

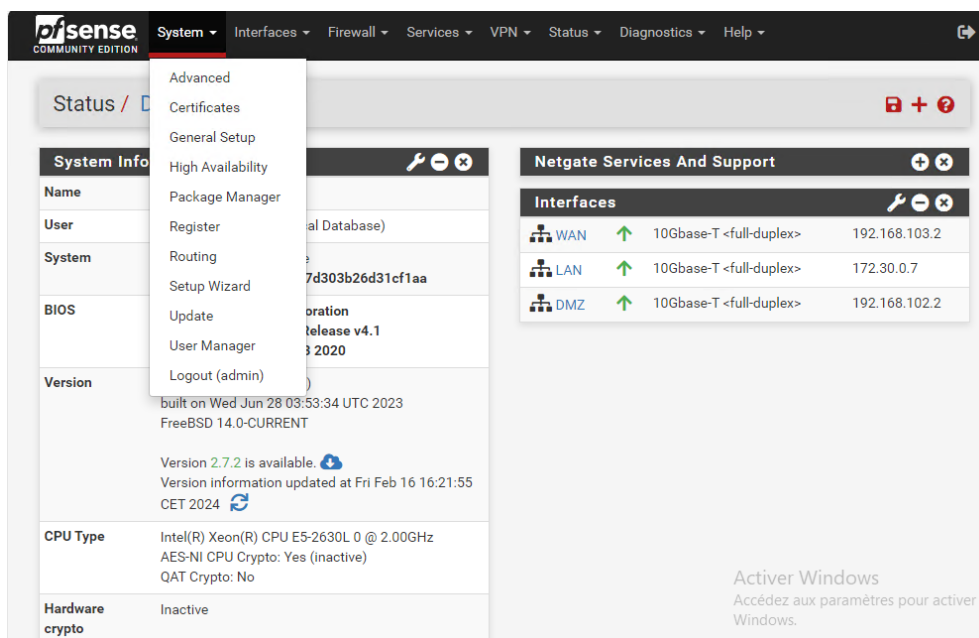
Système de détection d'intrusion (IDS) Snort

Snort est un système de détection d'intrusion (IDS) open source et un système de prévention d'intrusion (IPS), il est largement utilisé pour détecter et prévenir les intrusions réseau en analysant le trafic réseau en temps réel.

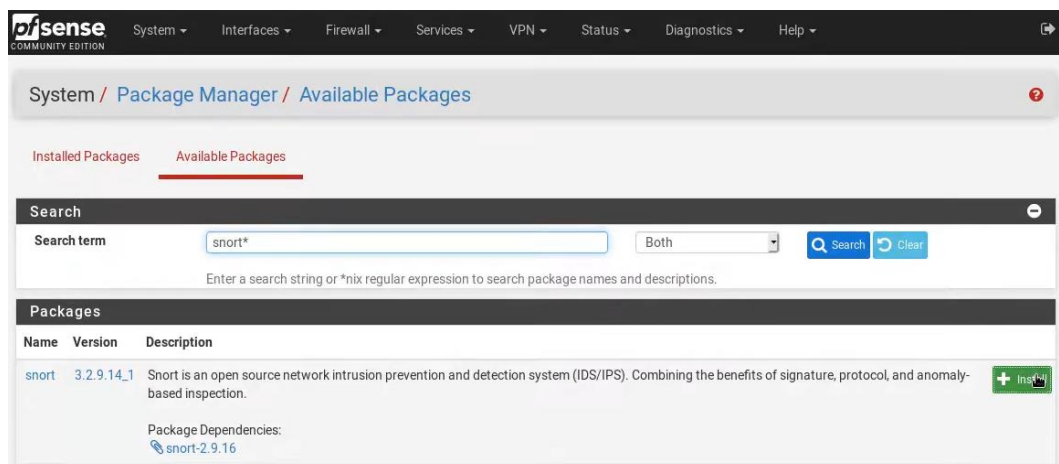
Installation du package Snort :

Snort est un package qui peut être installé sur pfSense pour renforcer les fonctionnalités de détection et de prévention d'intrusion du pare-feu.

Pour installer Snort, nous devons nous connecter à l'interface d'administration de pfSense, puis naviguer vers **System > Package Manager**.

