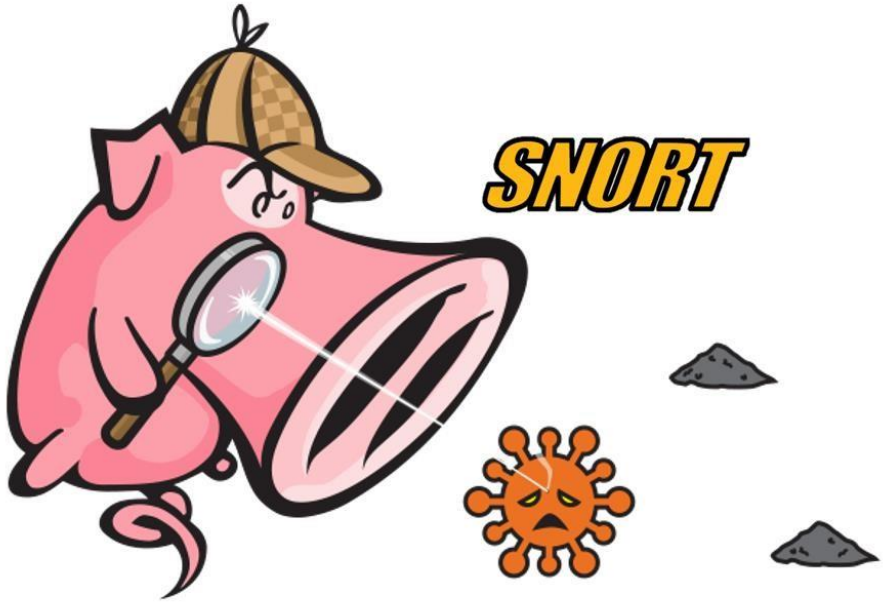
BTS Services Informatique à l'Organisation

