Contexte GSB

Le laboratoire Galaxy Swiss Bourdin est issu de la fusion entre le géant américain Galaxy et le conglomérat européen Swiss Bourdin, lui-même déjà union de trois petits laboratoires.En 2009, les deux géants pharmaceutiques unissent leurs forces pour créer un leader de ce secteur industriel. L'entité GSB Europe a établi son siège administratif à Paris.Le siège social de la multinationale est situé à Philadelphie, Pennsylvanie, aux Etats-Unis.La France a été choisie comme témoin pour l'amélioration du suivi de l'activité de visite.

Besoins :

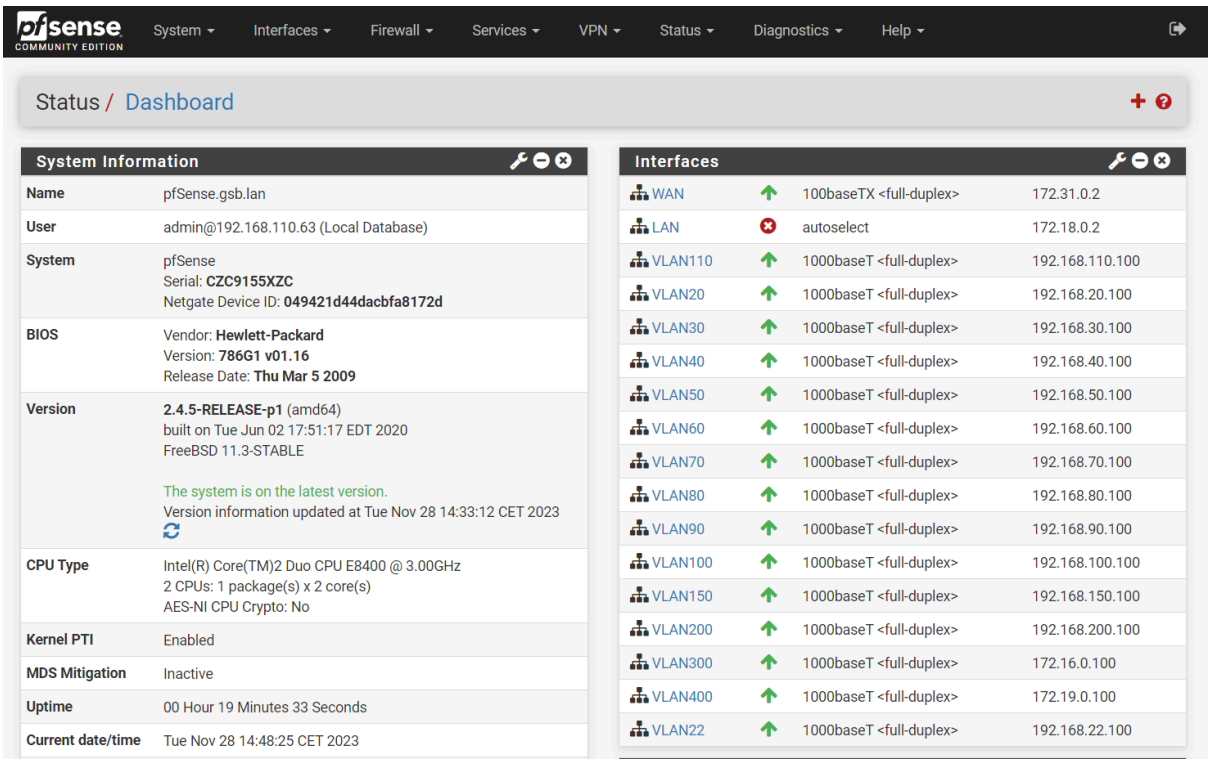
Depuis la réorganisation de GSB l'entreprise fonctionne bien et a connu une hausse de son activité. Suite à cela Galaxy Swiss Bourdin a décidé de mettre en place

Solution:

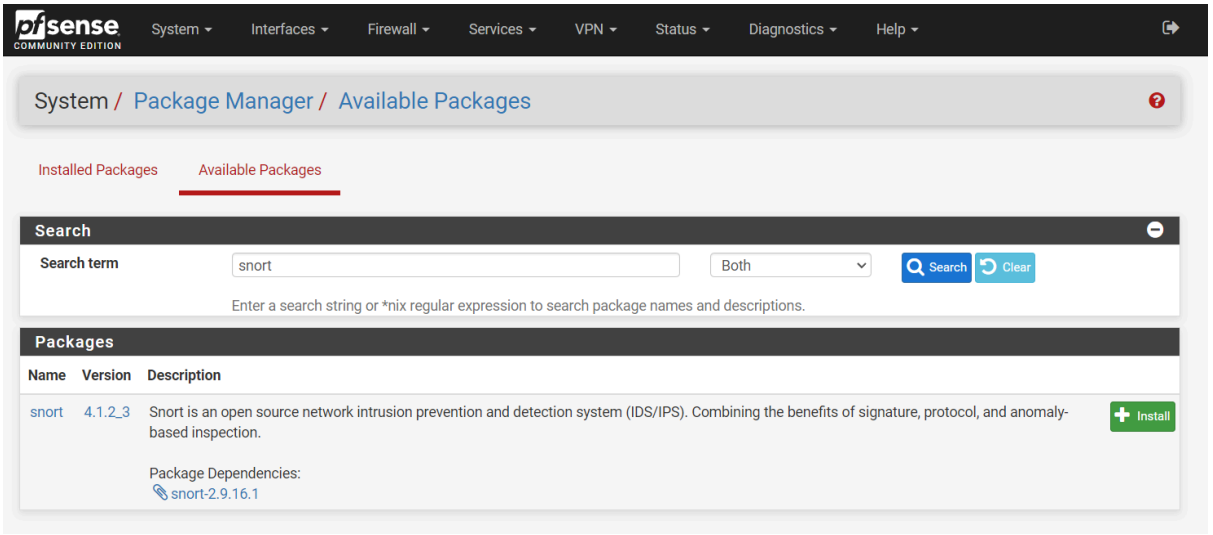
Sécurisation d'un service informatique avec PFSENS

1. Le pare feu IDS, IPS avec Snort sur PFsens

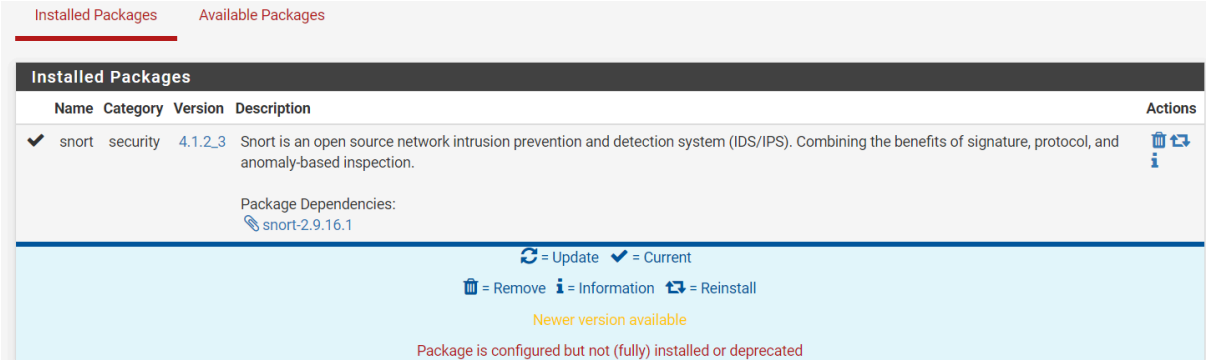
Pour commencer nous allons installer Snort sur le pfsens, pour se faire nous allons sur l'adresse suivante avec notre Vlan: 192.168."Vlan".100



Puis se rendre sur Système > Package manager > Available package, rechercher Snort et l'installer:



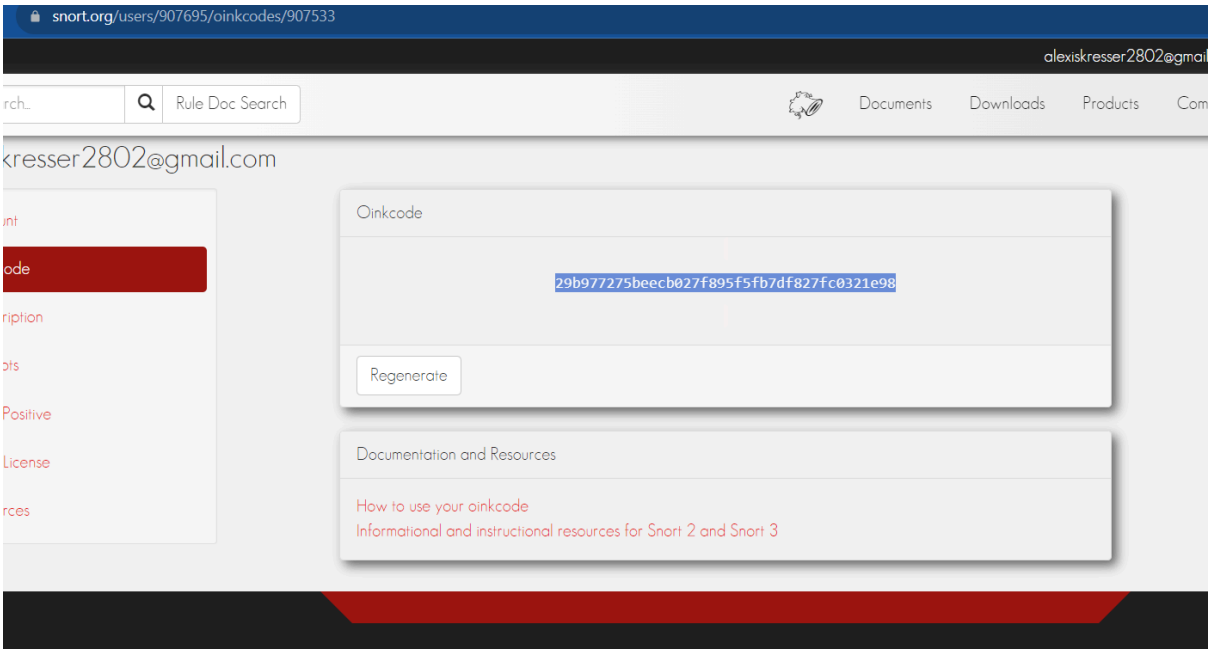
Une fois installé il doit apparaître dans " installed package" comme ceci:



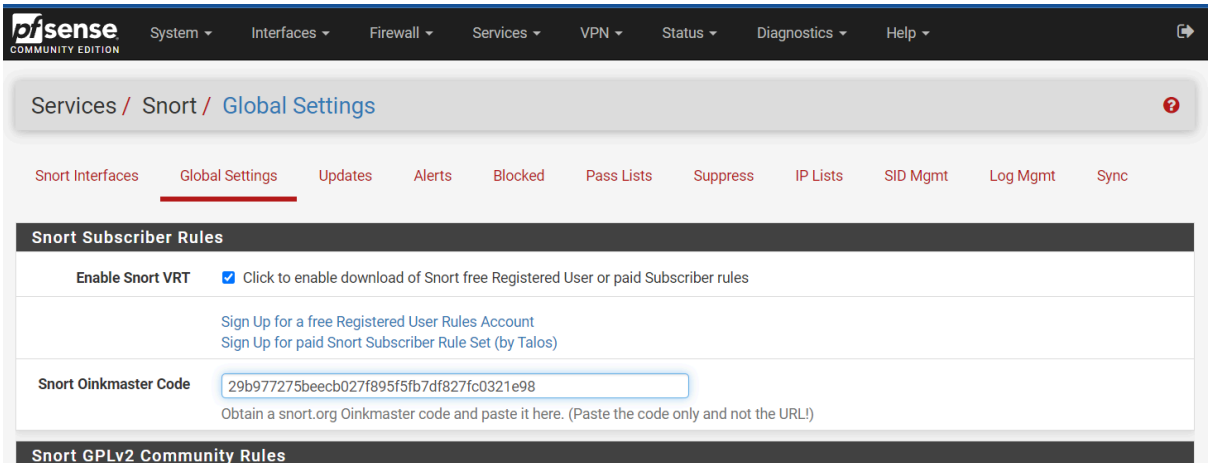
Maintenant nous pouvons nous rendre dans l'onglet service > Snort pour le configurer.

La première étape est d'activer le téléchargement de règles gratuites, en cochant la première case (Enable Snort VRT). Il faudra renseigner une clé et pour l'obtenir il vous faudra créer un compte sur le site officiel de Snort.

