

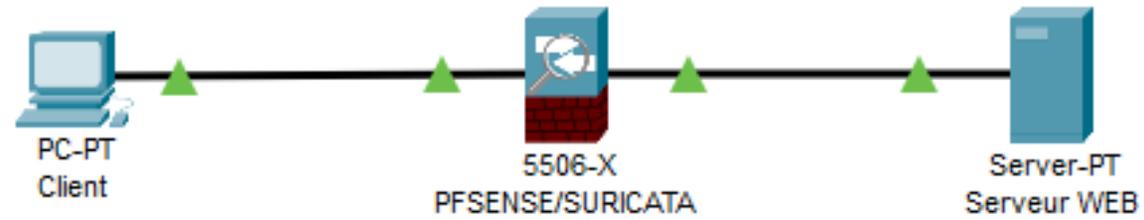


Suricata

TP IDS Suricata

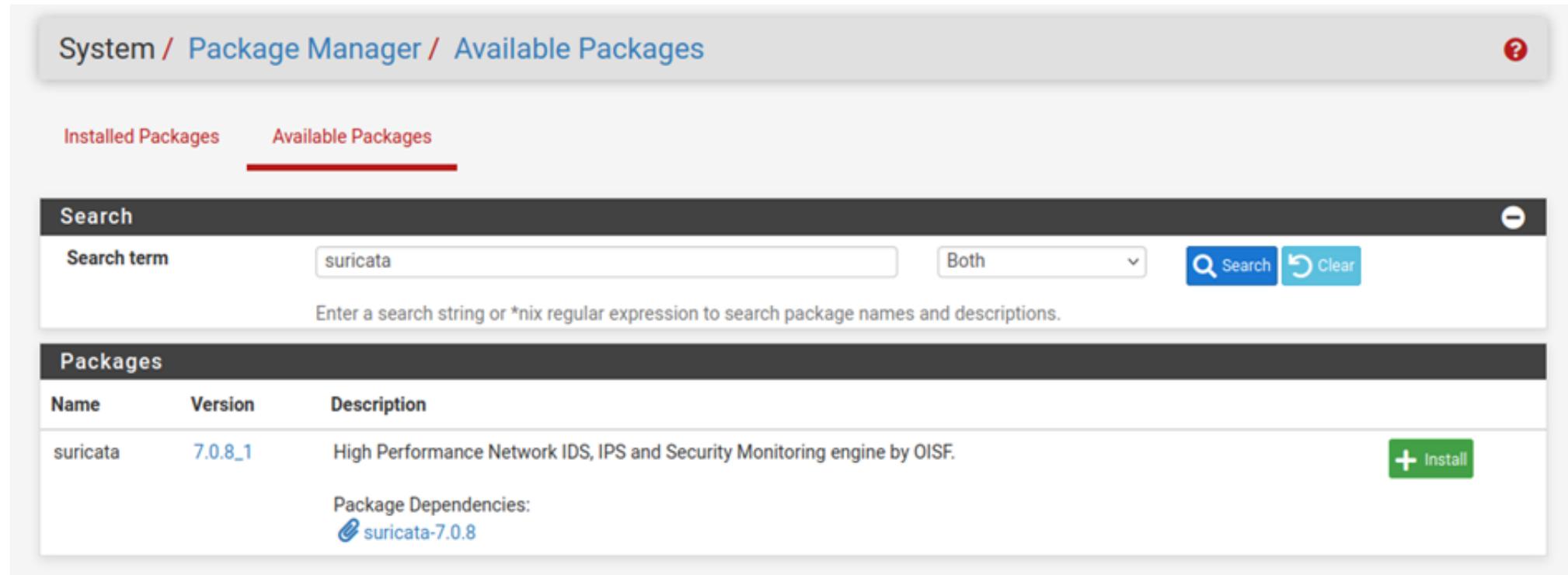
FLORENTIN BRACQ- -FLABAT, BTS 2 SIO

Schéma réseau



Installation de Suricata sur Pfsense

Se rendre dans le gestionnaire de paquets de Pfsense pour rechercher et installer Suricata



The screenshot shows the Pfsense Package Manager interface. At the top, there is a breadcrumb trail: "System / Package Manager / Available Packages". Below this, there are two tabs: "Installed Packages" and "Available Packages", with the latter being selected. A search bar is present with the search term "suricata" and a dropdown menu set to "Both". There are "Search" and "Clear" buttons. Below the search bar, there is a table of packages. The table has columns for "Name", "Version", and "Description". One package is listed: "suricata" with version "7.0.8_1" and description "High Performance Network IDS, IPS and Security Monitoring engine by OISF.". To the right of the package name is a green "+ Install" button. Below the description, there is a section for "Package Dependencies:" which lists "suricata-7.0.8".

