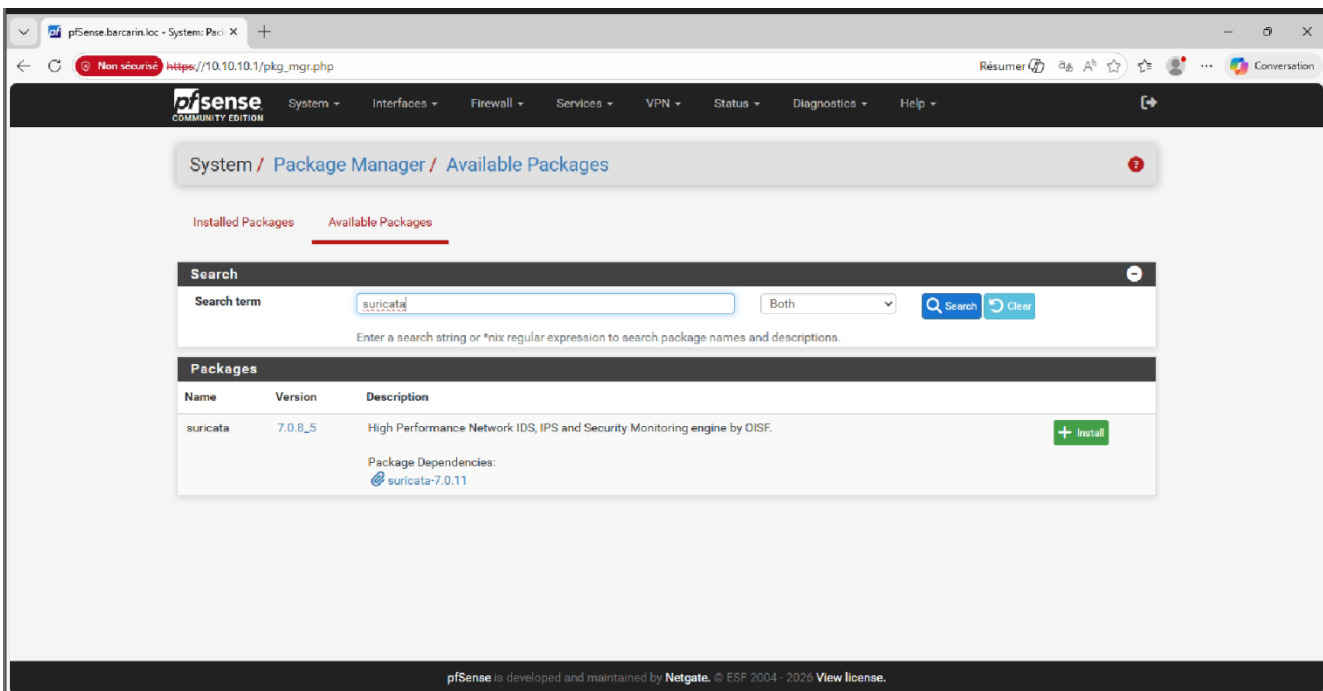


Procédure Installation et configuration Suricata dans pfsense:

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.

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 ETPro Emerging Threats rules ETPro for Suricata offers daily updates and extensive coverage of current malware threats. Use a custom URL for ETPro rule downloads
The ETPro rules contain all of the ETOpen rules, so the ETOpen rules are not required and are disabled when the ETPro rules are selected. [Sign Up for an ETPro Account](#). Enabling the custom URL option will force the use of a custom user-supplied URL when downloading ETPro rules.

Install Snort rules Snort free Registered User or paid Subscriber rules Use a custom URL for Snort rule downloads
[Sign Up for a free Registered User Rules Account](#)
[Sign Up for paid Snort Subscriber Rule Set \(by Talos\)](#)
Enabling the custom URL option will force the use of a custom user-supplied URL when downloading Snort Subscriber rules.

Snort Rules Filename
Enter the rules tarball filename (filename only, do not include the URL)
Example: snortrules-snapshot-29200.tar.gz
DO NOT specify a Snort3 rules file! Snort3 rules are incompatible with Suricata and will break your installation!

Snort Oinkmaster Code
Obtain a snort.org Oinkmaster code and paste it here.

Install Snort GPLv2 Community rules The Snort Community Ruleset is a GPLv2 Talos-certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. Use a custom URL for Snort GPLv2 rule downloads
This ruleset is updated daily and is a subset of the subscriber ruleset. If you are a Snort Subscriber Rules customer (paid subscriber), the community ruleset is already built into your download of the Snort Subscriber rules, and there is no benefit in adding this rule set separately.

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.

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 :

Rules Update Settings

Update interval 6 HOURS
Please select the interval for rule updates. Choosing NEVER disables auto-updates.
Hint: In most cases, every 12 hours is a good choice.

Update Start Time 00:00
Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.

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.

GeoLite2 DB Update Enable downloading of free GeoLite2 Country IP Database updates. Default is Not Checked
When enabled, Suricata will automatically download updates for the free GeoLite2 country IP database.
If you have a subscription for more current GeoIP2 updates, uncheck this option and instead create your own process to place the required database file in /usr/local/share/suricata/GeoLite2/.

GeoLite2 DB Account ID 1304644
To utilize the free MaxMind GeoLite2 GeoIP functionality, you must register for a free MaxMind user account. Use the GeoIP Update version 3.1.1 or newer registration option.

GeoLite2 DB License Key [REDACTED]
To utilize the free MaxMind GeoLite2 GeoIP functionality, you must register for a free MaxMind user account. Use the GeoIP Update version 3.1.1 or newer registration option.

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

General Settings

Remove Blocked Hosts Interval 1 HOUR
Please select the amount of time you would like hosts to be blocked. Note this setting is only applicable when using Legacy Mode blocking! This setting is ignored when using Inline IPS Mode.
Hint: in most cases, 1 hour is a good choice.

Log to System Log Copy Suricata messages to the firewall system log.

Log Facility LOCAL1
Select system log facility to use for reporting. Default is LOCAL1.

Log Priority NOTICE
Select system log Priority (Level) to use for reporting. Default is NOTICE.

Keep Suricata Settings After Deinstall Settings will not be removed during package deinstallation.

Clear Blocked Hosts After Deinstall Click to clear all blocked hosts added by Suricata when removing the package. Default is checked.

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

General Settings

Enable Checking this box enables Suricata inspection on the interface.

Interface WAN (em0)
Choose which interface this Suricata instance applies to. In most cases, you will want to choose LAN here if this is the first Suricata-configured interface.

Description WAN
Enter a meaningful description here for your reference. The default is the pfSense interface friendly description.

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

Logging Settings	
Send Alerts to System Log	<input checked="" type="checkbox"/> Suricata will send Alerts from this interface to the firewall's system log. NOTE: the FreeBSD syslog daemon will automatically truncate exported messages to 480 bytes max.
Log Facility	LOCAL1 Select system log Facility to use for reporting. Default is LOCAL1.
Log Priority	NOTICE Select system log Priority (Level) to use for reporting. Default is NOTICE.
Enable Stats Collection	<input type="checkbox"/> Suricata will periodically gather performance statistics for this interface. Default is Not Checked.
Enable HTTP Log	<input checked="" type="checkbox"/> Suricata will log decoded HTTP traffic for the interface. Default is Checked.
HTTP Log File Type	Regular 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	<input checked="" type="checkbox"/> Suricata will append-to instead of clearing HTTP log file when restarting. Default is Checked.
Log Extended HTTP Info	<input checked="" type="checkbox"/> Suricata will log extended HTTP information. Default is Checked.
Enable TLS Log	<input type="checkbox"/> Suricata will log TLS handshake traffic for the interface. Default is Not Checked.
Enable File-Store	<input type="checkbox"/> 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	<input type="checkbox"/> 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	<input type="checkbox"/> Suricata will log additional information to the suricata.log file when starting up and shutting down. Default is Not Checked.

