Boumrah Samy

PFSENSE : Chapitre 1 : Configuration de la PFSENSE.

pfSense est une solution open source de pare-feu et de routage basée sur FreeBSD. Elle permet de sécuriser un réseau en filtrant les flux, en gérant les adresses IP, en assurant le partage de connexion et en appliquant des règles de sécurité adaptées à l'infrastructure mise en place.

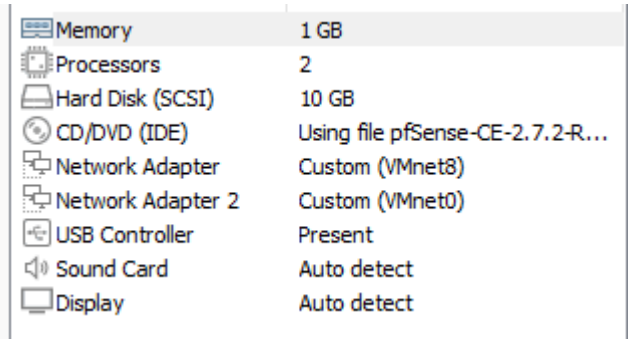
Dans notre projet, pfSense joue le rôle de pare-feu principal entre le réseau local et l'extérieur. Il va nous permettre de définir les interfaces réseau, d'attribuer des adresses IP, de mettre en place un serveur DHCP et de contrôler les communications entre les machines du lab.

Installation de pfSense

Pour commencer, il nous faut télécharger l'image ISO de pfSense afin de l'installer sur une machine virtuelle. Cette méthode permet de tester la configuration dans un environnement de laboratoire sans avoir besoin d'un matériel dédié.
https://www.pfsense.org/download/

Nous allons ensuite créer une nouvelle machine virtuelle et l'a configurée pour accueillir pfSense. Une fois la VM prête, nous pourrons lancer l'installation depuis l'ISO afin de démarrer la configuration.

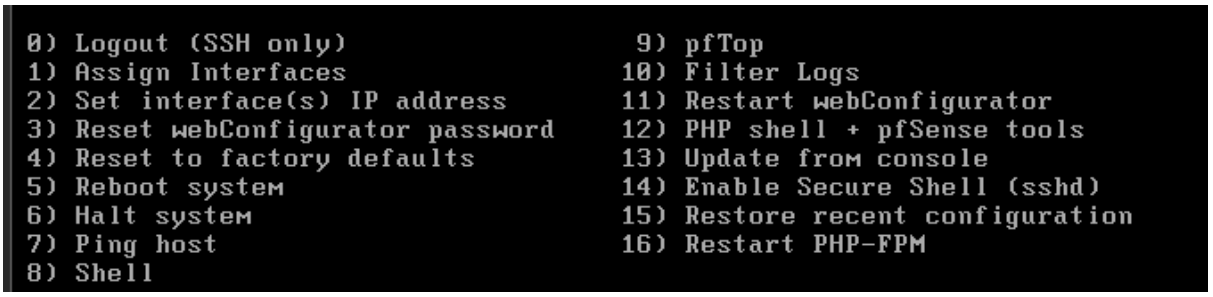
Il faut également ajouter une deuxième carte réseau dans les paramètres de la machine virtuelle afin de pouvoir faire fonctionner le réseau correctement.



L'une est placée sur **VMnet8** et l'autre sur **VMnet0** : ces deux interfaces représentent respectivement le **WAN** et le **LAN** de pfSense. Le réseau du LAN doit être similaire à celui des autres machines virtuelles afin qu'elles soient toutes sur le même réseau en **VMnet0**.

Début de la configuration

Après le démarrage de la machine virtuelle, pfSense affiche son menu de configuration en console. C'est à partir de cette interface que nous allons d'abord assigner les interfaces réseau, puis configurer les adresses IP et les services nécessaires au bon fonctionnement du réseau.



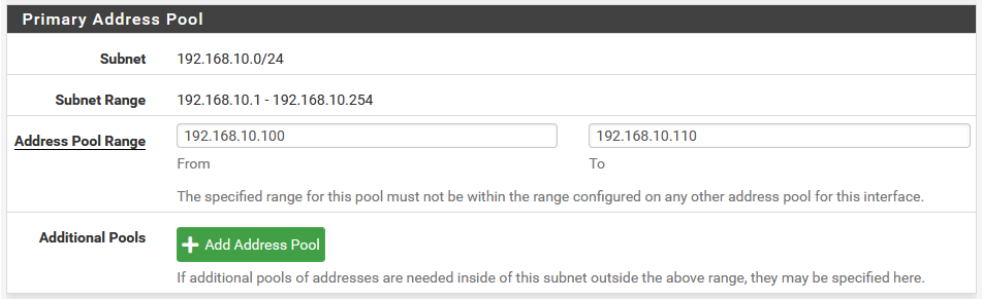
Pour assigner les interfaces, nous choisissons l'option **2** puis nous associons **WAN = em0** et **LAN = em1**.

