

Installation de Suricata sur PfSense

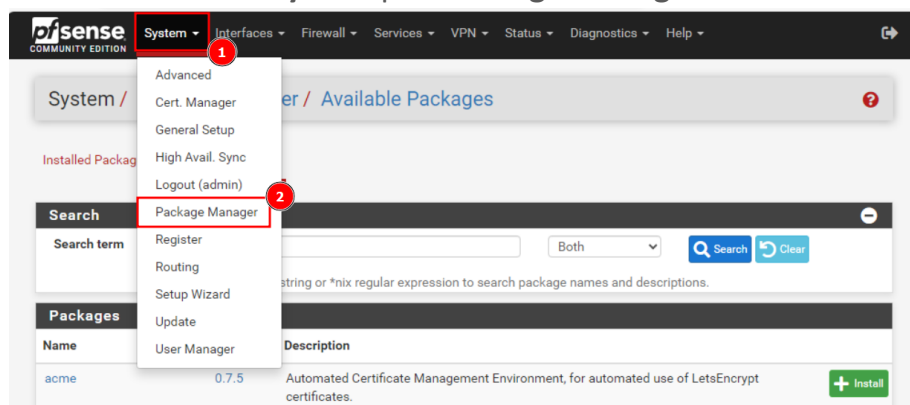
Version de PfSense : 2.6.0

Version de Suricata : 7.0.2

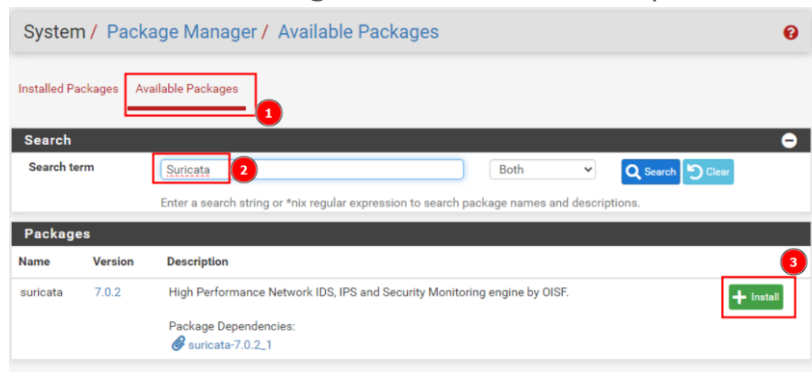
1 – Installation des Packages sur PfSense	1
2 – Ajout des interfaces sur Suricata	3
3 – Configuration de base des règles	4

1 – Installation des Packages sur PfSense

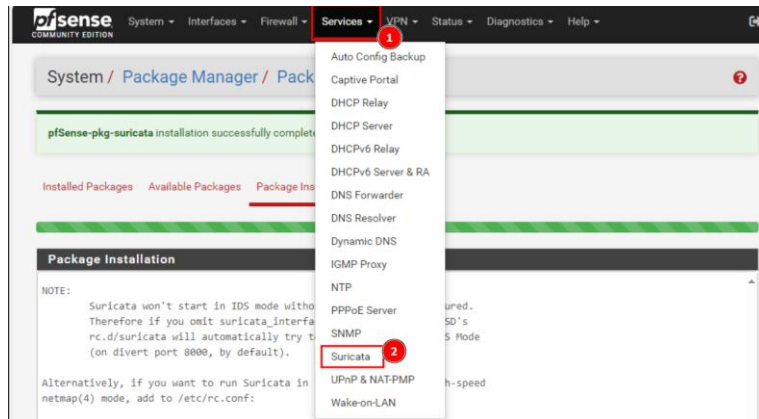
Rendez-vous dans **System** puis **Package Manager**



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

Please Choose The Type Of Rules You Wish To Download

Install ETOpen Emerging Threats rules ☒ ETOpen is a free open source set of Suricata rules whose coverage is more limited than ETPro. ☐ Use a custom URL for ETOpen downloads

Enabling the custom URL option will force the use of a custom user-supplied URL when downloading ETOpen rules.

Install Feodo Tracker Botnet C2 IP rules ☒ The Feodo Botnet C2 IP Ruleset contains Dridex and Emotet/Heodo botnet command and control servers (C&Cs) tracked by Feodo Tracker.

Install ABUSE.ch SSL Blacklist rules ☒ The ABUSE.ch SSL Blacklist Ruleset contains the SSL cert fingerprints of all SSL certs blacklisted by ABUSE.ch.

Update Interval Please select the interval for rule updates. Choosing NEVER disables auto-updates.

Hint: In most cases, every 12 hours is a good choice.

Live Rule Swap on Update ☒ Enable "Live Swap" reload of rules after downloading an update. Default is Not Checked

When enabled, Suricata will perform a live load of the new rules following an update instead of a hard restart. If issues are encountered with live load, uncheck this option to perform a hard restart of all Suricata instances following an update.

Update ☐ Rules, GeoIP and IQRisk update notifications.

