



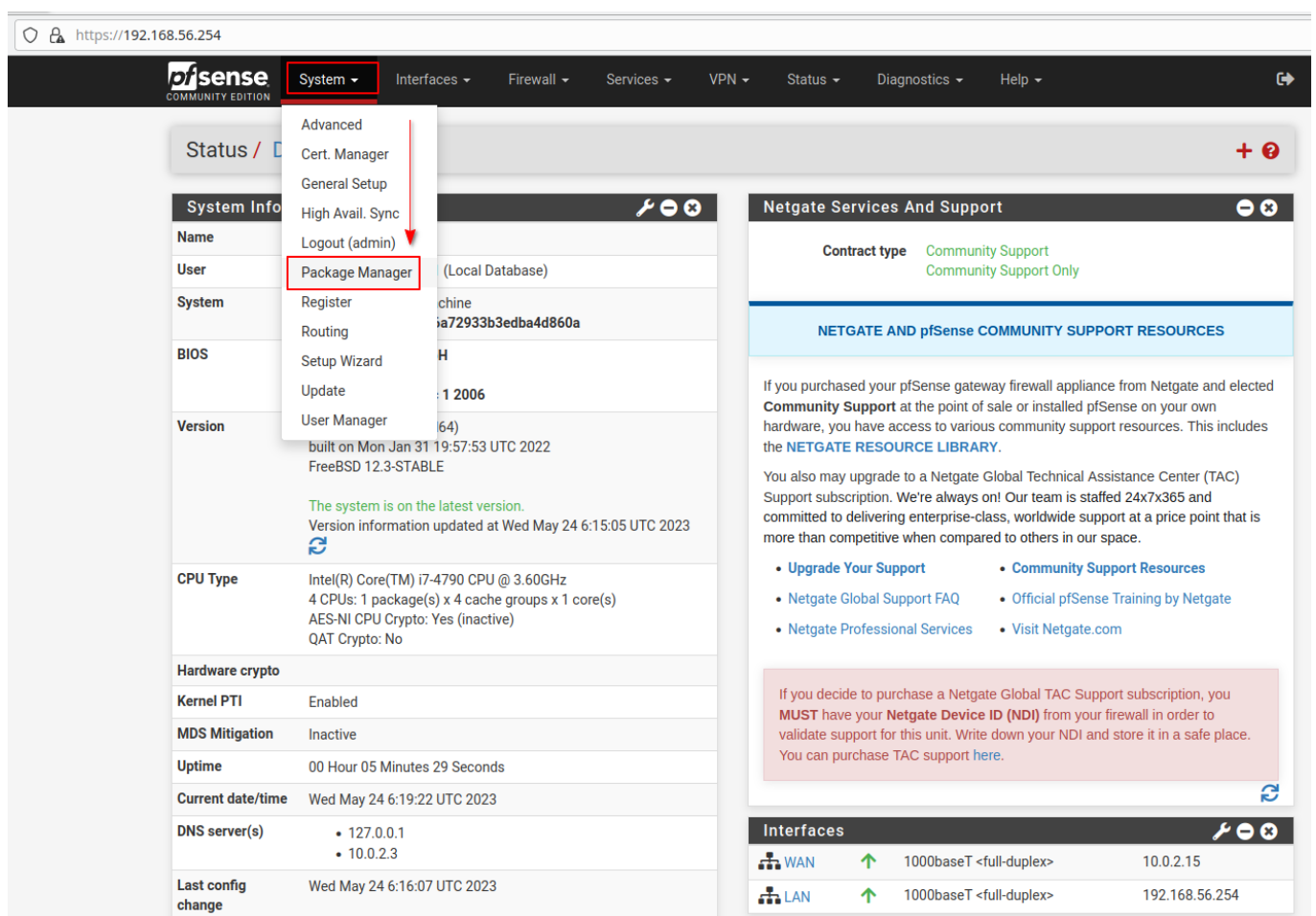
Document d'exploitation

# Installation de Snort

Snort n'étant pas installé par défaut par pfsense, pour pouvoir l'utiliser il est nécessaire de passer par la case installation.

