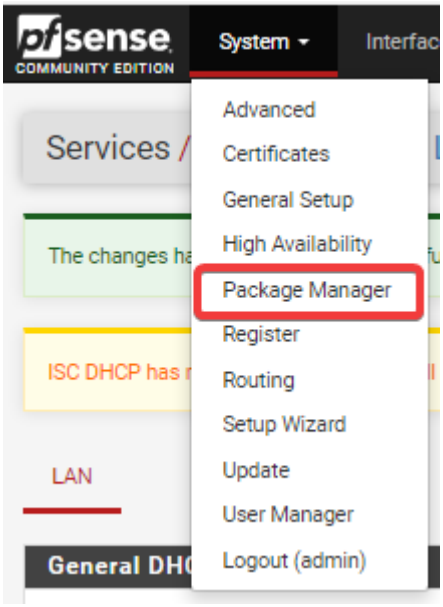
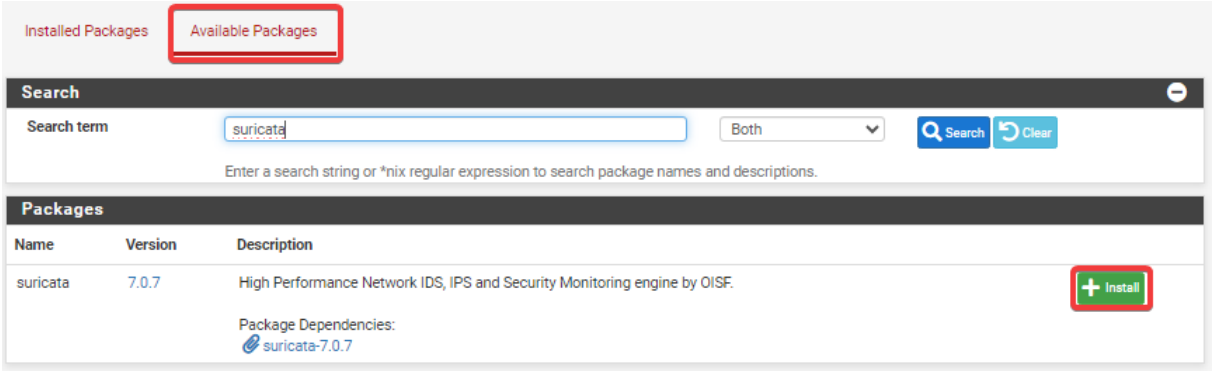
Configuration d'un IPS/IDS :

Dans cette partie nous allons voir comment configurer un IDS/IPS avec le suricata sur unPfSense pour améliorer la sécurité de son réseau. Qui est un programme qui permet de surveiller notre réseau

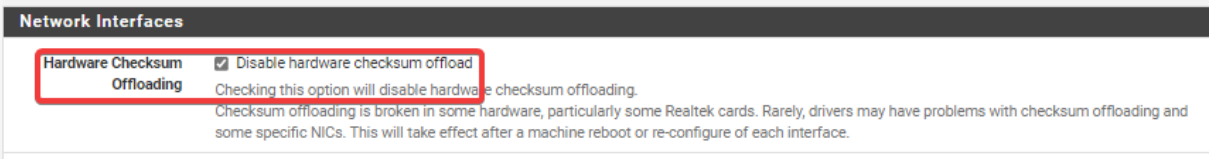
Je commence tout d'abord par me rendre dans **System > Package Manager** sur l'interface web de mon PfSense



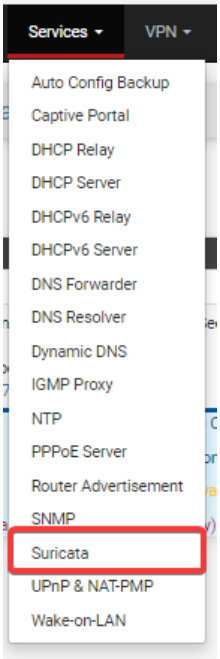
Ensuite je clique sur **Available Packages** et je recherche **Suricata** et je clique sur **Install**



