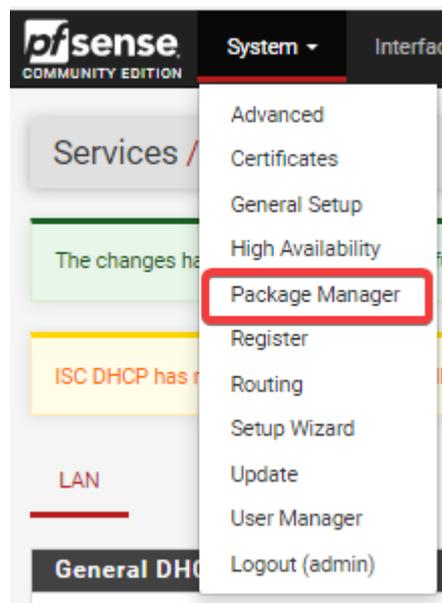


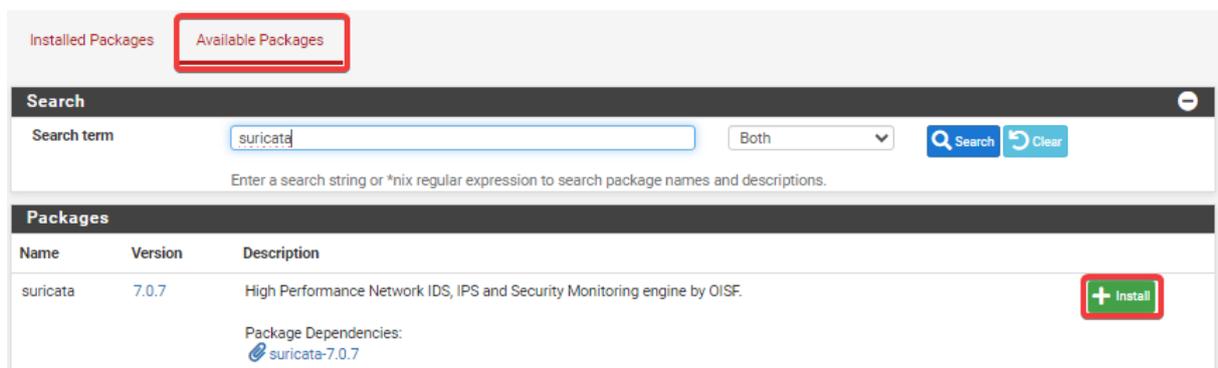
## Configuration d'un IPS/IDS :

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

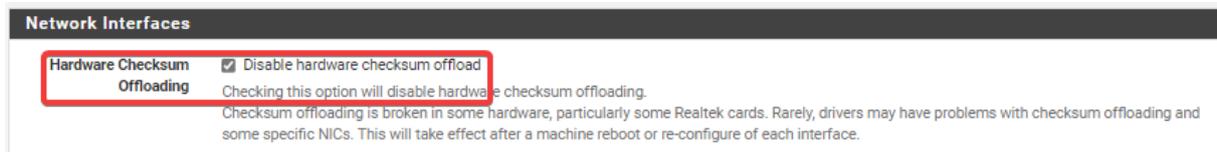
Je commence tout d'abord par me rendre dans **System > Package Manager** sur l'interface web de mon PfSense



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



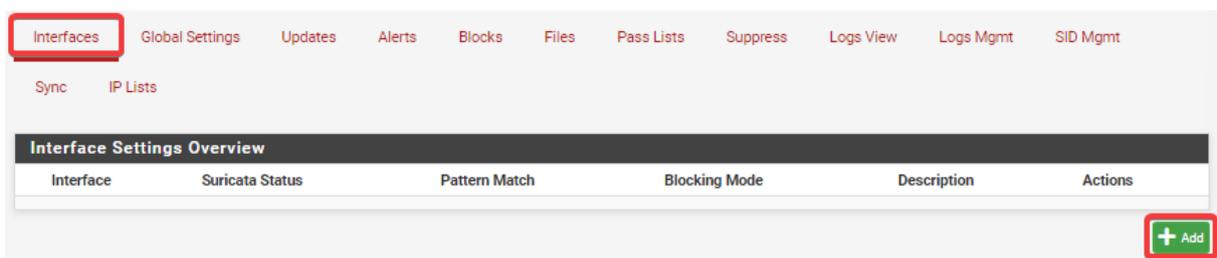
Pour que le Suricata fonctionne bien il faudra tout d'abord désactiver cette option dans **System > Advanced > Networking**



