Documentation technique

27/02/2024

Installation et configuration d'un système de détection des intrusions

Sommaire

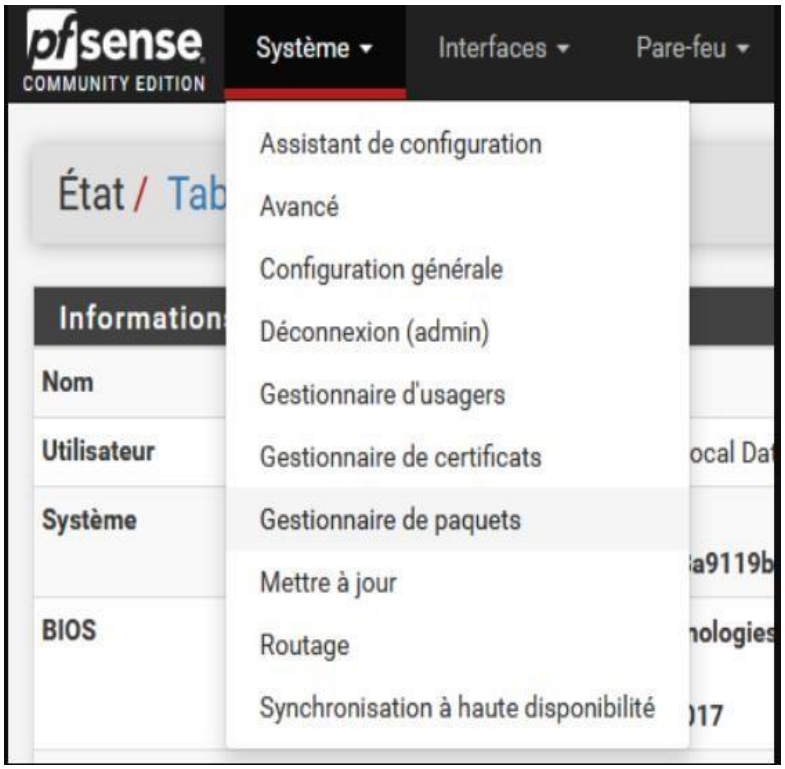
Définition

Snort est un système de détection d'intrusion (IDS) et de prévention d'intrusion (IPS) gratuit et open-source créé en 1998 par Martin Roesch.

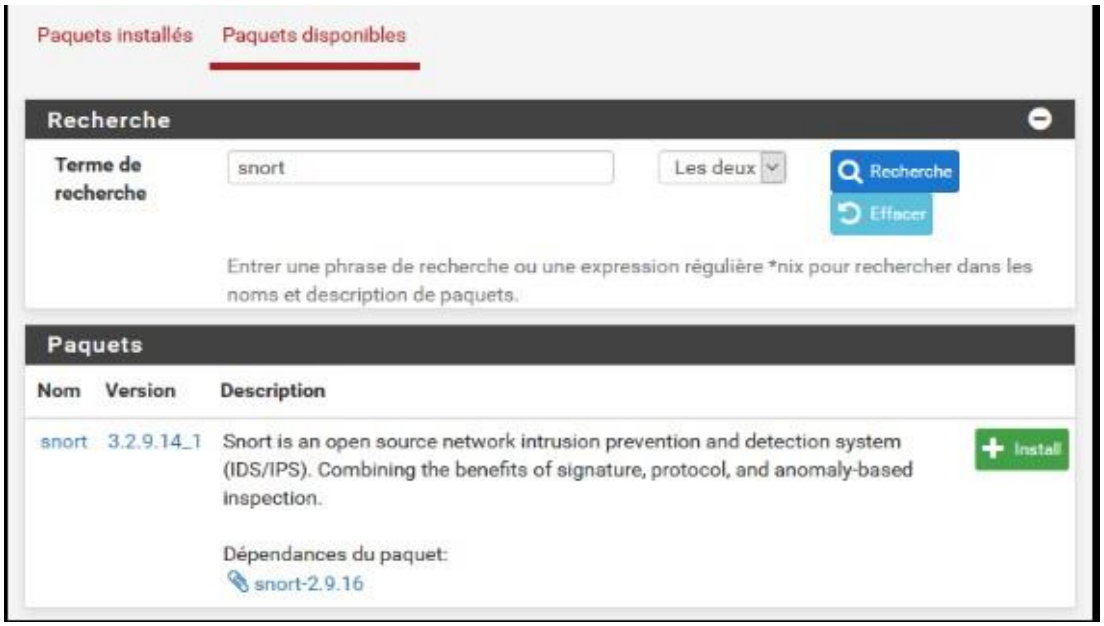
Développé à l'origine par la société Sourcefire, il est aujourd'hui maintenu par Cisco Systems à la suite du rachat de Sourcefire en 2013.

