



Installation et configuration

TANET Margaux

CPI 2024-2025

Table des matières

I-	Installation du paquet Snort	. 3
II-	Configuration de Snort	. 3
111-	Configuration de la règle ICMP	. 5
IV-	Tests	. 5
V-	Conclusion	. 6

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 :

Instal	led Packag	Available Packages
Sear	ch	•
Searc	:h term	snort Both V Q Search Clear
		Enter a search string or *nix regular expression to search package names and descriptions.
Pack	ages	
Name	Version	Description
snort	4.1.6_17	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly- based inspection.
		Package Dependencies:

Le paquet a bien été installé :

Į	Installed Packages Available Packages										
	Installed Pa	ckages									
	Name	Category	Version	Description	Actions						
•	 Lightsquid 	www	3.0.7_3	LightSquid is a high performance web proxy reporting tool. Includes proxy realtime statistics (SQStat). Requires Squid package. Package Dependencies: Ø lightspuid-1.4.72 Ø lightsquid-1.8.5	首ね						
	snort	security	4.1.6_17	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection. Package Dependencies: Ø snort-2.9.20_8	亩ta i						

II- Configuration de Snort

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

Services - VPN -												
Auto Config Backup												
Captive Portal												
DHCP Relay												
DHCP Server												
DHCPv6 Relay												
DHCPv6 Server												
DNS Forwarder												
DNS Resolver												
Dynamic DNS												
IGMP Proxy	Services / S	Snort / Interfac	es									0
NTP	Sport Interfaces	Global Settings	Undates	Alerte	Blocked	Page Liste	Suppress	ID Lists	SID Mont	Log Mant	Sume	
PPPoE Server		-	opanies		broches		ooppiess.		olo ingrit	e gangan	ojne	
Router Advertisement	Interface Sett	ings Overview										
SNMP	Interface	Snort Status		Pattern M	Match	Block	ing Mode		Description	Act	tions	_
Snort												• ^44

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

Services / Snort /	/ WAN - Interface Settings
Snort Interfaces Glob	val Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync
WAN Settings	
General Settings	
Enable	C Enable Interface
Interface	WAN (em0) Choose the interface where this Short instance will inspect traffic
Description	WAN Enter a meaningful description here for your reference.
Snap Length	1518 Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.
Alert Settings	
Send Alerts to System Log	Short will send Alerts to the firewall's system log. Default is Not Checked.
System Log Facility	LOG_AUTH Select system log Facility to use for reporting. Default is LOG_AUTH.
System Log Priority	LOG_ALERT Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.
Enable Packet Captures	Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file
Packet Capture File Size	128 Enter a value in megabytes for the packet capture file size limit. Default is 128 megabytes. When the limit is reached, the current packet capture file in directory /var/log/snort/snort_em044061 is rotated and a new file opened.
Enable Unified2 Logging	Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked. Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

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.

CPI 2024-2025

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.

SNORT

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

Services / S	nort / Interfac	ce Settings	/ WAN	- Rules							0
Snort Interfaces	Global Settings	Updates	Alerts	Blocked	Pass Lists	Suppress	IP Lists	SID Mgmt	Log Mgmt	Sync	
WAN Settings	WAN Categories	WAN Rules	WAN V	ariables	WAN Preprocs	WAN IP Re	p WAN	Logs			
Available Rule	Categories										
Category Selec	ction: custom.ru	Jes				•					
-	Select the h	ule category to vi	ew and man	age.		_					

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

Defined Custom Rules							
	<pre>alert icmp any any -> \$HOME_NET any (msg:"ICMP Ping detected"; sid:1000001; rey:1;)</pre>						

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 :

Inte	rface Settings (Overview				
	Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
0	WAN (em0)	0 C 💿	AC-BNFA	DISABLED	WAN	/08
-						+ Add 🛅 Delete