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

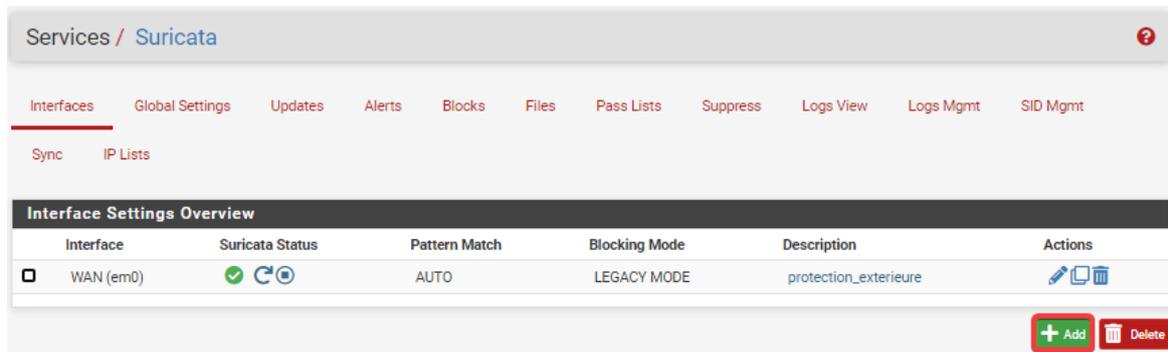
The screenshot shows the 'WAN Settings' page in pfSense. It is divided into two main sections: 'General Settings' and 'Logging Settings'. In the 'General Settings' section, the 'Enable' checkbox is checked. The 'Interface' dropdown is set to 'WAN (em0)'. The 'Description' field contains 'protection\_exterieure'. In the 'Logging Settings' section, 'Send Alerts to System Log' is checked. 'Log Facility' is set to 'LOCAL1' and 'Log Priority' is set to 'NOTICE'. 'Enable Stats Collection' is unchecked. 'Enable HTTP Log' is checked. 'HTTP Log File Type' is set to 'Regular'.

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

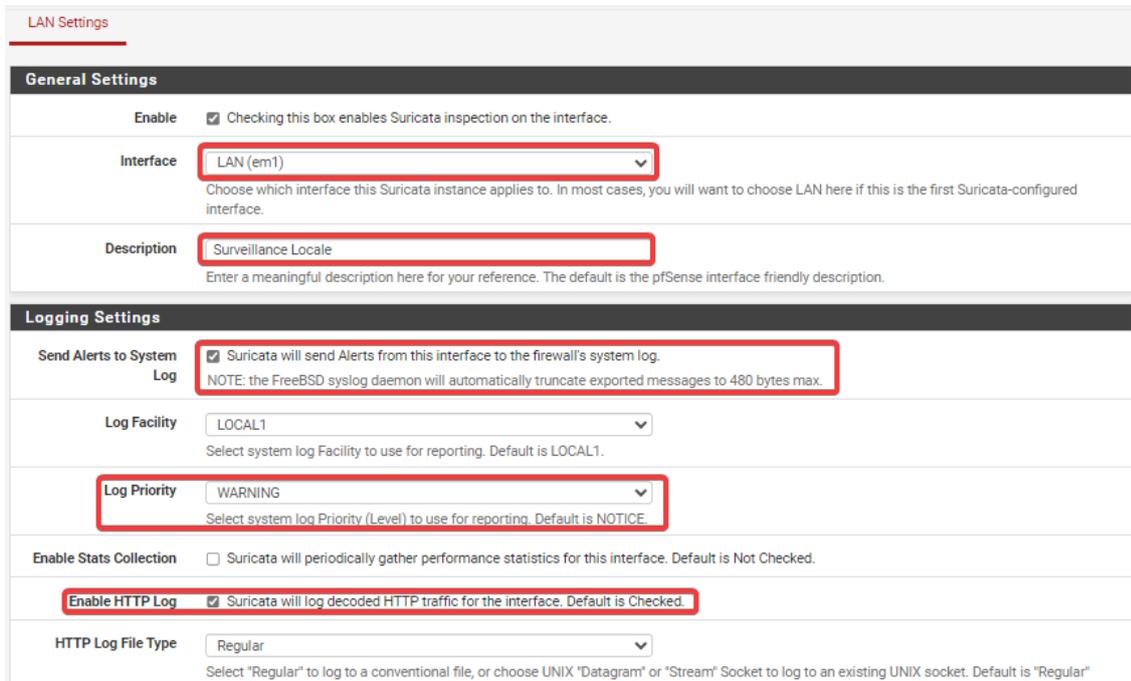
The screenshot shows the 'Alert and Block Settings' page in pfSense. The 'Block Offenders' checkbox is checked. The 'IPS Mode' dropdown is set to 'Legacy Mode'. The 'Kill States' checkbox is checked. The 'Which IP to Block' dropdown is set to 'BOTH'.

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**

The screenshot shows the Mikrotik WinBox interface for configuring Outbound NAT. At the top, there are tabs for 'Port Forward', '1:1', 'Outbound', and 'NPT', with 'Outbound' selected. Below this is the 'Outbound NAT Mode' section, which contains four radio button options: 'Automatic outbound NAT rule generation. (IPsec passthrough included)', 'Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)', 'Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)', and 'Disable Outbound NAT rule generation. (No Outbound NAT rules)'. The 'Hybrid' option is selected. A 'Save' button is located below the mode selection. The 'Mappings' section is a table with columns: Interface, Source, Source Port, Destination, Destination Port, NAT Address, NAT Port, Static Port, Description, and Actions. A single mapping is listed for the 'WAN' interface with source '192.168.1.0/24' and destination 'WAN address'. At the bottom right, there are buttons for 'Add', 'Add', 'Delete', 'Toggle', and 'Save'. The first 'Add' button is highlighted with a red box.

Mode	Automatic outbound NAT rule generation. (IPsec passthrough included)	Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)	Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)	Disable Outbound NAT rule generation. (No Outbound NAT rules)
------	--	---	--	---

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<input checked="" type="checkbox"/>	WAN	192.168.1.0/24	*	*	*	WAN address	*		

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

### Edit Advanced Outbound NAT Entry

**Disabled**  Disable this rule

**Do not NAT**  Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules  
In most cases this option is not required.

**Interface**   
The interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.

**Address Family**   
Select the Internet Protocol version this rule applies to.

**Protocol**   
Choose which protocol this rule should match. In most cases "any" is specified.

**Source**   /   
Type: Source network for the outbound NAT mapping. Port or Range

**Destination**  /   
Type: Destination network for the outbound NAT mapping. Port or Range

Not  
Invert the sense of the destination match.

### Translation

**Address**   
Type: Connections matching this rule will be mapped to the specified address. If specifying a custom network or alias, it must be routed to the firewall.

**Port or Range**   Static Port  
Enter the external source **Port or Range** used for remapping the original source port on connections matching the rule.  
Port ranges are a low port and high port number separated by ":".  
Leave blank when **Static Port** is checked.

### Misc

**No XMLRPC Sync**   
Prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

**Description**   
A description may be entered here for administrative reference (not parsed).

Et voila la configuration de mon IDS est terminée