22/01/2024

Procédure SNORT

Sommaire

Table des matières

Table des illustrations

1- Introduction

Cette procédure explique comment paramétrer SNORT sur pfSense.

Snort est un système de détection d'intrusion et de prévention d'intrusion gratuit et open-source créé en 1998 par Martin Roesch. Développé à l'origine par la société Sourcefire, il est aujourd'hui maintenu par Cisco Systems à la suite du rachat de Sourcefire en 2013.

1.1– Schéma

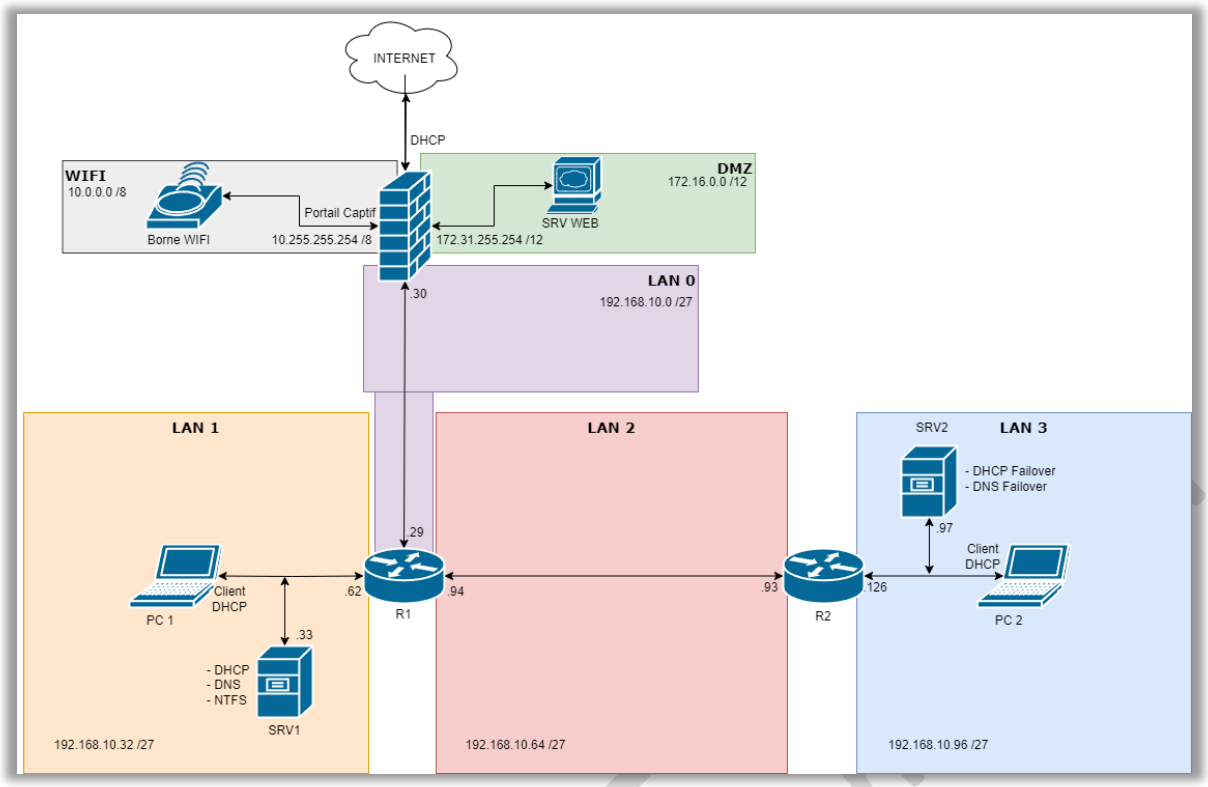
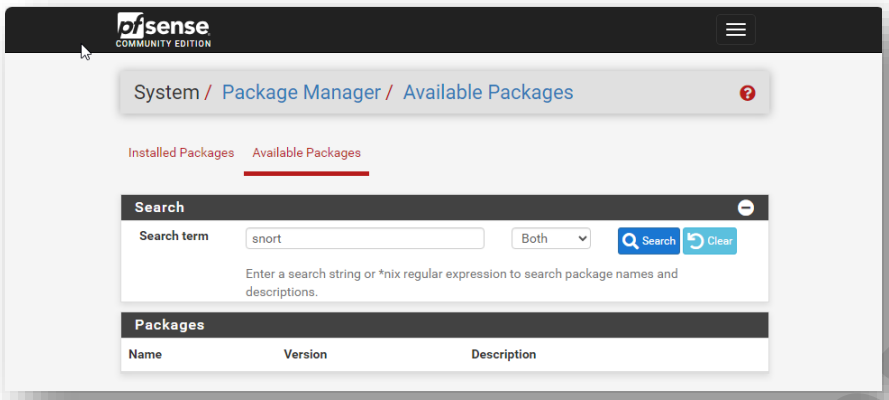


