

# Installation Suricata sur Pfsense

## Introduction :

Pour assurer la sécurité d'un réseau, vous pouvez déployer des systèmes IDS ou IPS.

Il est recommandé de commencer par configurer un système en mode IDS avant de le transformer en système IPS. Activer Suricata en mode IPS dès le départ pourrait être déroutant. Il est conseillé d'observer d'abord ce qui se passe sur le réseau afin d'éviter de générer trop d'alertes et de blocages faux positifs.

**IDS (Intrusion Detection System) et IPS (Intrusion Prevention System)** sont des systèmes de sécurité réseau conçus pour détecter et gérer les menaces.

- **IDS (Système de Détection d'Intrusions)** : Il surveille le trafic réseau et signale les activités suspectes sans les bloquer. Il est principalement utilisé pour analyser et alerter en cas de tentative d'attaque.
- **IPS (Système de Prévention d'Intrusions)** : Il agit comme un IDS, mais en plus, il peut bloquer automatiquement les menaces détectées afin de protéger le réseau en temps réel.

Ces systèmes sont essentiels pour améliorer la sécurité en détectant ou empêchant les intrusions malveillantes avant qu'elles n'affectent les systèmes informatiques.

## Installation et configuration de Suricata en mode IDS

Suricata, un système IDS/IPS, peut être installé en tant que package autonome sans pfSense, mais il est particulièrement utile lorsqu'il est utilisé avec une installation de pare-feu/routeur.








### Installation sous pfSense






1. Accédez à System > Package Manager > Available Packages.
2. Recherchez Suricata dans la liste des paquets disponibles.
3. Cliquez sur Installer et attendez la fin du processus.

Une fois installé, Suricata peut être configuré en mode IDS pour détecter les menaces sans bloquer automatiquement le trafic.

Installed Packages

Available Packages

Installed Packages				
Name	Category	Version	Description	Actions
✓ haproxy	net	0.61_7	The Reliable, High Performance TCP/HTTP(S) Load Balancer. This package implements the TCP, HTTP and HTTPS balancing features from haproxy. Supports ACLs for smart backend switching.  Package Dependencies: <a href="#">haproxy18-1.8.30</a>	  
✓ openvpn-client-export	security	1.6_4	Allows a pre-configured OpenVPN Windows Client or Mac OS X's Viscosity configuration bundle to be exported directly from pfSense.  Package Dependencies: <a href="#">openvpn-client-export-2.5.2</a> <a href="#">openvpn-2.5.4_1</a> <a href="#">zip-3.0_1</a> <a href="#">p7zip-16.02_3</a>	 
✓ suricata	security	6.0.4_1	High Performance Network IDS, IPS and Security Monitoring engine by OISF.  Package Dependencies: <a href="#">suricata-6.0.4</a>	 

 = Update  = Current  
 = Remove  = Information  = Reinstall  
Newer version available  
Package is configured but not (fully) installed or deprecated

Après l'installation, la page de configuration de **Suricata** est accessible via le menu **Services**.

## Configuration initiale

1. Accédez à **Services > Suricata**.
2. Commencez par les **Global Settings** (paramètres globaux).
3. Cochez les options suivantes :
  - **Install ETOpen Emerging Threats rules** (Installer les règles ETOpen Emerging Threats).
  - **Hide Deprecated Rules Categories** (Masquer les catégories de règles obsolètes).

Cela permet d'activer un ensemble de règles de détection des menaces et de masquer celles qui ne sont plus pertinentes.

