MISE EN PLACE ET CONFIGURATION DE SNORT SOUS PFSENSE

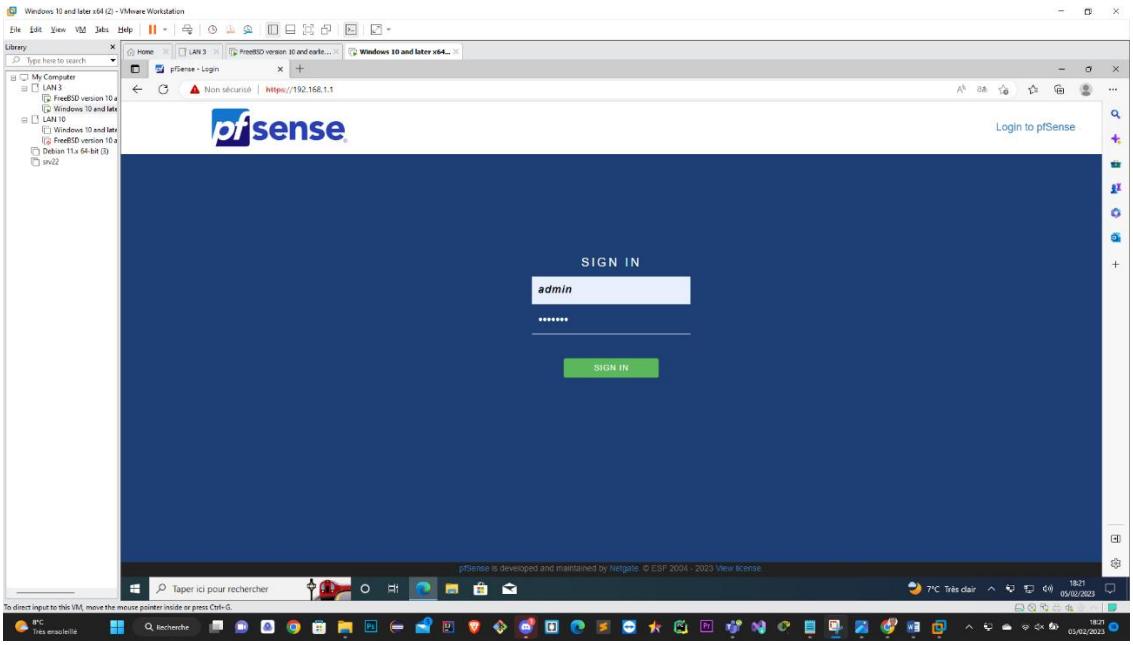
1. *INTRODUCTUON*
2. *INSTALLER, CONFIGURER SNORT ET CREER SON USER SNORT*
3. *TEST D'INTRUSION*

1. INTRODUCUTION

Snort est le premier système de prévention des intrusions (IPS) Open Source au monde. Snort IPS utilise une série de règles qui aident à définir l'activité réseau malveillante et utilisent ces règles pour trouver les paquets qui correspondent à celles-ci et génère des alertes pour les utilisateurs.

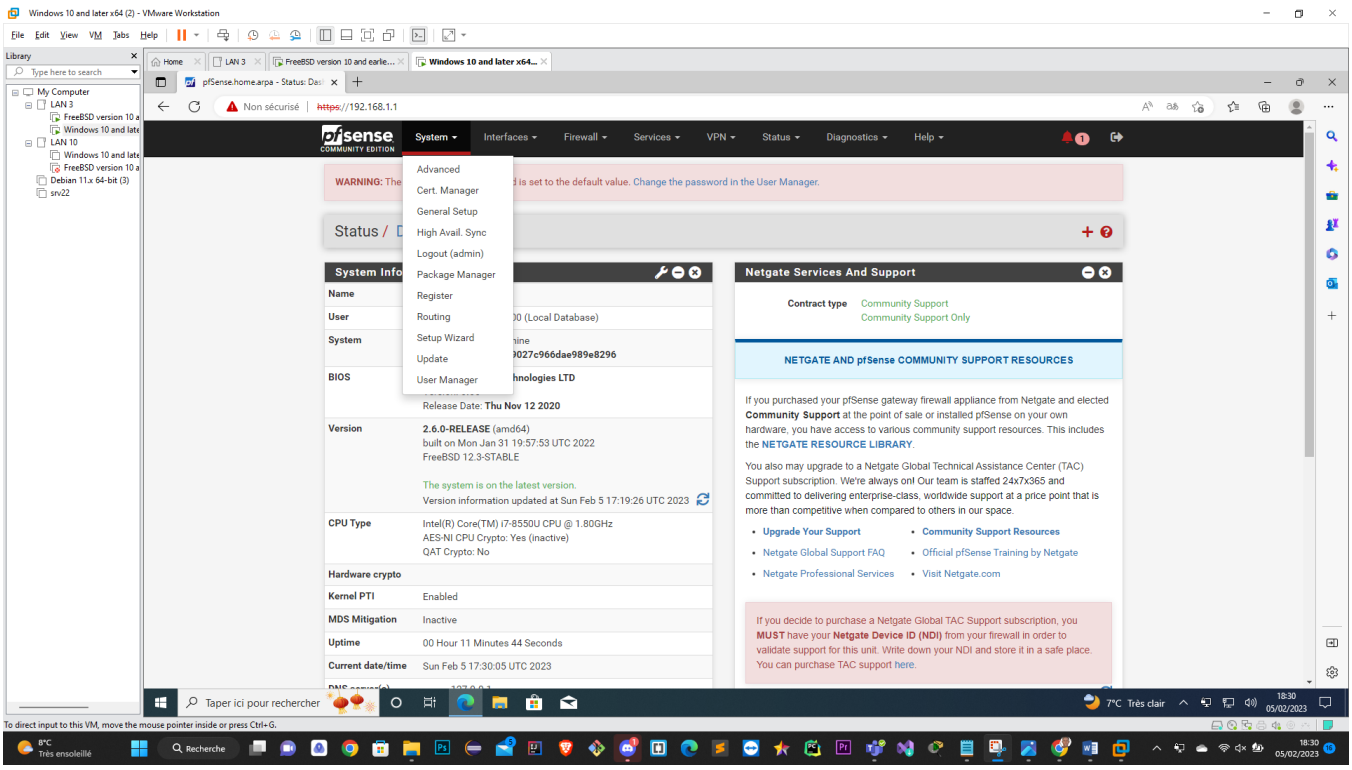
Snort peut également être déployé en ligne pour arrêter ces paquets. Snort a trois utilisations principales: **En tant que renifleur de paquets comme tcpdump, en tant qu'enregistreur de paquets - ce qui est utile pour le débogage du trafic réseau, ou il peut être Utilisé comme un système complet de prévention des intrusions sur le réseau**. Snort peut être téléchargé et configuré pour le personnel et l'utilisation professionnelle.