Figure 1 - Schéma réseau

2. Installation de SNORT su PfSense

2.1- Installer SNORT dans : System / Packet Manager / Available Packages

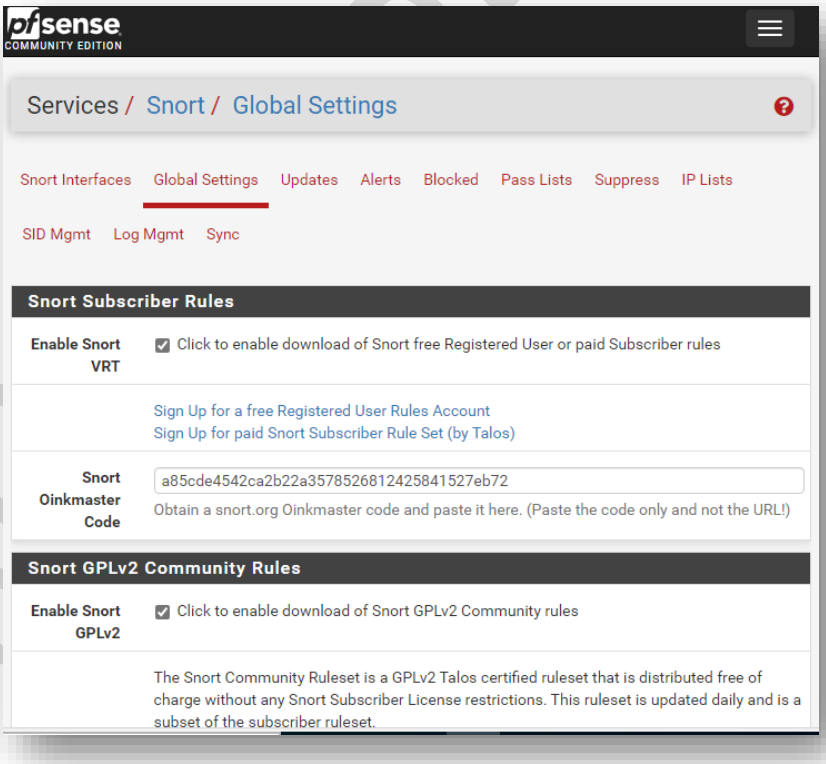
On clique ensuite sur **Install** puis **Confirm** et l'installation se lance !



3. configuration de SNORT su PfSense

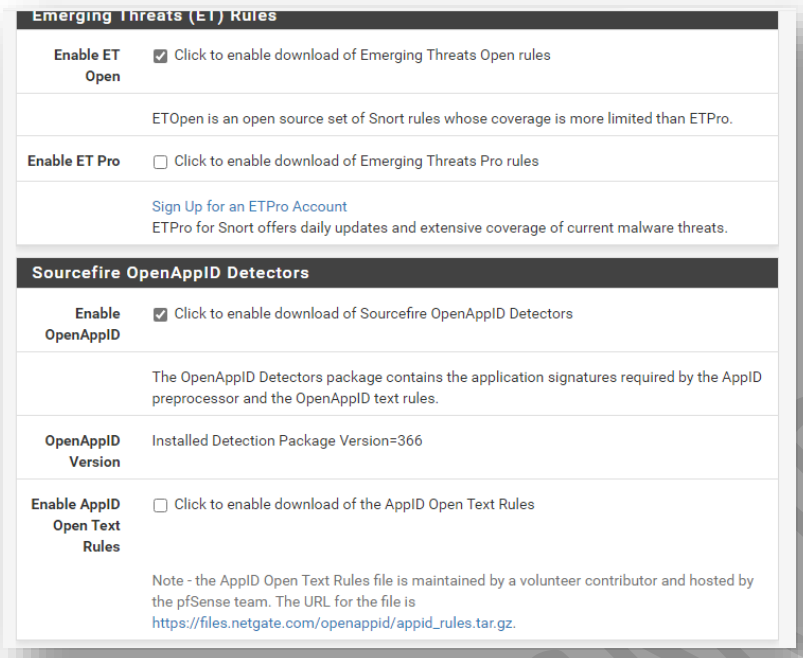
3.1- Une fois installé, Snort apparaîtra dans l'onglet **Services**. Une fois rendu dessus, nous allons dans un premier temps aller sur l'onglet **Global Settings** :

2.2- La première étape est donc 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 Sort.