Installation de SNORT sur PfSense

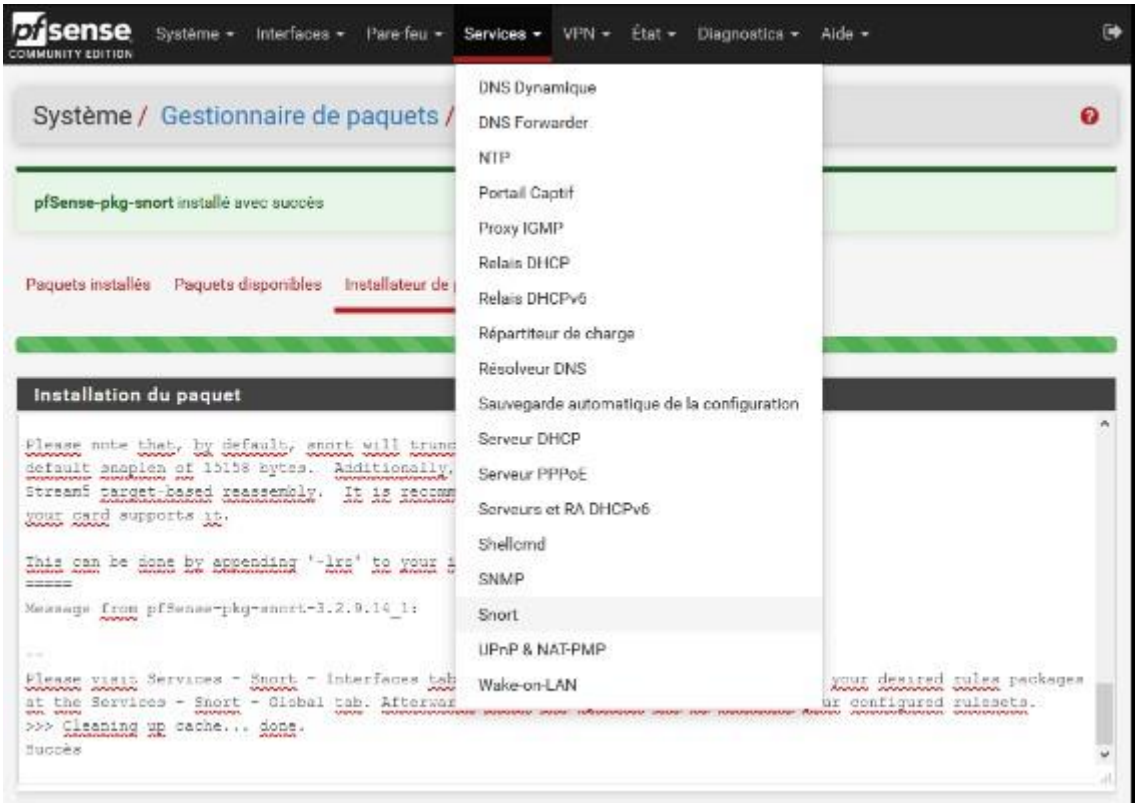
On va venir chercher SNORT dans le gestionnaire de paquets du menu principal.