Récupération du code:



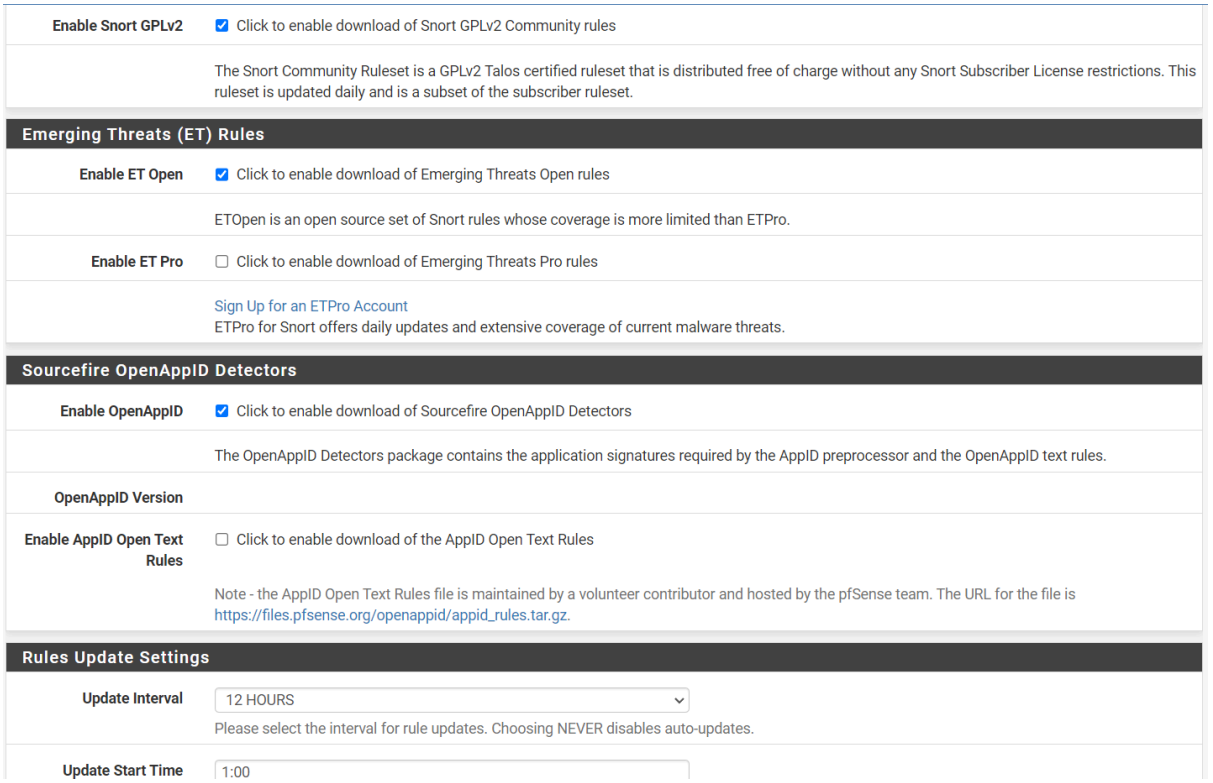
Mettre le code dans **"Snort Oinkmaster Code"**



Ensuite nous pouvons cocher les cases :

- **Enable Snort GPLv2**, pour les règles communautaires
- **Enable ET Open**, qui sont des règles proposées par la société ET
- **Enable Open AppID**, éventuellement, qui est une autre société

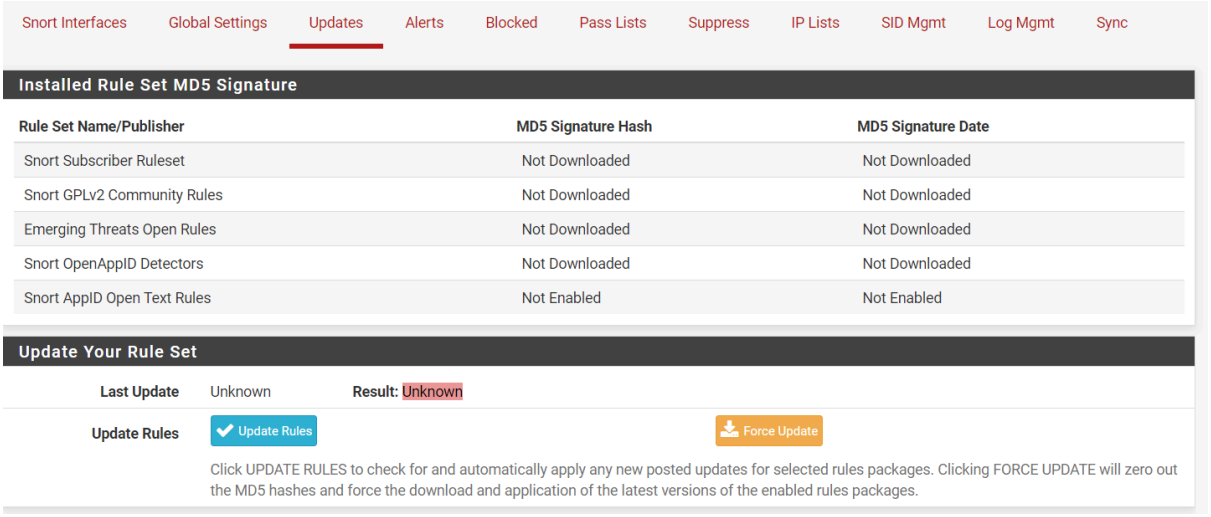
Puis, pour les derniers paramètres il convient simplement de configurer l'update pour les différentes règles, c'est-à-dire le délai avant de vérifier les mises à jour pour les différentes règles:

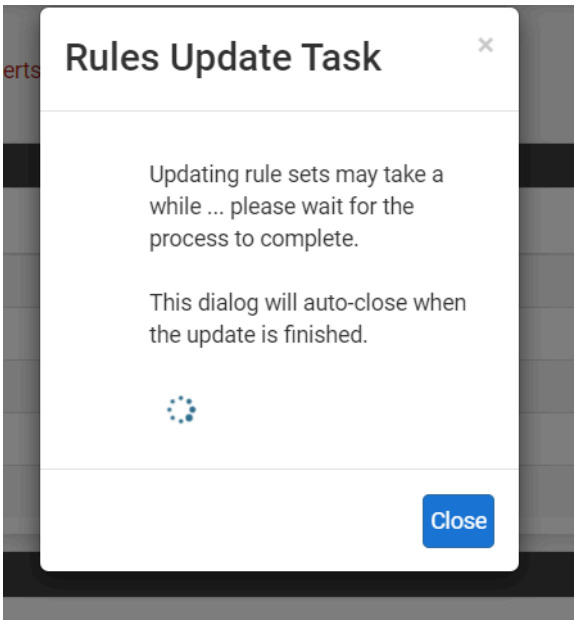


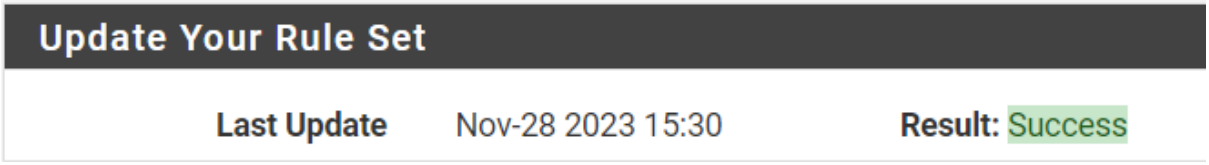
Dans notre cas l'intervalles des mise à jour sera de 12h minimum et l’heure de mise à jour sera 1h du matin pour ne pas gêner l’activité des collaborateurs

Ne pas oublier de sauvegarder le paramétrage

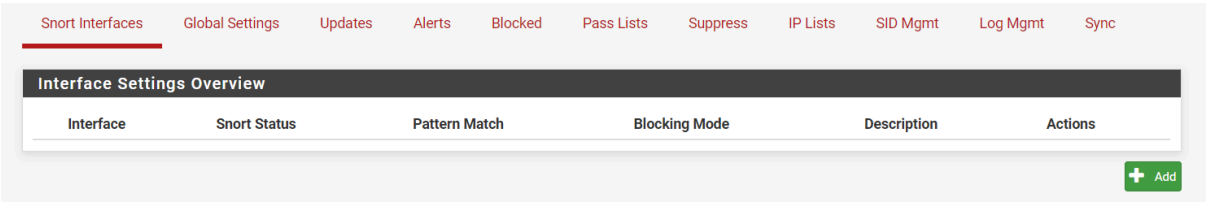
Une fois sauvegarder, nous pouvons nous rendre sur l’onglet Updates et manuellement mettre à jour les différentes règles que nous avons cochées précédemment en cliquant sur ‘“update rules” (dans notre cas cela prendra un peu de temps, car nous allons toutes les télécharger une première fois).



