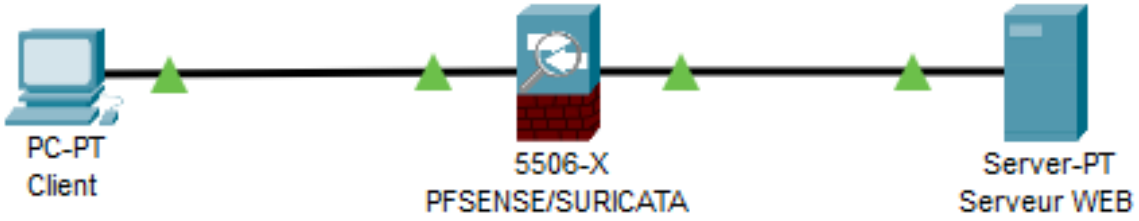
TP IDS Suricata

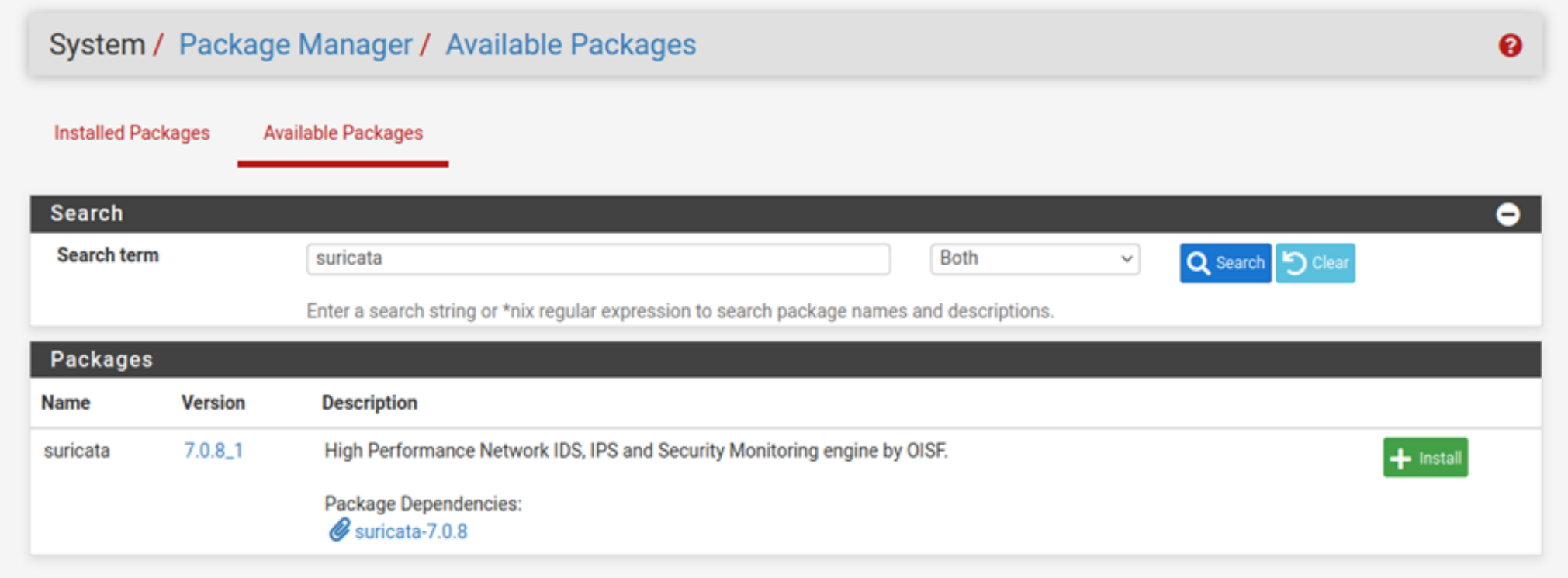
FLORENTIN BRACQ- -FLABAT, BTS 2 SIO

Schéma réseau



Installation de Suricata sur Pfsense

Se rendre dans le gestionnaire de paquets de Pfsense pour rechercher et installer Suricata



Configuration de Suricata

Dans un premier temps, nous allons nous rendre dans Global Settings

On renseigne :