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term: Both

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description
suricata	7.0.8_1	High Performance Network IDS, IPS and Security Monitoring engine by OISF.

Package Dependencies:
suricata-7.0.8

+ Install

Configuration de Suricata

Dans un premier temps, nous allons nous rendre dans Global Settings

On renseigne :

Install ETOpen Emerging Threats rules : cocher la case ETOpen...

Install Snort GPLv2 Community rules : The Snort...

Update Start Time : l'heure de vous voulez

GeoLite2 DB Update : cocher si vous avez un compte sur le site MaxMind (la création du compte et l'utilisation de DB est gratuite)

Il ne reste plus qu'à enregistrer

Configuration de Suricata

Services / Suricata / Global Settings

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

Sync IP Lists

Please Choose The Type Of Rules You Wish To Download

Install ETOpen Emerging Threats rules	<input checked="" type="checkbox"/> ETOpen is a free open source set of Suricata rules whose coverage is more limited than ETPro.	<input type="checkbox"/> 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	<input type="checkbox"/> ETPro for Suricata offers daily updates and extensive coverage of current malware threats.	<input type="checkbox"/> 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	<input type="checkbox"/> Short free Registered User or paid Subscriber rules	<input type="checkbox"/> 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.		
Install Snort GPLv2 Community rules	<input checked="" type="checkbox"/> The Snort Community Ruleset is a GPLv2 Talos-certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions.	<input type="checkbox"/> 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		

Rules Update Settings

Update Interval NEVER
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 00:19
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 Enter your MaxMind GeoLite2 Account ID
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 Enter your MaxMind GeoLite2 License Key
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.

General Settings

Remove Blocked Hosts Interval NEVER
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.

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.

Configuration de Suricata

Se rendre ensuite dans l'onglet Updates. Dans cette partie, nous pouvons voir les paquets de règles, forcer les mises à jour et voir s'il y a des problèmes.

Services / Suricata / Updates ?

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

Sync IP Lists

INSTALLED RULE SET MD5 SIGNATURES

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 Downloaded	Not Downloaded
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled
ABUSE.ch SSL Blacklist Rules	Not Enabled	Not Enabled

UPDATE YOUR RULE SET

Last Update: Unknown
Result: Unknown

[✓ Update](#) [⬇ Force](#)

UPDATE YOUR RULE SET

Last Update: Mar-25 2025 15:13
Result: success

[✓ Update](#) [⬇ Force](#)

Configuration de Suricata

Pour configurer Suricata, se rendre dans services, puis Suricata, dans Interfaces en dessous de General Settings, cocher la case enable pour activer Suricata et sélectionner l'interface LAN.

General Settings	
Enable	<input checked="" type="checkbox"/> Checking this box enables Suricata inspection on the interface.
Interface	<input type="text" value="LAN (vtnet1)"/> 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	<input type="text" value="LAN"/> Enter a meaningful description here for your reference. The default is the pfSense interface friendly description.

