Installation Suricata sur Pfsense

Introduction :

Pour assurer la sécurité d’un réseau, vous pouvez déployer des systèmes IDS ou IPS.

Il est recommandé de commencer par configurer un système en mode IDS avant de le transformer en système IPS. Activer Suricata en mode IPS dès le départ pourrait être déroutant. Il est conseillé d’observer d’abord ce qui se passe sur le réseau afin d’éviter de générer trop d’alertes et de blocages faux positifs.

IDS (Intrusion Detection System) et IPS (Intrusion Prevention System) sont des systèmes de sécurité réseau conçus pour détecter et gérer les menaces.

- **IDS (Système de Détection d'Intrusions)** : Il surveille le trafic réseau et signale les activités suspectes sans les bloquer. Il est principalement utilisé pour analyser et alerter en cas de tentative d'attaque.
- **IPS (Système de Prévention d'Intrusions)** : Il agit comme un IDS, mais en plus, il peut bloquer automatiquement les menaces détectées afin de protéger le réseau en temps réel.

Ces systèmes sont essentiels pour améliorer la sécurité en détectant ou empêchant les intrusions malveillantes avant qu'elles n'affectent les systèmes informatiques.

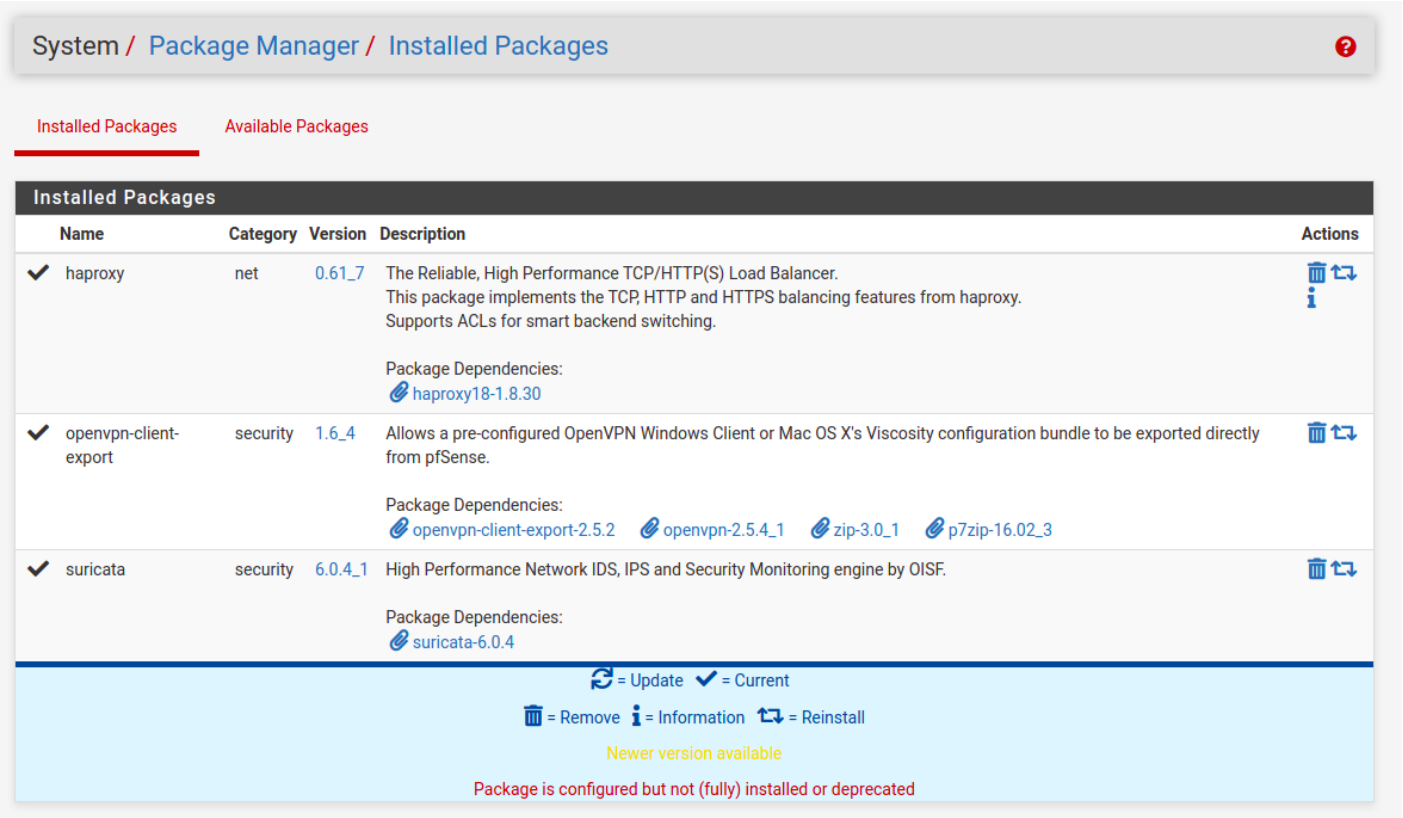
Installation et configuration de Suricata en mode IDS

