# SNORT sur pfSense

## Sommaire

## Introduction

Cette documentation présentera l'installation et la configuration de snort sur pfSense. Snort est un système de détection d'intrusion open source (IDS) pour la surveillance du réseau. Il est complémentaire à un pare-feu.

Snort permet de :

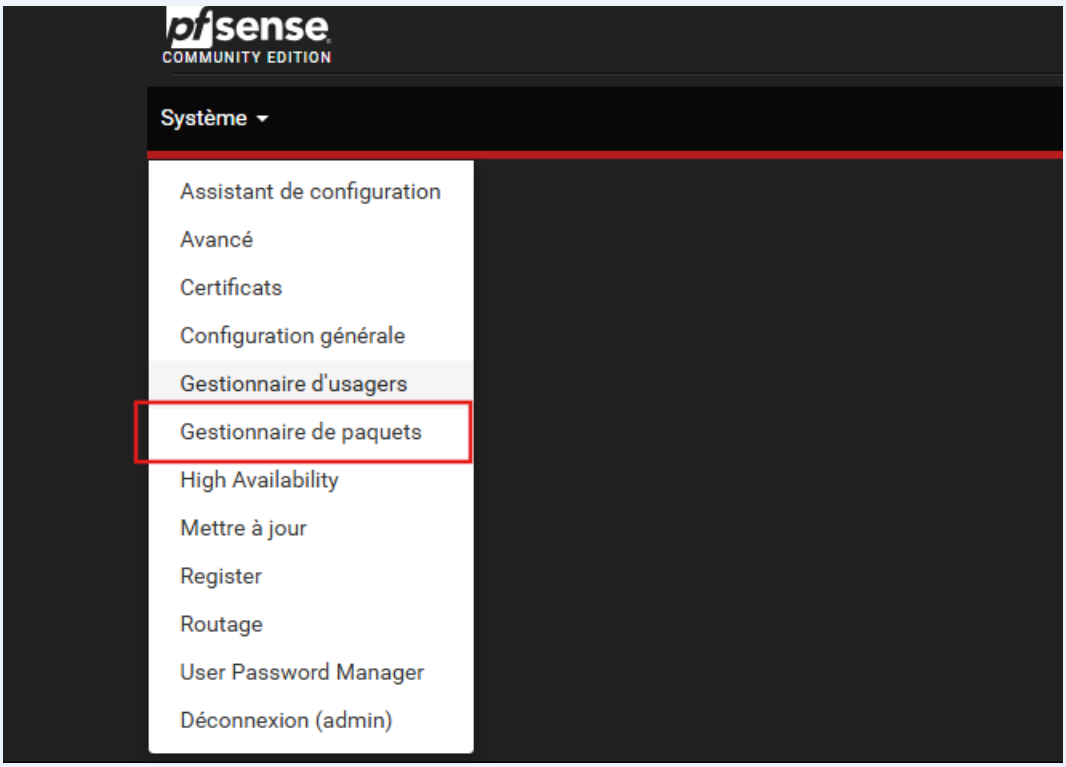
- l'analyse de protocoles : Snort inspecte le trafic réseau pour identifier les protocoles utilisés et les anomalies potentiels
- la détection basée sur les signatures : il compare le trafic réseau aux signatures connues d'attaques pour détecter les menaces
- la prévention en temps réel : Snort peut bloquer le trafic réseau suspect automatiquement empêchant ainsi les intrusions avant qu'elles ne se produisent

Pour une configuration avancée il est possible de :

- personnaliser les règles de détection selon les besoins spécifiques du réseau. Cela permet d'améliorer les précisions
- utiliser des outils complémentaires (ex : Barnyard2) pour améliorer la gestion des logs et l'analyse des données

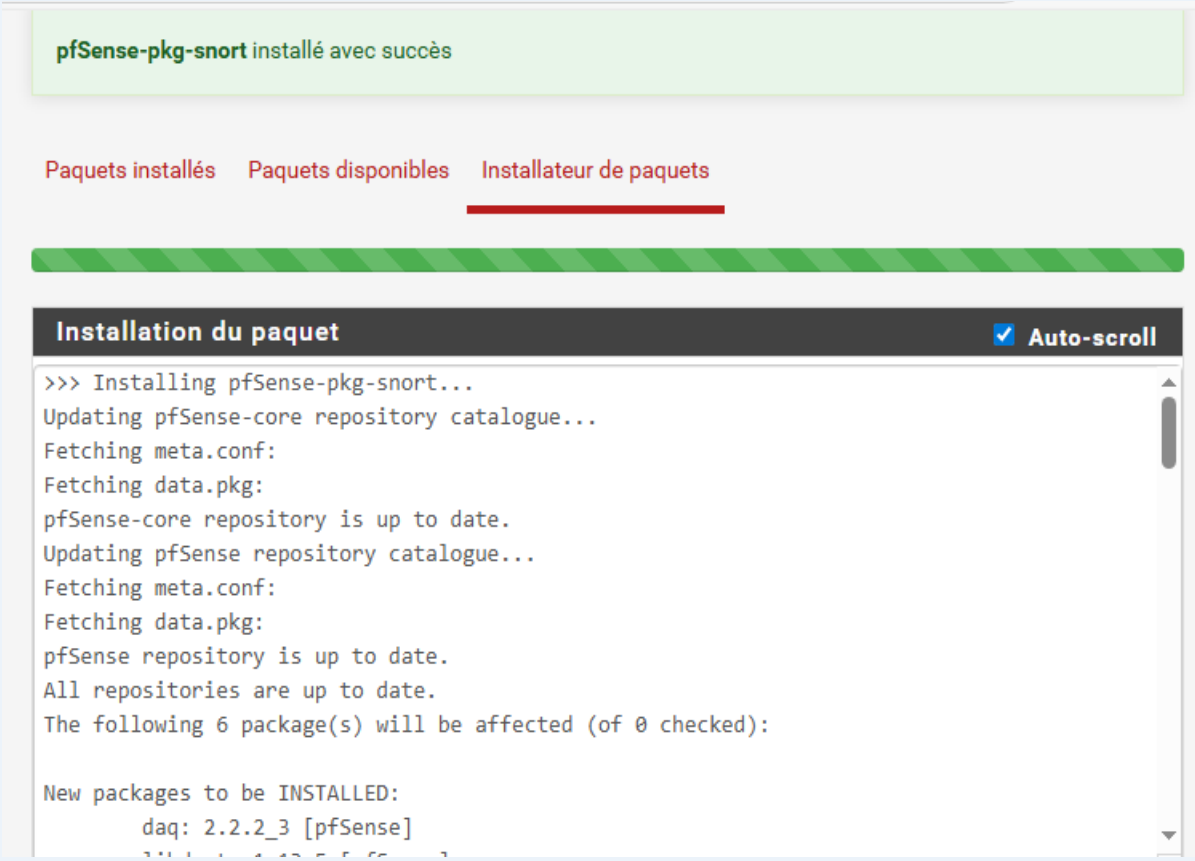
## Étape 1 : Installer SNORT

Sur pfSense, dans l'onglet système, aller dans gestionnaire de paquets.




Rechercher **Snort** et **installer**


Système / Gestionnaire de paquets / Paquets disponibles
Paquets installés
Paquets disponibles
Recherche
Terme de recherche
snort
Les deux
Recherche
Effacer
Entrer une phrase de recherche ou une expression régulière *nix pour rechercher dans les noms et description de paquets.
Paquets
Nom
Version
Description
snort
4.1.6_28
Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.
Install
Dépendances du paquet:
snort-2.9.20_8


pfSense-pkg-snort installé avec succès
Paquets installés
Paquets disponibles
Installateur de paquets
Installation du paquet
Auto-scroll
>>> Installing pfSense-pkg-snort...
Updating pfSense-core repository catalogue...
Fetching meta.conf:
Fetching data.pkg:
pfSense-core repository is up to date.
Updating pfSense repository catalogue...
Fetching meta.conf:
Fetching data.pkg:
pfSense repository is up to date.
All repositories are up to date.
The following 6 package(s) will be affected (of 0 checked):
New packages to be INSTALLED:
daq: 2.2.2_3 [pfSense]

> Après avoir installer, aller dans paquets disponibles > installeurs de paquets > confirmer

## Étape 2 : règles par défaut

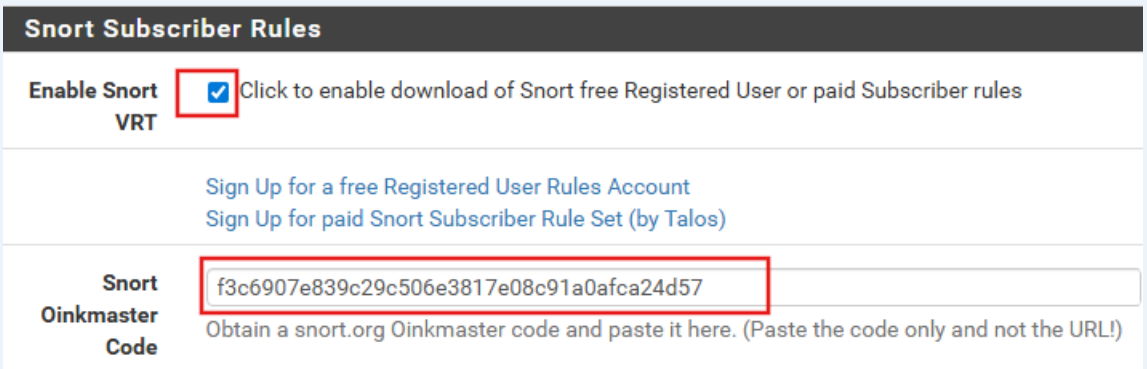
> Aller dans l'onglet services > Snort > global settings

Dans la section « snort subscriber rules » cocher la règle « VRT » + mettre le code Oinkmaster

Règles VRT (vulnerability Research Team) : règles « officielles » de snort, basées sur des recherches de vulnérabilités réelles et régulièrement mises à jour.

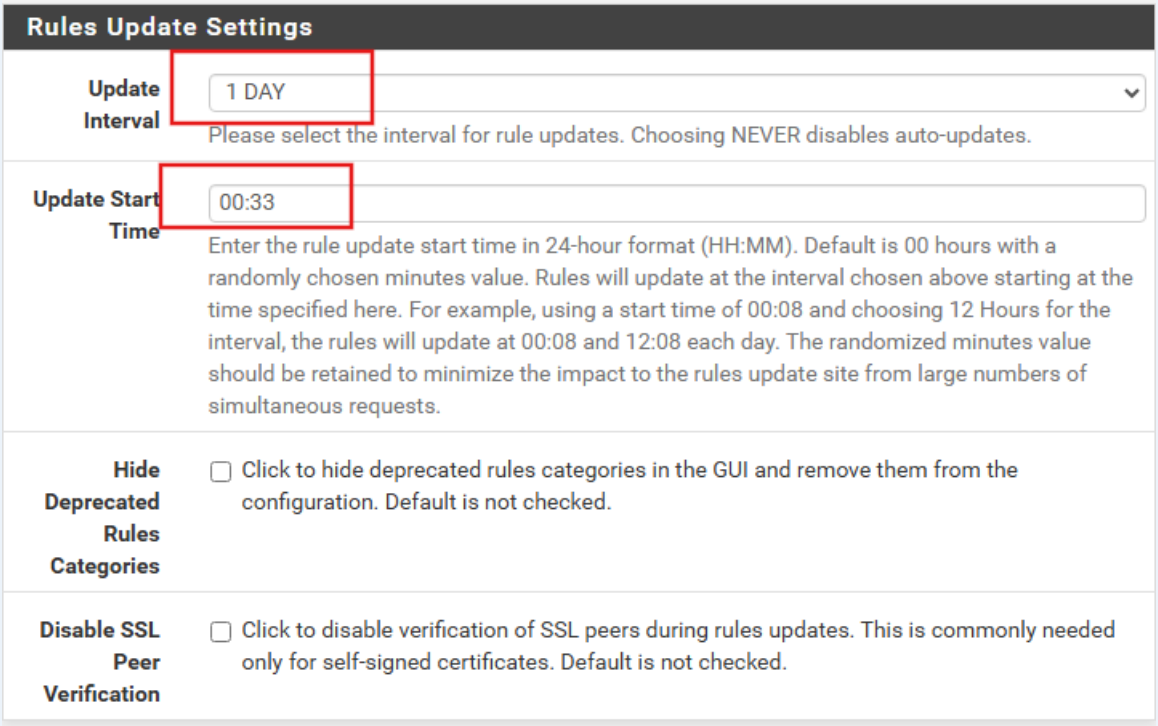
Elles détectent :

- Exploits connus
- Tentatives d'intrusion
- Malware
- Commandes et contrôle
- Scan réseau
- Attaques Web
- Attaques sur services




**Pour trouve le code, aller sur snort.org et créer un compte . Une fois le compte créer le code se trouvera dans l'onglet « oinkcode »**

Dans la section « rules update setting » > sélectionner l'intervalle souhaité dans « update interval ». Ensuite dans « update start time », choisir l'heure de la mise à jour.