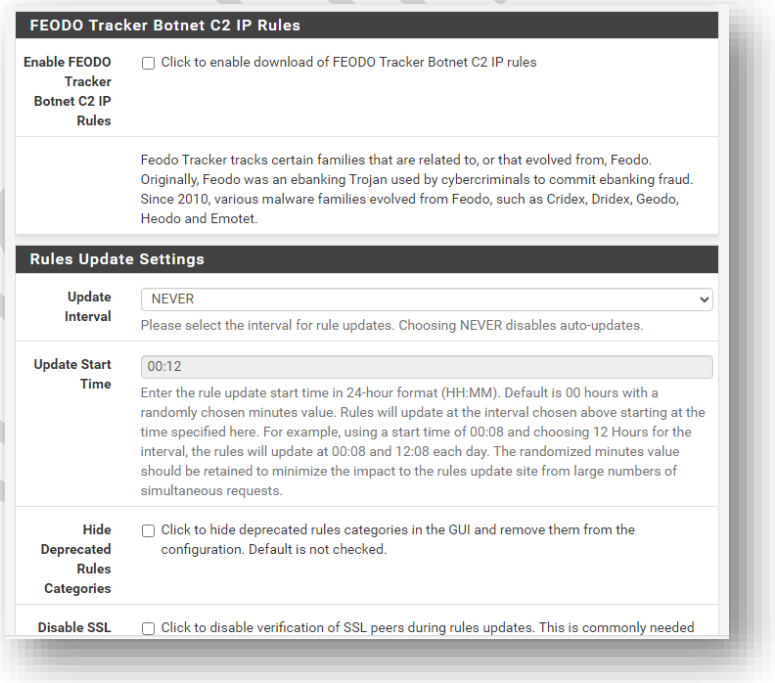


2.4- Et ensuite nous pouvons cocher les cases :

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



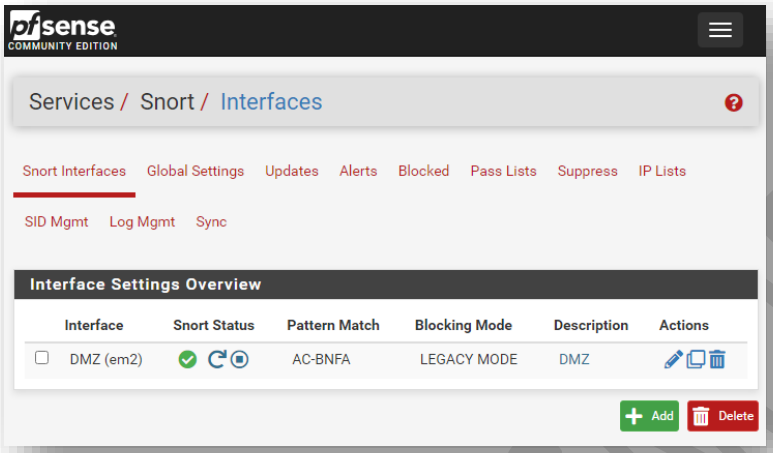
2.5- Et ensuite, pour les derniers paramètres il convient simplement de configurer l'update pour les différentes règles, c'est-à-dire le délai avant de vérifier les mises à jour pour les différentes règles ou pour de nouvelles : 12H est suffisant, mais en entreprise il conviendra de mettre 6H par précaution. Et pour l'heure de début de vérification pour les updates, j'ai choisi 01:00 (à vous de choisir l'heure qui vous convient).