Suricata, un système IDS/IPS, peut être installé en tant que package autonome sans pfSense, mais il est particulièrement utile lorsqu’il est utilisé avec une installation de pare-feu/routeur.

Installation sous pfSense

1. Accédez à System > Package Manager > Available Packages.
2. Recherchez Suricata dans la liste des paquets disponibles.
3. Cliquez sur Installer et attendez la fin du processus.

Une fois installé, Suricata peut être configuré en mode IDS pour détecter les menaces sans bloquer automatiquement le trafic.

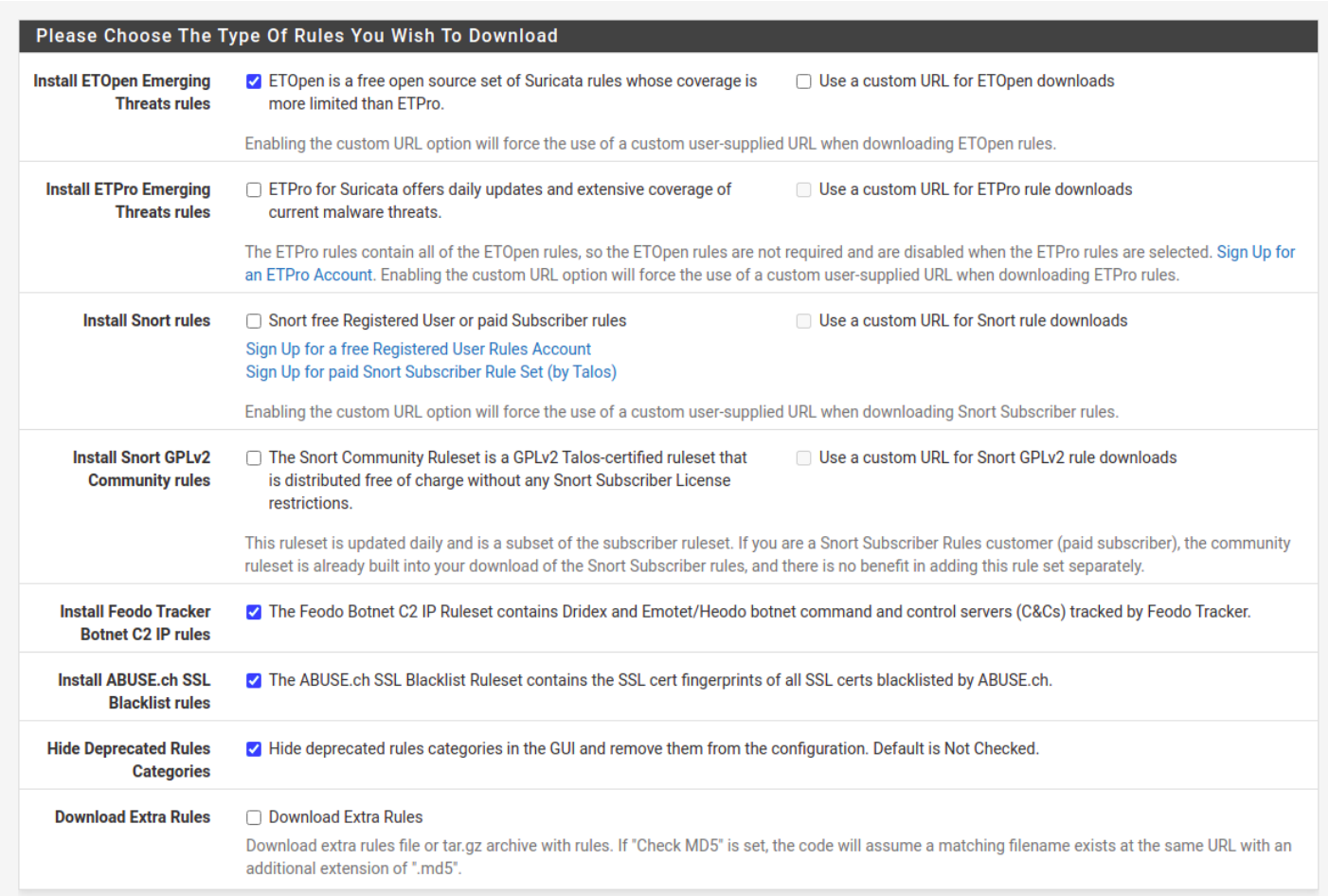


Après l'installation, la page de configuration de **Suricata** est accessible via le menu **Services**.

Configuration initiale

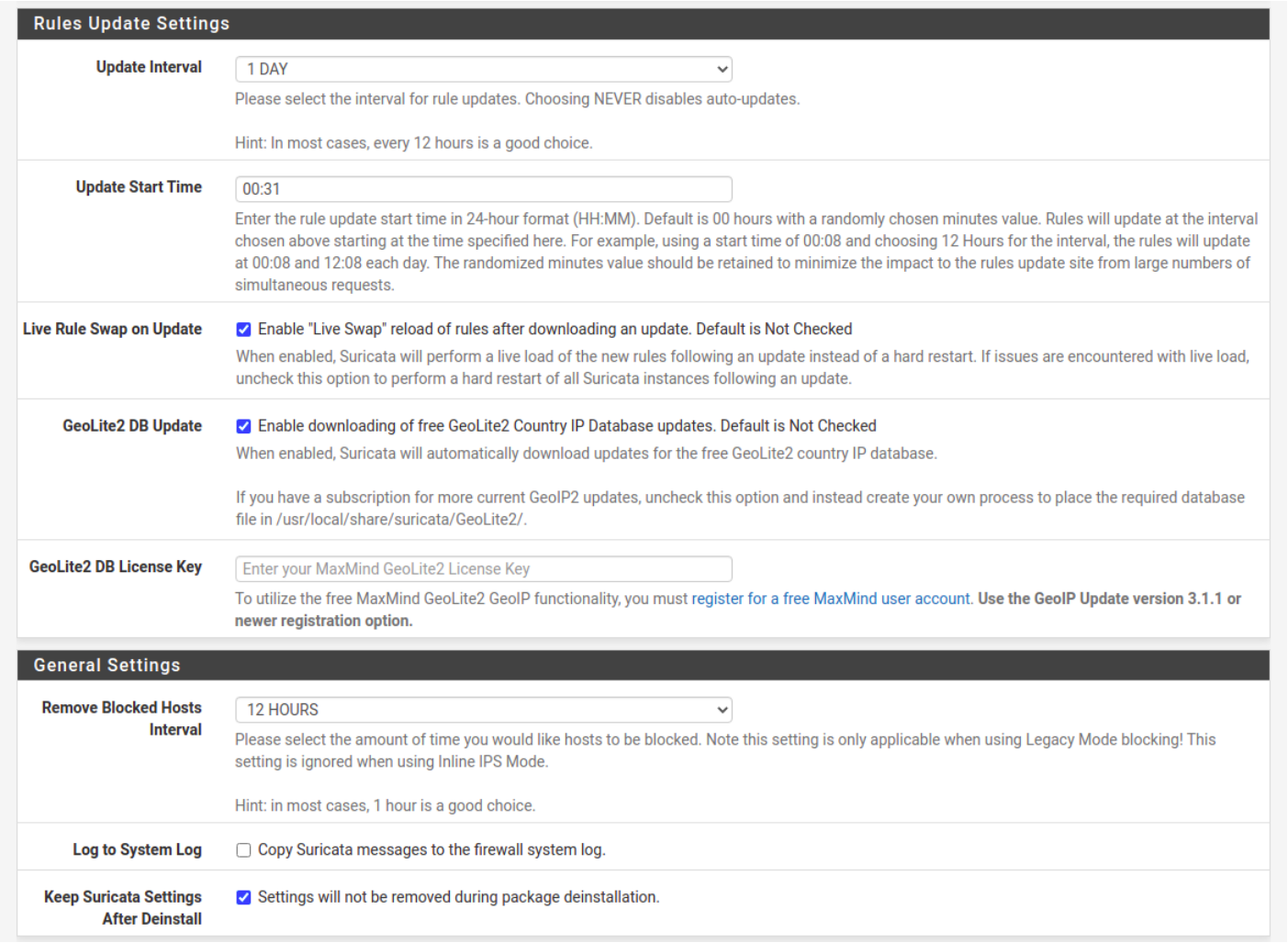
1. Accédez à **Services** > **Suricata**.
2. Commencez par les **Global Settings** (paramètres globaux).
3. Cochez les options suivantes :
   - ☑ **Install ETOpen Emerging Threats rules** (Installer les règles ETOpen Emerging Threats).
   - ☑ **Hide Deprecated Rules Categories** (Masquer les catégories de règles obsolètes).

