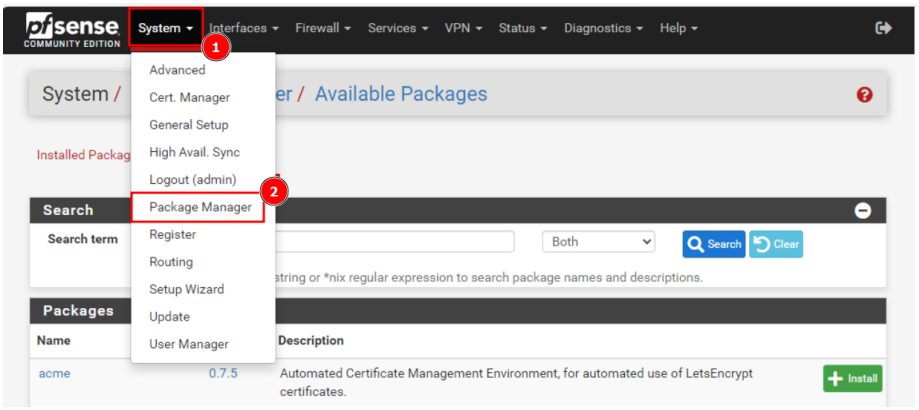
Installation de Suricata sur PfSense

Version de PfSense : 2.6.0
Version de Suricata : 7.0.2

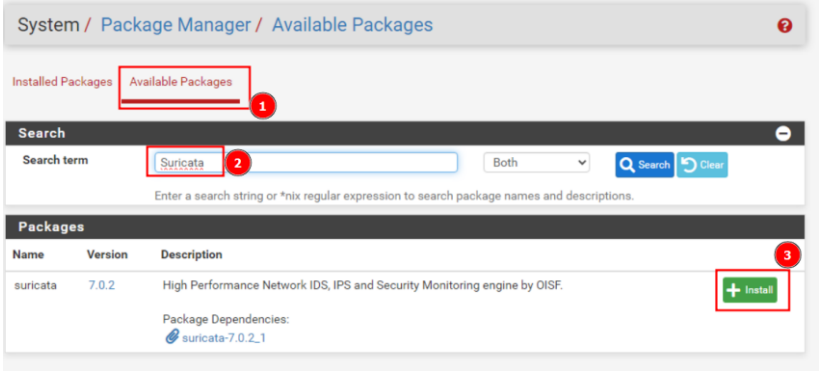
1 – Installation des Packages sur PfSense 1
2 – Ajout des interfaces sur Suricata 3
3 – Configuration de base des règles 4

1 – Installation des Packages sur PfSense

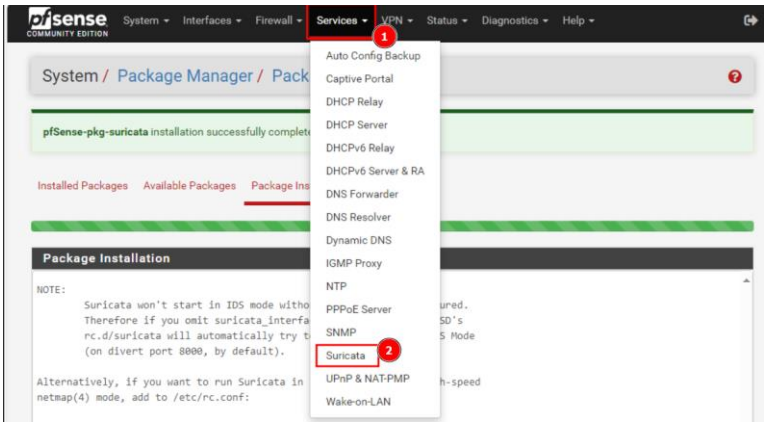
Rendez-vous dans **System** puis **Package Manager**



