SNORT

-

PFSENSE

Installation et configuration

TANET Margaux

CPI 2024-2025

Table des matières

Introduction :

Dans ce document, nous allons mettre en place Snort. Nous configurerons Snort pour que lors d'un ping envoyé, une alerte remonte.

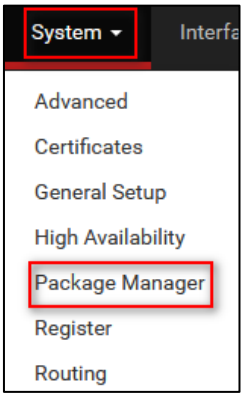
- **Qu'est-ce que Snort ?**

Snort est le premier système de prévention des intrusions (IPS) Open Source au monde. Snort IPS utilise une série de règles qui aident à définir l'activité réseau malveillante et utilisent ces règles pour trouver les paquets qui correspondent à celles-ci et génère des alertes pour les utilisateurs.

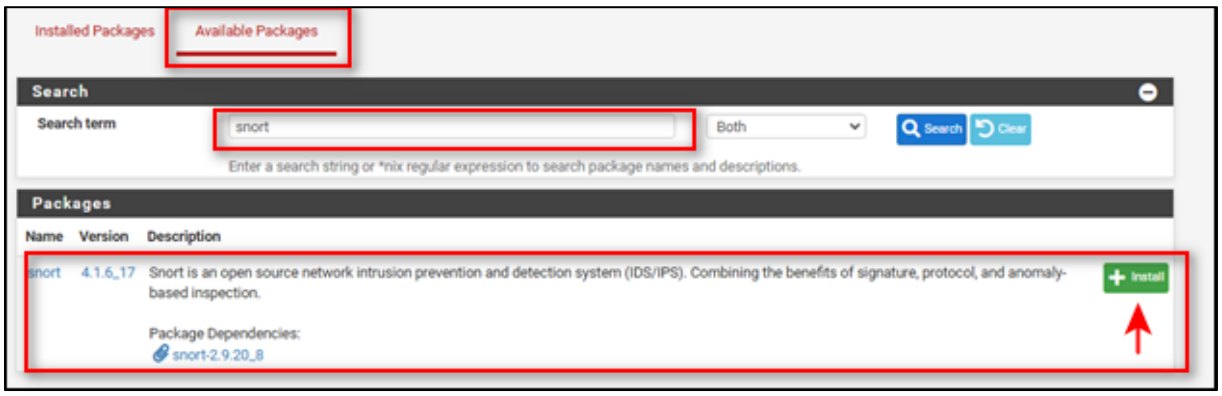
I- Installation du paquet Snort

Nous allons dans un premier temps installer le paquet **Snort**.

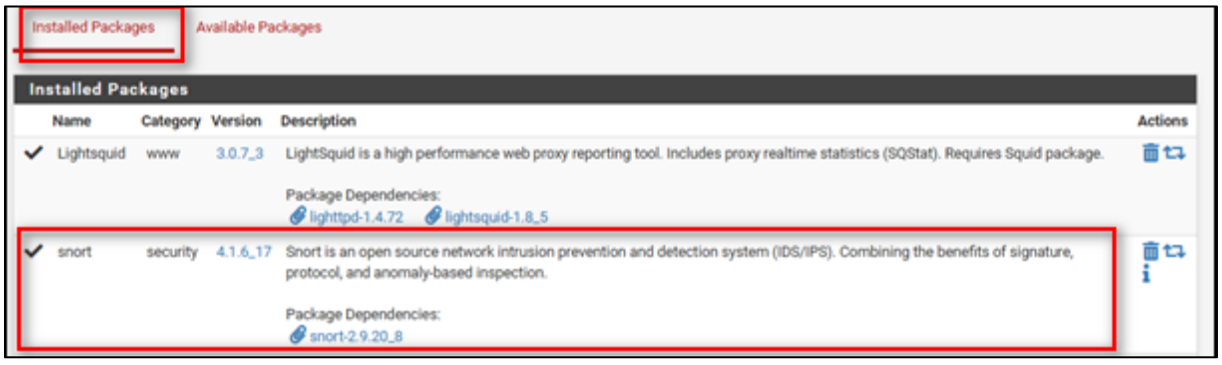
- Se rendre dans **System** puis **Package Manager**.