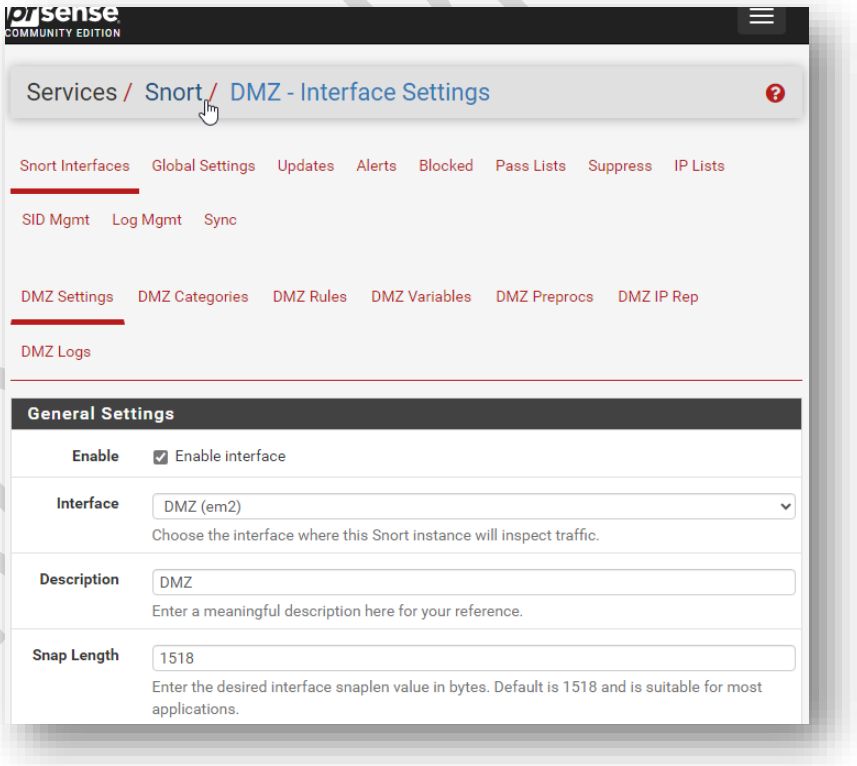
3.6- Une fois cliqué sur **Save**, nous pouvons nous rendre sur l'onglet **Updates** et manuellement mettre à jour les différentes règles que nous avons cochées juste avant (ici cela prendra un peu plus de temps, car nous allons toutes les télécharger une première fois, forcément) :

4. Configuration de l'interface

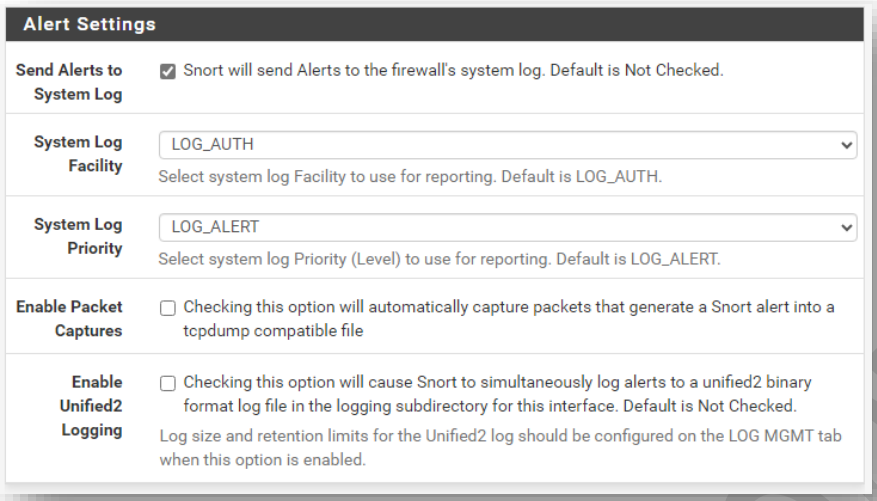
4.1- Une fois la mise à jour terminé, nous approchons de la fin ! Rendons-nous donc sur **Snort interfaces** pour choisir l'interface (ou les interfaces) sur laquelle Snort va écouter et analyser le trafic :