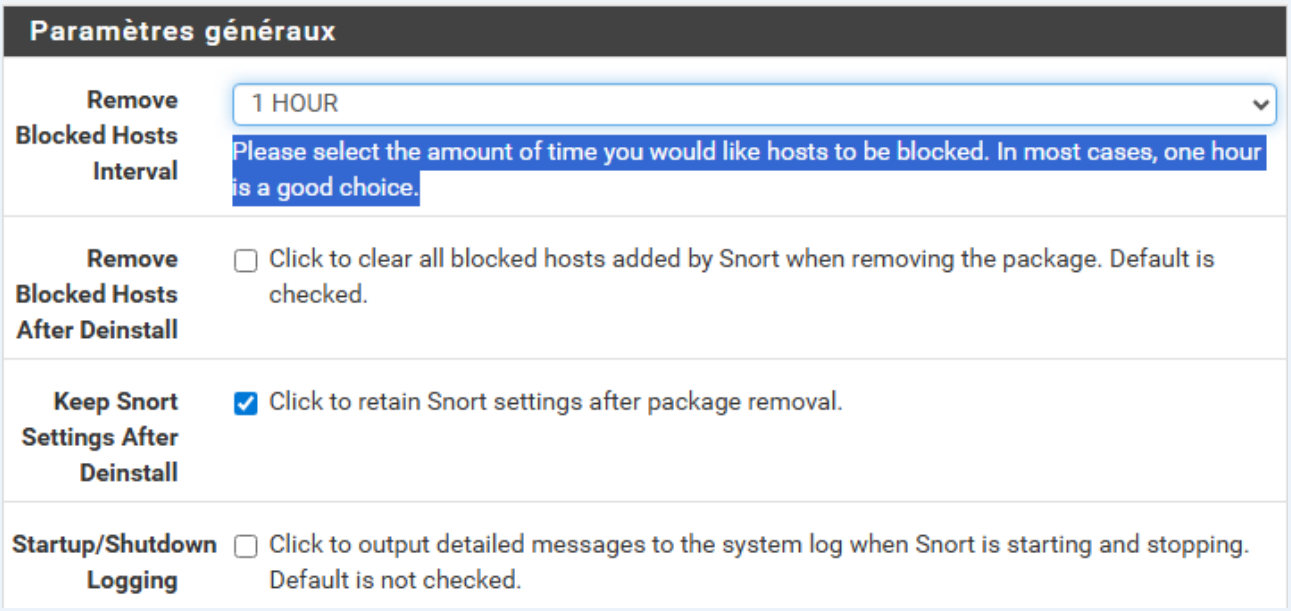



Dans « supprimer les intervalles des hôtes bloqués » : 1h (choix le plus souvent)

Dans « supprimer les hôtes bloqués après la désinstallation » : NON

Dans « conserver les paramètres snort après la désinstallation » : OUI

Dans « intervalles de mises à jour de démarrage / shutdown » : NON

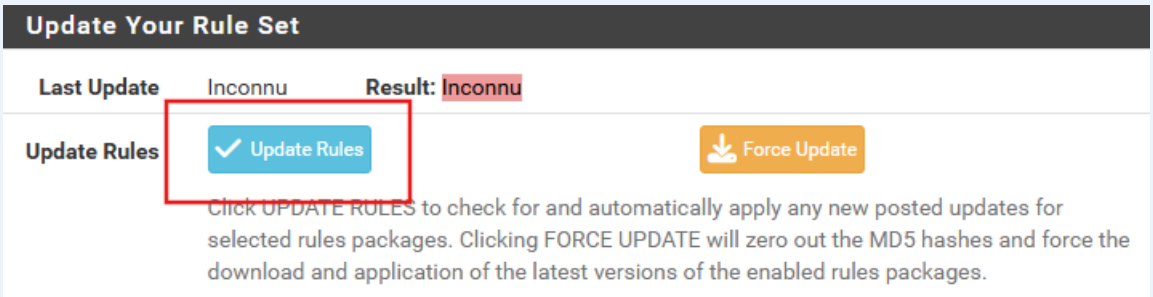


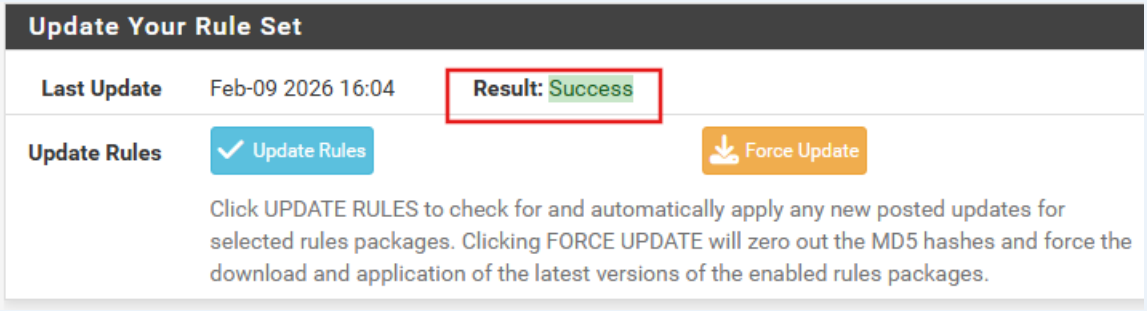

Cliquer sur « **Enregistrer** »

