Documentation technique

27/03/2024

Installation et configuration du pare-feu PfSense

Sommaire

Définition

PfSense

PfSense est un système d'exploitation open source basé sur FreeBSD, conçu pour être utilisé comme pare-feu, routeur et passerelle de sécurité. Parmis les pares-feu gratuit les plus utilisés, il offre une gamme de fonctionnalités avancées de sécurité et de routage.

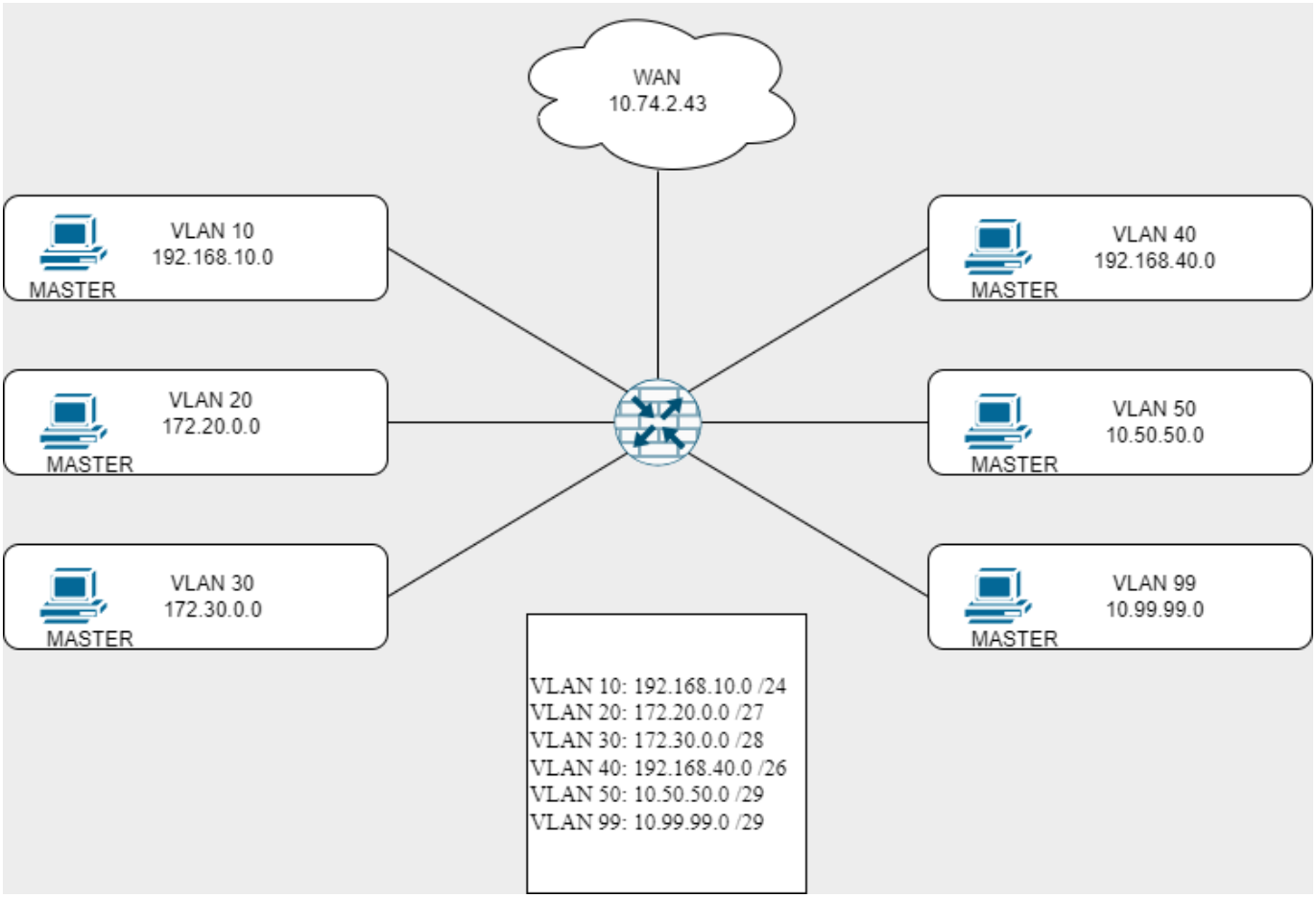
Pare-feu

Un pare-feu est un équipement de protection du réseau. Il surveille le trafic entrant et sortant et décide s'il est autorisé ou non à passer par certains ports en fonction des règles de sécurité prédéfinies.

Fonctionnalités

- ***Pare-feu avancé*** : PfSense inclut un pare-feu puissant qui peut être configuré pour filtrer le trafic réseau en fonction de critères tels que les adresses IP source et destination, les ports TCP/UDP, les protocoles, etc.
- **NAT** (Network Address Translation) : Il prend en charge la translation d'adresses réseau pour permettre à plusieurs périphériques sur un réseau privé d'accéder à Internet via une seule adresse IP publique.
- **VPN** (Virtual Private Network) : PfSense permet la création de tunnels VPN pour sécuriser la communication entre différents réseaux ou pour permettre l'accès sécurisé à distance aux ressources réseau.
- **Load balancing** et haute disponibilité : Il offre des fonctionnalités de répartition de charge et de redondance pour garantir la disponibilité et la performance des services réseau.
- **Proxy Web** : Il peut être configuré pour agir en tant que serveur proxy HTTP/HTTPS (avec SQUID) et pour filtrer le contenu Web en fonction de politiques définies par l'utilisateur.
- **Contrôle de la bande passante** : PfSense permet de limiter et de prioriser le trafic réseau en fonction de différents critères, ce qui est utile pour optimiser l'utilisation de la bande passante dans un réseau.la fonction ou toute autre caractéristique pertinente.