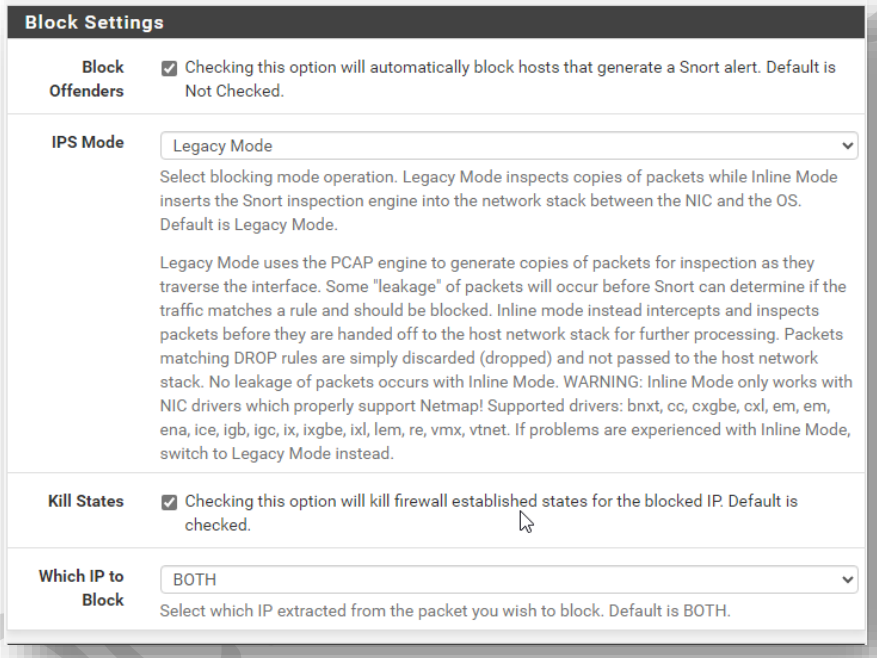


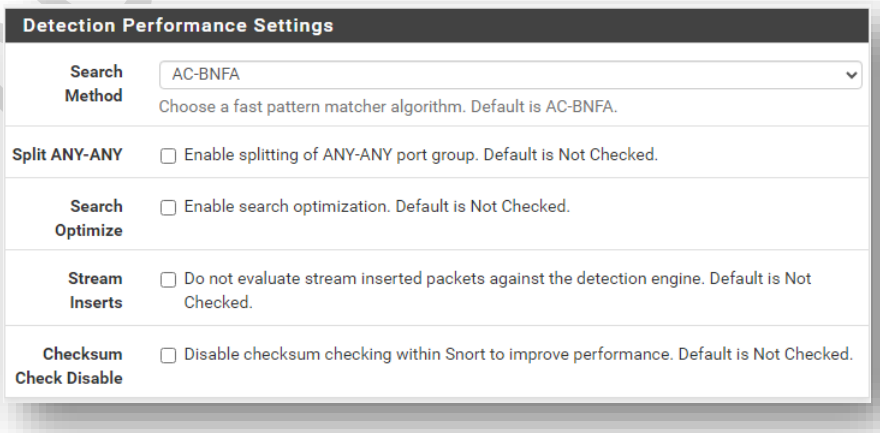
4.2- Ici nous choisissons donc l'interface de notre choix (DMZ ici), puis une courte description, et ensuite nous cochons simplement le fait d'envoyer les alertes sur le système de log interne, ce qui est toujours bien.