2. INSTALLER ET CONFIGURER SNORT

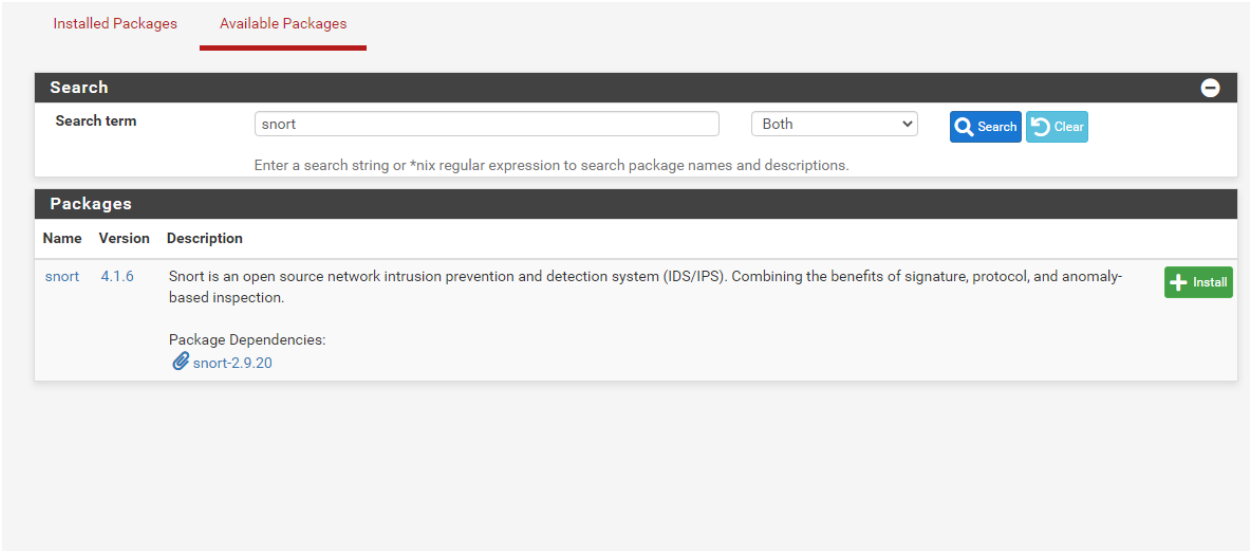


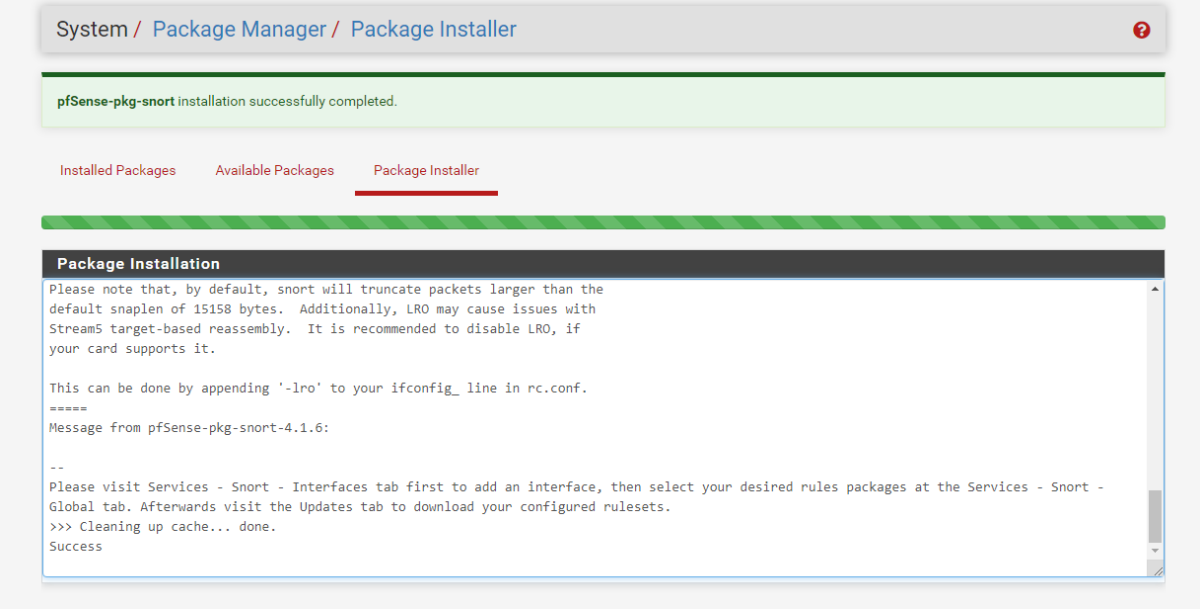
Par défaut le paquet SNORT n'est installé sur PFSense il faut donc le télécharger puis l'installer.

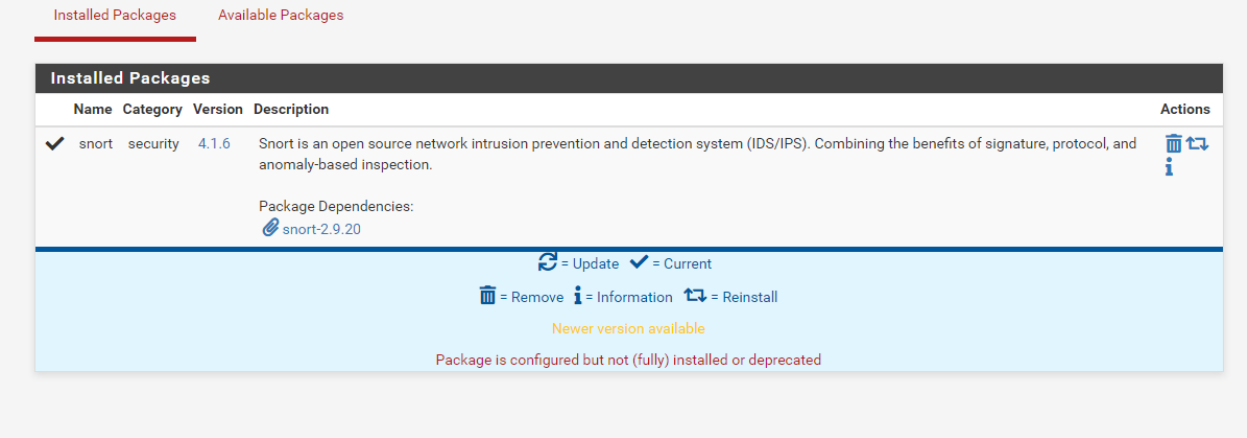
Une fois dans PFSense on va dans le système ensuite Package manager pour voir les paquets installés et les paquets disponible.



