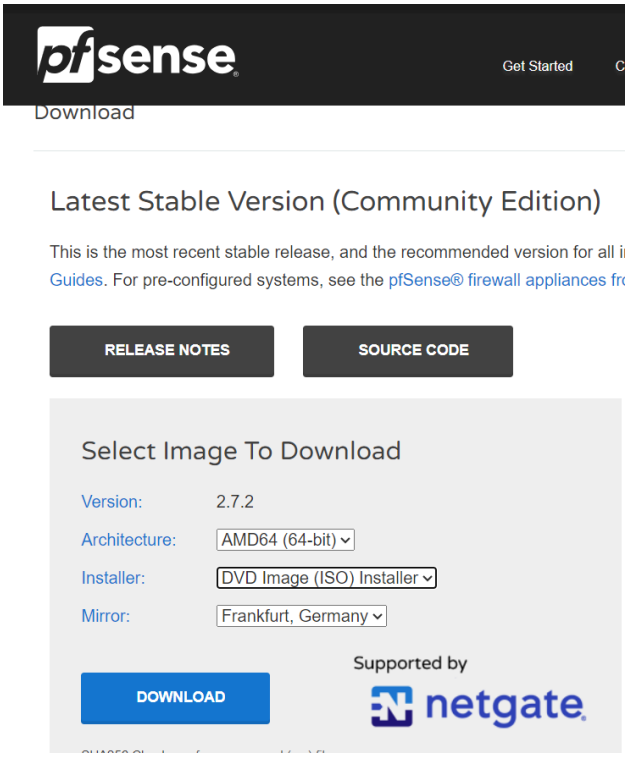
Lebeau Mathéo BTS SIO 1

TP pare-feu Pfsense

Intro :

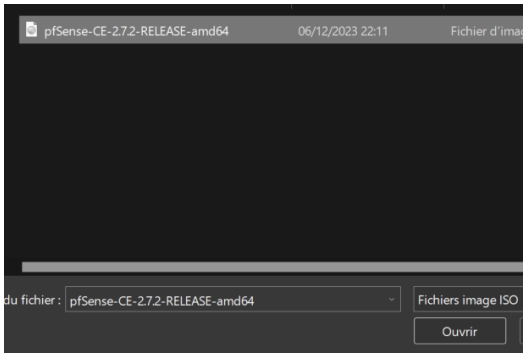
Aujourd'hui nous allons installer un par feu sur nos vm windows server et client pour filtrer les communications douteuses sur nos appareils et ainsi les protéger d'éventuelles attaques extérieures.

Tout d'abord nous allons télécharger l'iso de Pfsense (le firewall que nous allons utiliser)

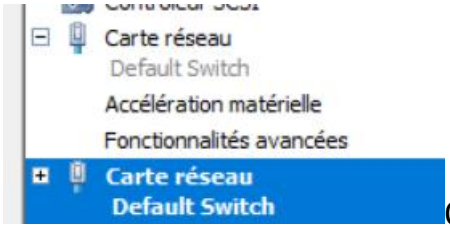


Et nous allons installer l'iso sur une nouvelle vm configuré comme dans les précédents tp à quelques exceptions près :

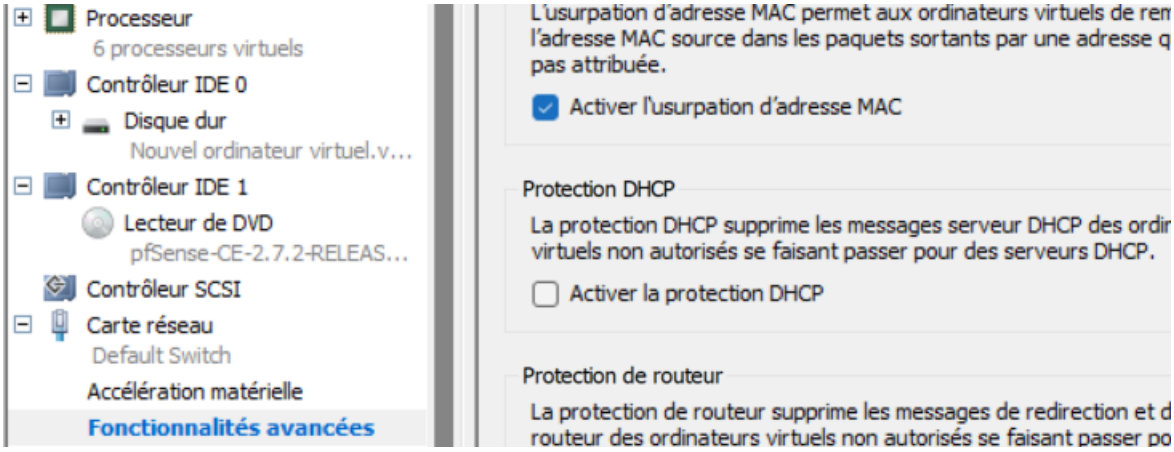
On va utiliser l'iso pfsense pour l'installer directement sur notre vm



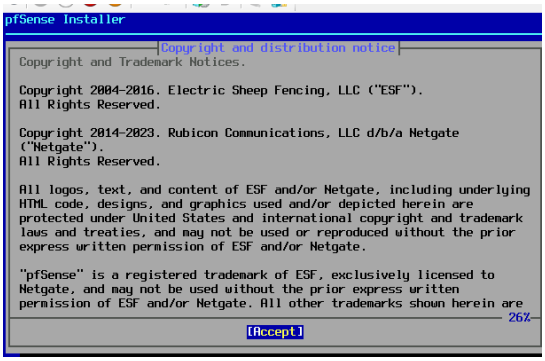
Puis dans les paramètres de notre VM on va y ajouter une deuxieme carte réseau

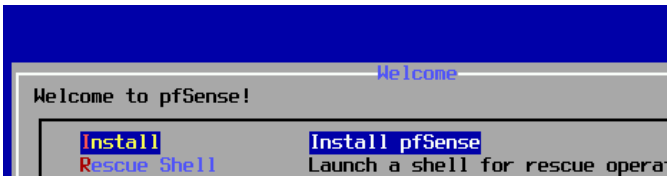


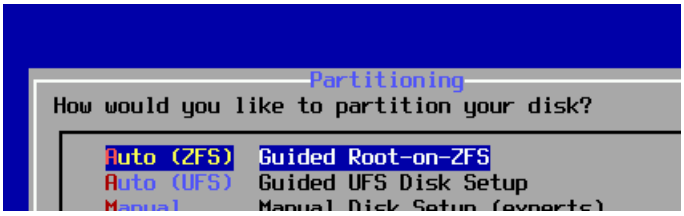
On a bien nos deux cartes et il faut juste dans les fonctionnalités avancées cocher la case d'usurpation d'adresse mac

