Nom : Kresser

Prénom : Alexis

N° Candidat : **02045540456**

BTS Service Informatique aux organisation

Solution d’infrastructure système et réseaux

*Réalisation Professionnel n*1 : Mise en place d’un système de détection d’intrusion de SNORT*

Tables des matières

1. Description Réalisation Professionnel

Propriétés	Description
Intitulé	**Mise en place d'un système de détection d'intrusion avec architecture centralisée sur SNORT**
Présentation rapide	Les systèmes de détection et intrusions (IDS) et de prévention des intrusions (IPS) sont des pare-feu qui sécurisent toutes les données entrant ou sortant d'un réseau.
Objectifs	- Automatiser les sécurité réseaux - Conformité des technologies et systèmes dédiés à la protection des données - Les IDS/IPS sont configurables, ce qui contribue à l'application des politiques de sécurité internes au niveau du réseau.
Compétences mobilisées	2.1 Concevoir une solution d'infrastructure réseau 2.2 Installer, tester et déployer une solution d'infrastructure réseau 2.3 Exploiter, dépanner et superviser une solution d'infrastructure réseau
Outils	L'application va s'appuyer sur l'infrastructure existante de GSB comportant : - Pfsens - réseau
Documents joints	Schéma réseau GSB (actuel et attendu), Procédure d'installation, Fiche technique des équipements ...
Modalités de réception	Présentation d'un système opérationnel - Documentation technique, Mode opératoire et compte rendu d'installation
Evolution possible	Mise en place d'un VLAN protéger à travers SNORT

2. Présentation GSB(Galaxy Swiss bourdin) et de son contexte

2.1 L'entreprise:

Le laboratoire Galaxy Swiss Bourdin est issu de la fusion entre le géant américain Galaxy et le conglomérat européen Swiss Bourdin, lui-même déjà union de trois petits laboratoires.
En 2009, les deux géants pharmaceutiques unissent leurs forces pour créer un leader de ce secteur industriel. L'entité GSB Europe a établi son siège administratif à Paris.
Le siège social de la multinationale est situé à Philadelphie, Pennsylvanie, aux Etats-Unis.
La France a été choisie comme témoin pour l'amélioration du suivi de l'activité de visite.

2.2 Réorganisation :

Une conséquence de cette fusion est la recherche d'une optimisation de l'activité du groupe en réalisant des économies d'échelle dans la production et la distribution des médicaments et d'augmenter la sécurité de cette fusion tout en prenant le meilleur des deux laboratoires sur les produits concurrents.
L'entreprise compte 480 visiteurs médicaux en France métropolitaine, et 60 dans les départements et territoires d'outre-mer.

2.3 Besoin :

Depuis la réorganisation de GSB l'entreprise fonctionne bien et a connu une hausse de son activité. Suite à cela Galaxy Swiss Bourdin a décidé de sécuriser son réseau en mettant en place un système de détection des intrusions et un système de prévention des intrusions en installant un pare-feu IDS/IPS. Pour réaliser cette mission, GSB nous a fourni un schéma de leur réseau actuel, grâce à celui-ci nous allons pouvoir étudier l'emplacement ou l'IPS/IDS sera le plus efficace contre les attaques sans bloquer les autres connexion dans le réseau.

Schéma actuel :

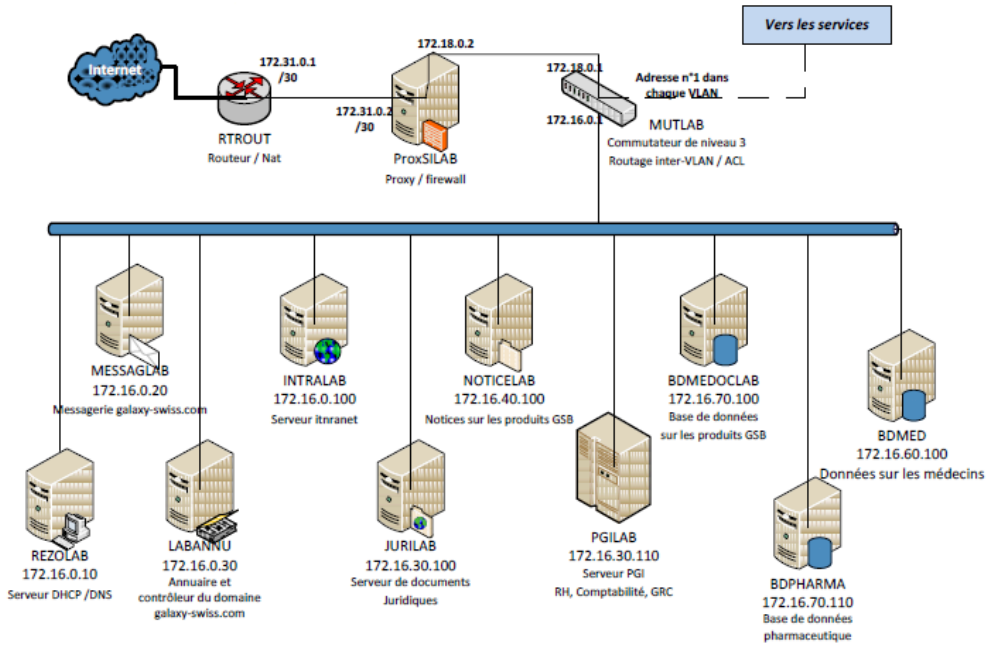
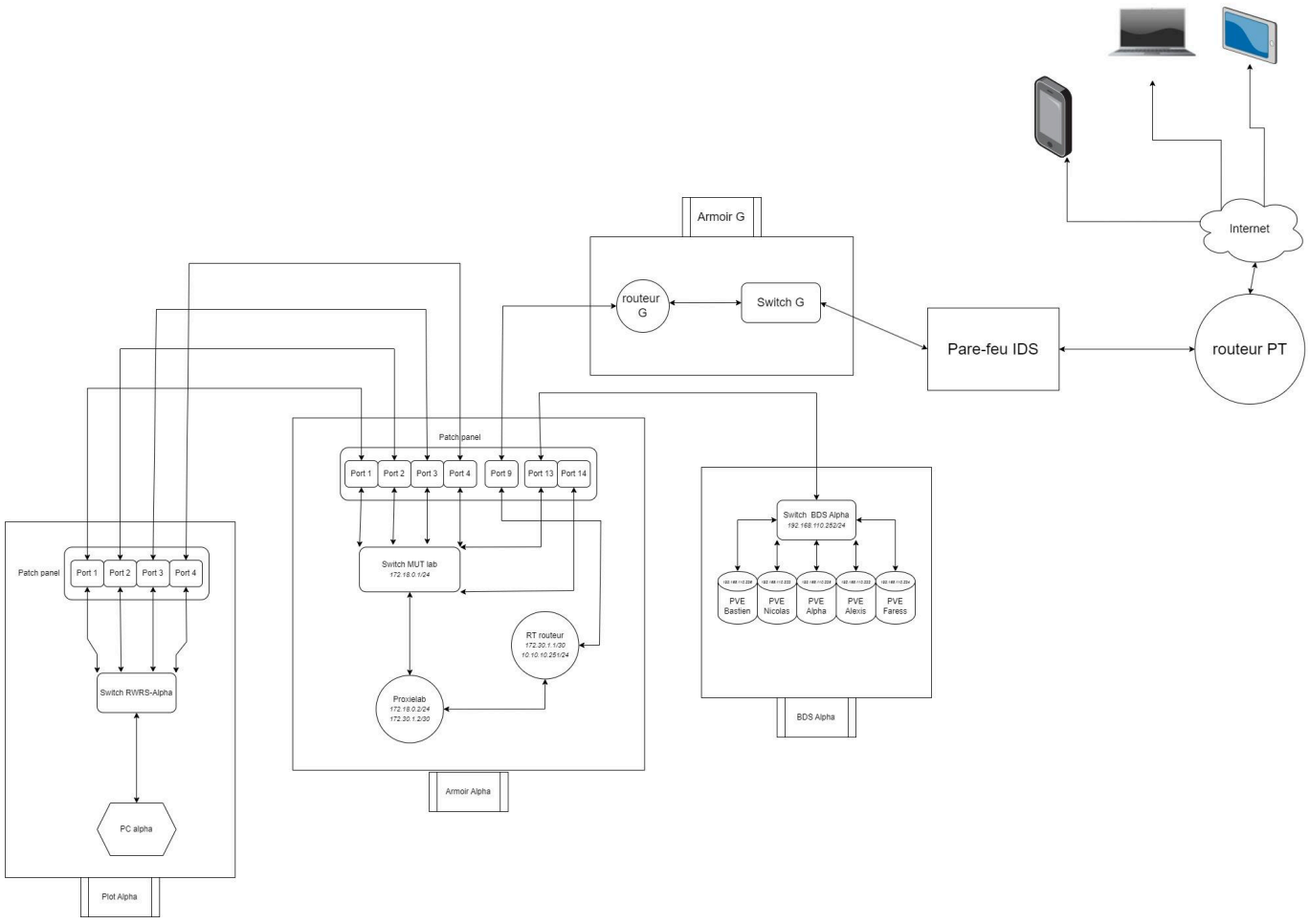