Schéma réseau

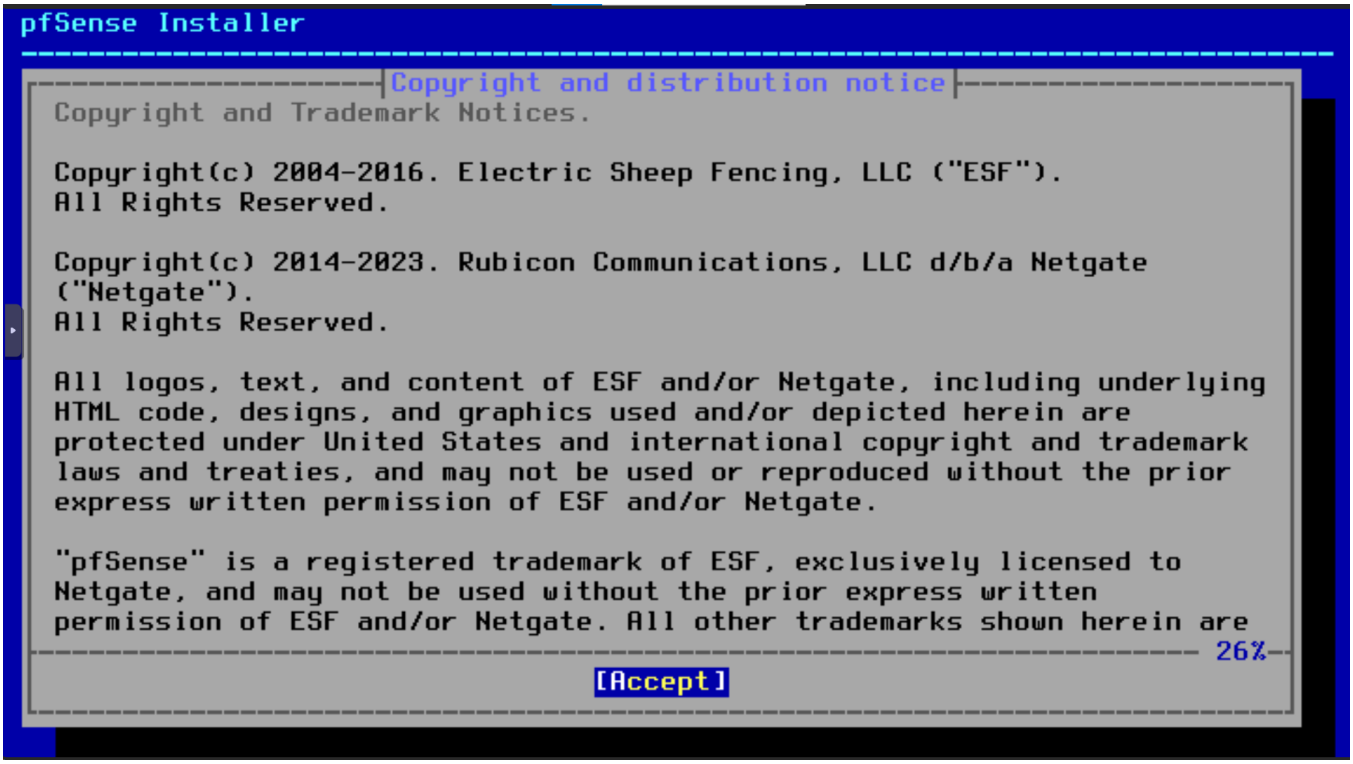


Prérequis

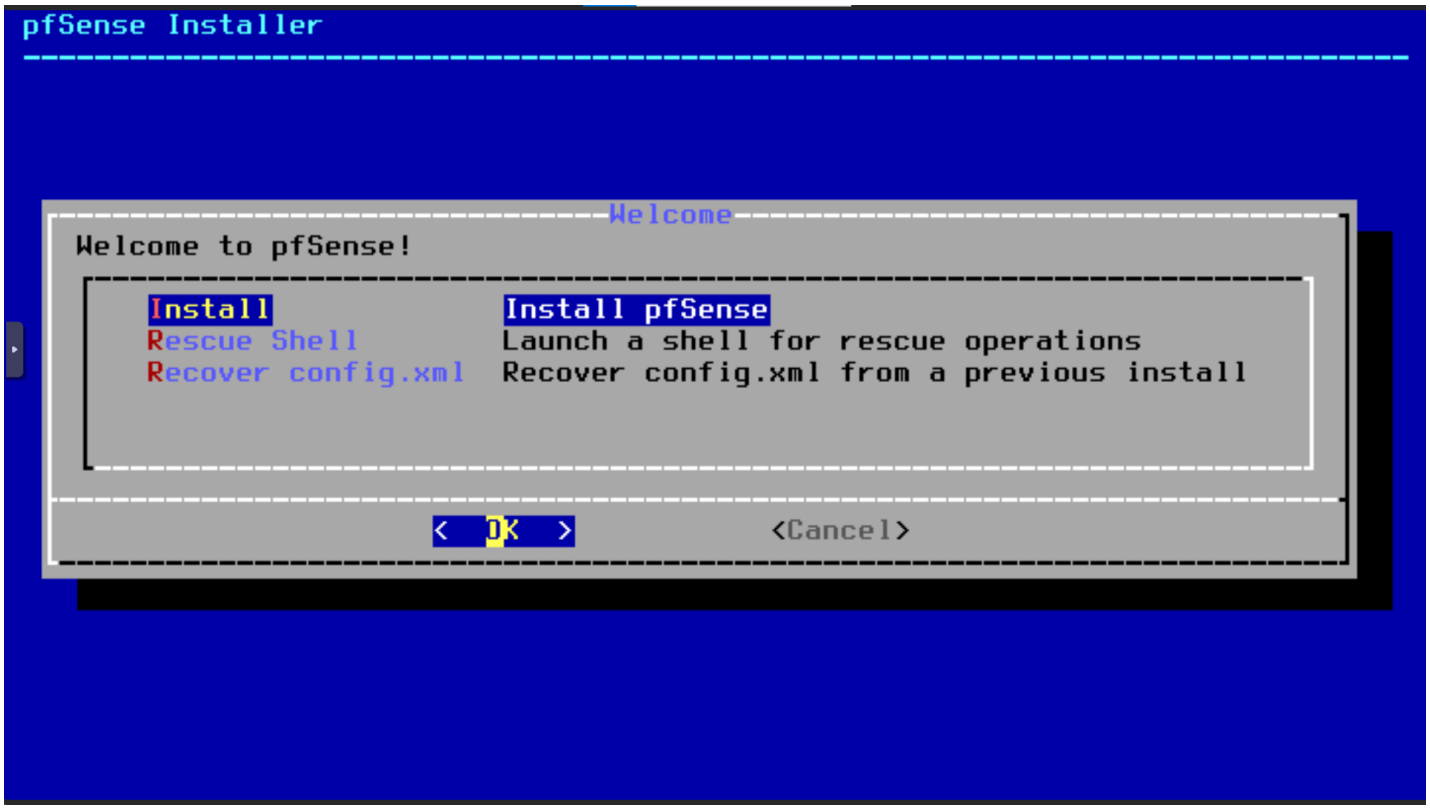
- Processeur 1,4 GHz 64 bits
- A minima 1 Go de RAM
- 8 Go d'espace disque
- Une ou plusieurs cartes réseaux
- Une clé bootable avec l'ISO de la dernière version de PfSense

Installation de PfSense

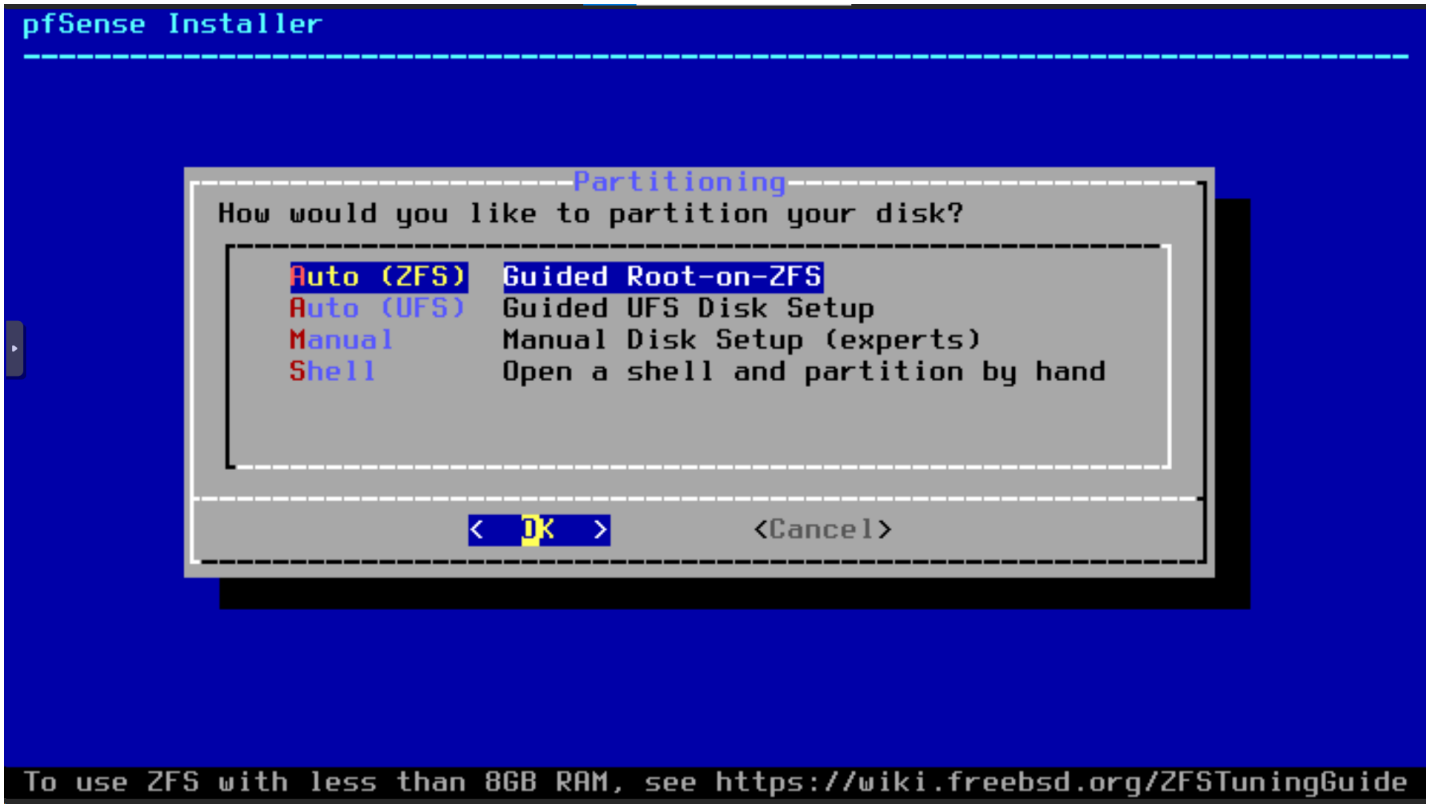
Après avoir fait booter la machine sur l'ISO PfSense, l'installation commence.
Il faut accepter la licence utilisateur.