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

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

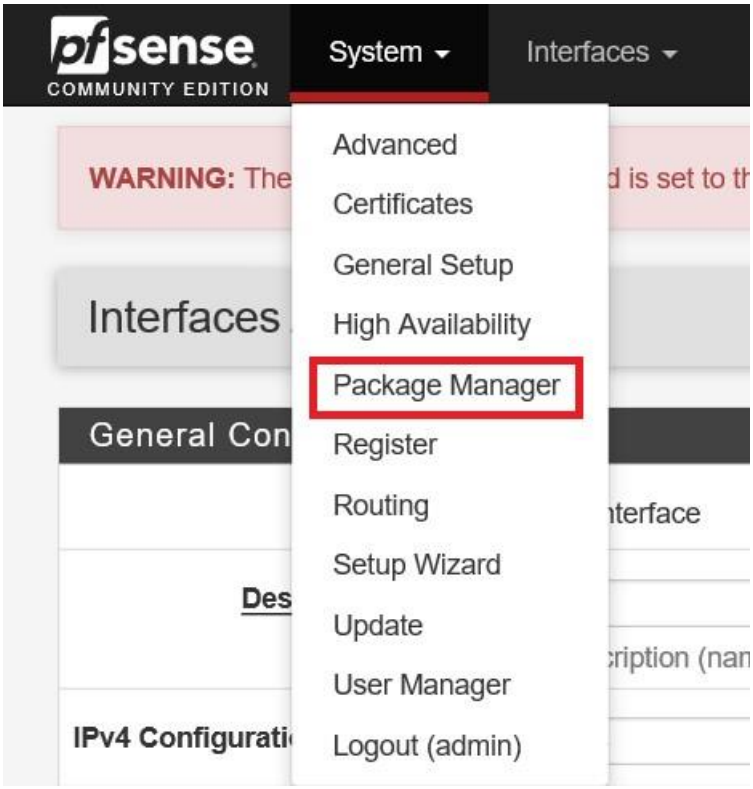
4.1. Préparation de l'environnement

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

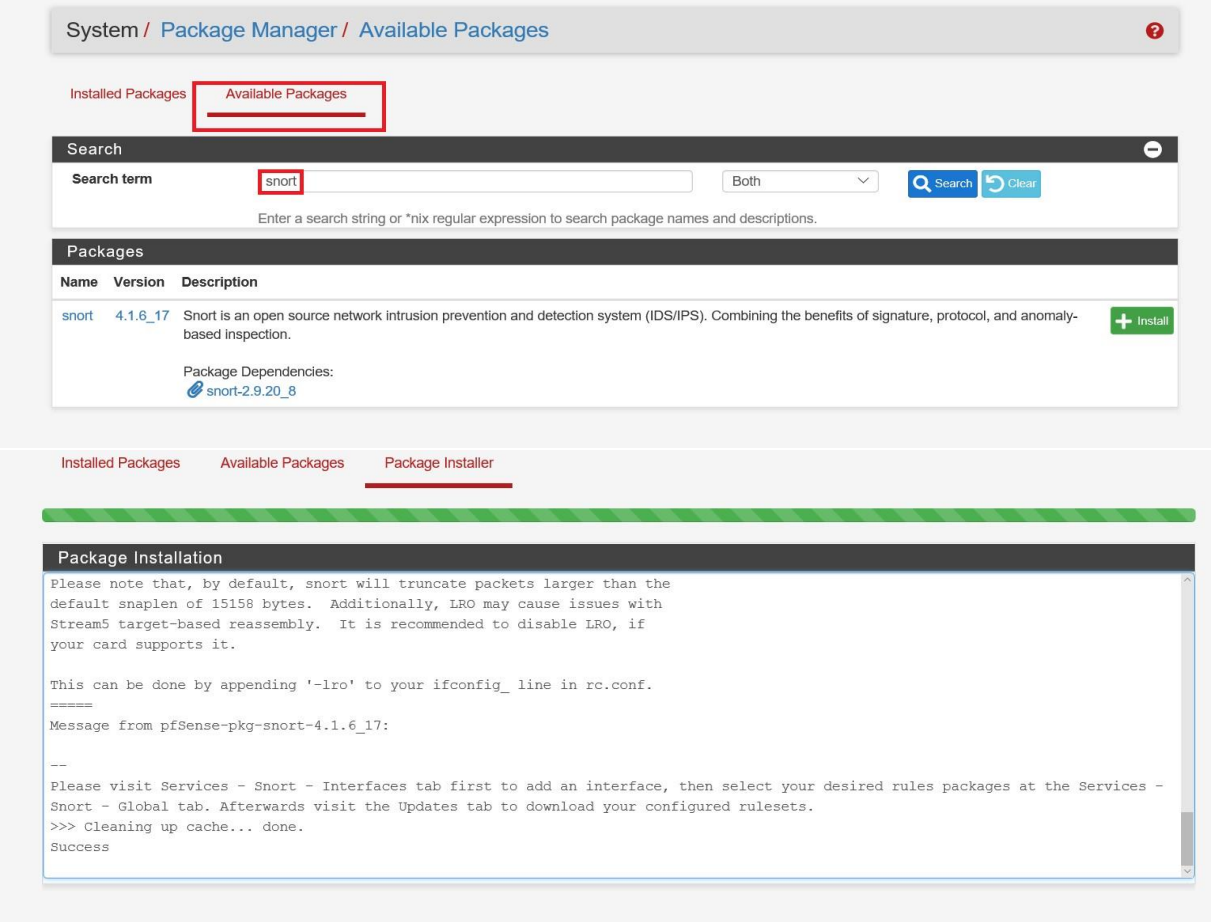
Dans le « shell » de pfSense il faudra effectuer ces commandes : pkg update && pkg upgrade

4.2. Installation de Snort

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



Installez-le.