Schéma réseau attendu :



3.Matériel à disposition

3.1 Ressources documentaire :

- Contexte GSB
- Schéma réseau (contexte)

3.2 Ressource matérielles:

- un hyperviseur de type 1 : Proxmox hébergeant les machine virtuelle du contexte
- Un Hyperviseur de type 1 : Proxmox hébergeant les machine virtuelle de mes réalisation professionnel
- un routeur (RT-ROUT)
- Un par-feu ProxSilab (PFSENSE)
- Plusieur switch de niveau 3 (Cisco-3750G)
- Un switch niveau 2 (Cisco 2960)
- Un Switch BDS
- plusieur ordinateur pour effectuer les simulations et les tests

3.3 Logiciel utilisées:

- PFsense
- virtualBox

3.4 Table d'adressage IP :

Matériel	IP de connexion	ID de connexion	Mot de passe	Protocol
Switch RWRS 3750G	192.168.110.253	admin	Aristee.2022	SSH2
MUTLAB	192.168.110.1	admin	Aristee.2022	SSH2
RT-ROUT	172.30.0.1		Aristee.2024	Telnet
PFSENSE	192.168.110.100	admin	Aristee.2024	SSH2
Switch BDS	192.168.110.252	admin	Aristee.2022	SSH2
Proxmox Alpha	192.168.110.235	root	Aristee.2024	SSH2
Proxmox Alexis	192.168.110.232	root	Aristee.2024	SSH2
SRV-DC01	192.168.110.101	a.kresser	Aristee.2024	SSH2
JURILAB	172.16.30.100	root	Aristee.2024	SSH2

Matériel	IP de connexion	ID de connexion	Mot de passe	Protocol
MESSAGELAB	172.16.0.20	root	Aristee.2024	SSH2
NOTICELAB	172.16.40.100	root	Aristee.2024	SSH2
BDMED	172.16.60.100	root	Aristee.2024	SSH2
BDMEDCOLAB	176.16.70.100	root	Aristee.2024	SSH2
BDPHARMA	176.16.70.110	root	Aristee.2024	SSH2
REZOLAB	176.16.0.10	root	Aristee.2024	SSH2
PC Student	X	1133941414	Aristee.2024	Anydesk

3.5 Tableau des Vlans :

Numéro Vlan	Services(s)	Adressage IP
20	Direction / DSI	192.168.20.0/24
30	RH / Compta / Juridique / Secrétariat / Administratif	192.168.30.0/24
40	Communication / Rédaction	192.168.40.0/24
50	Développement	192.168.50.0/24
60	Commercial	192.168.60.0/24
70	Labo-Recherche	192.168.70.0/24
100	Accueil	192.168.100.0/24
110	Réseau et système	192.168.110.100/24
150	Visiteurs	192.168.150.0/24
200	Démonstration	192.168.200.0/24
300	Serveurs	172.16.0.0/17
400	Sortie	172.18.0.0/30

4. Présentation du projet

Dans le cadre de notre mission pour Galaxy Swiss Bourdin et de la sécurisation de leur équipement, nous allons mettre en place un système de détection des intrusions (IDS) et de prévention des intrusions (IPS).

Leur fonctionnement est simple, les IDS/IPS comparent les paquets de réseau à une base de données de cybermenaces contenant des signatures connues de cyberattaques et repèrent tous les paquets qui concordent avec ces signatures.

La principale différence entre les deux tient au fait que l'IDS est un système de surveillance, alors que l'IPS est un système de contrôle.

L'IDS ne modifie en aucune façon les paquets réseau, alors que l'IPS empêche la transmission du paquet en fonction de son contenu, tout comme un pare-feu bloque le trafic en se basant sur l'adresse IP.

> Les IDS (Intrusion Detection Systems) : analysent et surveillent le trafic réseau pour détecter des signes indiquant que des hackers utilisent une cybermenace connue afin de s'infiltrer dans votre réseau ou y voler des données. Les systèmes d'IDS comparent l'activité réseau en cours avec une base de données d'attaques connues afin de détecter divers types de comportements tels que les violations de la politique de sécurité, les malwares et les scanners de port.
>
> Les IPS (Intrusion Prevention Systems) agissent dans la même zone du réseau qu'un pare-feu, entre le monde extérieur et le réseau interne. Les IPS *rejettent* de façon proactive les paquets réseau en fonction d'un profil de sécurité si ces paquets représentent une menace connue.

Les équipes de sécurité sont confrontées à un risque croissant de fuite de données et d'amendes pour non-conformité. Parallèlement, elles continuent d'être confrontées à des problèmes de contraintes budgétaires et de politique d'entreprise. La technologie IDS/IPS recouvre des tâches spécifiques et importantes en matière de stratégie de cybersécurité :

> Automatisation : les systèmes IDS/IPS sont dans une large mesure automatiques, ce qui

en fait des candidats parfaits à l'intégration à la pile de sécurité actuelle. Les IPS procurent la tranquillité d'esprit que le réseau est protégé contre les menaces connues, et ce avec des besoins limités en ressources.

Conformité : dans le cadre du respect de la conformité, il est souvent nécessaire de prouver que vous avez investi dans des technologies et systèmes dédiés à la protection de vos données. La mise en œuvre d'une solution d'IDS/IPS permet de satisfaire une condition de conformité et de réaliser un certain nombre de contrôles de sécurité du CIS. Surtout, les données d'audit constituent un élément essentiel des enquêtes en matière de conformité.

Application de la politique : les IDS/IPS sont configurables, ce qui contribue à l'application des politiques de sécurité internes au niveau du réseau. Par exemple, si vous n'utilisez qu'un VPN, vous pouvez utiliser l'IPS pour bloquer le trafic provenant d'un autre VPN

Afin de mettre IDS/IPS en place nous allons avoir besoin de certain outils déjà présent ou non dans notre réseau, les voici:

4.1 VirtualBox:

C'est un logiciel libre de virtualisation, une solution pour pouvoir exécuter d'autres systèmes d'exploitation sur une seule machine et faire un test d'un réseau réel dans un seul ordinateur.. Il marche sur les trois plateformes (Linux, Windows, macOS).