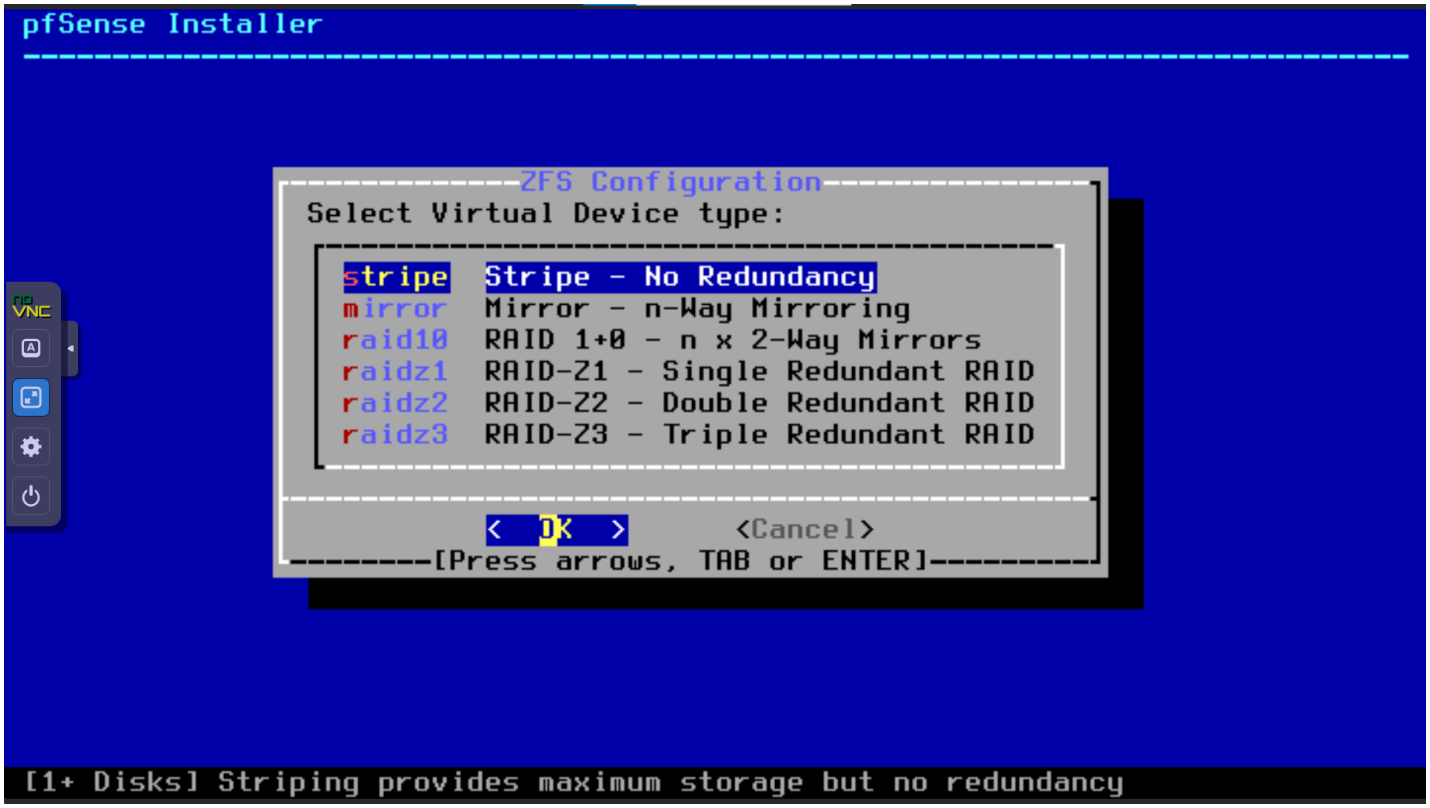
Choisir l'installation.



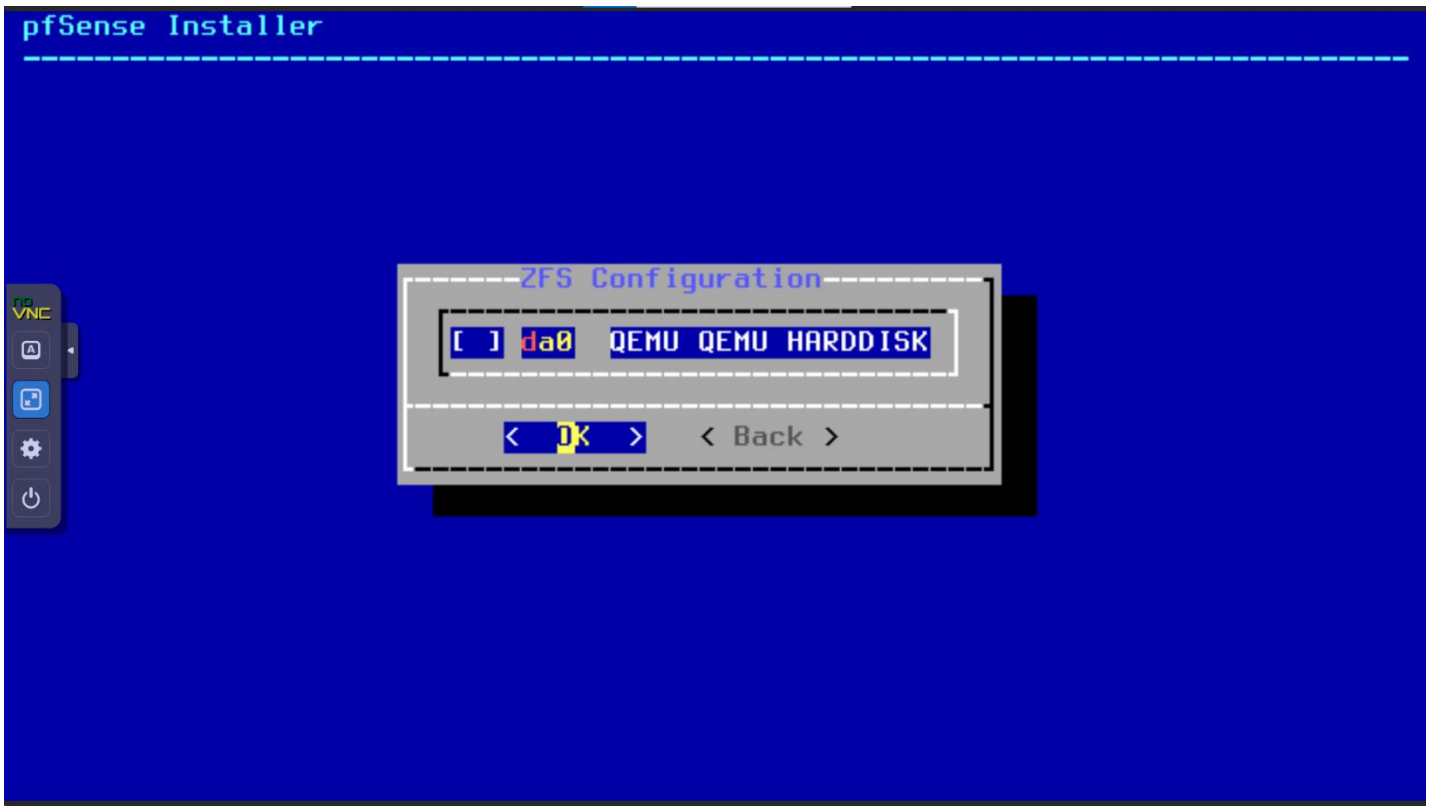
Sélectionner l'installation Auto en ZFS (système de fichiers open source sous licence CDDL).