## Étape 3 : MAJ

Aller dans l'onglet « Mises à jour »

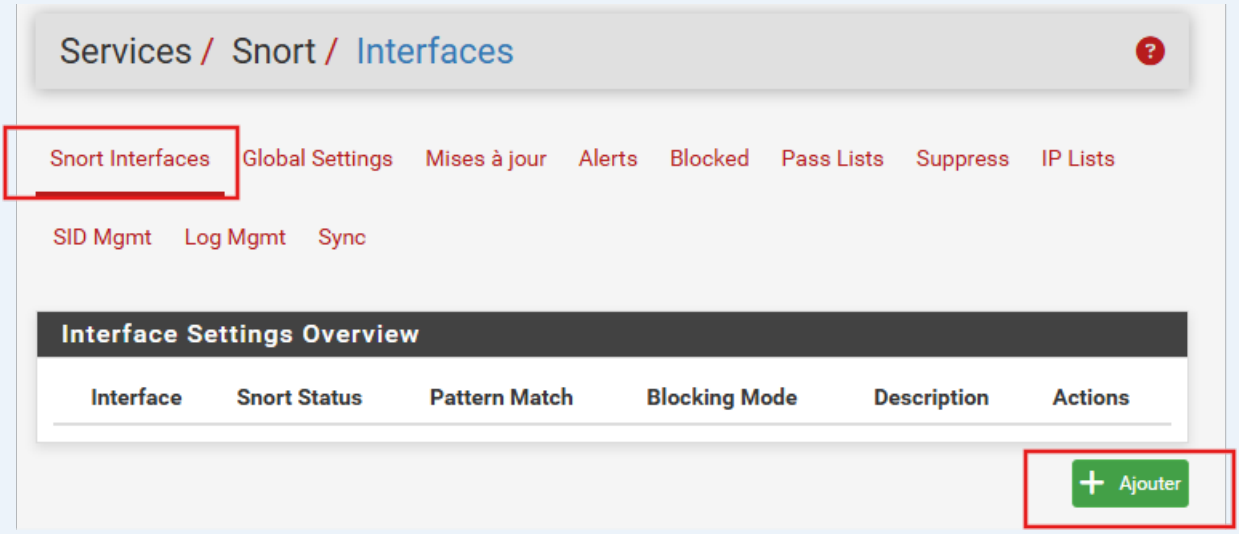
Dans « Update your rule set » , cliquer sur Update rules

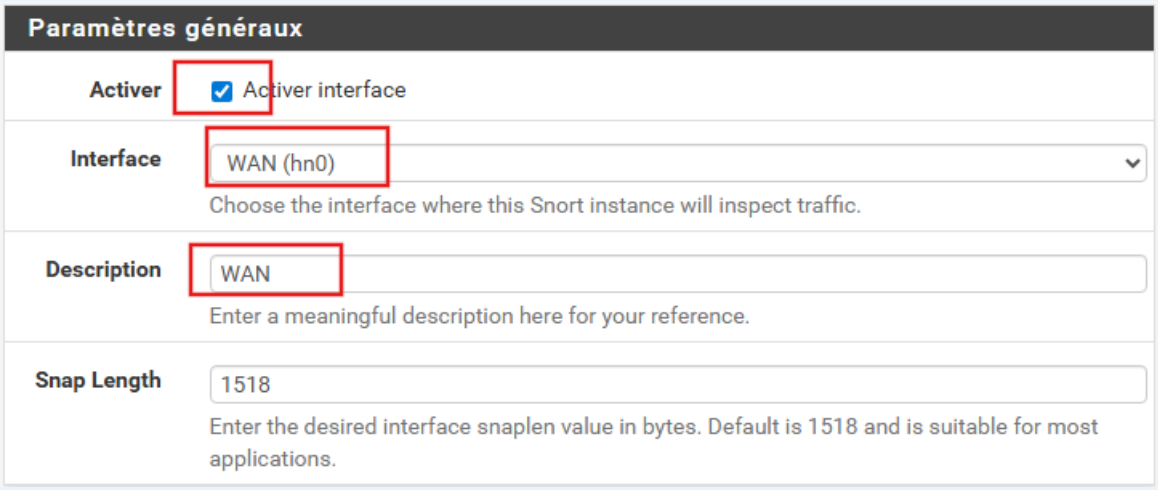





## Étape 4 : Interface

Dans l'onglet services, aller dans Snort puis dans « interfaces » > ajouter > sélectionner l'interface désirée pour surveiller