Configuration de Suricata

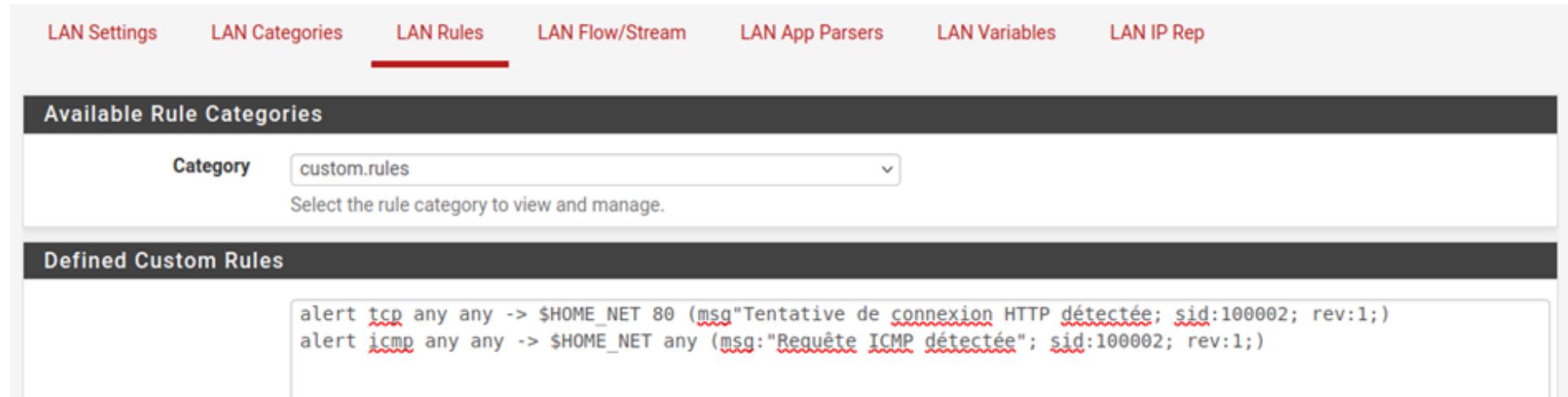
Passage en mode IDS

Dans Logging Settings cacher la case Send Alerts to System Log, penser à cliquer sur save pour enregistrer les modifications

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.

Configuration de Suricata

Dans LAN Rules, dans la catégorie custom.rules, créer les règles suivantes



The screenshot shows the Suricata configuration interface with the following elements:

- Navigation tabs: LAN Settings, LAN Categories, LAN Rules (selected), LAN Flow/Stream, LAN App Parsers, LAN Variables, LAN IP Rep.
- Section: Available Rule Categories
- Category dropdown: custom.rules
- Text: Select the rule category to view and manage.
- Section: Defined Custom Rules
- Code block containing two rules:

```
alert tcp any any -> $HOME_NET 80 (msg"Tentative de connexion HTTP détectée; sid:100002; rev:1;)
alert icmp any any -> $HOME_NET any (msg:"Requête ICMP détectée"; sid:100002; rev:1;)
```

Test

Test suricata ping serveur :

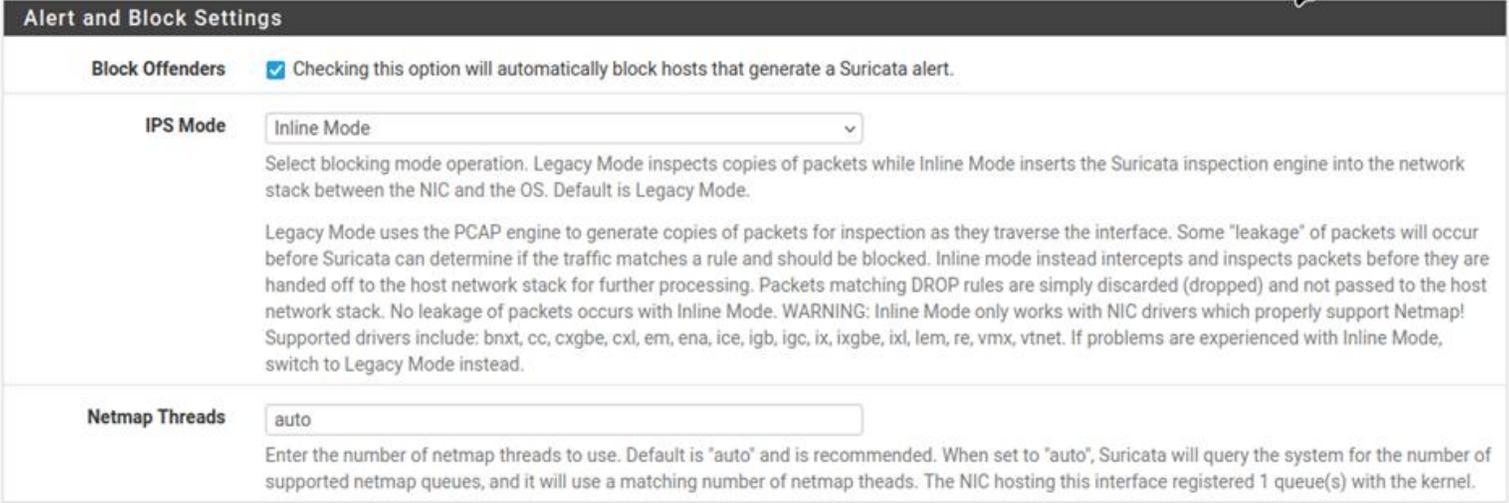
Last 250 Alert Entries. (Most recent entries are listed first)										
Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
04/04/2025 13:03:34		3	IPv6- ICMP	Not Assigned	fe80::26dd:cb73: b89e:9b5f   	135	fe80::be24:11ff:fe94: 936f   	0	1:100002  	Requête ICMP détectée
04/04/2025 13:03:33		3	UDP	Generic Protocol Command Decode	192.168.1.109  	37725	34.117.188.166   	443	1:2231000  	SURICATA QUIC failed decrypt