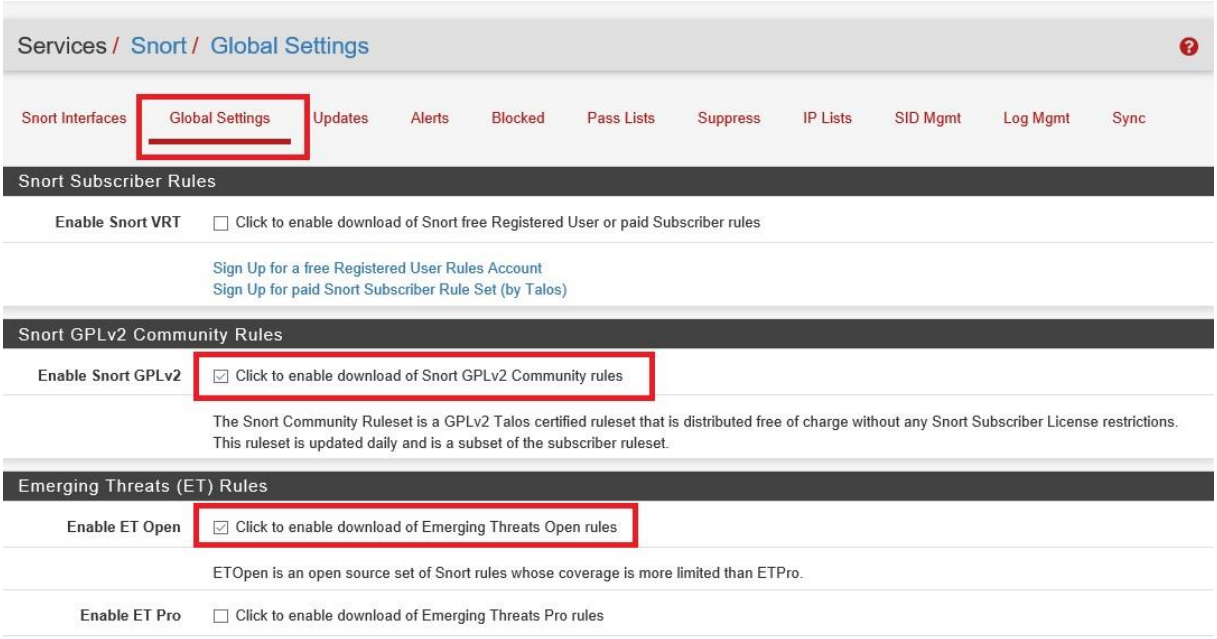


Snort est maintenant installé !

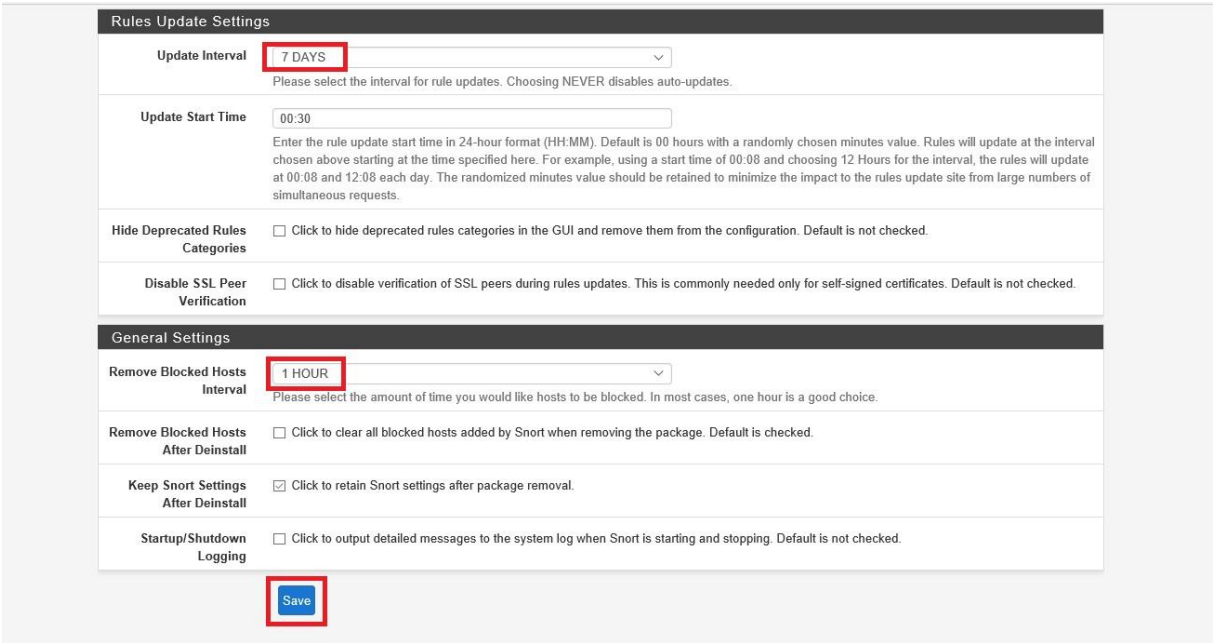
Snort fonctionne sur base de règles permettant de détecter les comportements suspects.

