

MISE EN PLACE ET CONFIGURATION DE SNORT SOUS PFSENSE



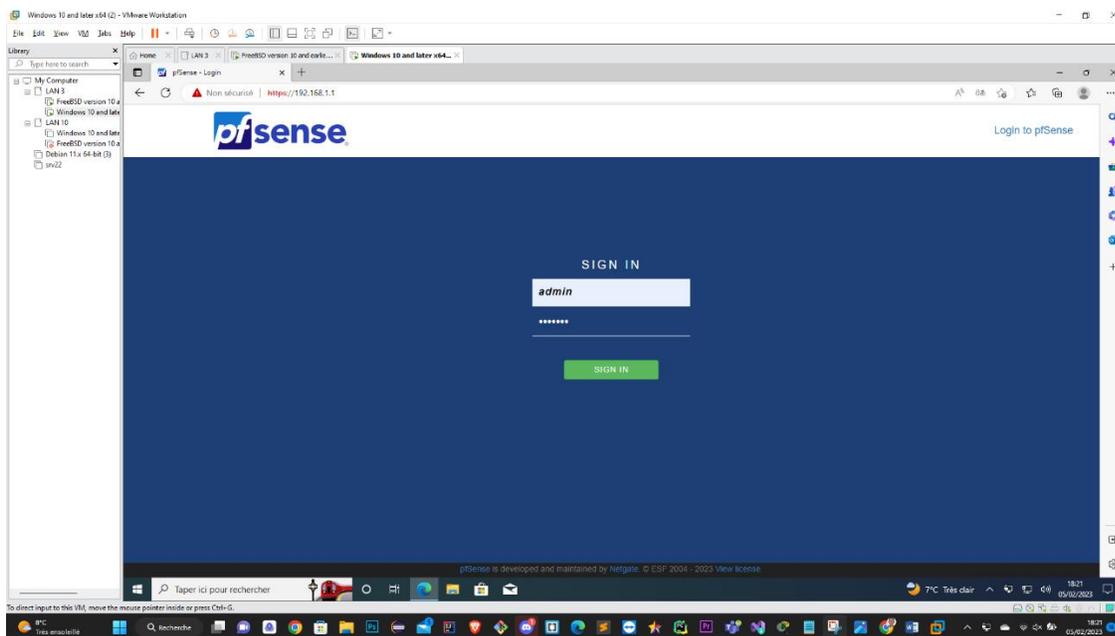
- 1. INTRODUCTUON***
- 2. INSTALLER, CONFIGURER SNORT ET CREER SON USER SNORT***
- 3. TEST D'INTRUSION***

1. INTRODUCTION

Snort est le premier système de prévention des intrusions (IPS) Open Source au monde. Snort IPS utilise une série de règles qui aident à définir l'activité réseau malveillante et utilisent ces règles pour trouver les paquets qui correspondent à celles-ci et génère des alertes pour les utilisateurs.