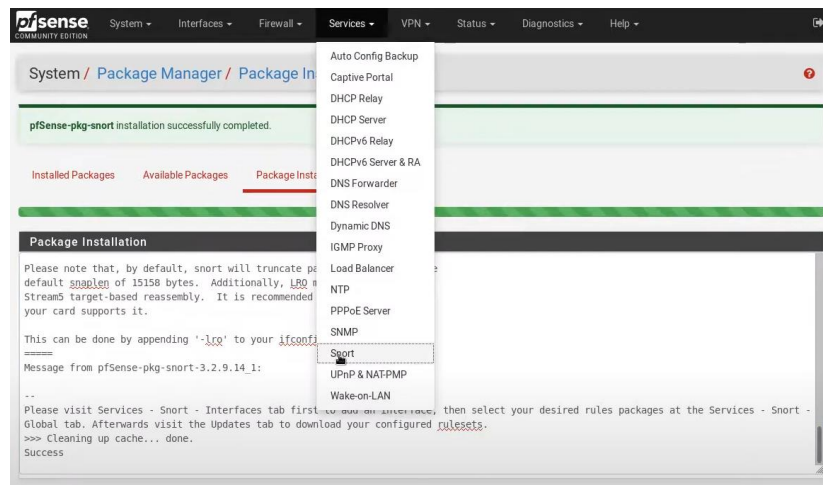


Dans la section "**Available Packages**", nous utilisons la barre de recherche pour localiser le package **Snort**, puis nous procédons à son installation "**Install**".

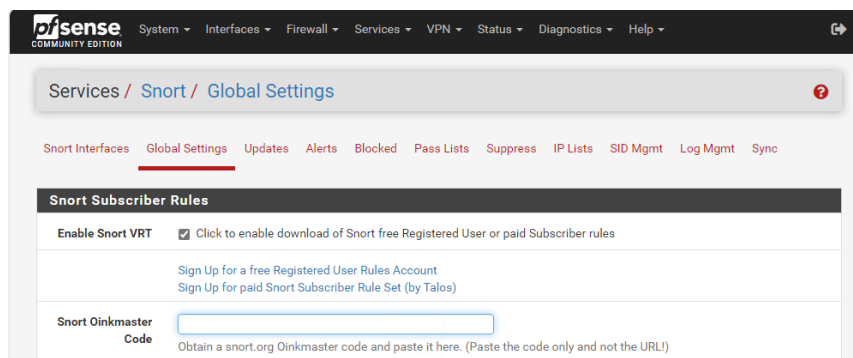


Configuration de Snort :

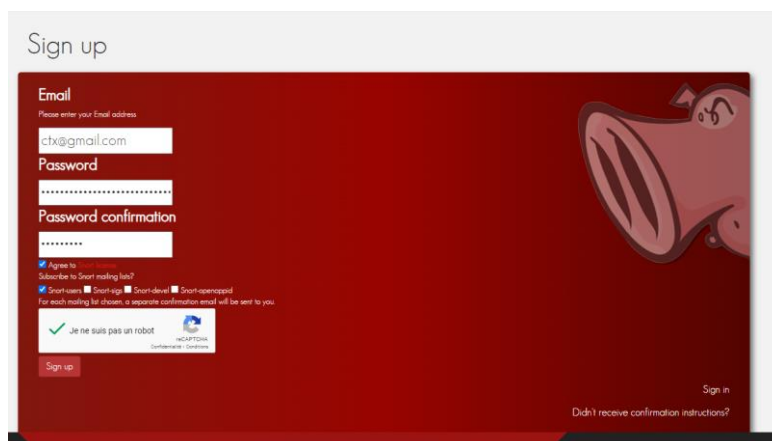
Une fois l'installation du package terminée, nous pouvons configurer Snort. Nous accédons à **Services > Snort** dans l'interface pfSense.



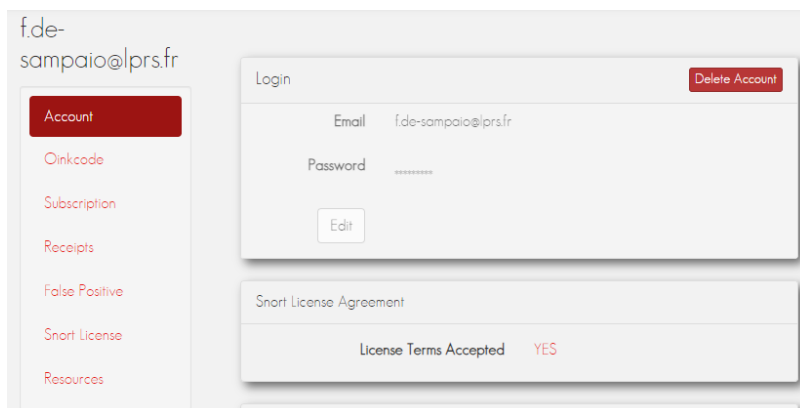
Dans les **"Global Settings"**, le premier élément requis est le **code Oinkmaster de Snort**, nécessaire pour accéder aux dernières détections et aux packages de règles.



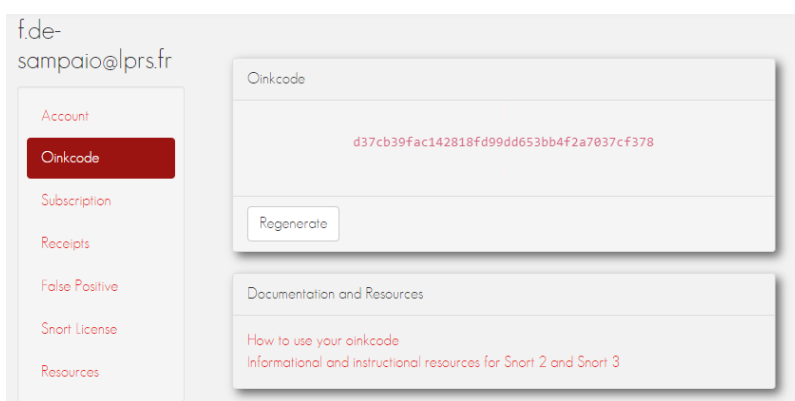
Pour obtenir un code Oinkmaster, nous devons **créer un compte** sur le site officiel de Snort (https://www.snort.org/users/sign_up). Après avoir saisi notre **adresse e-mail** et notre **mot de passe**, accepté les termes de la **licence** Snort et coché la case **Snort-users**, nous validons le compte via l'e-mail de confirmation.



Une fois connectés au compte sur le site de Snort, nous accédons à la section "**Oinkcode**" où le code est généré.



Nous copions ce code et le collons dans l'interface de configuration de pfSense.



Ensuite, nous cocherons "**Enable Snort GPLv2**" pour accepter les termes de la licence GPLv2 associée à Snort.

Snort GPLv2 Community Rules	
Enable Snort GPLv2	<input checked="" type="checkbox"/> Click to enable download of 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. This ruleset is updated daily and is a subset of the subscriber ruleset.	

Nous sélectionnerons l'option "**Enable ET Open**" pour activer un ensemble de règles de Snort contre les menaces de logiciels malveillants. Pour "**Enable ET Pro**", une licence est requise.

Emerging Threats (ET) Rules	
Enable ET Open	<input checked="" type="checkbox"/> Click to enable download of Emerging Threats Open rules
ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.	
Enable ET Pro	<input type="checkbox"/> Click to enable download of Emerging Threats Pro rules
Sign Up for an ETPro Account ETPro for Snort offers daily updates and extensive coverage of current malware threats.	

Pour la configuration des mises à jour des règles, nous définissons l'intervalle de mise à jour **"Update Interval"** sur une base **quotidienne** avec un démarrage à **01:00**, pour que les mises à jour s'effectuent **chaque jour à 1 heure du matin**. Nous cocherons également la case **"Hide Deprecated Rules Categories"** pour masquer les catégories de règles obsolètes dans l'interface graphique et les supprimer de la configuration.

Rules Update Settings	
Update Interval	<div>1 DAY</div> <div>Please select the interval for rule updates. Choosing NEVER disables auto-updates.</div>
Update Start Time	<div>01:00</div> <div>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.</div>
Hide Deprecated Rules Categories	<input checked="" type="checkbox"/> Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.
Disable SSL Peer Verification	<input type="checkbox"/> Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.

Dans les paramètres généraux, nous définirons la durée pendant laquelle les hôtes bloqués seront conservés à **1 heure** avec **"Blocked Hosts Interval"**. Nous activerons **"Keep Snort Settings After Deinstall"** pour conserver les paramètres après la désinstallation. **"Startup/Shutdown Logging"** permet de journaliser le démarrage et l'arrêt de Snort, ce qui est **activé** pour obtenir des logs pertinents.

General Settings	
Remove Blocked Hosts Interval	<div>1 HOUR</div> <div>Please select the amount of time you would like hosts to be blocked. In most cases, one hour is a good choice.</div>
Remove Blocked Hosts After Deinstall	<input type="checkbox"/> Click to clear all blocked hosts added by Snort when removing the package. Default is checked.
Keep Snort Settings After Deinstall	<input checked="" type="checkbox"/> Click to retain Snort settings after package removal.
Startup/Shutdown Logging	<input checked="" type="checkbox"/> Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.