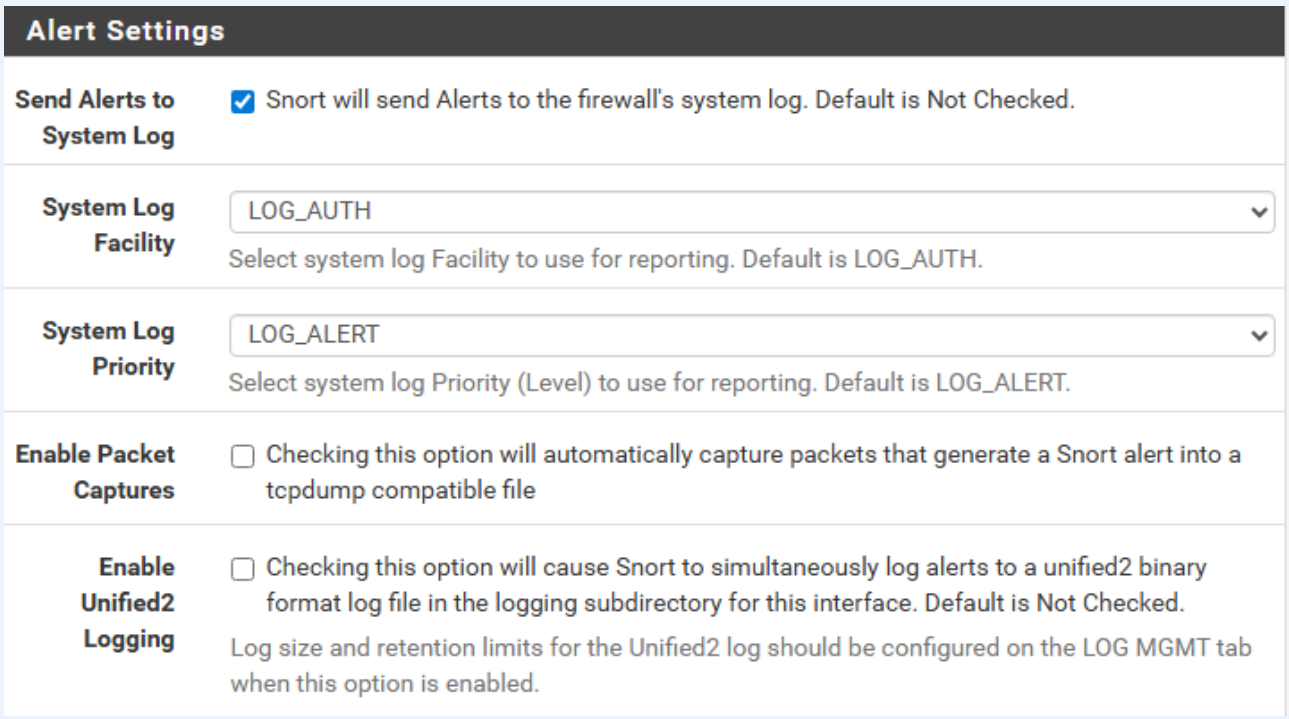





Dans la zone d'alerte :

« Envoyer les alertes au journal du système » : cocher OUI

« Bloquer automatiquement les hôtes qui génèrent une alerte Snort ». Par défaut, elle n'est pas cochée, ici cocher OUI



### Block Settings

Activer « block offenders » sur l'interface WAN. Cela bloquera les IP qui généreront une alerte.