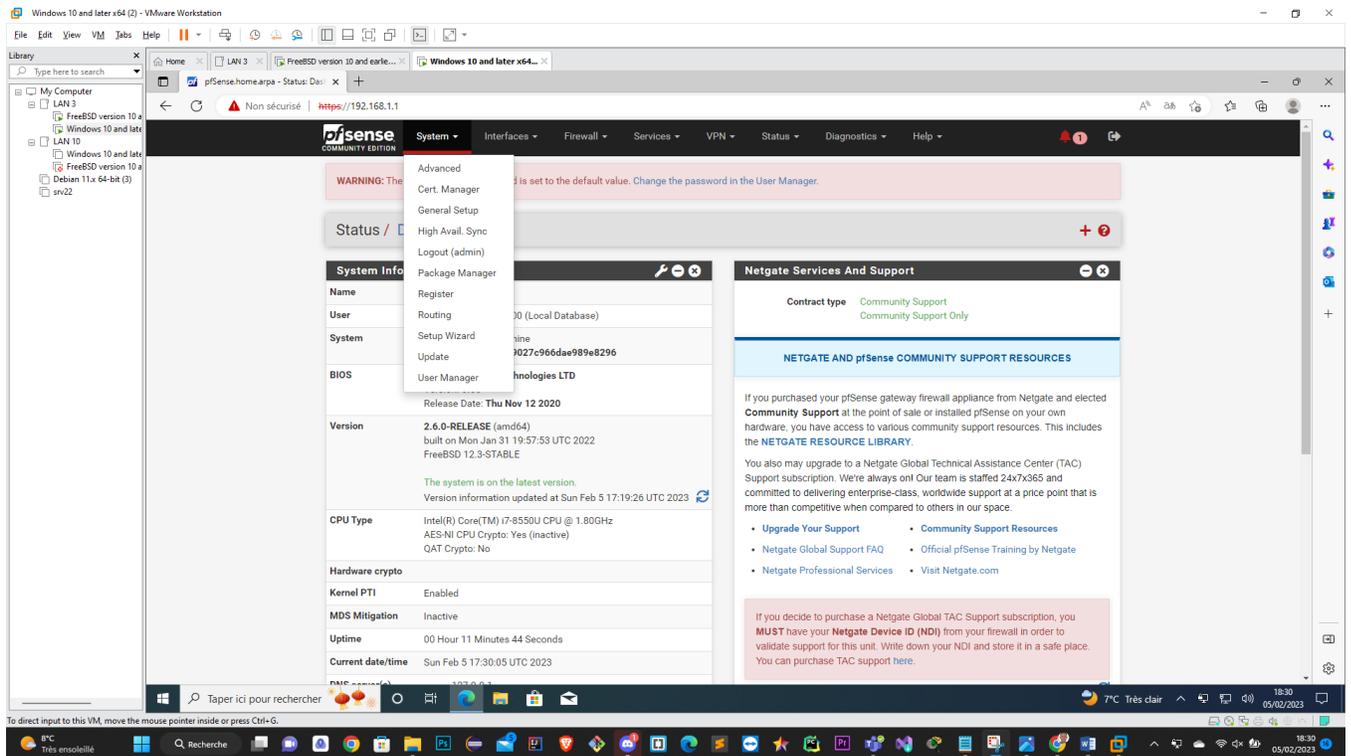
Snort peut également être déployé en ligne pour arrêter ces paquets. Snort a trois utilisations principales: **En tant que renifleur de paquets comme tcpdump, en tant qu'enregistreur de paquets - ce qui est utile pour le débogage du trafic réseau, ou il peut être Utilisé comme un système complet de prévention des intrusions sur le réseau.** Snort peut être téléchargé et configuré pour le personnel et l'utilisation professionnelle.

2. INSTALLER ET CONFIGURER SNORT

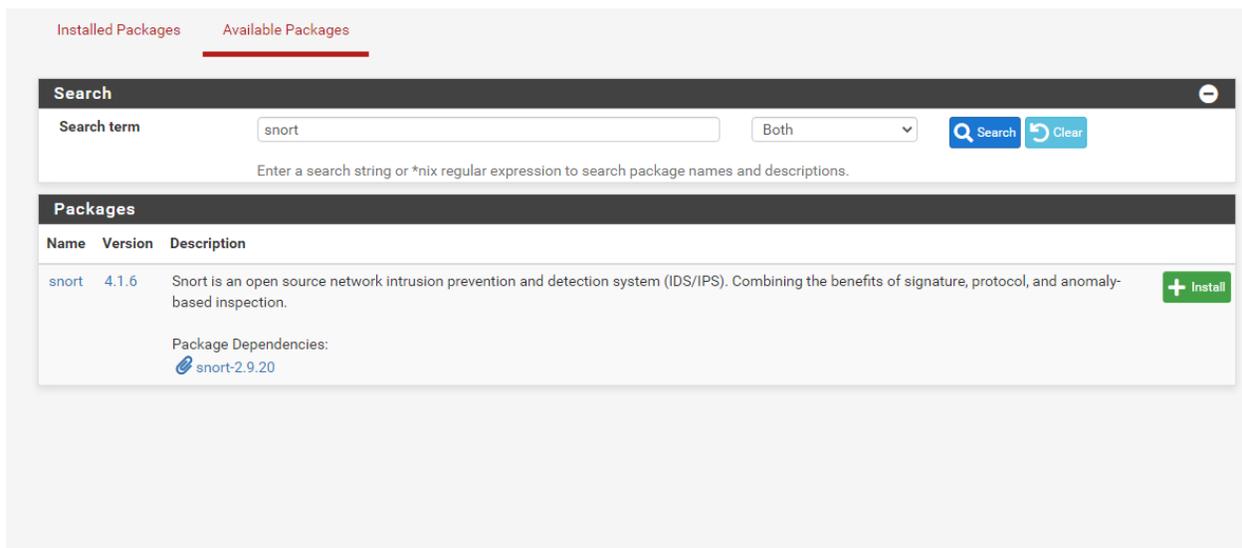


Par défaut le paquet SNORT n'est installé sur PFSense il faut donc le télécharger puis l'installer.

Une fois dans PFSense on va dans le système ensuite Package manager pour voir les paquets installés et les paquets disponible.



SNORT se trouvera donc dans les paquets disponibles, on ira donc le chercher pour l'installer





pfSense-pkg-snort installation successfully completed.

Installed Packages

Available Packages

Package Installer

Package Installation

Please note that, by default, snort will truncate packets larger than the default snaplen of 15158 bytes. Additionally, LRO may cause issues with Stream5 target-based reassembly. It is recommended to disable LRO, if your card supports it.

This can be done by appending '-lro' to your ifconfig_line in rc.conf.

Message from pfSense-pkg-snort-4.1.6:

--

Please visit Services - Snort - Interfaces tab first to add an interface, then select your desired rules packages at the Services - Snort - Global tab. Afterwards visit the Updates tab to download your configured rulesets.

>>> Cleaning up cache... done.

Success

Installed Packages

Available Packages

Installed Packages

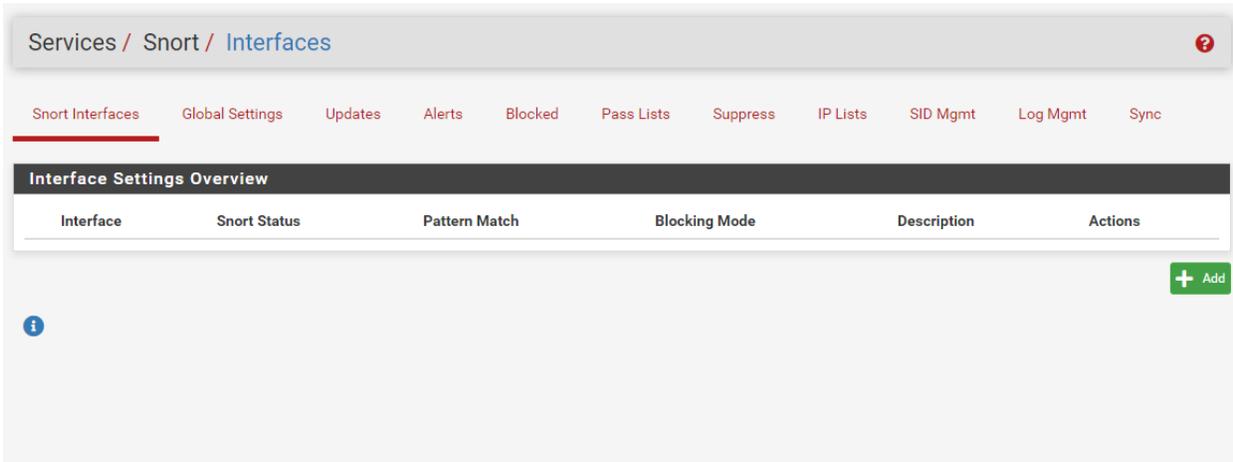
Name	Category	Version	Description	Actions
✓ snort	security	4.1.6	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection. Package Dependencies: snort-2.9.20	