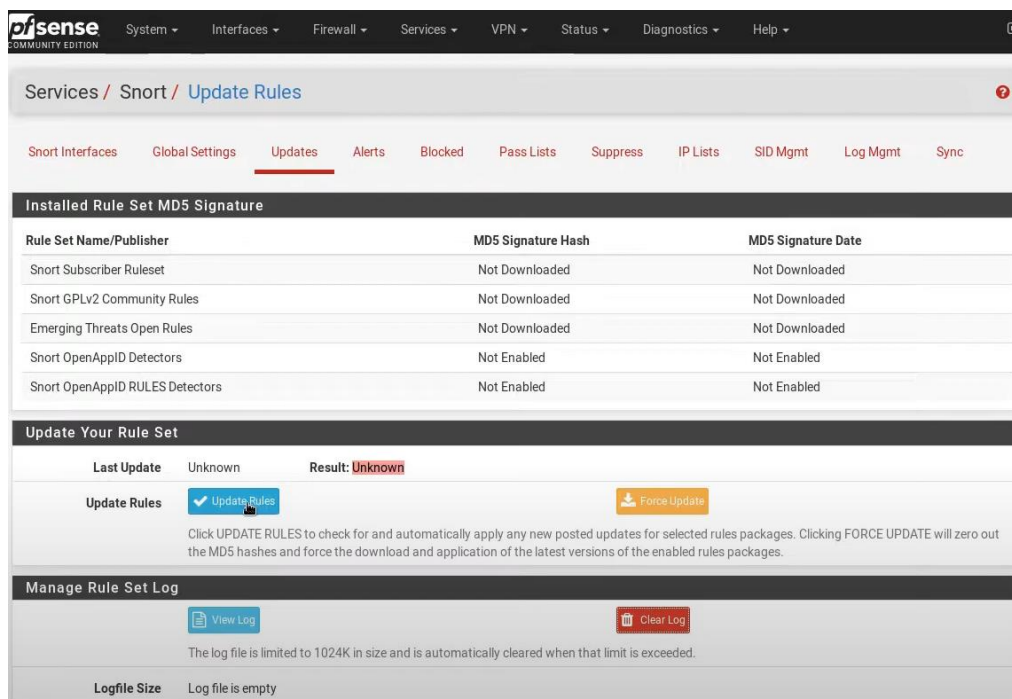
Save

Enfin, nous enregistrons les paramètres en cliquant sur **"Save"**.

Mise à jour des règles Snort :

Pour maintenir la pertinence de la détection d'intrusion, il est crucial de maintenir à jour les règles Snort.

Nous accédons donc à l'onglet "**Updates**" et cliquons sur "**Update Rules**". Un processus de chargement s'engage alors, effectuant la recherche et le téléchargement des mises à jour des règles pour Snort.



Services / Snort / Update Rules

Snort Interfaces Global Settings **Updates** Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	Not Downloaded	Not Downloaded
Snort GPLv2 Community Rules	Not Downloaded	Not Downloaded
Emerging Threats Open Rules	Not Downloaded	Not Downloaded
Snort OpenAppID Detectors	Not Enabled	Not Enabled
Snort OpenAppID RULES Detectors	Not Enabled	Not Enabled

Update Your Rule Set

Last Update: Unknown Result: **Unknown**

Update Rules [Update Rules](#) [Force Update](#)

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

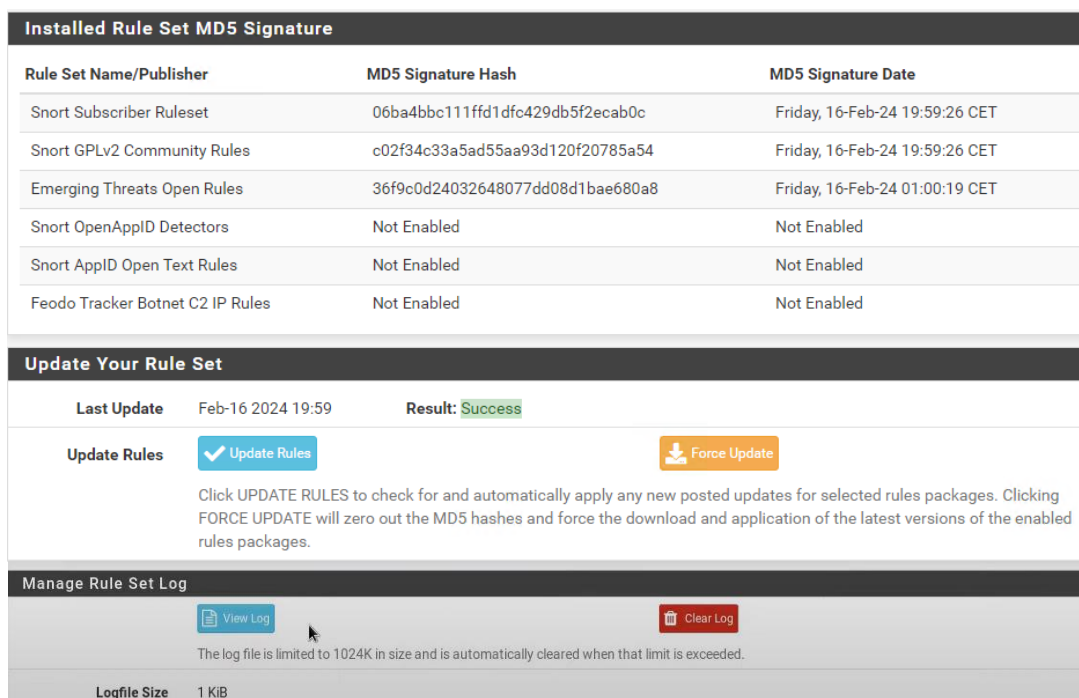
Manage Rule Set Log

[View Log](#) [Clear Log](#)

The log file is limited to 1024K in size and is automatically cleared when that limit is exceeded.