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

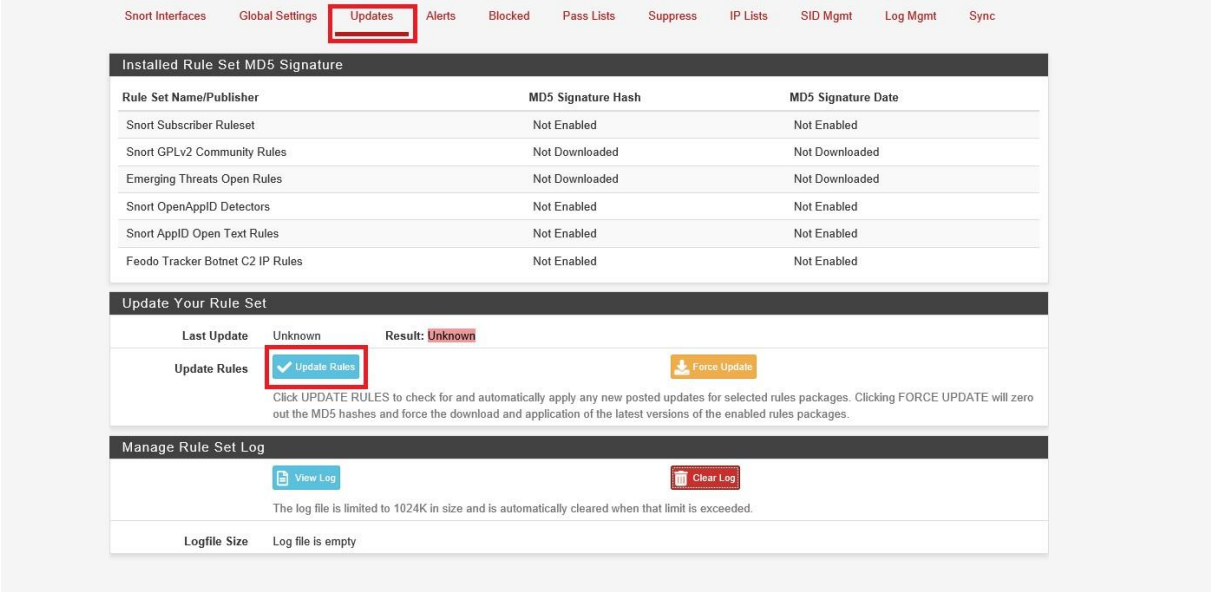
On sélectionne les listes de règles que l'on veut utiliser, ici, je sélectionne deux listes communautaires.