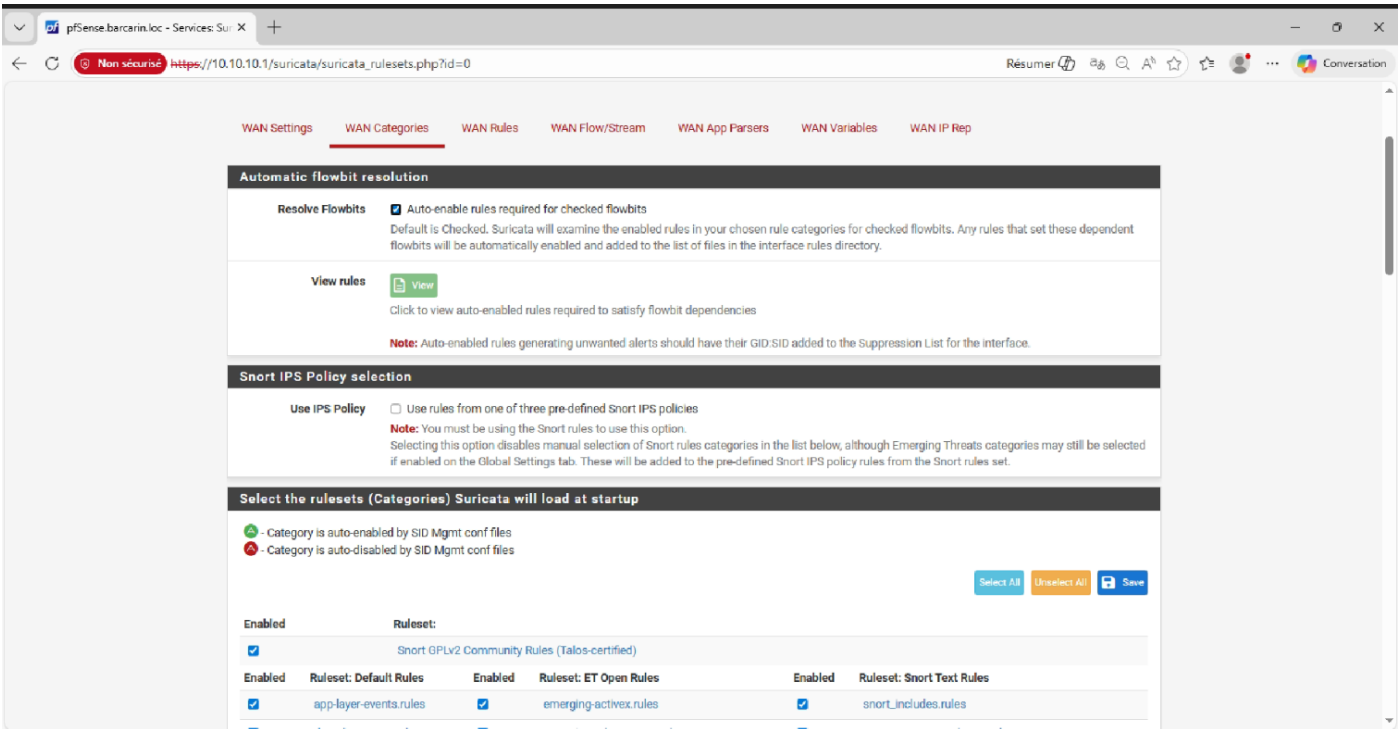
Sélectionner bien Block Offenders c'est ce qui vas bloquer les adresse IP quand un scan ou une attaque et effectuer m'était le mode IPS en Inline Mode pour bloquer casi instantanément lorsqu'une attaque et effectué :

Alert and Block Settings	
Block Offenders	<input checked="" type="checkbox"/> Checking this option will automatically block hosts that generate a Suricata alert.
IPS Mode	Legacy Mode 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. 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	<input checked="" type="checkbox"/> Checking this option will kill firewall states for the blocked IP. Default is Checked.
Which IP to Block	BOTH 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	<input type="checkbox"/> 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 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. 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	<input type="checkbox"/> Checking this option will enable detailed Passlist operations logging to file /var/log/suricata/suricata_em060761/passlist_debug.log. Default is Not Checked.