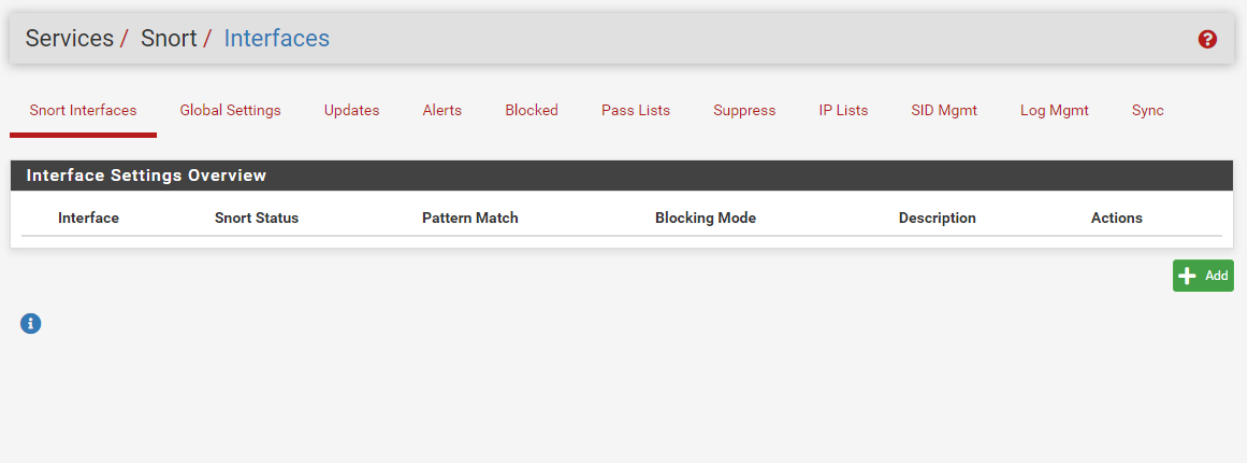
SNORT se trouvera donc dans les paquets disponibles, on ira donc le chercher pour l'installer



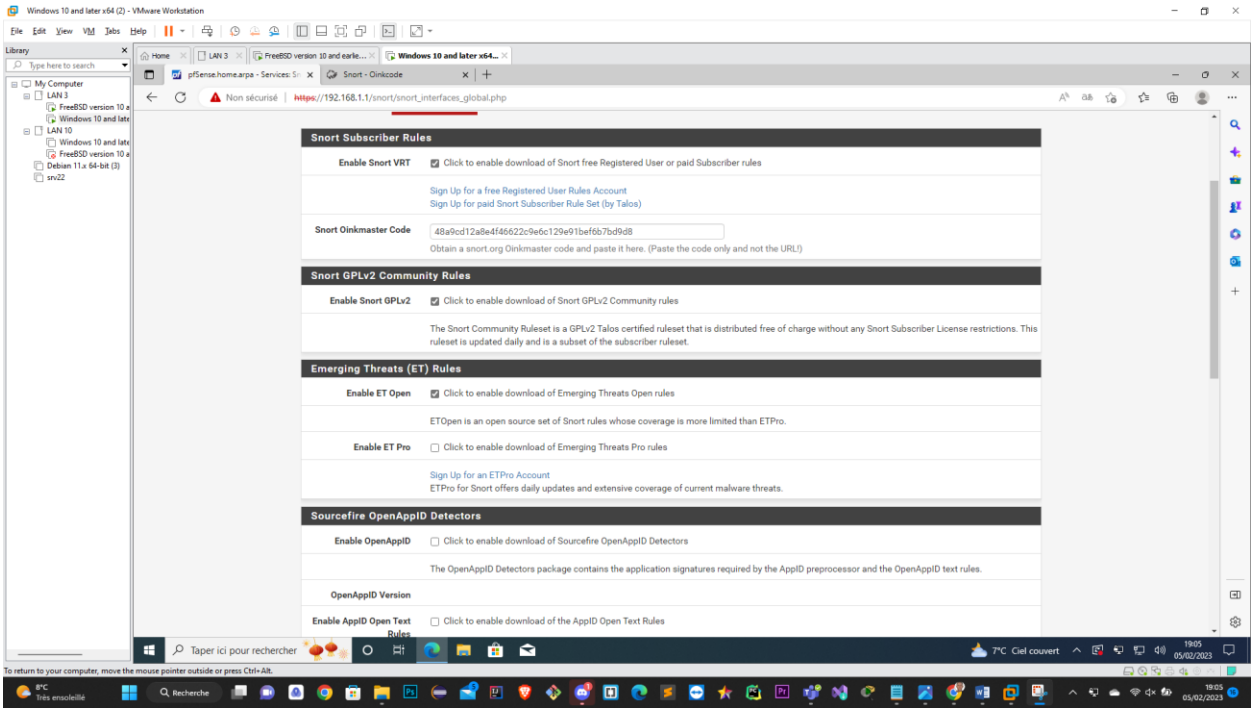

System / Package Manager / Package Installer
pfSense-pkg-snort installation successfully completed.
Installed Packages
Available Packages
Package Installer
Package Installation
Please note that, by default, snort will truncate packets larger than the
default snaplen of 15158 bytes. Additionally, LRO may cause issues with
Stream5 target-based reassembly. It is recommended to disable LRO, if
your card supports it.
This can be done by appending '-lro' to your ifconfig_ line in rc.conf.
=====
Message from pfSense-pkg-snort-4.1.6:
--
Please visit Services - Snort - Interfaces tab first to add an interface, then select your desired rules packages at the Services - Snort - Global tab. Afterwards visit the Updates tab to download your configured rulesets.
>>> Cleaning up cache... done.
Success