Cela permet d'activer un ensemble de règles de détection des menaces et de masquer celles qui ne sont plus pertinentes.



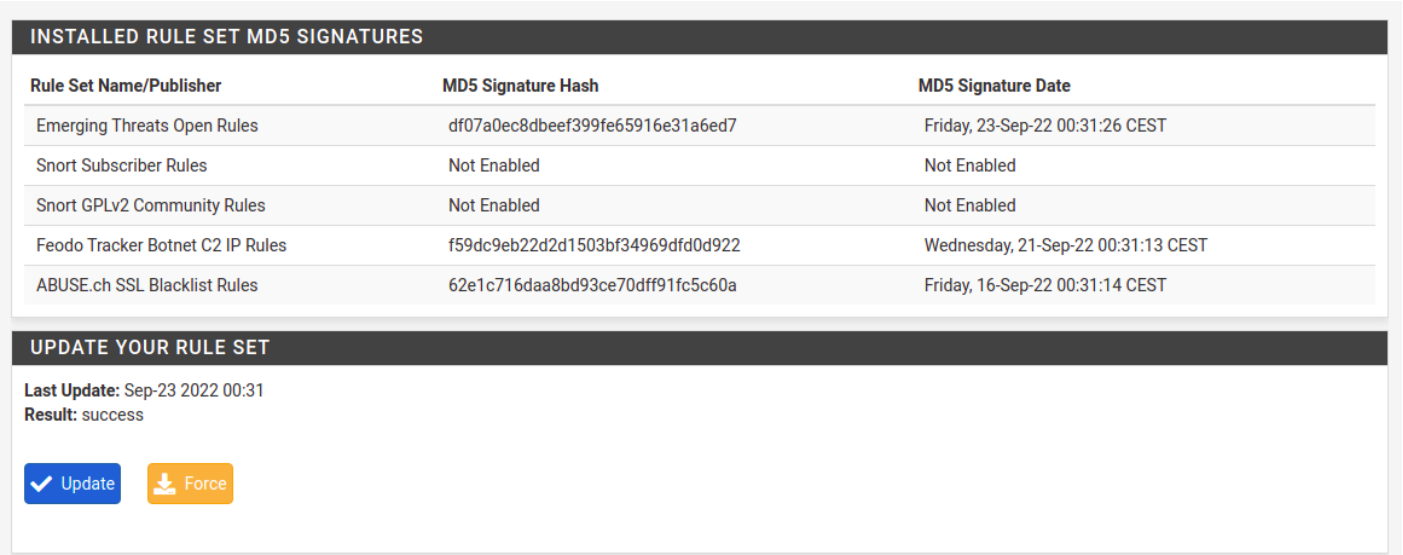
Ensuite, dans les paramètres globaux :

1. **Sélectionnez la fréquence de mise à jour** dans le menu déroulant **"Update Interval"** .
   - Je recommande de choisir **"1 DAY"** (1 jour) pour des mises à jour régulières des règles de détection.
2. **Activez l’option "Live Rule Swap on Update"** (Remplacement en direct des règles lors de la mise à jour).
   - Cette option permet de recharger les règles sans redémarrer complètement le service, évitant ainsi une interruption du trafic.