Rien de compliqué cependant, c'est un paquet à installer.

Pour aller installer un paquet, il faut naviguer sur la page "packet manager"



The screenshot shows the pfSense web interface at the URL <https://192.168.56.254>. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The 'System' menu is open, showing options: Advanced, Cert. Manager, General Setup, High Avail. Sync, Logout (admin), Package Manager (highlighted with a red box and a red arrow), Register, Routing, Setup Wizard, Update, and User Manager. The main content area is divided into two panels. The left panel, titled 'System Info', displays system details such as Name, User, System, BIOS, Version, CPU Type, Hardware crypto, Kernel PTI, MDS Mitigation, Uptime, Current date/time, DNS server(s), and Last config change. The right panel, titled 'Netgate Services And Support', shows the contract type as 'Community Support' and provides links to various support resources. Below this, there is a section for 'Interfaces' showing WAN and LAN configurations.

System Info	Value
Name	
User	
System	
BIOS	
Version	built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE
CPU Type	Intel(R) Core(TM) i7-4790 CPU @ 3.60GHz 4 CPUs: 1 package(s) x 4 cache groups x 1 core(s) AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	00 Hour 05 Minutes 29 Seconds
Current date/time	Wed May 24 6:19:22 UTC 2023
DNS server(s)	• 127.0.0.1 • 10.0.2.3
Last config change	Wed May 24 6:16:07 UTC 2023

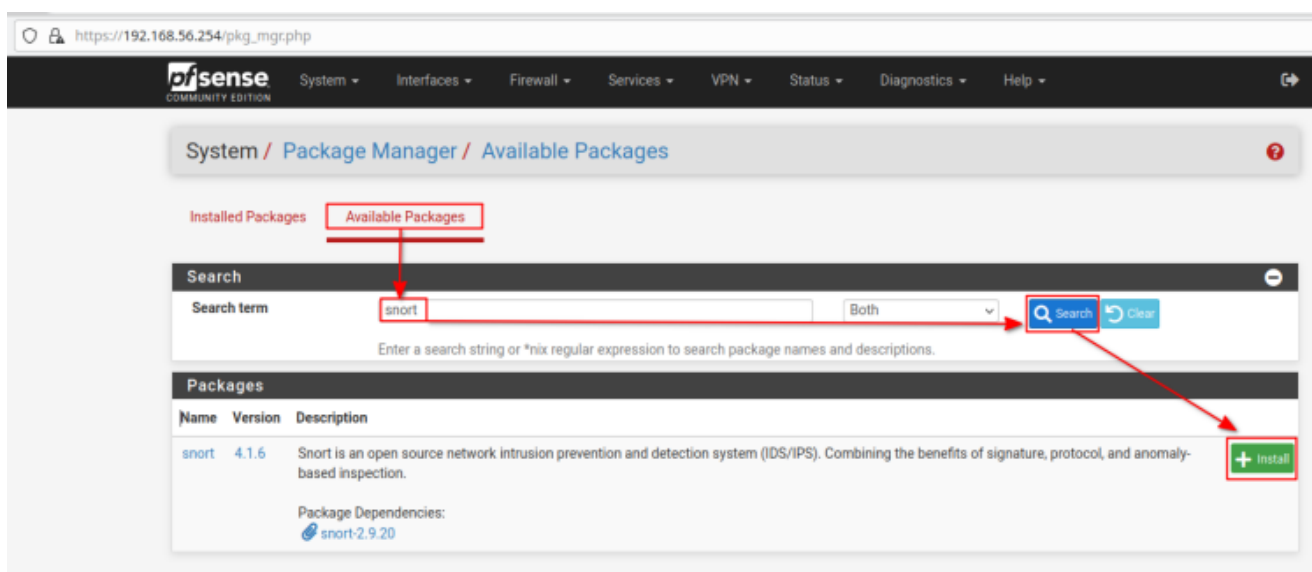
Interfaces	Speed	MAC
WAN	1000baseT <full-duplex>	10.0.2.15
LAN	1000baseT <full-duplex>	192.168.56.254