Logfile Size Log file is empty

Après le chargement, nous vérifions la date de la dernière mise à jour "**Last Update**" et le résultat "**Result**" pour confirmer que les règles ont été correctement mises à jour. Nous pouvons également examiner les logs en cliquant sur "**View Logs**" pour visualiser ce qui a été téléchargé.



Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	06ba4bbc111ffd1dfc429db5f2ecab0c	Friday, 16-Feb-24 19:59:26 CET
Snort GPLv2 Community Rules	c02f34c33a5ad55aa93d120f20785a54	Friday, 16-Feb-24 19:59:26 CET
Emerging Threats Open Rules	36f9c0d24032648077dd08d1bae680a8	Friday, 16-Feb-24 01:00:19 CET
Snort OpenAppID Detectors	Not Enabled	Not Enabled
Snort AppID Open Text Rules	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

Update Your Rule Set

Last Update: Feb-16 2024 19:59 Result: **Success**

Update Rules [Update Rules](#) [Force Update](#)

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

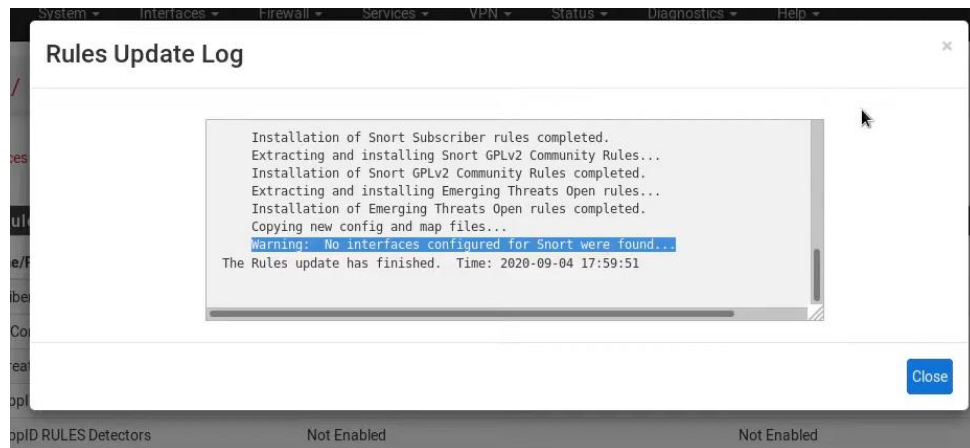
Manage Rule Set Log

[View Log](#) [Clear Log](#)

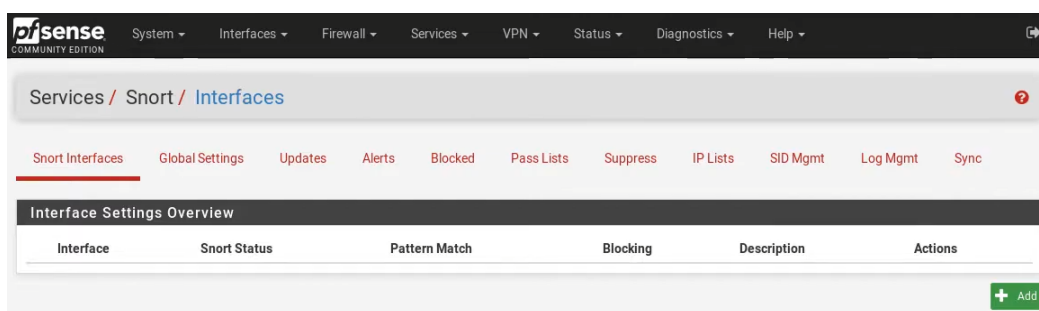
The log file is limited to 1024K in size and is automatically cleared when that limit is exceeded.

