Procédure PFSense - Snort Installation

- Ouvrez un logiciel de navigateur, entrez l'adresse IP de votre pare-feu Pfsense et accédez à l'interface Web.

- Dans le contexte HSP, l'URL suivante a été saisie dans le navigateur :

https://172.16.0.101

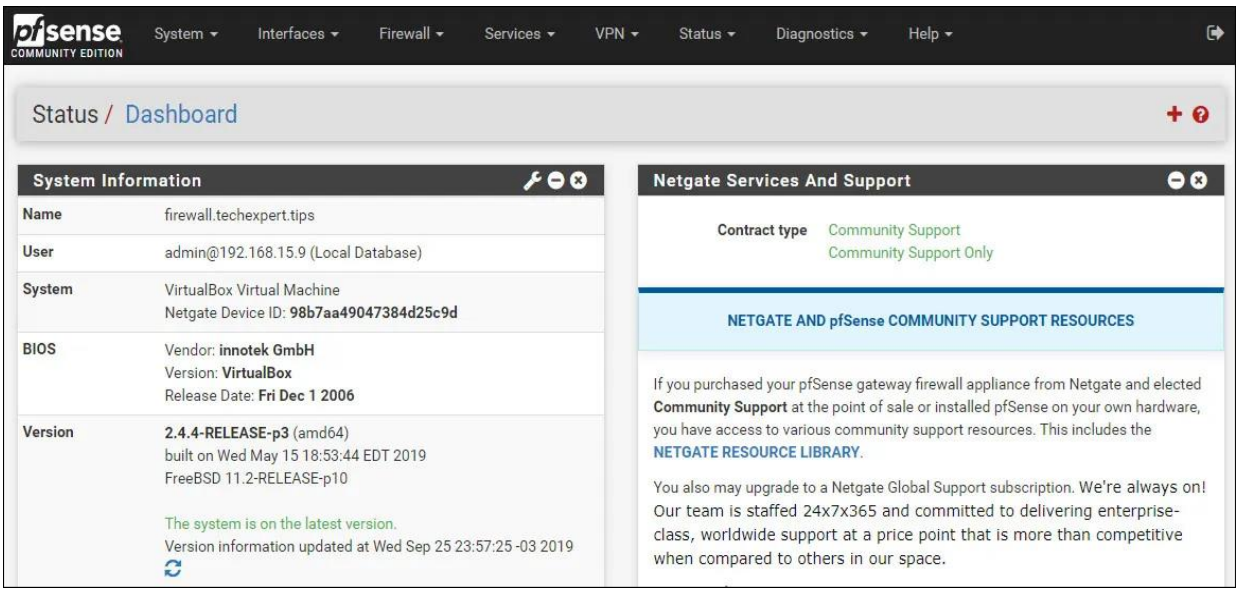
L'interface web Pfsense doit être présentée.

- Sur l'écran rapide, entrez les informations de connexion Pfsense Default Password.

• Username : pfsense

●Mot de passe : **********

Après une connexion réussie, vous serez envoyé au tableau de bord Pfsense.



- Accéder au menu Pfsense System et sélectionner l'option De gestionnaire de paquets.

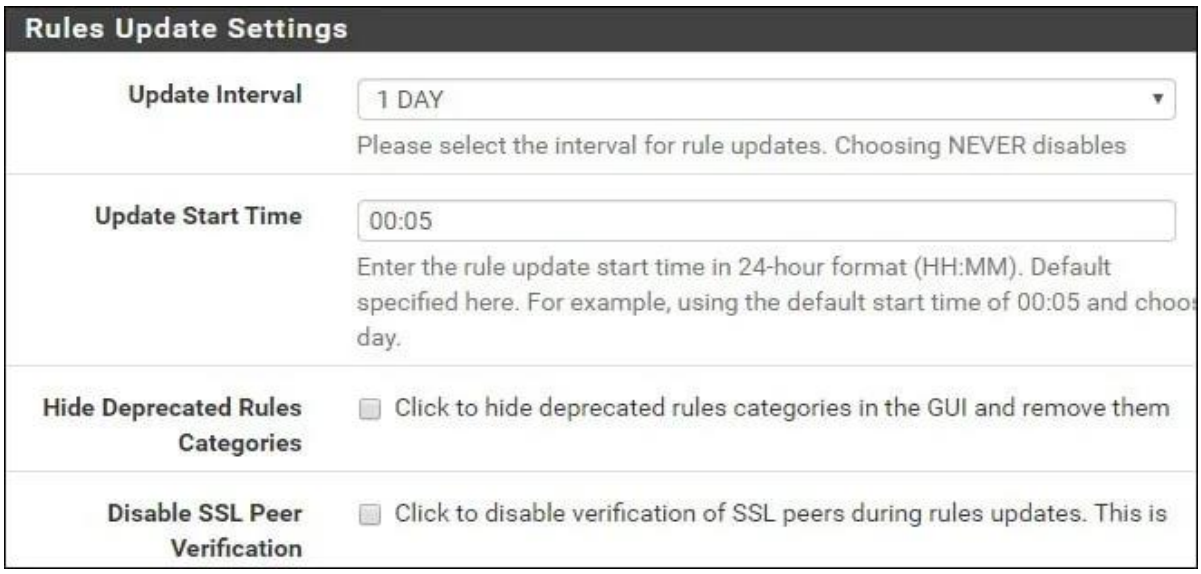
- Sur l'écran du gestionnaire de paquets, accéder à l'onglet Paquets disponibles.
- Sur l'onglet Paquets disponibles, recherchez SNORT et installer le paquet SNORT.