- Se rendre dans **Available Packages,** dans la barre de recherche taper **Snort** et installer le paquet :



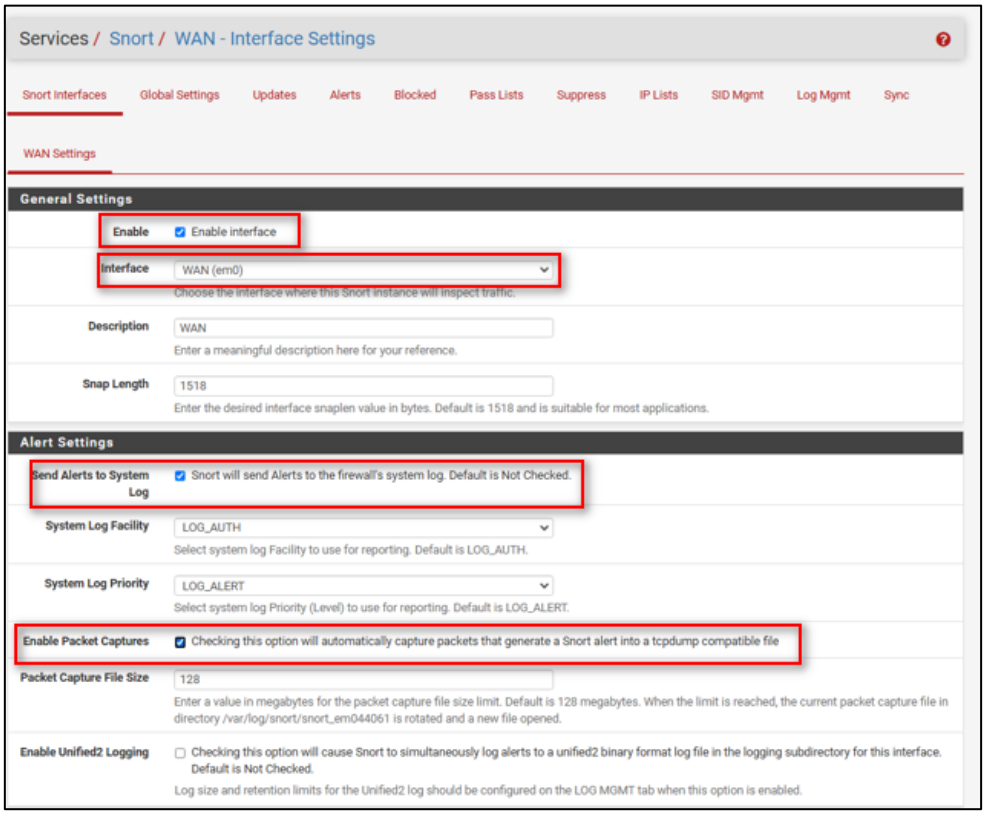
Le paquet a bien été installé :



II- Configuration de Snort

- Se rendre dans l'onglet **Services** puis cliquer sur **Snort**. Cliquer sur le bouton **Add** en bas :

- Dans les paramètres WAN, cocher les différentes cases : **enable interface, send alerts to system log** et **enable packet captures** :



En cochant l'option **send alerts to system log** cela permet à **Snort** d'envoyer des alertes détectées directement dans le journal système du pare-feu (syslog).

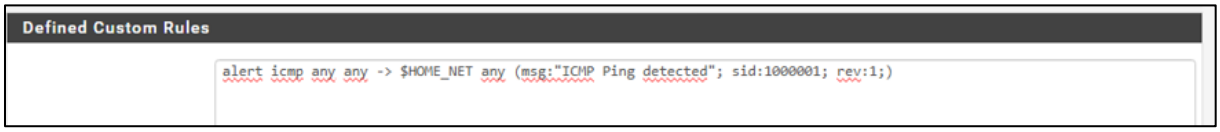
Enable Packet Capture permet de capturer et d'enregistrer les paquets qui déclenchent les alertes. Les paquets sont enregistrés dans un fichier qui peut être ensuite analyser avec des outils (exemple : Wireshark). Il permet de faire une analyse approfondie et donc de distinguer les véritables menaces des fausses.

III- Configuration de la règle ICMP

ICMP est utilisé pour le diagnostic réseau comme les commandes **ping** ou **traceroute**. C'est pourquoi, il est possible de créer des règles **ICMP** avec **Snort** pour surveiller, alerter ou bloquer certaines activités suspectes.

- Se rendre dans l'onglet **WAN Rules** et sélectionner dans les **Catégories, Custom.rules**.

