



Document d'exploitation

Table des matières

1. Définition
2. Prérequis
3. Installation
4. Configuration

Intallation du SNORT :

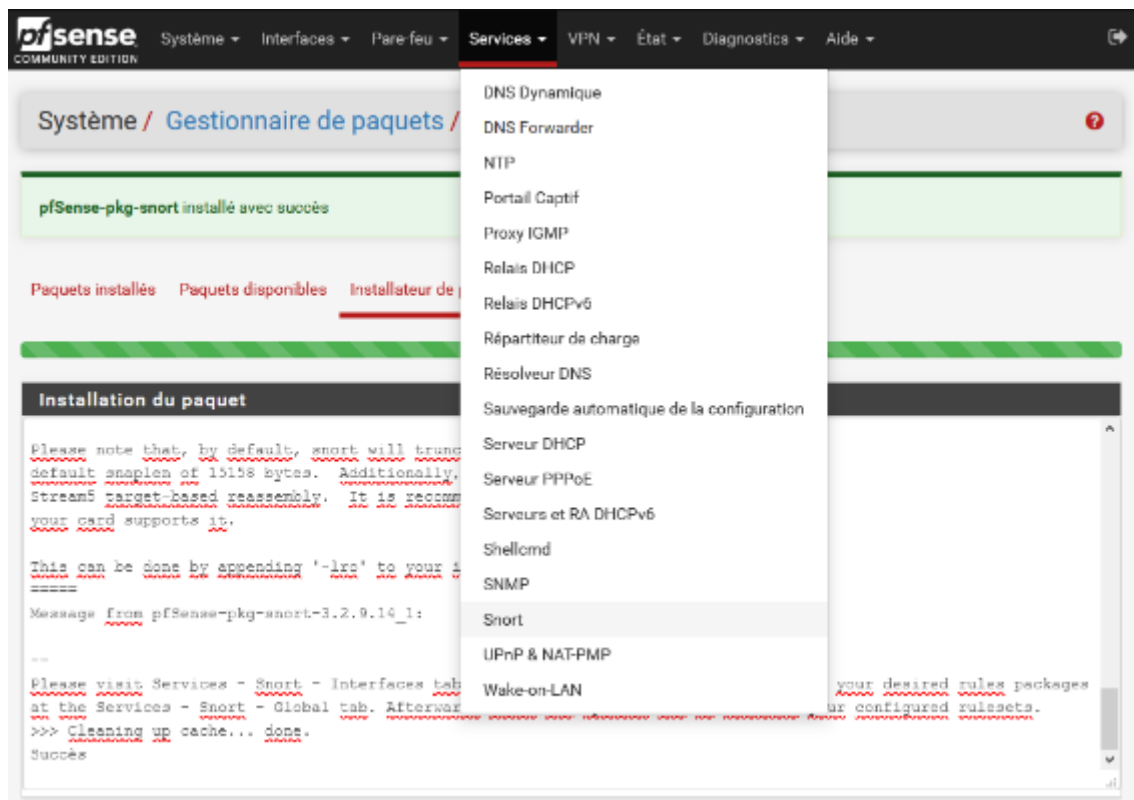
On va venir chercher SNORT dans les gestionnaires de paquets du menu principal.



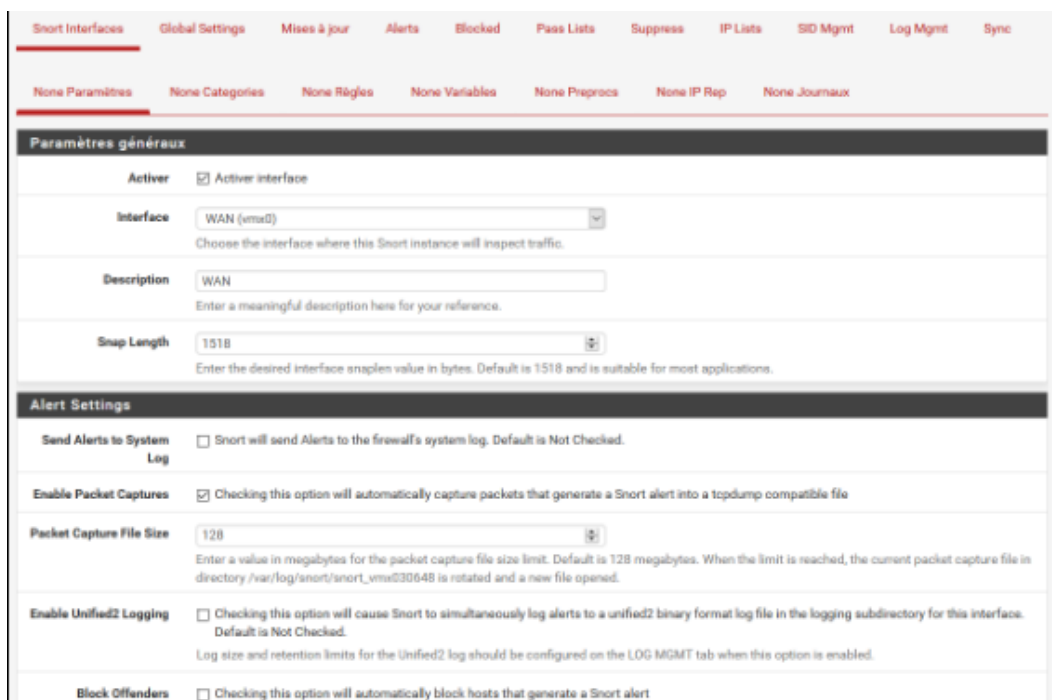
Installation du SNORT via Pfsense :



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



Choisir l'interface sur laquelle appliquer les paramètres :



Une fois que l'interface est choisit 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 au NAS :

Floating WAN **VLAN10** VLAN20 VLAN30 VLAN40 VLAN99 OpenVPN

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input 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	*	*	*	*	*	none			

↑ Add ↓ Add Delete Save + Separator

Activer Windows pour activer

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

Alert Log View Settings

Interface to Inspect: VLAN10 (v) Choose interface.. Auto-refresh view: ☐ Alert lines to display: 250 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

Activer Windows Accédez aux paramètres pour activer Windows.