- Dans notre exemple, nous avons installé la version 3.2.9.10 du paquet SNORT.
- Attendre la fin de l'installation SNORT.
- Accéder au menu Pfsense Services et sélectionnez l'option SNORT.

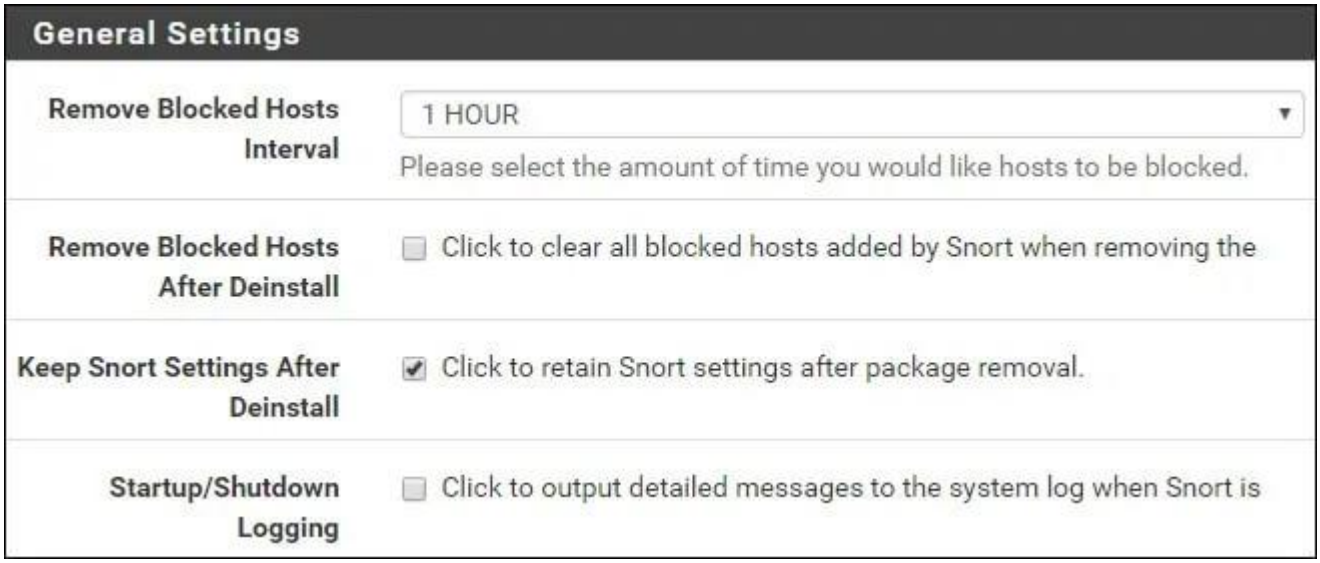
- Sur l'onglet Paramètres Global, localisez les règles d'abonné SNORT et effectuez la configuration suivante :
- Activer Snort VRT - Oui
  > accédez au site Web Snort, créez un compte et obtenez un Oinkcode gratuit.

