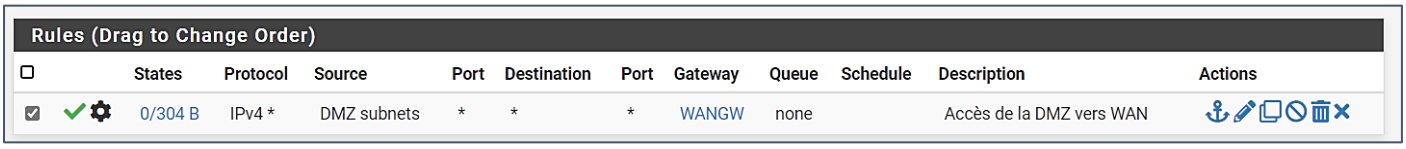
- Cliquez sur « **Firewall** » - « **Rules** »
- Cliquez sur l'interface « **DMZ** »
- Cliquez le bouton « **Add** » et configurez votre règle ainsi :



- Cliquez les boutons « **Save** » et « **Apply Changes** » pour valider et appliquer la règle :



La règle s'affiche :

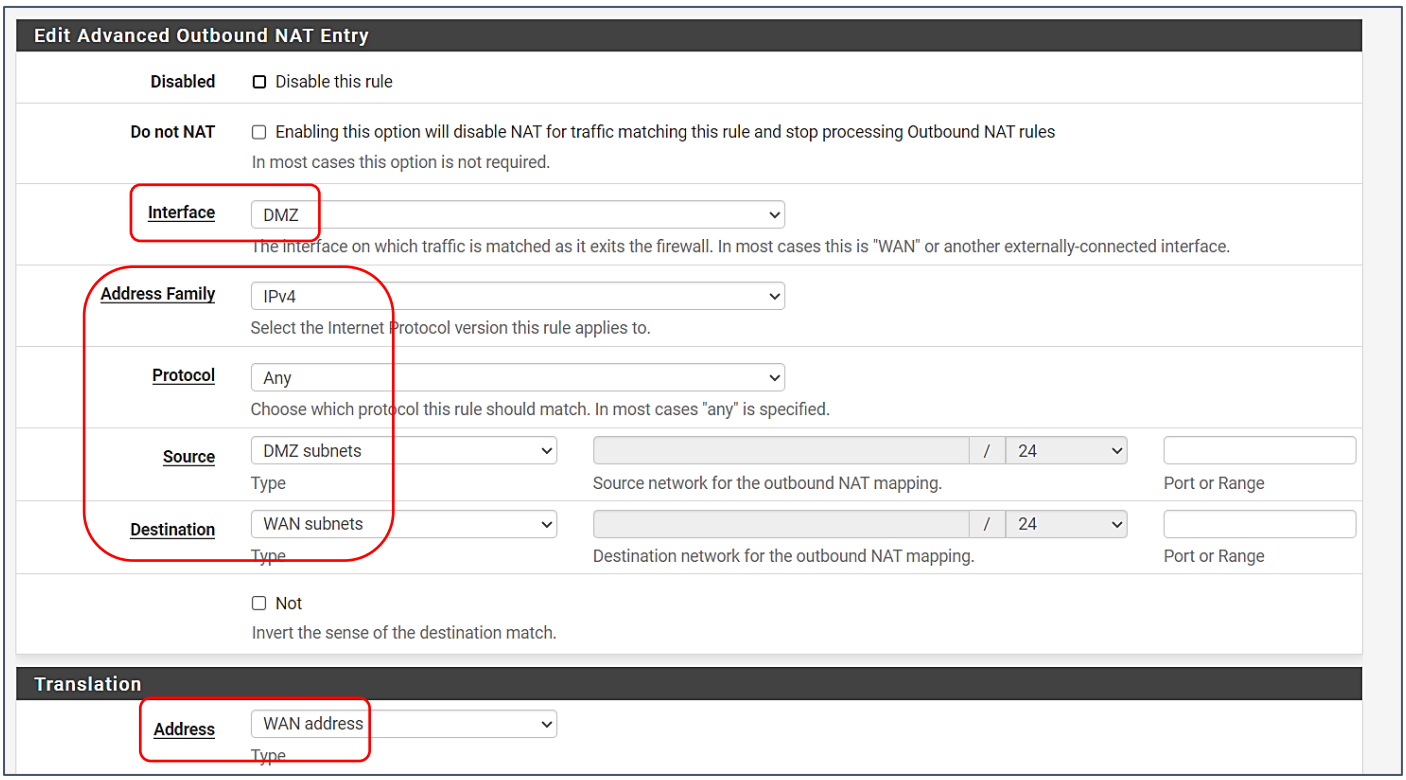


REGLE 3 – CONFIGURER LE NAT OUTBOUND POUR AUTORISER LA DMZ A UTILISER LA WAN

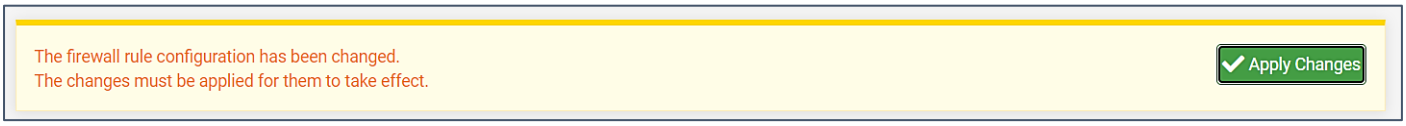
Cette règle permettra au réseau DMZ de « sortir » sur Internet via l'interface WAN.

Pour cela, effectuez les manipulations suivantes :

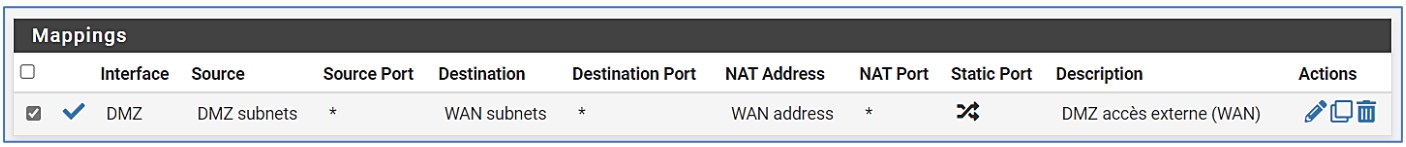
- Cliquez sur « **Firewall** » - « **NAT** »
- Cliquez sur « **Outbond** »
- Cliquez le bouton « **Add** » et configurez votre règle ainsi :



- Cliquez les boutons « **Save** » et « **Apply Changes** » pour valider la règle :



La règle s'affiche :