Logfile Size 1 KIB

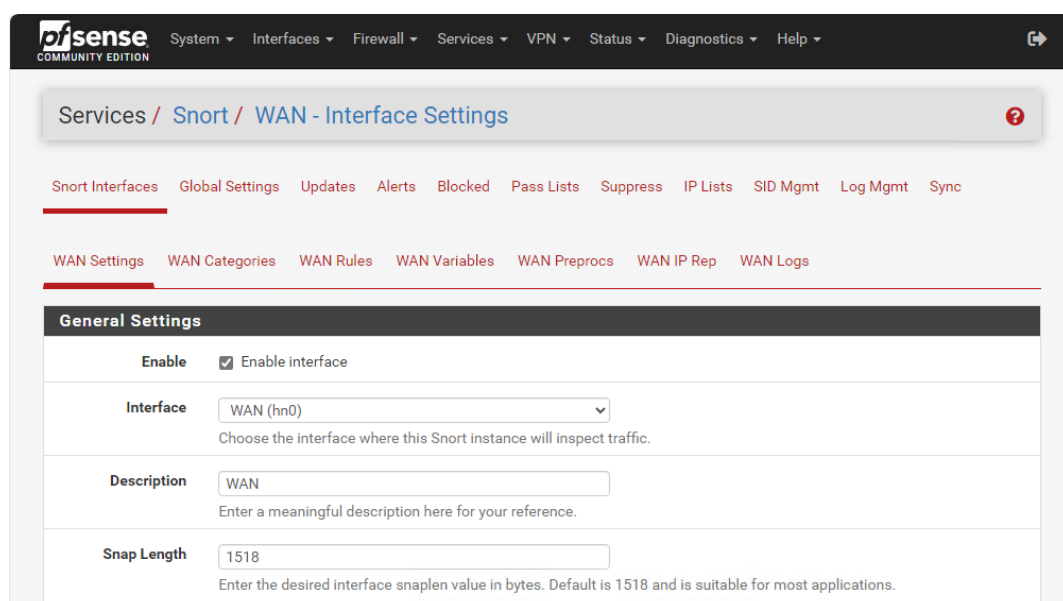
Il est probable que nous recevions un avertissement signalant qu'aucune interface n'a été configurée pour Snort. Nous devons donc configurer une interface pour que Snort puisse fonctionner correctement.



Nous accédons à "**Snort Interfaces**" et ajoutons une nouvelle interface avec "**Add**".



Nous activons d'abord l'interface en cochant "**Enable**", puis sélectionnons notre "**interface**", dans notre cas **WAN (hn0)**, en laissant les autres paramètres par défaut.



Pour les alertes, nous cocherons **"Send Alerts to System Log"** pour recevoir les alertes système, ce qui est essentiel pour l'efficacité de Snort. Nous activons également **"Enable Packet Captures"** pour capturer automatiquement les paquets générant des alertes Snort dans un fichier compatible avec tcpdump, facilitant ainsi l'analyse avec Wireshark.

Alert Settings

Send Alerts to System Log

☒ Snort will send Alerts to the firewall's system log. Default is Not Checked.

System Log Facility

LOG_AUTH

Select system log Facility to use for reporting. Default is LOG_AUTH.

System Log Priority

LOG_ALERT

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

Enable Packet Captures

☒ Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file

Packet Capture File Size



128


Enter a value in megabytes for the packet capture file size limit. Default is 128 megabytes. When the limit is reached, the current packet capture file in directory /var/log/snort/snort_hn037296 is rotated and a new file opened.

Enable Unified2 Logging

☐ Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked.
Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.






Une fois les paramètres configurés, nous enregistrons. Snort est désormais configuré sur notre interface WAN.



 **System** ▾ **Interfaces** ▾ **Firewall** ▾ **Services** ▾ **VPN** ▾ **Status** ▾ **Diagnostics** ▾ **Help** ▾ 

Services / Snort / Interfaces 

Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/> WAN (hn0)	 	AC-BNFA	DISABLED	WAN	  

 Add  Delete

Configuration des catégories sur l'interface WAN :

Nous devons maintenant définir la politique IPS (Intrusion Prevention System) pour notre interface WAN. Dans "**WAN Categories**", nous cocherons "**Use IPS Policy**", puis sélectionnerons "**balanced**" dans la section "**IPS Policy Selection**". Cette stratégie offre un équilibre entre connectivité, sécurité et détection maximale.

- **Connectivity** : Priorise la connectivité, minimisant les interruptions de service au détriment de la sécurité.
- **Balanced** : Équilibre entre la connectivité et la sécurité pour maintenir un niveau acceptable des deux.
- **Security** : Met l'accent sur la sécurité, même au prix de quelques interruptions de service.
- **Max-Detect** : Maximise la détection d'intrusions, même si cela entraîne des interruptions plus fréquentes pour assurer la sécurité maximale.

Snort Subscriber IPS Policy Selection

Use IPS Policy ☒ If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.

Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.

IPS Policy Selection

Balanced

Connectivity

Balanced

Security

Max-Detect

Max-Detect. positives. Balanced is a good starter policy. It is speedy, has ay. It includes all rules in Connectivity. Security is a stringent rules such as a Flash object in an Excel file. Max-Detect is a policy created for testing network traffic through your device. This policy should be used with caution on production systems!

Nous activons toutes les règles de la colonne "**ET Open Rules**" en cliquant sur "**Select All**", puis enregistrons les paramètres.