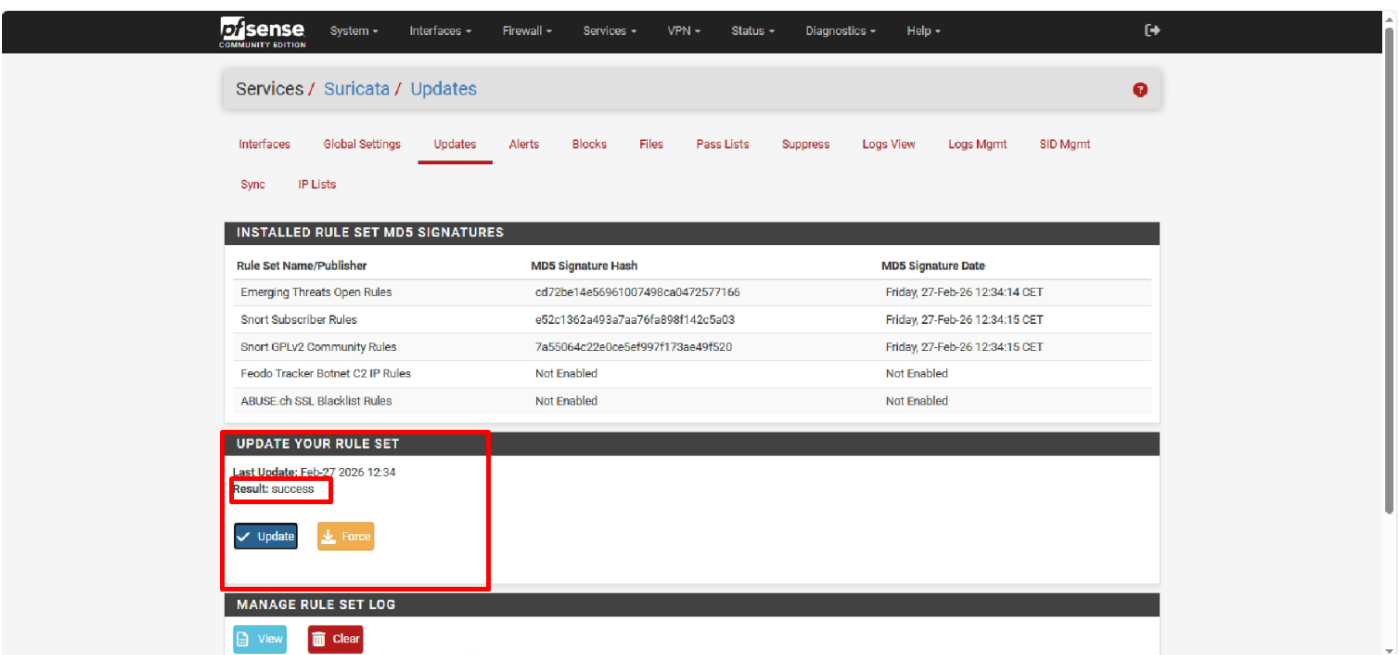
Laisser le bloc « Performance and Detection Engine Settings » avec les paramètres par défaut qui suffisent amplement pour notre lab vérifier bien le mode de promiscuité et bien cocher et Sauvegarder la conf :



