SNORT SUR_PFSENSE

Présentation et installation de SNORT sur PFSense :

SNORT est un **IDS** (Système de Détection d'Intrusion) et **IPS** (Système de Prévention d'Intrusion) :

Un IDS est un outil de sécurité réseau conçu pour surveiller et analyser le trafic réseau à la recherche d'activités suspectes ou malveillantes. Il fonctionne en inspectant les paquets de données circulant sur le réseau et en comparant ces paquets à une base de données de signatures connues de menaces. Si une correspondance est trouvée, l'IDS déclenche un évènement pour avertir d'une potentielle intrusion.

Snort est l'un des IDS les plus populaires et largement utilisés. Il est développé Cisco et est devenu une référence dans le domaine de la détection d'intrusion. Snort utilise une approche basée sur des règles pour identifier les activités suspectes.

Alors que les IDS détecte Snort, va au-delà de la simple détection et prend des mesures pour prévenir les intrusions en temps réel (IPS). Lorsqu'une activité suspecte est détectée, Snort peut déclencher des contre-mesures automatiques pour bloquer le trafic malveillant.

En combinant les fonctionnalités d'un IDS et d'un IPS, Snort offre une solution de sécurité réseau puissante et complète.

Les règles de Snort sont écrites dans un format spécifique, composé de plusieurs champs qui fournissent des informations importantes pour la détection des intrusions.

Action : Le champ d'action spécifie ce que Snort doit faire lorsqu'une règle correspond à un paquet réseau. Il peut inclure des actions telles que "alert" (générer une alerte), "log" (enregistrer l'événement), "pass" (laisser passer le trafic), "drop" (bloquer le trafic), "reject" (rejeter le trafic avec une notification ICMP), etc.

Protocole : Ce champ indique le protocole réseau sur lequel la règle doit être appliquée, comme TCP, UDP, ICMP, etc.

Source IP : Le champ d'adresse IP source spécifie l'adresse IP ou la plage d'adresses IP source à laquelle la règle s'applique. Il peut être spécifié sous la forme d'une adresse IP unique, d'un réseau CIDR (Classless Inter-Domain Routing) ou d'une plage d'adresses.

Source Port : Ce champ indique le port source ou la plage de ports source à laquelle la règle s'applique. Il peut être spécifié comme un port unique ou une plage de ports.

Direction : Le champ de direction indique la direction du flux de trafic réseau, par exemple "->" pour indiquer du client vers le serveur ou "<-" pour indiquer du serveur vers le client.

Destination IP : Le champ d'adresse IP de destination spécifie l'adresse IP ou la plage d'adresses IP de destination à laquelle la règle s'applique. Il peut être spécifié de la même manière que le champ d'adresse IP source.

Destination Port : Ce champ indique le port de destination ou la plage de ports de destination à laquelle la règle s'applique. Il peut être spécifié comme un port unique ou une plage de ports.

Options : Les options fournissent des informations supplémentaires pour affiner la détection. Elles peuvent inclure des informations telles que des mots clés spécifiques à rechercher, des signatures d'attaques, des conditions de détection, des priorités, des seuils, etc.

. Voici quelques exemples courants d'options :

msg : Cette option permet de spécifier un message personnalisé qui sera inclus dans l'alerte générée lorsqu'une règle correspond à un paquet.

sid : L'option sid (Signature ID) est un identifiant unique attribué à chaque règle Snort. Il est utilisé pour référencer une règle spécifique dans les journaux et les alertes.

rev : L'option rev (Revision) indique la révision de la règle. Elle est utile pour suivre les modifications apportées aux règles au fil du temps.

classtype : Cette option permet de classifier la règle en fonction de la catégorie d'attaque à laquelle elle se rapporte, par exemple, "attempted-admin", "attempted-user", "bad-unknown", etc.

content : (détails dans 8-2) Bien que le champ "contenu" soit également présent dans le format des règles, l'option content est utilisée pour spécifier un contenu spécifique à rechercher dans un paquet, en ajoutant des mots clés ou des signatures d'attaques.

Contenu : Le champ de contenu spécifie le contenu spécifique que Snort doit rechercher dans les paquets réseau. Il peut s'agir d'une chaîne de caractères, d'une séquence hexadécimale ou d'une expression régulière.

content : L'opérateur content est utilisé pour spécifier un contenu spécifique à rechercher dans un paquet. Il peut s'agir d'une chaîne de caractères, d'une séquence hexadécimale ou d'une expression régulière. Par exemple, pour détecter la présence de la chaîne "admin" dans un paquet, vous pouvez utiliser content:"admin";.

nocase : L'opérateur nocase est utilisé en conjonction avec l'opérateur content pour effectuer une recherche sans tenir compte de la casse des caractères. Par exemple, content:"password"; nocase; détectera les occurrences de "password" indépendamment de leur casse (majuscules ou minuscules).

pcre : L'opérateur pcre permet d'effectuer une recherche en utilisant une expression régulière Perl Compatible Regular Expression (PCRE). Les expressions régulières PCRE offrent une puissance et une flexibilité supplémentaires pour la recherche de motifs complexes. Par exemple, pcre:"/^[A-Za-z0-9]+$/"; recherchera une chaîne qui ne contient que des lettres majuscules et minuscules ainsi que des chiffres.

