



Sommaire

SNORT.....	1
Introduction	3
Étape 1 : Installer SNORT.....	3
Étape 2 : règles par défaut.....	6
Étape 3 : MAJ.....	8
Étape 4 : Interface.....	8
Étape 5 : Activer l'interface.....	11
Étape 6 : Créer des règles.....	11
Étape 7 : Activer des modes.....	12

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 :

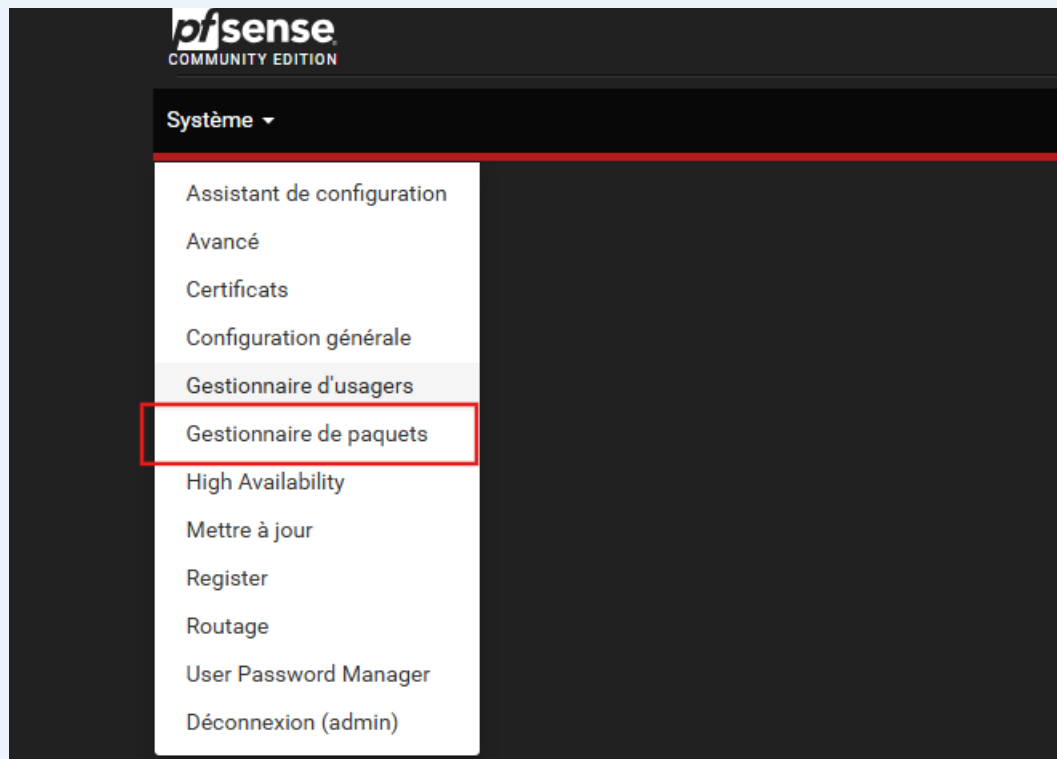
- l'analyse de protocoles : Snort inspecte le trafic réseau pour identifier les protocoles utilisés et les anomalies potentiels
- la détection basée sur les signatures : il compare le trafic réseau aux signatures connues d'attaques pour détecter les menaces
- la prévention en temps réel : Snort peut 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**



Paquets installés Paquets disponibles

Recherche

Terme de recherche

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 Installeur 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

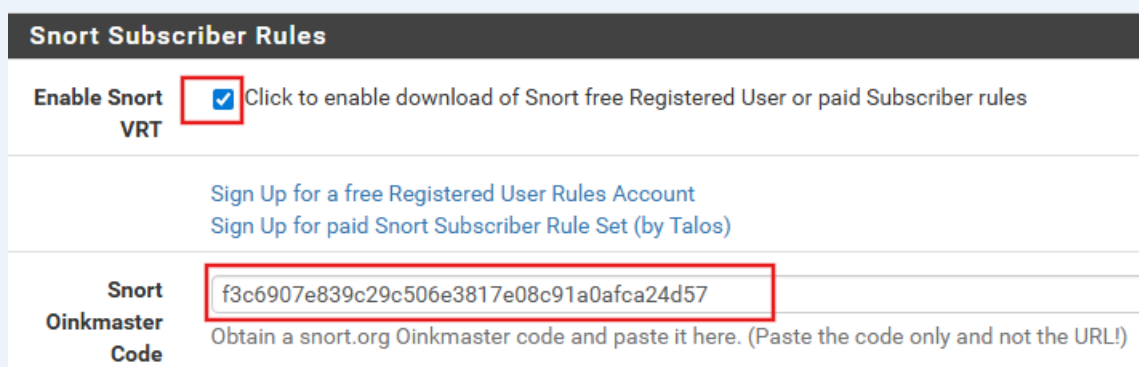
> Aller dans l'onglet [services](#) > [Snort](#) > [global settings](#)

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



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!)