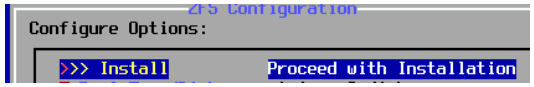


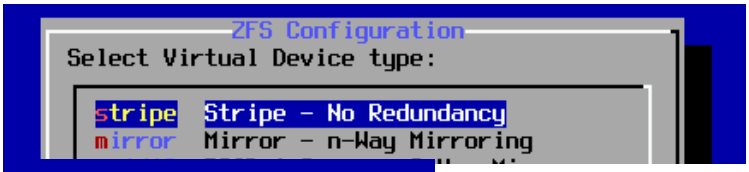
Une fois la vm lancée on va suivre les étapes suivantes :

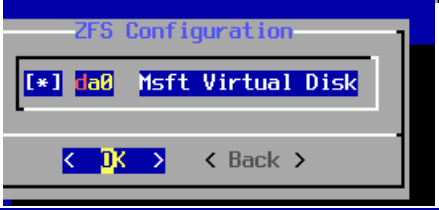




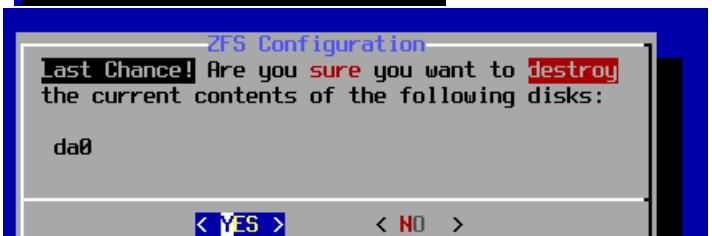




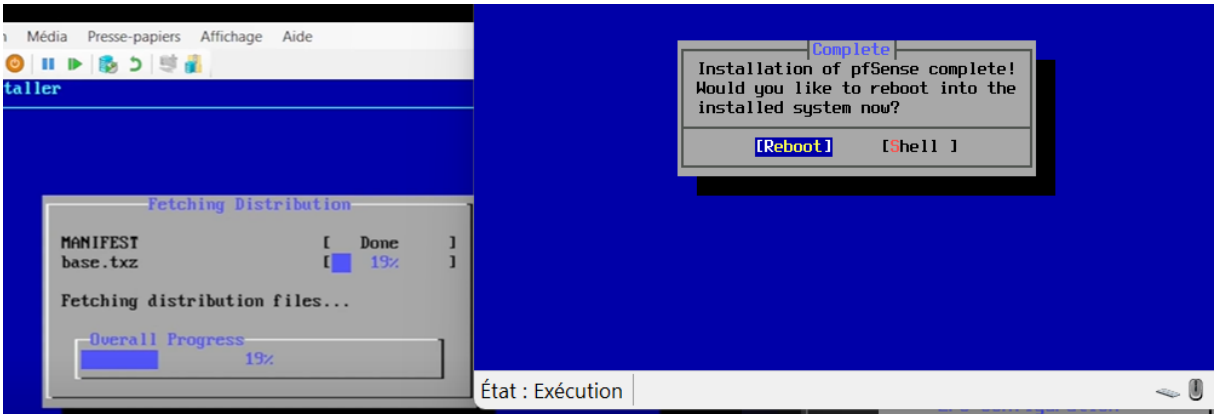




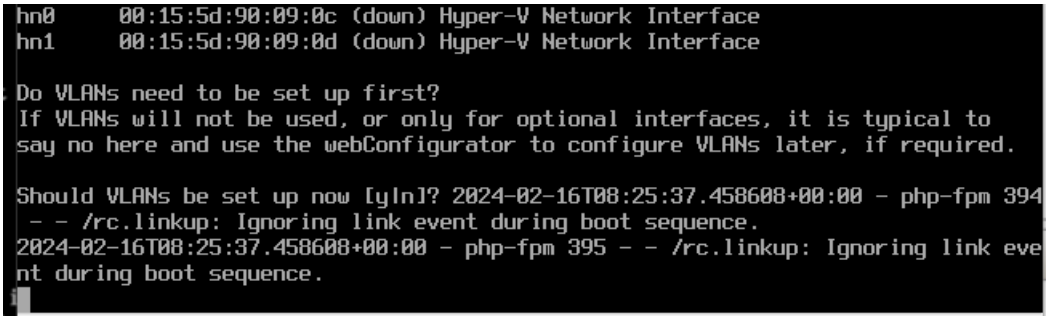
Appuyez sur espace pour sélectionner



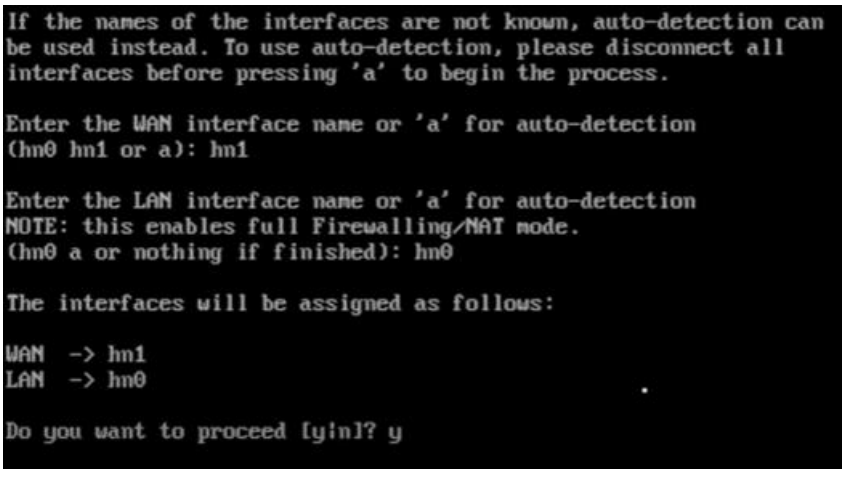
Une fois le téléchargement fais il suffira de reboot le système en sortant l'iso du cycle de démarrage car il est déjà installé.