Test suricata ouverture page web http :

Last 250 Alert Entries. (Most recent entries are listed first)										
Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
04/04/2025 13:06:04		3	UDP	Generic Protocol Command Decode	192.168.1.109  	48883	34.117.188.166   	443	1:2231000  	SURICATA QUIC failed decrypt

Passage en mode IPS

Pour activer le mode IPS se rendre dans Services/Suricata puis LAN settings du LAN



The screenshot shows the 'Alert and Block Settings' configuration page. It includes three main sections: 'Block Offenders' with a checked checkbox and explanatory text; 'IPS Mode' with a dropdown menu set to 'Inline Mode' and detailed text explaining the difference between Legacy and Inline modes; and 'Netmap Threads' with a text input field set to 'auto' and explanatory text.

Alert and Block Settings

Block Offenders Checking this option will automatically block hosts that generate a Suricata alert.

IPS 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.

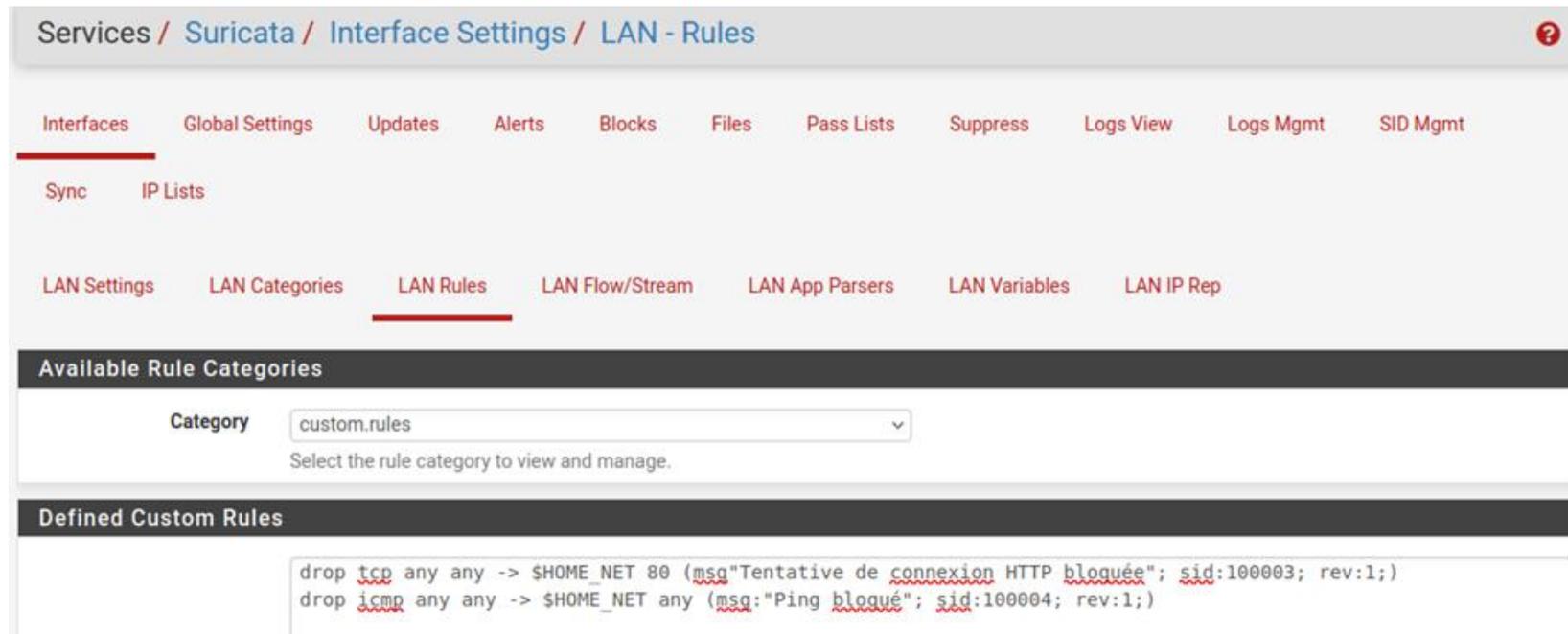
Netmap Threads

Enter the number of netmap threads to use. Default is "auto" and is recommended. When set to "auto", Suricata will query the system for the number of supported netmap queues, and it will use a matching number of netmap threads. The NIC hosting this interface registered 1 queue(s) with the kernel.

Penser à cliquer sur save pour enregistrer les modifications

Modifications des règles

Modifier les règles pour bloquer certaines activités



