

# Documentation technique

*27/02/2024  
Installation et  
configuration d'un  
système de  
détection des  
intrusions*

# Sommaire

- Définition
- Installation de Snort sur PfSense

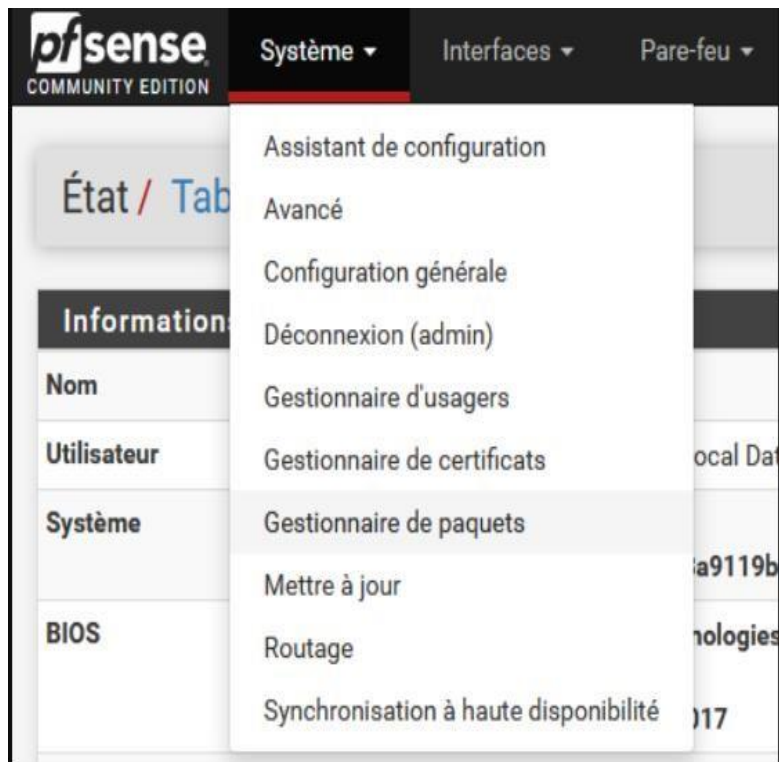
# Définition

*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.*

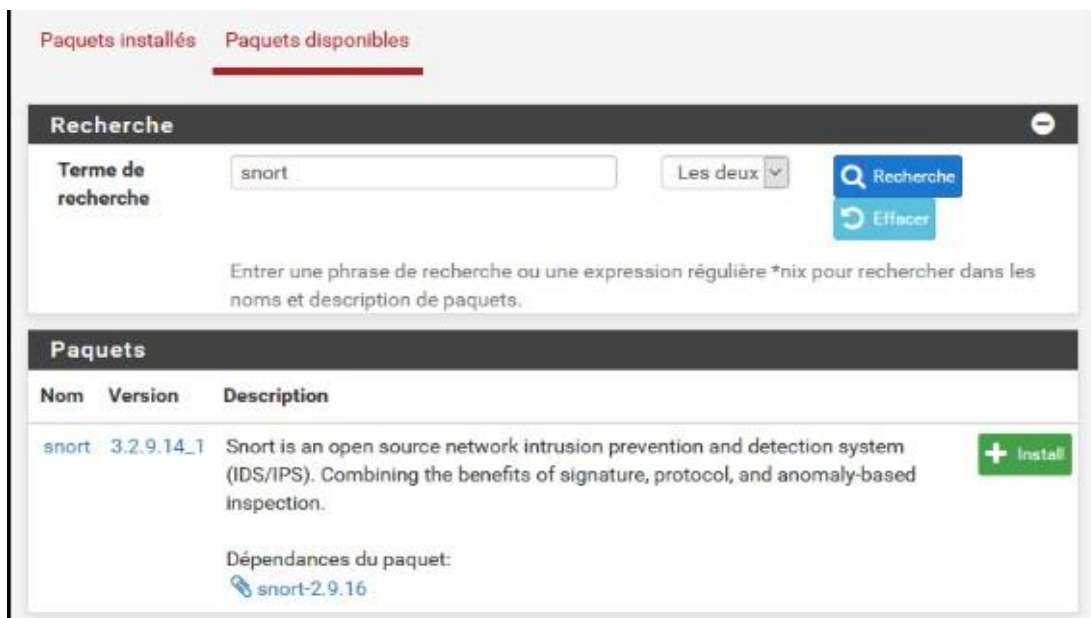
*Développé à l'origine par la société Sourcefire, il est aujourd'hui maintenu par Cisco Systems à la suite du rachat de Sourcefire en 2013.*