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

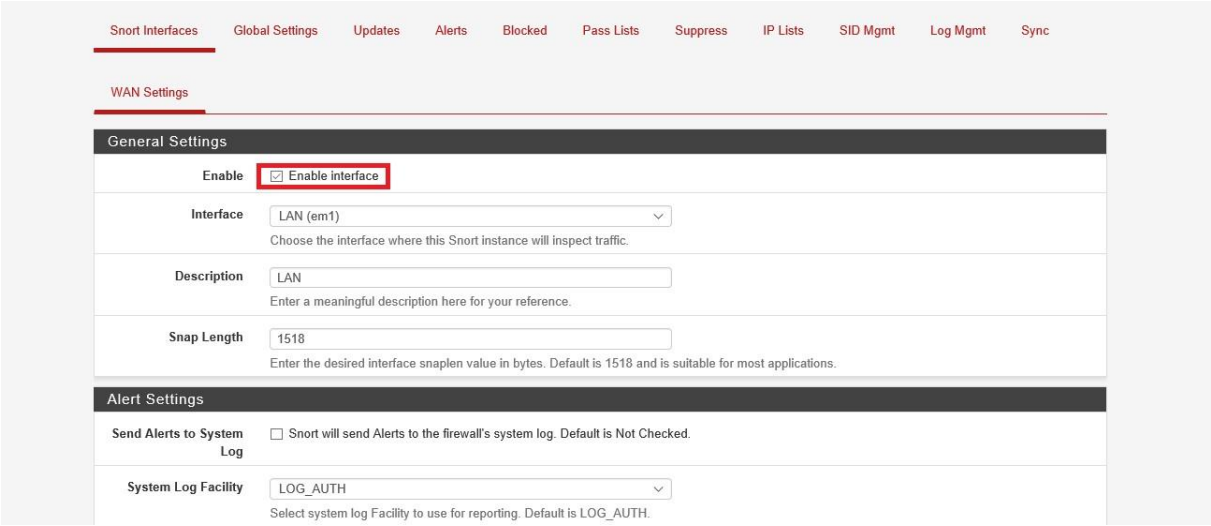


On peut maintenant passer sur l'onglet update et lancer le téléchargement des listes.

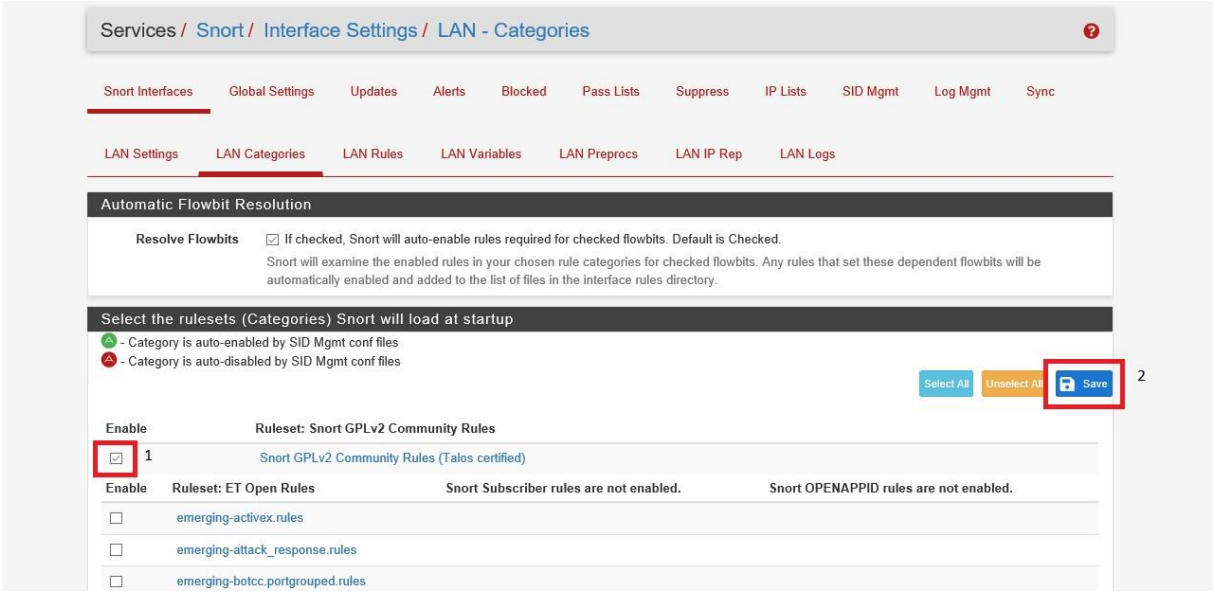


Une fois que la mise à jour est terminée, on peut activer l'interface que snort va écouter.