Select the rulesets (Categories) Snort will load at startup

🟢 - Category is auto-enabled by SID Mgmt conf files
🔴 - Category is auto-disabled by SID Mgmt conf files

Select All Unselect All Save

Enable Ruleset: Snort GPLv2 Community Rules

☒ Snort GPLv2 Community Rules (Talos certified)

Enable	Ruleset: ET Open Rules	Enable	Ruleset: Snort Text Rules	Enable	Ruleset: Snort SO Rules	Snort OPENAPPID rules are not enabled.
<input checked="" type="checkbox"/>	emerging-activex.rules	<input type="checkbox"/>	snort_app-detect.rules	<input type="checkbox"/>	snort_browser-chrome.so.rules	
<input checked="" type="checkbox"/>	emerging-attack_response.rules	<input type="checkbox"/>	snort_blacklist.rules	<input type="checkbox"/>	snort_browser-ie.so.rules	
<input checked="" type="checkbox"/>	emerging-botcc.portgrouped.rules	<input type="checkbox"/>	snort_browser-chrome.rules	<input type="checkbox"/>	snort_browser-other.so.rules	
<input checked="" type="checkbox"/>	emerging-botcc.rules	<input type="checkbox"/>	snort_browser-firefox.rules	<input type="checkbox"/>	snort_browser-webkit.so.rules	
<input checked="" type="checkbox"/>	emerging-chat.rules	<input type="checkbox"/>	snort_browser-ie.rules	<input type="checkbox"/>	snort_exploit-kit.so.rules	
<input checked="" type="checkbox"/>	emerging-ciarmy.rules	<input type="checkbox"/>	snort_browser-other.rules	<input type="checkbox"/>	snort_file-executable.so.rules	
<input checked="" type="checkbox"/>	emerging-compromised.rules	<input type="checkbox"/>	snort_browser-plugins.rules	<input type="checkbox"/>	snort_file-flash.so.rules	
<input checked="" type="checkbox"/>	emerging-current_events.rules	<input type="checkbox"/>	snort_browser-webkit.rules	<input type="checkbox"/>	snort_file-image.so.rules	
<input checked="" type="checkbox"/>	emerging-deleted.rules	<input type="checkbox"/>	snort_content-replace.rules	<input type="checkbox"/>	snort_file-java.so.rules	
<input checked="" type="checkbox"/>	emerging-dns.rules	<input type="checkbox"/>	snort_deleted.rules	<input type="checkbox"/>	snort_file-multimedia.so.rules	
<input checked="" type="checkbox"/>	emerging-dos.rules	<input type="checkbox"/>	snort_exploit-kit.rules	<input type="checkbox"/>	snort_file-office.so.rules	
<input checked="" type="checkbox"/>	emerging-drop.rules	<input type="checkbox"/>	snort_file-executable.rules	<input type="checkbox"/>	snort_file-other.so.rules	
<input checked="" type="checkbox"/>	emerging-dshield.rules	<input type="checkbox"/>	snort_file-flash.rules	<input type="checkbox"/>	snort_file-pdf.so.rules	
<input checked="" type="checkbox"/>	emerging-exploit.rules	<input type="checkbox"/>	snort_file-identify.rules	<input type="checkbox"/>	snort_indicator-shellcode.so.rules	
<input checked="" type="checkbox"/>	emerging-ftp.rules	<input type="checkbox"/>	snort_file-image.rules	<input type="checkbox"/>	snort_malware-cnc.so.rules	

Pour vérifier les règles mises en place, nous accédons à **"WAN Rules"**. Nous pouvons choisir de filtrer les règles par catégories si nécessaire.

The screenshot shows the pfSense Community Edition interface. The breadcrumb trail is: Services / Snort / Interface Settings / WAN - Rules. The main navigation bar includes: Snort Interfaces, Global Settings, Updates, Alerts, Blocked, Pass Lists, Suppress, IP Lists, SID Mgmt, Log Mgmt, and Sync. The sub-navigation bar includes: WAN Settings, WAN Categories, WAN Rules (selected), WAN Variables, WAN Preprocs, WAN IP Rep, and WAN Logs.

Available Rule Categories

Category Selection:
 Select the rule category to view and manage.

Rule Signature ID (SID) Enable/Disable Overrides

SID Actions:
 When finished, click APPLY to save and send any SID enable/disable changes made on this tab to Snort.
 Note: You should not disable flowbit rules! Add Suppress List entries for them instead by clicking here.

Rules View Filter +

Selected Category's Rules

Legend:
✔ Default Enabled ✔ Enabled by user ✔ Auto-enabled by SID Mgmt ⚠ Action/content modified by SID Mgmt ⚠ Rule action is alert
✘ Default Disabled ✘ Disabled by user ✘ Auto-disabled by SID Mgmt

State	Action	GID	SID	Proto	Source	SPort	Destination	DPort	Message
✔	⚠	1	2420	tcp	\$HOME_NET	any	\$EXTERNAL_NET	\$HTTP_PORTS	FILE-IDENTIFY

Pour consulter les logs, nous nous rendons dans **"WAN Logs"** et sélectionnons le fichier de logs à visualiser, généralement **"alert"**. Si aucun événement n'apparaît, c'est normal car Snort doit être démarré.

The screenshot shows the pfSense Community Edition interface. The breadcrumb trail is: Services / Snort / Interface Logs / WAN. The main navigation bar is the same as the previous screenshot. The sub-navigation bar includes: WAN Settings, WAN Categories, WAN Rules, WAN Variables, WAN Preprocs, WAN IP Rep, and WAN Logs (selected).