4.2 Pfsens:

C'est une distribution de pare-feu réseau gratuite, il intègre aussi un gestionnaire de paquets pour installer (logiciels) supplémentaires, désinstaller des paquets et d'autres fonctionnalités. Plusieurs services peuvent être gérés par pfSense, et ces services peuvent être arrêtés ou activés depuis une interface graphique. Voici une liste des services proposés par Pfsense :

- VPN client PPTP, VPN site à site OpenVPN et IPSec.
- Gestion des VLAN.
- Filtrage d'URL.
- Serveur DHCP.
- Partage de bande passante Traffic Shaper (régulation de flux est le contrôle du volume des échanges sur un réseau informatique dans le but d'optimiser ou de garantir les performances).

- Répartition de charge (Load Balancer).
- IDS-IPS Snort.

pour réaliser cette installation nous pouvons utiliser 2 services différents, voici un petit comparatif, Les 4 principales différence entre Snort et Suricata:

1. Architecture : Suricata utilise une architecture multi thread, ce qui lui permet de tirer parti du matériel moderne doté de plusieurs cœurs. Snort, en revanche, fonctionne principalement sur un seul thread.

2. Prise en charge du protocole : Suricata offre une prise en charge étendue des protocoles, notamment HTTP, SMTP, FTP, SSH, etc. Bien que complet, Snort n'a peut-être pas le même niveau de couverture protocolaire que Suricata.

3. Performances : l'architecture multithread et le traitement optimisé de Suricata offrent un débit et une évolutivité plus élevés, ce qui le rend adapté aux réseaux à haut débit. La nature monothread de Snort peut limiter ses performances sur de tels réseaux.

4. Langage de règles : Suricata utilise son langage de règles, Suricata Rule Language (SRL), conçu pour être expressif et puissant. Snort utilise son langage de règles appelé Snort Rules Language (SRL), mais prend également en charge un sous-ensemble compatible de règles Suricata.

Pour notre projet nous allons choisir de prendre Snort car il comporte tous les services dont nous avons besoin en restant assez léger à installer et configurer.

4.3 Snort:

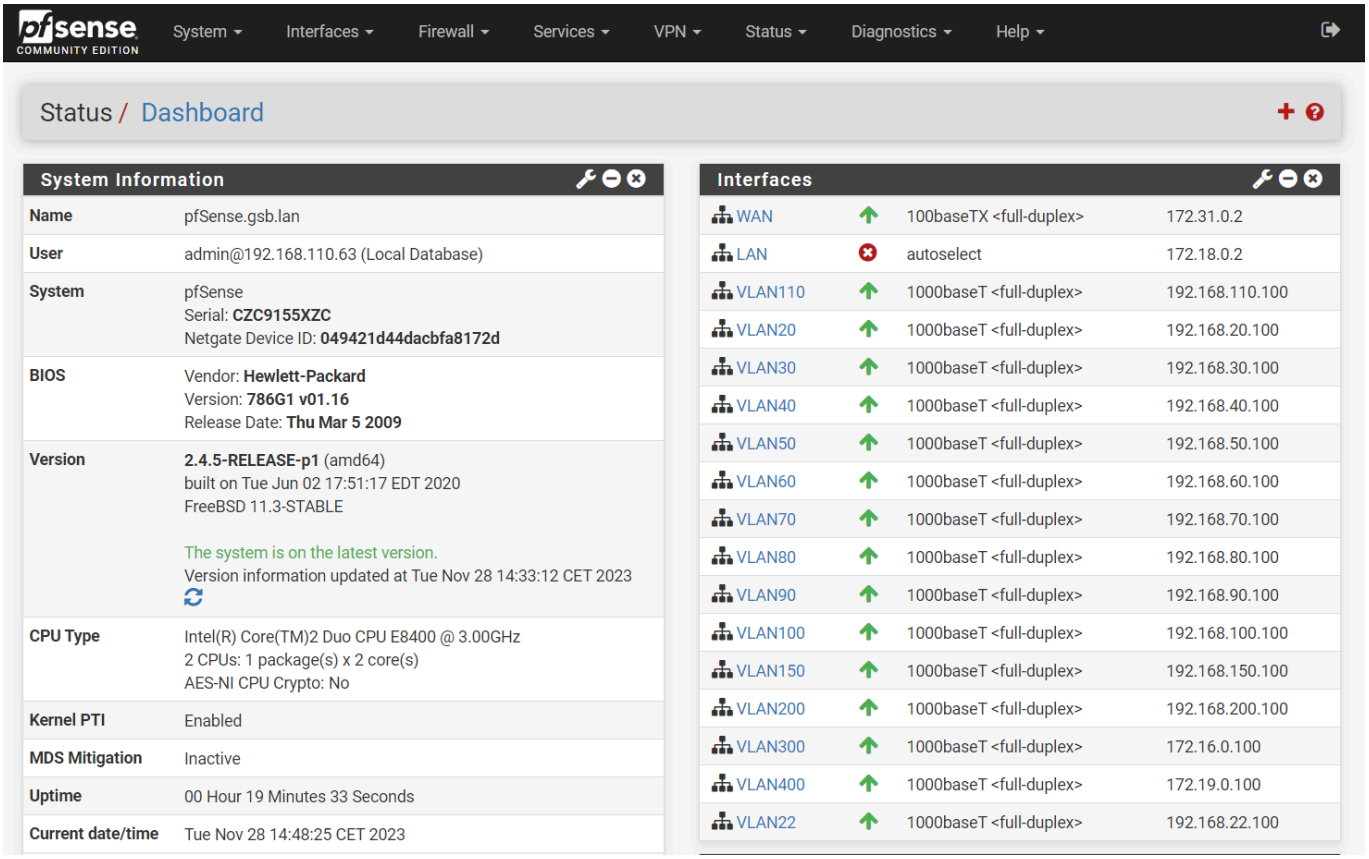
C'est un hybride d'IPS et d'IDS efficace et le projet Open Source le plus avancé au monde. Il utilise une série de règles qui aident à définir l'activité réseau malveillante et utilise ces règles pour trouver les paquets qui leur correspondent et génère des alertes pour les utilisateurs. Snort peut être téléchargé et configuré pour une utilisation personnelle et professionnelle, c'est un outil multi-plateformes (Linux, Windows, FreeBSD). Snort a trois utilisations principales:

- Un détecteur de paquets (renifleur)
- Un enregistreur de paquets - ce qui est utile pour le débogage du trafic réseau.
- Un système de prévention des intrusions réseau à part entière.