Sur la page Packet Manager, il y a deux onglets :

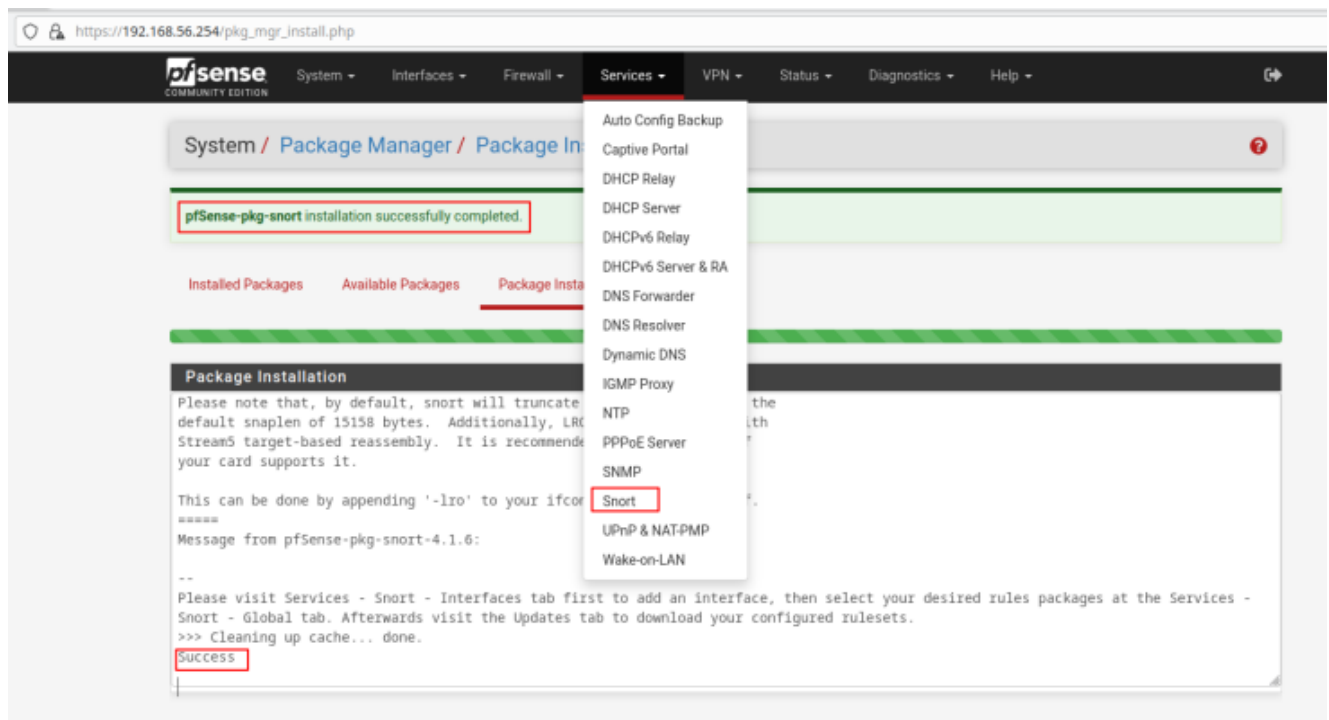
- Installed Packages
- Available Packages

On va donc sélectionner l'onglet "Available Package" et taper snort en barre de recherche.

Une fois le paquet trouvé, il ne reste plus qu'à cliquer sur le bouton d'installation.



Une fois l'installation terminée, une entrée snort est maintenant disponible depuis le menu service.



On selectionne les liste de règles que l'on veut utiliser, ici, je selectionne deux listes communautaires.

https://192.168.56.254/snort/snort\_interfaces\_global.php

**Pfsense**  
COMMUNITY EDITION

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

Services / **Snort** / Global Settings

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

**Snort Subscriber Rules**

Enable Snort VRT ☐ Click to enable download of Snort free Registered User or paid Subscriber rules

[Sign Up for a free Registered User Rules Account](#)  
[Sign Up for paid Snort Subscriber Rule Set \(by Talos\)](#)

**Snort GPLv2 Community Rules**

Enable Snort GPLv2 ☒ 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.

