|  |  |
| --- | --- |
|  |  |
| Documentation technique |  |
|  |  |
|  | 27/02/2024**Installation et configuration d’un système de détection des intrusions** |

### Sommaire

* Définition
* Installation de Snort sur PfSense

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  | 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.

Une image contenant texte, capture d’écran, logiciel, Police

Description générée automatiquement

On va ensuite l’installer.

Une image contenant texte, logiciel, Page web, Site web

Description générée automatiquement

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

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

On choisit l’interface sur laquelle appliquer les paramètres :

Une image contenant texte, nombre, capture d’écran, reçu

Description générée automatiquement

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 :

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

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

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement