

## Contexte GSB

Le laboratoire Galaxy Swiss Bourdin est issu de la fusion entre le géant américain Galaxy et le conglomérat européen Swiss Bourdin, lui-même déjà union de trois petits laboratoires. En 2009, les deux géants pharmaceutiques unissent leurs forces pour créer un leader de ce secteur industriel. L'entité GSB Europe a établi son siège administratif à Paris. Le siège social de la multinationale est situé à Philadelphie, Pennsylvanie, aux Etats-Unis. La France a été choisie comme témoin pour l'amélioration du suivi de l'activité de visite.

## Besoins :

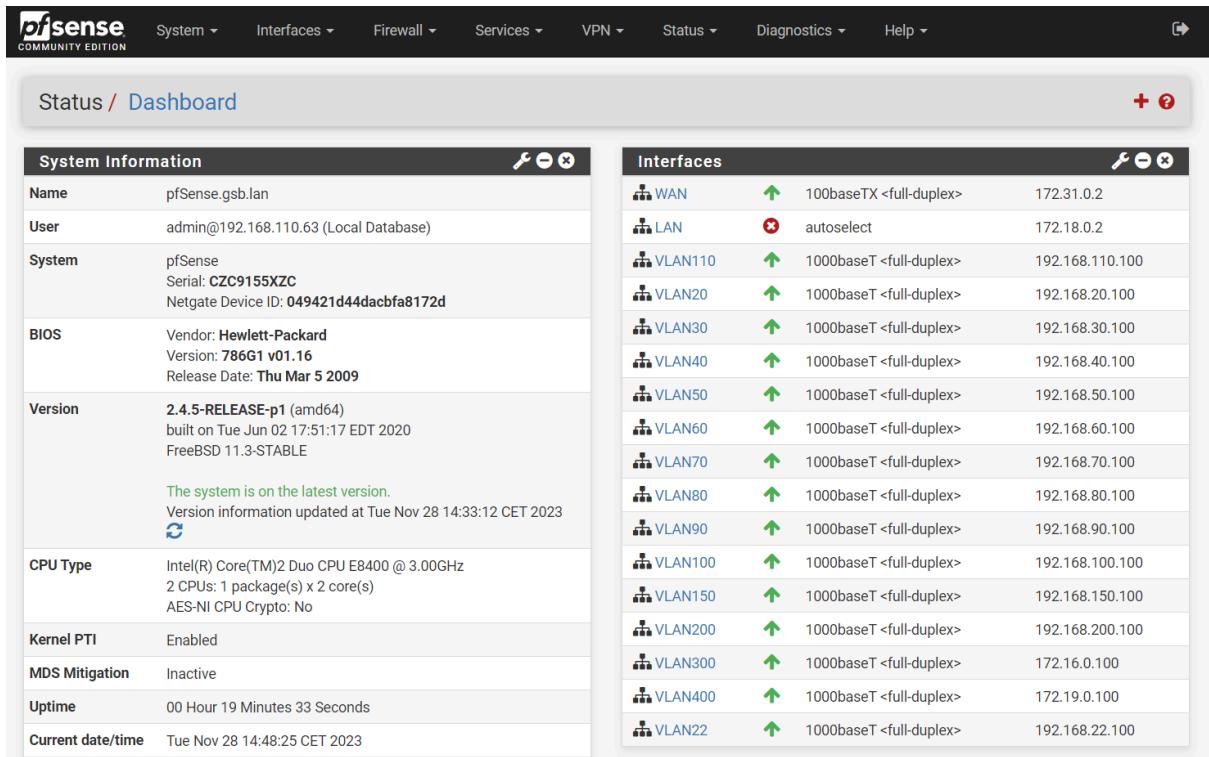
Depuis la réorganisation de GSB l'entreprise fonctionne bien et a connu une hausse de son activité. Suite à cela Galaxy Swiss Bourdin a décidé de mettre en place

## Solution:

Sécurisation d'un service informatique avec  
PFSENS

### 1. Le pare feu IDS, IPS avec Snort sur PFsens

Pour commencer nous allons installer Snort sur le pfsens, pour se faire nous allons sur l'adresse suivante avec notre Vlan: 192.168."Vlan".100



The screenshot shows the pfSense Status / Dashboard page. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is divided into two sections: 'System Information' on the left and 'Interfaces' on the right.

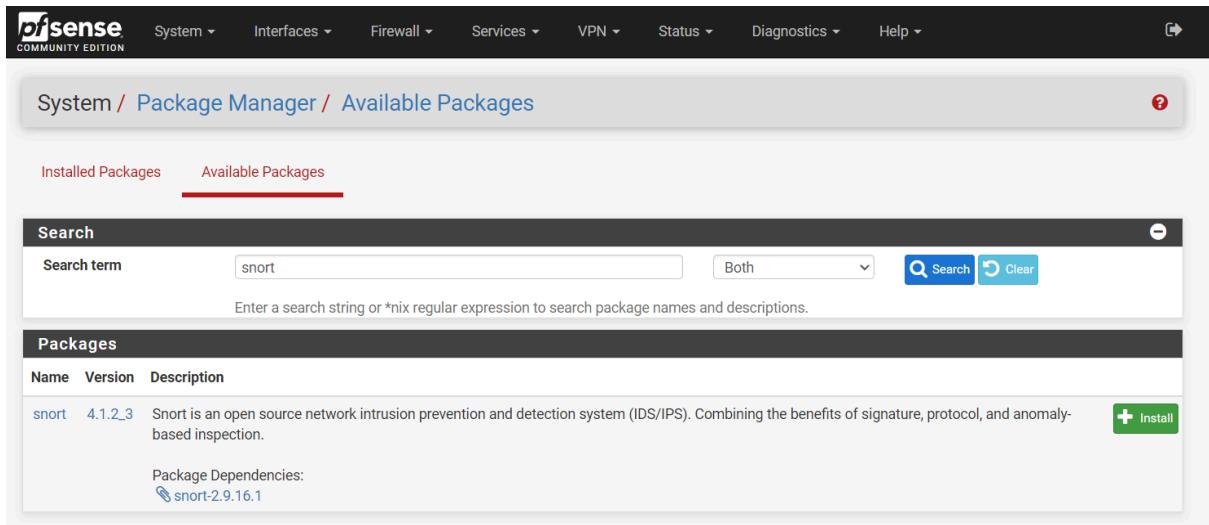
**System Information** (Left):

Name	pfSense.gsb.lan
User	admin@192.168.110.63 (Local Database)
System	pfSense Serial: CZC9155XZC Netgate Device ID: 049421d44dacbfa8172d
BIOS	Vendor: Hewlett-Packard Version: 786G1 v01.16 Release Date: Thu Mar 5 2009
Version	2.4.5-RELEASE-p1 (amd64) built on Tue Jun 02 17:51:17 EDT 2020 FreeBSD 11.3-STABLE
CPU Type	Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz 2 CPUs: 1 package(s) x 2 core(s) AES-NI CPU Crypto: No
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	00 Hour 19 Minutes 33 Seconds
Current date/time	Tue Nov 28 14:48:25 CET 2023

**Interfaces** (Right):

WAN	100baseTX <full-duplex>	172.31.0.2
LAN	autoselect	172.18.0.2
VLAN110	1000baseT <full-duplex>	192.168.110.100
VLAN20	1000baseT <full-duplex>	192.168.20.100
VLAN30	1000baseT <full-duplex>	192.168.30.100
VLAN40	1000baseT <full-duplex>	192.168.40.100
VLAN50	1000baseT <full-duplex>	192.168.50.100
VLAN60	1000baseT <full-duplex>	192.168.60.100
VLAN70	1000baseT <full-duplex>	192.168.70.100
VLAN80	1000baseT <full-duplex>	192.168.80.100
VLAN90	1000baseT <full-duplex>	192.168.90.100
VLAN100	1000baseT <full-duplex>	192.168.100.100
VLAN150	1000baseT <full-duplex>	192.168.150.100
VLAN200	1000baseT <full-duplex>	192.168.200.100
VLAN300	1000baseT <full-duplex>	172.16.0.100
VLAN400	1000baseT <full-duplex>	172.19.0.100
VLAN22	1000baseT <full-duplex>	192.168.22.100

Puis se rendre sur Système > Package manager > Available package, rechercher Snort et l'installer:



The screenshot shows the pfSense System / Package Manager / Available Packages page. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area has tabs for 'Installed Packages' and 'Available Packages', with 'Available Packages' selected.

**Search** (Top):

Search term: snort

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

**Packages** (Table):

Name	Version	Description	Action
snort	4.1.2_3	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.	<a href="#">Install</a>
Package Dependencies:			<a href="#">snort-2.9.16.1</a>

Une fois installé il doit apparaître dans “installed package” comme ceci:

Installed Packages Available Packages

**Installed Packages**

Name	Category	Version	Description	Actions
✓ snort	security	4.1.2.3	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-2.9.16.1

= Update = Current  
 = Remove = Information = Reinstall

Newer version available

Package is configured but not (fully) installed or deprecated

Maintenant nous pouvons nous rendre dans l'onglet service > Snort pour le configurer.

La première étape est d'activer le téléchargement de règles gratuites, en cochant la première case (Enable Snort VRT). Il faudra renseigner une clé et pour l'obtenir il vous faudra créer un compte sur le site officiel de Snort.

Récupération du code:

snort.org/users/907695/oinkcodes/907533 alexiskresser2802@gmail.com

rch... Rule Doc Search Documents Downloads Products Com

kresser2802@gmail.com

unt

ode

ription

ots

Positive

License

rces

Oinkcode

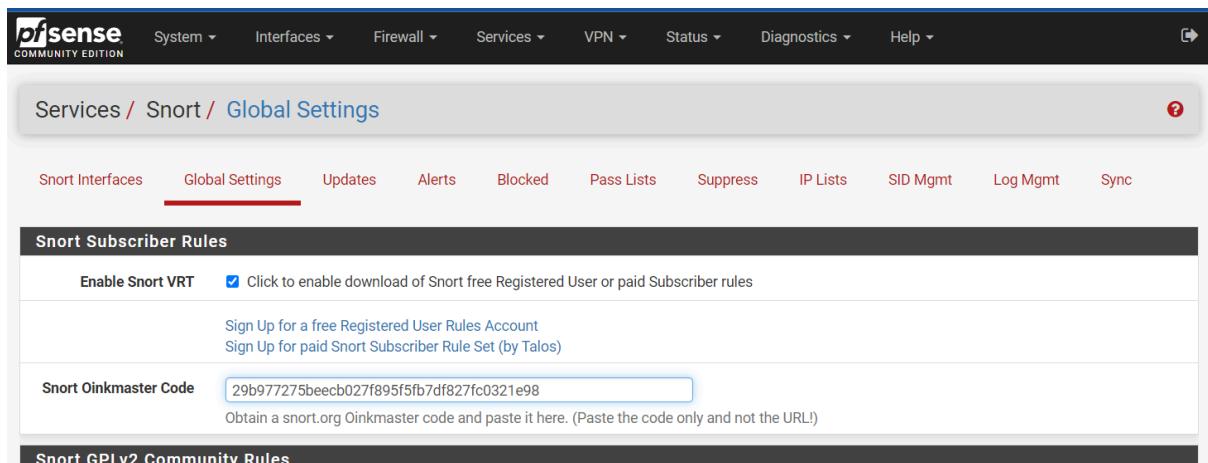
**29b977275beecb027f895f5fb7df827fc0321e98**

Regenerate

Documentation and Resources

How to use your oinkcode  
Informational and instructional resources for Snort 2 and Snort 3

Mettre le code dans “**Snort Oinkmaster Code**”



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 Oinkmaster Code

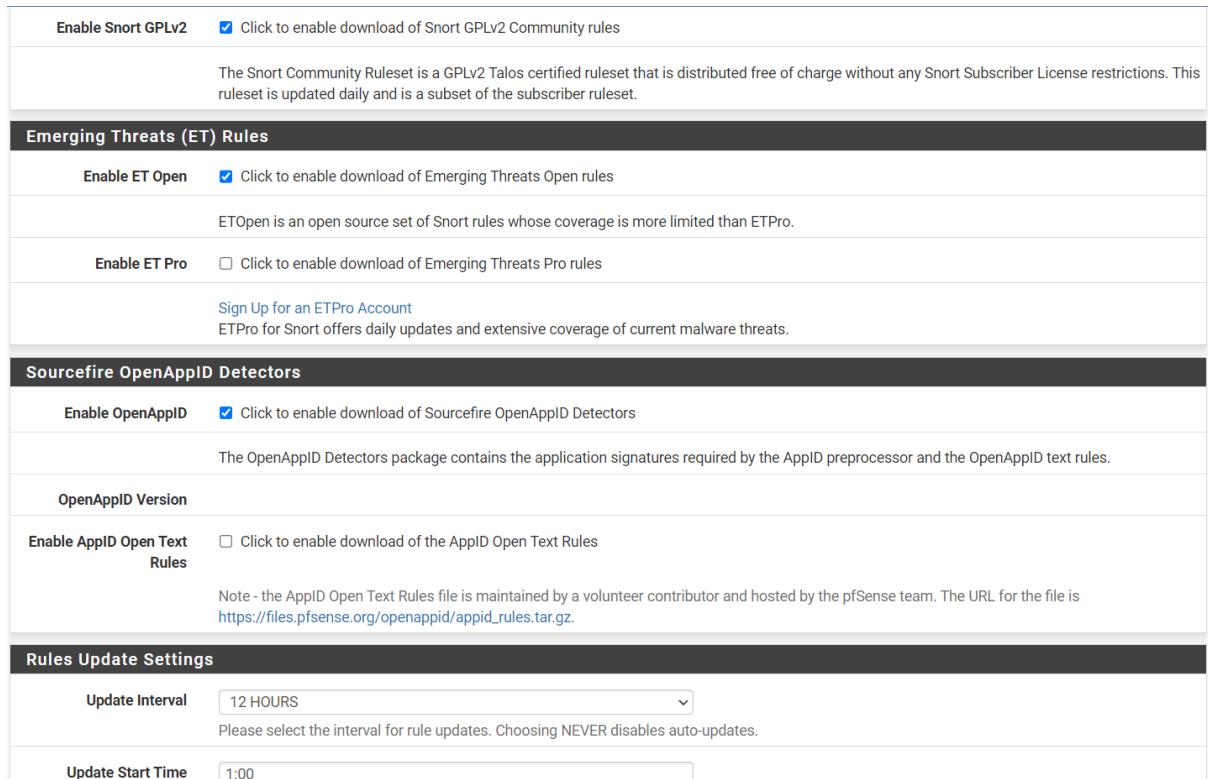
Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)

**Snort GPLv2 Community Rules**

Ensute nous pouvons cocher les cases :

- **Enable Snort GPLv2**, pour les règles communautaires
- **Enable ET Open**, qui sont des règles proposées par la société ET
- **Enable Open AppID**, éventuellement, qui est une autre société

Puis, pour les derniers paramètres il convient simplement de configurer l'update pour les différentes règles, c'est-à-dire le délai avant de vérifier les mises à jour pour les différentes règles:



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.

**Sourcefire OpenAppID Detectors**

Enable OpenAppID  Click to enable download of Sourcefire OpenAppID Detectors

The OpenAppID Detectors package contains the application signatures required by the AppID preprocessor and the OpenAppID text rules.