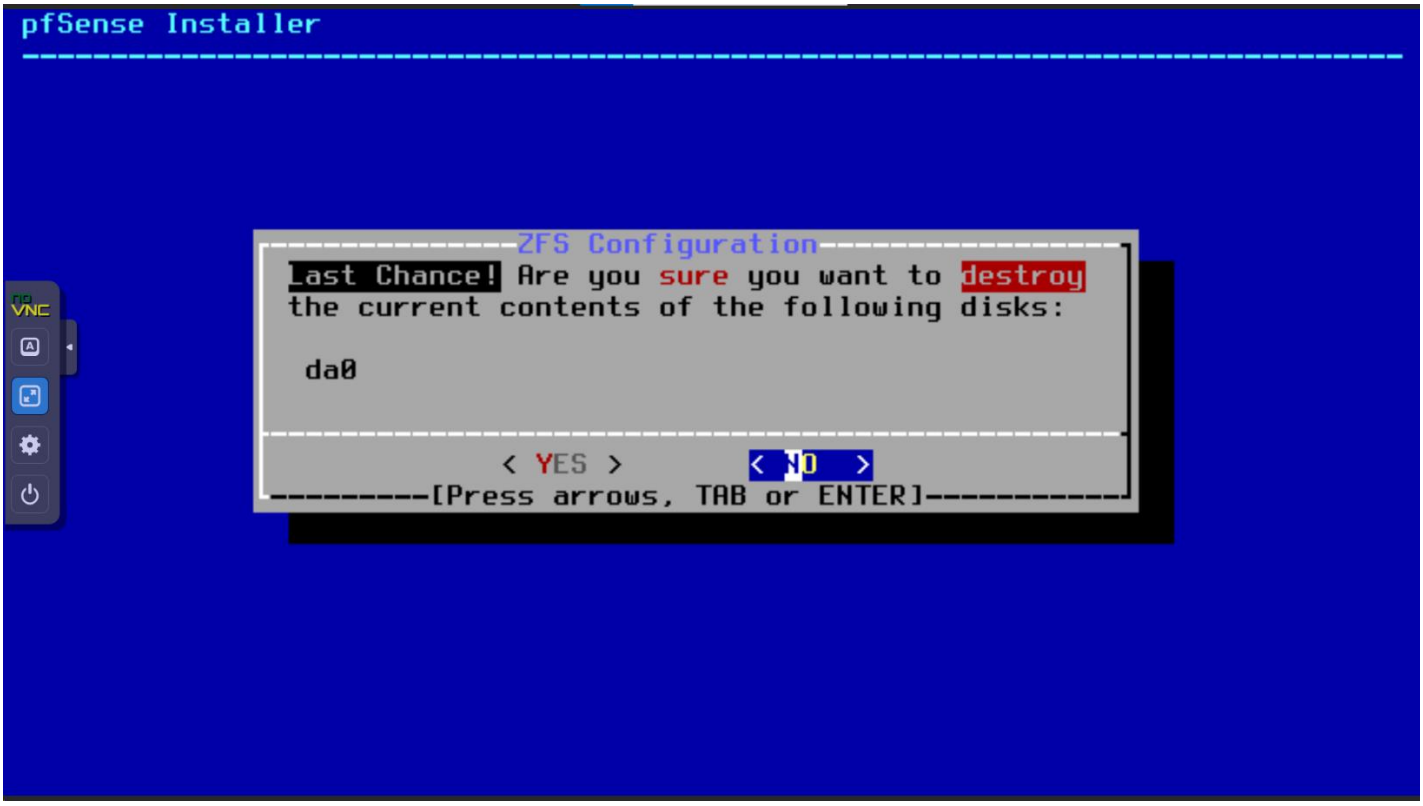
Prendre l'installation sur un équipement (sans redondance).



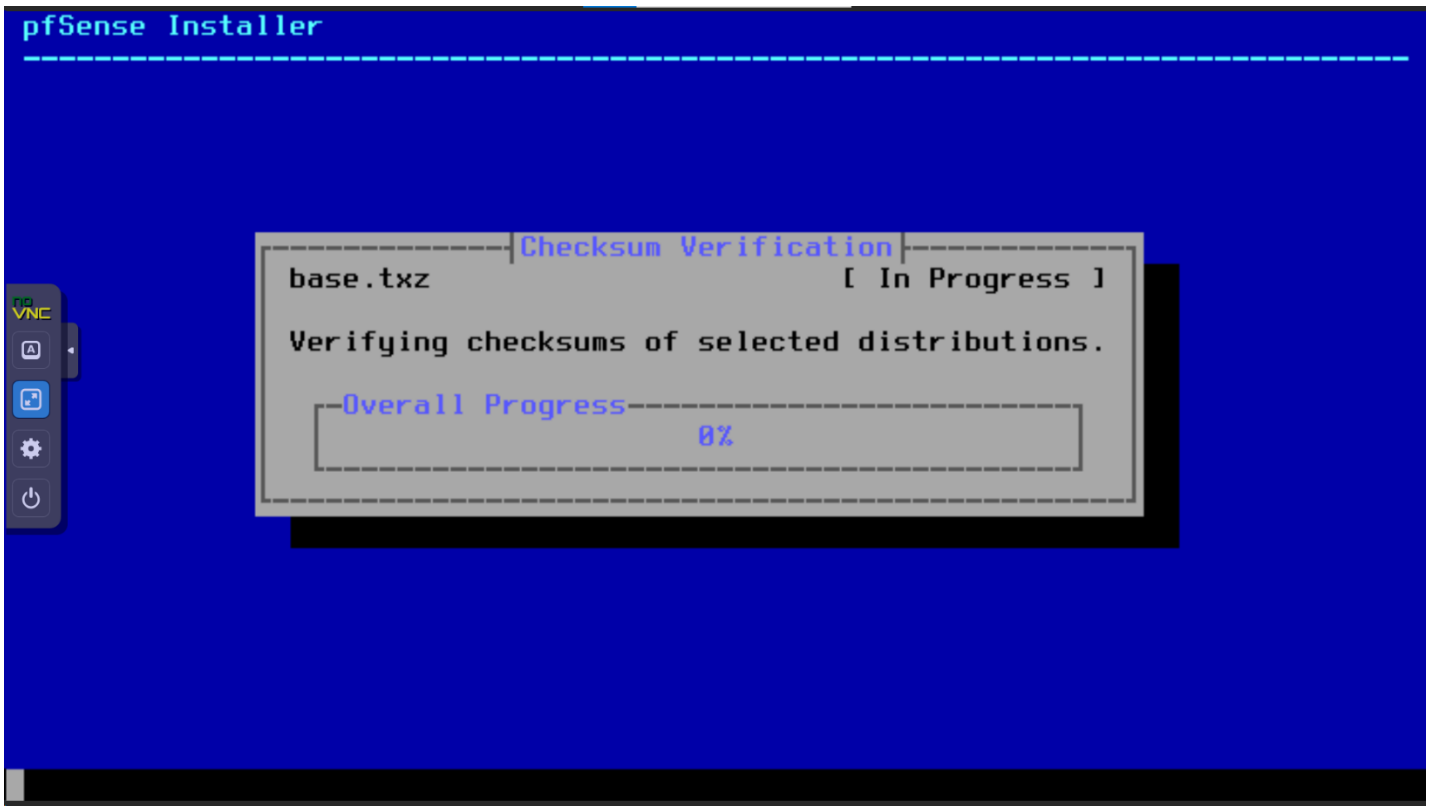
Sélectionner son disque.



