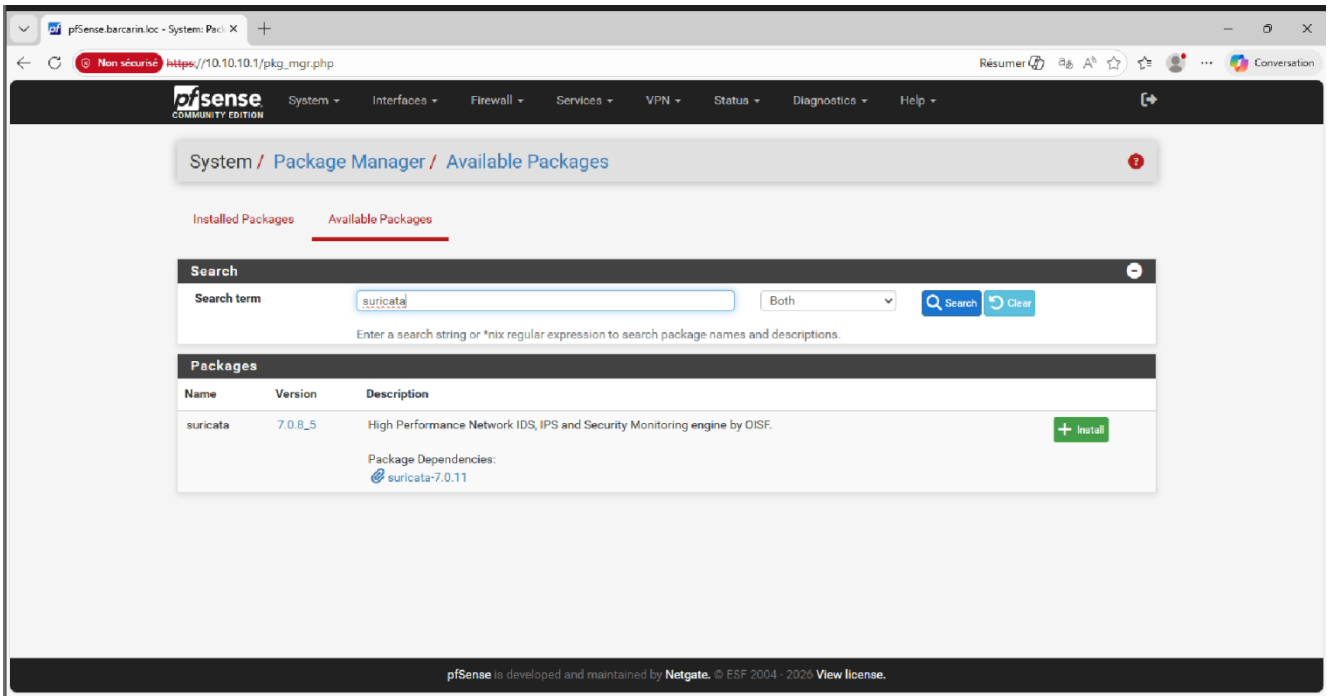
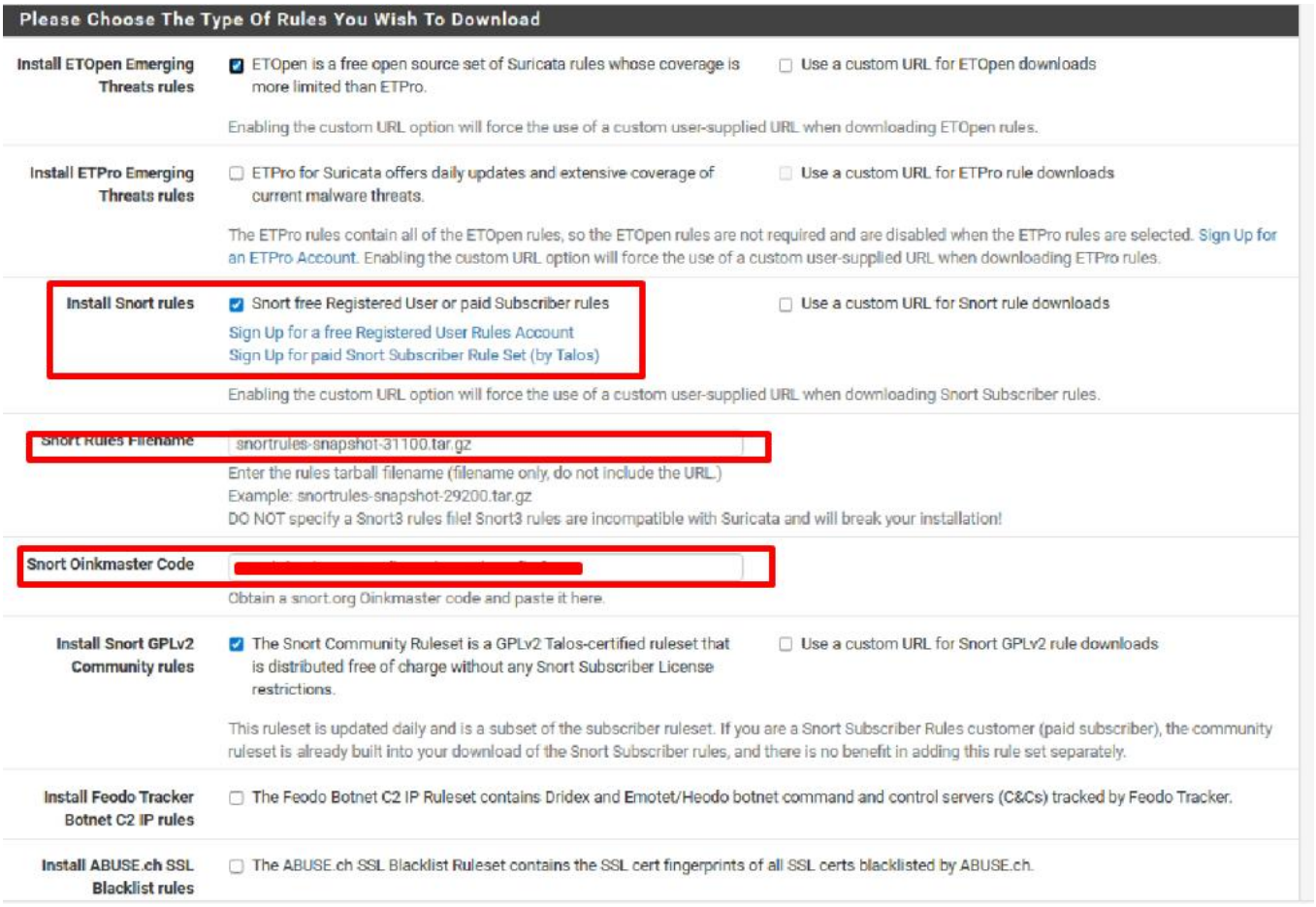
# Procédure Installation et configuration Suricata dans pfsense:

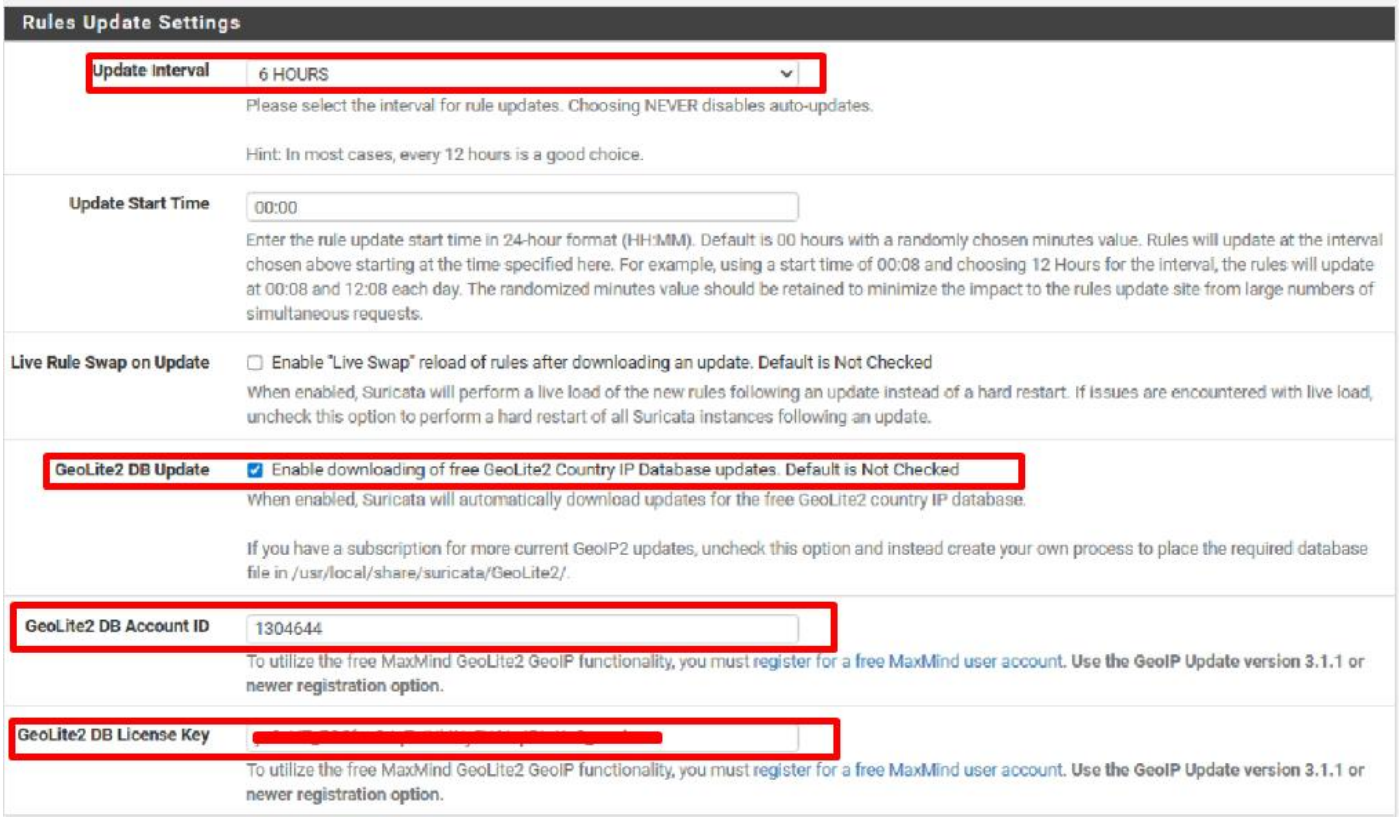
Pour commencer rdv dans System → Package Manager → Available Package, et chercher Suricata installer le :