**OpenAppID Version**

Enable AppID Open Text Rules  Click to enable download of the AppID Open Text Rules

Note - the AppID Open Text Rules file is maintained by a volunteer contributor and hosted by the pfSense team. The URL for the file is [https://files.pfsense.org/openappid/appid\\_rules.tar.gz](https://files.pfsense.org/openappid/appid_rules.tar.gz).

**Rules Update Settings**

Update Interval  Please select the interval for rule updates. Choosing NEVER disables auto-updates.

Update Start Time

Dans notre cas l'intervalles des mise à jour sera de 12h minimum et l'heure de mise à jour sera 1h du matin pour ne pas gêner l'activité des collaborateurs

### Ne pas oublier de sauvegarder le paramétrage

Une fois sauvegarder, nous pouvons nous rendre sur l'onglet Updates et manuellement mettre à jour les différentes règles que nous avons cochées précédemment en cliquant sur “update rules” (dans notre cas cela prendra un peu de temps, car nous allons toutes les télécharger une première fois).

The screenshot shows the Snort interface with the 'Updates' tab selected. The 'Installed Rule Set MD5 Signature' table lists several rule sets with their MD5 signature status:

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 Downloaded	Not Downloaded
Snort AppID Open Text Rules	Not Enabled	Not Enabled

Below the table is the 'Update Your Rule Set' section, which includes a 'Result: Unknown' status, a 'Update Rules' button (with a checked checkbox), and a 'Force Update' button.

At the bottom, a 'Rules Update Task' dialog box is displayed, containing the following text and a progress indicator:

Updating rule sets may take a while ... please wait for the process to complete.  
This dialog will auto-close when the update is finished.