UN fois relancée une première question nous est posé on répondra simplement non car nous avons une carte réseau physique avec un petit n pour non

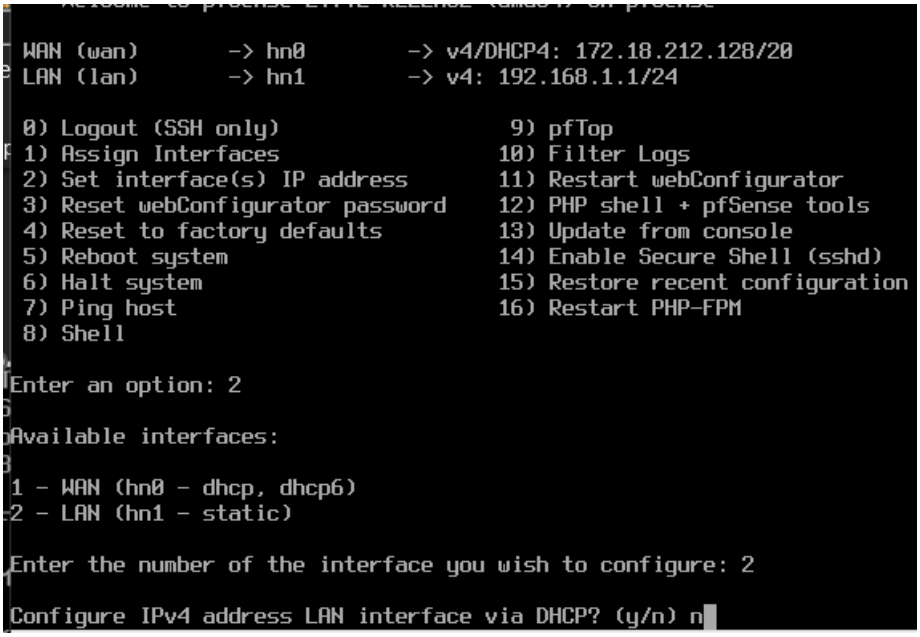


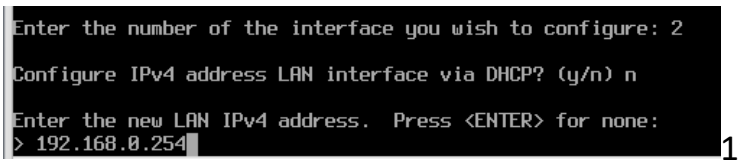
Pour la prochaine question on va attribuer le lan et wan a chaque carte réseau installé hn0 pour le lan et hn1 pour le wan dans notre cas



Une fois fini on pourra voir les ip de nos carte réseaux pour pouvoir y accéder via l'interface web

Puis on va choisir de changer l'adresse ipv4 nous même

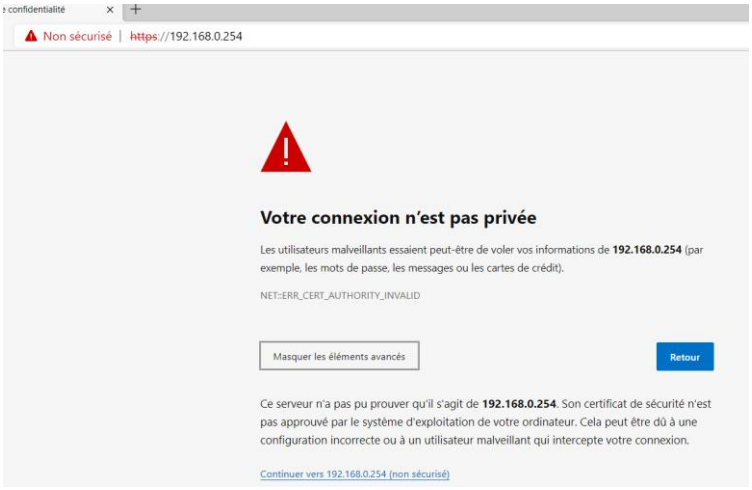


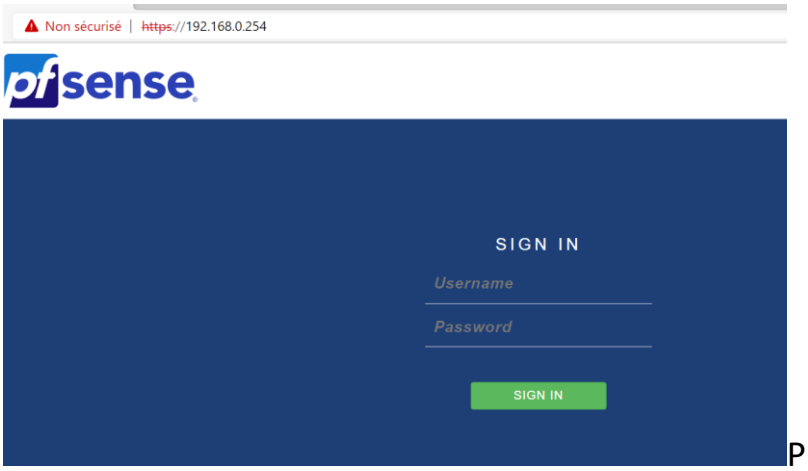


192.168.0.254/24 sera notre ip

Ensuite on dira non aux autres paramètres. Et en faisant entrer on va revenir aux options de bases on peut maintenant se rendre sur une vm connectée à se même réseau pour ce faire on utilisera la vm Windows 10 pro créer dans un tp précédent.