byte_test : L'opérateur byte_test permet de rechercher des valeurs spécifiques dans les octets d'un paquet. Il est généralement utilisé pour effectuer des recherches binaires sur des données spécifiques. Par exemple, byte_test:1, =, 0x41, 0, relative; recherchera la présence de la valeur hexadécimale 0x41 (correspondant au caractère "A") à un certain emplacement dans le paquet.

uricontent : L'opérateur uricontent est utilisé pour rechercher un contenu spécifique dans l'URI (Uniform Resource Identifier) d'une requête HTTP. Par exemple, uricontent:"/admin"; détectera les URI contenant "/admin".

depth : L'opérateur depth permet de spécifier la profondeur maximale de la recherche de contenu dans un paquet. Il est souvent utilisé pour limiter la portée de la recherche à une partie spécifique du paquet. Par exemple, content:"password"; depth:100; limitera la recherche à une profondeur de 100 octets à partir du début du paquet.

distance : L'opérateur distance permet de spécifier la distance entre deux occurrences de contenu dans un paquet. Il est utile lorsque vous souhaitez rechercher la présence de deux motifs distincts dans un ordre spécifique, mais avec une distance donnée entre eux.

Ces champs sont combinés de manière spécifique pour créer des règles de détection d'intrusion efficaces dans

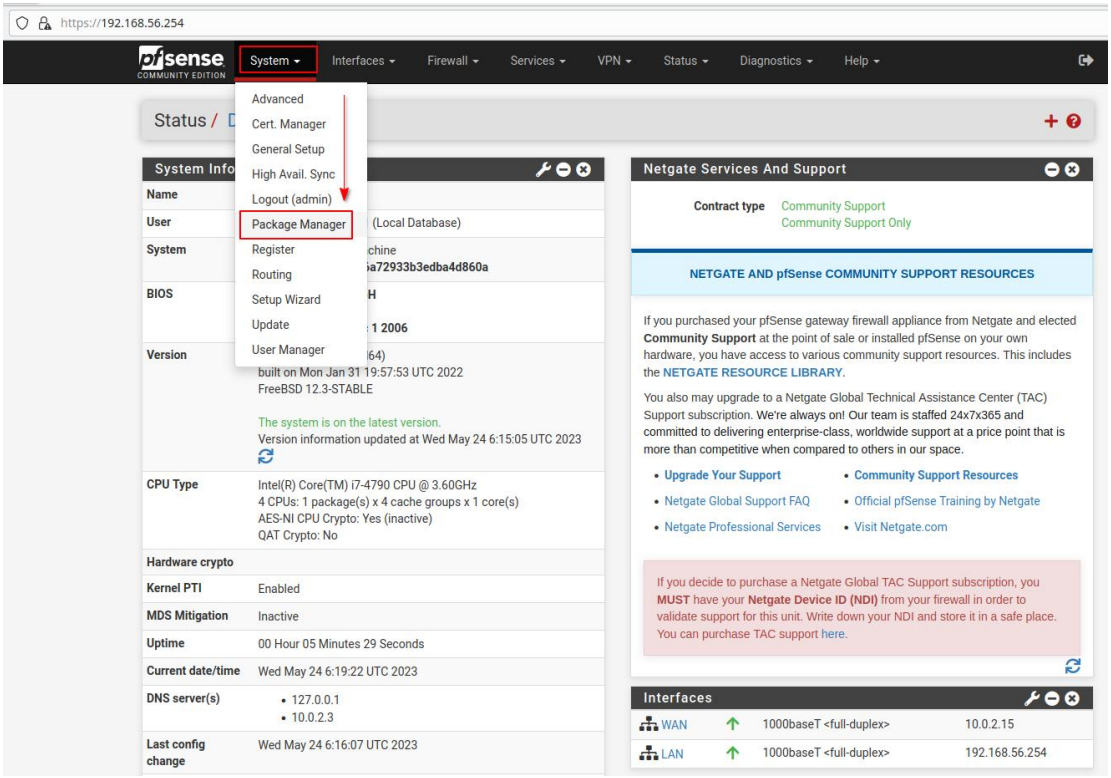
Snort. En utilisant ces champs de manière appropriée, les administrateurs peuvent personnaliser les règles pour répondre aux besoins spécifiques de leur réseau et améliorer la détection des activités malveillantes

L'installation de SNORT

Snort n'étant pas installé par défaut par pfsense, pour pouvoir l'utiliser il est nécessaire de passer par la case installation.

Rien de compliqué cependant, c'est un paquet à installer.