**Close**

## Update Your Rule Set

Last Update

Nov-28 2023 15:30

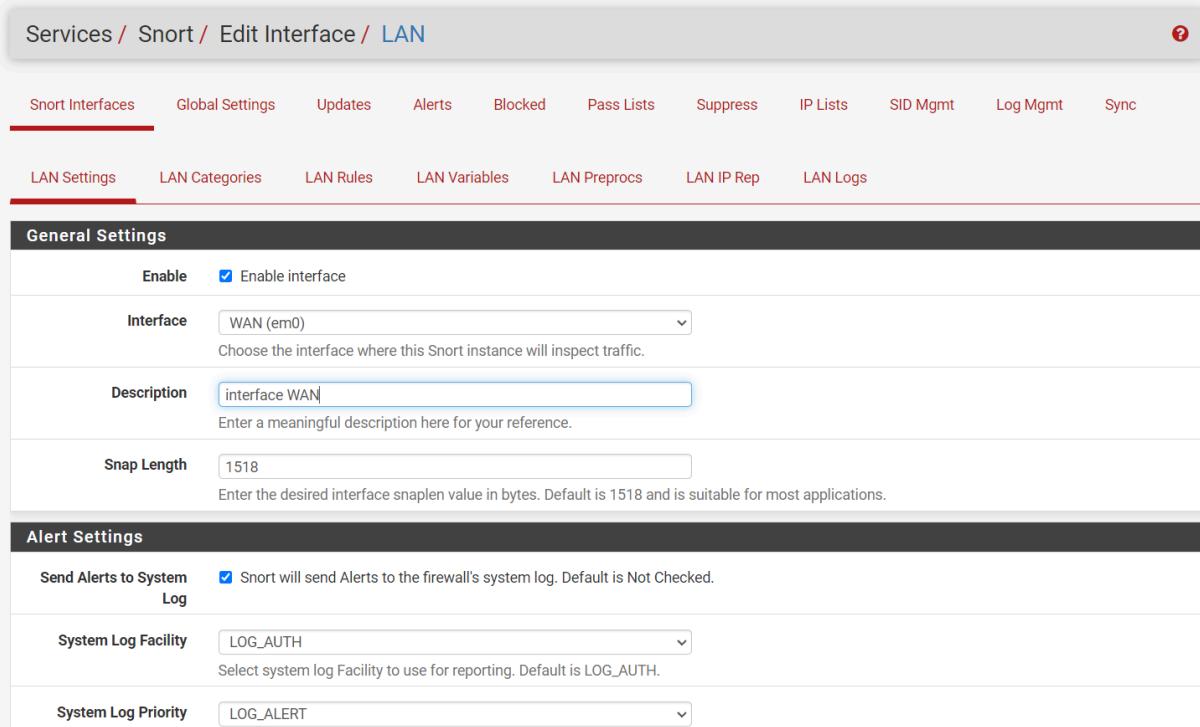
Result: Success

Maintenant que Snort est bien installé et configuré nous pouvons nous rendre sur “Snort interfaces” pour choisir l’interface (ou les interfaces) sur laquelle Snort va écouter et analyser le trafic et appuyer sur “add” pour ajouter:



The screenshot shows the 'Snort Interfaces' tab selected in the top navigation bar. Below it is a table titled 'Interface Settings Overview' with columns: Interface, Snort Status, Pattern Match, Blocking Mode, Description, and Actions. A green 'Add' button is located in the bottom right corner of the table area.

Ici nous choisissons donc l’interface que nous voulons surveiller, puis une description du réseau et ensuite nous cochons simplement le fait d’envoyer les alertes sur le système de log interne, pour les analyser en cas de tentative d’intrusion