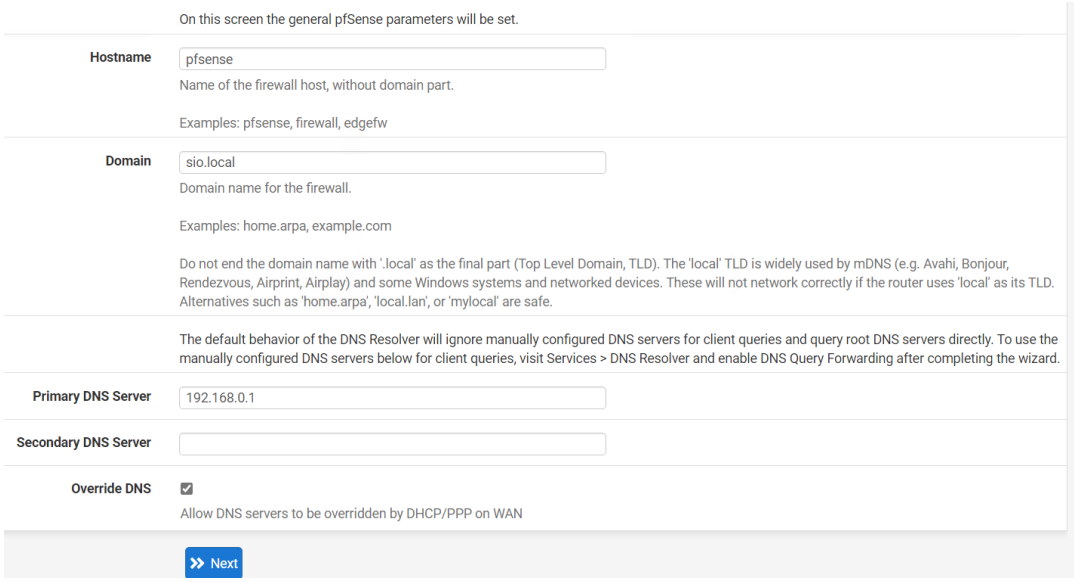
Une fois sur la vm on va ouvrir un navigateur et se rendre sur l'ip correspondante et faire continuer si on est bloqué.





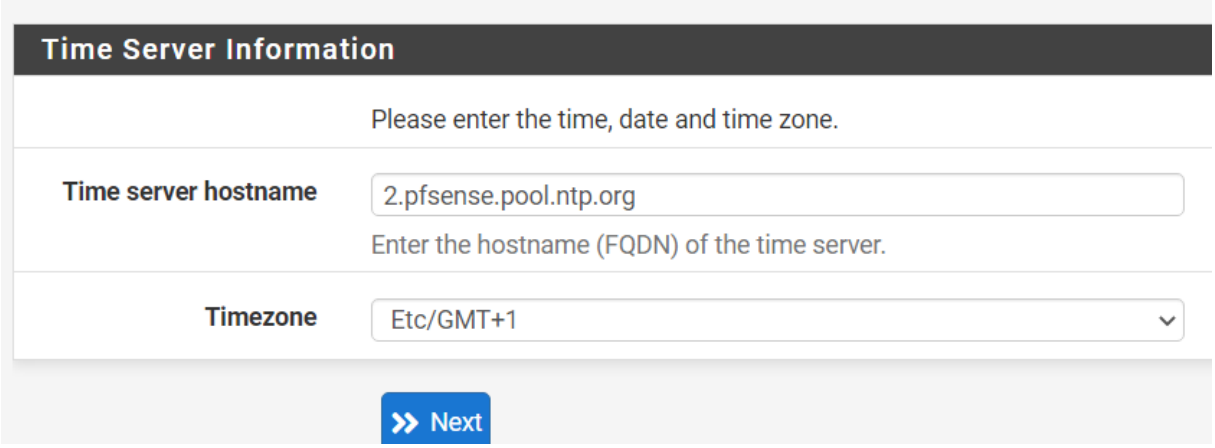
Puis on arrive sur une interface pour se login avec les identifiants par défaut admin et pfsens (changeable si besoin).

Une fois sur la plateforme on va faire suivant et commencer le paramétrage des différentes chose demandé.

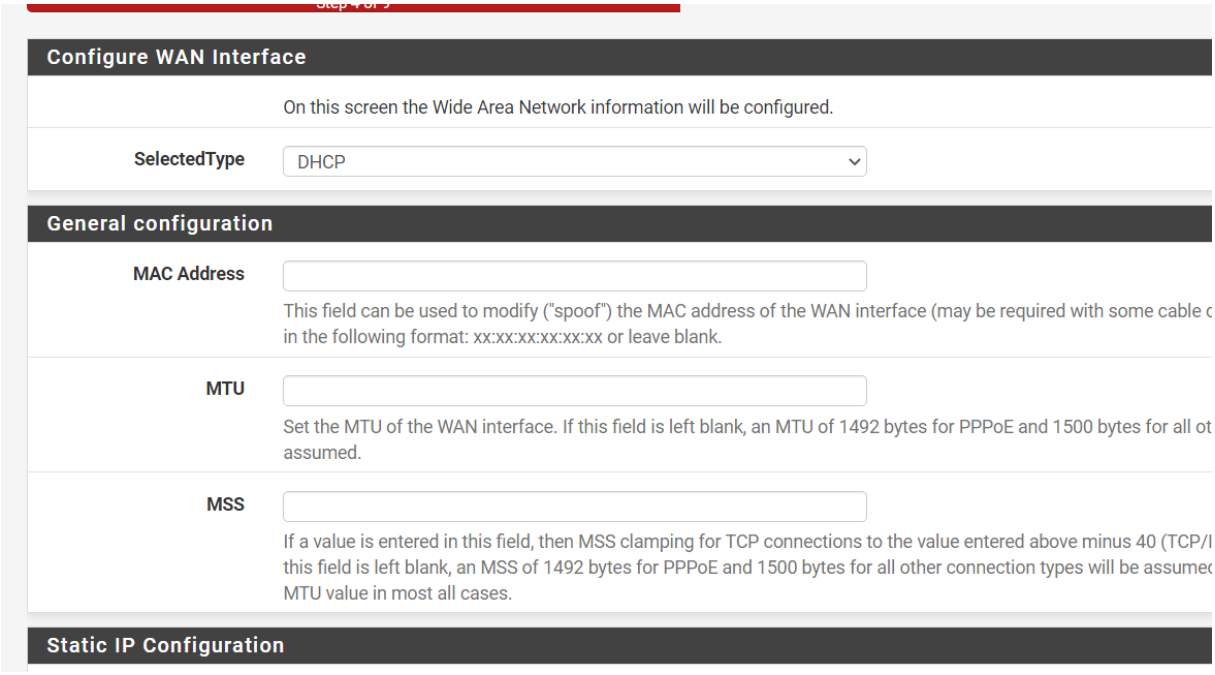


Il a donc fallut remplir le nom du server donc de la vm le nom du domaine active directory et l'adresse de notre dns toutes ces infos qui ont été utilisés les tp précédents.