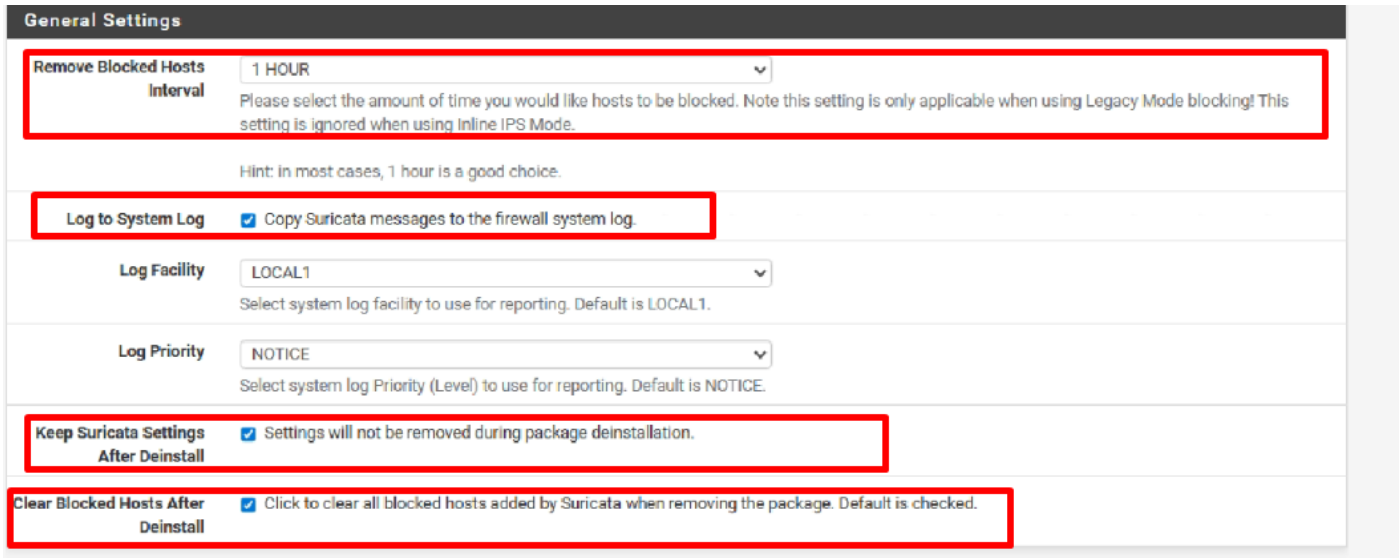

Ensuite rdv dans Services → Suricata → General Settings : Sélectionnez les options suivantes ensuite pour les règle ou vas utiliser Snort. Rdv sur le site https://snort.org/ crée vous un compte et dans l'onglet download vous verrez les noms des dernière version copier-coller la dans Snort Rules Filename sur pfsense. Ensuite pour le Snort Oinkmaster code rdv dans votre compte snort sur votre profil vous y trouverais votre Oinkcode.



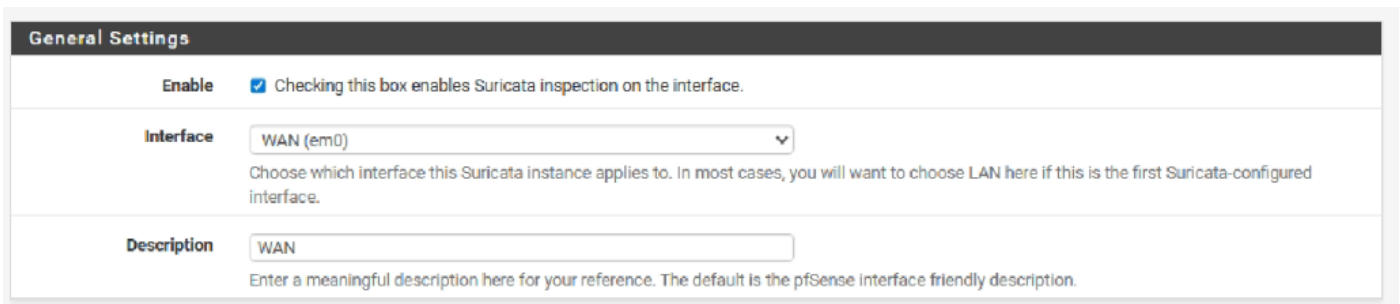
Les règles vont être mis à jour toute les 6h, Ensuite activer GeoLite2, Pour acount ID et licence Key crée un compte sur https://www.maxmind.com/ aller dans l'onglet Manage Licence Key et généré une nouvelle clé :