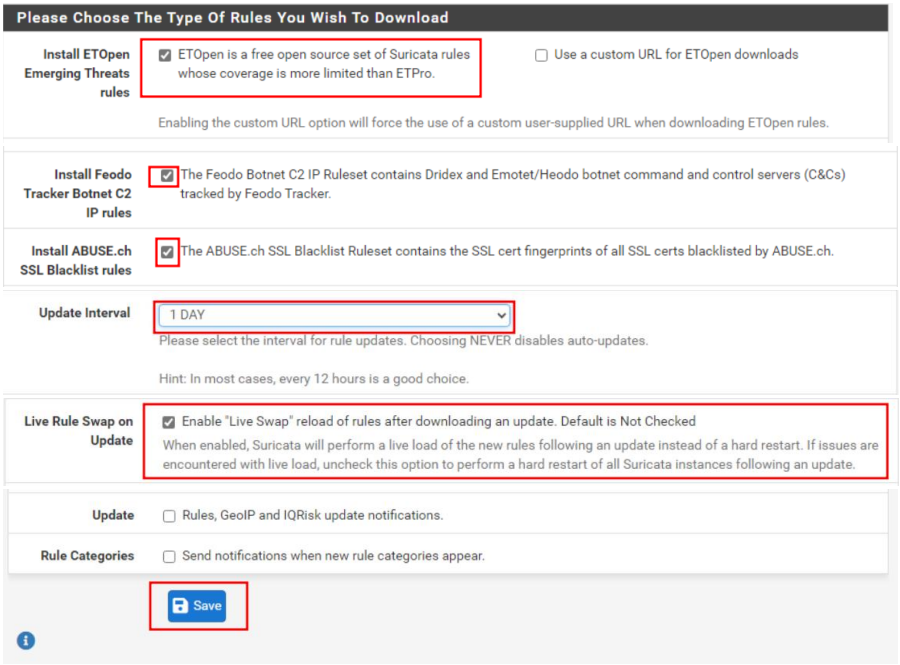
Dans **Available Packages** recherchez **Suricata** puis installez-le



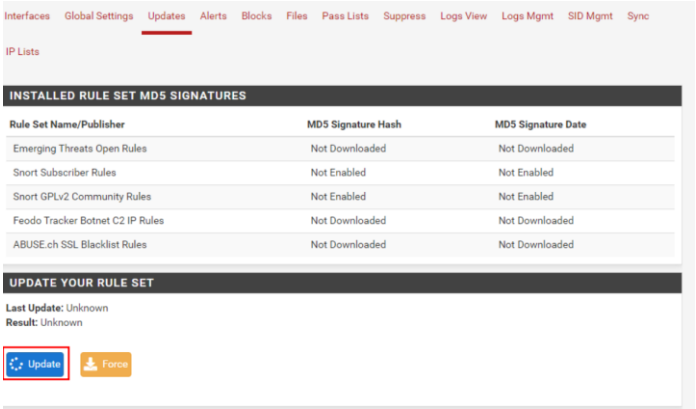
Une fois terminée, allez dans **Services** -> **Suricata**



Dans **Global Settings**, cochez les options suivantes et laissez-le reste par défaut