IV- Tests

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

use	er@labl	o:~\$ p	oing	192.	168.	187.3	145					
PII	NG 192	.168.3	187.1	45 (192.	168.3	187.145)	56((84) by	tes of	data.	
64	bytes	from	192.	168.	187.	145:	icmp_sec	q=1	ttl=64	time=0	.799	ms
64	bytes	from	192.	168.	187.	145:	icmp_sec	q=2	ttl=64	time=0	.762	ms
64	bytes	from	192.	168.	187.	145:	icmp_sec	q=3	ttl=64	time=1	47 n	ns
64	bytes	from	192.	168.	187.	145:	icmp_sec	q=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									
Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description			
	192.168.187.2 Q 🛨		192.168.187.145 Q 🛨		1:1000001	ICMP Ping detected			
	192.168.187.145 Q ⊕		192.168.187.2 Q 🛨		1:1000001	ICMP Ping detected			
	192.168.187.2 Q 🛨		192.168.187.145 Q ⊕		1:1000001	ICMP Ping detected			
	192.168.187.145 Q 🛨		192.168.187.2 Q 🛨		1:1000001	ICMP Ping detected			
	192.168.187.2 Q ⊕		192.168.187.145 Q ⊞		1:1000001	ICMP Ping detected			
	192.168.187.145 Q ⊞		192.168.187.2 Q 🕀		1:1000001	ICMP Ping detected			
	192.168.187.2 Q 🛨		192.168.187.145 Q 🕀		1:1000001	ICMP Ping detected			
	Log Class	Log Class Source IP 192.168.187.2 Q	Log Source IP SPort 192.168.187.2 Q 192.168.187.2 192.168.187.145 Q 192.168.187.2 192.168.187.2 Q 192.168.187.2	Log SPort Destination IP 192.168.187.2 192.168.187.145 Q. 192.168.187.145 Q. Q. 192.168.187.145 Q. Q. 192.168.187.145 Q. Q. 192.168.187.2 Q. Q. 192.168.187.2 Q. Q. 192.168.187.2 Q. Q. 192.168.187.145 Q. Q. 192.168.187.2 Q. Q. 192.168.187.2 Q. Q. 192.168.187.2 Q. Q.	Log SPort Destination IP DPort 192.168.187.2 192.168.187.145 Q. ⊕ IP2.168.187.145 192.168.187.145 192.168.187.2 Q. ⊕ IP2.168.187.2 192.168.187.2 192.168.187.2 Q. ⊕ IP2.168.187.2 192.168.187.2 192.168.187.2 IP2.168.187.2 IP2.168.187.2 192.168.187.2 192.168.187.2 IP2.168.187.2 IP2.168.187.2 192.168.187.2 192.168.187.145 IP2.168.187.145 IP2.168.187.145 192.168.187.2 192.168.187.2 IP2.168.187.2 IP2.168.187.2 192.168.187.2 192.168.187.145 IP2.168.187.2 IP2.168.187.2 192.168.187.2 IP2.168.187.2 IP2.168.187.2 IP2.168.187.2 IP2.168.187.2 IP2.168.187.2 IP2.168.187.2 IP2.168.187.2 IP2.168.187.2 IP2.168.187.145 IP2.168.187.2 IP2.168.187.2 IP2.168.187.2 IP2.168.187.145 IP2.168.187.145 IP2.168.187.145	Log Class Source IP SPort Destination IP DPort GID:SID 192.168.187.2 192.168.187.145 192.168.187.145 1:1000001 $\pm \times$ 192.168.187.145 192.168.187.2 192.168.187.2 1:1000001 Q< \pm Q< \pm 192.168.187.2 1:1000001 192.168.187.2 192.168.187.2 1:1000001 Q< \pm Q< \pm 192.168.187.2 1:1000001 192.168.187.145 192.168.187.2 1:1000001 Q< \pm Q< \pm $\pm \times$ 1:1000001 192.168.187.2 192.168.187.145 1:1000001 Q< \pm Q< \pm $\pm \times$ 1:1000001 192.168.187.2 192.168.187.145 1:1000001 Q< \pm Q< \pm $\pm \times$ 1:1000001 192.168.187.2 192.168.187.2 1:1000001 Q< \pm Q< \pm $\pm \times$ 1:1000001 Q< \pm Q< \pm $\pm \times$ 1:1000001 Q< \pm Q< \pm $\pm \times$ 1:1000001			

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.