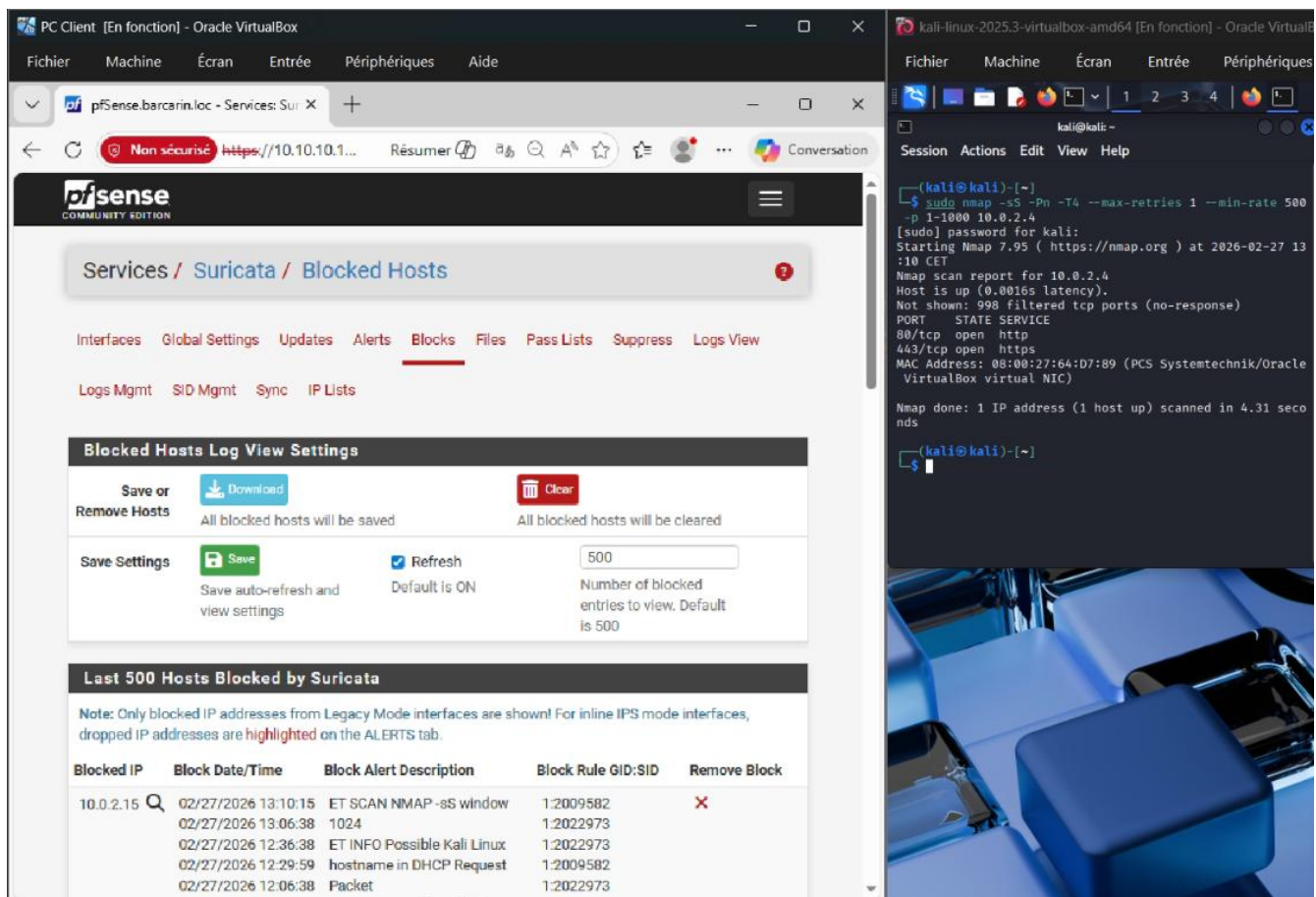
Ensuite dans WAN Catégorie cliquer sur Select All puis Save :