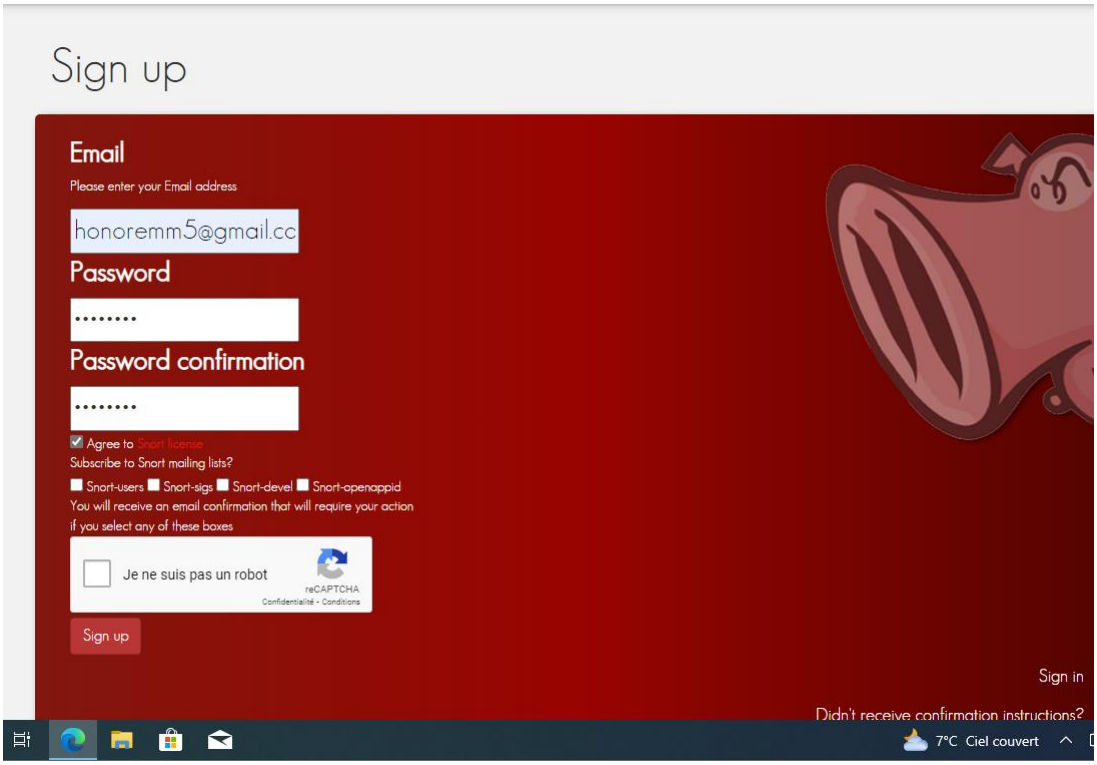

Installed Packages
Available Packages
Installed Packages
Name Category Version Description Actions
snort security 4.1.6 Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.
Package Dependencies:
snort-2.9.20
= Update = Current
= Remove = Information = Reinstall
Newer version available
Package is configured but not (fully) installed or deprecated

Après l'installation du paquet Snort nous procèderons à l'ajout de service Snort, donc nous irons à l'onglet service puis sectionner Snort.



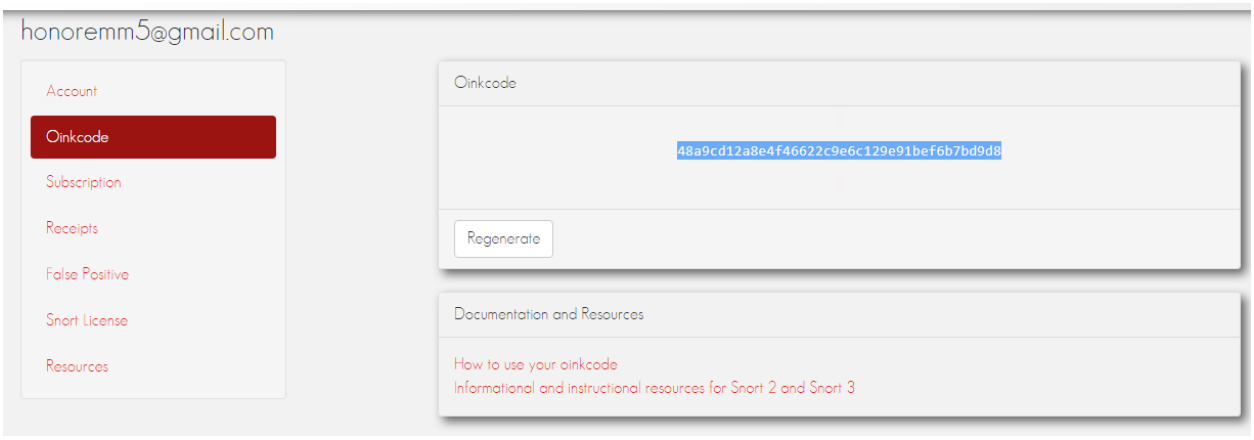
Et accéder au Global Setting, la première étape est donc d'activer le téléchargement de règles gratuites, en cochant la première case (Enable Snort VRT), on nous demandera **L'Oinkmaster Code** qui est une clé qu'on devra aller chercher sur Snort.org Et ensuite nous pouvons cocher les cases Enable Snort GPLv2 pour les règles communautaires et Enable ET Open.