> Localiser la zone Paramètres de mise à jour des règles et effectuer la configuration suivante :

- Intervalle de mise à jour - Sélectionnez l'intervalle de mise à jour souhaité
- Heure de démarrage de mise à jour - Définir l'heure désirée pour mettre à jour les règles Snort

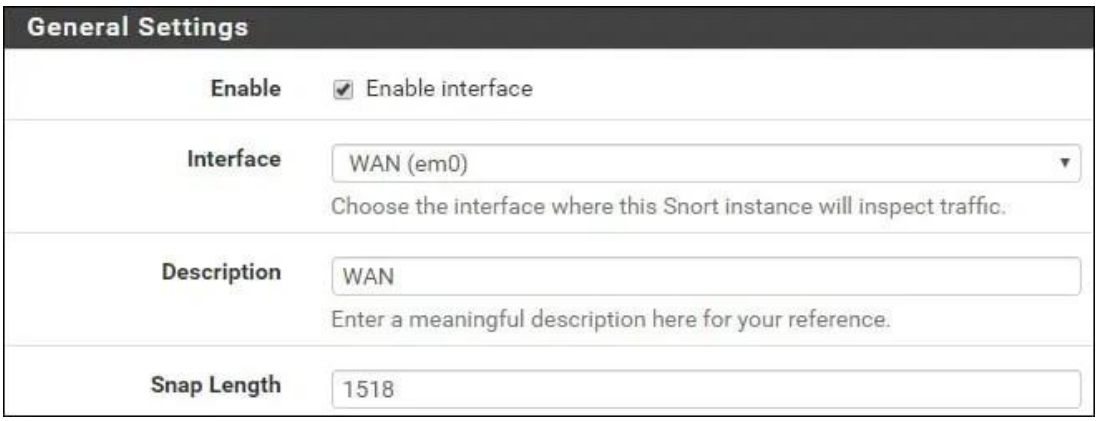


- Localiser la zone Paramètres généraux et effectuer la configuration suivante :
- Supprimer l'intervalle des hôtes bloqués - 1 heure
- Supprimer les hôtes bloqués après la désinstallation – Non
- Conserver les paramètres snort après la désinstallation – Oui
- Intervalle de mise à jour de démarrage/shutdown - non



- Sur l'onglet Mises à jour, cliquez sur le bouton Règles de mise à jour pour télécharger les règles Snort.

- Sur l'onglet Interfaces Snort, cliquez sur le bouton Ajouter et effectuez la configuration suivante.
- Activer – Oui
- Interface - Sélectionnez l'interface désirée pour surveiller



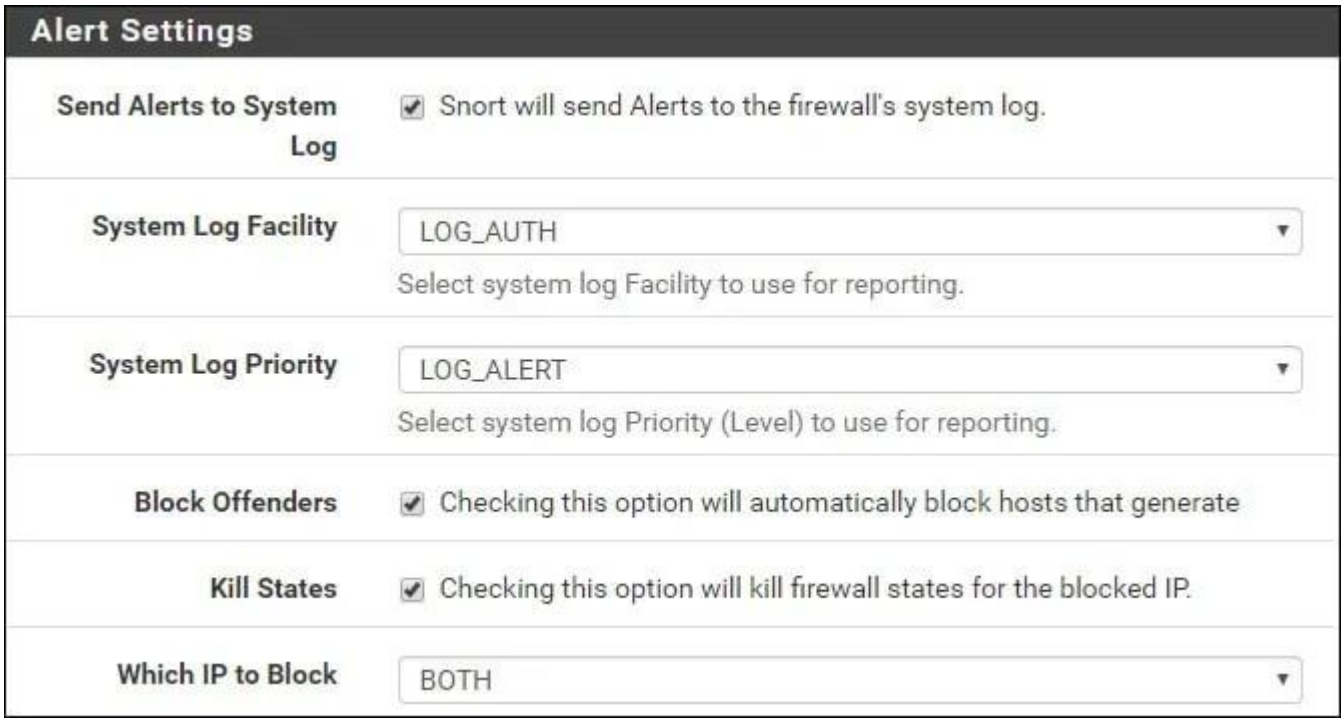
➢ Localiser la zone Paramètres d'alerte et effectuer la configuration suivante :