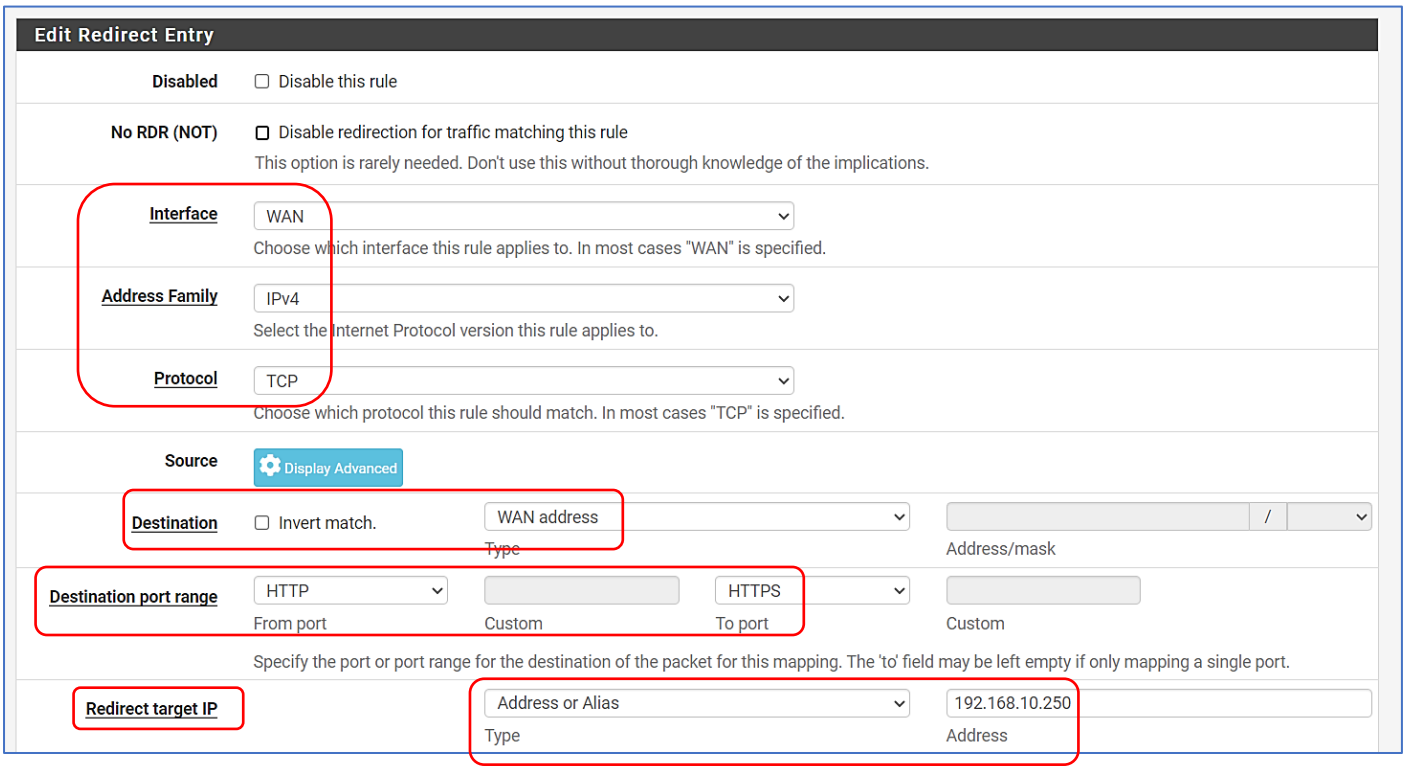


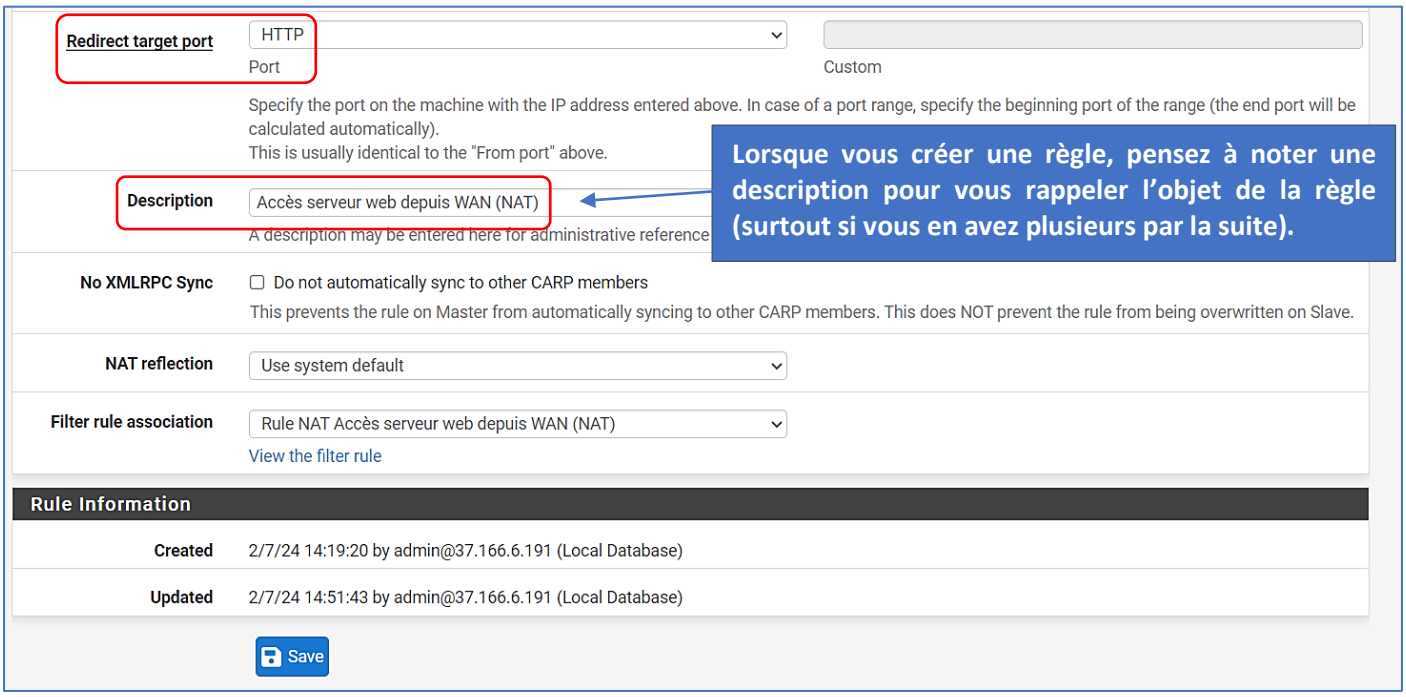
REGLE 4 – REDIRIGER LES FLUX ENTRANTS DEPUIS LA WAN VERS LE SERVEUR WEB

Ici, nous allons autoriser les flux entrants depuis l'interface WAN à être redirigés vers la DMZ et en direction de notre serveur web Apache uniquement.

Pour cela effectuez les manipulations suivantes :

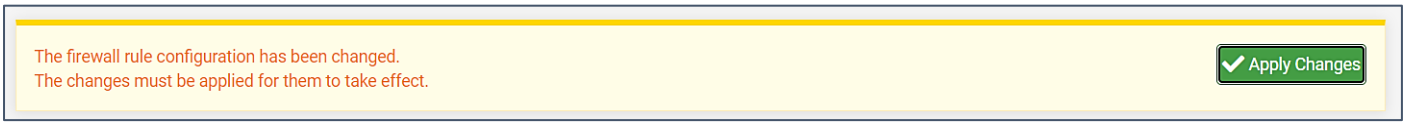
- Connectez-vous à l'interface de gestion de pfSENSE
- Cliquez sur « **Firewall** » - « **NAT** »
- Cliquez sur l'interface « **WAN** »
- Cliquez le bouton « **Add** » et configurez votre règle ainsi :



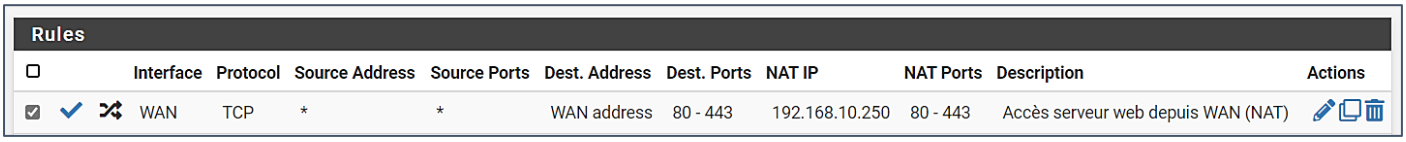


Lorsque vous créer une règle, pensez à noter une description pour vous rappeler l'objet de la règle (surtout si vous en avez plusieurs par la suite).

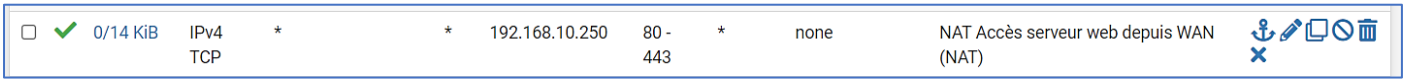
- Cliquez les boutons « **Save** » et « **Apply Changes** » pour valider et activer la règle :



La règle s'affiche :

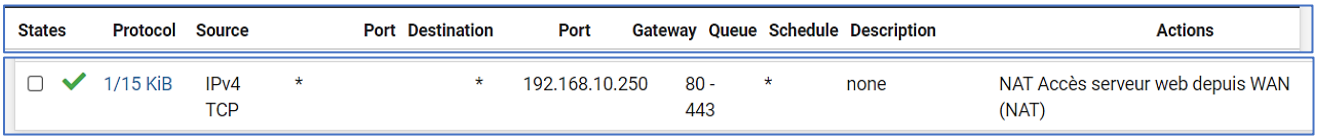


La règle s'affiche également dans la partie « Rules » du pare-feu ainsi :

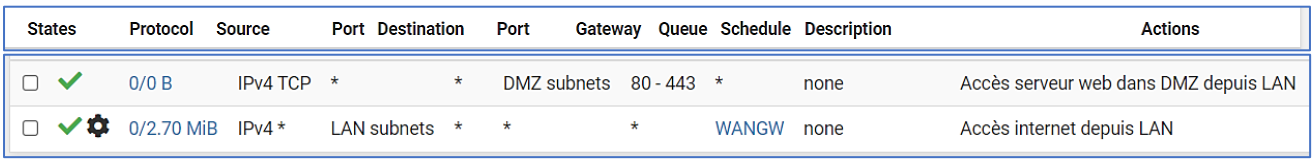


RESUME DES REGLES A CONFIGURER

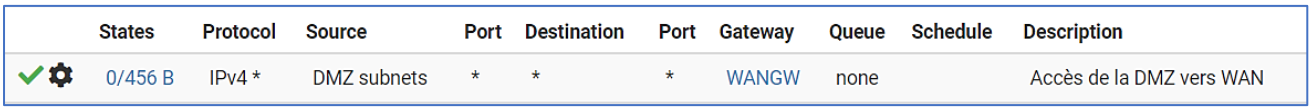
INTERFACE WAN (rules)