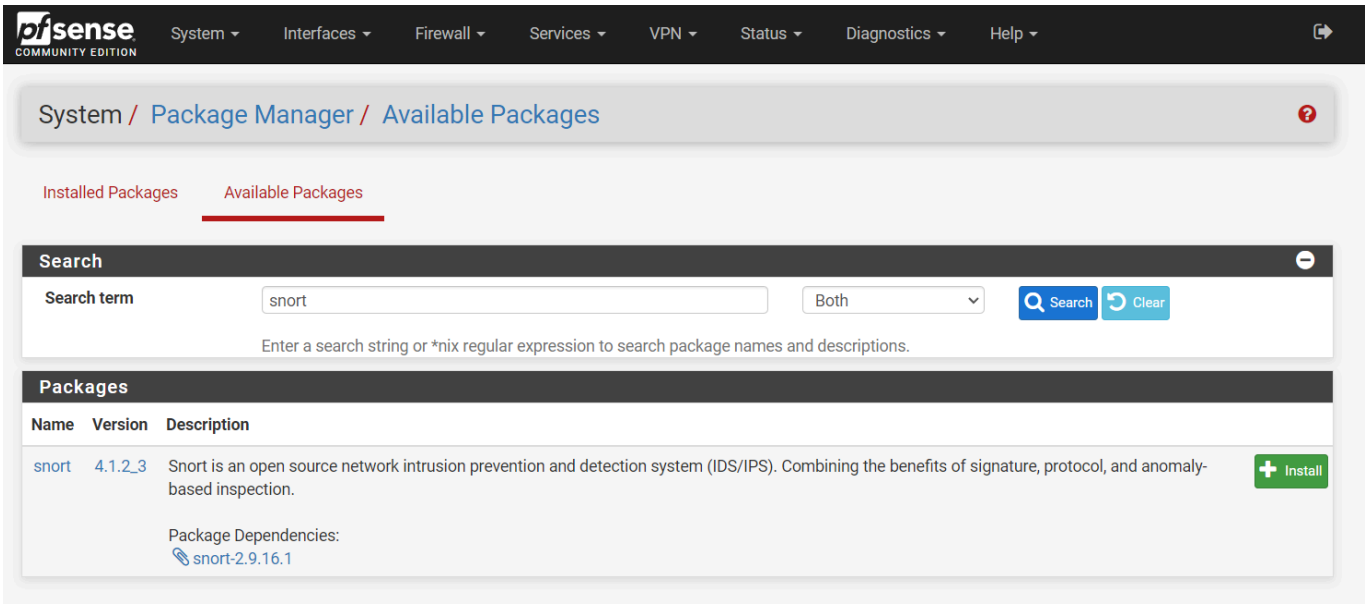
5. Mise en place

5.1 Le pare feu IDS, IPS avec Snort sur PFsens

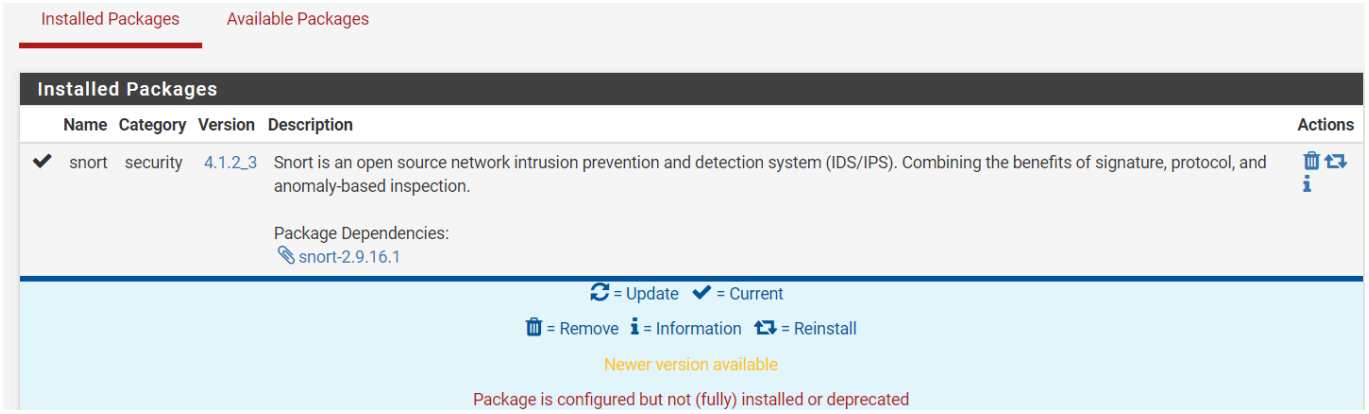
Pour commencer nous allons installer Snort sur le pfsens, pour se faire nous allons sur l'adresse suivante avec notre Vlan: 192.168."Vlan".100



Puis se rendre sur Système > Package manager > Available package, rechercher Snort et l'installer:



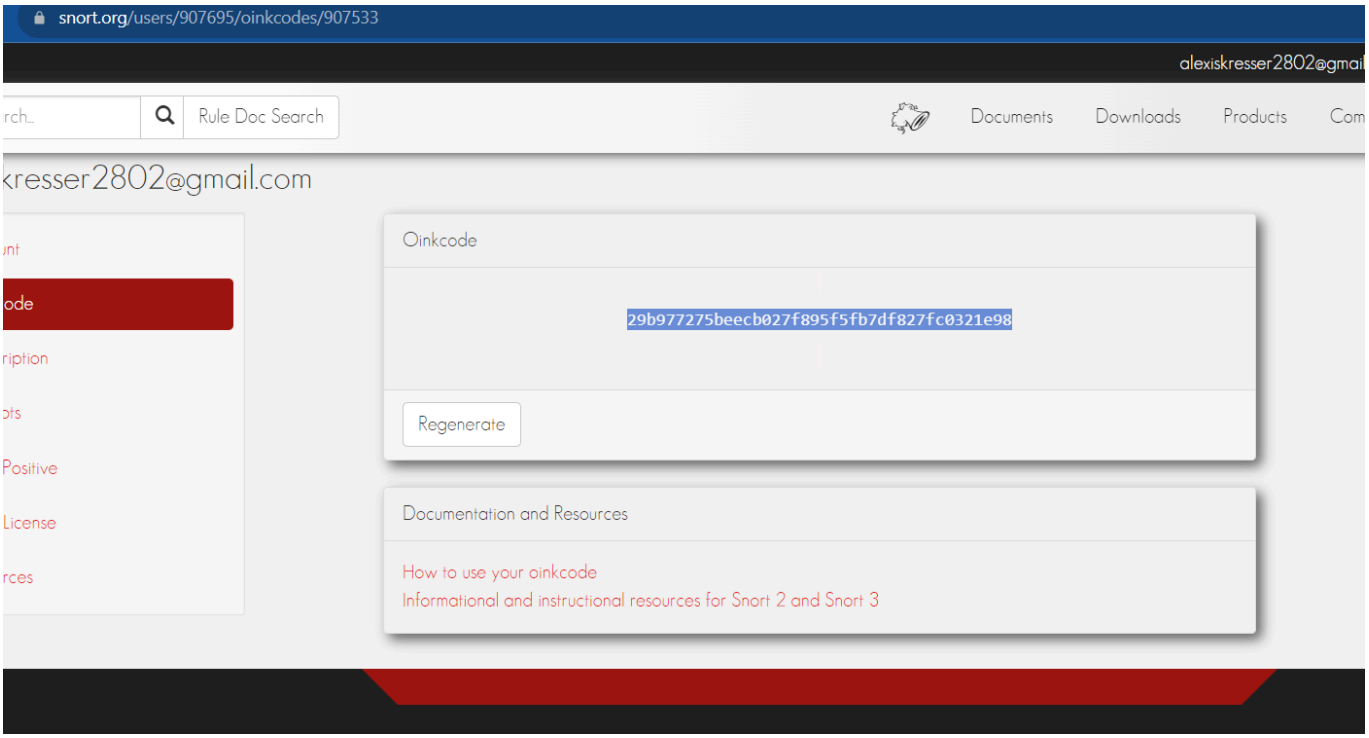
Une fois installé il doit apparaître dans “ installed package” comme ceci:



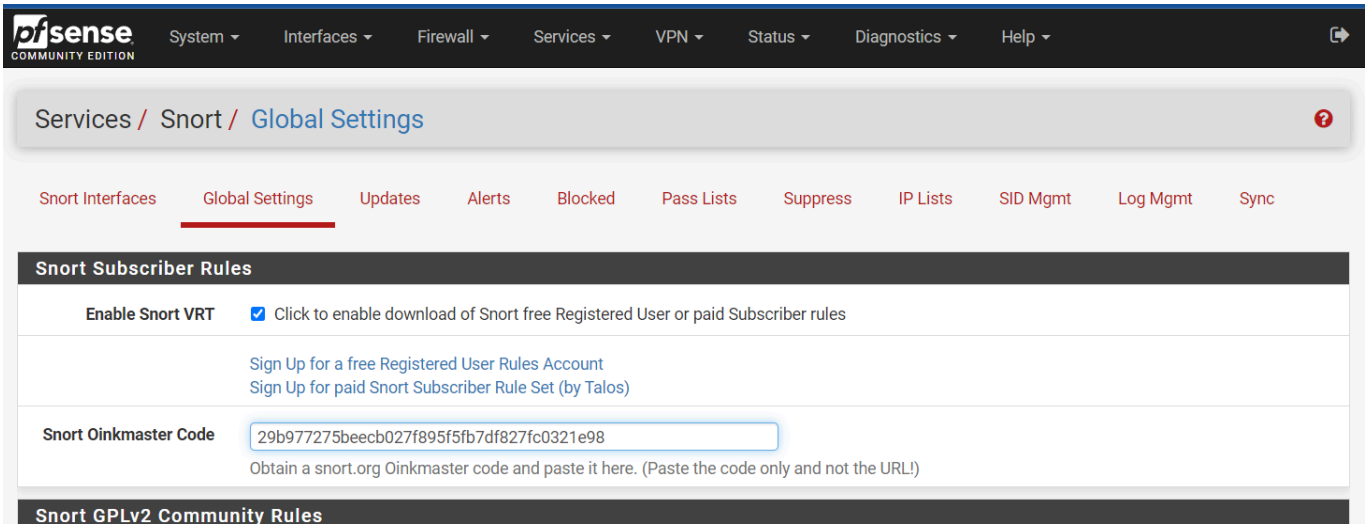
Maintenant nous pouvons nous rendre dans l’onglet service > Snort pour le configurer.

La première étape est 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 Snort.

Récupération du code:



Mettre le code dans **“Snort Oinkmaster Code”**

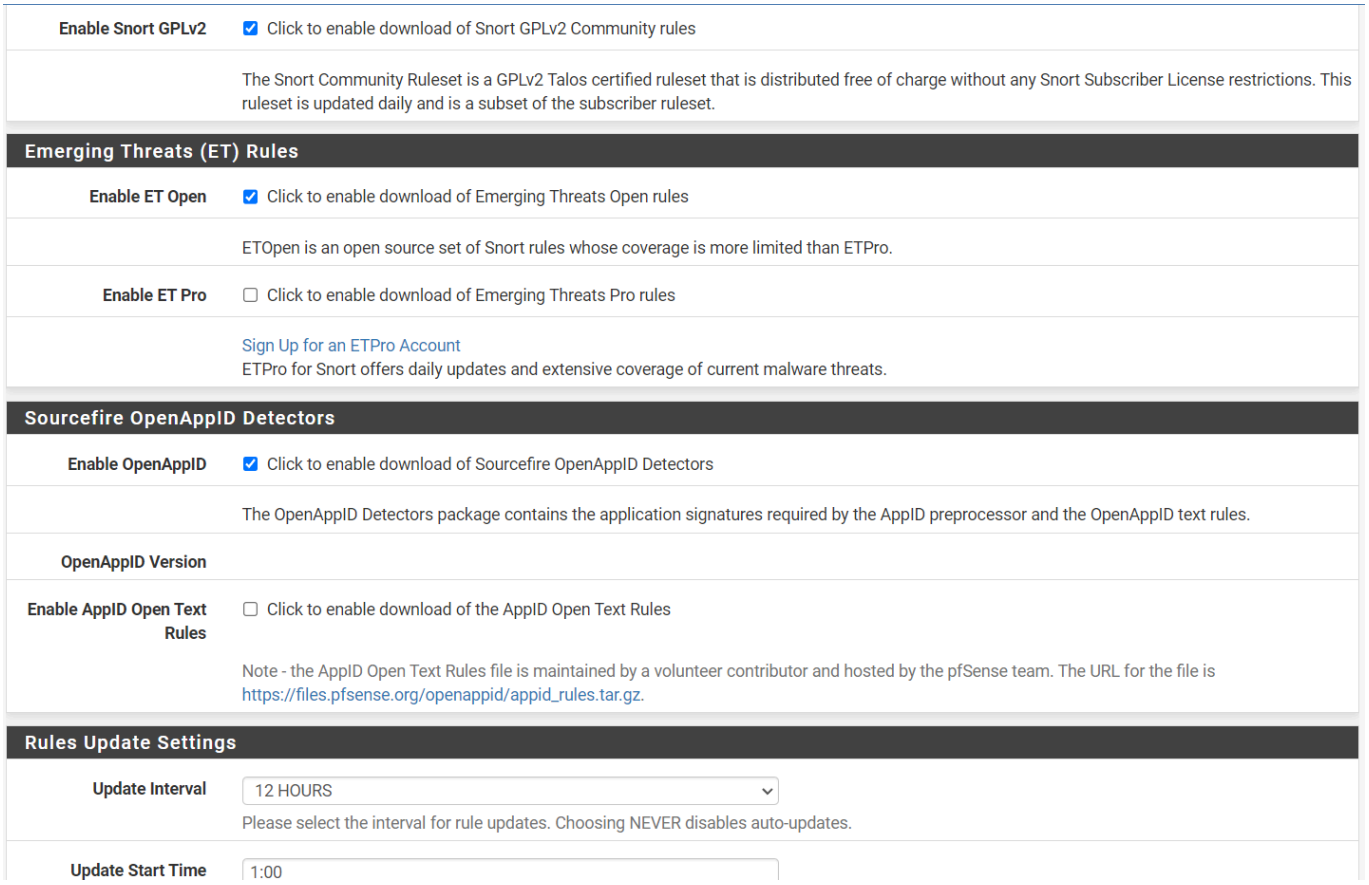


Ensuite nous pouvons cocher les cases :

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

Puis, 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

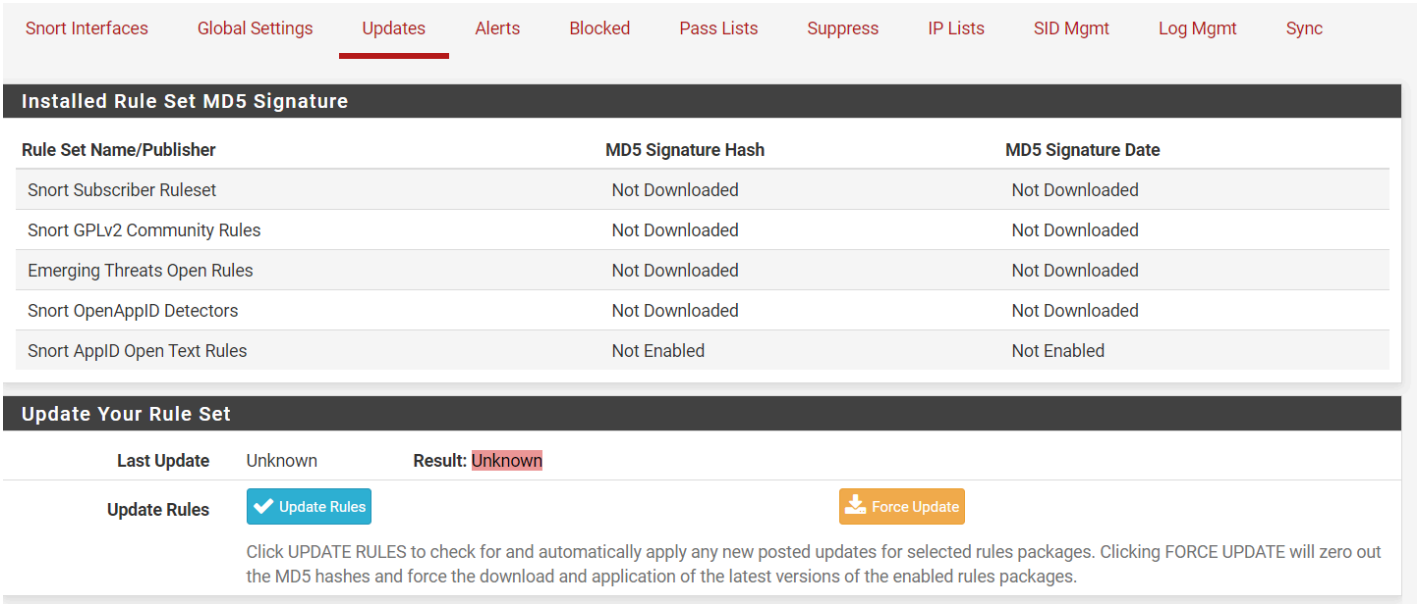
règles:

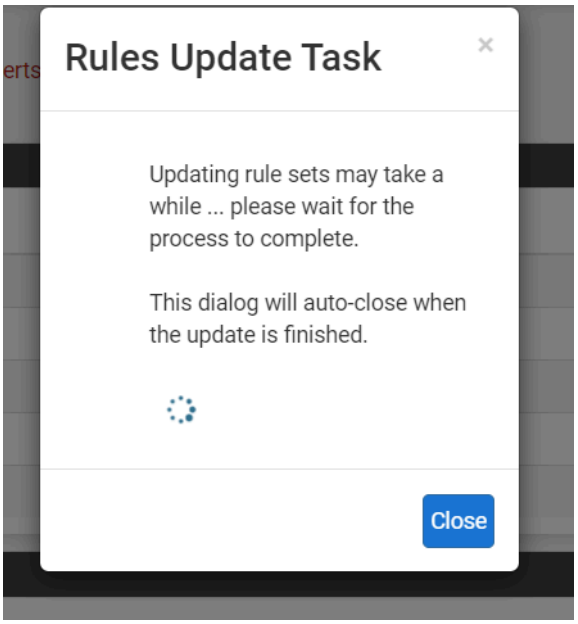


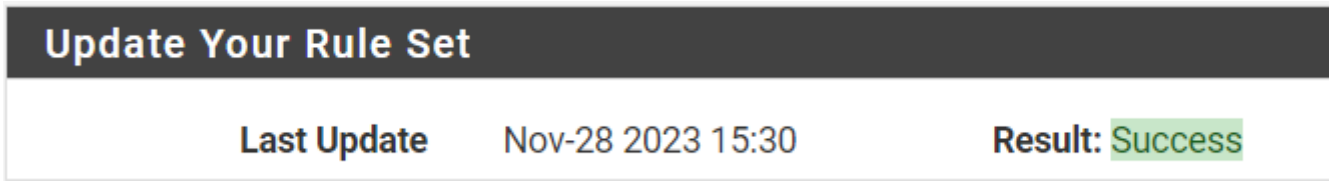
Dans notre cas l'intervalles des mise à jour sera de 12h minimum et l'heure de mise à jour sera 1h du matin pour ne pas gêner l'activité des collaborateurs

Ne pas oublier de sauvegarder le paramétrage

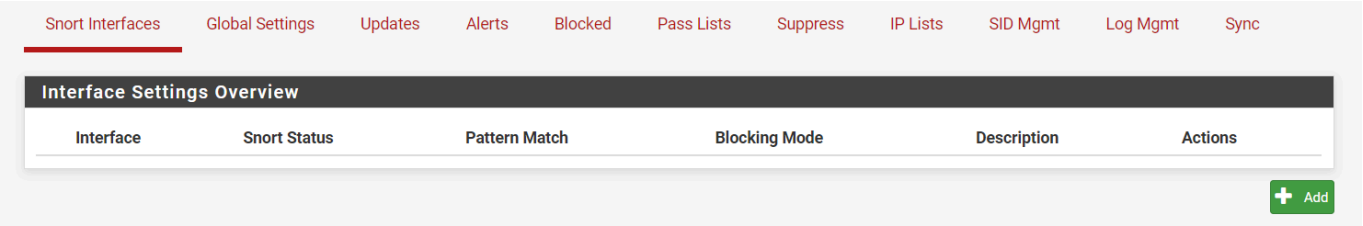
Une fois sauvegarder, nous pouvons nous rendre sur l'onglet Updates et manuellement mettre à jour les différentes règles que nous avons cochées précédemment en cliquant sur '"update rules" (dans notre cas cela prendra un peu de temps, car nous allons toutes les télécharger une première fois).



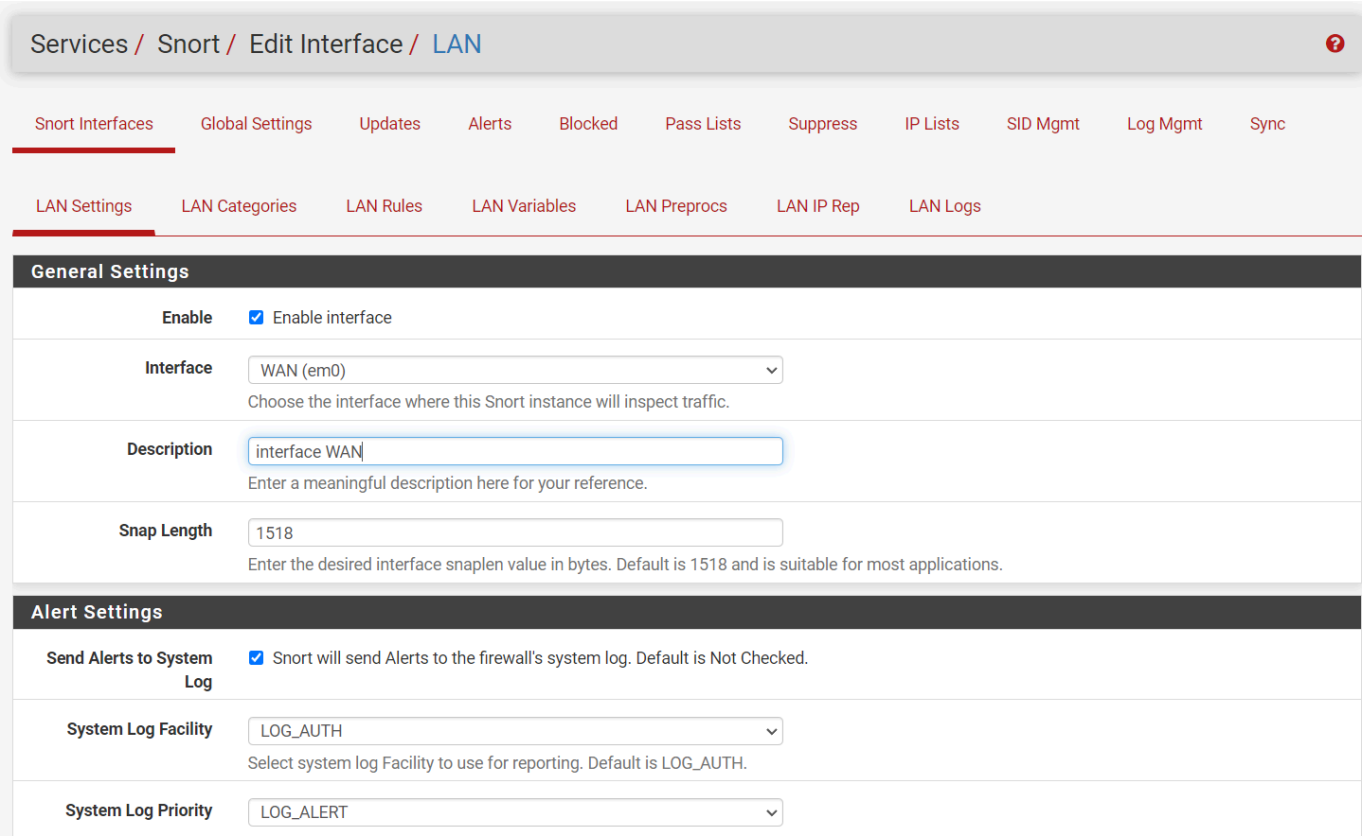




Maintenant que Snort est bien installé et configuré nous pouvons nous rendre sur “Snort interfaces” pour choisir l’interface (ou les interfaces) sur laquelle Snort va écouter et analyser le trafic et appuyer sur “add” pour ajouter:



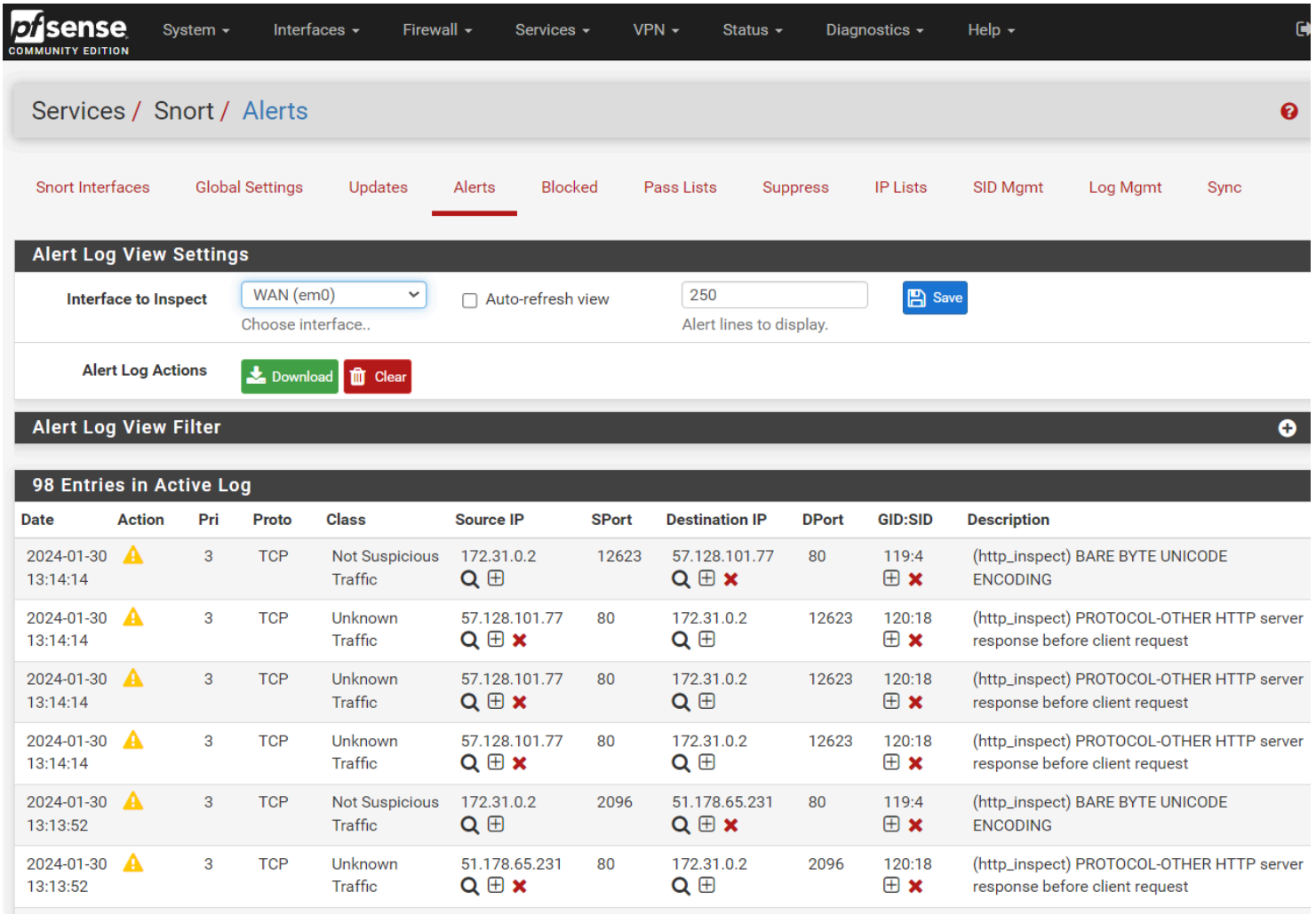
Ici nous choisissons donc l'interface que nous voulons surveiller, puis une description du réseau et ensuite nous cochons simplement le fait d'envoyer les alertes sur le système de log interne, pour les analyser en cas de tentative d'intrusion



A partir de ces options nous avons mis en place notre IDS car ils nous envoie les informations du pare-feu dans des logs consultables.

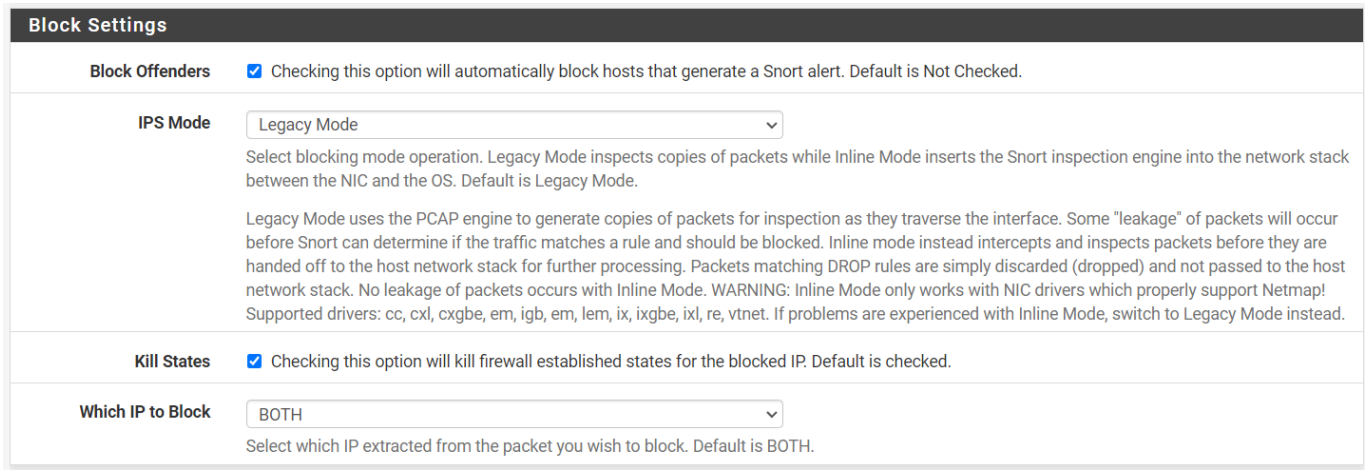
5. Test de Fonctionnement IDS

Maintenant que nous l'avons activé, en allant dans l'interface Service > Snort > Alerte ont peut observer les logs qui arrivent et qui nous prévient de toute connexion suspecte sur le réseau sans bloquer la connexion au réseau qu'il tente d'accéder.