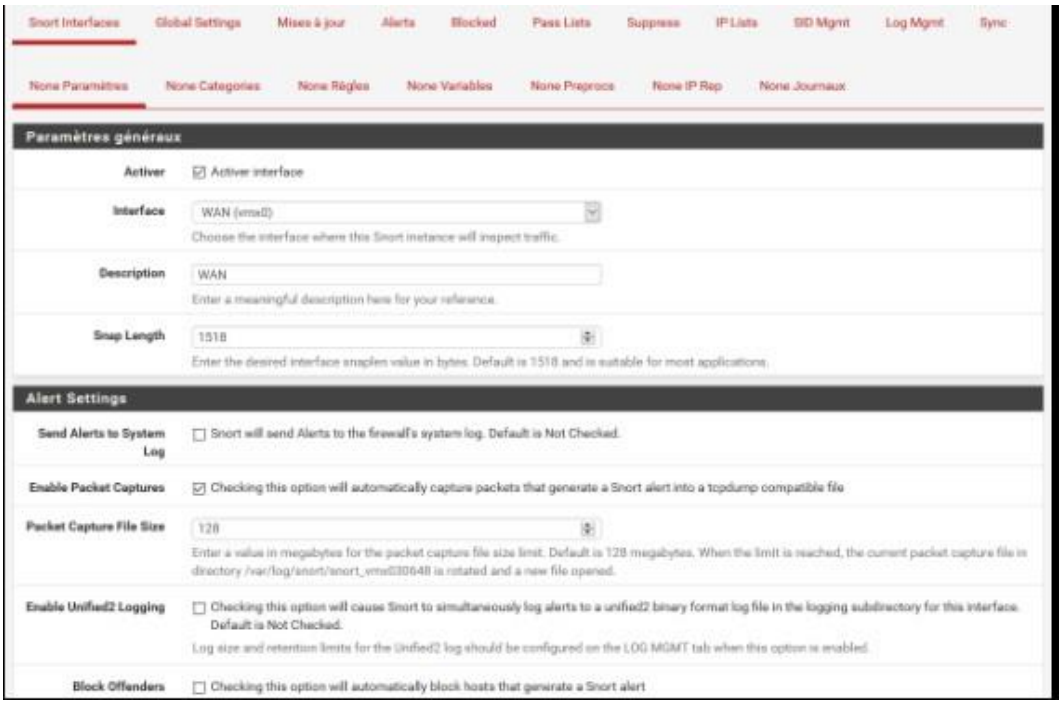
On va ensuite l'installer.



Après l'installation, on se rend dans SNORT, dans le menu 'services', puis 'Snort' :

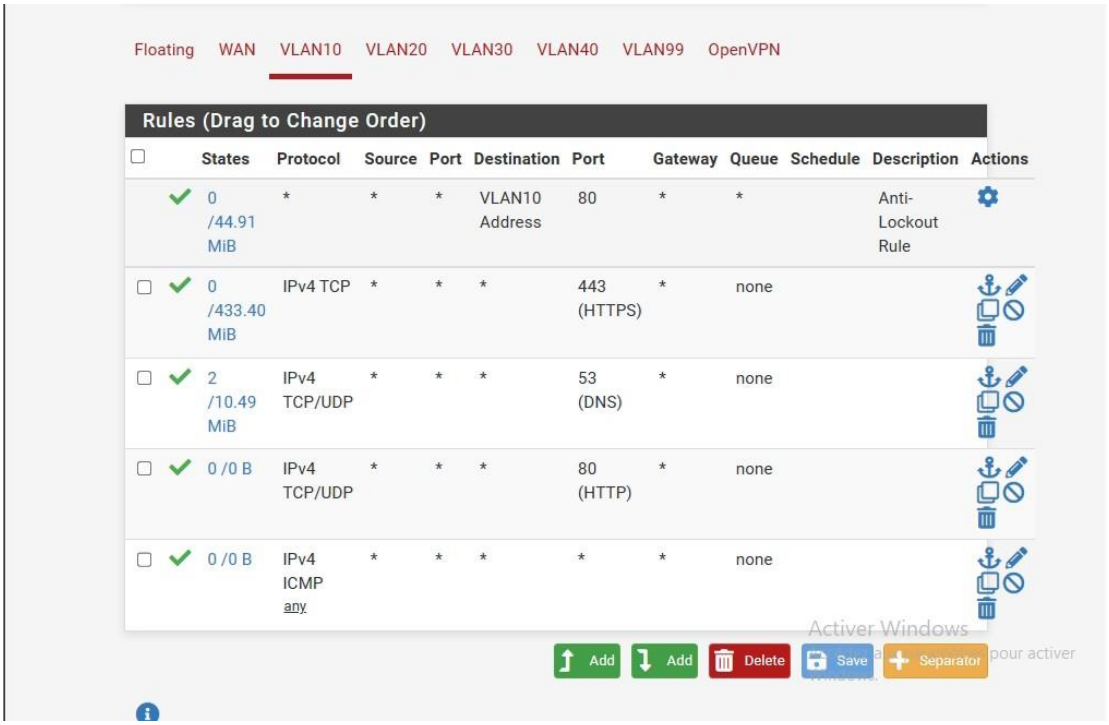


On choisit l'interface sur laquelle appliquer les paramètres :



Une fois que l'interface est choisie on va dans 'WAN categories', 'select all' puis on choisit toutes règles que l'on souhaite mettre en action.

Règles « Rules » mis en place sur le pare-feu :



Grâce à cela nous bénéficions d'alertes créées par nos règles :