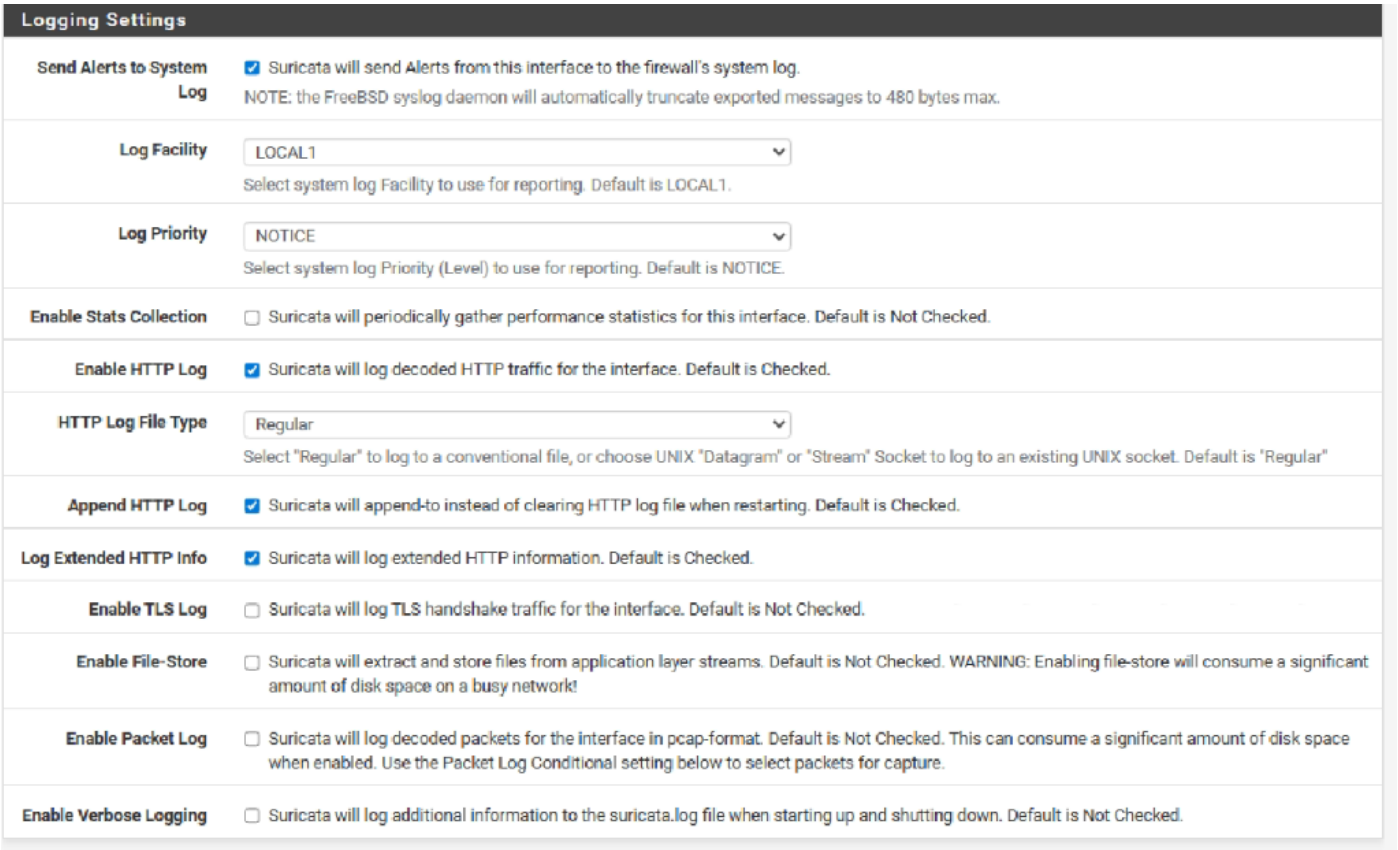

Ensuite pas besoins de trop toucher à General Settings et cliquer sur Save :




Rdv Dans l'onglet Interface cliquer sur Add Sélectionner votre interface WAN :



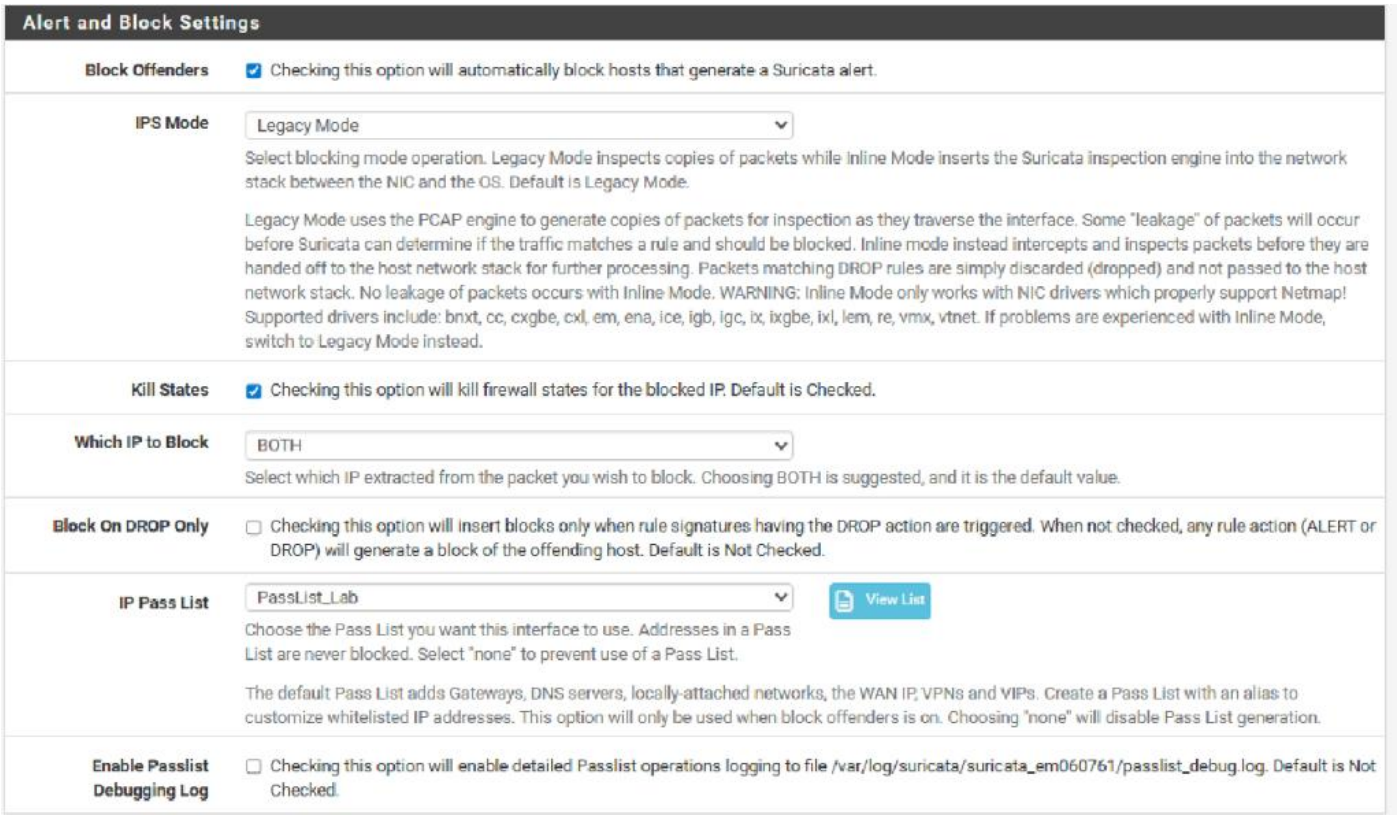
Sélectionner cette configuration cela vs nous permettre de connecter Wazuh plus tard :