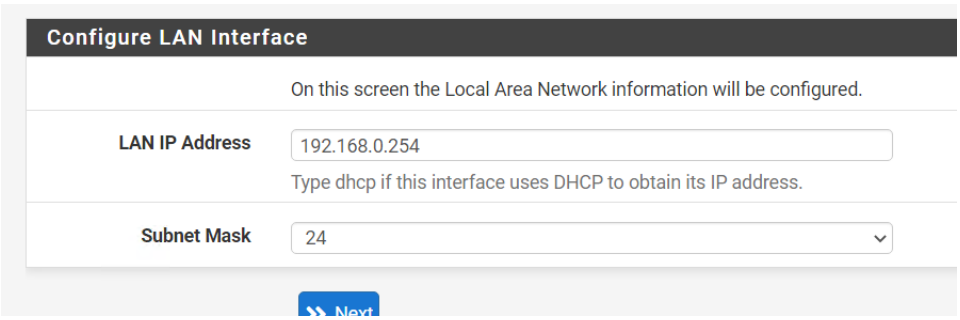
Ensuite on règle l'heure



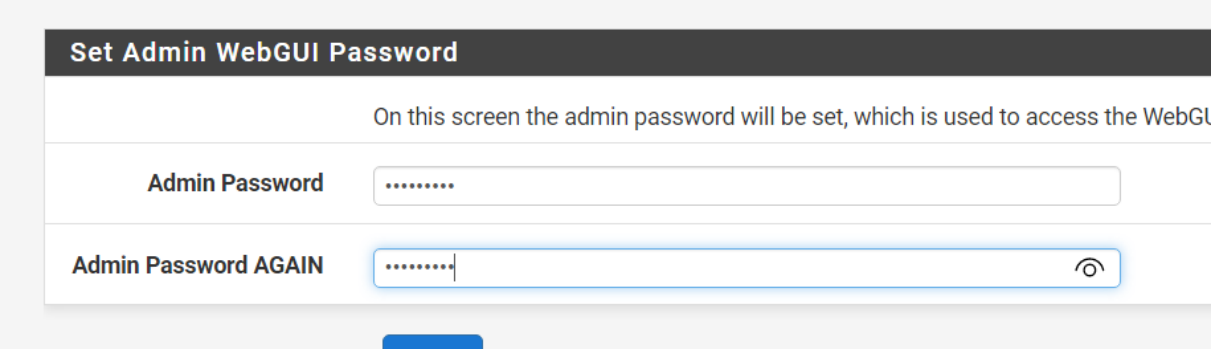
Puis lors de la prochaine étape on ne touchera à rien et on laissera tout en dhcp.



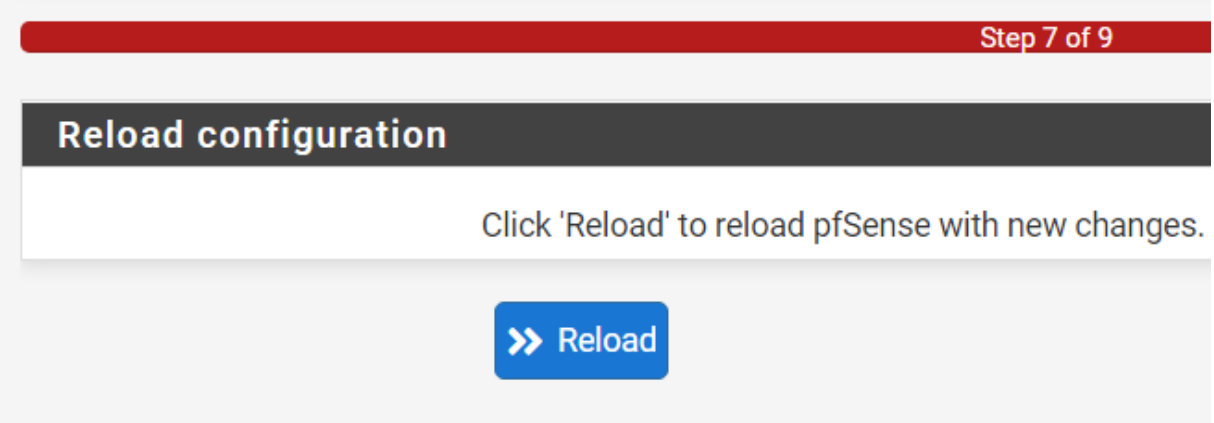
De même pour l'adresse ip lan changée plus tôt.



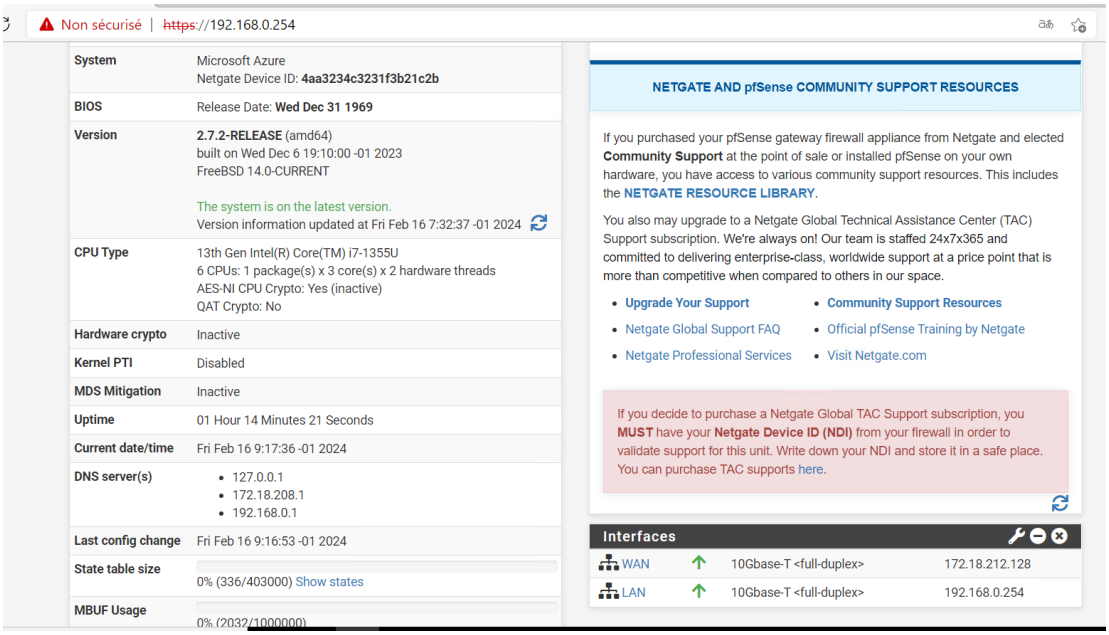
Ensuite on va créer un mot de passe : ici Azerty123 fera l'affaire pour nos test