# Installation de SNORT sur PfSense

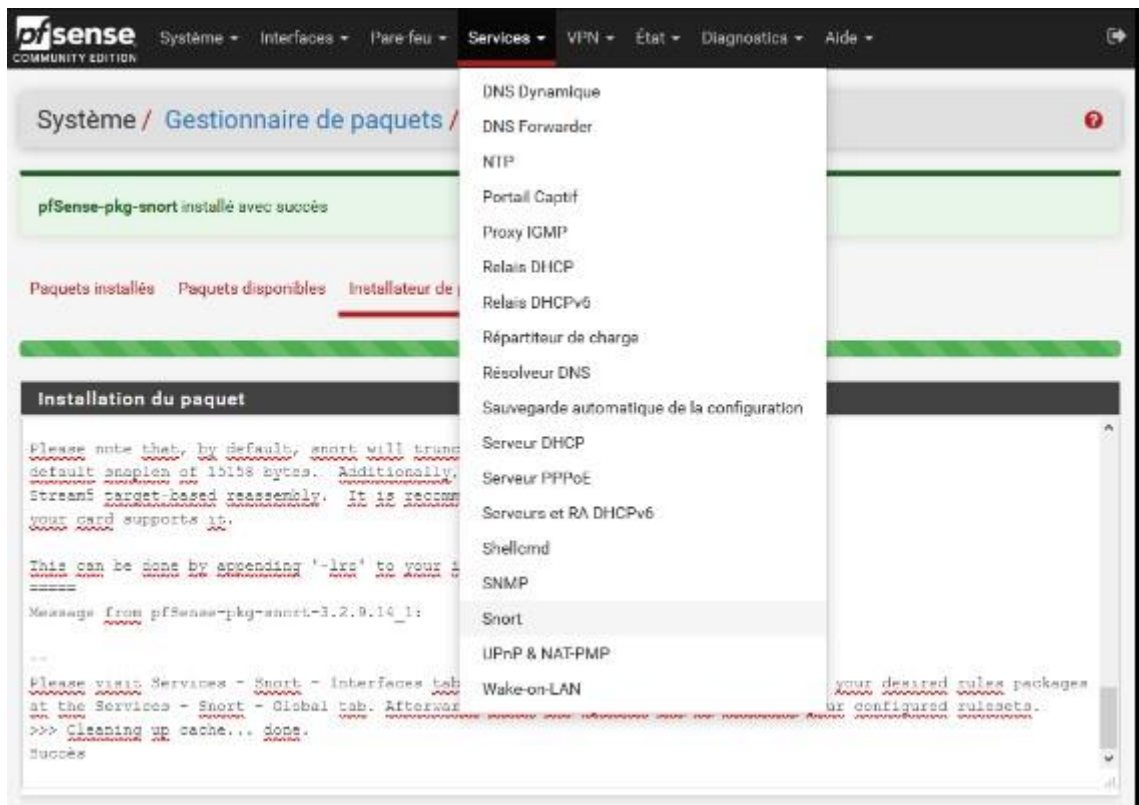
On va venir chercher SNORT dans le gestionnaire de paquets du menu principal.



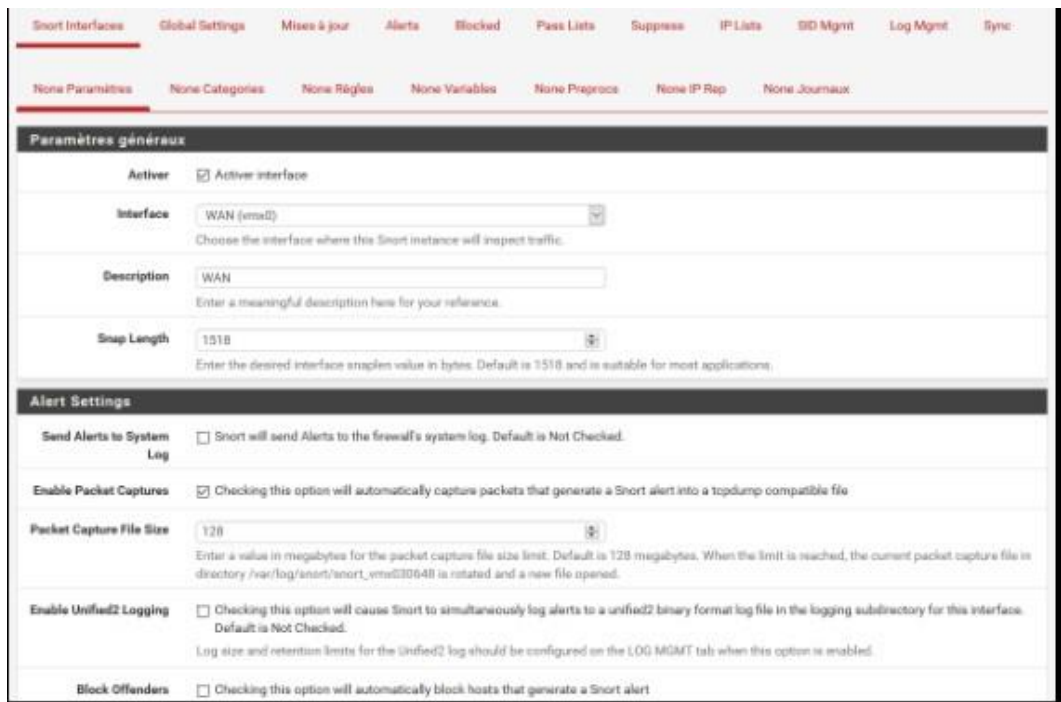
On va ensuite l'installer.



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 :

FloatingWANVLAN10VLAN20VLAN30VLAN40VLAN99OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0 /44.91 MiB	*	*	*	VLAN10 Address	80	*	*		Anti- Lockout Rule	
<input type="checkbox"/>	0 /433.40 MiB	IPv4 TCP	*	*	*	443 (HTTPS)	*	none			 
<input type="checkbox"/>	2 /10.49 MiB	IPv4 TCP/UDP	*	*	*	53 (DNS)	*	none			 
<input type="checkbox"/>	0 / 0 B	IPv4 TCP/UDP	*	*	*	80 (HTTP)	*	none			 
<input type="checkbox"/>	0 / 0 B	IPv4 ICMP any	*	*	*	*	*	none			 

Add

Add

Delete

Save

Separator

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

Alert Log View Settings

Interface to Inspect

VLAN10 (▼)  
Choose interface..

☐ Auto-refresh view

250  
Alert lines to display.

Save

Alert Log Actions

Download

Clear

Alert Log View Filter

12 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID
2023-04-27 14:46:38		1	UDP	Attempted User Privilege Gain	8.8.8.8	53	192.168.10.5	57038	3:1
2023-04-27 14:44:39		3	TCP	Unknown Traffic	10.74.1.109	80	192.168.10.11	59092	120