The screenshot displays the Suricata web interface for configuring LAN rules. The breadcrumb trail at the top reads "Services / Suricata / Interface Settings / LAN - Rules". A navigation menu below includes "Interfaces", "Global Settings", "Updates", "Alerts", "Blocks", "Files", "Pass Lists", "Suppress", "Logs View", "Logs Mgmt", and "SID Mgmt". Under "Interfaces", "Sync" and "IP Lists" are visible. The "LAN Rules" tab is selected in the "LAN Settings" section. Below this, the "Available Rule Categories" section features a dropdown menu set to "custom.rules" with the instruction "Select the rule category to view and manage." The "Defined Custom Rules" section contains a text area with the following rule definitions:

```
drop tcp any any -> $HOME_NET 80 (msg:"Tentative de connexion HTTP bloquée"; sid:100003; rev:1;)
drop icmp any any -> $HOME_NET any (msg:"Ping bloqué"; sid:100004; rev:1;)
```

Vérification

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	Description
04/06/2025 17:48:34		3	IPv6- ICMP	Not Assigned	fe80::26dd:cb73: b89e:9b5f 	135	fe80::be24:11ff:fe94: 936f 	0	1:100004 	Ping bloqué
04/06/2025 17:43:34		3	IPv6- ICMP	Not Assigned	fe80::26dd:cb73: b89e:9b5f 	135	fe80::be24:11ff:fe94: 936f 	0	1:100004 	Ping bloqué
04/06/2025 17:42:28		3	UDP	Generic Protocol Command Decode	192.168.1.109 	39916	34.117.188.166 	443	1:2231000 	SURICATA QUIC failed decrypt
04/06/2025 17:38:34		3	IPv6- ICMP	Not Assigned	fe80::26dd:cb73: b89e:9b5f 	135	fe80::be24:11ff:fe94: 936f 	0	1:100002 	Requête ICMP détectée
04/06/2025 17:33:20		3	IPv6- ICMP	Not Assigned	fe80::26dd:cb73: b89e:9b5f 	135	fe80::be24:11ff:fe94: 936f 	0	1:100002 	Requête ICMP détectée
04/06/2025 17:32:22		3	IPv6- ICMP	Not Assigned	fe80::26dd:cb73: b89e:9b5f 	135	fe80::be24:11ff:fe94: 936f 	0	1:100002 	Requête ICMP détectée

Sources

<https://www.ctechmat.fr/pfsense-paquet-suricata/>