

BTS Services Informatique à l'Organisation

Option : Solutions d'Infrastructure, Systèmes et Réseaux



**Epreuve E5 : Conception et maintenance
de solution informatique**

Document technique

**Projet #2 - Installation et configuration
de Snort pour la détection d'intrusions
sur le réseau interne**

SOMMAIRE

1. Introduction

1.1. Présentation de l'entreprise Kalo-Brazza

1.2. Objectifs du projet

1.3. Contexte et enjeux

2. Présentation de Snort

2.1. Définition et fonctionnalités

2.2. Avantages de l'utilisation de Snort

2.3. Rôle de Snort dans la cybersécurité

3. Spécifications Techniques

3.1. Configuration matérielle requise

4. Plan de Déploiement de Snort

4.1. Préparation de l'environnement

4.2. Installation de Snort

5. Analyse des alertes

1. Introduction

1.1. Présentation de l'entreprise Kalo-Brazza

Kalo-Brazza offre divers services numériques, notamment le développement d'applications, la maintenance de systèmes, et la sécurisation des infrastructures. Pour protéger ses actifs numériques, l'entreprise souhaite mettre en place **Snort** pour la détection et la prévention d'intrusions.

1.2. Objectifs du projet

L'objectif est d'intégrer **Snort** pour assurer une surveillance proactive du réseau, identifier les menaces potentielles, et fournir une réponse rapide aux incidents de sécurité.

1.3. Contexte et enjeux

Face à l'augmentation des cyberattaques, **Kalo-Brazza** doit renforcer ses mesures de sécurité pour protéger ses données sensibles et garantir la continuité de ses services. Snort sera une extension du pfSense précédemment configuré.

2. Présentation de Snort

2.1. Définition et fonctionnalités

Snort est un système open-source de détection et de prévention d'intrusions (IDS/IPS) développé par Cisco, permettant d'analyser le trafic réseau pour détecter des comportements suspects ou des attaques connues.

2.2. Avantages de l'utilisation de Snort

- Surveillance en temps réel du trafic réseau.
- Détection rapide des menaces avec alertes exploitables. •
Possibilité de personnaliser les règles de détection.

2.3. Rôle de Snort dans la cybersécurité

En tant qu'IDS/IPS, **Snort** joue un rôle clé dans la protection du réseau en identifiant et en bloquant les menaces avant qu'elles n'affectent les systèmes critiques.

3. Spécifications Techniques

3.1. Configuration matérielle requise

Snort sera installé sur le pfSense directement.

4. Plan de Déploiement de Snort

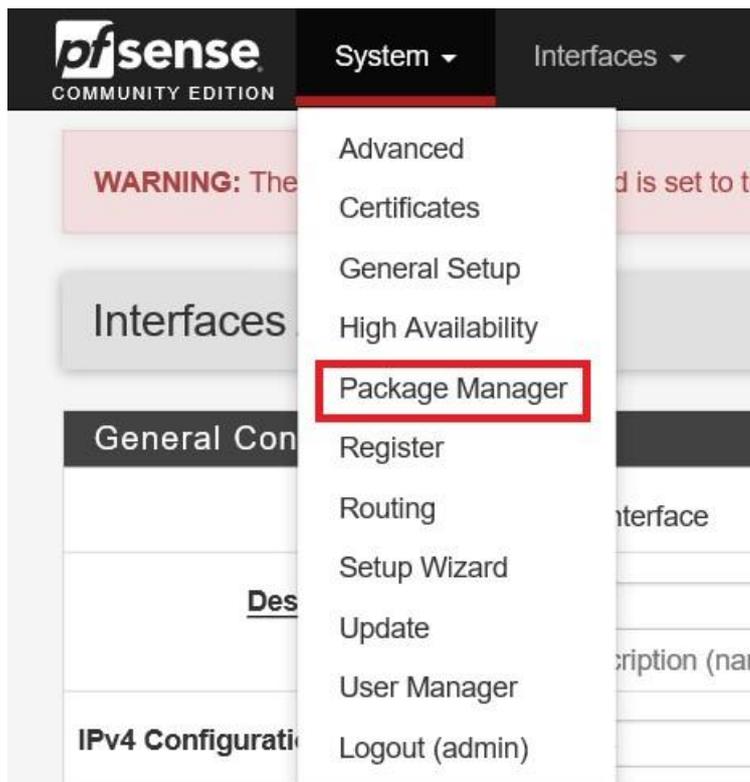
4.1. Préparation de l'environnement

Mise à jour des paquets et installation des dépendances nécessaires pour Snort.

Dans le « shell » de pfSense il faudra effectuer ces commandes : `pkg update && pkg upgrade`

4.2. Installation de Snort

Allez dans Package manager et recherchez le paquet « snort ».