Pour aller installer un paquet, il faut naviguer sur la page "packet manager"



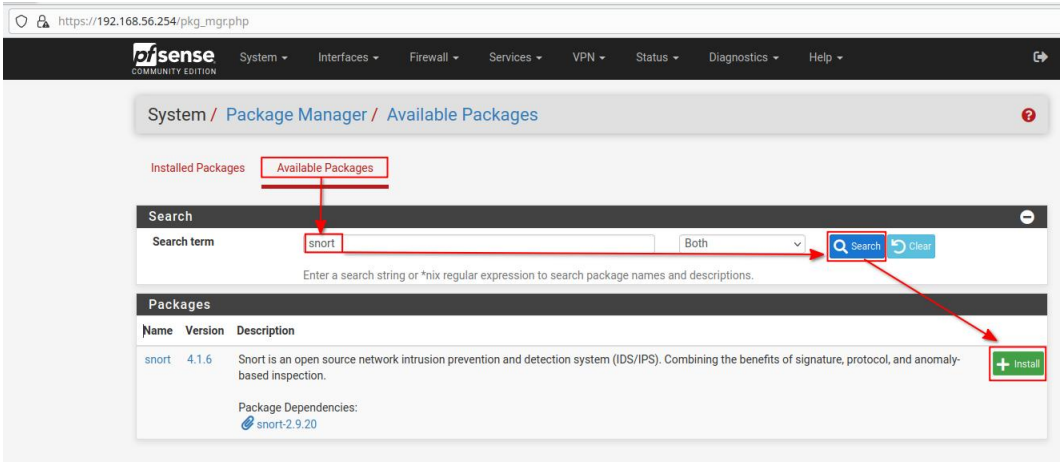
Sur la page Packet Manager, il y a deux onglets :

Installed Packages

Available Packages

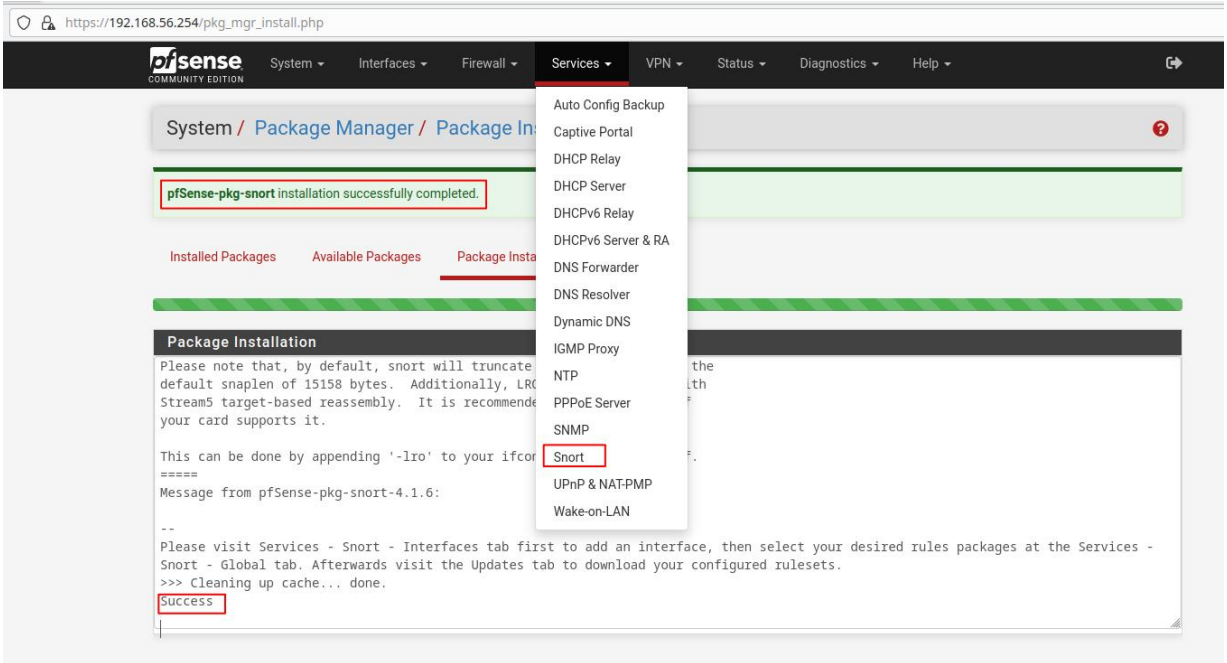
On va donc sélectionner l'onglet "Available Package" et taper snort en barre de recherche.

Une fois le paquet trouvé, il ne reste plus qu'a cliquer sur le bouton d'installation.

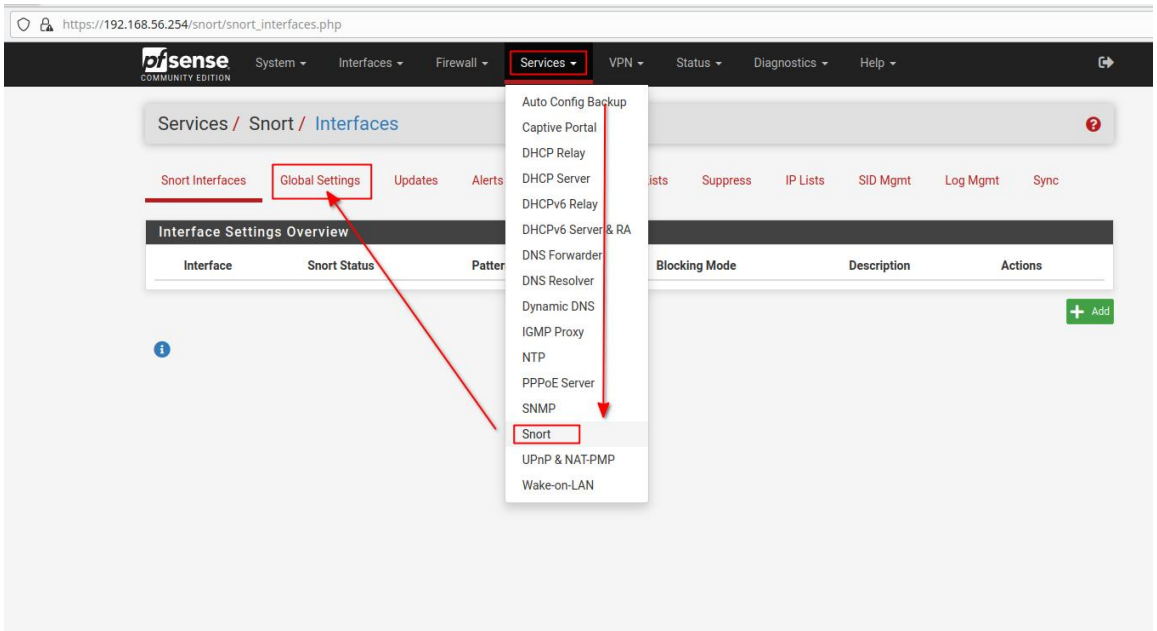


Il ne reste plus qu'a confirmer pour lancer l'installation

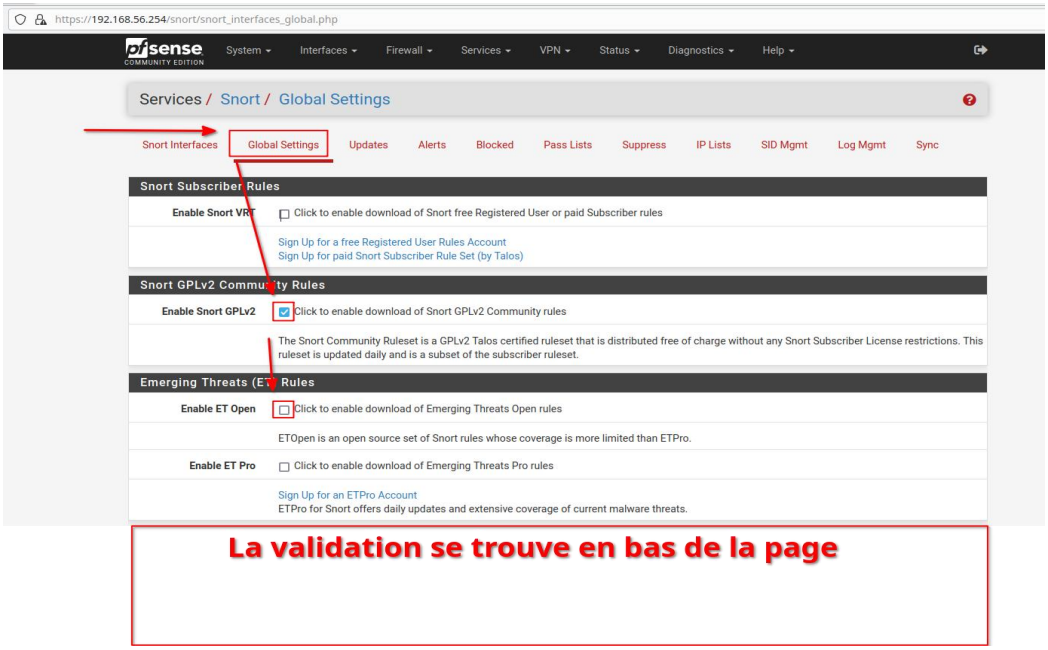
Une fois l'installation terminée, une entrée snort est maintenant disponible depuis le menu service.