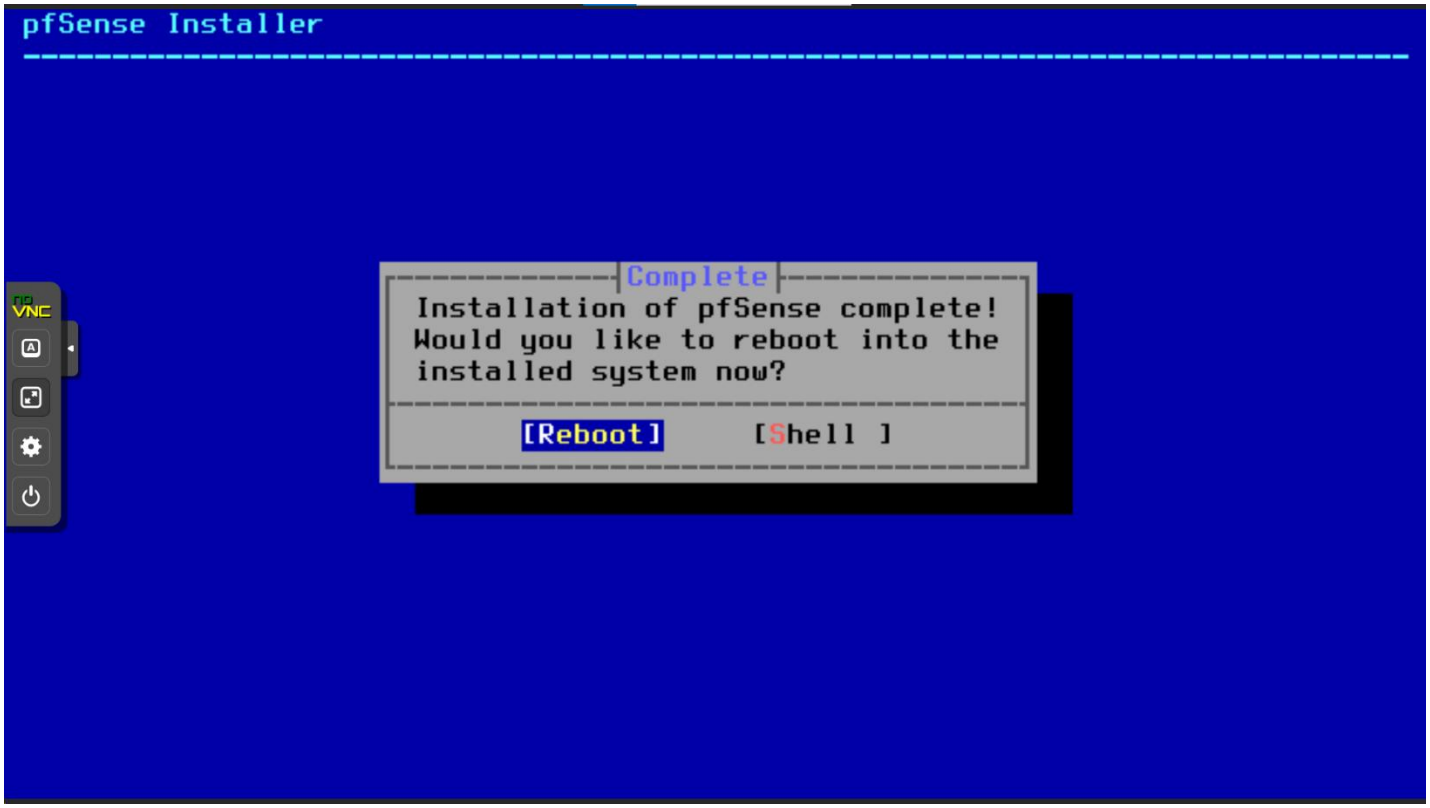
Et valider l'écriture.



L’installation va se faire.



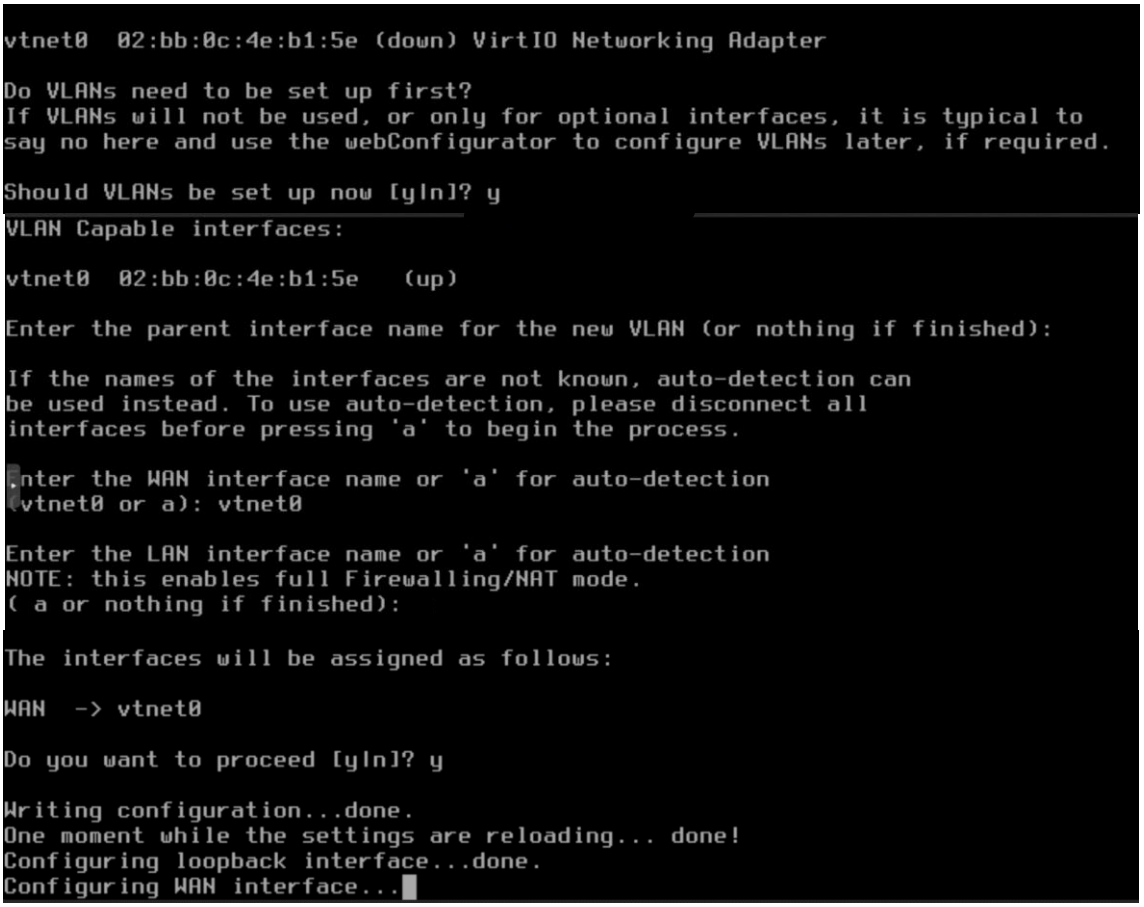
A la fin de l’installation, redémarrer la machine.