Pour **"Remove Blocked Hosts Interval"**, choisissez une durée entre **6 et 24 heures**, selon votre système. Même si vous ne démarrez pas en mode IPS, configurez cette option dès le début pour éviter d’avoir à y revenir plus tard.

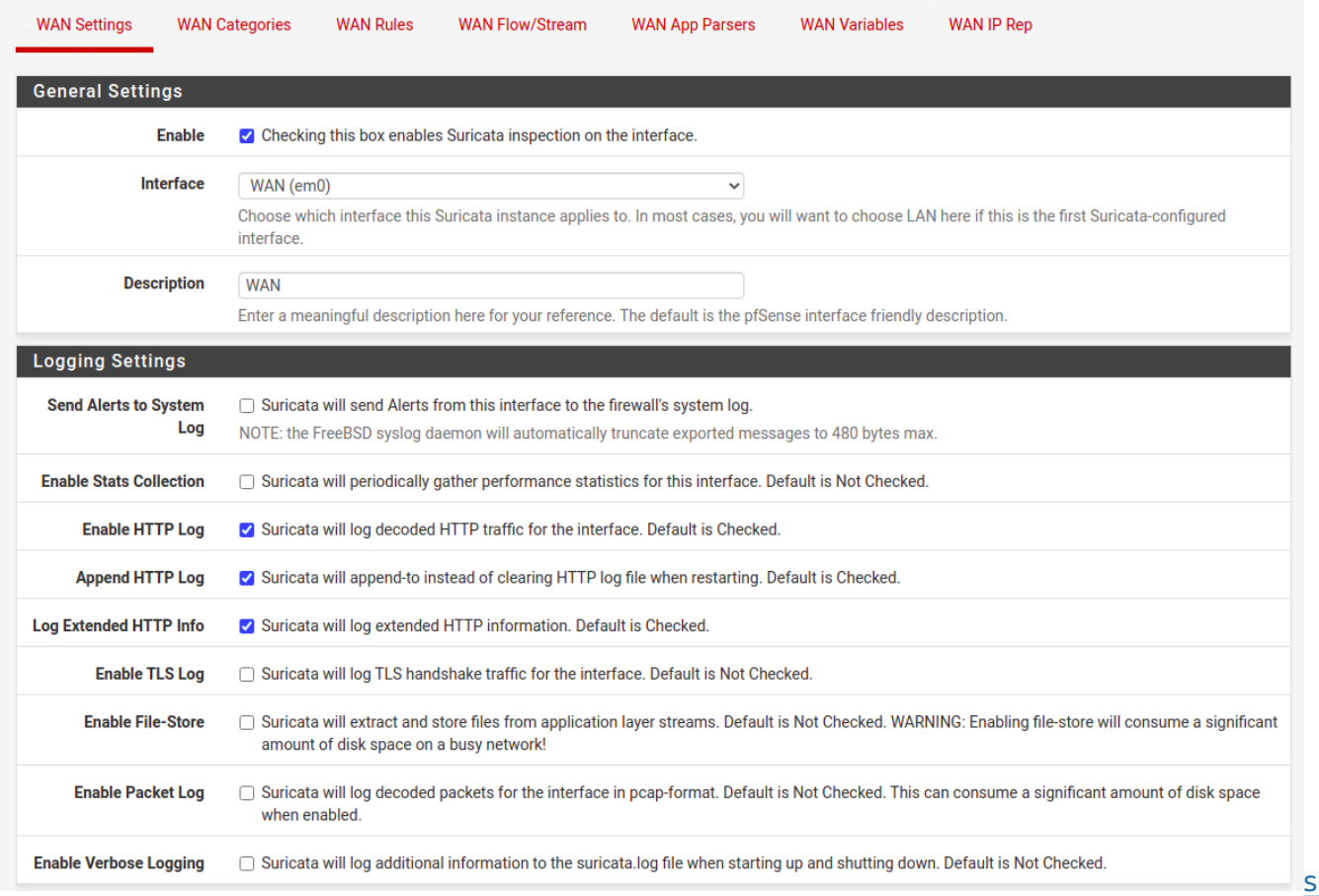
Ensuite, allez dans l’onglet **Updates** et forcez le téléchargement des règles. Cela ne se fait pas toujours automatiquement, donc dès que possible, cliquez sur **Update**.