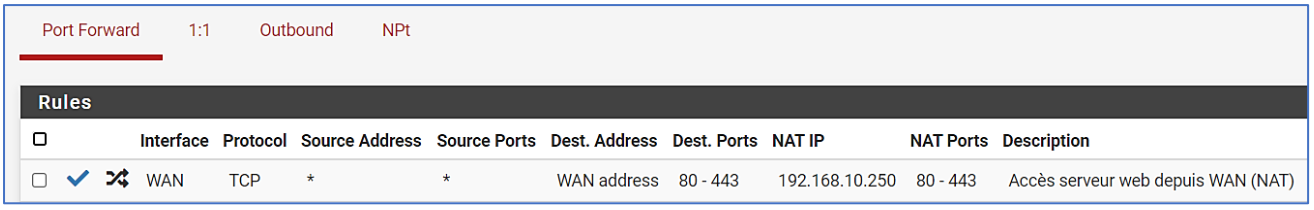
INTERFACE LAN (rules)



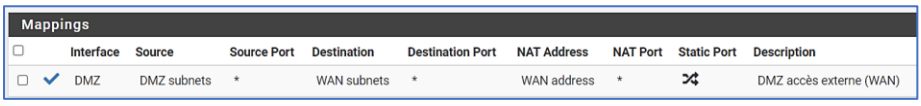
INTERFACE DMZ (rules)



PORT FORWARDING (NAT)



NAT OUTBOUND



Maintenant que vos règles sont configurées, testez l'accès à Internet depuis votre conteneur en faisant la mise à jour des paquets :

- Mettez à jour les paquets de votre conteneur Debian avec « **apt update** » et « **apt upgrade -y** » :

```
root@CT-Debian:~# apt update
Hit:1 http://security.debian.org bookworm-security InRelease
Hit:2 http://deb.debian.org/debian bookworm InRelease
Hit:3 http://deb.debian.org/debian bookworm-updates InRelease
Reading package lists... Done
Building dependency tree... Done
30 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```
root@CT-Debian:~# apt upgrade -y
```

```
Preparing to unpack .../4-postfix_3.7.9-0+deb12u1_amd64.deb ...
Unpacking postfix (3.7.9-0+deb12u1) over (3.7.6-0+deb12u2) ...
Preparing to unpack .../5-libgnutls30_3.7.9-2+deb12u1_amd64.deb
Unpacking libgnutls30:amd64 (3.7.9-2+deb12u1) over (3.7.9-2) ...
Setting up libgnutls30:amd64 (3.7.9-2+deb12u1) ...

Progress: [ 47%] [#########################################....
```

- Installez le serveur web Apache avec la commande « **apt install apache2 -y** » :

```
root@CT-Debian:~# apt install apache2 -y
```

- Vérifiez que votre serveur web est actif avec la commande « **systemctl status apache2** » :

```
root@CT-Debian:~# systemctl status apache2
* apache2.service - The Apache HTTP Server
     Loaded: loaded (/lib/systemd/system/apache2.service; enabled; preset: enabled)
     Active: active (running) since Sat 2024-02-03 15:12:24 UTC; 14min ago
       Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 3842 (apache2)
```

- Testez la connexion à Apache, depuis une machine du réseau « LAN » en saisissant, dans la barre d'adresses du navigateur, l'IP de votre conteneur (ici http://192.168.10.250) :

Test de l'accès au serveur web depuis l'extérieur :

- Depuis un navigateur d'une machine extérieure, saisissez l'adresse IP publique (ou la WAN ou un sous-domaine hébergé) de votre pfSENSE : votre page Apache doit s'afficher :

La connexion ne sera pas sécurisée car nous n'avons pas de certificat Let's Encrypt. La page Apache par défaut doit s'afficher. Si cela n'est pas le cas, revoyez vos règles de pare-feu.