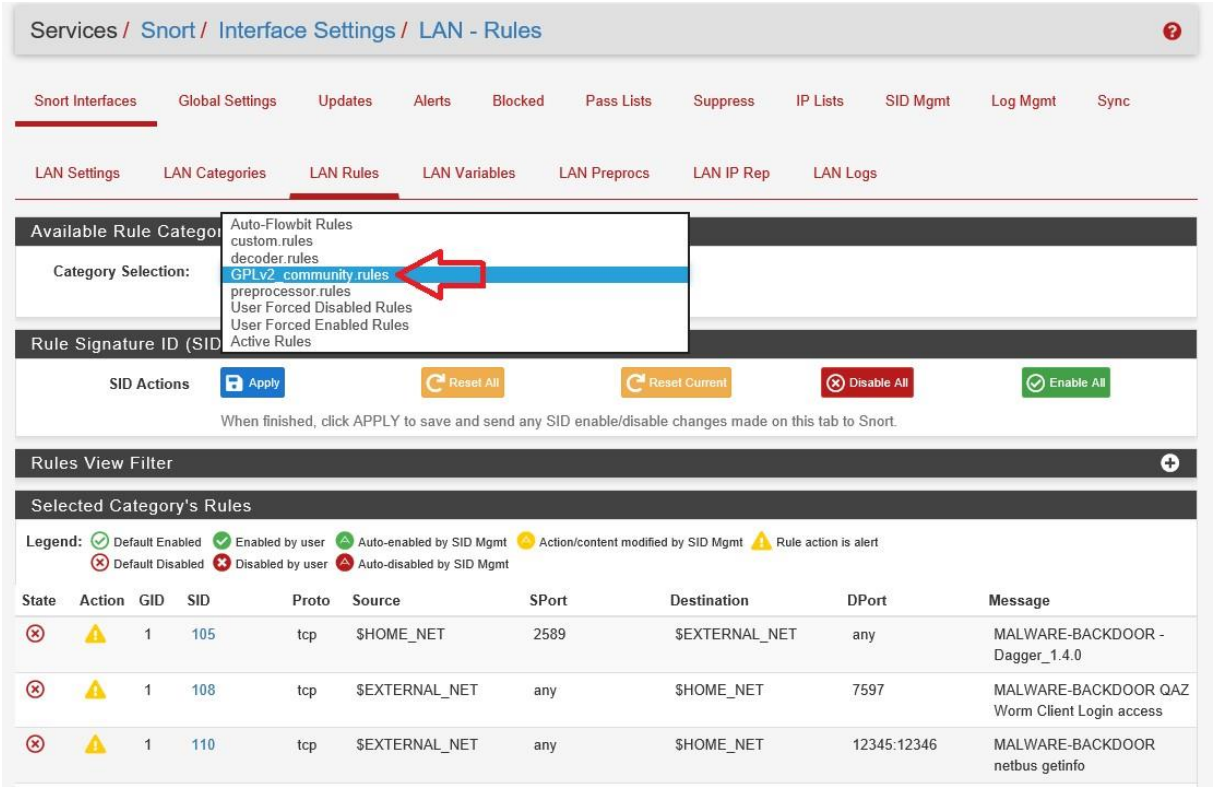
Il faut donc sélectionner la carte (généralement LAN) et l'activer.