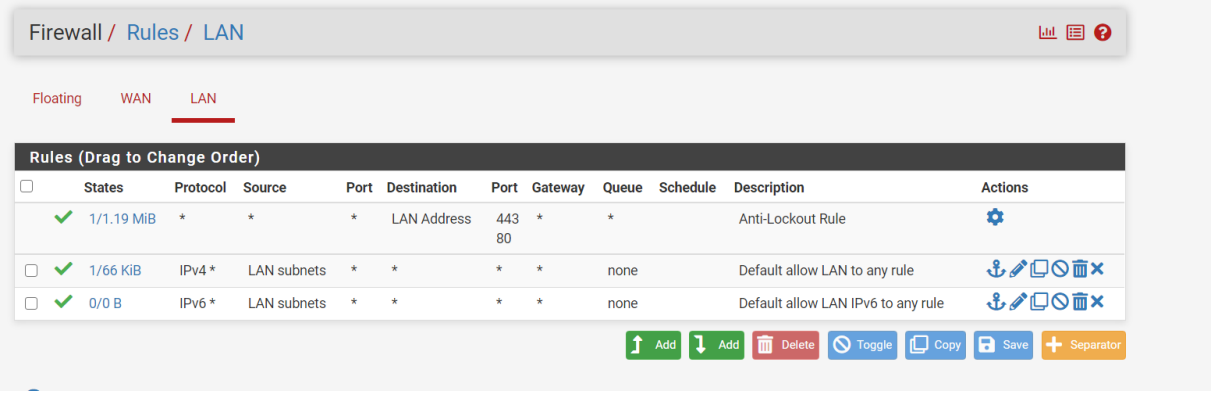
Puis on pourra mettre l'interface à jour



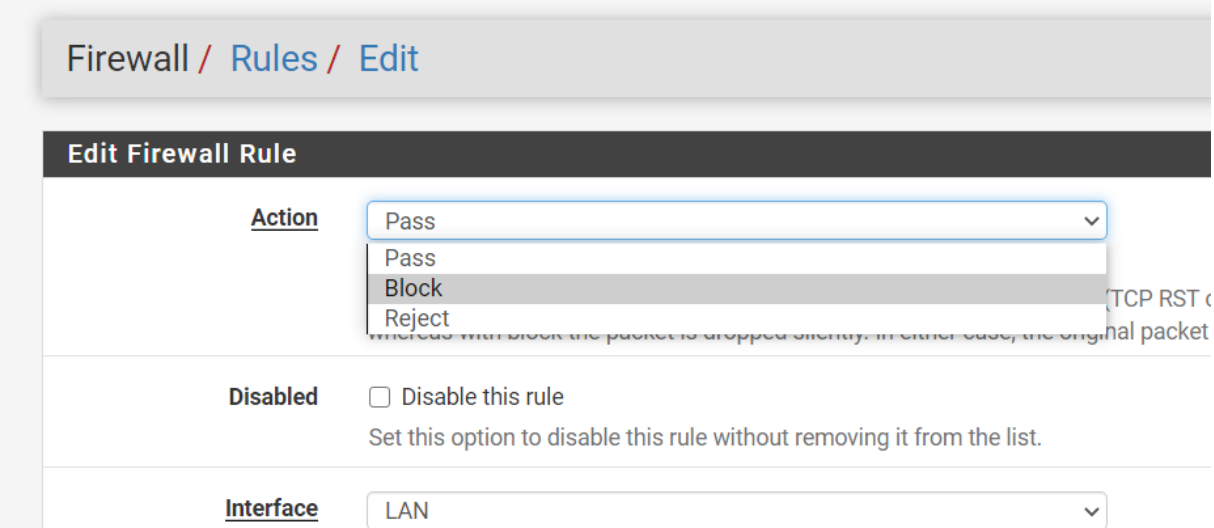
Une fois notre page rechargé on peut voir en bas à droite que nos lan et wan sont bien présent et fonctionnels



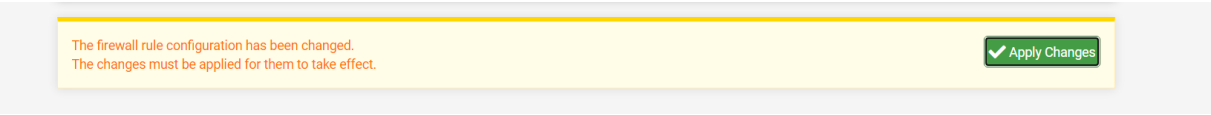
Ensuite on va apporter quelques modifications. On va pour cela modifier les règles par défaut du firewall.



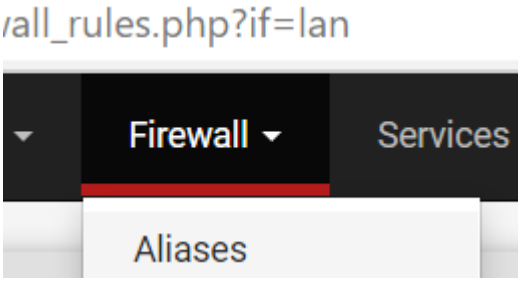
On va déjà bloquer.



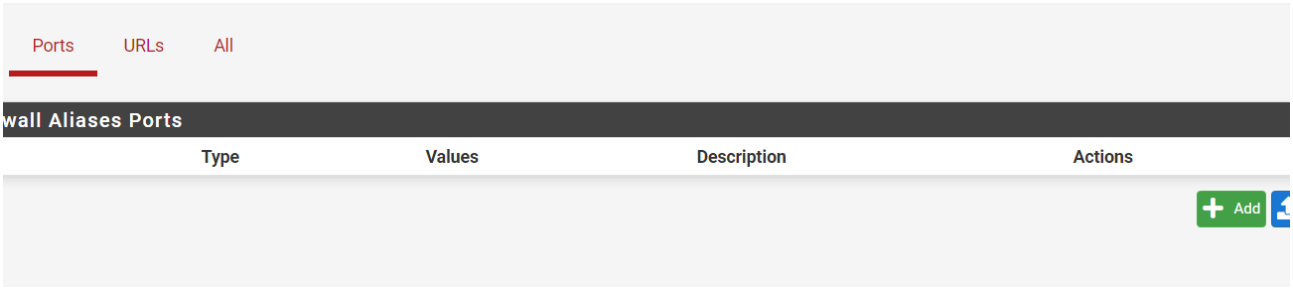
En ipv4 ou 6 puis ne pas oublier d'appliquer les modifications.