Log File Selection

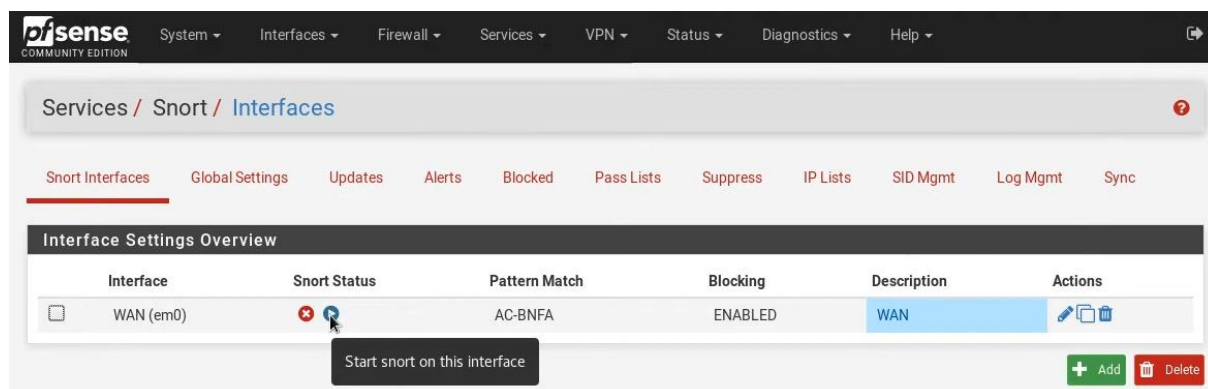
Log File to View:
 Choose which log you want to view..

Log file contents: Log file does not exist or that logging feature is not enabled.
 Log File Path

Log Contents

Activation de Snort sur l'interface WAN :

Pour démarrer Snort sur l'interface WAN, nous retournons à "**Snort Interfaces**" et **activons** Snort pour cette interface.

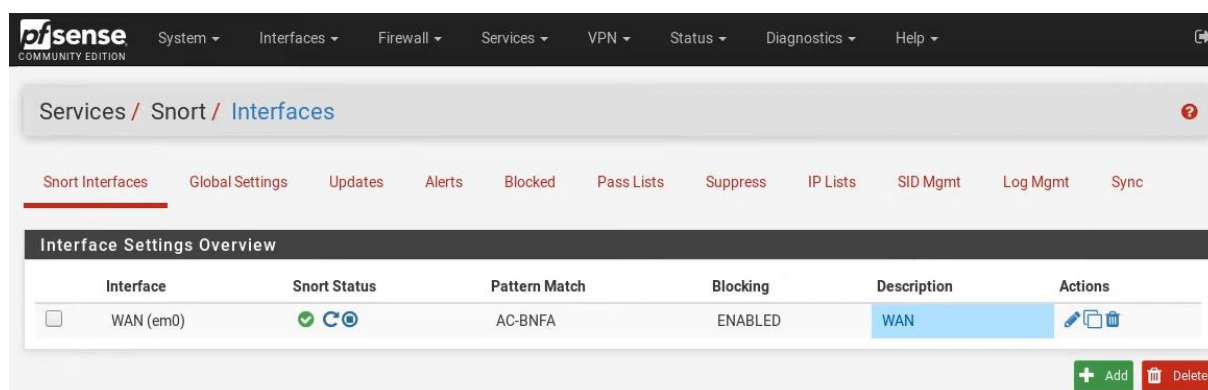


The screenshot shows the Pfsense web interface. The top navigation bar includes 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', 'Diagnostics', and 'Help'. The breadcrumb trail is 'Services / Snort / Interfaces'. Below this, there are tabs for 'Snort Interfaces', 'Global Settings', 'Updates', 'Alerts', 'Blocked', 'Pass Lists', 'Suppress', 'IP Lists', 'SID Mgmt', 'Log Mgmt', and 'Sync'. The 'Snort Interfaces' tab is active. The main section is titled 'Interface Settings Overview' and contains a table with the following data:

Interface	Snort Status	Pattern Match	Blocking	Description	Actions
WAN (em0)	OFF	AC-BNFA	ENABLED	WAN	[Edit] [Copy] [Delete]

A tooltip 'Start snort on this interface' is displayed over the 'OFF' status icon. At the bottom right, there are '+ Add' and 'Delete' buttons.

Snort est désormais activé et opérationnel sur l'interface WAN, prêt à détecter et à prévenir les intrusions conformément à notre configuration.



The screenshot shows the Pfsense web interface after activation. The 'Snort Status' for the 'WAN (em0)' interface is now 'ON', indicated by a green checkmark and a blue circular icon. The rest of the interface remains the same as in the previous screenshot.