Envoyer des alertes au journal du système - Oui

- Bloquer les contrevenants - Activer si vous voulez bloquer les délinquants

États de tuer - Oui

Quel IP bloquer - BOTH



➢ Après avoir terminé la configuration, cliquez sur le bouton Enregistrer.

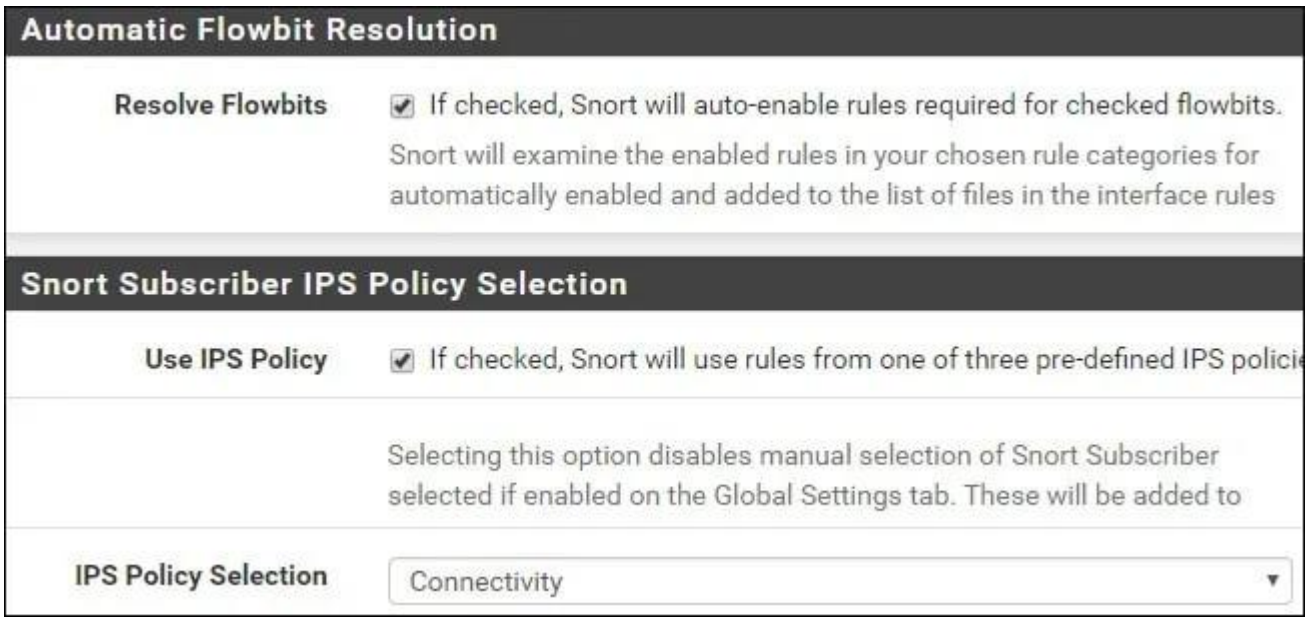
➢ Sur l'écran des interfaces Snort, modifiez la configuration de l'interface.

➢ Accédez à l'onglet Catégories Wan et effectuez la configuration suivante :

Résoudre les débits - Oui

- Utiliser la politique IPS - Oui

Sélection des politiques IPS - Connectivité



- Dans notre exemple, nous avons activé la fonctionnalité IPS et sélectionné la stratégie nommée **Connectivité**.
- Après avoir terminé la configuration, cliquez sur le bouton Enregistrer et démarrez le service Snort sur l'interface.

SNORT est désormis installé sur PFSense