⚠ Si tu rencontres des problèmes liés à des paquets obsolètes, la meilleure solution est de mettre à jour PfSense en premier.

Pour la configuration des interfaces :

1. Va dans l'onglet **Interfaces**.
2. Clique sur **Ajouter une interface**.
3. Active Suricata sur l'interface souhaitée.
4. Configure le mode d'inspection (mode en ligne ou mode hérité)



SS

Tu peux tester différentes options ici pour **TLS**, **file-store** et **packet log**.

À part **TLS**, les autres nécessitent beaucoup d'espace disque sur un réseau très actif. Pense donc à allouer suffisamment de stockage.

Il y a une autre chose à configurer dans cette section : le **Detect-Engine Profile**. Je recommande de le mettre sur **High** plutôt que le réglage par défaut **Medium**.

Pour l'instant, on ne bloque pas les attaquants. On reste en mode **IDS** (détection) plutôt qu'en **IPS** (prévention).

Pour les tests, je recommande d’activer les catégories de règles **"3coresec"**, **"compromised"** et **"scan"**.

Une fois cela fait :

1. Va dans l’onglet **Interfaces** et redémarre Suricata sur l’interface concernée.
2. Si Suricata ne démarre pas, va dans l’onglet **Logs View** et consulte **suricata.log** pour voir les erreurs.
3. La plupart du temps, le problème vient d’un conflit entre la taille de la mémoire et la configuration dans l’onglet **Flow/Stream** (mais ça, c’est un sujet à part).

Activation du mode IPS

Pour préparer le mode de prévention, commence par aller dans l’onglet **Alerts** et examine les journaux pendant un certain temps. Selon le contexte, cela peut prendre **un jour à un mois** pour bien comprendre ce qui se passe sur ton ou tes réseaux.

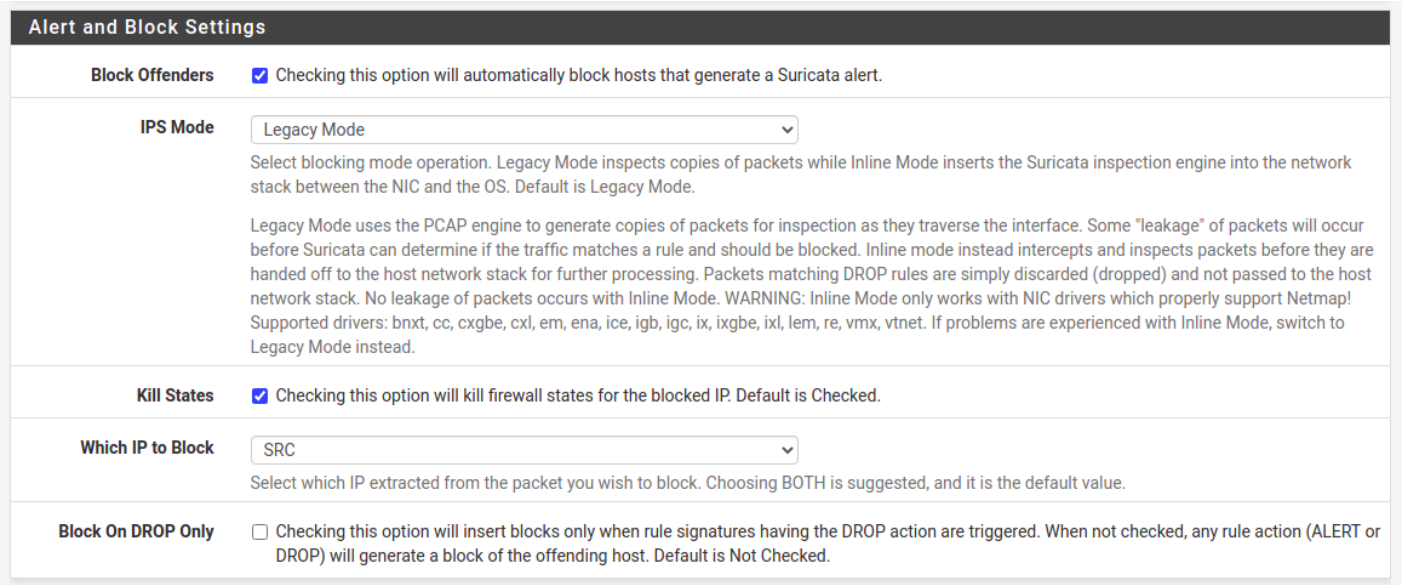
- **Pour les réseaux d’entreprise**, le trafic **sortant** est généralement plus intéressant à analyser que le trafic entrant.
- **Pour les fournisseurs de services**, c’est l’inverse : le trafic **entrant** est celui à surveiller en priorité.