Snort.org

Après création et confirmation de mon compte Snort j'ai pu avoir la clé Oinkmaster code



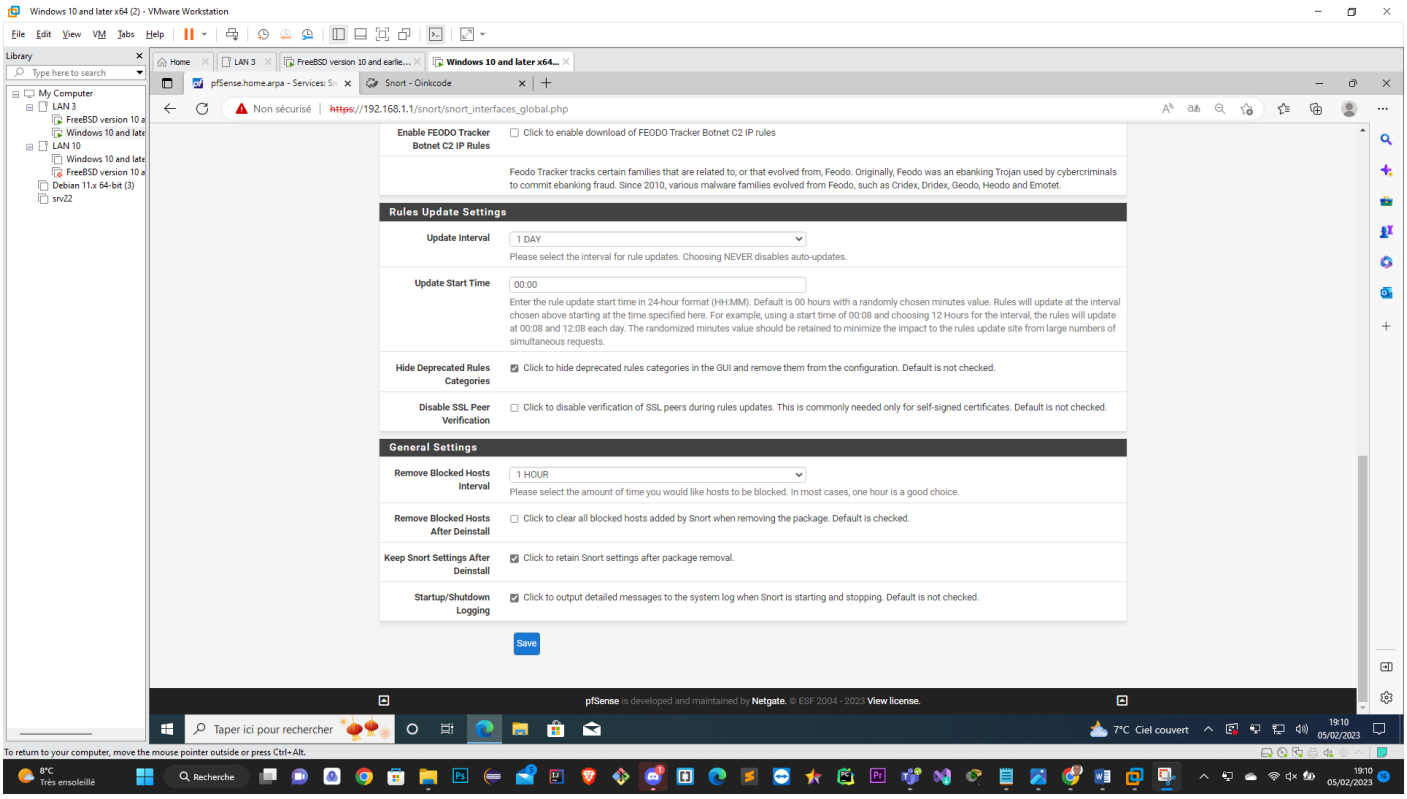
Dans la zone Rules Update Settings on effectue les config ci-dessous :

Update Interval: 1 Day

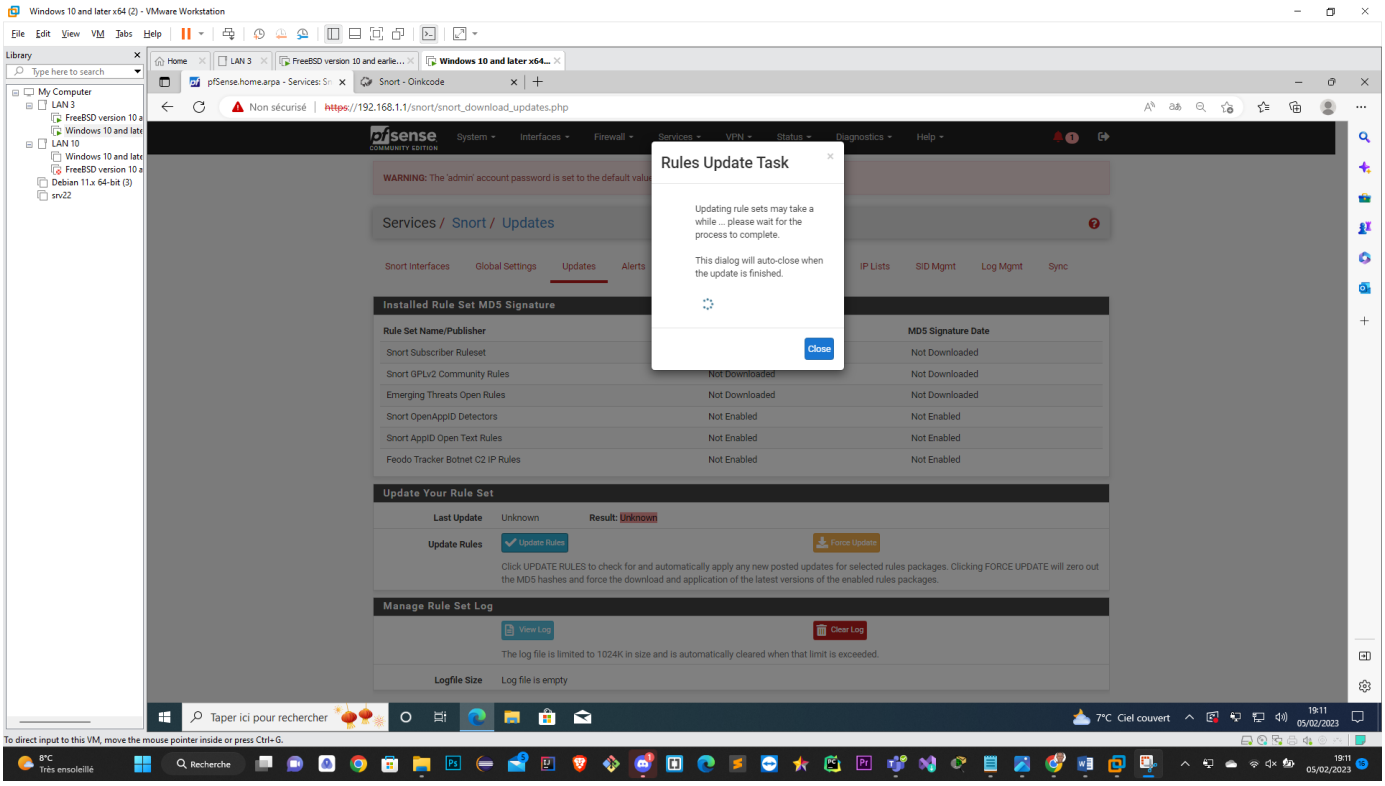
Update Start Time: 00 :00

On coche Keep Snort Settings After Deinstall et Startup/Shutdown Logging, pour que quand on désinstallera Snort on garde les paramètres de configuration et avoir les log