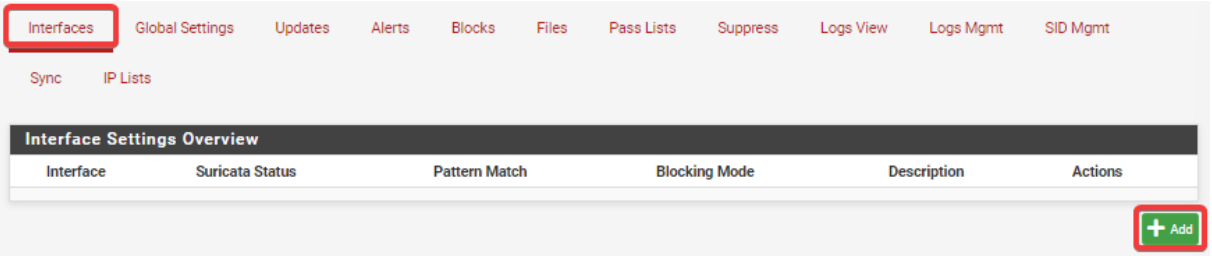
Pour que le Suricata fonctionne bien il faudra tout d'abord désactiver cette option dans **System > Advanced > Networking**



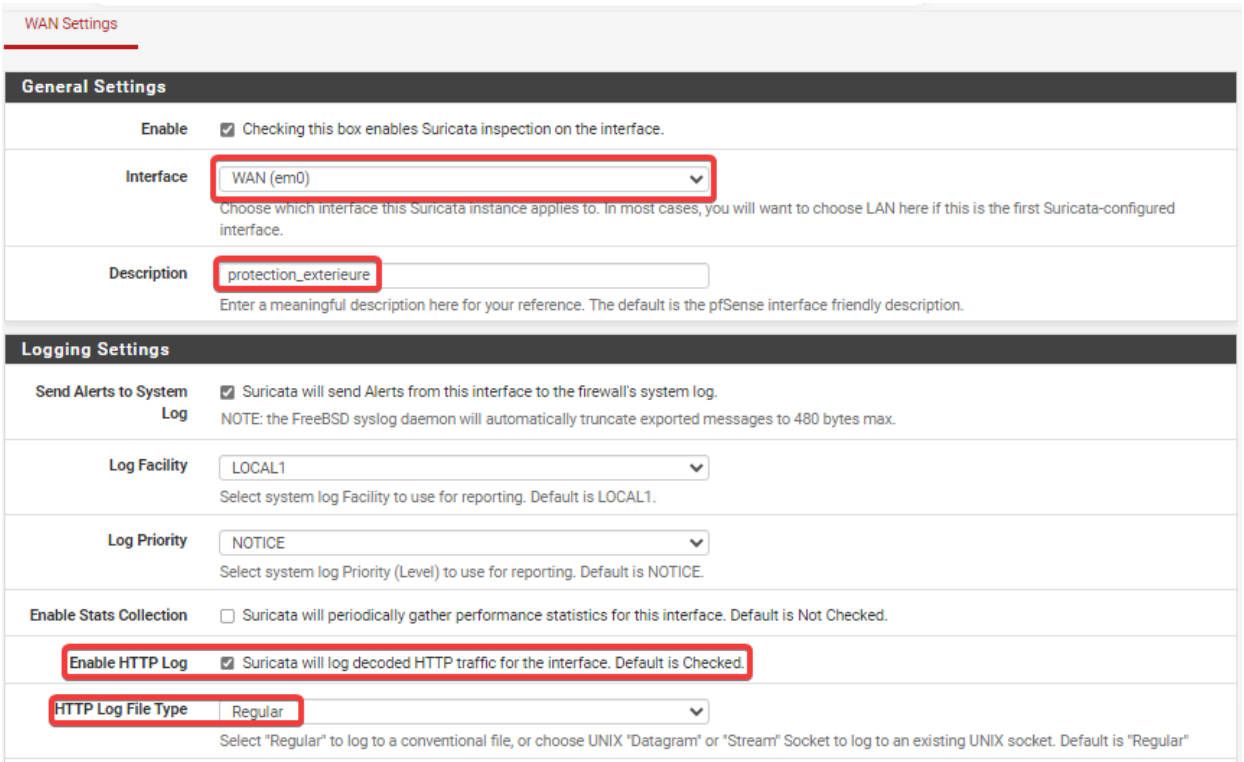
Ensuite on va maintenant le configurer, je me rends dans **Services > Suricata**