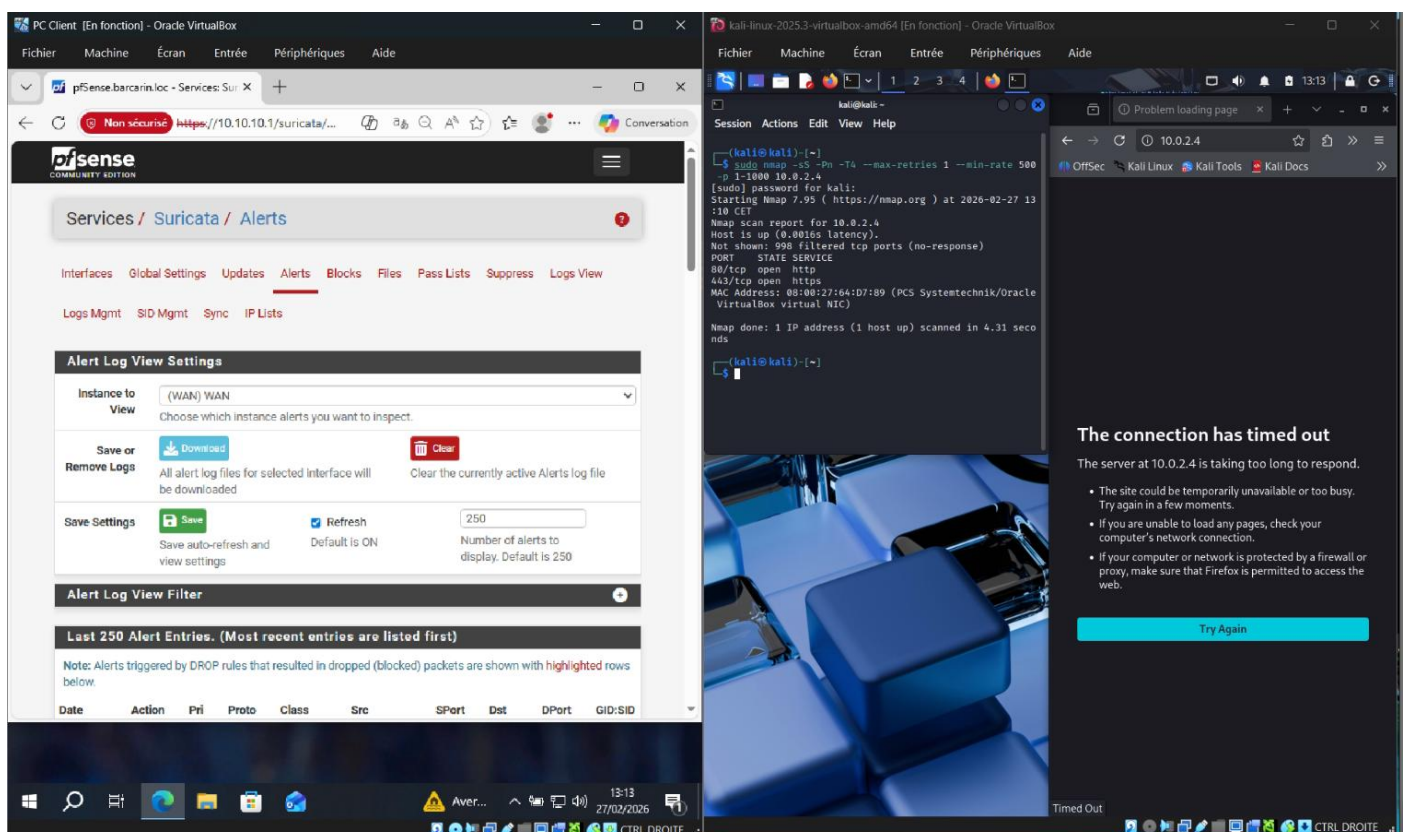
Ensuite rdv dans Update vérifier que cela ressemble à peu près à ceci et cliquer sur Update vérifier ensuite que la MAJ a bien réussi sinon cliquer sur Force puis update :