System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term Both

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

Packages

Name	Version	Description	
snort	4.1.6_17	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.	<input type="button" value="+ Install"/>

Package Dependencies:
[snort-2.9.20_8](#)

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_17:

--
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

```

Snort est maintenant installé !

Snort fonctionne sur base de règles permettant de détecter les comportements suspects.

Il existe plusieurs sources pour ces règles, certaines sont gratuites, certaines sont payantes.

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

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

On va modifier la période de rafraichissement et la période avant la suppression automatique du "ban" et ensuite appuyer sur save.

Rules Update Settings

Update Interval **7 DAYS** Please select the interval for rule updates. Choosing NEVER disables auto-updates.

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.

Hide Deprecated Rules Categories Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.

Disable SSL Peer Verification 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 **1 HOUR** 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 Click to clear all blocked hosts added by Snort when removing the package. Default is checked.

Keep Snort Settings After Deinstall Click to retain Snort settings after package removal.

Startup/Shutdown Logging Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.

Save

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

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 Enabled	Not Enabled
Snort GPLv2 Community Rules	Not Downloaded	Not Downloaded
Emerging Threats Open Rules	Not Downloaded	Not Downloaded
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

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

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.

Il faut donc sélectionner la carte (généralement LAN) et l'activer.

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: LAN (em1)
Choose the interface where this Snort instance will inspect traffic.

Description: LAN
Enter a meaningful description here for your reference.

Snap Length: 1518
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.

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

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

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 1 **Ruleset: Snort GPLv2 Community Rules**
 Snort GPLv2 Community Rules (Talos certified)

Enable **Ruleset: ET Open Rules** Snort Subscriber rules are not enabled. Snort OPENAPPID rules are not enabled.

- emerging-activex.rules
- emerging-attack_response.rules
- emerging-botcc.portgrouped.rules

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

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 Category

Category Selection: Auto-Flowbit Rules, custom.rules, decoder.rules, **GPLV2_community.rules**, preprocessor.rules, User Forced Disabled Rules, User Forced Enabled Rules, Active Rules

Rule Signature ID (SID)

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
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	105	tcp	\$HOME_NET	2589	\$EXTERNAL_NET	any	MALWARE-BACKDOOR - Dagger_1.4.0
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	108	tcp	\$EXTERNAL_NET	any	\$HOME_NET	7597	MALWARE-BACKDOOR QAZ Worm Client Login access
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	110	tcp	\$EXTERNAL_NET	any	\$HOME_NET	12345:12346	MALWARE-BACKDOOR netbus getinfo

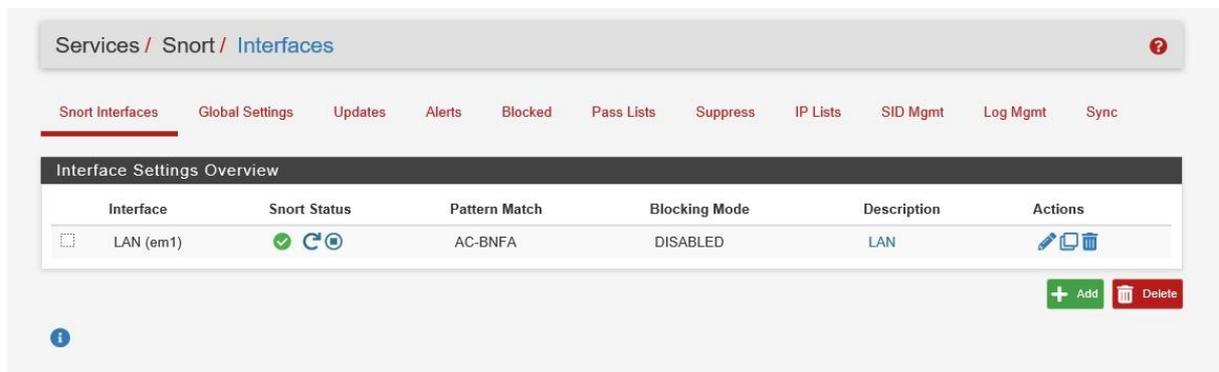
Il reste à activer ce que l'on souhaite.

Pour démarrer snort : on lance le service sur l'interface



The screenshot shows the 'Services / Snort / Interfaces' configuration page. The 'Snort Interfaces' tab is selected. The 'Interface Settings Overview' table lists the LAN (em1) interface with a Snort Status of 'Stopped' (indicated by a red 'X' icon). A red box highlights the 'Start' button (a blue play icon) next to the status. Other columns include Pattern Match (AC-BNFA), Blocking Mode (DISABLED), and Description (LAN). Action buttons for 'Add' and 'Delete' are visible at the bottom right.

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
LAN (em1)	Stopped	AC-BNFA	DISABLED	LAN	  



The screenshot shows the same 'Services / Snort / Interfaces' configuration page. The 'Snort Status' for the LAN (em1) interface is now 'Running' (indicated by a green checkmark icon). The 'Start' button is now disabled. The rest of the interface remains the same.

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
LAN (em1)	Running	AC-BNFA	DISABLED	LAN	  

5. Analyse des alertes

Mise en place d'outils d'analyse pour interpréter les alertes générées par **Snort** et prioriser les réponses aux incidents.

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



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

Alert Log View Settings

Interface to Inspect: LAN (em1) Auto-refresh view Save

Choose interface.. Alert lines to display.

Alert Log Actions Download Clear

Alert Log View Filter +

12 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2025-01-22 23:30:47		3	TCP	Unknown Traffic	172.16.1.102 	50669	172.16.1.254 	80	119:34 	(http_inspect) TOO MANY PIPELINED REQUESTS
2025-01-22 23:26:23		3	TCP	Unknown Traffic	172.16.1.102 	50598	172.16.1.254 	80	119:34 	(http_inspect) TOO MANY PIPELINED REQUESTS
2025-01-22 23:24:29		3	TCP	Unknown Traffic	172.16.1.102 	50575	172.16.1.254 	80	119:34 	(http_inspect) TOO MANY PIPELINED REQUESTS
2025-01-22 23:18:11		3	TCP	Unknown Traffic	172.16.1.102 	50470	172.16.1.254 	80	119:34 	(http_inspect) TOO MANY PIPELINED REQUESTS