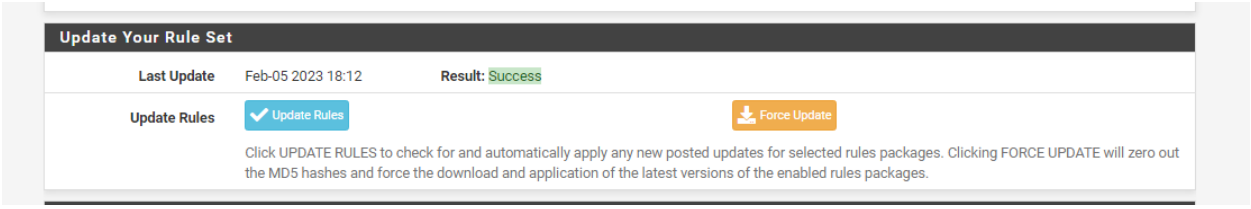
Et dans les paramètres généraux on met 1h pour supprimer l'intervalle des hôtes bloqués.



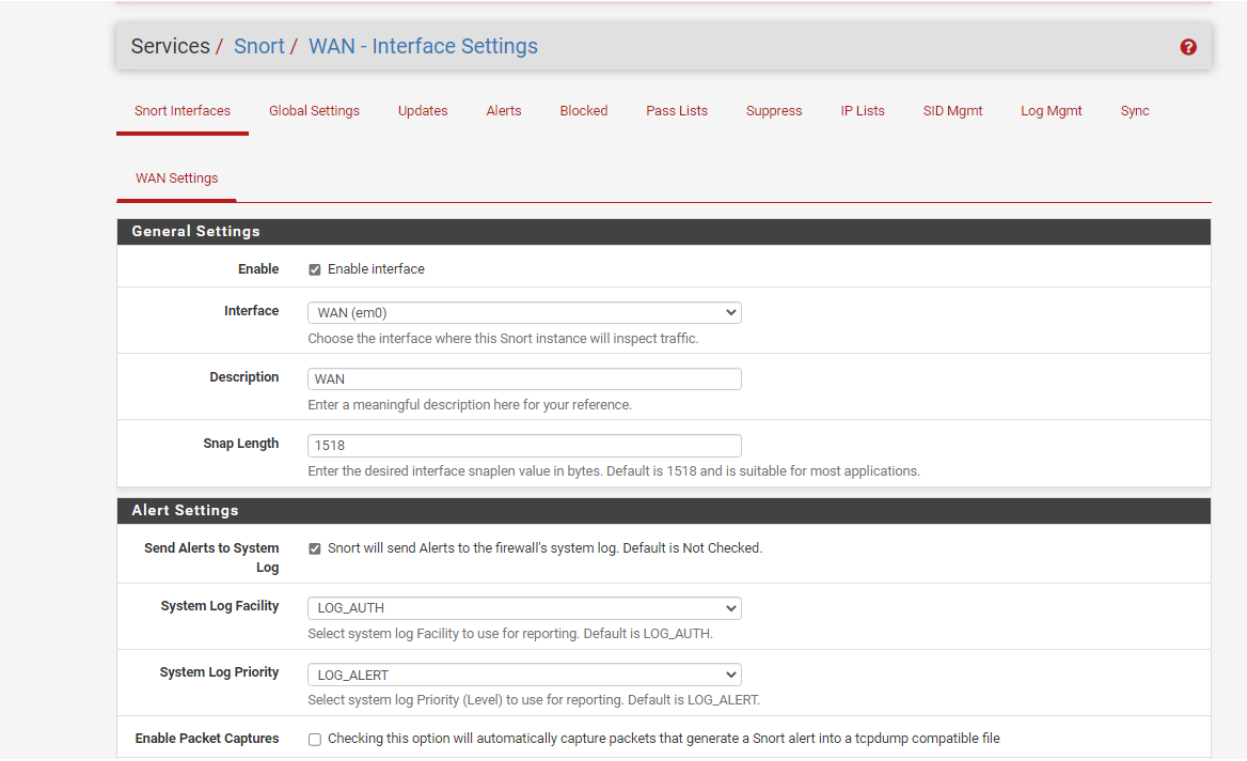
Et on poursuivra dans l'onglet mise à jour pour cliquer sur le bouton règle de mise à jour pour mettre à jour les règles Snort.