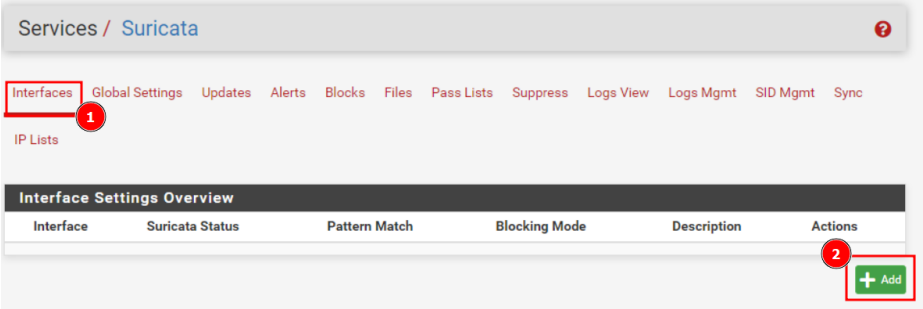


Allez ensuite dans l'onglet **Updates** et cliquez sur **Update**

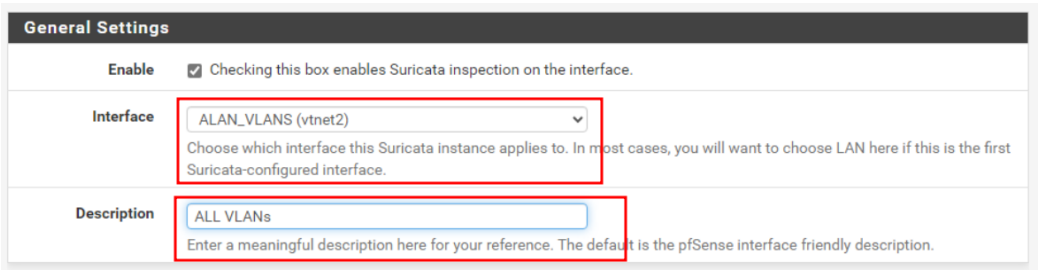


2 – Ajout des interfaces sur Suricata

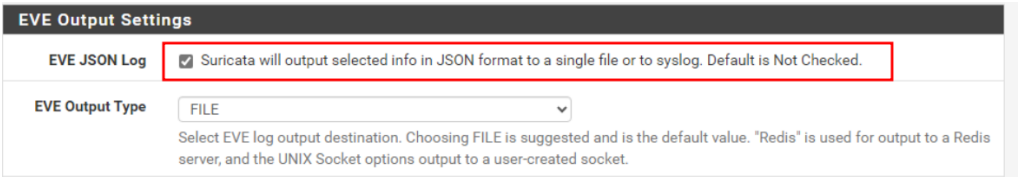
Allez dans **Interfaces** puis cliquez sur **Add**



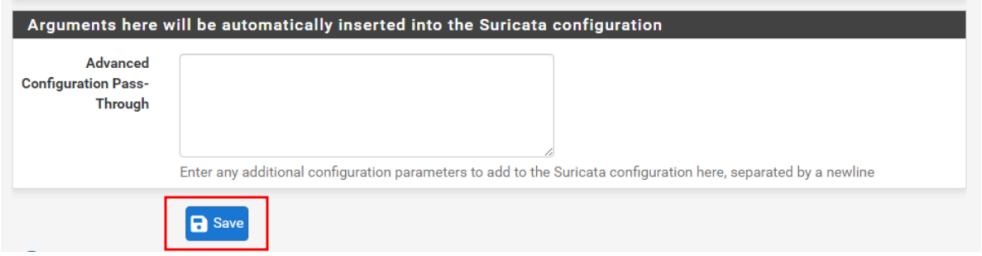
Sélectionnez maintenant l'interface que vous souhaitez surveiller. Dans mon cas je souhaite surveiller tous les vlans, donc je sélectionne l'interface parente aux vlans.



Ensuite, cochez la case pour que les logs soient au format JSON. Laissez tout le reste par défaut