Rule Categories ☐ Send notifications when new rule categories appear.

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

Interfaces Global Settings **Updates** Alerts Blocks Files Pass Lists Suppress Logs View Logs Mgmt SID Mgmt Sync

IP Lists

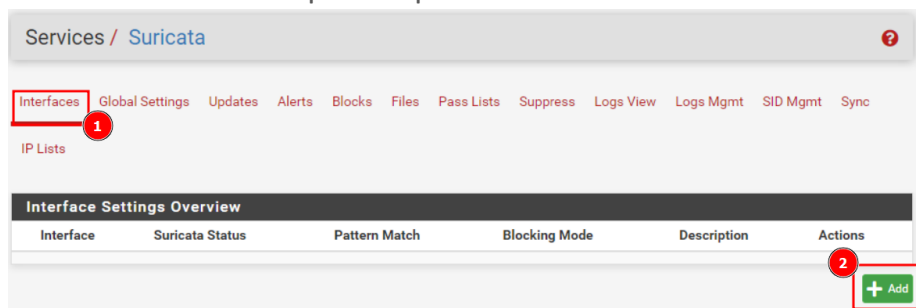
Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Emerging Threats Open Rules	Not Downloaded	Not Downloaded
Snort Subscriber Rules	Not Enabled	Not Enabled
Snort GPLv2 Community Rules	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP Rules	Not Downloaded	Not Downloaded
ABUSE.ch SSL Blacklist Rules	Not Downloaded	Not Downloaded

UPDATE YOUR RULE SET

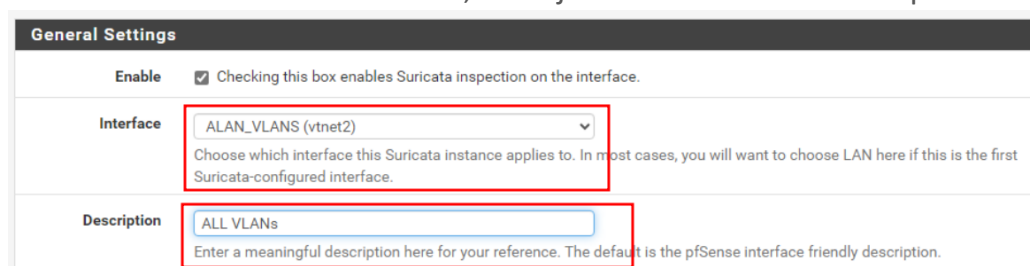
Last Update: Unknown
Result: Unknown

2 – Ajout des interfaces sur Suricata

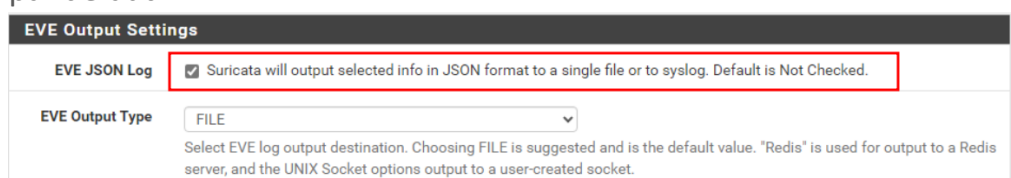
Allez dans **Interfaces** puis cliquez sur **Add**



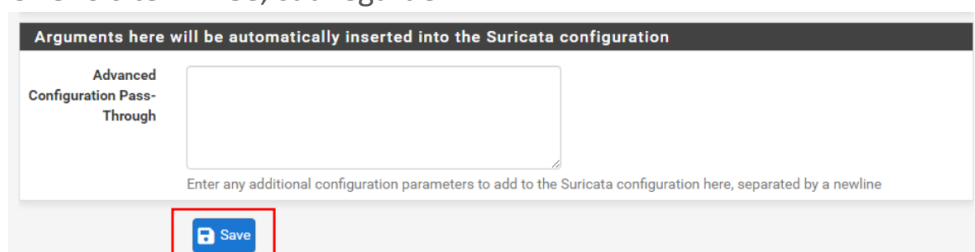
Sélectionnez maintenant l'interface que vous souhaitez surveiller. Dans mon cas je souhaite surveiller tous les vlans, donc je sélectionne l'interface parente aux vlans.