= Update ✓ = Current
 = Remove = Information = Reinstall

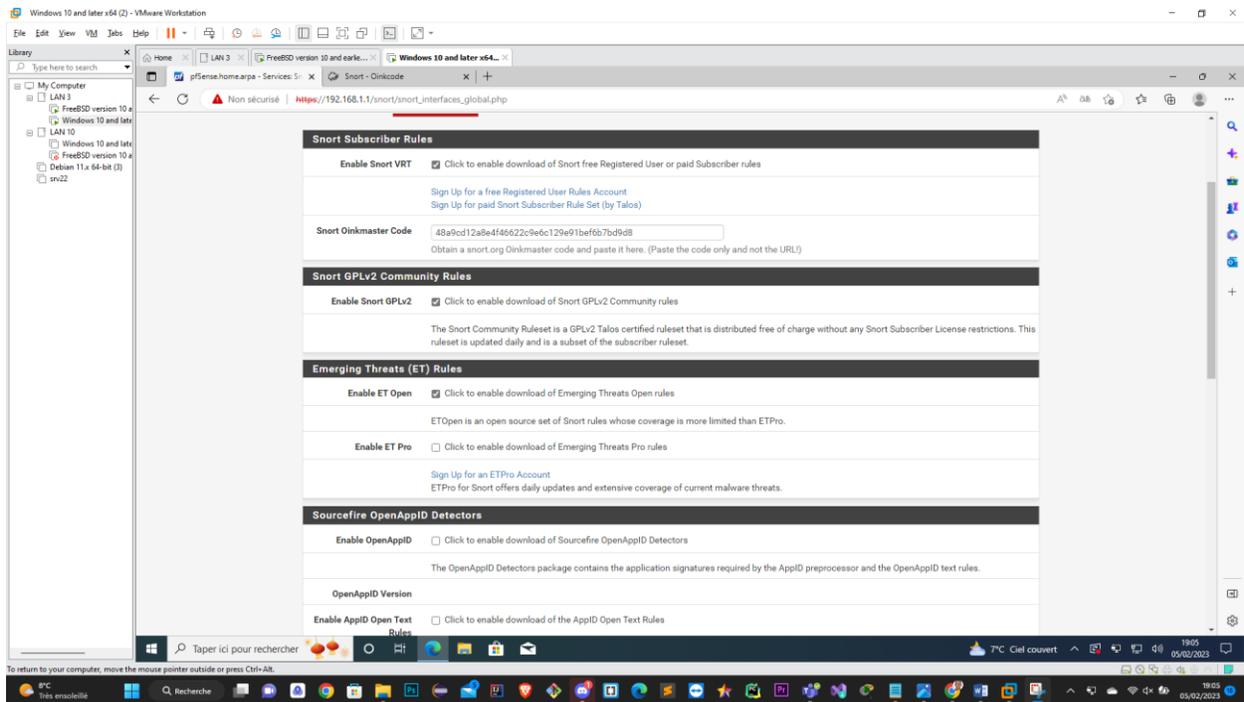
Newer version available

Package is configured but not (fully) installed or deprecated

Après l'installation du paquet Snort nous procéderons à l'ajout de service Snort, donc nous irons à l'onglet service puis sectionner Snort.



Et accéder au Global Setting, la première étape est donc d'activer le téléchargement de règles gratuites, en cochant la première case (Enable Snort VRT), on nous demandera **L'Oinkmaster Code** qui est une clé qu'on devra aller chercher sur Snort.org Et ensuite nous pouvons cocher les cases Enable Snort GPLv2 pour les règles communautaires et Enable ET Open.



Sign up

Email

Please enter your Email address

Password

Password confirmation

Agree to [Snort license](#)

Subscribe to Snort mailing lists?

Snort-users Snort-sigs Snort-devel Snort-openappid

You will receive an email confirmation that will require your action if you select any of these boxes

Je ne suis pas un robot



reCAPTCHA

Confidentialité - Conditions

Sign up

[Sign in](#)

[Didn't receive confirmation instructions?](#)

Snort.org

Après création et confirmation de mon compte Snort j'ai pu avoir la clé Oinkmaster code

honoremm5@gmail.com

Account

Oinkcode

Subscription

Receipts

False Positive

Snort License

Resources

Oinkcode

48a9cd12a8e4f46622c9e6c129e91bef6b7bd9d8

Regenerate

Documentation and Resources

[How to use your oinkcode](#)

Informational and instructional resources for Snort 2 and Snort 3

Dans la zone Rules Update Settings on effectue les config ci-dessous :

Update Interval: 1 Day

Update Start Time: 00 :00

On coche Keep Snort Settings After Deinstall et Startup/Shutdown Logging, pour que quand on désinstallera Snort on garde les paramètres de configuration et avoir les log