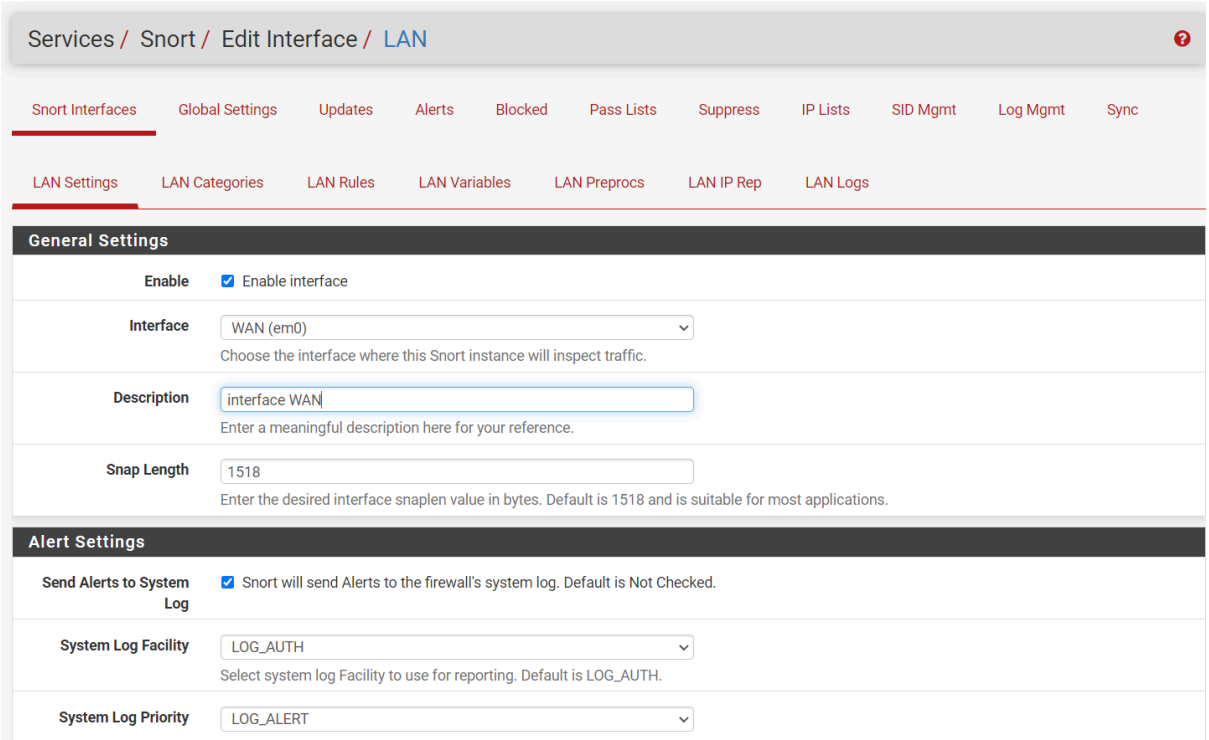




Maintenant que Snort est bien installé et configuré nous pouvons nous rendre sur “Snort interfaces” pour choisir l’interface (ou les interfaces) sur laquelle Snort va écouter et analyser le trafic et appuyer sur “add” pour ajouter:



Ici nous choisissons donc l’interface que nous voulons surveiller, puis une description du réseau et ensuite nous cochons simplement le fait d’envoyer les alertes sur le système de log interne, pour les analyser en cas de tentative d’intrusion



A partir de ces options nous avons mis en place notre IDS car ils nous envoie les informations du pare-feu dans des logs consultables.

Test de Fonctionnement IDS

Maintenant que nous l'avons activé, en allant dans l'interface Service > Snort > Alerte ont peut observer les logs qui arrivent et qui nous prévient de toute connexion suspecte sur le réseau sans bloquer la connexion au réseau qu'il tente d'accéder.