Ensuite, nous configurons les adresses IP de chaque interface. Pour le **WAN**, nous laissons l'interface récupérer une adresse automatiquement via **DHCP**, puisque la machine hôte lui fournit la connectivité grâce au **NAT**.

Pour le **LAN**, nous refusons également l'attribution automatique afin de définir manuellement l'adresse **192.168.10.1**.

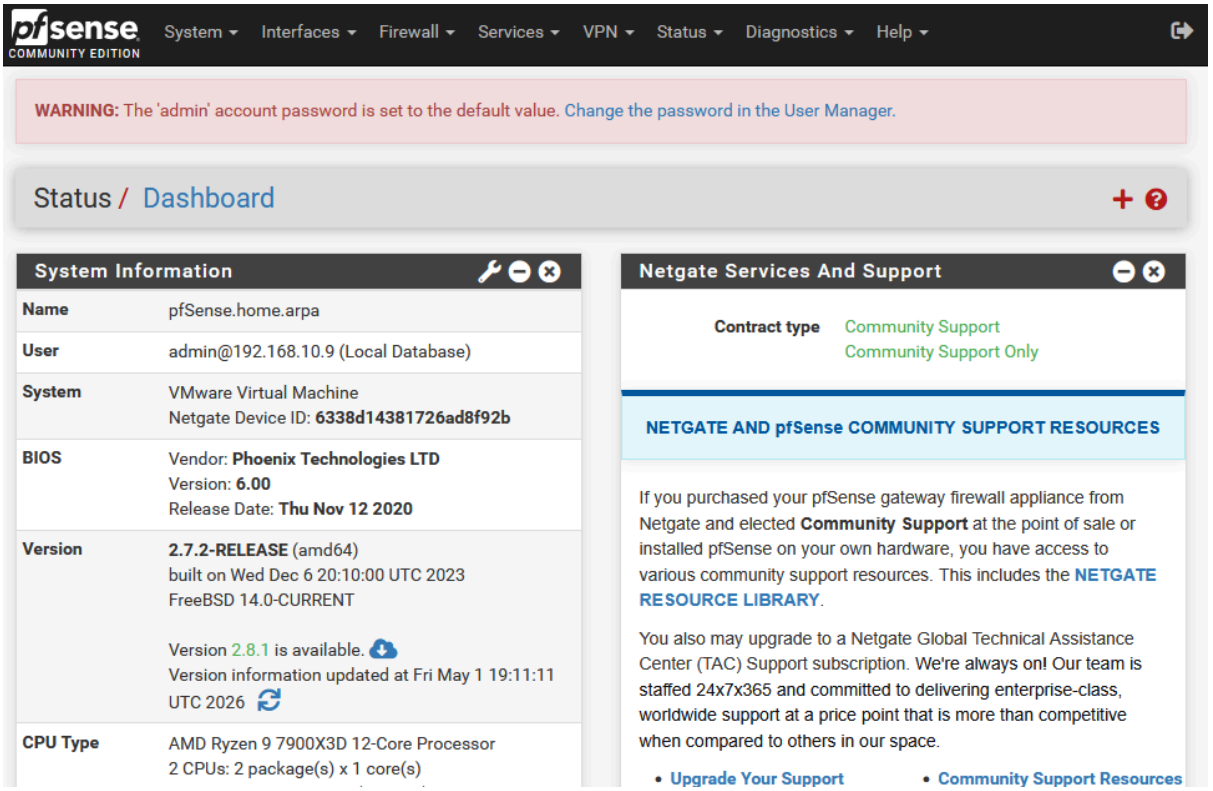
Nous pouvons ensuite ignorer l'étape **DHCPv6**. Lorsqu'il nous est proposé de créer un **serveur DHCP**, nous acceptons afin de configurer la plage d'adresses du réseau local. La plage définie est la suivante :

- Début de plage : **192.168.10.100**
- Fin de plage : **192.168.10.110**



Lorsque notre contrôleur de domaine est placé sur le même réseau **192.168.10.x**, il peut accéder à l'interface graphique de pfSense avec l'addresse : http://IP_PFsense

Ce qui rend la gestion beaucoup plus simple.



Une fois la configuration réseau terminée, nous pouvons donc nous connecter à l'interface web de pfSense depuis un poste du réseau local afin de poursuivre les réglages plus facilement. Depuis ce tableau de bord, il devient possible de gérer les interfaces, les règles de pare-feu et les services du pare-feu de manière plus pratique que depuis la console.

Conclusion du chapitre

La mise en place de pfSense nous a permis de disposer d'un pare-feu fonctionnel pour sécuriser et organiser le réseau du projet. Grâce à la configuration des interfaces, à l'attribution des adresses IP et à l'activation du serveur DHCP, nous avons pu établir une base réseau claire et opérationnelle.

L'accès à l'interface graphique depuis le réseau local a ensuite facilité l'administration du pare-feu et la poursuite des réglages. Cette solution nous a donc permis de centraliser la gestion du trafic réseau tout en préparant l'environnement nécessaire pour les autres services du projet.

Fin du chapitre 1