**Emerging Threats (ET) Rules**

Enable ET Open ☐ Click to enable download of Emerging Threats Open rules

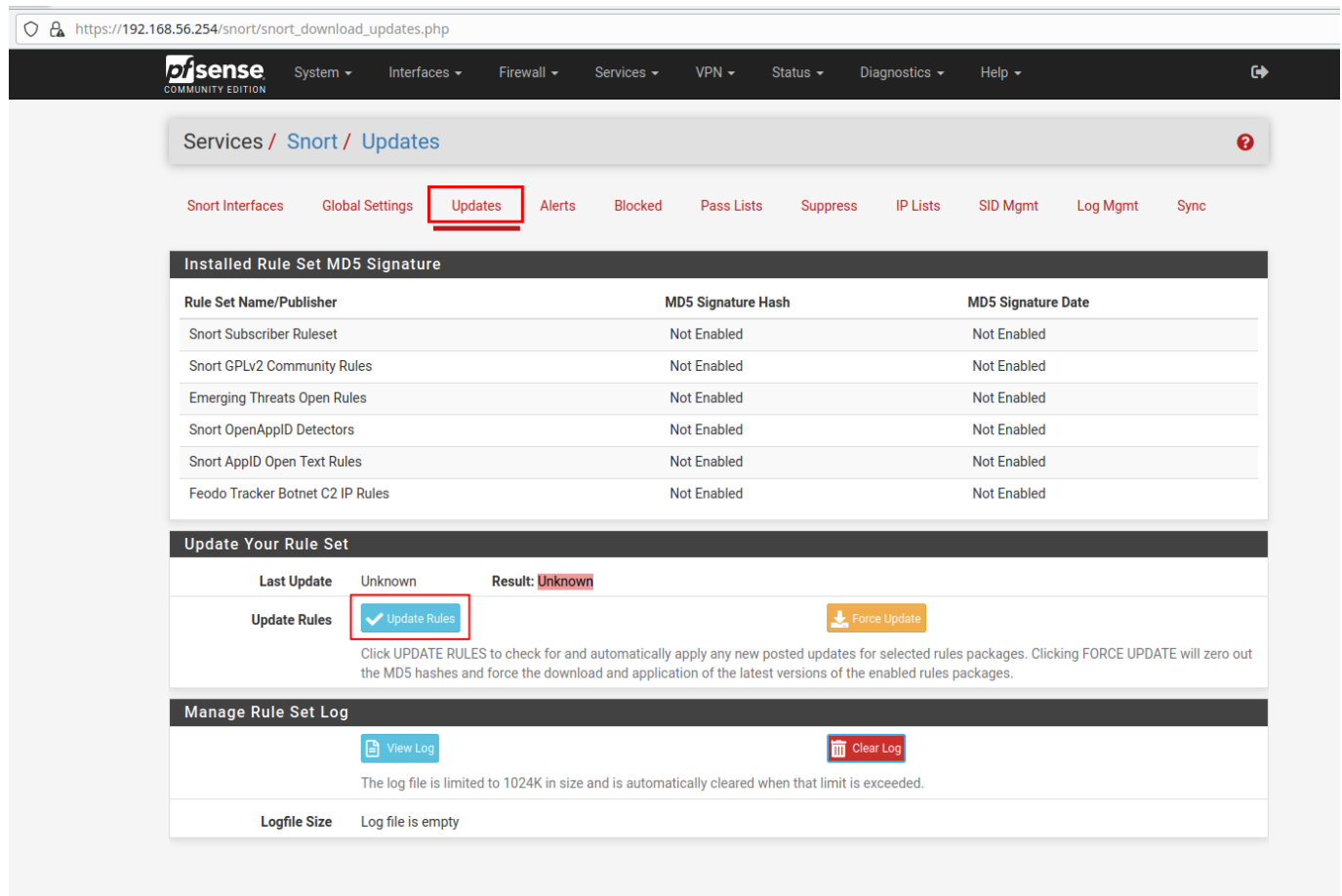
ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.