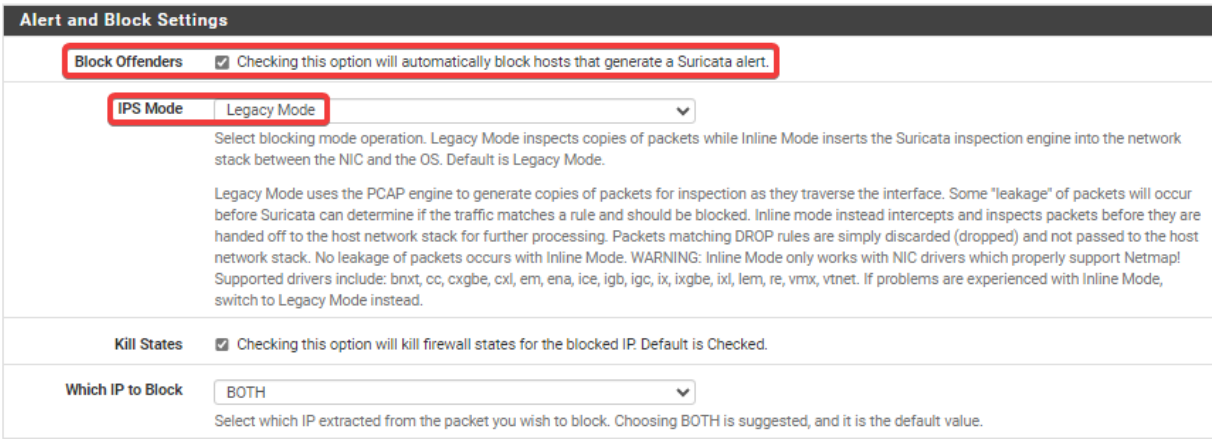
Ensuite dans **Interfaces** je clique sur **Add** pour ajouter une nouvelle interface



Arrivé sur cette page je sélectionne l'interface **WAN** pour détecter les intrusions venant de l'extérieur, ensuite je donne la description **protection_exterieure**, ensuite je coche **Enable HTTP Log**, pour recevoir des journaux d'événements des événements http et je laisse **Regular** pour le type de log

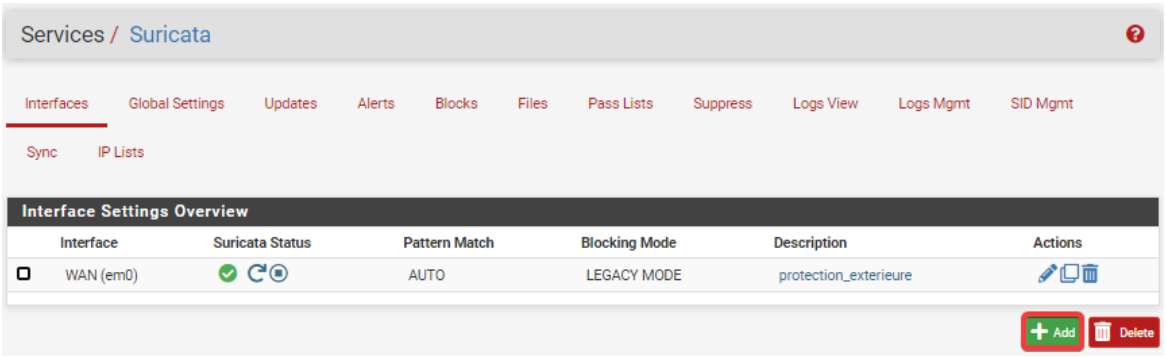


Ensuite dans **Alert and Block Settings** je coche **Block Offenders** pour automatiquement bloquer les hôtes ayant générés des alertes Suricata