Please Choose The Type Of Rules You Wish To Download	
<b>Install ETOpen Emerging Threats rules</b>	<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.
<b>Install ETPro Emerging Threats rules</b>	<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. <a href="#">Sign Up for an ETPro Account</a> . Enabling the custom URL option will force the use of a custom user-supplied URL when downloading ETPro rules.
<b>Install Snort rules</b>	<input type="checkbox"/> Snort free Registered User or paid Subscriber rules <input type="checkbox"/> Use a custom URL for Snort rule downloads <a href="#">Sign Up for a free Registered User Rules Account</a> <a href="#">Sign Up for paid Snort Subscriber Rule Set (by Talos)</a> Enabling the custom URL option will force the use of a custom user-supplied URL when downloading Snort Subscriber rules.
<b>Install Snort GPLv2 Community rules</b>	<input 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 ruleset is already built into your download of the Snort Subscriber rules, and there is no benefit in adding this rule set separately.
<b>Install Feodo Tracker Botnet C2 IP rules</b>	<input checked="" type="checkbox"/> The Feodo Botnet C2 IP Ruleset contains Dridex and Emotet/Heodo botnet command and control servers (C&Cs) tracked by Feodo Tracker.
<b>Install ABUSE.ch SSL Blacklist rules</b>	<input checked="" type="checkbox"/> The ABUSE.ch SSL Blacklist Ruleset contains the SSL cert fingerprints of all SSL certs blacklisted by ABUSE.ch.
<b>Hide Deprecated Rules Categories</b>	<input checked="" type="checkbox"/> Hide deprecated rules categories in the GUI and remove them from the configuration. Default is Not Checked.
<b>Download Extra Rules</b>	<input type="checkbox"/> Download Extra Rules Download extra rules file or tar.gz archive with rules. If "Check MD5" is set, the code will assume a matching filename exists at the same URL with an additional extension of ".md5".

Ensuite, dans les paramètres globaux :

- Sélectionnez la fréquence de mise à jour** dans le menu déroulant **"Update Interval"**.
  - Je recommande de choisir **"1 DAY"** (1 jour) pour des mises à jour régulières des règles de détection.
- Activez l'option "Live Rule Swap on Update"** (Remplacement en direct des règles lors de la mise à jour).
  - Cette option permet de recharger les règles sans redémarrer complètement le service, évitant ainsi une interruption du trafic.

### Rules Update Settings

**Update Interval**    
 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**    
 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 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**    
 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.

Pour "**Remove Blocked Hosts Interval**", choisissez une durée entre **6 et 24 heures**, selon votre système. Même si vous ne démarrez pas en mode IPS, configurez cette option dès le début pour éviter d'avoir à y revenir plus tard.

Ensuite, allez dans l'onglet **Updates** et forcez le téléchargement des règles. Cela ne se fait pas toujours automatiquement, donc dès que possible, cliquez sur **Update**.

### INSTALLED RULE SET MD5 SIGNATURES

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Emerging Threats Open Rules	df07a0ec8dbeef399fe65916e31a6ed7	Friday, 23-Sep-22 00:31:26 CEST
Snort Subscriber Rules	Not Enabled	Not Enabled
Snort GPLv2 Community Rules	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP Rules	f59dc9eb22d2d1503bf34969dfd0d922	Wednesday, 21-Sep-22 00:31:13 CEST
ABUSE.ch SSL Blacklist Rules	62e1c716daa8bd93ce70dff91fc5c60a	Friday, 16-Sep-22 00:31:14 CEST

### UPDATE YOUR RULE SET

**Last Update:** Sep-23 2022 00:31   
**Result:** success

△ Si tu rencontres des problèmes liés à des paquets obsolètes, la meilleure solution est de mettre à jour PfSense en premier.

Pour la configuration des interfaces :

1. Va dans l'onglet **Interfaces**.
2. Clique sur **Ajouter une interface**.
3. Active Suricata sur l'interface souhaitée.
4. Configure le mode d'inspection (mode en ligne ou mode hérité)

WAN Settings   WAN Categories   WAN Rules   WAN Flow/Stream   WAN App Parsers   WAN Variables   WAN IP Rep

### General Settings

**Enable**  Checking this box enables Suricata inspection on the interface.

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

### Logging Settings

**Send Alerts to System Log**  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.

**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.

**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.

**Enable Verbose Logging**  Suricata will log additional information to the suricata.log file when starting up and shutting down. Default is Not Checked.

[SS](#)

Tu peux tester différentes options ici pour **TLS**, **file-store** et **packet log**.

À part **TLS**, les autres nécessitent beaucoup d'espace disque sur un réseau très actif. Pense donc à allouer suffisamment de stockage.

Il y a une autre chose à configurer dans cette section : le **Detect-Engine Profile**. Je recommande de le mettre sur **High** plutôt que le réglage par défaut **Medium**.

Pour l'instant, on ne bloque pas les attaquants. On reste en mode **IDS** (détection) plutôt qu'en **IPS** (prévention).

Pour les tests, je recommande d'activer les catégories de règles "**3coresec**", "**compromised**" et "**scan**".

