Lycée LouisPergaud Besançon

CS - 10 - IDS/IPS
Analyse de trafic

PINOT Julien

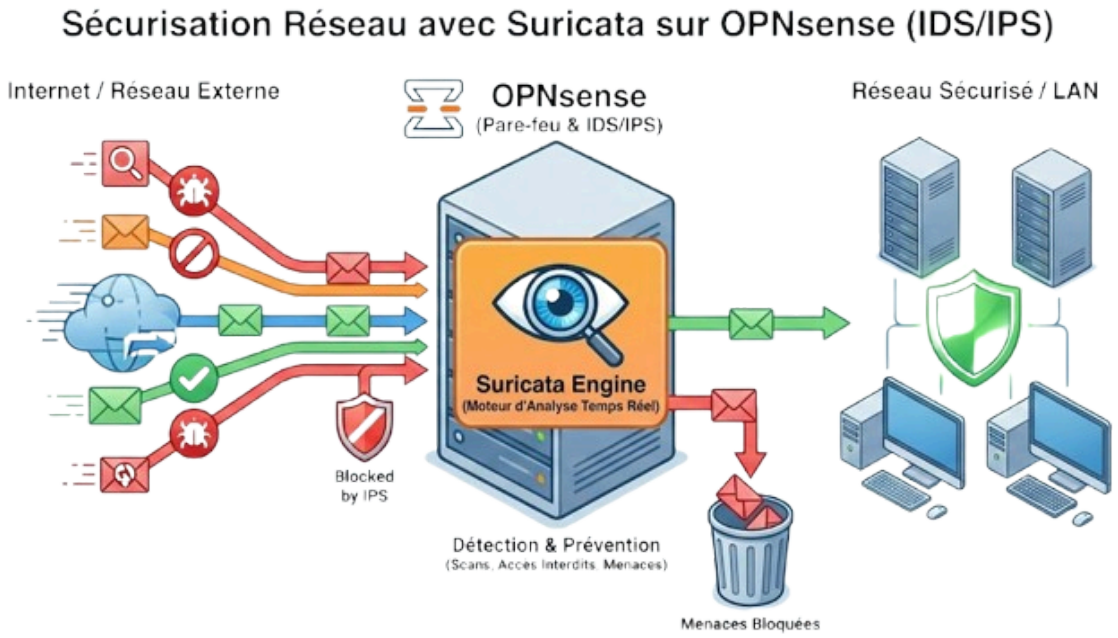
26/01/2026

SOMMAIRE

I. Objectif.....2
II. Architecture et Positionnement.....2
1. Schéma Réseau.....2
2. Pré-requis techniques.....3
III. Configuration de la Sonde (Suricata).....4
1. Activation du service.....4
2. Gestion des règles (Rulesets).....5
IV. Test et Preuves.....5
V. Conclusion.....6

I. Objectif

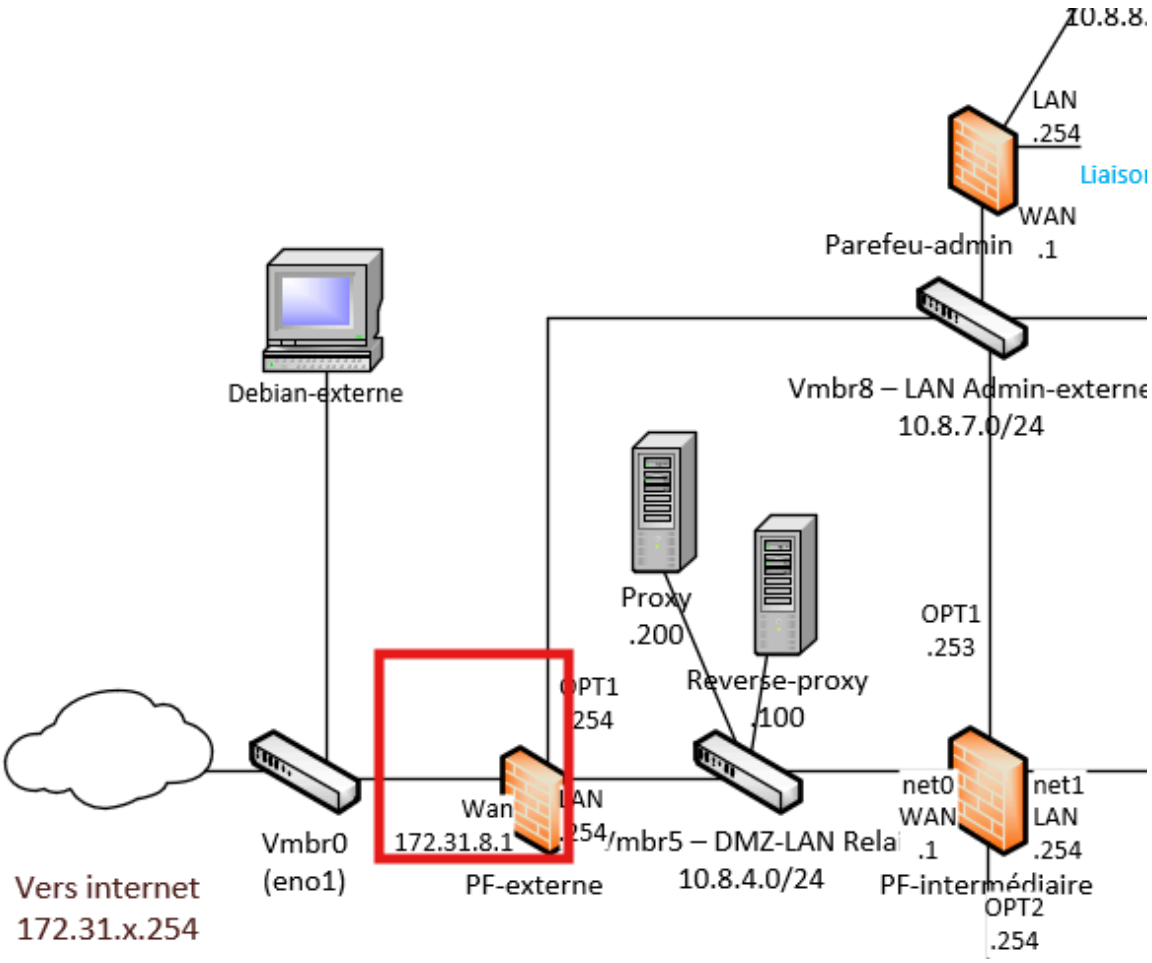
L'objectif est de sécuriser le réseau en déployant une sonde IDS/IPS (Intrusion Detection System / Intrusion Prevention System). Nous avons utilisé le moteur Suricata intégré à la solution OPNsense. La sonde a pour but d'analyser le trafic en temps réel pour détecter des comportements suspects (scans, accès interdits) et bloquer les menaces.



II. Architecture et Positionnement

1. Schéma Réseau

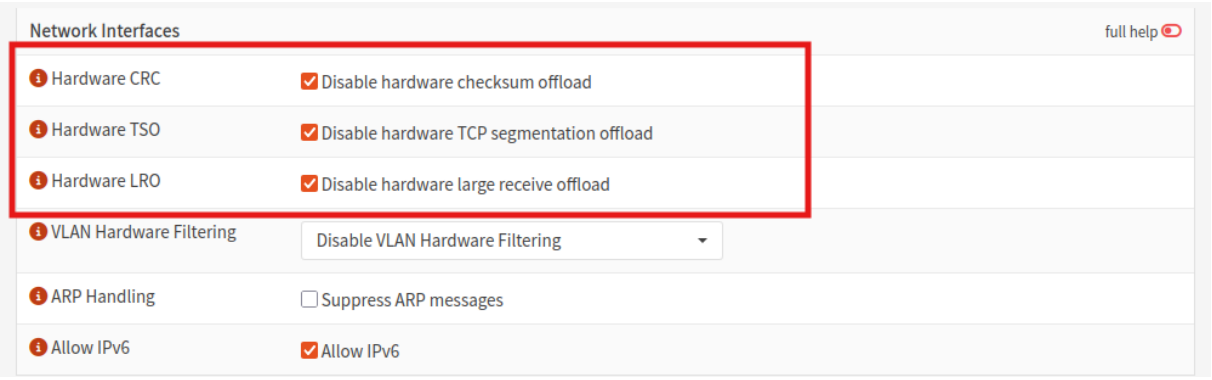
La sonde a été positionnée sur le Pare-feu Externe, au niveau de l'interface WAN (, car c'est le point d'entrée critique du trafic venant de l'extérieur (Internet).



2. Pré-requis techniques

Avant d'activer la sonde, il a été nécessaire de désactiver l'accélération matérielle (Hardware Offloading) de la carte réseau.

Il faut se rendre dans Interfaces > Settings.

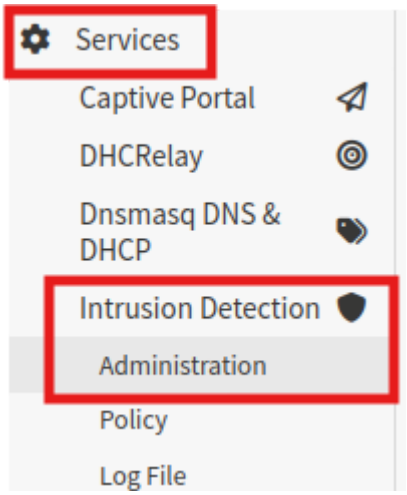


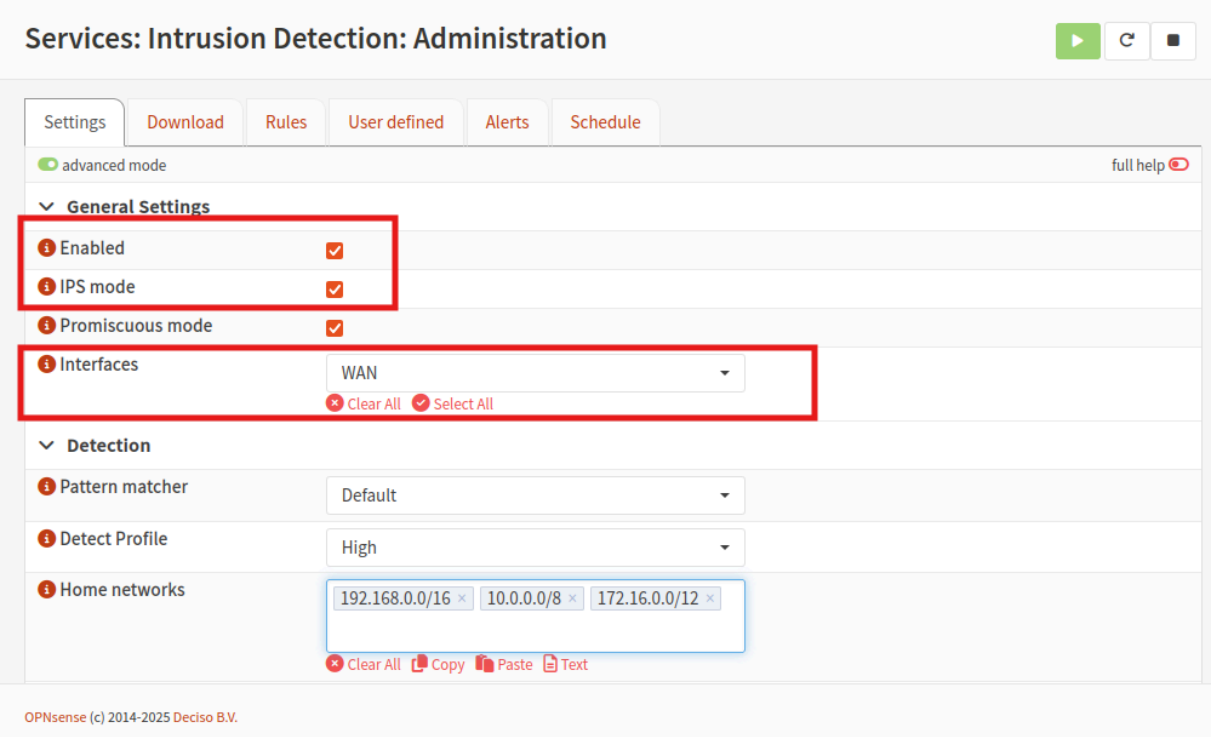
Pourquoi ? Si la carte réseau traite les paquets elle-même (CRC, TSO, LRO), la sonde logicielle ne voit pas le trafic brut ou voit des paquets tronqués, ce qui rend la détection impossible.

III. Configuration de la Sonde (Suricata)

1. Activation du service

Nous avons activé Suricata dans Services > Intrusion Detection > Administration.



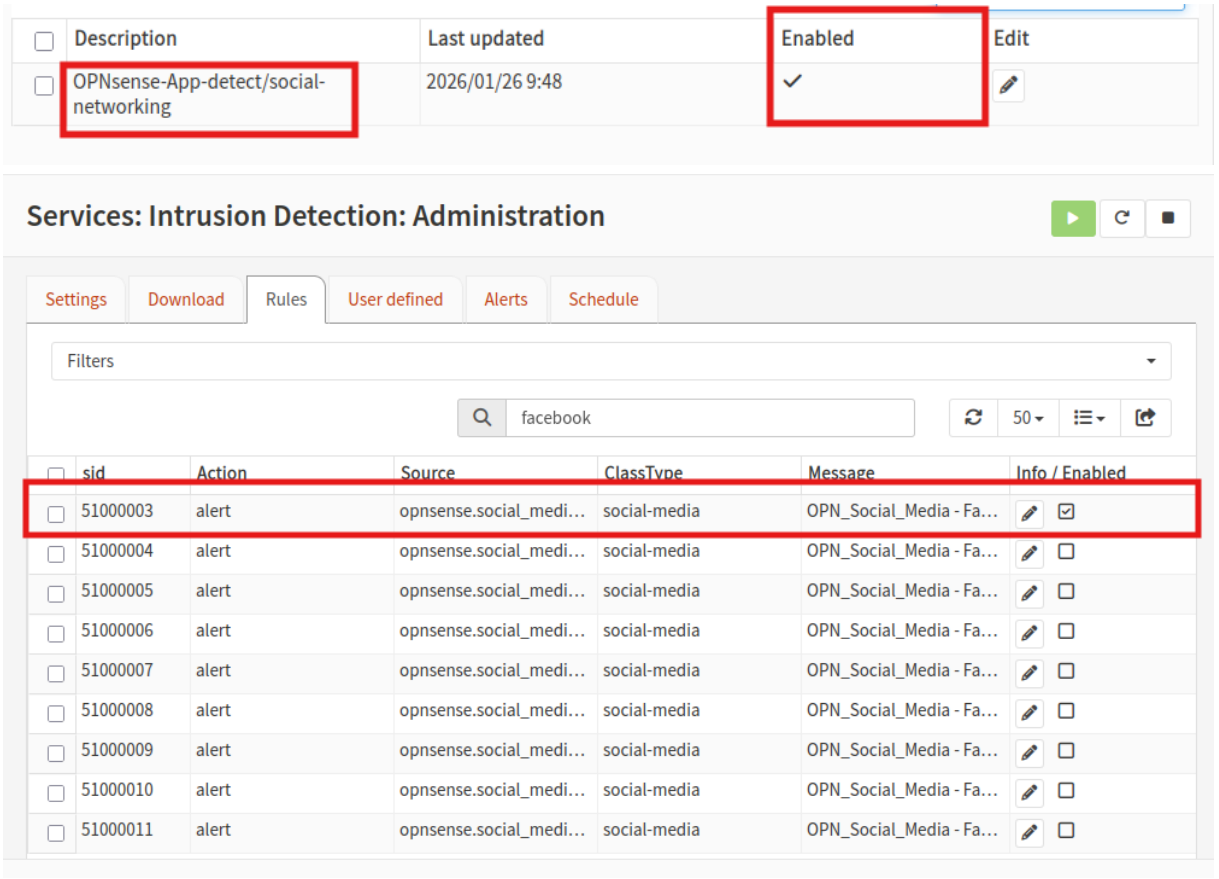


Mode IPS activé : Contrairement au mode IDS (qui ne fait qu'alerter), le mode IPS (Intrusion Prevention System) permet de bloquer (Drop) les paquets malveillants.

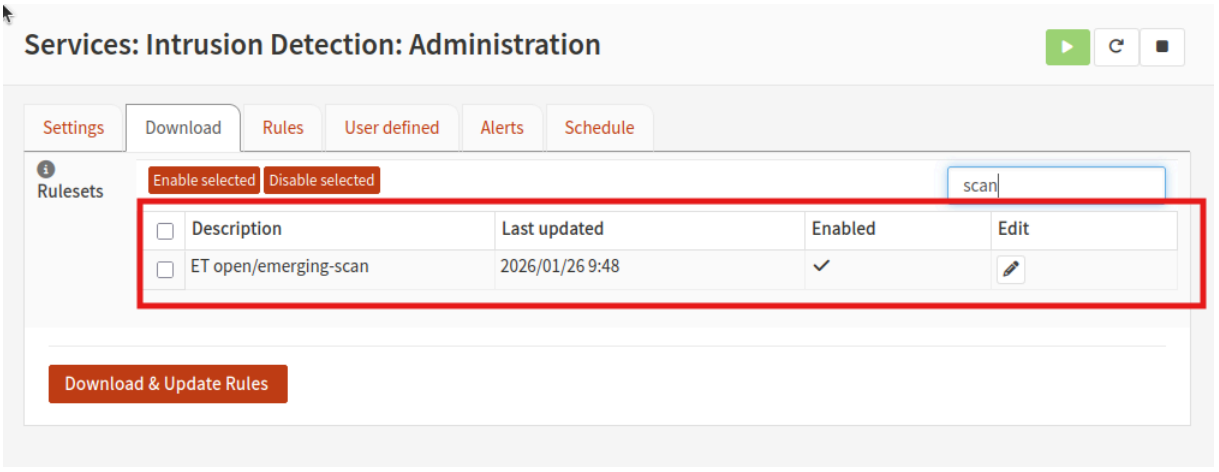
Interfaces écoutées : WAN (pour les attaques externes) et LAN (pour les menaces internes ou la propagation).

2. Gestion des règles (Rulesets)

Les ensembles de règles permettant la détection d'une utilisation de Facebook ont été téléchargés.



Les ensembles de règles permettant la détection d'un scan NMAP ont été téléchargés.



On laisse les règles par défauts elles suffisent

IV. Test et Preuves

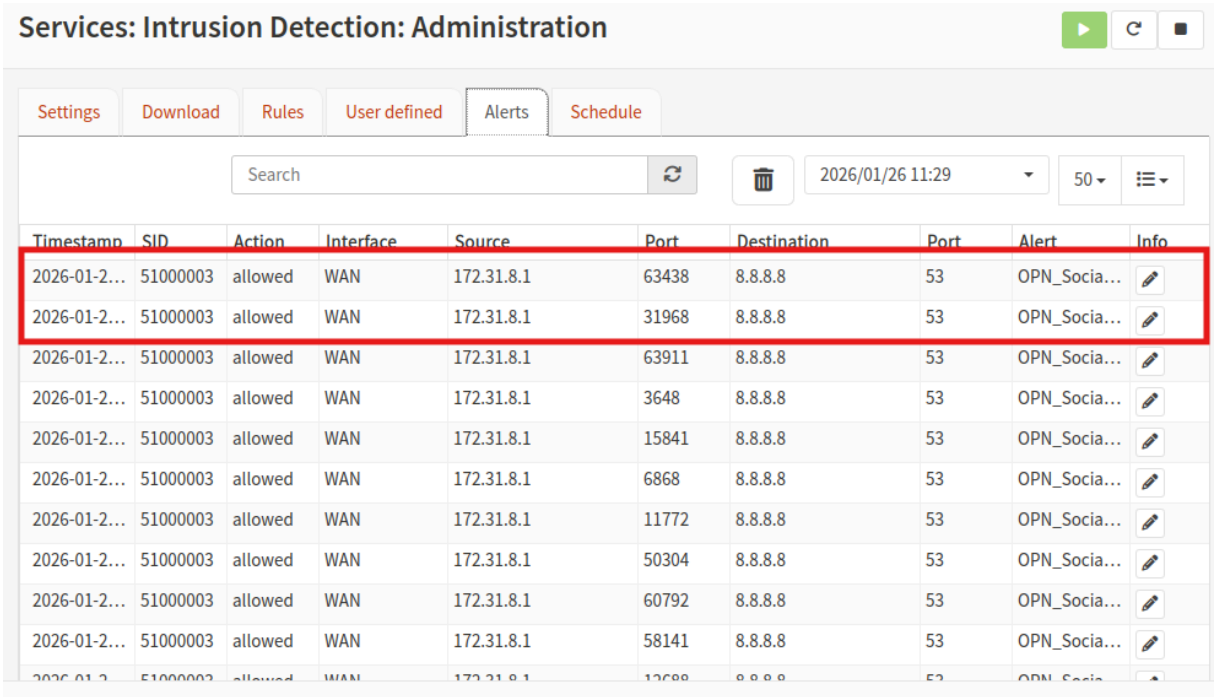
Objectif : Etre informé lorsqu'une connection à Facebook a lieu

Manipulation : Activation de la règle concernant les requêtes DNS ou IP liées à Facebook.

Test client : Tentative de connexion depuis un poste client via un navigateur.

Résultat : La connexion est réussie et l'action est relevée.

Preuve (Logs OPNsense) : Ci-dessous, les logs montrant que Suricata a intercepté la requête vers Facebook.



Timestamp	SID	Action	Interface	Source	Port	Destination	Port	Alert	Info
2026-01-2…	51000003	allowed	WAN	172.31.8.1	63438	8.8.8.8	53	OPN_Socia…	
2026-01-2…	51000003	allowed	WAN	172.31.8.1	31968	8.8.8.8	53	OPN_Socia…	
2026-01-2…	51000003	allowed	WAN	172.31.8.1	63911	8.8.8.8	53	OPN_Socia…	
2026-01-2…	51000003	allowed	WAN	172.31.8.1	3648	8.8.8.8	53	OPN_Socia…	
2026-01-2…	51000003	allowed	WAN	172.31.8.1	15841	8.8.8.8	53	OPN_Socia…	
2026-01-2…	51000003	allowed	WAN	172.31.8.1	6868	8.8.8.8	53	OPN_Socia…	
2026-01-2…	51000003	allowed	WAN	172.31.8.1	11772	8.8.8.8	53	OPN_Socia…	
2026-01-2…	51000003	allowed	WAN	172.31.8.1	50304	8.8.8.8	53	OPN_Socia…	
2026-01-2…	51000003	allowed	WAN	172.31.8.1	60792	8.8.8.8	53	OPN_Socia…	
2026-01-2…	51000003	allowed	WAN	172.31.8.1	58141	8.8.8.8	53	OPN_Socia…	

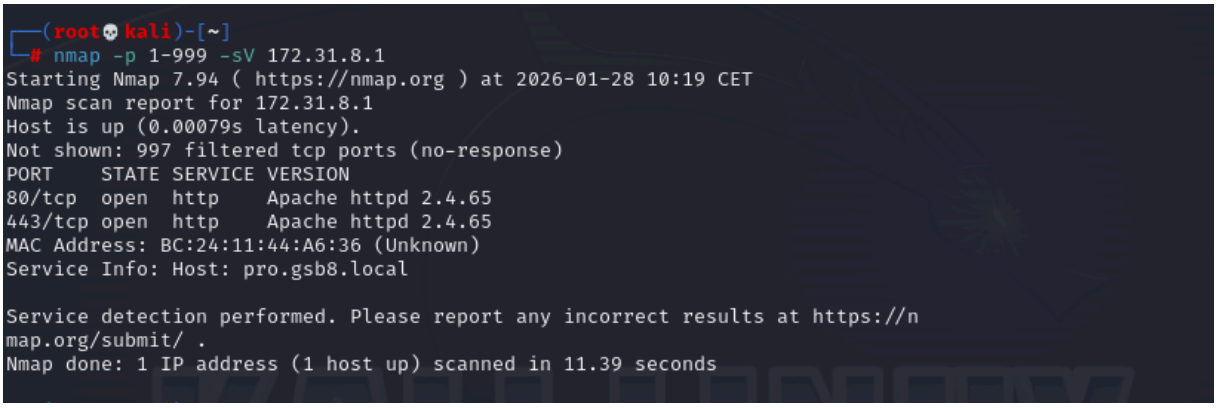
Objectif : Etre informé lorsqu'un scan a lieu

Manipulation : Activation de la règle concernant les scans.

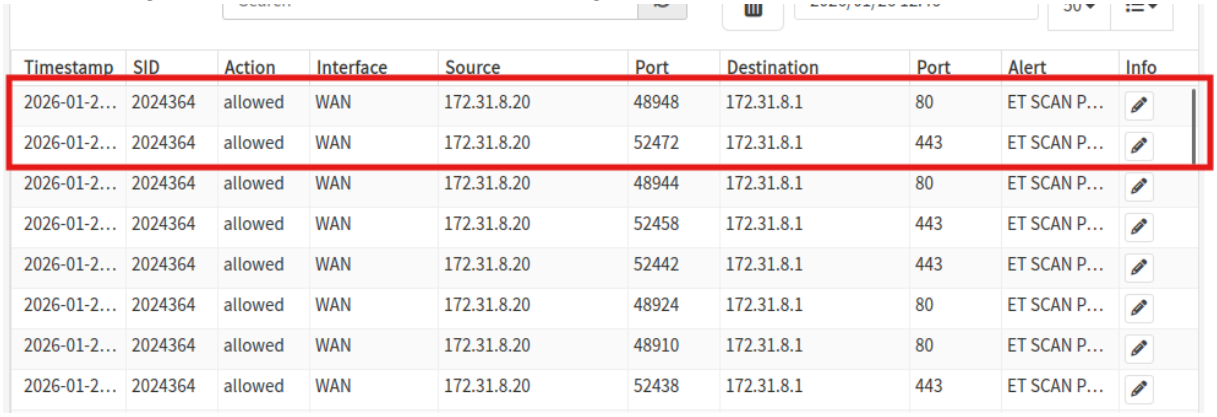
Test attaquant : Scan nmap.

Résultat : Le scan est relevé.

Preuve (Kali) : Ci-dessous, le scan nmap.



Preuve (Logs OPNsense) : Ci-dessous, les logs montrant que Suricata a intercepté le scan.



Timestamp	SID	Action	Interface	Source	Port	Destination	Port	Alert	Info
2026-01-2…	2024364	allowed	WAN	172.31.8.20	48948	172.31.8.1	80	ET SCAN P…	
2026-01-2…	2024364	allowed	WAN	172.31.8.20	52472	172.31.8.1	443	ET SCAN P…	
2026-01-2…	2024364	allowed	WAN	172.31.8.20	48944	172.31.8.1	80	ET SCAN P…	
2026-01-2…	2024364	allowed	WAN	172.31.8.20	52458	172.31.8.1	443	ET SCAN P…	
2026-01-2…	2024364	allowed	WAN	172.31.8.20	52442	172.31.8.1	443	ET SCAN P…	
2026-01-2…	2024364	allowed	WAN	172.31.8.20	48924	172.31.8.1	80	ET SCAN P…	
2026-01-2…	2024364	allowed	WAN	172.31.8.20	48910	172.31.8.1	80	ET SCAN P…	
2026-01-2…	2024364	allowed	WAN	172.31.8.20	52438	172.31.8.1	443	ET SCAN P…	

V. Conclusion

La mise en place de Suricata sur OPNsense permet d'ajouter une couche de sécurité "intelligente" au pare-feu. Contrairement au filtrage simple (ports/IP), l'IPS analyse le contenu et le comportement du trafic. Nous avons validé son fonctionnement.