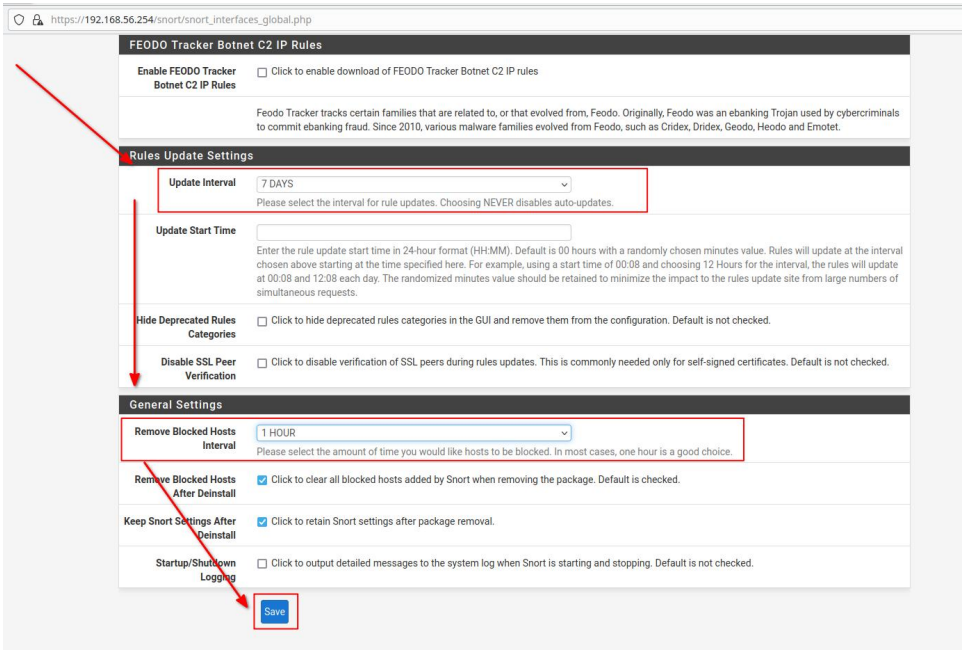
Snort est maintenant installé !
Comme expliqué au début de l'article, Snort fonctionne sur base de règles permettant de détecter les comportements suspects.
Il existe plusieurs sources pour ces règles, certaines sont gratuites, certaines sont payantes.
Donc, dans un scénario réaliste, avant de pouvoir utiliser snort, on va devoir sélectionner les sources que l'on veut utiliser et les télécharger