**Logging Settings**

| | |
|---|---|
| **Send Alerts to System Log** | ☑ Suricata will send Alerts from this interface to the firewall's system log.<br>NOTE: the FreeBSD syslog daemon will automatically truncate exported messages to 480 bytes max. |
| **Log Facility** | LOCAL1<br>Select system log Facility to use for reporting. Default is LOCAL1. |
| **Log Priority** | NOTICE<br>Select system log Priority (Level) to use for reporting. Default is NOTICE. |
| **Enable Stats Collection** | ☐ Suricata will periodically gather performance statistics for this interface. Default is Not Checked. |
| **Enable HTTP Log** | ☑ Suricata will log decoded HTTP traffic for the interface. Default is Checked. |
| **HTTP Log File Type** | Regular<br>Select "Regular" to log to a conventional file, or choose UNIX "Datagram" or "Stream" Socket to log to an existing UNIX socket. Default is "Regular" |
| **Append HTTP Log** | ☑ Suricata will append-to instead of clearing HTTP log file when restarting. Default is Checked. |
| **Log Extended HTTP Info** | ☑ Suricata will log extended HTTP information. Default is Checked. |
| **Enable TLS Log** | ☐ Suricata will log TLS handshake traffic for the interface. Default is Not Checked. |
| **Enable File-Store** | ☐ Suricata will extract and store files from application layer streams. Default is Not Checked. WARNING: Enabling file-store will consume a significant amount of disk space on a busy network! |
| **Enable Packet Log** | ☐ Suricata will log decoded packets for the interface in pcap-format. Default is Not Checked. This can consume a significant amount of disk space when enabled. Use the Packet Log Conditional setting below to select packets for capture. |
| **Enable Verbose Logging** | ☐ Suricata will log additional information to the suricata.log file when starting up and shutting down. Default is Not Checked. |

Sélectionner bien Block Offenders c'est ce qui vas bloquer les adresse IP quand un scan ou une attaque et effectuer m'était le mode IPS en Inline Mode pour bloquer casi instantanément lorsqu'une attaque et effectué :