Enable ET Pro ☐ 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.

**La validation se trouve en bas de la page**

On peut maintenant passer sur l'onglet update et lancer le téléchargement des listes



The screenshot shows the pfSense web interface at the URL `https://192.168.56.254/snort/snort_download_updates.php`. The breadcrumb trail is `Services / Snort / Updates`. The `Updates` tab is highlighted in the top navigation bar. Below the navigation bar, there is a table titled `Installed Rule Set MD5 Signature` with columns `Rule Set Name/Publisher`, `MD5 Signature Hash`, and `MD5 Signature Date`. The table lists several rule sets, all with `Not Enabled` status. Below this table is the `Update Your Rule Set` section, which shows `Last Update` as `Unknown` and `Result` as `Unknown`. The `Update Rules` button is highlighted with a red box. Below it, there is a `Force Update` button. A note explains that clicking `UPDATE RULES` will check for and apply new updates, while `FORCE UPDATE` will zero out MD5 hashes and force the download of the latest versions. At the bottom, there is a `Manage Rule Set Log` section with `View Log` and `Clear Log` buttons. A note states that the log file is limited to 1024K in size and is automatically cleared when that limit is exceeded. The `Logfile Size` is shown as `Log file is empty`.

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	Not Enabled	Not Enabled
Snort GPLv2 Community Rules	Not Enabled	Not Enabled
Emerging Threats Open Rules	Not Enabled	Not Enabled
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: 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.