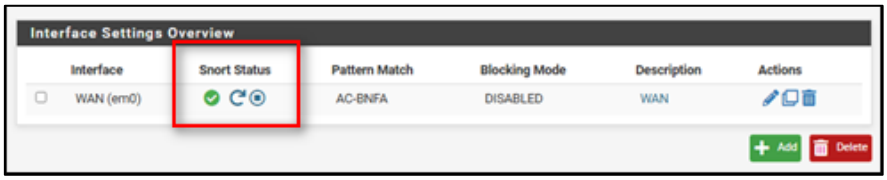
- En dessous, définir une règle qui activera une alerte sur le ping :



La règle : *alert icmp any any -> $HOME_NET any (msg:"ICMP Ping detected"; sid:1000001; rev:1;)*

Cette règle génère une alerte lorsqu'elle est déclenchée. Elle concerne les paquets ICMP. La source peut venir de n'importe quelle adresse IP, même chose pour le port (any any). La destination est le réseau interne sans port définit ($HOME_NET). Quand un paquet correspond à cette règle, un message **"ICMP Ping detected"** est affiché dans les logs.

- Ensuite, il faut activer l'interface :



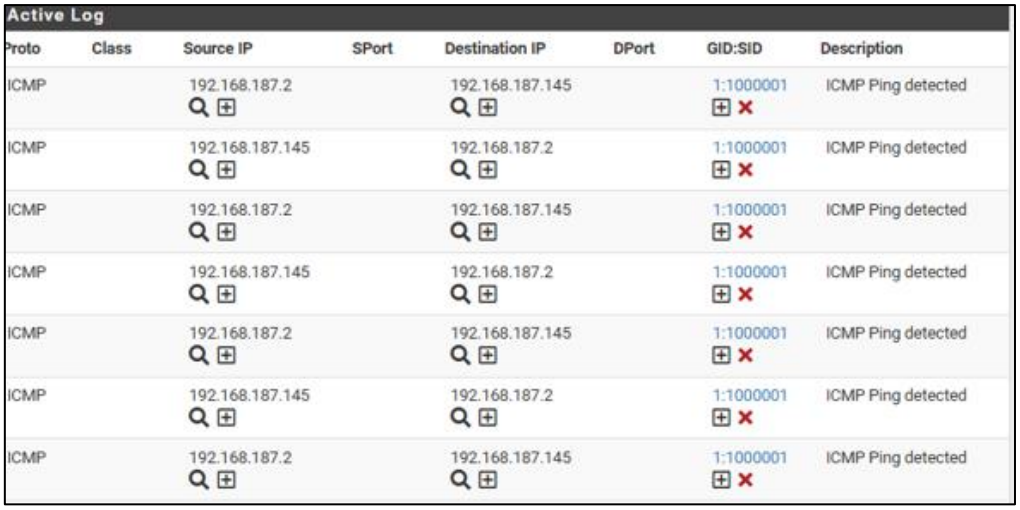
IV- Tests

Nous allons effectuer un ping d'une machine cliente sur la patte WAN de PfSense pour simuler une requête :

```
user@labb:~$ ping 192.168.187.145
PING 192.168.187.145 (192.168.187.145) 56(84) bytes of data.
64 bytes from 192.168.187.145: icmp_seq=1 ttl=64 time=0.799 ms
64 bytes from 192.168.187.145: icmp_seq=2 ttl=64 time=0.762 ms
64 bytes from 192.168.187.145: icmp_seq=3 ttl=64 time=1.47 ms
64 bytes from 192.168.187.145: icmp_seq=4 ttl=64 time=0.439 ms
```

Se rendre sur notre interface web PfSense de nouveau. Nous allons regarder si nous avons reçu des alertes.

- Se rendre dans l'onglet **Alerts :**



Active Log

Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
ICMP		192.168.187.2		192.168.187.145		1:1000001	ICMP Ping detected
ICMP		192.168.187.145		192.168.187.2		1:1000001	ICMP Ping detected
ICMP		192.168.187.2		192.168.187.145		1:1000001	ICMP Ping detected
ICMP		192.168.187.145		192.168.187.2		1:1000001	ICMP Ping detected
ICMP		192.168.187.2		192.168.187.145		1:1000001	ICMP Ping detected
ICMP		192.168.187.145		192.168.187.2		1:1000001	ICMP Ping detected
ICMP		192.168.187.2		192.168.187.145		1:1000001	ICMP Ping detected

Nous recevons bien des alertes, la règle a bien été configurée.

V- Conclusion

Nous avons mis une règle ICMP en place pour que lors d'envoi de ping on reçoive une alerte. La règle a été correctement configurée.