Une fois cela fait :

1. Va dans l'onglet **Interfaces** et redémarre Suricata sur l'interface concernée.
2. Si Suricata ne démarre pas, va dans l'onglet **Logs View** et consulte **suricata.log** pour voir les erreurs.
3. La plupart du temps, le problème vient d'un conflit entre la taille de la mémoire et la configuration dans l'onglet **Flow/Stream** (mais ça, c'est un sujet à part).

## Activation du mode IPS

Pour préparer le mode de prévention, commence par aller dans l'onglet **Alerts** et examine les journaux pendant un certain temps. Selon le contexte, cela peut prendre **un jour à un mois** pour bien comprendre ce qui se passe sur ton ou tes réseaux.

- **Pour les réseaux d'entreprise**, le trafic **sortant** est généralement plus intéressant à analyser que le trafic entrant.
- **Pour les fournisseurs de services**, c'est l'inverse : le trafic **entrant** est celui à surveiller en priorité.

Il est important de noter que le package Suricata de pfSense ajoute automatiquement à une **pass list** (liste d'exclusion) les **adresses du réseau local**, les **adresses des interfaces** et même les **sous-réseaux des tunnels** pour éviter de les bloquer.

Si tu souhaites **bloquer certaines adresses internes**, pense à vérifier cette liste par défaut ou à créer ta propre **pass list**.

Une fois que tu as bien analysé le trafic de ton réseau, y compris le trafic entrant, il est temps d'activer le mode de blocage.

→ **Va dans les paramètres de l'interface et coche l'option "Block Offenders"** pour activer le blocage des menaces.

Alert and Block Settings	
<b>Block Offenders</b>	<input checked="" type="checkbox"/> Checking this option will automatically block hosts that generate a Suricata alert.
<b>IPS Mode</b>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">Legacy Mode</div> <p>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.</p> <p>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. <b>WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet.</b> If problems are experienced with Inline Mode, switch to Legacy Mode instead.</p>
<b>Kill States</b>	<input checked="" type="checkbox"/> Checking this option will kill firewall states for the blocked IP. Default is Checked.
<b>Which IP to Block</b>	<div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">SRC</div> <p>Select which IP extracted from the packet you wish to block. Choosing BOTH is suggested, and it is the default value.</p>
<b>Block On DROP Only</b>	<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.

## Préférences pour le mode IPS

### 1. Choix du mode IPS : "Legacy Mode"

- Je recommande de sélectionner "**Legacy Mode**", car il **copie** les paquets au lieu de les intercepter entre la carte réseau (NIC) et le système d'exploitation.
- C'est plus simple pour commencer, car cela demande **moins de configuration** par rapport au mode "**Inline Mode**".

### 2. Blocage basé sur l'adresse source ("SRC")

- Dans les paramètres "**Which IP to Block**", je préfère bloquer uniquement les **adresses sources ("SRC")**.
- Pour le trafic sortant, l'adresse source sera une **adresse locale**, mais **elle ne sera pas bloquée** car elle est présente dans la **pass list** du réseau domestique.

### 3. Adaptation selon le réseau

- Le choix de bloquer les adresses source ou destination **dépend du type de trafic** sur ton réseau :
  - **Si tu as plus de trafic sortant**, envisage de bloquer les **adresses cibles**.
  - Certains recommandent de bloquer **les adresses source et destination**, mais ce n'est pas toujours adapté à tous les cas d'usage.

## Analyse des menaces

### 1. Redémarrage et observation

- Après avoir **enregistré la configuration**, redémarre le service **Suricata** sur l'interface concernée.
- Attends quelques minutes pour observer l'activité du réseau.

### 2. Surveillance des scans et tentatives d'exploration

- Les **adresses IPv4 publiques** sont bien connues et scannées en permanence.
- Ne sois pas surpris si, **en quelques minutes**, des **crawlers** ou des scripts automatisés commencent à explorer ton adresse IP.
- Même une **nouvelle adresse publique** sera rapidement détectée et scannée.

### 3. Nombre de menaces détectées

- En général, avec **Suricata actif**, on observe entre **50 et 500 adresses IP publiques bloquées par jour**.
  - Sur un **réseau domestique ou de bureau**, tu verras surtout du trafic lié aux mises à jour et aux connexions des appareils.
  - Pour les **grandes entreprises**, le trafic sera **beaucoup plus varié** et nécessitera une analyse plus approfondie (ce qui sera abordé plus tard).
- 

Revision #3

Created 2025-04-01 07:06:36 UTC by GianniO

Updated 2025-04-08 10:03:26 UTC by GianniO