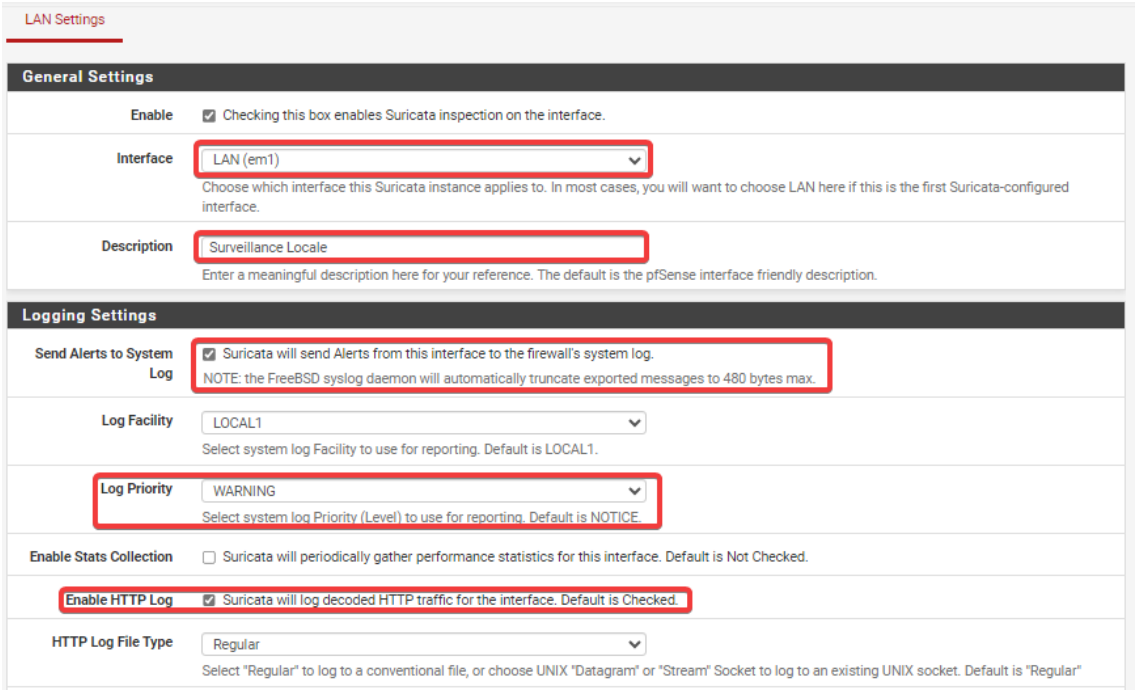


Et ensuite pour la suite je laisse les paramètres par défaut.

Ensuite nous allons aussi surveiller l'interface **LAN,** pour ce faire je commence par retourner sur la page de mon **Suricata** et sur la page **interfaces** et ici je clique sur **Add**

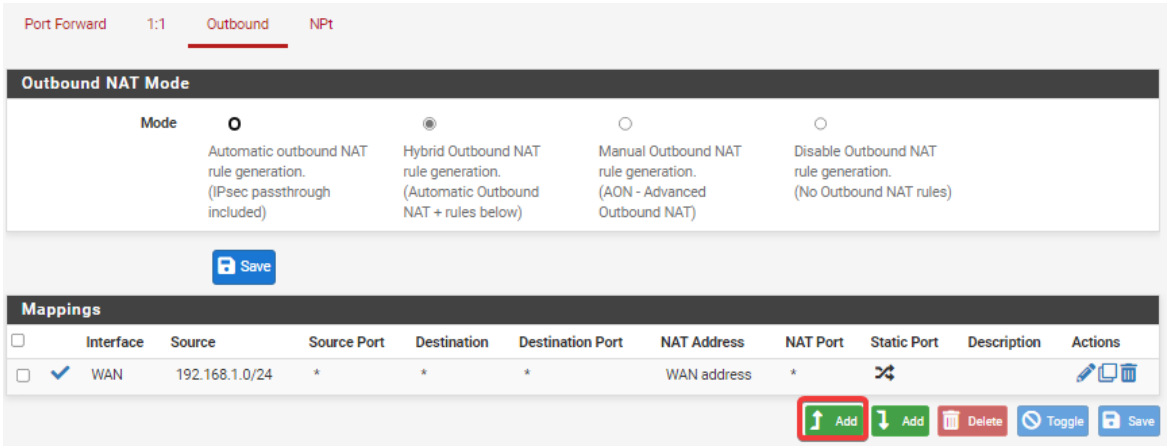


Ensuite sur cette fenêtre je rentre ces informations, je sélectionne **LAN** car c'est l'interface qu'on veut surveiller, je la nomme **« surveillance locale »** je coche ensuite **Send Alerts to system Log** pour être alerter de ce qui se passe sur mon interface et je laisse les autres options par défaut