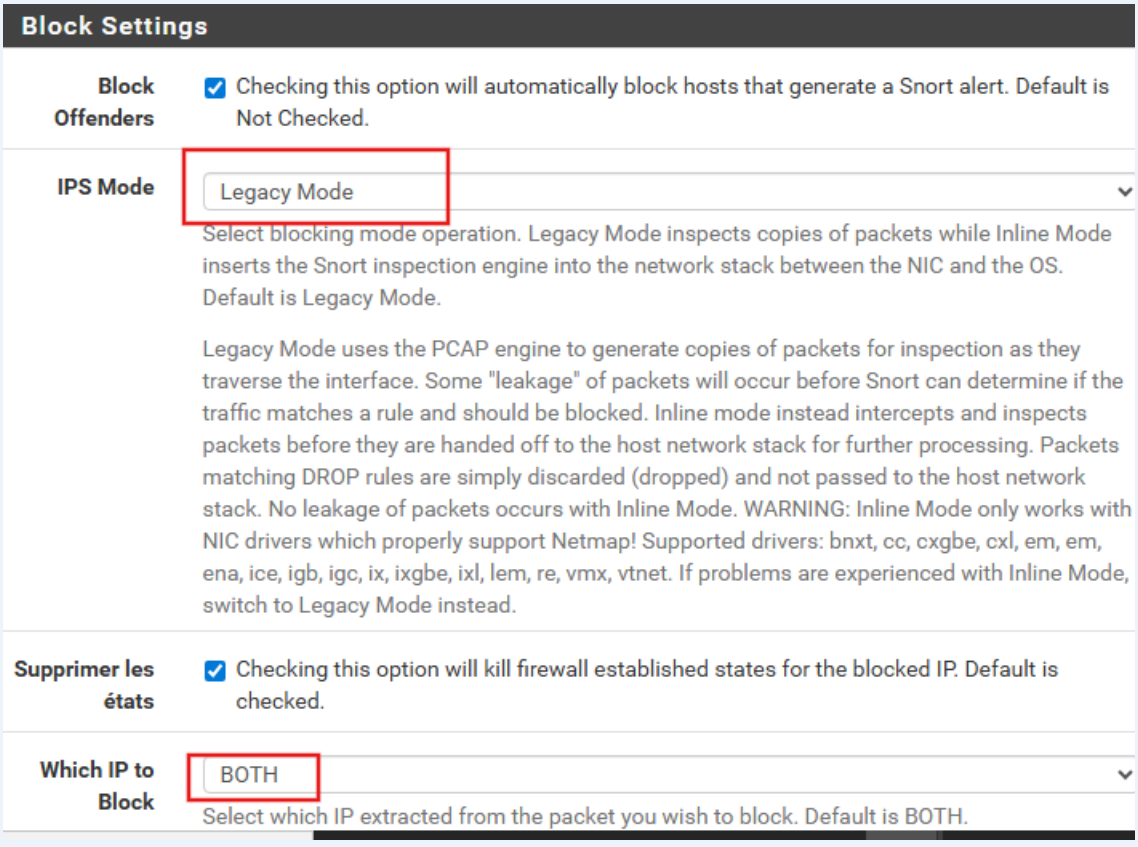
IPS mode : mode de blocage.

LEGACY MODE :

- obsolète
- utilise l'ancien système de blocage basé sur les tables ip (snort2) donc contournable
- une attaque peut passer une première fois avant blocage
- maintenu pour compatibilité
- plus recommandé pour les nouvelles installations

INLINE IPS :

- la paquet est analysé avant d'être accepté par le pare feu → si malveillant = bloqué automatiquement
- pas de blocage de table temporaire
- plus efficace contre attaques dynamiques.
- analyse en temps réel, plus moderne et plus fiable



> **Enregistrer**

On peut voir un menu spécial pour l'interface WAN apparaître.

Dans « WAN-catégories » :