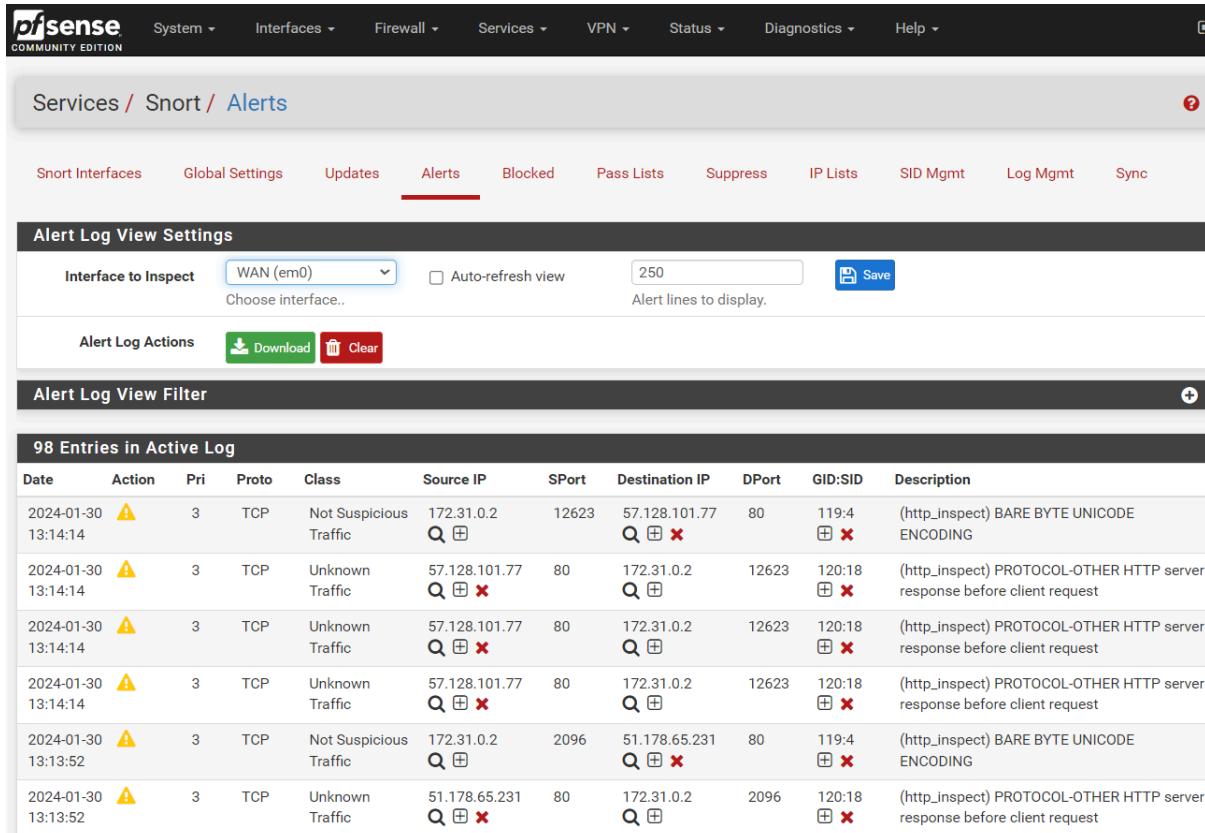


The screenshot shows the 'Edit Interface / LAN' page. The 'Snort Interfaces' tab is selected in the top navigation bar. Below it are tabs for LAN Settings, LAN Categories, LAN Rules, LAN Variables, LAN Preprocs, LAN IP Rep, and LAN Logs. The 'General Settings' section contains fields for Enable (checked), Interface (WAN (em0)), Description (interface WAN), and Snap Length (1518). The 'Alert Settings' section contains fields for Send Alerts to System Log (checked), System Log Facility (LOG\_AUTH), and System Log Priority (LOG\_ALERT).

A partir de ces options nous avons mis en place notre IDS car ils nous envoie les informations du pare-feu dans des logs consultables.

## Test de Fonctionnement IDS

Maintenant que nous l'avons activé, en allant dans l'interface Service > Snort > Alertes on peut observer les logs qui arrivent et qui nous prévient de toute connexion suspecte sur le réseau sans bloquer la connexion au réseau qu'il tente d'accéder.



The screenshot shows the pfSense Snort Alerts interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main page title is "Services / Snort / Alerts". Below the title, there are tabs for Snort Interfaces, Global Settings, Updates, **Alerts** (which is selected), Blocked, Pass Lists, Suppress, IP Lists, SID Mgmt, Log Mgmt, and Sync. The "Alert Log View Settings" section allows selecting the "Interface to Inspect" (WAN (em0)), enabling "Auto-refresh view" (set to 250), and saving the settings. The "Alert Log Actions" section includes "Download" and "Clear" buttons. The "Alert Log View Filter" section has a "+ Add" button. The main content area displays a table titled "98 Entries in Active Log" with the following columns: Date, Action, Pri, Proto, Class, Source IP, SPort, Destination IP, DPort, GID:SID, and Description. The table lists 98 entries, each with a timestamp, an alert icon (yellow triangle), a priority (3), TCP protocol, and various source and destination details. The descriptions provide context for each alert, such as "BARE BYTE UNICODE ENCODING" or "PROTOCOL-OTHER HTTP server response before client request".

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-01-30 13:14:14	⚠️	3	TCP	Not Suspicious Traffic	172.31.0.2	12623	57.128.101.77	80	119:4	(http_inspect) BARE BYTE UNICODE ENCODING
2024-01-30 13:14:14	⚠️	3	TCP	Unknown Traffic	57.128.101.77	80	172.31.0.2	12623	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request
2024-01-30 13:14:14	⚠️	3	TCP	Unknown Traffic	57.128.101.77	80	172.31.0.2	12623	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request
2024-01-30 13:14:14	⚠️	3	TCP	Unknown Traffic	57.128.101.77	80	172.31.0.2	12623	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request
2024-01-30 13:13:52	⚠️	3	TCP	Not Suspicious Traffic	172.31.0.2	2096	51.178.65.231	80	119:4	(http_inspect) BARE BYTE UNICODE ENCODING
2024-01-30 13:13:52	⚠️	3	TCP	Unknown Traffic	51.178.65.231	80	172.31.0.2	2096	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request