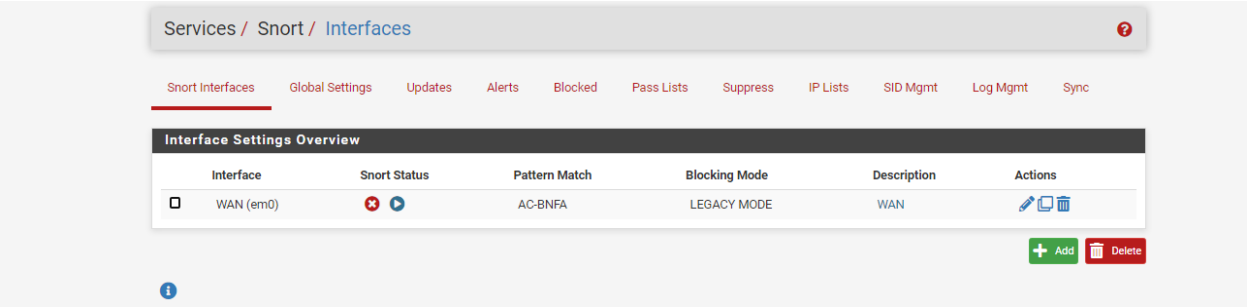


Patientez 1 à 2 minutes pendant la mise à jour

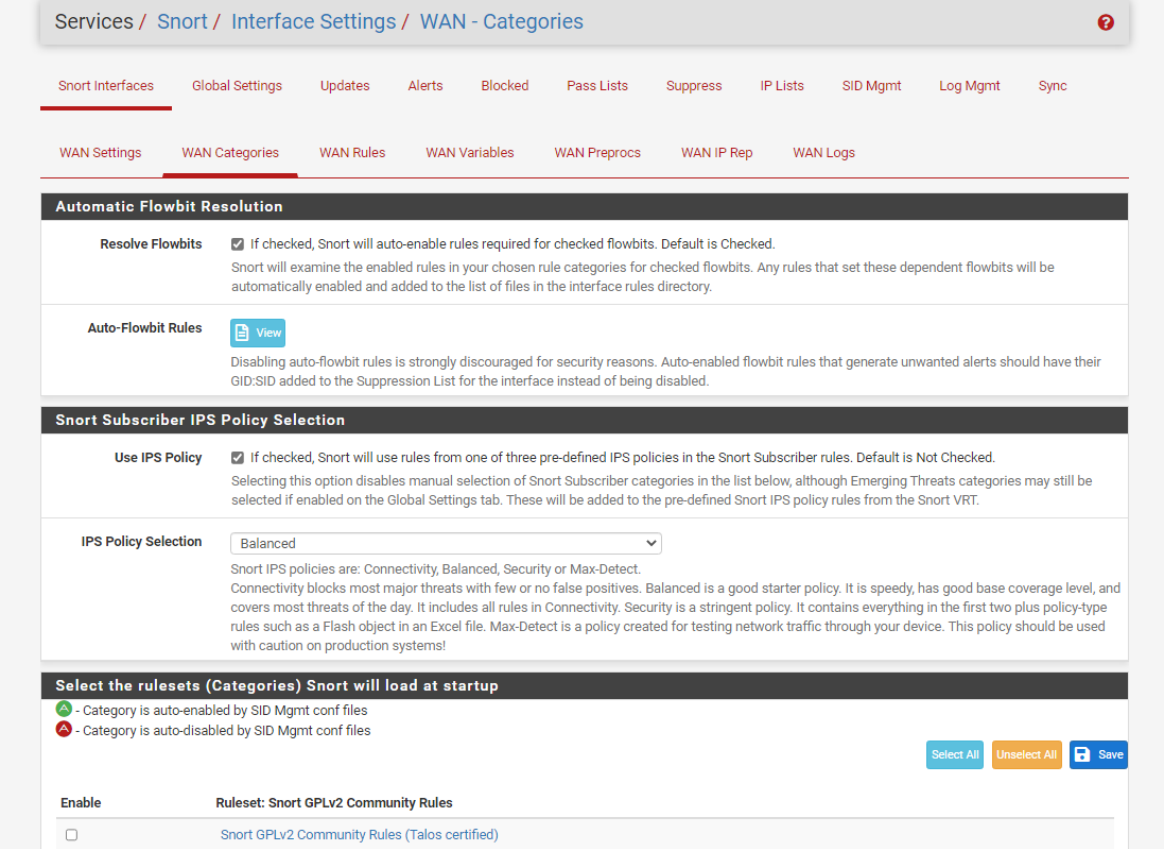


Après mise à jour de règles on va sur l'onglet Snort Interfaces pour ajouter l'interface à surveiller, on laissera notre WAN et les autres paramètres par défaut.





Après l'ajout de l'interface WAN on va l'éditer pour ajouter la politique IPS

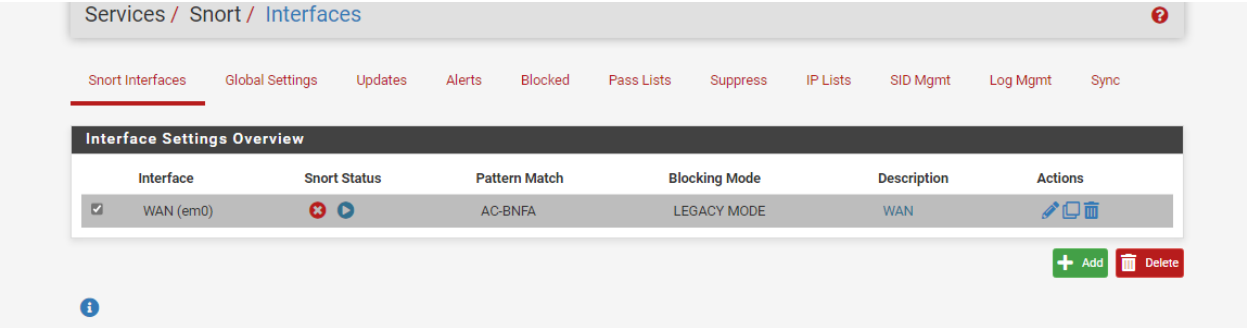


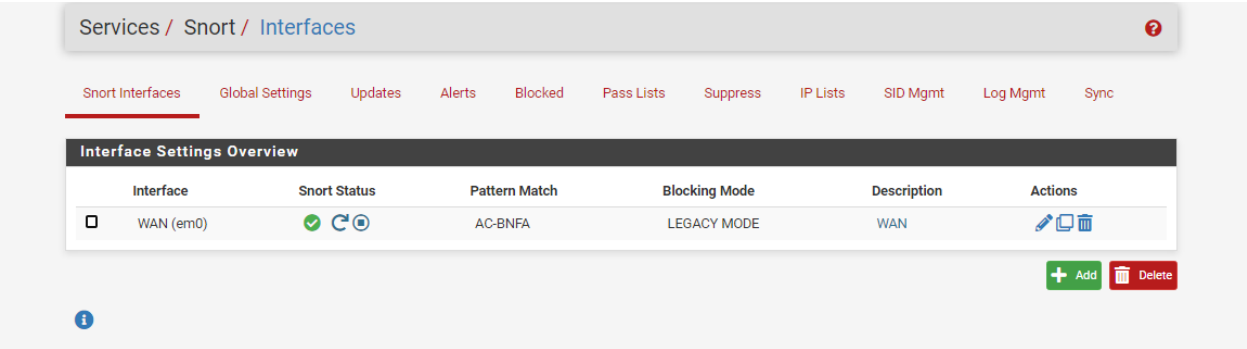
Les politiques Snort IPS sont Connectivity, Balanced, Sécurity et Max-Detect:

- **Connectivity** : bloque la plupart des menaces majeures avec peu ou pas de faux positifs.
- **Balanced** : est une bonne politique de départ. Il est rapide, a un bon niveau de couverture de base et couvre la plupart des menaces. Il inclut toutes les règles de Connectivité.
- **Sécurity** : est une politique stricte. Il contient tout ce qui se trouve dans les deux premiers plus les règles de type politique telles qu'un objet Flash dans un fichier Excel.
- **Max-Detect** : est une stratégie créée pour tester le trafic réseau via votre appareil. Cette politique doit être utilisée avec prudence sur les systèmes de production !