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

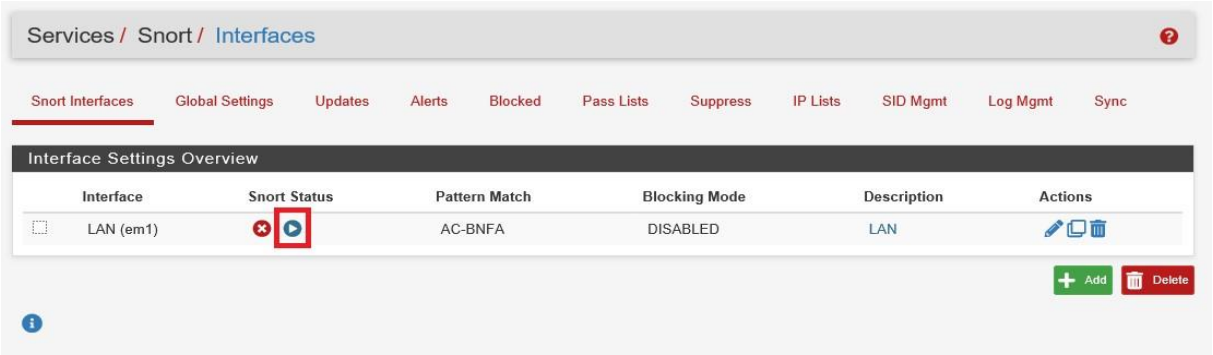


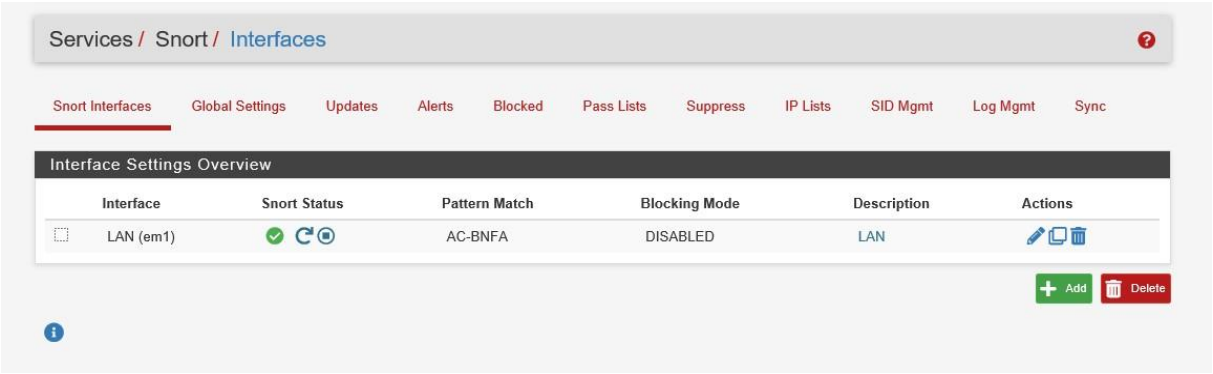
Pour activer/désactiver les règles individuellement, on doit passer sur l'onglet "Rules" et sélectionner une des listes que l'on a activées.



Il reste à activer ce que l'on souhaite.

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

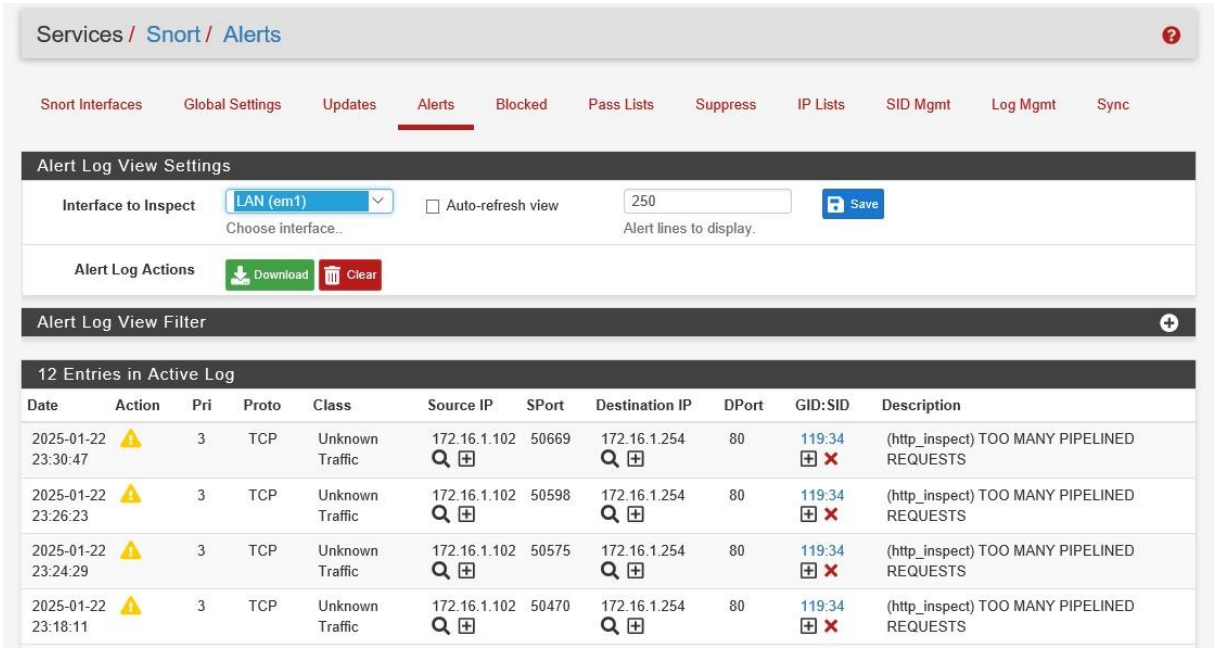




5. Analyse des alertes

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.


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
LAN (em1)
Choose interface..
Auto-refresh view
250
Alert lines to display.
Save
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