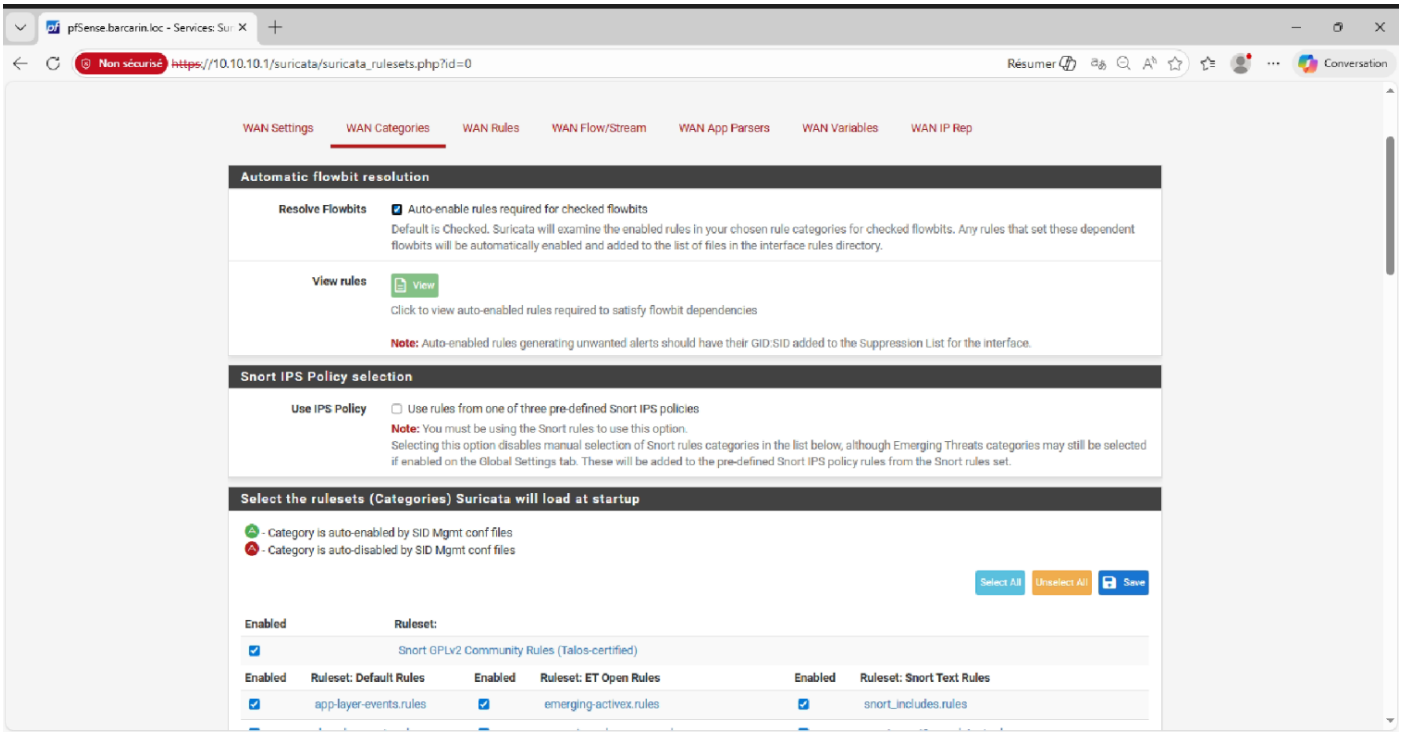


**Alert and Block Settings**

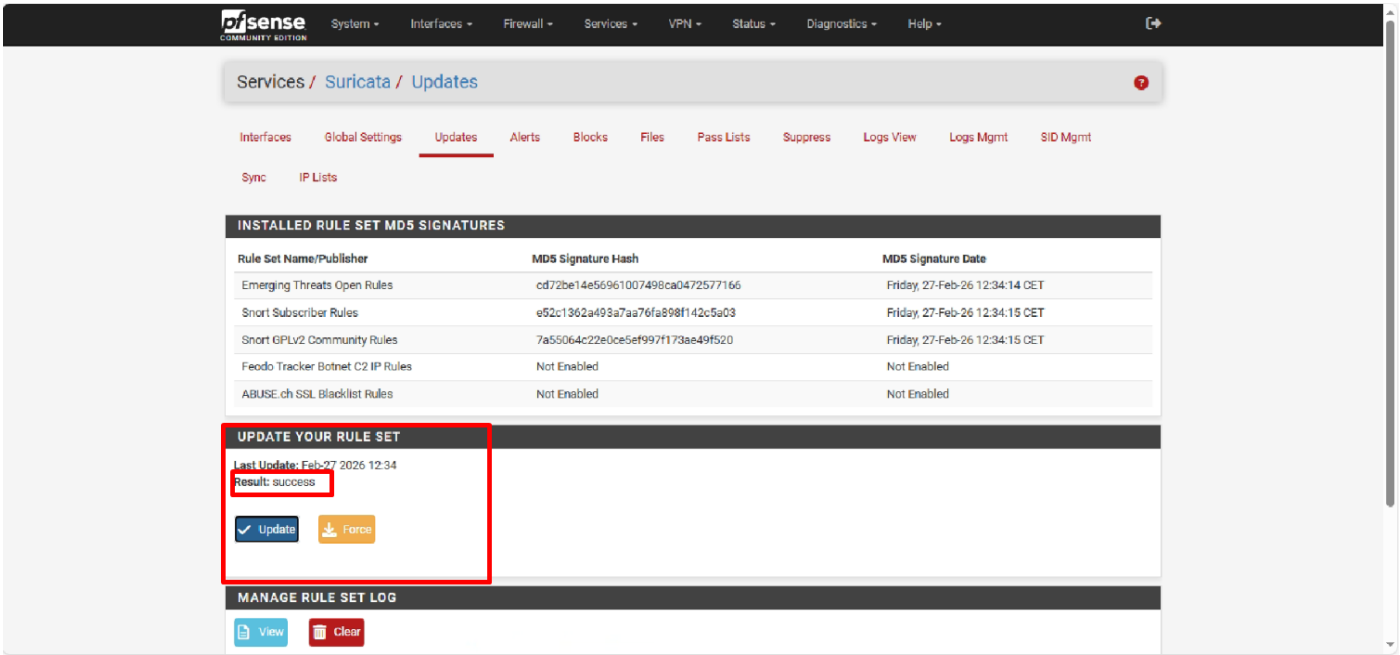
| | |
|---|---|
| **Block Offenders** | ☑ Checking this option will automatically block hosts that generate a Suricata alert. |
| **IPS Mode** | Legacy Mode<br>Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Suricata inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.<br>Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Suricata can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers include: bnxt, cc, cxgbe, cxl, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead. |
| **Kill States** | ☑ Checking this option will kill firewall states for the blocked IP. Default is Checked. |
| **Which IP to Block** | BOTH<br>Select which IP extracted from the packet you wish to block. Choosing BOTH is suggested, and it is the default value. |
| **Block On DROP Only** | ☐ Checking this option will insert blocks only when rule signatures having the DROP action are triggered. When not checked, any rule action (ALERT or DROP) will generate a block of the offending host. Default is Not Checked. |
| **IP Pass List** | PassList_Lab  View List<br>Choose the Pass List you want this interface to use. Addresses in a Pass List are never blocked. Select "none" to prevent use of a Pass List.<br>The default Pass List adds Gateways, DNS servers, locally-attached networks, the WAN IP, VPNs and VIPs. Create a Pass List with an alias to customize whitelisted IP addresses. This option will only be used when block offenders is on. Choosing "none" will disable Pass List generation. |
| **Enable Passlist Debugging Log** | ☐ Checking this option will enable detailed Passlist operations logging to file /var/log/suricata/suricata_em060761/passlist_debug.log. Default is Not Checked. |

Laisser le bloc « Performance and Detection Engine Settings » avec les paramétre par défaut qui suffise amplement pour notre lab vérifier bien le mode de promiscuité et bien cocher et Sauveguarder la conf :