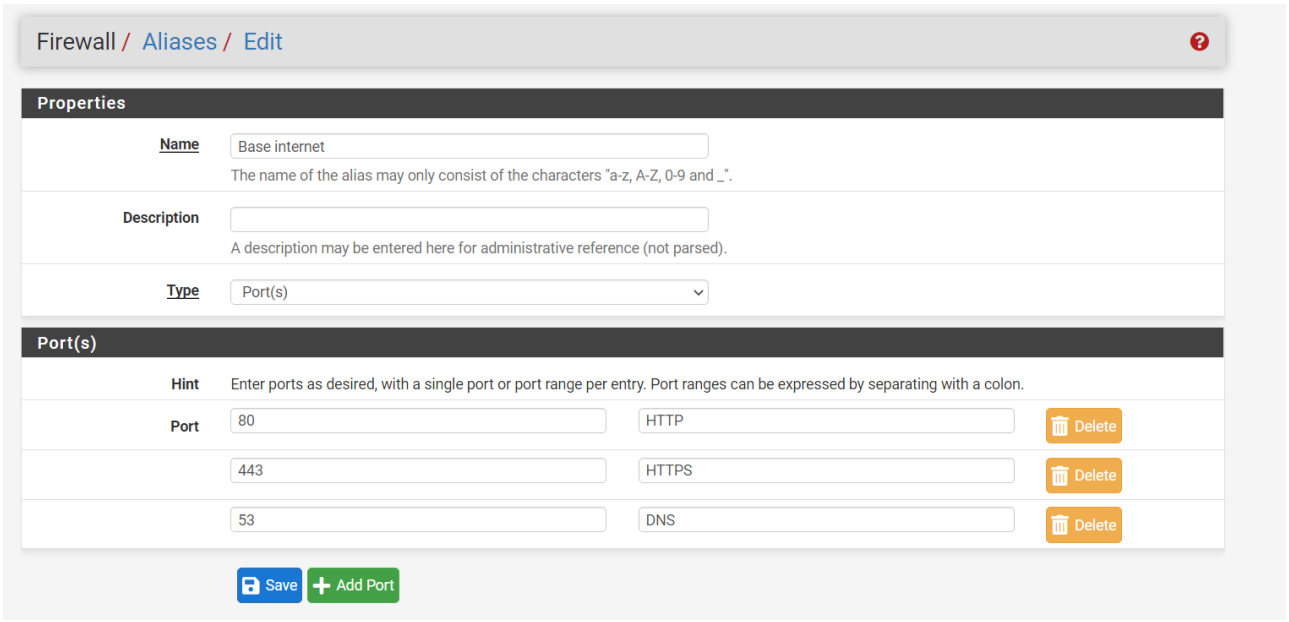
Puis dans firewall aliases on va accepter ce qui nous intéresse.



Dans ports on pourra ajouter ces règles.

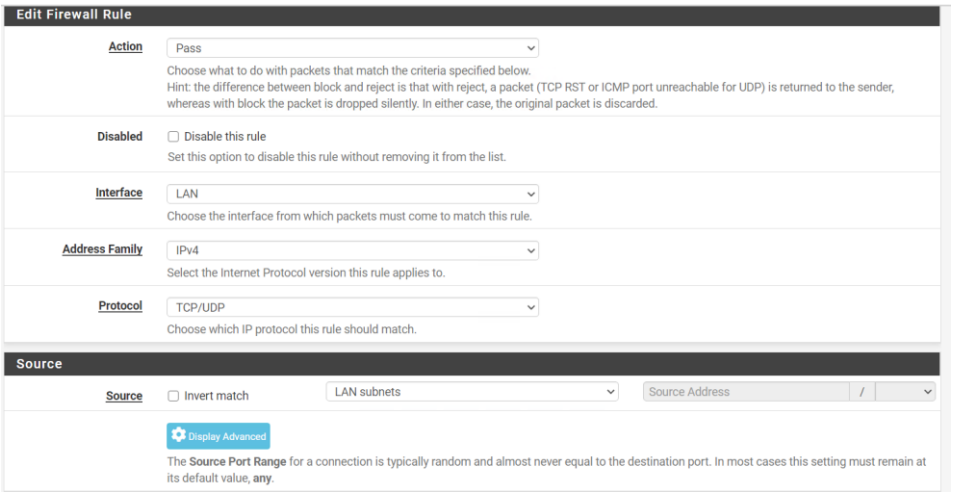


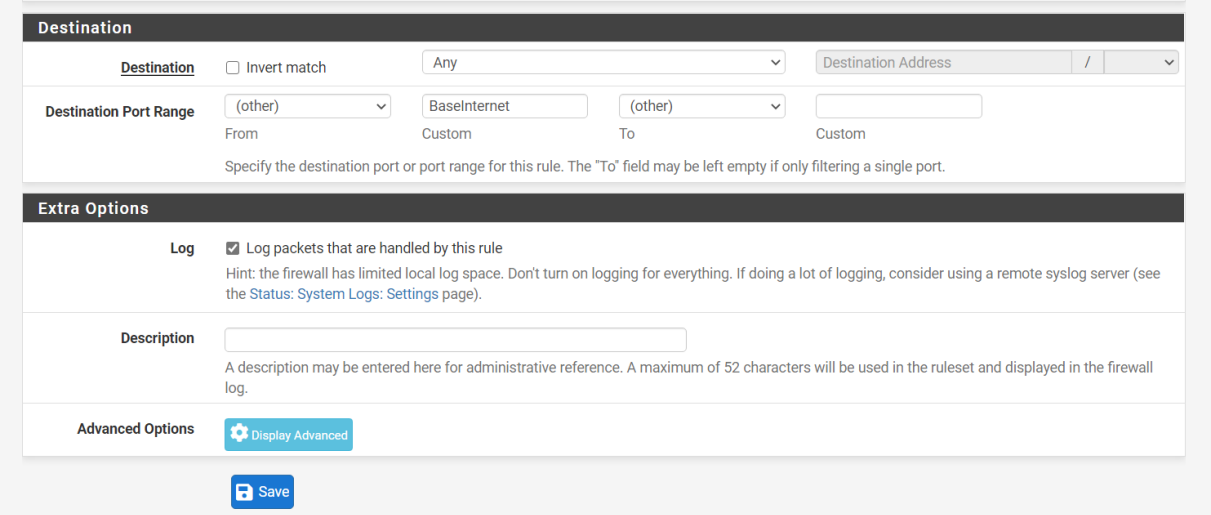
Une fois nos ports ajouté on peut sauvegarder.