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 :



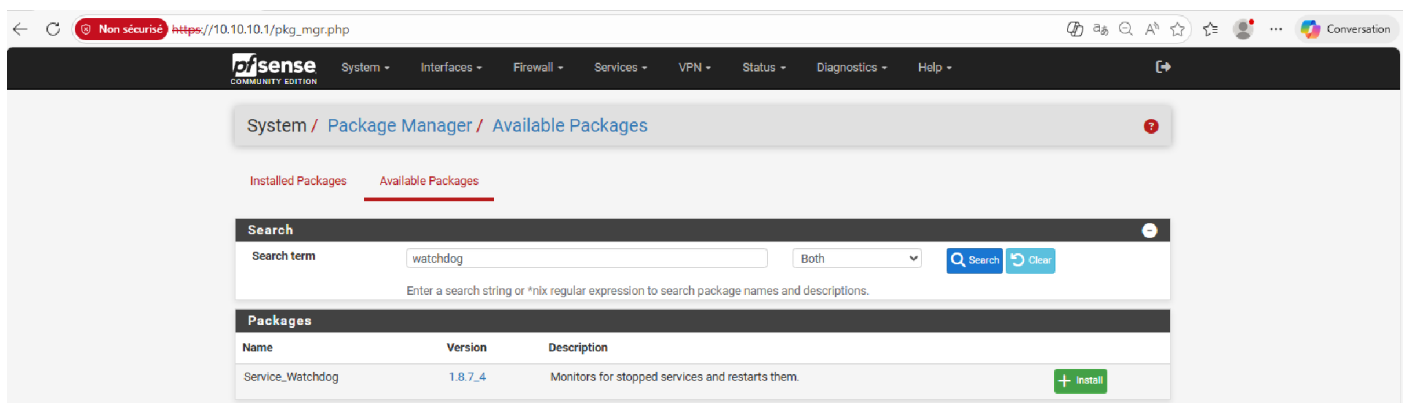
Si vous avez beaucoup d'alerte et de blocage pour rien a cause des Checksum notamment rdv dans alerts et cliquer sur ce bouton ça ajoutera une ligne a Suppress List ce qui vas masquer les alertes que vous trouverez inutile.

Last 250 Alert Entries. (Most recent entries are listed first)

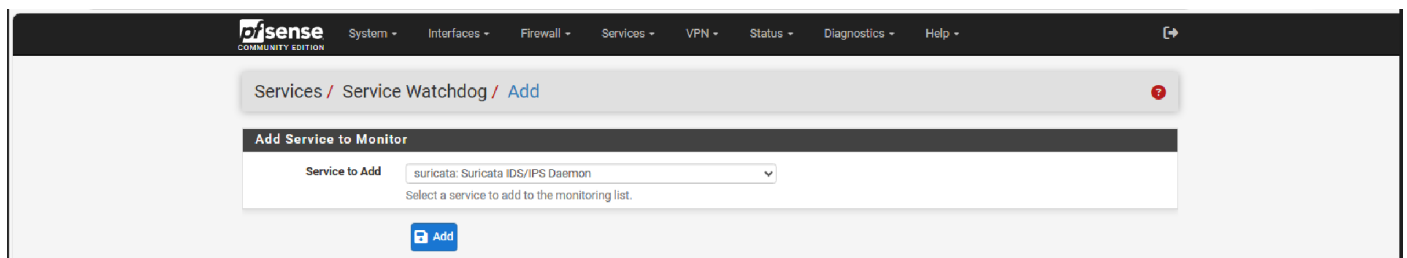
Note: Alerts triggered by DROP rules that resulted in dropped (blocked) packets are shown with highlighted rows below.

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID
02/27/2026 13:11:38	⚠	1	UDP	Potential Corporate Privacy Violation	10.0.2.15 🔍 + ✖	68	10.0.2.2 🔍 + ✖	67	1:20229 🔍 + ✖

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 !!!