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

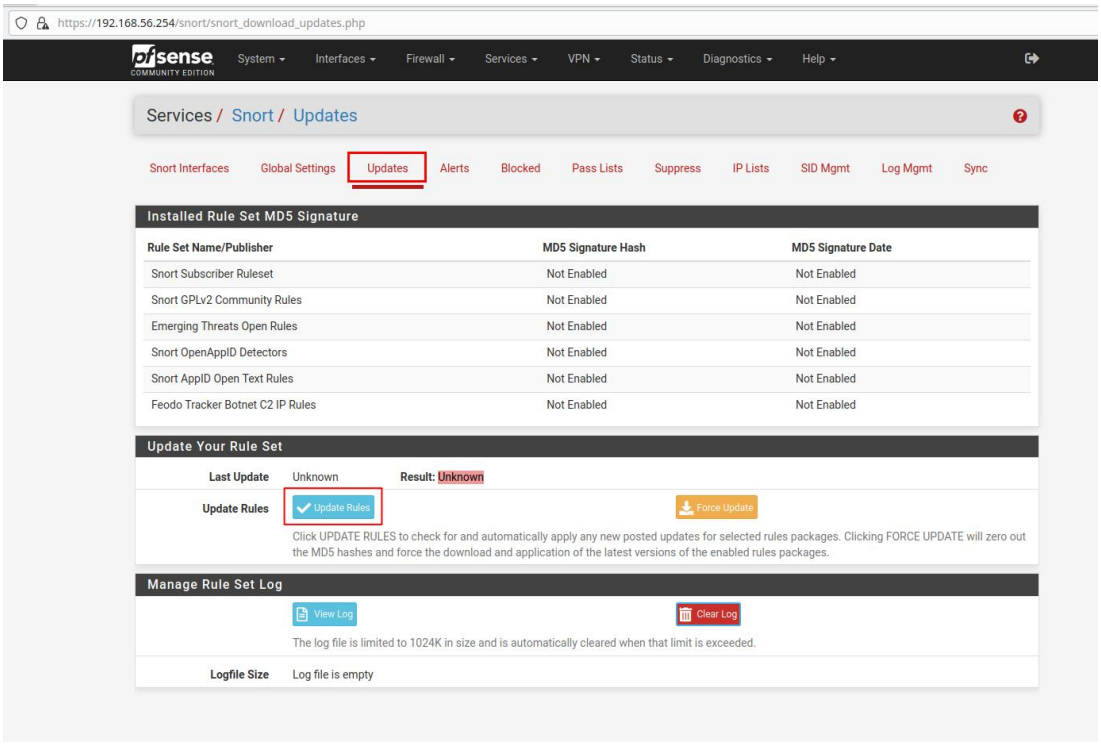


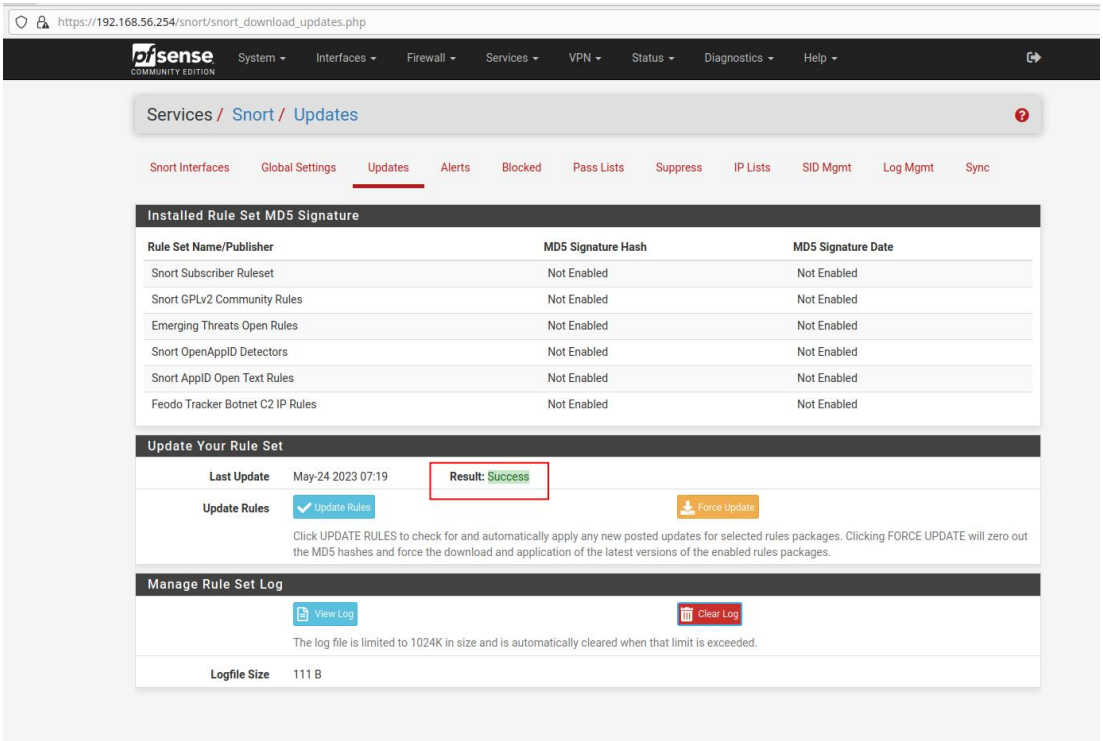
On va modifier la période de rafraichissement et la période avant la suppression automique du "ban"