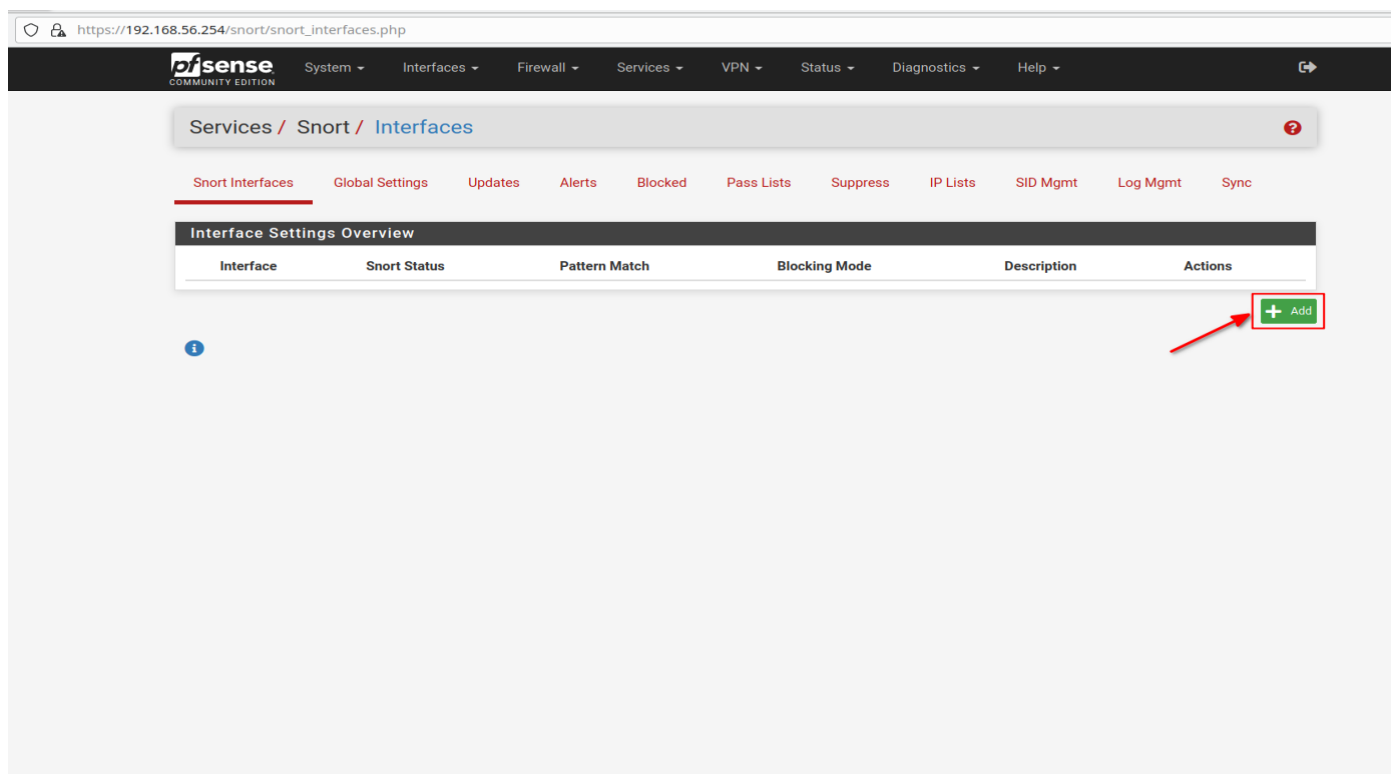
**Manage Rule Set Log**

[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

Une fois que la mise à jour est terminée, on peut activer l'interface que snort va écouter



The screenshot shows the pfSense web interface at the URL `https://192.168.56.254/snort/snort_interfaces.php`. The breadcrumb trail is `Services / Snort / Interfaces`. The `Interfaces` tab is highlighted in the top navigation bar. Below the navigation bar, there is a table titled `Interface Settings Overview` with columns `Interface`, `Snort Status`, `Pattern Match`, `Blocking Mode`, `Description`, and `Actions`. The table is currently empty. A red arrow points to the `+ Add` button in the `Actions` column.

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
-----------	--------------	---------------	---------------	-------------	---------

[+ Add](#)

https://192.168.56.254/snort/snort\_interfaces\_edit.php?id=0

**sense** COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Services / Snort / WAN - Interface Settings

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

WAN Settings

**General Settings**

Enable ☒ Enable interface

Interface  Choose the interface where this Snort instance will inspect traffic.

Description  Enter a meaningful description here for your reference.

Snap Length  Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

**Alert Settings**

Send Alerts to System Log ☐ Snort will send Alerts to the firewall's system log. Default is Not Checked.

Enable Packet Captures ☐ Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file

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.

**Block Settings**

Block Offenders ☐ Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.

**Il reste à valider en bas de la page**

Une fois validé, on peut passer à l'onglet "categories" pour activer les règles

https://192.168.56.254/snort/snort\_rulesets.php?id=0

**sense** COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Services / Snort / Interface Settings / LAN - Categories

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

LAN Settings LAN Categories LAN Rules LAN Variables LAN Preprocs LAN IP Rep LAN Logs

**Automatic Flowbit Resolution**

Resolve Flowbits ☒ If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked. Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.

**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)

Pour activer/désactiver les règles individuellement, on doit passer sur l'onglet "Rules" et sélectionner une des liste que l'on a activé.

https://192.168.56.254/snort/snort\_rules.php?id=0

**pfsense** COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Services / Snort / Interface Settings / LAN - Rules

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

LAN Settings LAN Categories LAN Rules LAN Variables LAN Preprocs LAN IP Rep LAN Logs

**Available Rule Categories**

Category Selection: Auto-Flowbit Rules

Rule Signature ID (SID) custom.rules decoder.rules GPLv2\_community.rules preprocessor.rules User Forced Disabled Rules User Forced Enabled Rules User Forced ALERT Action Rules

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
-------	--------	-----	-----	-------	--------	-------	-------------	-------	---------

Il reste à activer ce que l'on souhaite

https://192.168.56.254/snort/snort\_rules.php

**pfsense** COMMUNITY EDITION System Interfaces Firewall Services VPN Status Diagnostics Help

Services / Snort / Interface Settings / LAN - Rules

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

LAN Settings LAN Categories LAN Rules LAN Variables LAN Preprocs LAN IP Rep LAN Logs

**Available Rule Categories**

Category Selection: GPLv2\_community.rules

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.