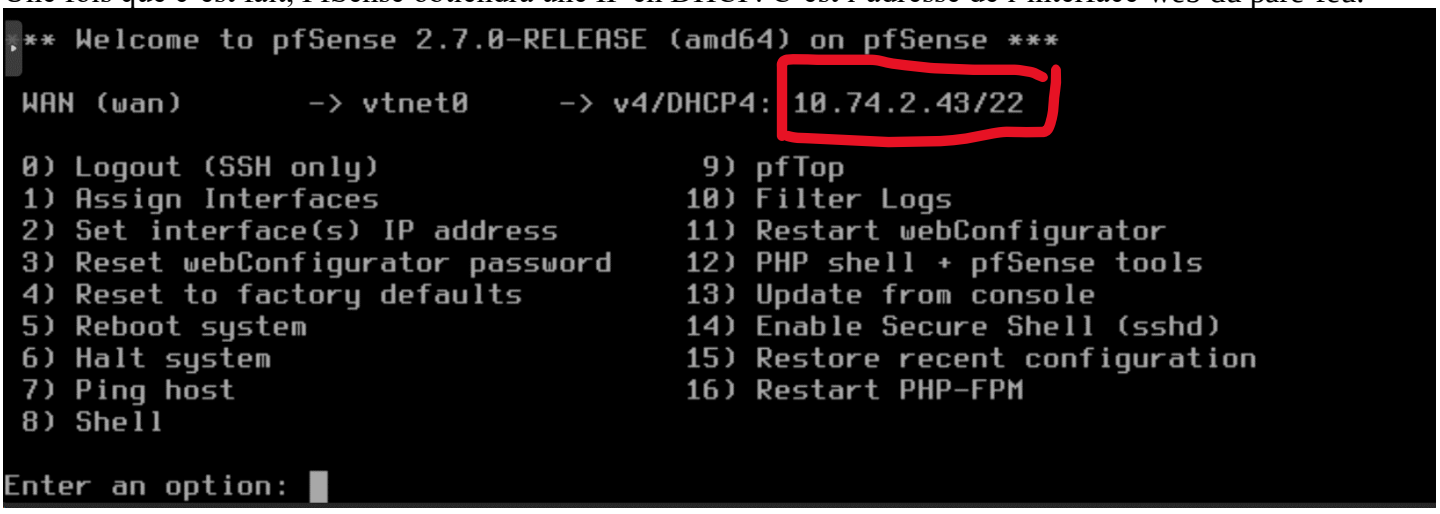
Configuration de l'IP de l'interface PfSense

PfSense est basé sur FreeBSD (une version d'Unix), il faudra donc faire la configuration en ligne de commandes.

Il faut dans un premier temps assigner une interface au WAN. Pour cela, il faut sélectionner vtnet0 qui correspond au vmbr0 de Proxmox qui est la carte réseau virtuelle WAN.

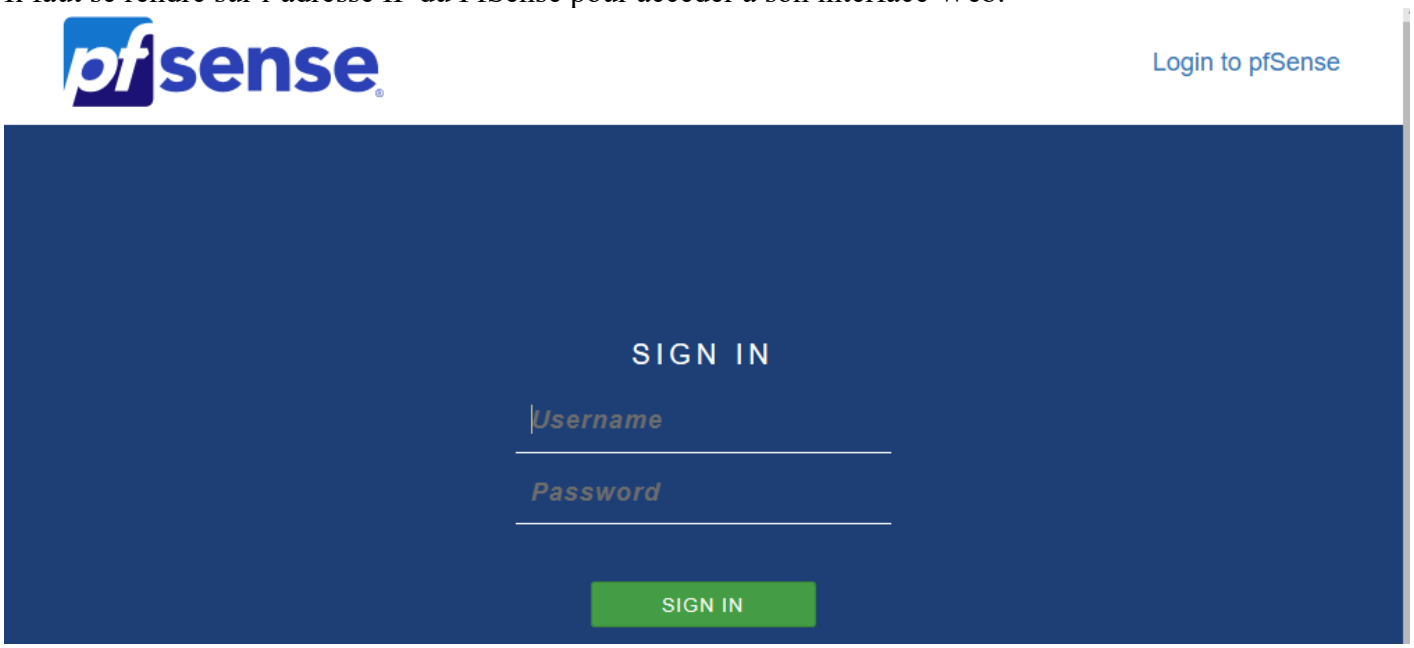


Une fois que c'est fait, PfSense obtiendra une IP en DHCP. C'est l'adresse de l'interface web du pare-feu.