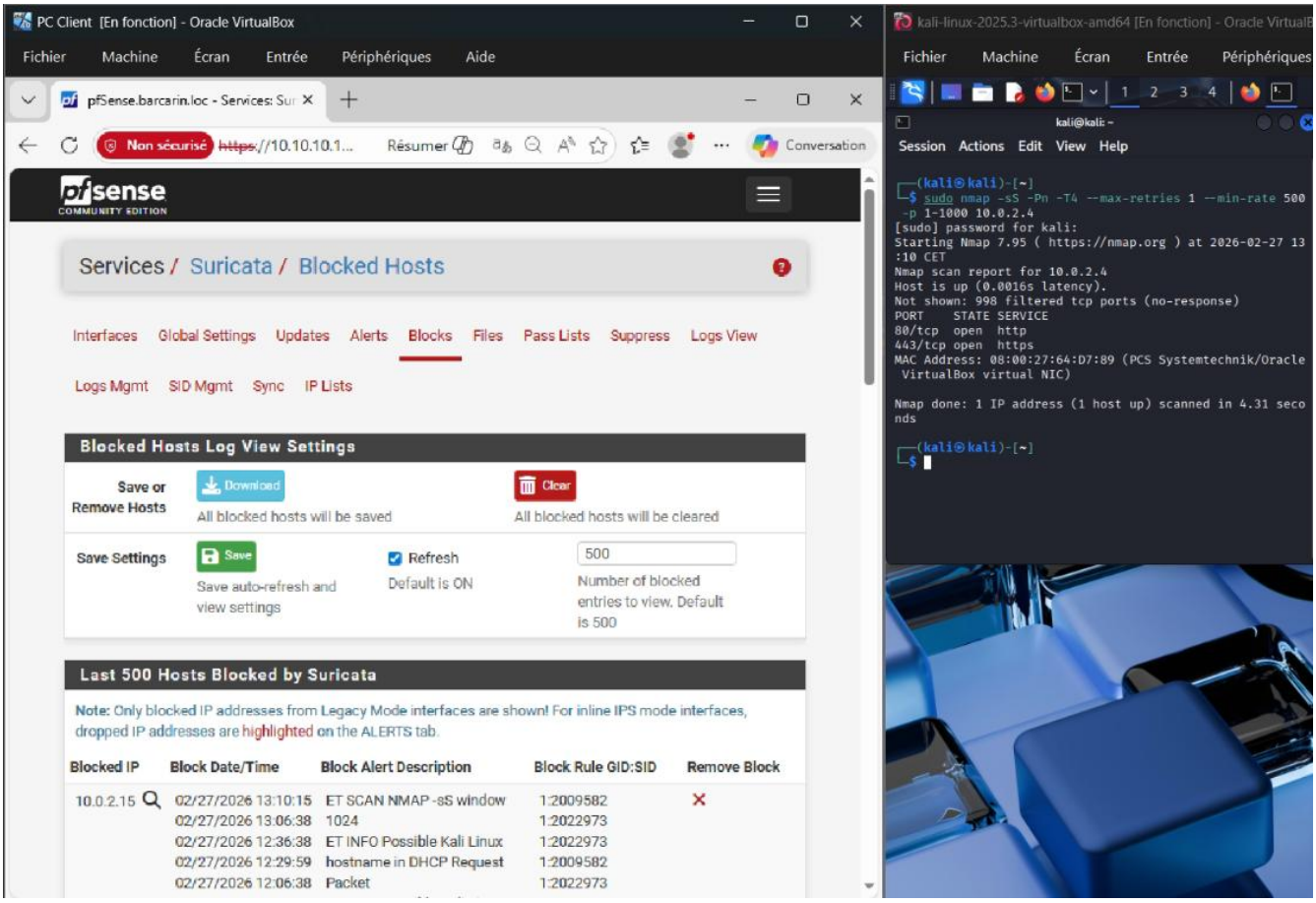

Ensuite dans WAN Catégorie cliquer sur Select All puis Save :



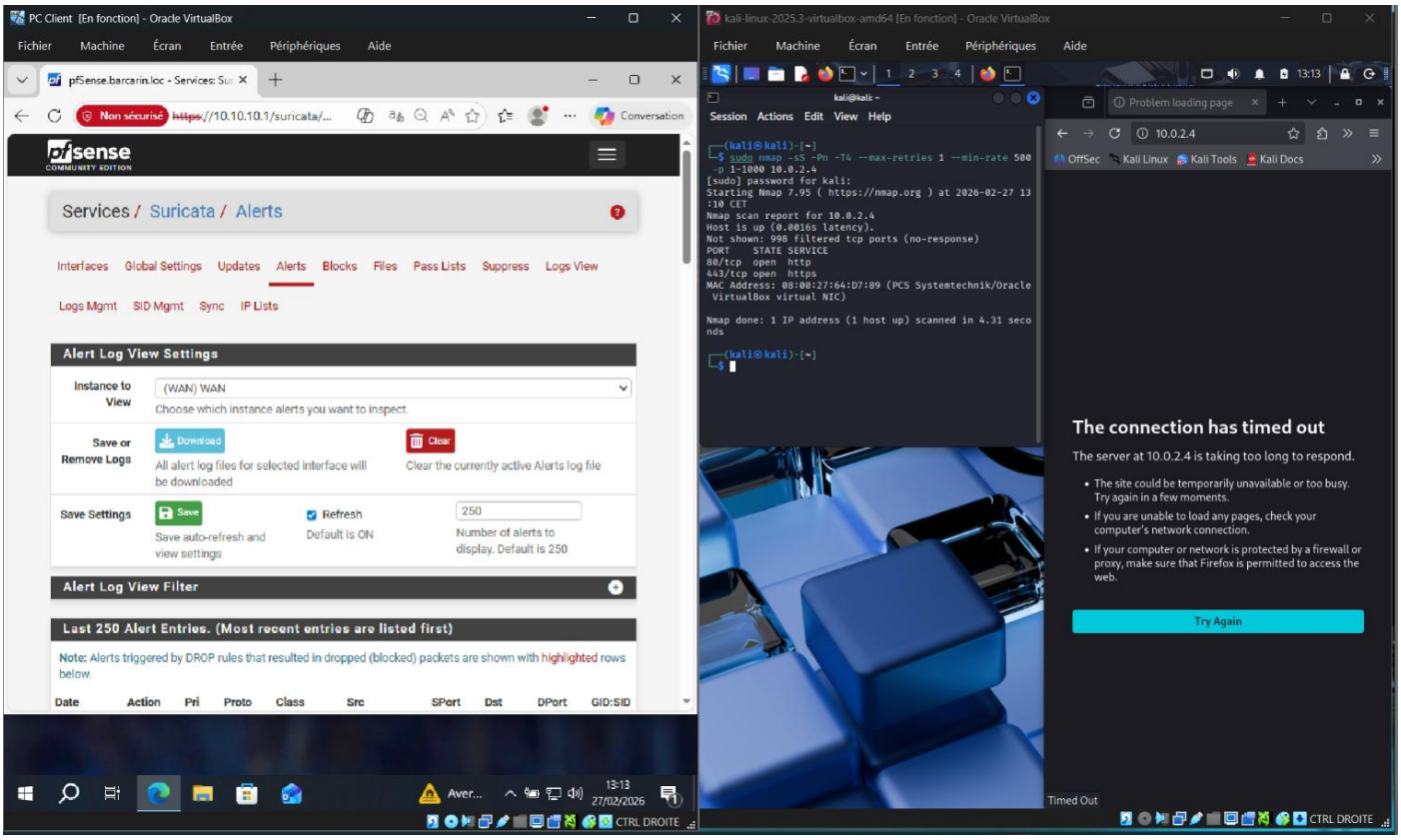

Ensuite rdv dans Update vérifier que cela ressemble à peut prés a ceci et cliquer sur Update vérifier ensuite que la MAJ a bien réussi sinon cliquer sur Force puis update :



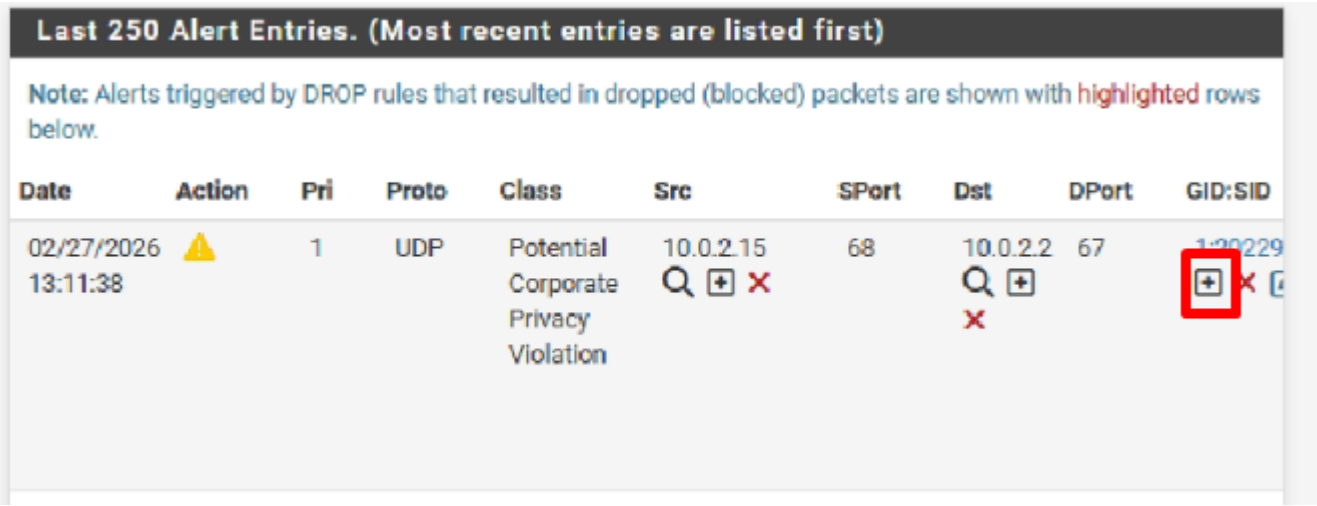
Ensuite rdv sur votre machine attaquant faite un nmap pour scanner l'interface WAN de PfSense puis rdv dans block pour vérifier quelle apparait bien dans les adresses bloquer : EX de commande nmap sudo nmap -sS -Pn -T4 --max-retries 1 --min-rate 500 -p 1-1000 @IP_A_SCANNER :



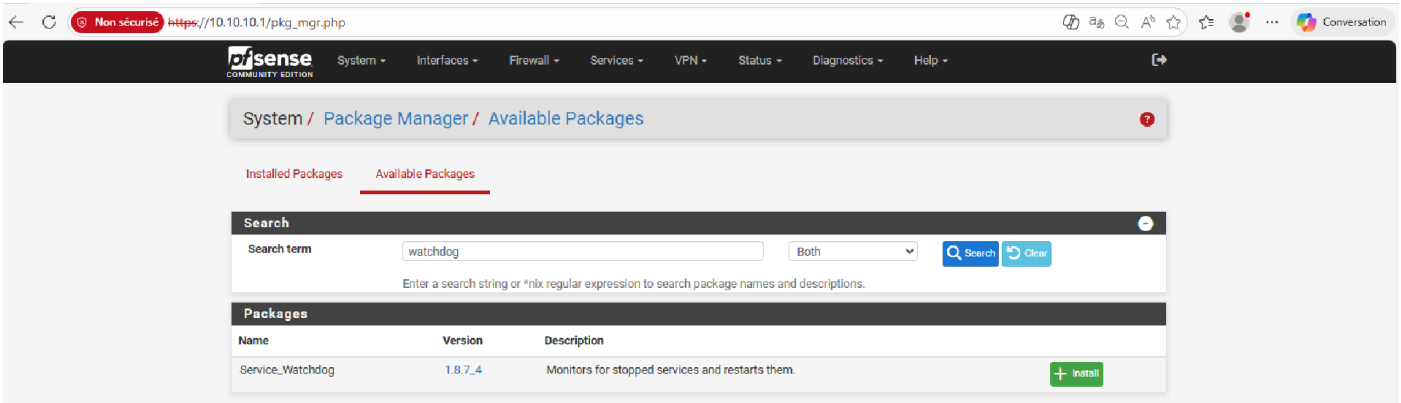

Vous pouvez aussi vous rendre dans Alerts et constatez que le scan a créé une alerte et que si j'essaie d'accéder au serveur web dans ma DMZ ça m'est impossible :



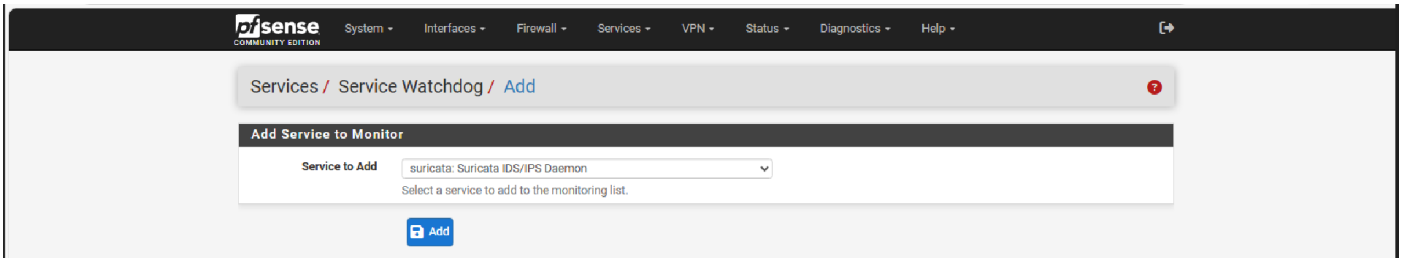
Si vous avez beaucoup d'alerte et de blocage pour rien a cause des Checksum notamment rdv dans alerts et cliquer sur ce bouton ça ajoutera une ligne a Suppress List ce qui vas masquer les alertes que vous trouverez inutile.




Pour terminer ou installe le Service_Watchdog pour que si Suricata Tombe pour une quelconque raison Suricata redémarre automatiquement :




Allé ensuite dans Service → Service_watchdog → add Service ajouter le service suricata et voila c'est fini :




Et voilà Suricata et installer configurer tester et marche très bien Bravo !!!