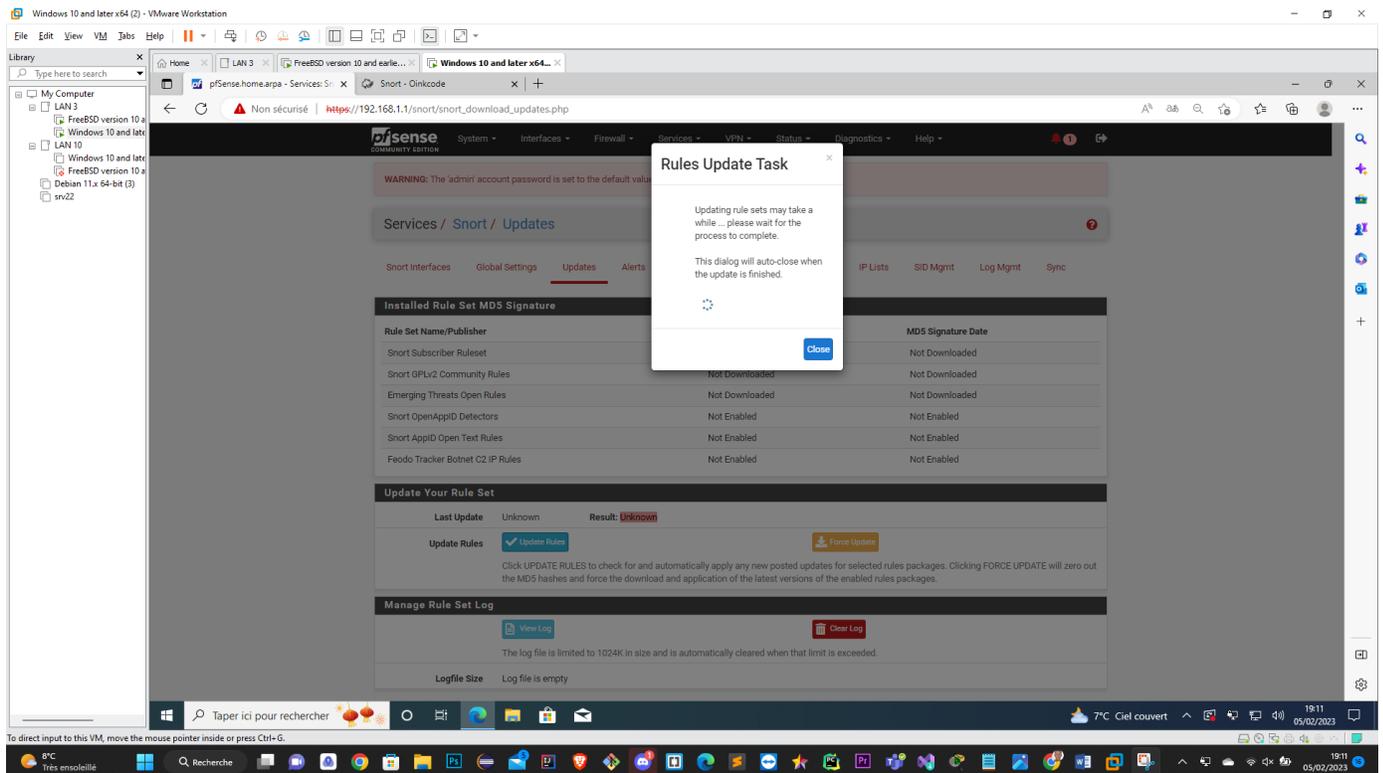
Et dans les paramètres généraux on met 1h pour supprimer l'intervalle des hôtes bloqués.

The screenshot displays the pfSense web interface for configuring Snort. The browser address bar shows the URL https://192.168.1.1/snort/snort_interfaces_global.php. The interface is divided into several sections:

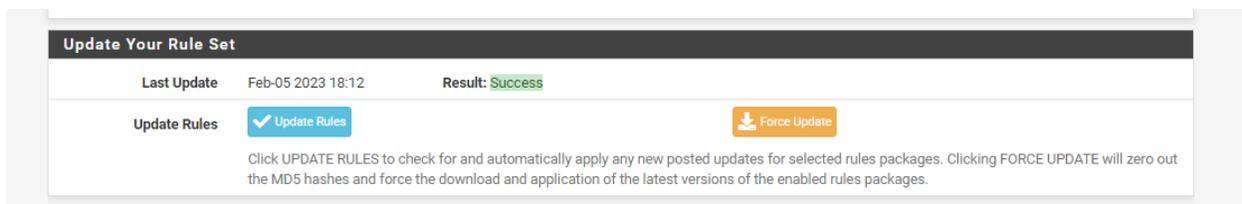
- Enable FEODO Tracker Botnet C2 IP Rules:** Includes a checkbox and a description: "Feodo Tracker tracks certain families that are related to, or that evolved from, Feodo. Originally, Feodo was an ebanking Trojan used by cybercriminals to commit ebanking fraud. Since 2010, various malware families evolved from Feodo, such as Cridex, Dridex, Geodo, Heodo and Emotet."
- Rules Update Settings:**
 - Update Interval:** Set to "1 DAY". A note states: "Please select the interval for rule updates. Choosing NEVER disables auto-updates."
 - Update Start Time:** Set to "00:00". A note explains: "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."
 - Hide Deprecated Rules Categories:** Checked. Note: "Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked."
 - Disable SSL Peer Verification:** Not checked. Note: "Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked."
- General Settings:**
 - Remove Blocked Hosts Interval:** Set to "1 HOUR". Note: "Please select the amount of time you would like hosts to be blocked. In most cases, one hour is a good choice."
 - Remove Blocked Hosts After Deinstall:** Not checked. Note: "Click to clear all blocked hosts added by Snort when removing the package. Default is checked."
 - Keep Snort Settings After Deinstall:** Checked. Note: "Click to retain Snort settings after package removal."
 - Startup/Shutdown Logging:** Checked. Note: "Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked."

A blue "Save" button is located at the bottom of the settings area. The footer of the page indicates "pfSense is developed and maintained by Netgate. © ESP 2004 - 2023 View license."

Et on poursuivra dans l'onglet mise à jour pour cliquer sur le bouton règle de mise à jour pour mettre à jour les règles Snort.



Patientez 1 à 2 minutes pendant la mise à jour



Après mise à jour de règles on va sur l'onglet Snort Interfaces pour ajouter l'interface à surveiller, on laissera notre WAN et les autres paramètres par défaut.

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	<input checked="" type="checkbox"/> Enable interface
Interface	<input type="text" value="WAN (em0)"/> <small>Choose the interface where this Snort instance will inspect traffic.</small>
Description	<input type="text" value="WAN"/> <small>Enter a meaningful description here for your reference.</small>
Snap Length	<input type="text" value="1518"/> <small>Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.</small>

Alert Settings

Send Alerts to System Log	<input checked="" type="checkbox"/> Snort will send Alerts to the firewall's system log. Default is Not Checked.
System Log Facility	<input type="text" value="LOG_AUTH"/> <small>Select system log Facility to use for reporting. Default is LOG_AUTH.</small>
System Log Priority	<input type="text" value="LOG_ALERT"/> <small>Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.</small>
Enable Packet Captures	<input type="checkbox"/> Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file

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 (em0)	⊗ ▶	AC-BNFA	LEGACY MODE	WAN	✎ 📄 🗑️

+ Add 🗑️ Delete

i

Après l'ajout de l'interface WAN on va l'éditer pour ajouter la politique IPS

The screenshot shows the 'WAN - Categories' configuration page in a web interface. The breadcrumb trail is 'Services / Snort / Interface Settings / WAN - Categories'. The navigation menu includes 'Snort Interfaces', 'Global Settings', 'Updates', 'Alerts', 'Blocked', 'Pass Lists', 'Suppress', 'IP Lists', 'SID Mgmt', 'Log Mgmt', and 'Sync'. Below this, there are sub-menus for 'WAN Settings', 'WAN Categories', 'WAN Rules', 'WAN Variables', 'WAN Preprocs', 'WAN IP Rep', and 'WAN Logs'. The 'WAN Categories' sub-menu is active.