> « Résoudre les débits » : OUI

> « Utiliser la politique IPS » : OUI

> « Sélection des politiques IPS » : Connectivité

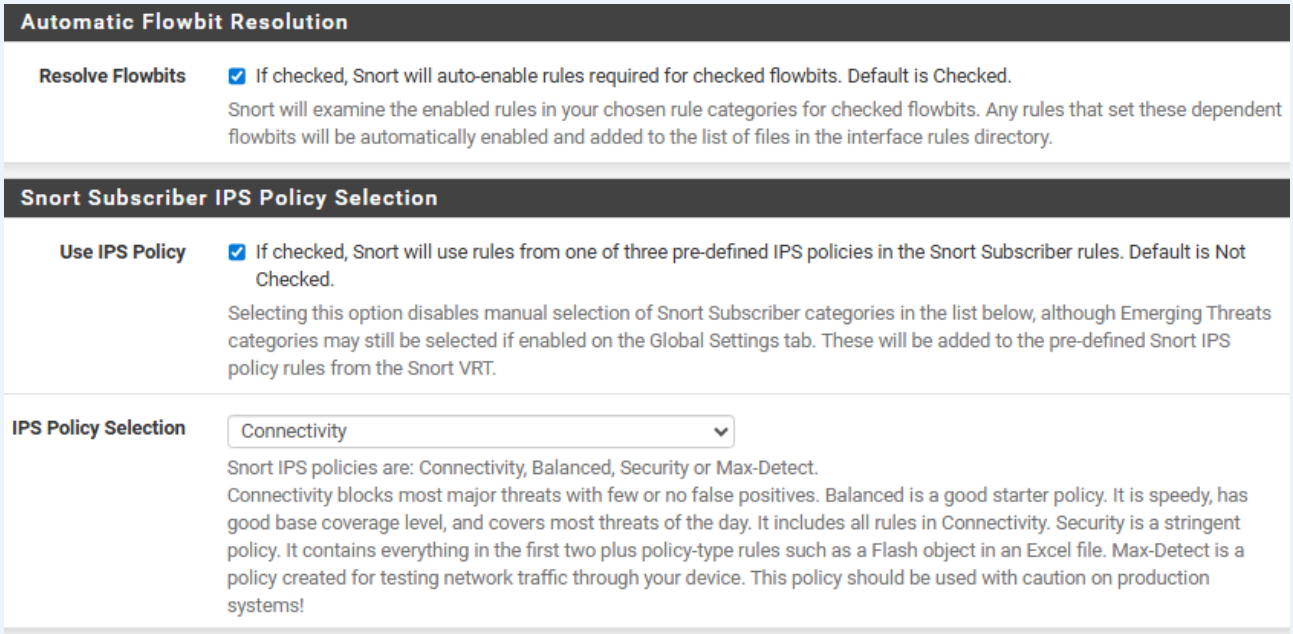
Les différentes politiques de Snort sont :

- Connectivité : permet de bloquer la plupart des menaces majeures avec peu ou pas de faux positifs

- Équilibrée : c'est une bonne politique de départ. Elle offre un bon niveau de couverture de base et couvre la plupart des menaces actuelles. Elle inclut toutes les règles de connectivité

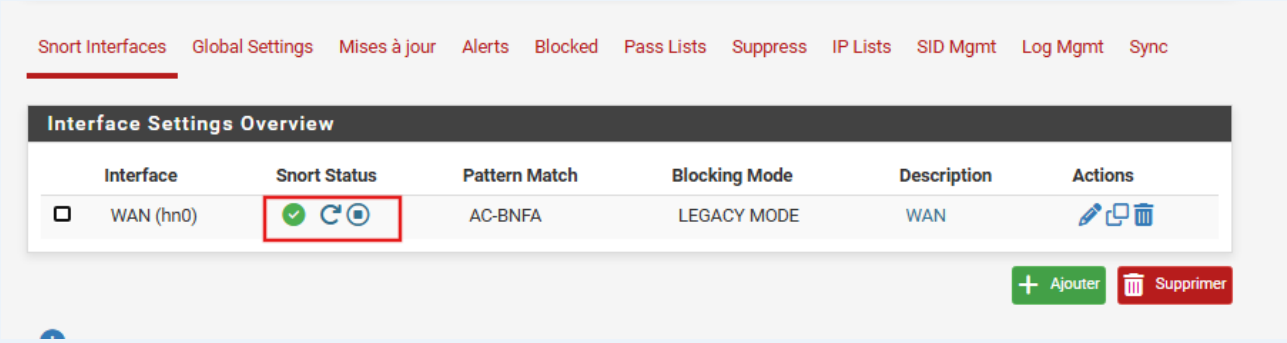
- Sécurité : c'est une politique stricte. Contient tout ce qu'il y a dans les deux premières politiques ainsi que des règles de type politique comme un objet flash dans un fichier excel

-Max-détection : c'est une politique créée pour tester le trafic réseau à travers l'appareil local. Cette politique doit être utilisée avec prudence dans les systèmes de production



Une fois les configurations terminées, revenir sur l'accueil des interfaces > et démarrer le service de l'interface

## Étape 5 : Activer l'interface




## Étape 6 : Créer des règles

Pass list

mettre :

- IP de l'AD : 192.168.26.2
- IP du RDS : 192.168.26.X
- IP du serveur de fichiers : 192.168.26.X
- passerelle du routeur (LAN) : 192.168.26.254
- localhost : 127.0.0.1

Pourquoi ? Pour ne pas que snort bloque le DC sinon :

- plus d'authentification
- plus de DNS interne
- plus de GPO
- RDS peut tomber

Ne pas mettre tout le LAN sinon le IDS devient inutile pour la détection latérale

## Étape 7 : Activer des modes