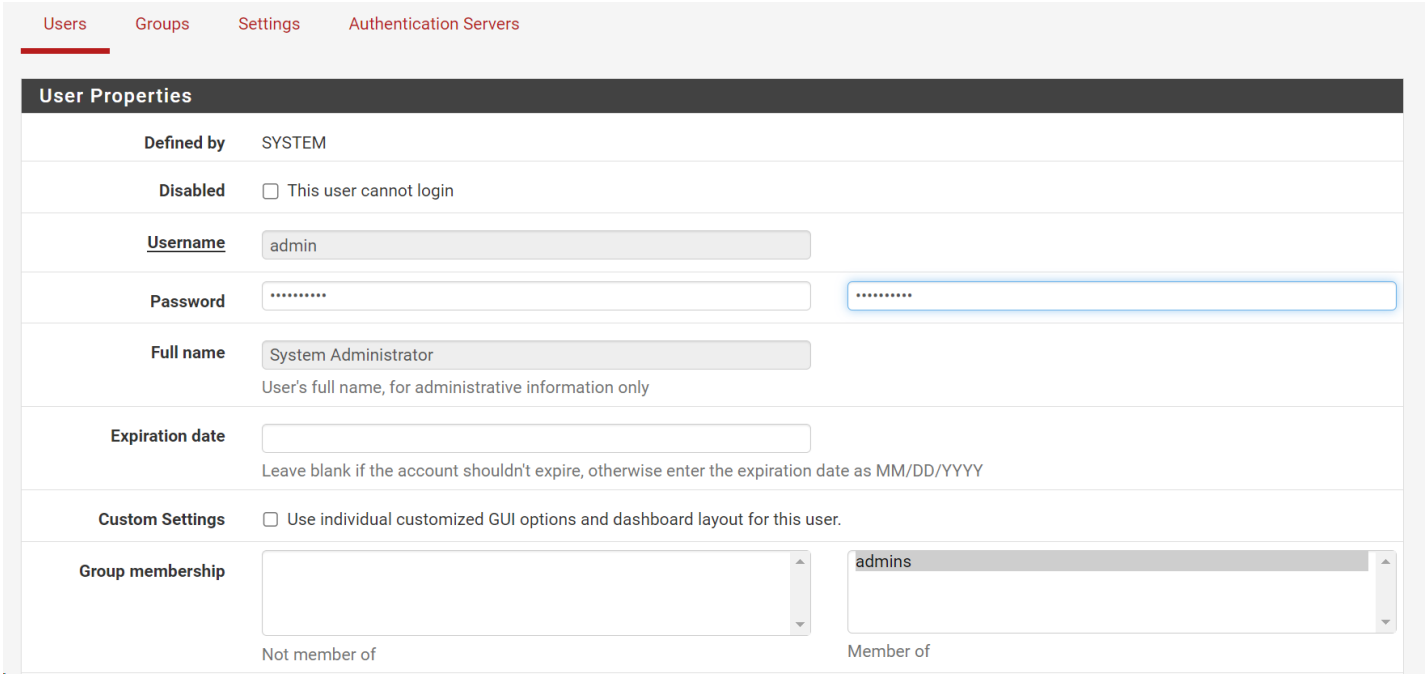


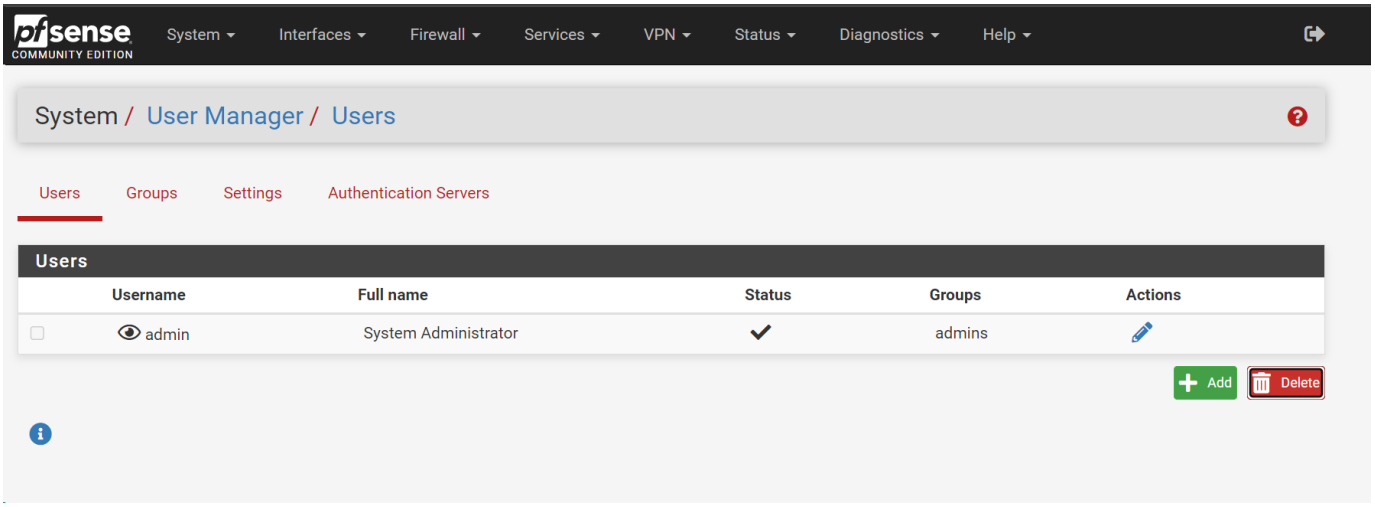
Configuration des VLAN sur l'interface PfSense

Il faut se rendre sur l'adresse IP du PfSense pour accéder à son interface Web.

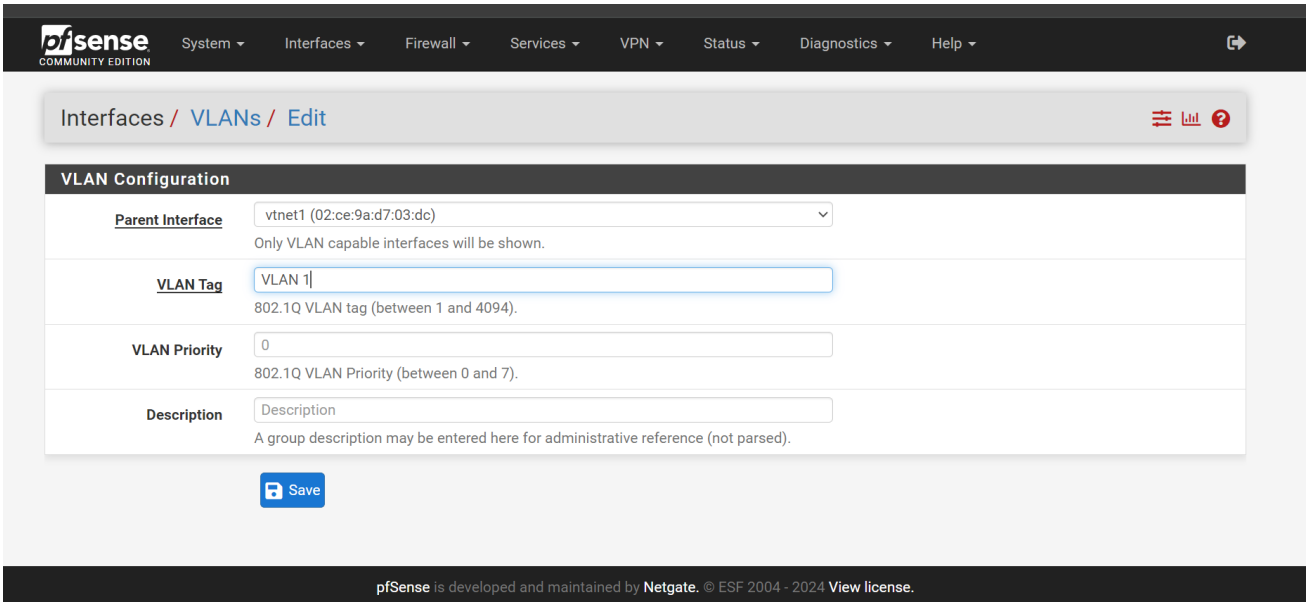


Une fois dessus, il faudra se connecter avec l'user *admin* et le *mot de passe par défaut*. Il sera par la suite demandé de le modifier en allant dans **System**, **User Manager**, **Users** et **Edit**.