The main content area is divided into three sections:

- Automatic Flowbit Resolution:**
 - Resolve Flowbits:** A checkbox is checked. Text: '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.'
 - Auto-Flowbit Rules:** A 'View' button is present. Text: 'Disabling auto-flowbit rules is strongly discouraged for security reasons. Auto-enabled flowbit rules that generate unwanted alerts should have their GID:SID added to the Suppression List for the interface instead of being disabled.'
- Snort Subscriber IPS Policy Selection:**
 - Use IPS Policy:** A checkbox is checked. Text: '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:** A dropdown menu is set to 'Balanced'. Text below: 'Snort IPS policies are: Connectivity, Balanced, Security or Max-Detect. Connectivity blocks most major threats with few or no false positives. Balanced is a good starter policy. It is speedy, has good base coverage level, and covers most threats of the day. It includes all rules in Connectivity. Security is a stringent policy. It contains everything in the first two plus policy-type 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!'
- Select the rulesets (Categories) Snort will load at startup:**
 - Legend: Green circle with plus - Category is auto-enabled by SID Mgmt conf files; Red circle with minus - Category is auto-disabled by SID Mgmt conf files.
 - Buttons: 'Select All', 'Unselect All', and 'Save'.
 - Table with columns 'Enable' and 'Ruleset: Snort GPLv2 Community Rules':

Enable	Ruleset: Snort GPLv2 Community Rules
<input type="checkbox"/>	Snort GPLv2 Community Rules (Talos certified)

Les politiques Snort IPS sont Connectivity, Balanced, Sécurité et Max-Detect:

- **Connectivity** : bloque la plupart des menaces majeures avec peu ou pas de faux positifs.
- **Balanced** : est une bonne politique de départ. Il est rapide, a un bon niveau de couverture de base et couvre la plupart des menaces. Il inclut toutes les règles de Connectivité.
- **Sécurité** : est une politique stricte. Il contient tout ce qui se trouve dans les deux premiers plus les règles de type politique telles qu'un objet Flash dans un fichier Excel.
- **Max-Detect** : est une stratégie créée pour tester le trafic réseau via votre appareil. Cette politique doit être utilisée avec prudence sur les systèmes de production !

Pour notre travail on a opté pour la politique **Balanced**

Et ensuite on passera au démarrage de l'interface

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 checked="" type="checkbox"/> WAN (em0)	✖ ▶	AC-BNFA	LEGACY MODE	WAN	✎ 📄 🗑️

+ Add 🗑️ Delete

i

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 (em0)	✔ 🔄 📄	AC-BNFA	LEGACY MODE	WAN	✎ 📄 🗑️