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

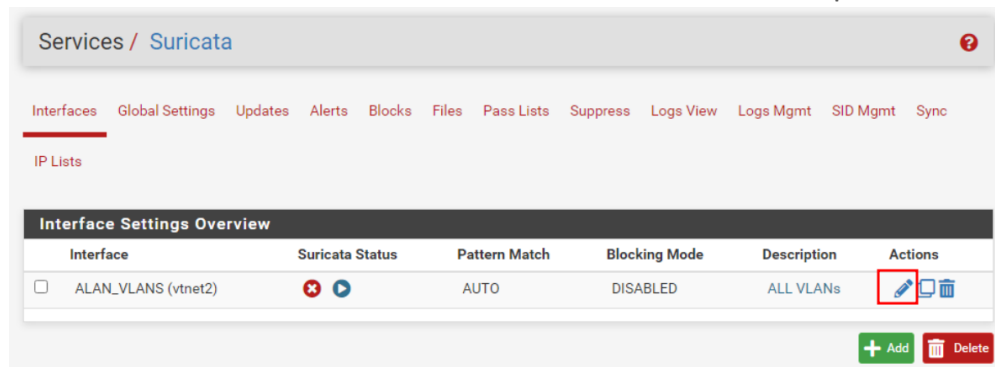


Une fois terminée, sauvegardez

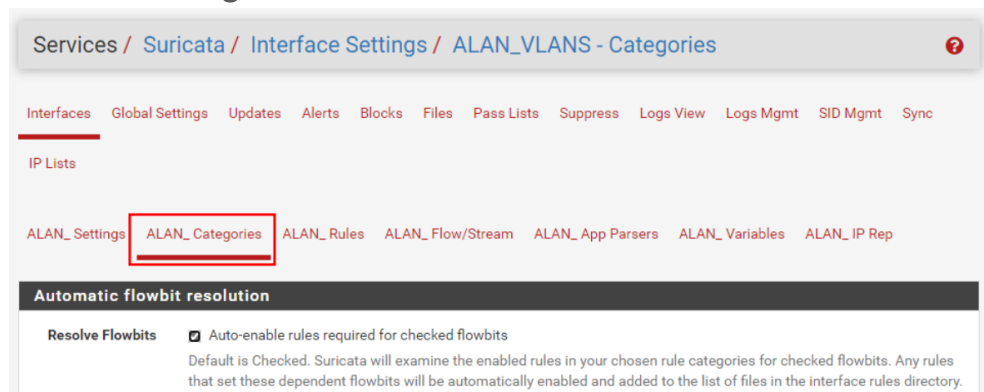


3 – Configuration de base des règles

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



Allez dans **Categories**

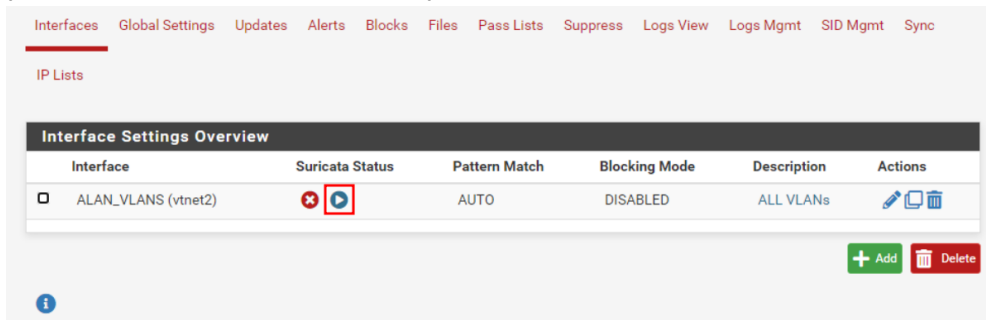


On se retrouve ici dans les règles. On va tout sélectionner et par la suite on pourra ajuster petit à petit et retirer les règles qui ne nous serviraient pas ou poseraient problèmes.

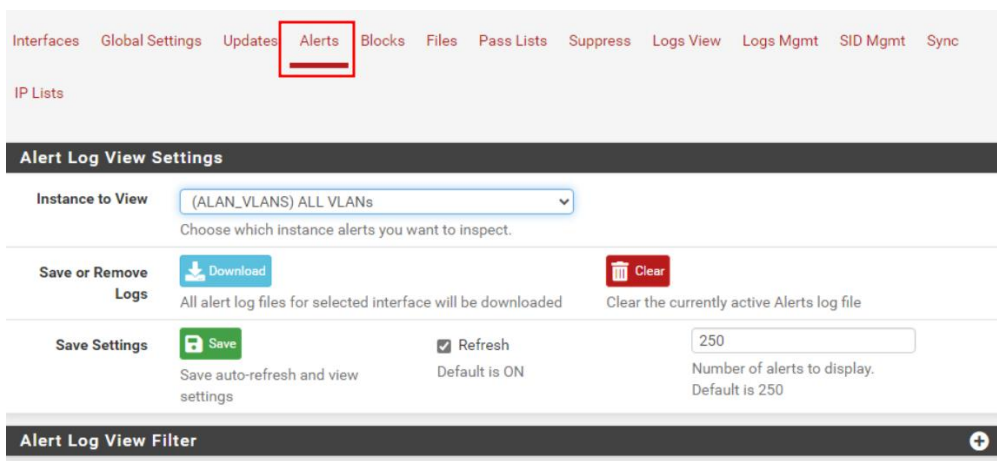


Une fois cela fait, il suffit de décocher les cases qui ne nous intéressent pas ou pour lesquelles nous ne voulons pas d'alerte.

Retournez maintenant dans **Interfaces** et démarrez Suricata. Il est important de noter que nous n'avons pas activé 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.