Et on va maintenant retourner dans les règle pour en ajouter une qui utilise cet alias.

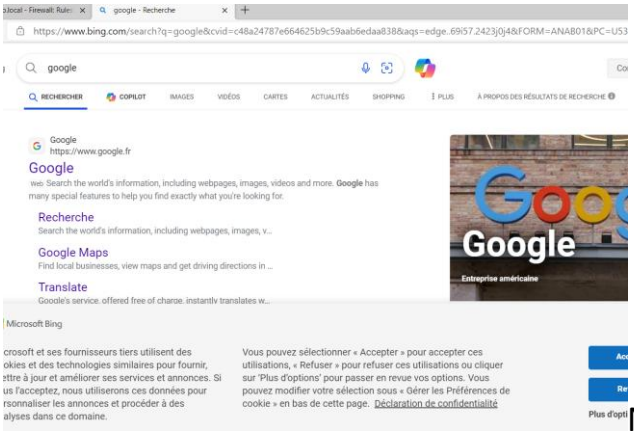
Et il faudra veiller à bien rentrer les bon paramètres suivant :





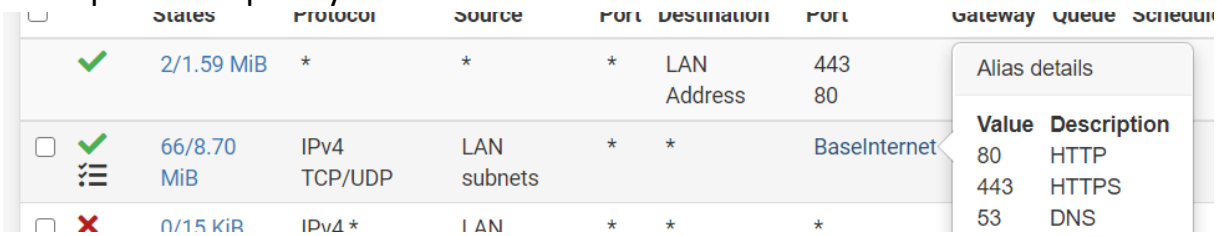
On a donc bien utilisé BaseInternet qui acceptera les bon ports et on applique avant de sauvegarder les changements.

Pour vérifier on fait simplement une recherche google :

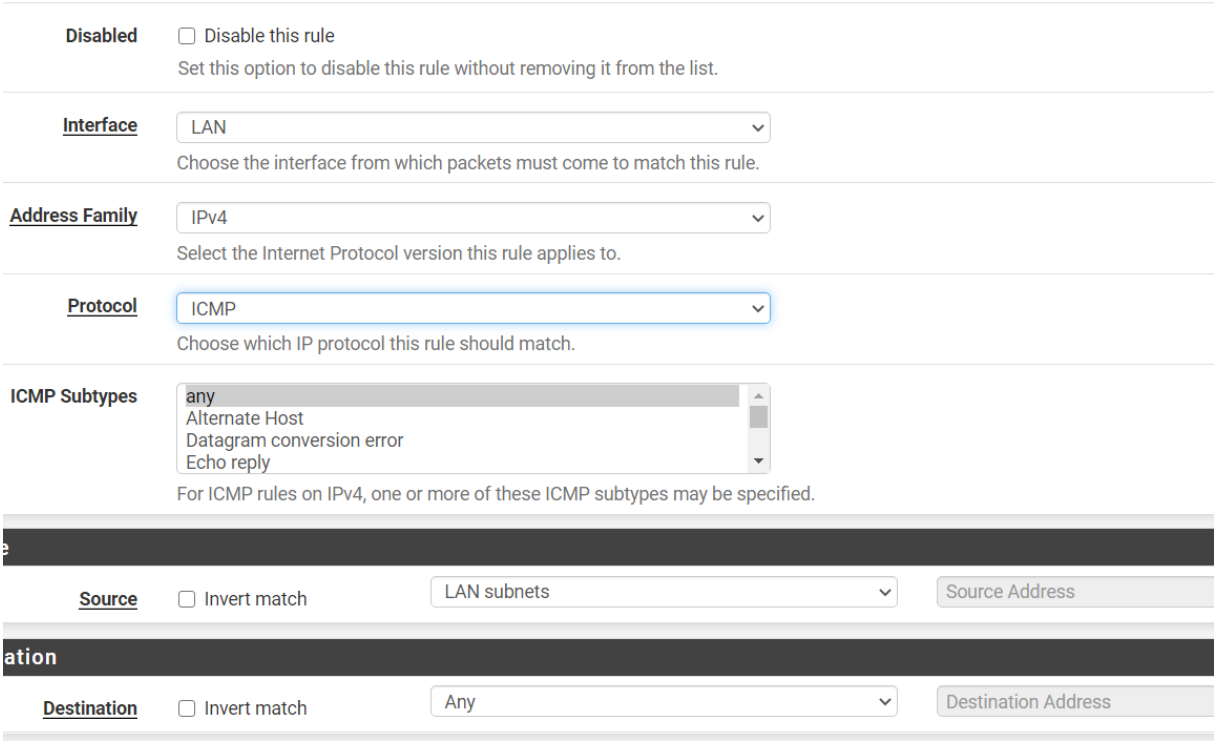


Notre par feu est donc bien fonctionnel

Et on peut voir que il y a eu du trafic



Enfin si on veut autoriser le ping on reffait une règle avec le protocole icmp



et nos ping vont à nouveau fonctionner via le pare feu

Conclusion :

Nous avons donc dans ce tp installé un firewall sous forme de vm et configuré les paramètres de bases sur les deux cartes réseaux lan et wan puis on lui a attribué une adresse ip pour se connecter à son interface web et y ajouter le filtrage en fonction des protocoles lors de la navigations sur le web pour sécuriser le tout. Mon premier pare-feu est installé !