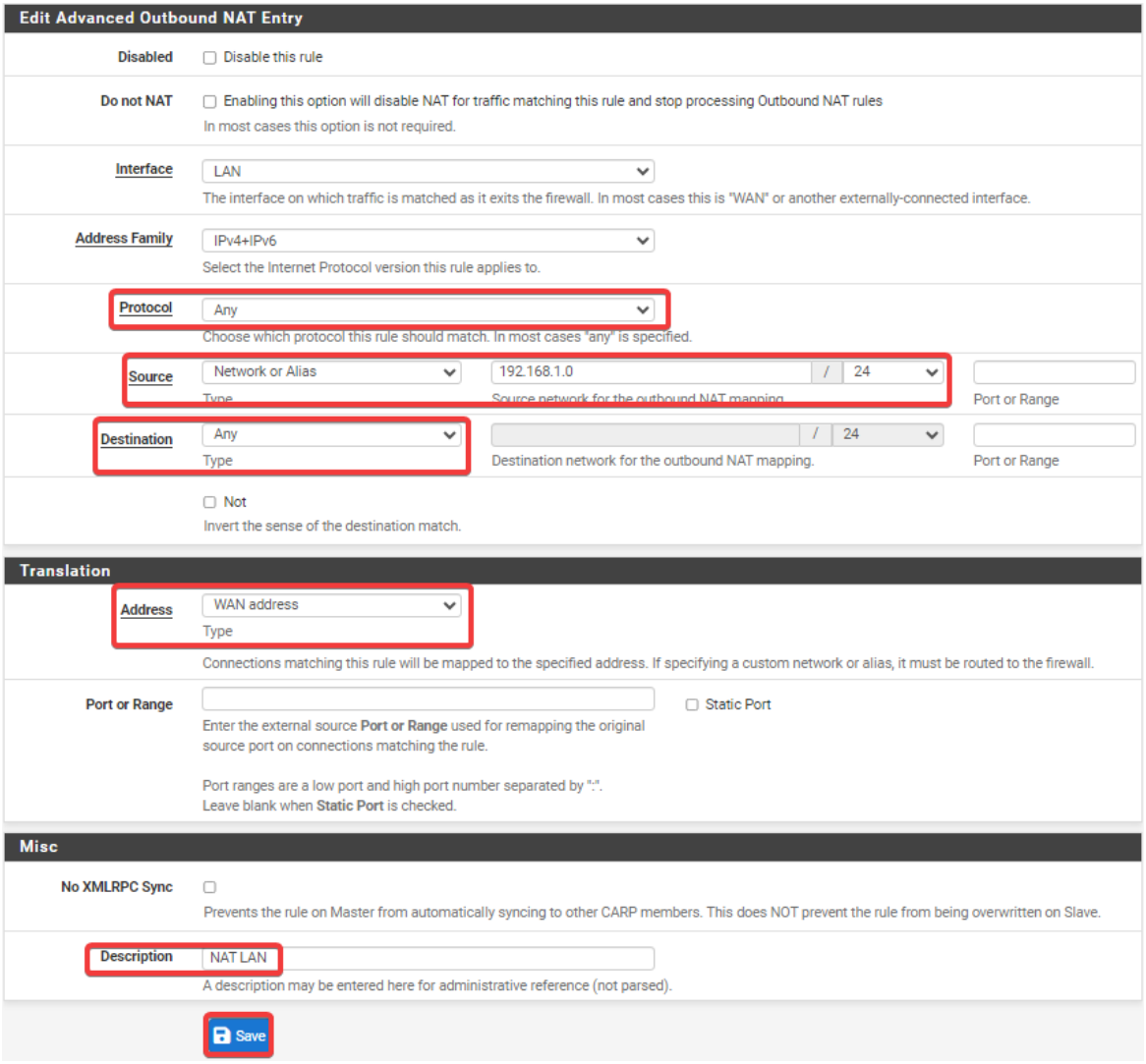


Et ensuite je laisse les autres options par défaut et je sauvegarde et applique la configuration.

Ensuite comme pour le WAN, je me rends dans **Firewall > Outbound** et clique ici sur **Add**



Ensuite cette page s’ouvre, et je sélectionne ces paramètres, sauvegarde et applique



Et voila la configuration de mon IDS est terminée