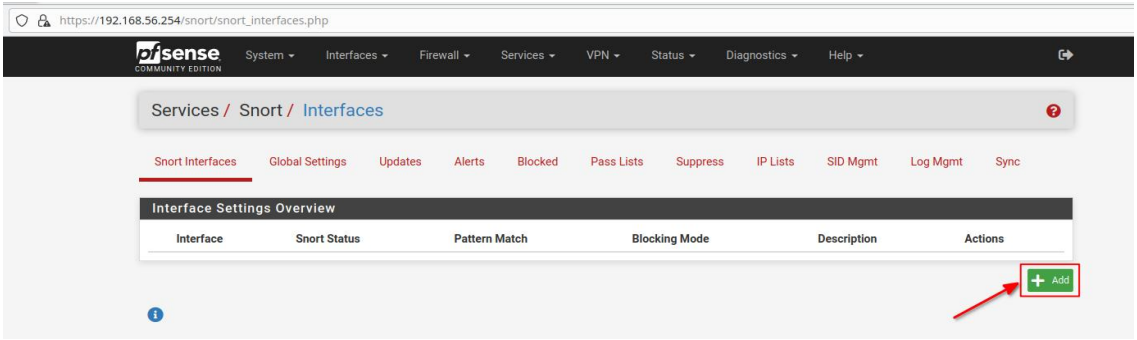
Et on valide

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

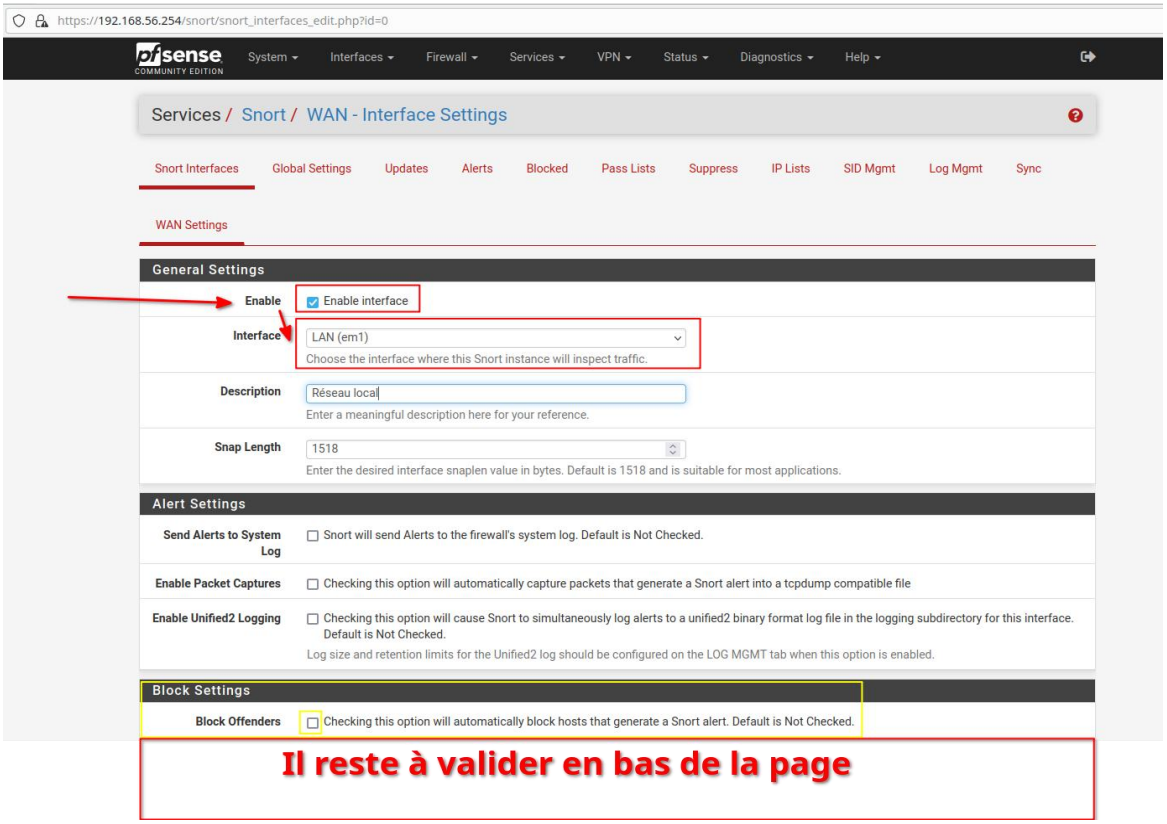




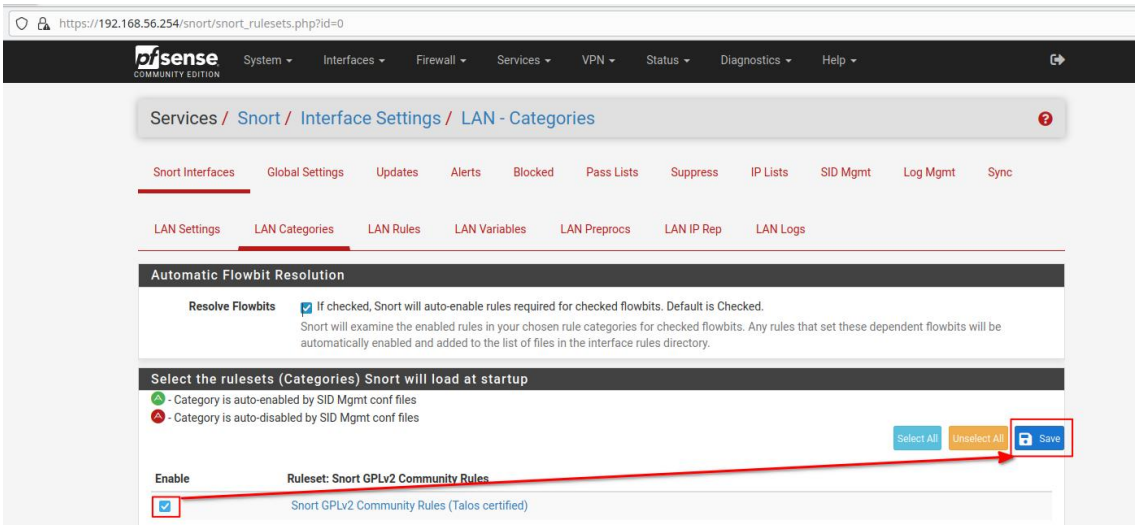
Une fois que la mise à jour est terminée, on peut activer l'interface que snort va écouter



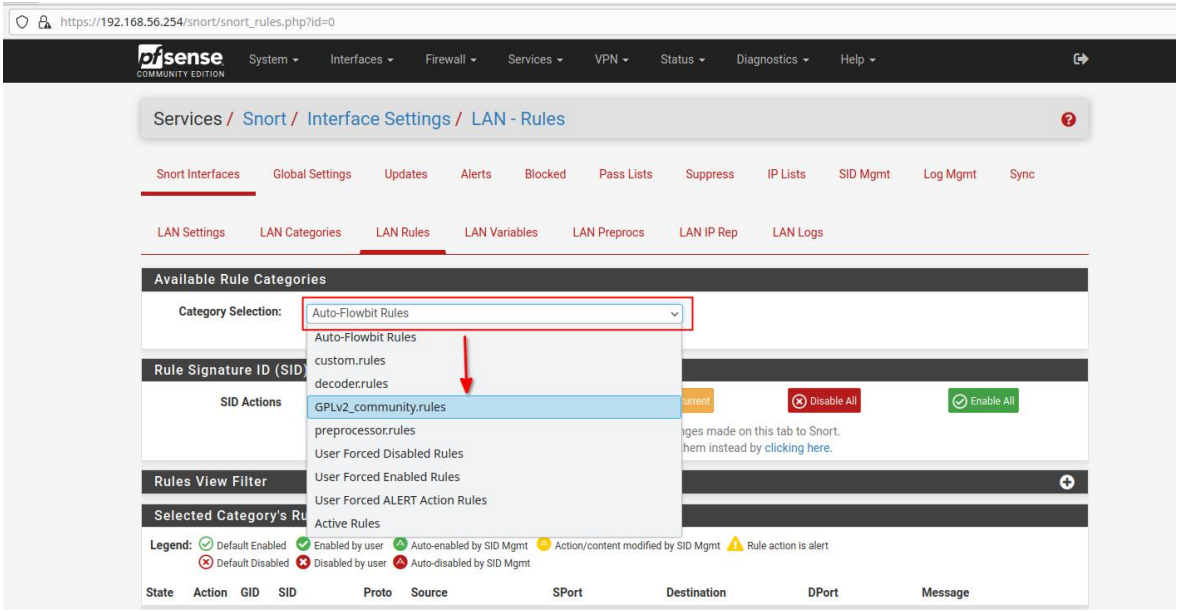
Il faut donc sélectionner la carte (généralement LAN) et l'activer.
Sur la partie encadrée en jaune (de l'image suivante), il est déconseillé de d'activer le blocage tout de suite, il est préférable de vérifier ce qui normal et ce qui ne l'est pas avant de voir tout son trafic bloqué.