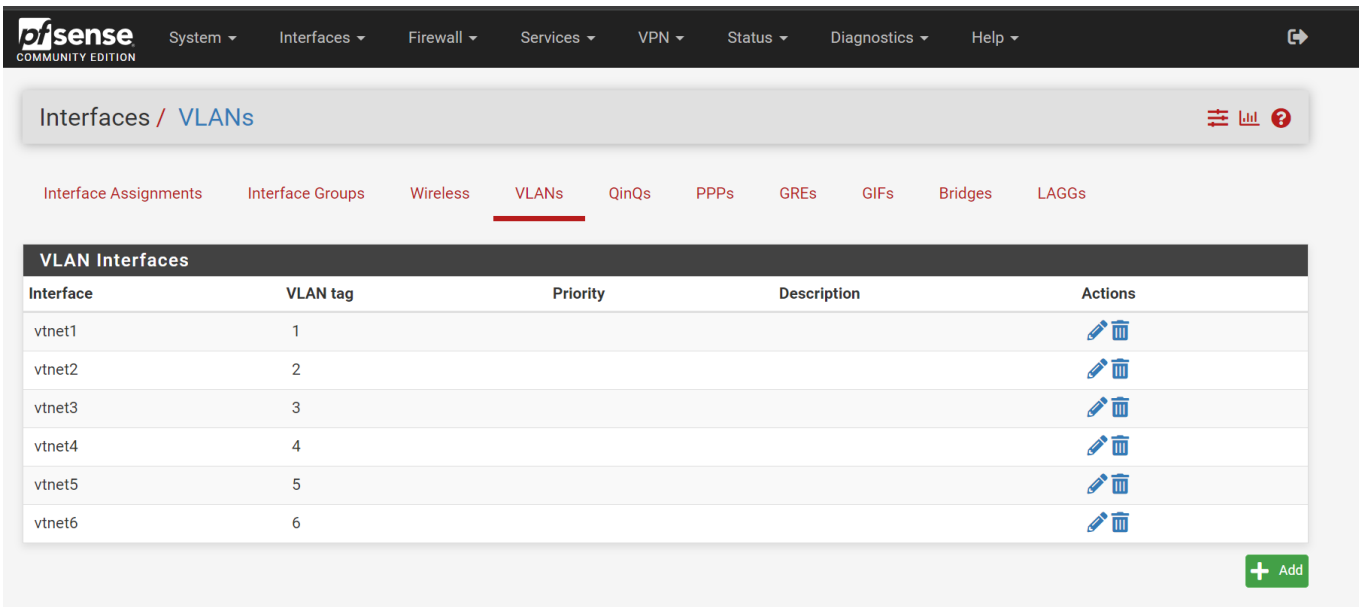




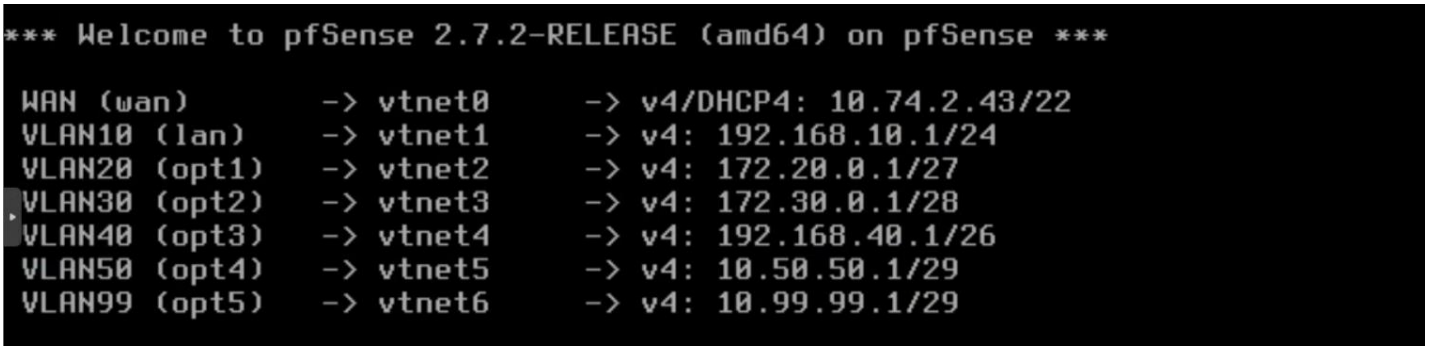
Une fois que c'est fait, il faut se rendre sur **Interfaces**, **VLANs** et **Edit** afin d'ajouter les VLAN créés préalablement sur Proxmox à PfSense.



Ici, tous les VLAN sont ajoutés :

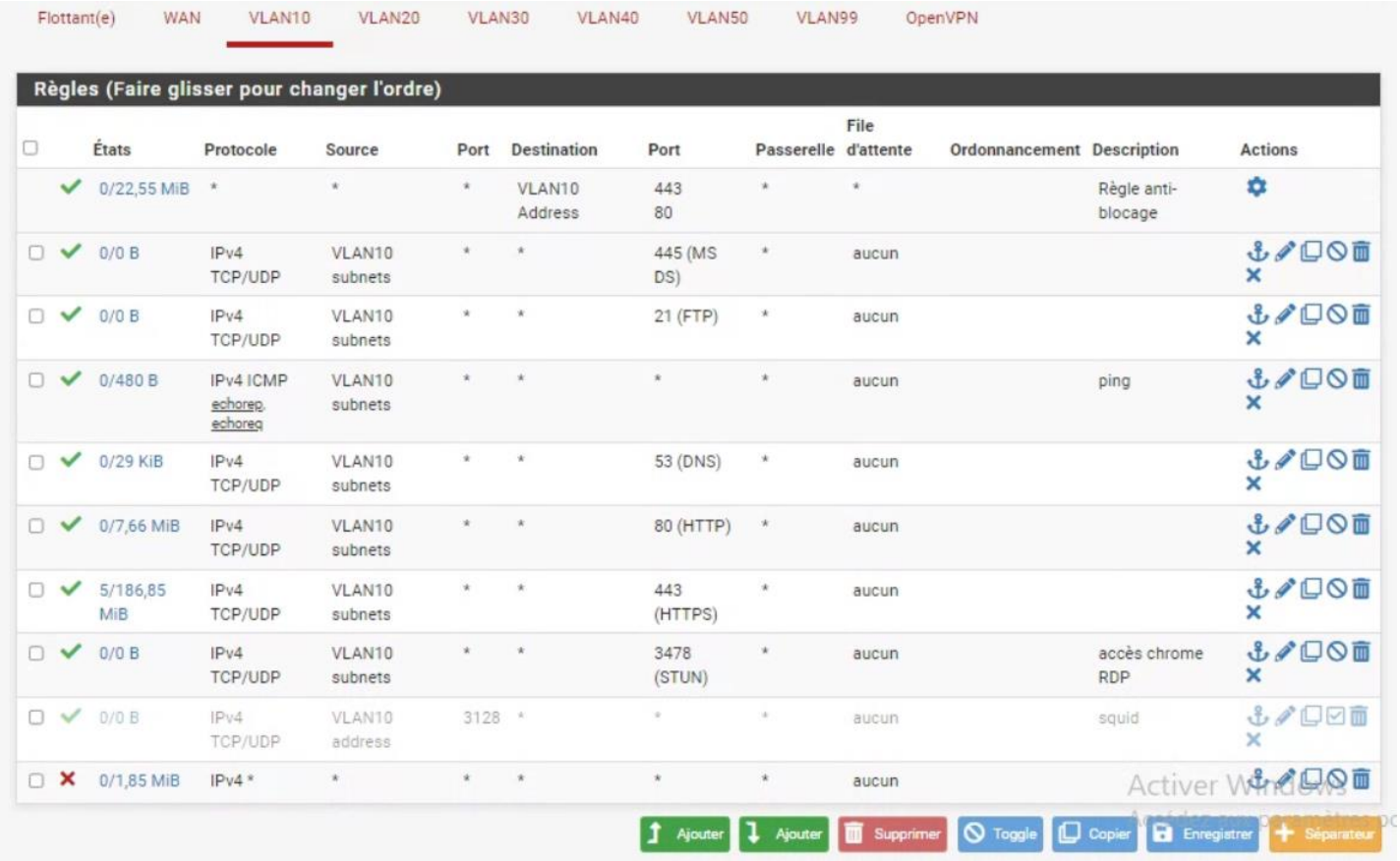


Une fois que les VLAN ont été ajoutés sur l'interface, il est possible de vérifier sur la machine qu'ils ont tous été pris en compte. Ici, nous pouvons voir que tous nos VLAN ont bien été ajouté au firewall.



Etablissement des règles de firewall

Afin d'utiliser le pare-feu, il est nécessaire d'établir des règles autorisant ou refusant le flux de tels ou tels paquets.



Dans les règles établies dans chaque VLAN, on retrouve celles qui permettent l'accès aux sites Internet (en autorisant les protocoles HTTP/HTTPS et DNS pour la résolution de nom de domaine).

Ainsi que celles qui permettent le transfert de fichiers (en autorisant les protocole FTP et SMB) pour permettre au NAS de fonctionner.

Ou encore le ping entre machines du même VLAN ou de VLAN différents (en autorisant le protocole ICMP en echo request et echo reply).

D'autres ports et protocoles plus spécifiques peuvent être autorisés en fonction de chaque VLAN comme le protocole STUN sur le port 3478 ici pour permettre la connexion en bureau à distance via Chrome Remote Desktop, l'ouverture du port 1723 pour le tunnel VPN, du port 3128 pour le proxy SQUID ou encore 3389 pour le protocole RDP.

Configuration du NAT

Le NAT peut être mis en place depuis **NAT** dans l'onglet **Pare-feu**. Sur PfSense, il fonctionne sous forme de règles. Il existe plusieurs méthodes de NAT dont le port forwarding (redirection de port) ou le 1:1.