Pare-feu : OPNsense

Installation & Configuration de OPNsense

On vas commencer par crée une clé bootable OPNsense, on téléchargera l'image sur le site officiel d'OPNsense et le créateur de media bootable Rufus. L'installation d'OPNsense se découpe en 7 étapes :

1. Le choix de la configuration clavier.
2. Le choix du systèmes de fichier :
    - Il y a deux choix UFS et ZFS, selon le site ZFS est le plus stable mais demande plus de puissance (RAM).
3. Le choix du partitionnement :
    - Toujours selon le site la meilleur option est stripe si on as qu'un seul disque.
4. La sélection du média d'installation.
5. La confirmation des options
6. La création du mot de passe root
7. La finalisation (Reboot de la machine)

La dernière étapes est la configuration des interfaces mais avant un peu de lexique :

- WAN : (Wide Area Network) L'interface WAN fait référence à l'interface qui est utilisé pour aller à l'extérieur du pare-feu.
- LAN : (Local Architecture Network) Une interface faisant référence au réseau privée que nous voulons protéger.
- OPT : Optionnel, réseau pouvant faire référence à un autre WAN, LAN ou dans notre cas DMZ.

Quand la machine aura redémarrez, vous aurez un menu la 1er chose est d'appuyez sur la touche 1 : pour assigner le rôle des interfaces réseau aux bonnes cartes réseaux, pour cela il faudra au préalable recueillir les adresses MAC des IRs et savoir les correspondances physiques.

Ensuite il faut appuyer sur le 2, pour donner leurs @IP à chaque IRs.

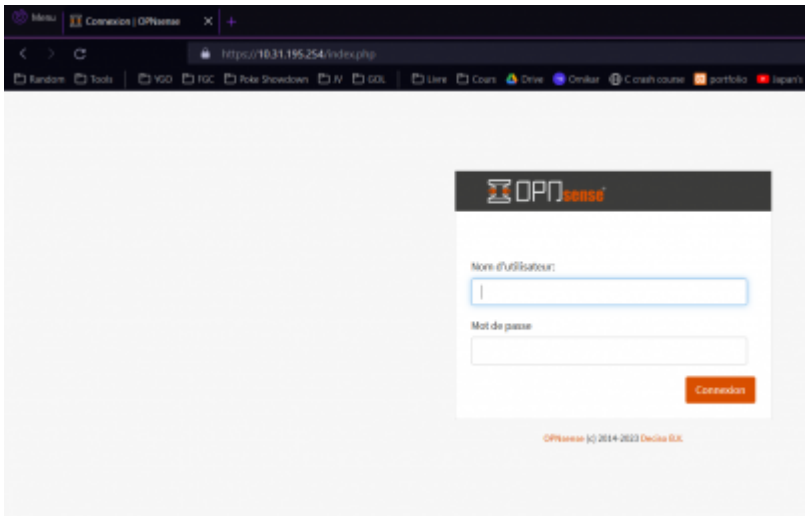
Maintenant pour accéder aux GUI du site il faut se connecter à l' @IP du pare feu qui gère le LAN via internet.
Mais le pare feu bloque de base toutes les connexions donc on vas le désactiver via cette commande.

Pour accéder aux commandes dans OPNsense sur le menu de base il faut appuyer sur 8

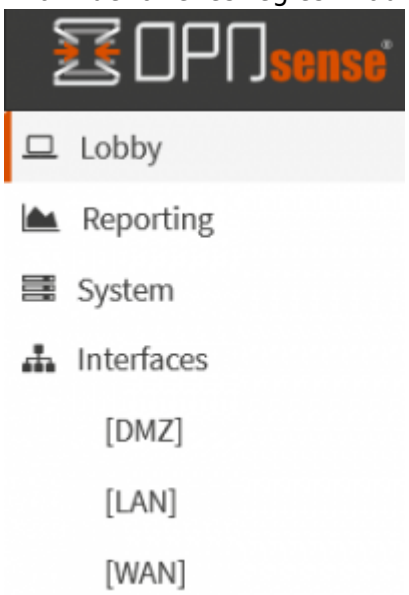
```
pfctl -d
```

Pour sortir des commandes il faut faire exit 0

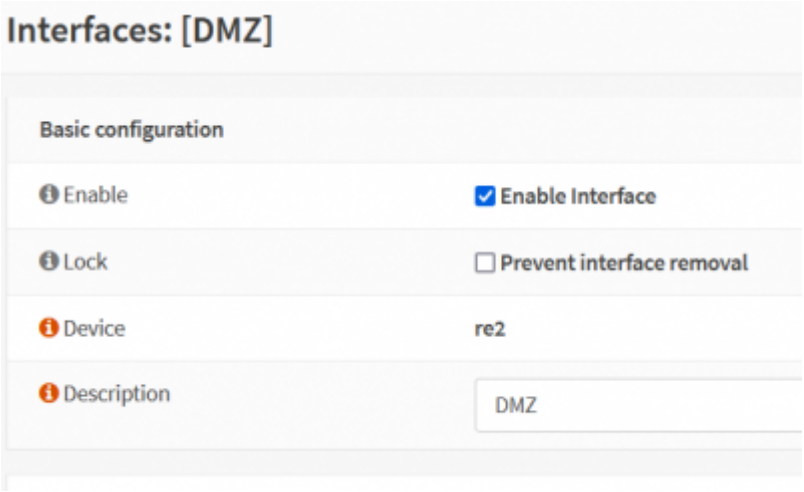
Maintenant on peut accéder au GUI, on se connecte à l'interface LAN via internet. Ici nous sommes sur une page de connexion, il faut rentrer les login/MDP de l'utilisateur root d'OPNsense.



Avant de faire les règles il faut vérifier plusieurs chose dans le menu interfaces.



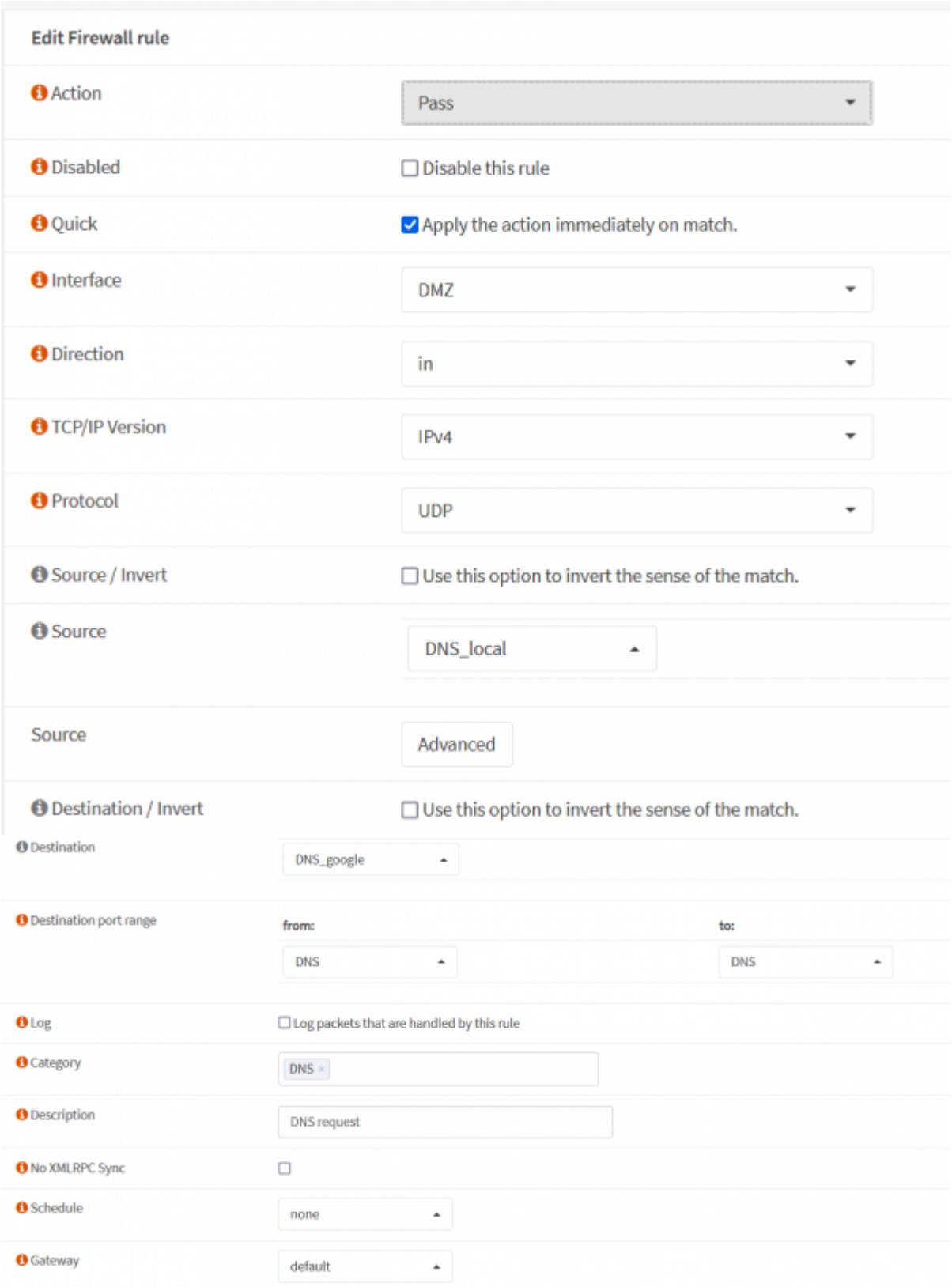
Les interfaces entre sont entre crochets dans les menus de ces interfaces il faut vérifier “Enable Interface”, “Description” pour renommer l' interface, “Block private networks” si on manipule des IPs privés et l'“IPv4 address”.



Pour faire les règles il y a plusieurs condition :

- Le pare-feu rejette tout ce qui veut rentrer par défaut donc tout les règles doivent être des “Pass”.
- Il accepte que tout puisse sortir
- Tout est en Stateful de base don pas besoin de s'occuper des réponses
- Toutes les règles doivent avoir des descriptions

Maintenant pour faire une règle :
Dans le menu “Firewall” puis “Rules” vous aurez le choix entre plusieurs interface celle qui nous intéresse sont “LAN”, “DMZ” et “floating” (pour DMZ). Une fois sur la liste des règles nous, On appuie sur l'icone orange avec une croix en haut à droite de la page qui vas nous amener au menu de création de règle,



Il y a 5 catégorie qui nous intéresse, “protocol” (pour TCP/UDP/ICMP…), “Source” (de ou doit venir la requête) , “Destination” (Ou doit aller), “Destination port range” (Protocole applicatif FTP, HTTP …) et “Description” (Que fait la règle).

En appuyant sur “Save”, on revient sur la liste des règles, au dessus un bandeau aura apparut :

Le bandeau indique que les règles ont changés et que pour les prendre en compte il faut appuyer sur

le bouton “Apply changes” pour que la nouvelle règles soit prisent en compte.