+ Add 🗑️ Delete

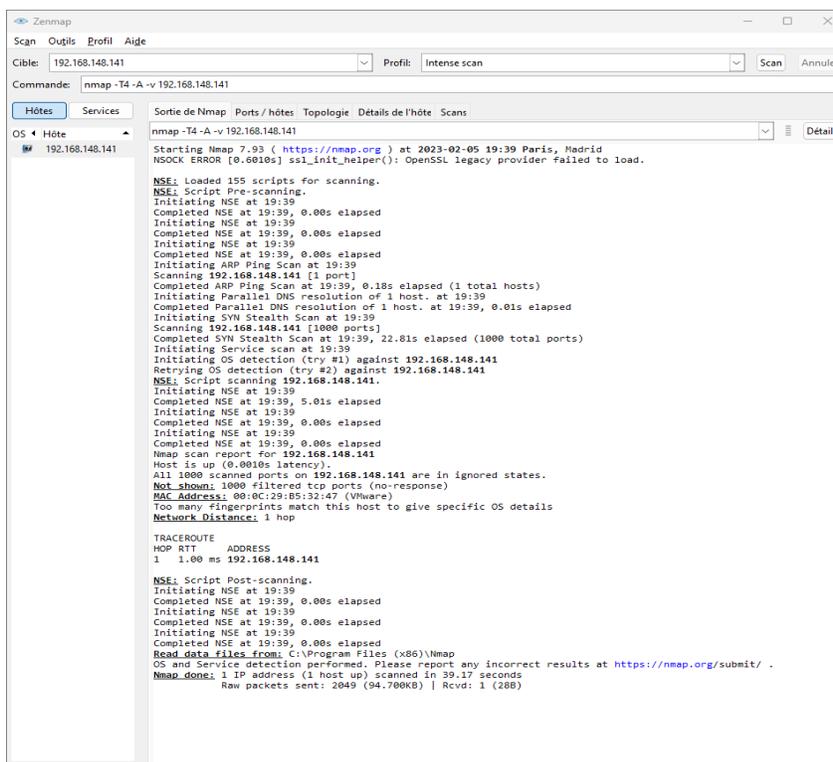
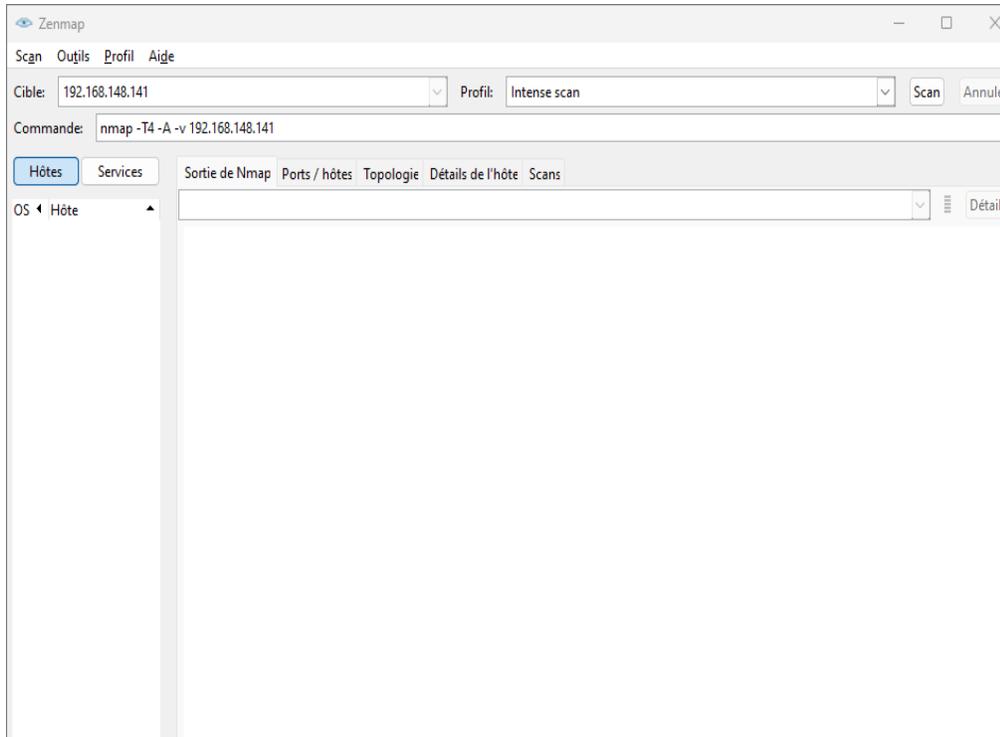
i

Et sur cette image on voit où les alertes et les adresses bloquées vont s'afficher

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

3. TEST D'INTRUSION

A l'aide de notre PC physique on installera l'utilitaire Zenmap qui nous aidera à scanner le port de notre PFSense qui a l'adresse 192.168.148.141/24.



Et pour finir quand on rentrera dans notre PfSense on verra l'alerte et l'adresse IP de notre machine physique qui sera bloquée.

Services / Snort / Alerts ?

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

Alert Log View Settings

Interface to Inspect: WAN (em0) Auto-refresh view 250 [Save](#)
Choose interface.. Alert lines to display.

Alert Log Actions [Download](#) [Clear](#)

Alert Log View Filter

+ +

1 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2023-02-05 18:38:33		3	TCP	Unknown Traffic	13.107.4.50	80	192.168.148.141	15337	120:3	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE

Services / Snort / Blocked Hosts ?

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

Blocked Hosts and Log View Settings

Blocked Hosts [Download](#) [Clear](#)
All blocked hosts will be saved All blocked hosts will be removed

Refresh and Log View [Save](#) Refresh 500
Save auto-refresh and view settings Default is ON Number of blocked entries to view. Default is 500

Last 500 Hosts Blocked by Snort (only applicable to Legacy Blocking Mode interfaces)

#	IP	Alert Descriptions and Event Times	Remove
1	13.107.4.50	(http_inspect) NO CONTENT-LENGTH OR TRANSFER-ENCODING IN HTTP RESPONSE -- 2023-02-05 18:38:33	

1 host IP address is currently being blocked Snort on Legacy Blocking Mode interfaces.