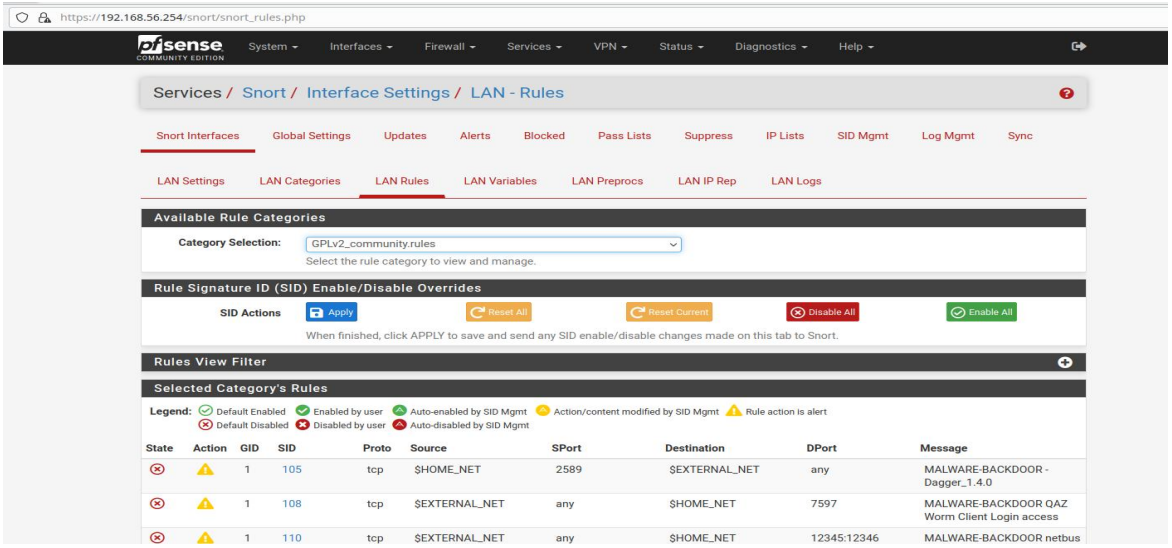
Une fois validé, on peut passer à l'onglet "categories" pour activer les règles



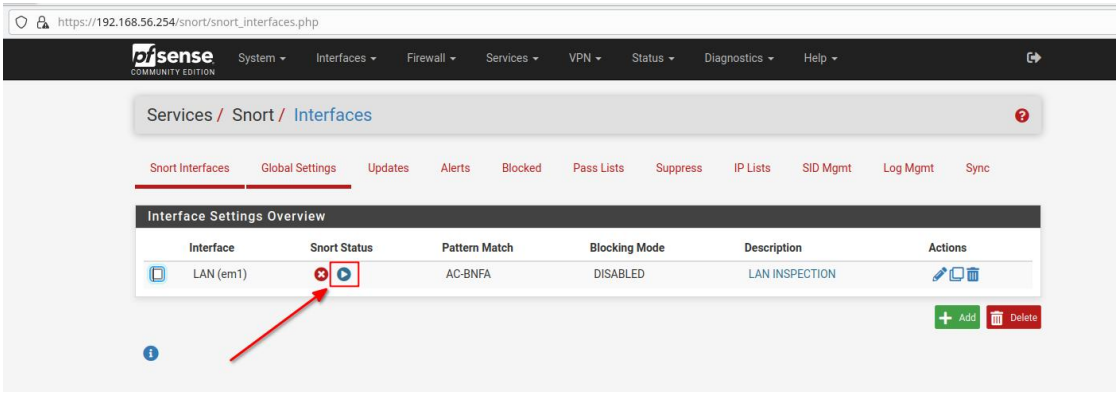
Pour activer/désactiver les règles individuellement, on doit passer sur l'onglet "Rules" et sélectionner une des liste que l'on a activé.



Il reste à activer ce que l'on souhaite



On valide et on applique et on peut vérifier les détection dans "Alerts" en mode "découverte" ou dans "Alert et Blocked" lorsque l'on passe en production.
Pour passer en production : on lance le service sur l'interface



Et hop ...

C'est fait