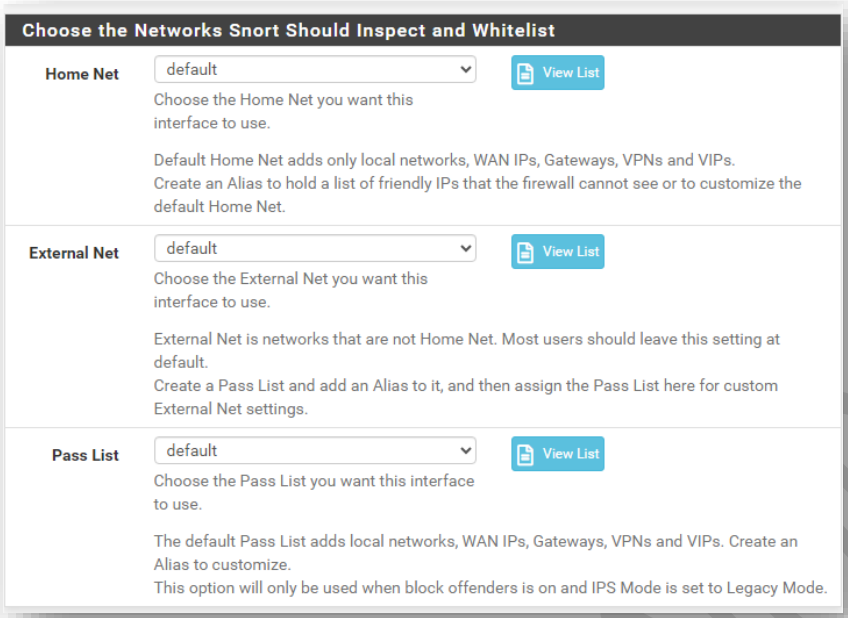


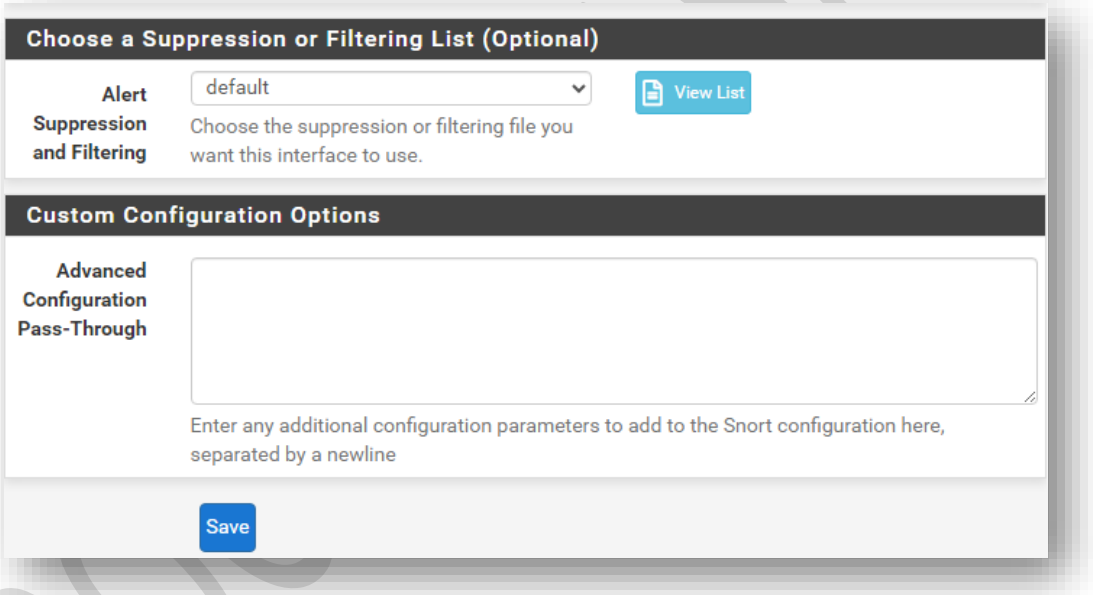
4.3- A noter qu'ici, nous pouvons justement faire **de Snort un IPS**, en cochant la case **Block Offenders** :


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.
System Log Priority
LOG_ALERT
Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.
Enable Packet Captures
Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file
Enable Unified2 Logging
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
Block Offenders
Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.
IPS Mode
Legacy Mode
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.
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.
Kill States
Checking this option will kill firewall established states for the blocked IP. Default is checked.
Which IP to Block
BOTH
Select which IP extracted from the packet you wish to block. Default is BOTH.


Detection Performance Settings
Search Method
AC-BNFA
Choose a fast pattern matcher algorithm. Default is AC-BNFA.
Split ANY-ANY
Enable splitting of ANY-ANY port group. Default is Not Checked.
Search Optimize
Enable search optimization. Default is Not Checked.
Stream Inserts
Do not evaluate stream inserted packets against the detection engine. Default is Not Checked.
Checksum Check Disable
Disable checksum checking within Snort to improve performance. Default is Not Checked.





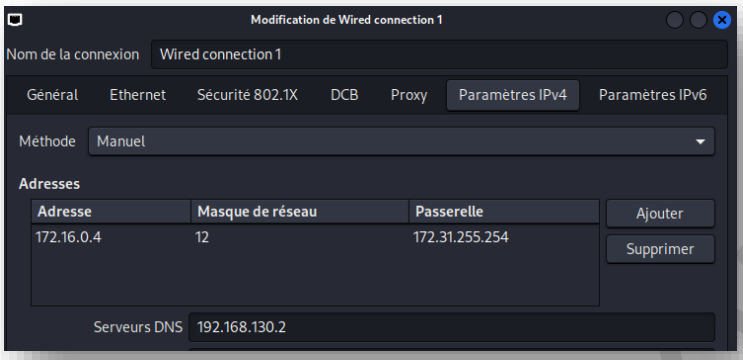
On valide et le tour est joué !

4.4- L'avant dernière étape est d'activer toutes les règles précédemment téléchargées en nous rendant dans **LAN Categories**, sur **Snort Interfaces**, **LAN** en cochant l'option **Use IPS Policy** :

4.5- On valide donc le tout, et on retourne à la liste des interfaces de Snort pour cliquer sur **Start** :

5. Vérification avec KALI

5.1- Installer KALI, configurer l'interface DMZ



5.2- Dans le terminal, faire un nmap de la passerelle de la DMZ.

5.3- Dans l'interface du pare-feu, Services / Snort / Alerts. Les alertes s'affiches