Il est important de noter que le package Suricata de pfSense ajoute automatiquement à une **pass list** (liste d’exclusion) les **adresses du réseau local**, les **adresses des interfaces** et même les **sous-réseaux des tunnels** pour éviter de les bloquer.

Si tu souhaites **bloquer certaines adresses internes**, pense à vérifier cette liste par défaut ou à créer ta propre **pass list**.

Une fois que tu as bien analysé le trafic de ton réseau, y compris le trafic entrant, il est temps d’activer le mode de blocage.

➡ **Va dans les paramètres de l’interface et coche l’option "Block Offenders"** pour activer le blocage des menaces.



Préférences pour le mode IPS

1. **Choix du mode IPS : "Legacy Mode"**
   - Je recommande de sélectionner **"Legacy Mode"**, car il **copie** les paquets au lieu de les intercepter entre la carte réseau (NIC) et le système d’exploitation.
   - C’est plus simple pour commencer, car cela demande **moins de configuration** par rapport au mode **"Inline Mode"**.
2. **Blocage basé sur l’adresse source ("SRC")**
   - Dans les paramètres **"Which IP to Block"**, je préfère bloquer uniquement les **adresses sources ("SRC")**.
   - Pour le trafic sortant, l’adresse source sera une **adresse locale**, mais **elle ne sera pas bloquée** car elle est présente dans la **pass list** du réseau domestique.
3. **Adaptation selon le réseau**
   - Le choix de bloquer les adresses source ou destination **dépend du type de trafic** sur ton réseau :
     - **Si tu as plus de trafic sortant**, envisage de bloquer les **adresses cibles**.
     - Certains recommandent de bloquer **les adresses source et destination**, mais ce n’est pas toujours adapté à tous les cas d’usage.

Analyse des menaces

1. **Redémarrage et observation**
   - Après avoir **enregistré la configuration**, redémarre le service **Suricata** sur l’interface concernée.
   - Attends quelques minutes pour observer l’activité du réseau.
2. **Surveillance des scans et tentatives d’exploration**
   - Les **adresses IPv4 publiques** sont bien connues et scannées en permanence.
   - Ne sois pas surpris si, **en quelques minutes**, des **crawlers** ou des scripts automatisés commencent à explorer ton adresse IP.
   - Même une **nouvelle adresse publique** sera rapidement détectée et scannée.
3. **Nombre de menaces détectées**

- En général, avec **Suricata actif**, on observe entre **50 et 500 adresses IP publiques bloquées par jour**.
- Sur un **réseau domestique ou de bureau**, tu verras surtout du trafic lié aux mises à jour et aux connexions des appareils.
- Pour les **grandes entreprises**, le trafic sera **beaucoup plus varié** et nécessitera une analyse plus approfondie (ce qui sera abordé plus tard).

Revision #3
Created 2025-04-01 07:06:36 UTC by GianniO
Updated 2025-04-08 10:03:26 UTC by GianniO