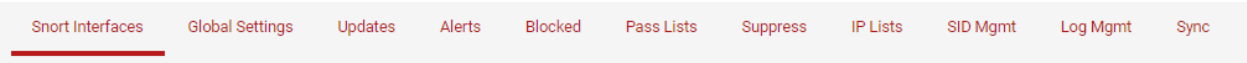
Pour notre travail on a opté pour la politique **Balanced**

Et ensuite on passera au démarrage de l'interface



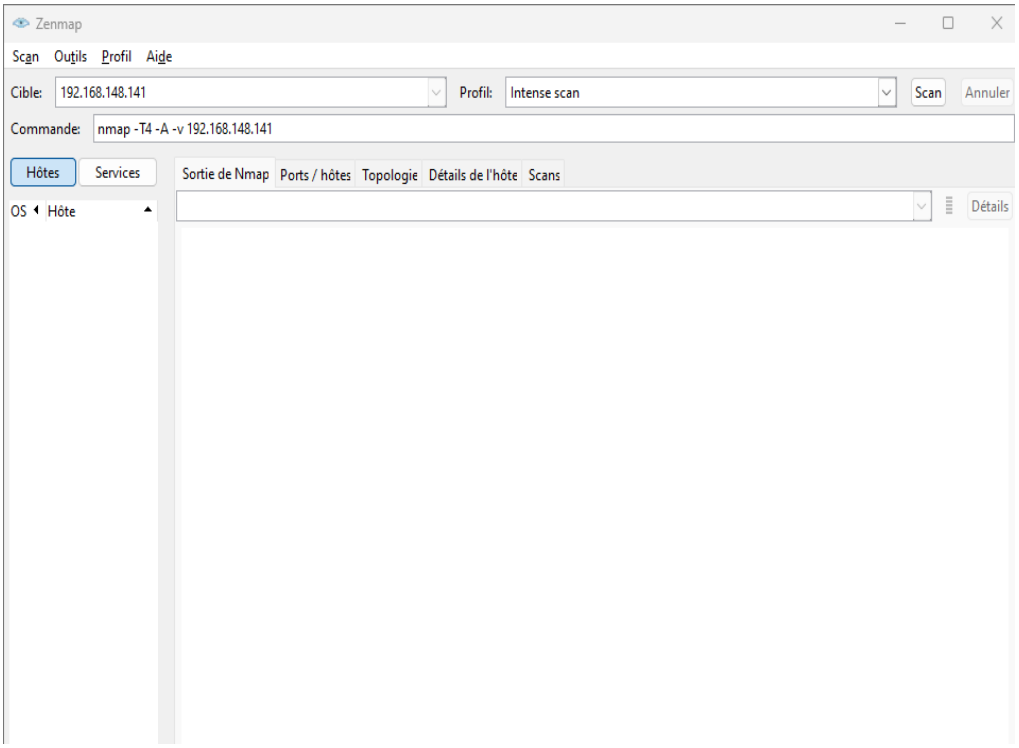


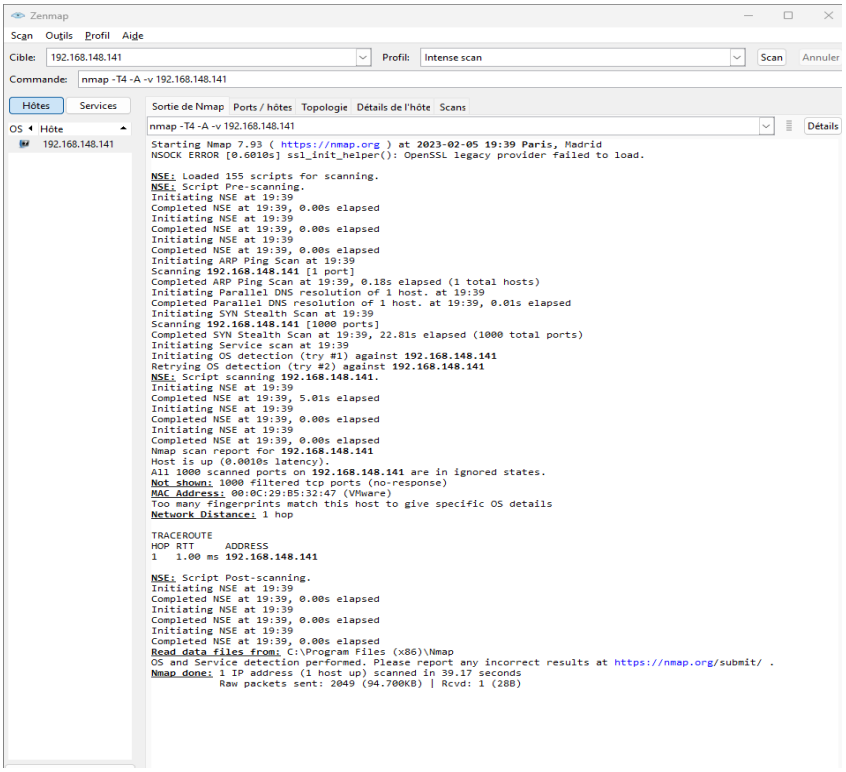
Et sur cette image on voit où les alertes et les adresses bloquées vont s'afficher



3. TEST D'INTRUSION

A l'aide de notre PC physique on installera l'utilitaire Zenmap qui nous aidera à scanner le port de notre PFSense qui a l'adresse 192.168.148.141/24.





Et pour finir quand on rentrera dans notre PFSense on verra l'alerte et l'adresse IP de notre machine physique qui sera bloquée.