**Rules View Filter**

**Selected Category's Rules**

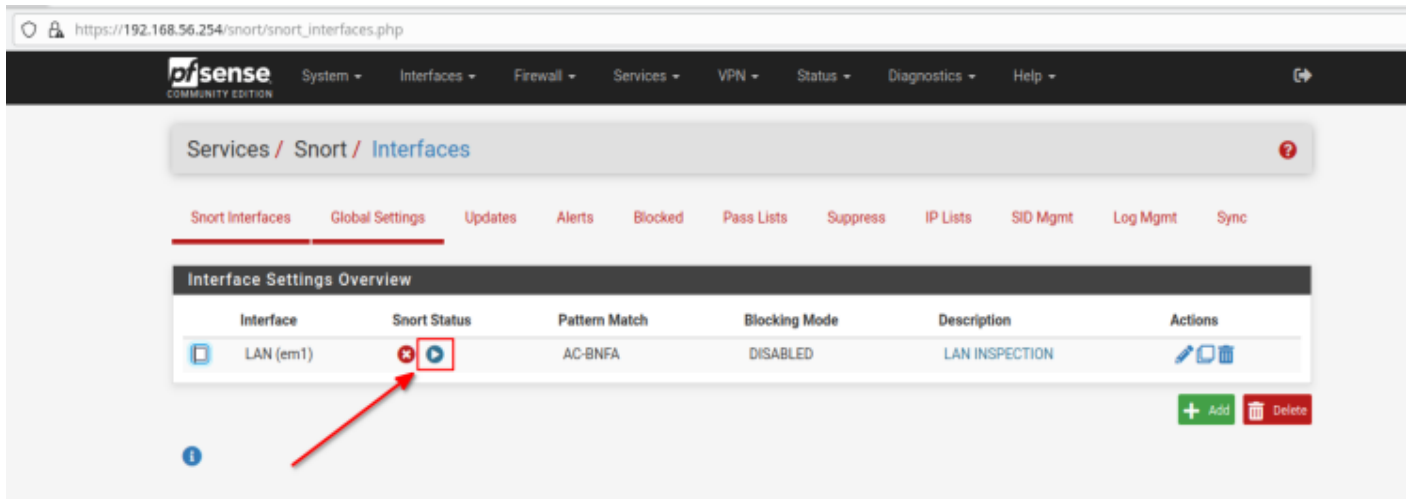
Legend: Default Enabled Enabled by user Auto-enabled by SID Mgmt Action/content modified by SID Mgmt Rule action is alert Default Disabled Disabled by user Auto-disabled by SID Mgmt

State	Action	GID	SID	Proto	Source	SPort	Destination	DPort	Message
		1	105	tcp	\$HOME_NET	2589	\$EXTERNAL_NET	any	MALWARE-BACKDOOR - Dagger_1.4.0
		1	108	tcp	\$EXTERNAL_NET	any	\$HOME_NET	7597	MALWARE-BACKDOOR QAZ Worm Client Login access
		1	110	tcp	\$EXTERNAL_NET	any	\$HOME_NET	12345:12346	MALWARE-BACKDOOR netbus getinfo
		1	115	tcp	\$HOME_NET	20034	\$EXTERNAL_NET	any	MALWARE-BACKDOOR NetBus Pro 2.0 connection established
		1	117	tcp	\$HOME_NET	any	\$EXTERNAL_NET	any	MALWARE-BACKDOOR Infector.1.x



On valide et on applique et on peut vérifier les détection dans "Alerts" en mode "découverte" ou dans "Alert et Blocked" lorsque l'on passe en production.

Pour passer en production : on lance le service sur l'interface



Pour tester si le bon fonctionnement de Snort, nous pouvons lancer un scan nmap depuis une machine du réseau LAN