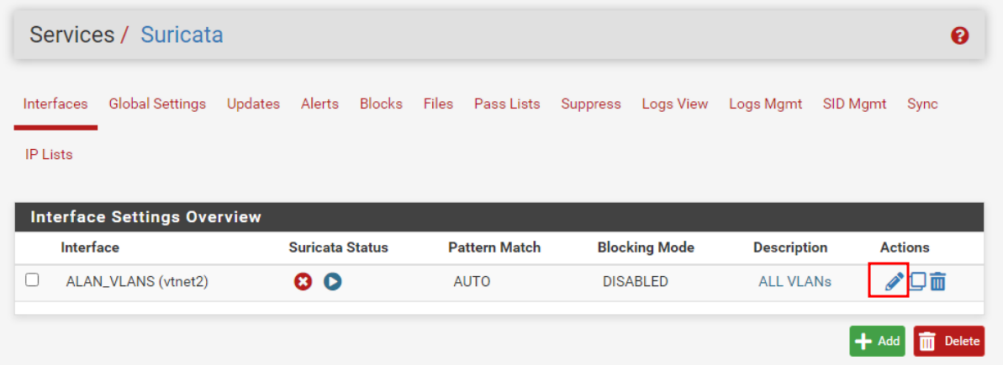


Une fois terminée, sauvegardez

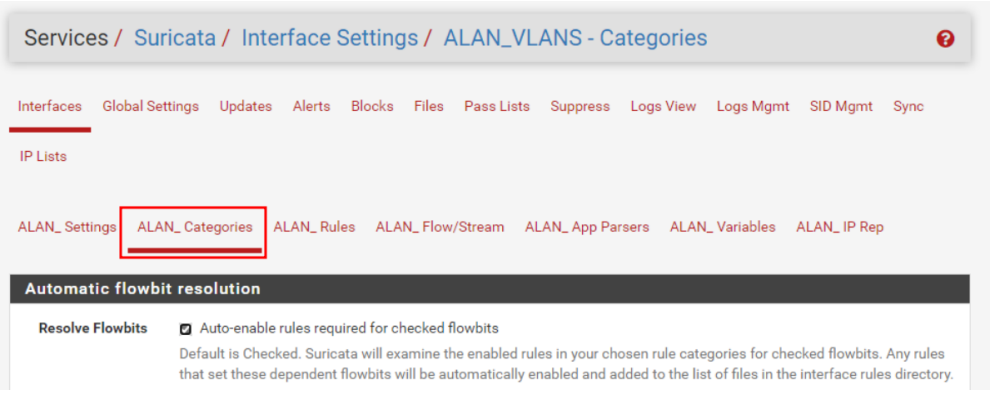


3 – Configuration de base des règles

Rendez-vous ensuite encore une fois dans **Interfaces** et cliquez sur le logo crayon



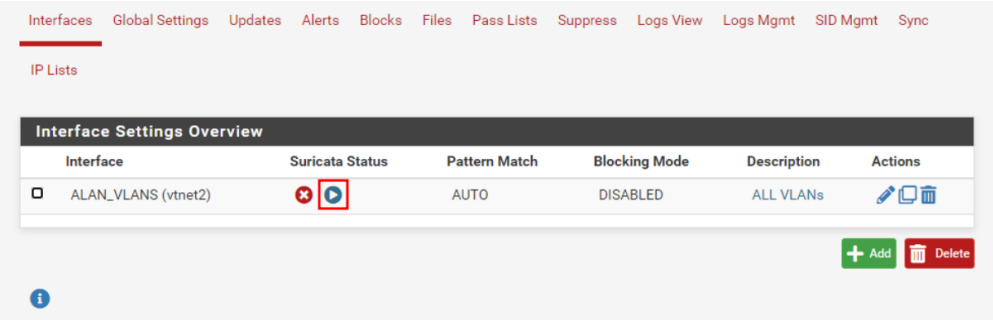
Allez dans **Categories**



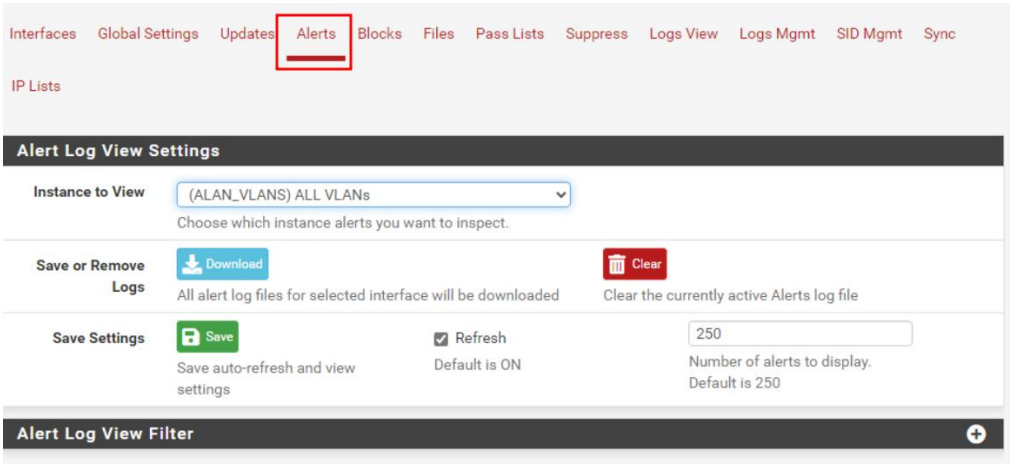
On se retrouve ici dans les règles. On va tout sélectionner et par la suite on pourra ajuster petit à petit et retirer les règles qui ne nous serviraient pas ou poseraient problèmes.

Une fois cela fait, il suffit de décocher les cases qui ne nous intéressent pas ou pour lesquelles nous ne voulons pas d'alerte.

Retournez maintenant dans **Interfaces** et démarrez Suricata. Il est important de noter que nous n'avons pas activer la fonction IPS pour le moment afin d'éviter toutes pertes de connexions ou tout problème de réseau.



Afin de tester vos règles et d'identifier celles que vous souhaitez ignorées car ce sont des faux positifs, utilisez votre réseau de manière habituelle pendant 2 à 3 jours puis allez voir dans l'onglet **Alerts** les alertes. Désactivez ensuite celles qui n'ont pas lieu d'être.



Fin de la procédure.