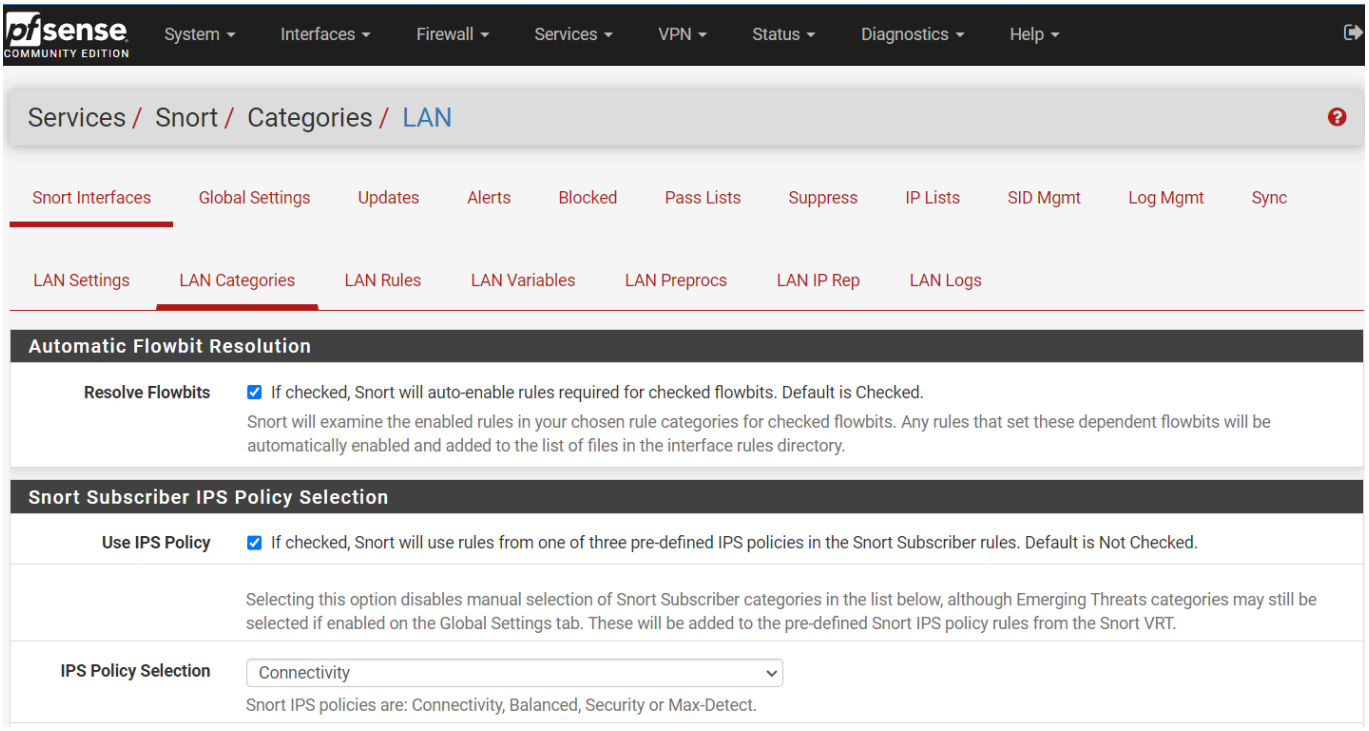


Maintenant nous allons faire de Snort un IPS, en cochant la case "Block Offenders "

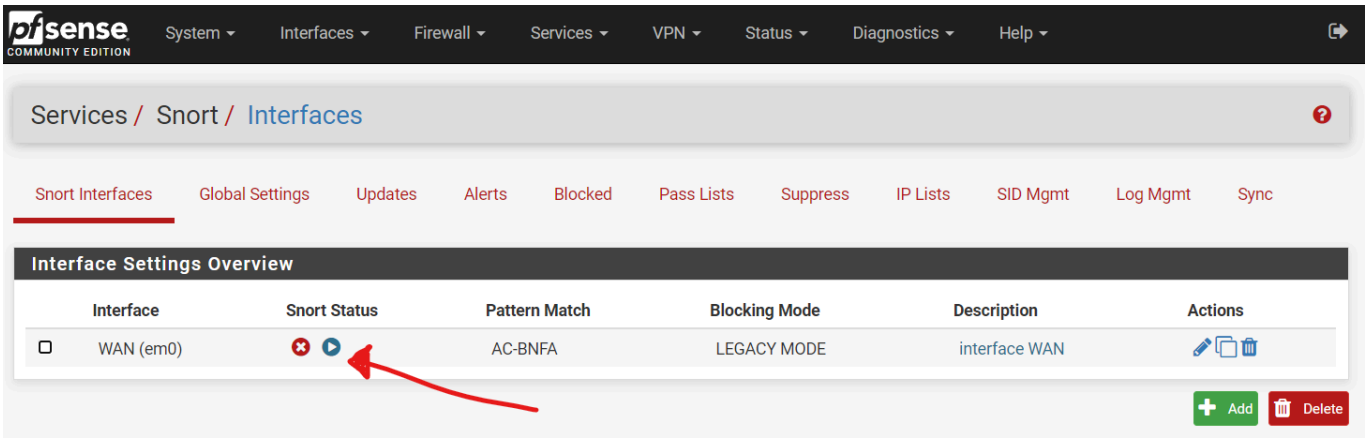
En faisant cela, Snort va donc bloquer les hôtes générant des alertes automatiquement



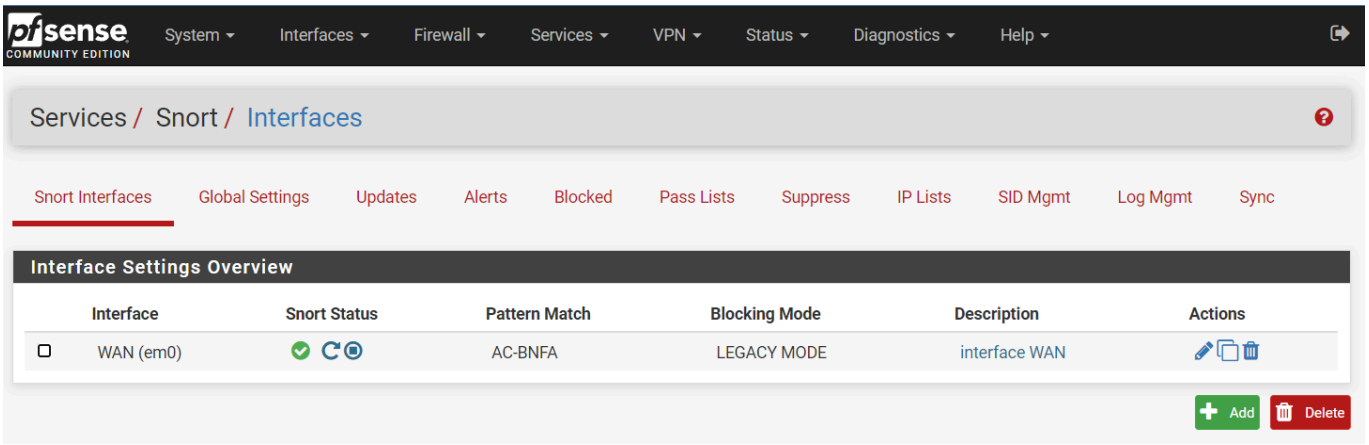
Maintenant nous pouvons activer toutes les règles précédemment téléchargées en nous rendant sur Snort Interfaces, LAN catégorie et cocher l'option Use IPS Policy. Bien penser à sauvegarder les paramètres.



Une fois les règles activer et sauvegarder nous pouvons retourner sur Snort l'interface et le démarrer:



Une fois démarré il est dans cette état:



Voilà l'IPS est en place, nous pouvons voir les logs dans alerte et les différentes options nous permettent de gérer en temps réel les entrées et sorties de notre réseau WAN.

6. Test de fonctionnement IPS

Maintenant que nous avons mis en place l'IPS nous pouvons vérifier qu'il fonctionne en allant dans Service > Snort > blocked Hosts. Ici on retrouve tous les host qui se sont fait bloquer par l'IPS, c'est hosts bloquer ont également créer des logs dans l'interface "Alerte" mais cela ne nous intéresse pas car ils sont

directement bloquer et ne peuvent donc pas entrer sur le réseau.