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.

Rules Update Settings	
Update Interval	<input type="text" value="1 DAY"/> Please select the interval for rule updates. Choosing NEVER disables auto-updates.
Update Start Time	<input type="text" value="00:33"/> 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	<input type="checkbox"/> Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.
Disable SSL Peer Verification	<input type="checkbox"/> Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.

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

Paramètres généraux	
Remove Blocked Hosts Interval	<div style="border: 1px solid #ccc; padding: 2px;">1 HOUR</div> <div style="font-size: 0.8em; color: #0056b3; background-color: #e6f2ff; padding: 2px;">Please select the amount of time you would like hosts to be blocked. In most cases, one hour is a good choice.</div>
Remove Blocked Hosts After Deinstall	<input type="checkbox"/> Click to clear all blocked hosts added by Snort when removing the package. Default is checked.
Keep Snort Settings After Deinstall	<input checked="" type="checkbox"/> Click to retain Snort settings after package removal.
Startup/Shutdown Logging	<input type="checkbox"/> Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.

Cliquer sur « [Enregistrer](#) »

Étape 3 : MAJ

Aller dans l'onglet « [Mises à jour](#) »

Dans « [Update your rule set](#) », cliquer sur [Update rules](#)

Update Your Rule Set	
Last Update	Inconnu Result: Inconnu
Update Rules	<div style="display: flex; justify-content: space-between; align-items: center;"> <div style="border: 2px solid red; padding: 5px;"> <input checked="" type="button" value="Update Rules"/> </div> <div> <input type="button" value="Force Update"/> </div> </div> <p style="font-size: 0.8em; color: #0056b3;">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.</p>

Update Your Rule Set

Last Update Feb-09 2026 16:04 **Result: Success**

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.

Étape 4 : Interface

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

Services / Snort / Interfaces ?

Snort Interfaces Global Settings Mises à jour 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="button" value="+ Ajouter"/>					

Paramètres généraux	
Activer	<input checked="" type="checkbox"/> Activer interface
Interface	<input type="text" value="WAN (hn0)"/> Choose the interface where this Snort instance will inspect traffic.
Description	<input type="text" value="WAN"/> Enter a meaningful description here for your reference.
Snap Length	<input type="text" value="1518"/> Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

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

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"/> Select system log Facility to use for reporting. Default is LOG_AUTH.
System Log Priority	<input type="text" value="LOG_ALERT"/> Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.
Enable Packet Captures	<input type="checkbox"/> Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file
Enable Unified2 Logging	<input type="checkbox"/> Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked. Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

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

Block Settings	
Block Offenders	<input checked="" type="checkbox"/> Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.
IPS Mode	<div style="border: 1px solid red; padding: 2px;">Legacy Mode</div> <p>Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.</p> <p>Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Snort can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers: bnxt, cc, cxgbe, cxl, em, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.</p>
Supprimer les états	<input checked="" type="checkbox"/> Checking this option will kill firewall established states for the blocked IP. Default is checked.
Which IP to Block	<div style="border: 1px solid red; padding: 2px;">BOTH</div> <p>Select which IP extracted from the packet you wish to block. Default is BOTH.</p>

> 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

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.

Snort Subscriber IPS Policy Selection

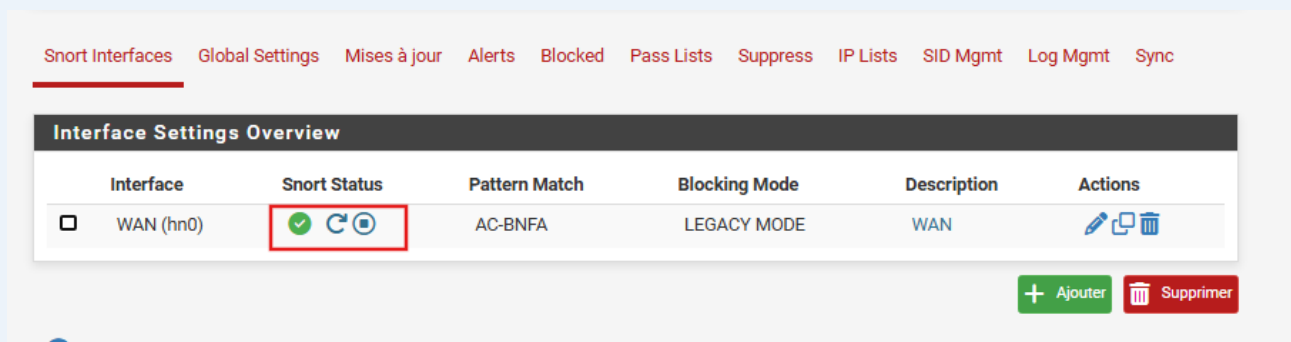
Use IPS Policy If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked.
Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected 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

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!

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