Install ETOpen Emerging Threats rules : cocher la case ETOpen…

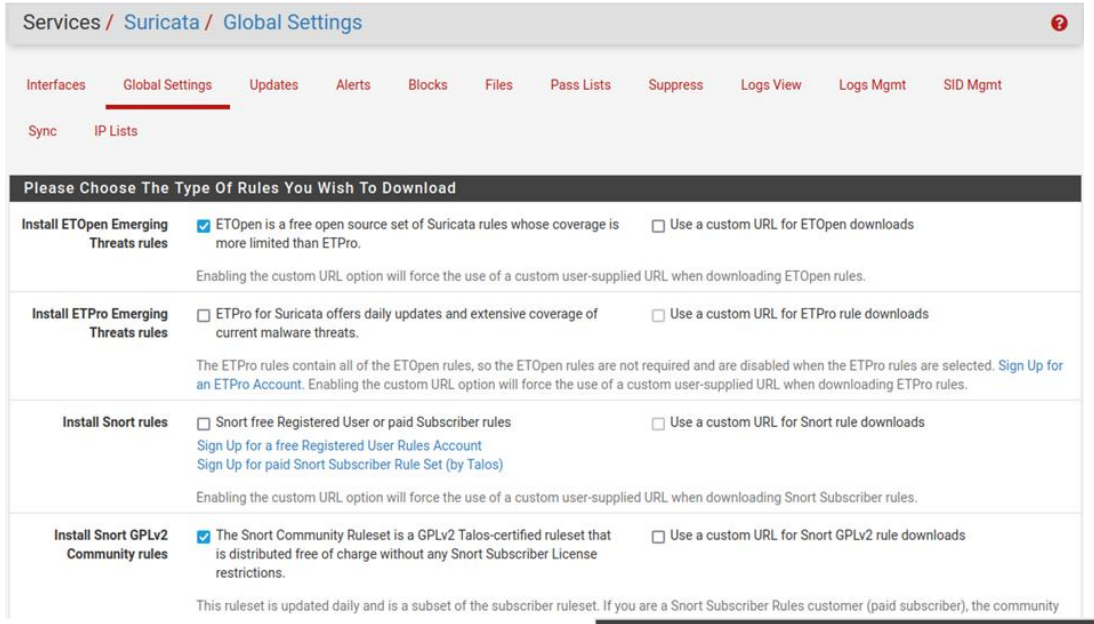
Install Snort GPLv2 Comunity rules : The Snort…

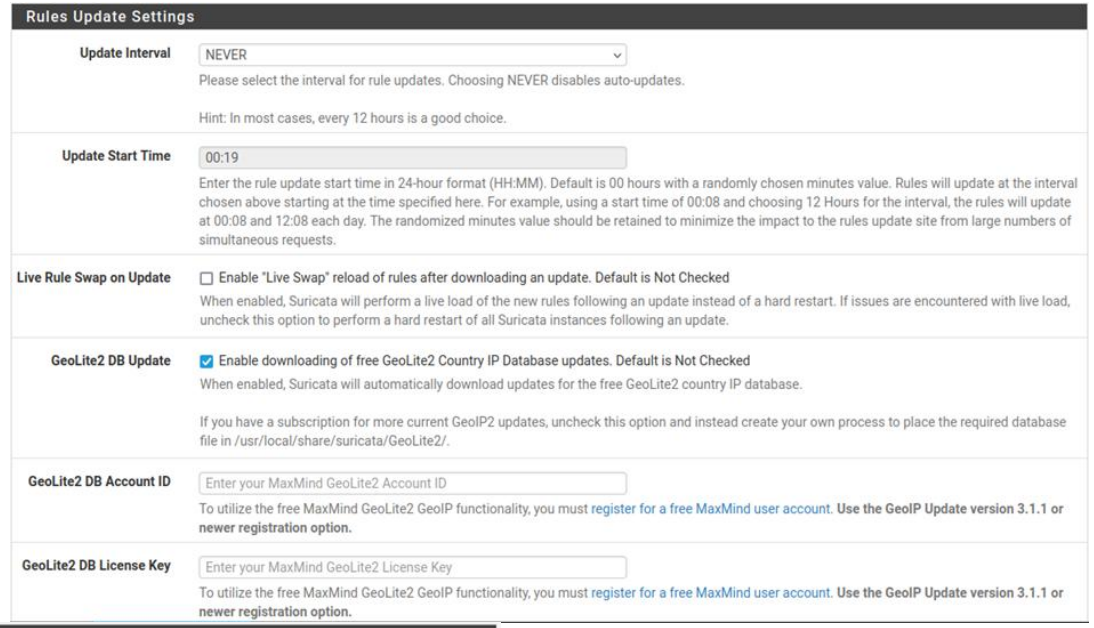
Update Start Time : l'heure de vous voulez

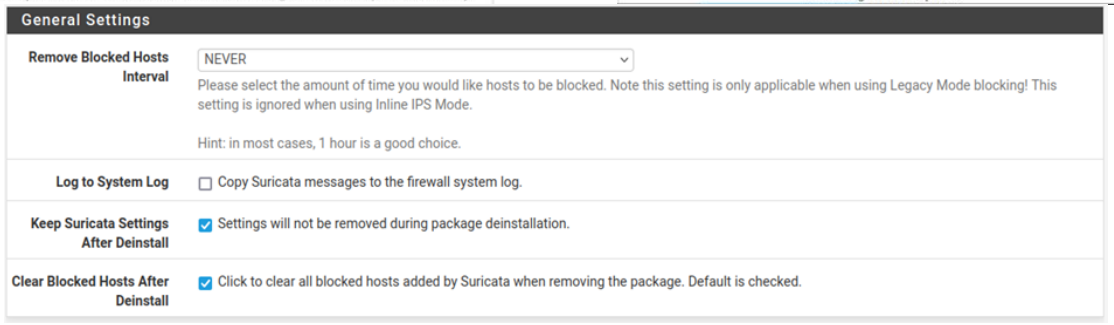
GeoLite2 DB Update : cocher si vous avez un compte sur le site MaxMind (la création du compte et l'utilisation de DB est gratuite)

Il ne reste plus qu'à enregistrer

Configuration de Suricata

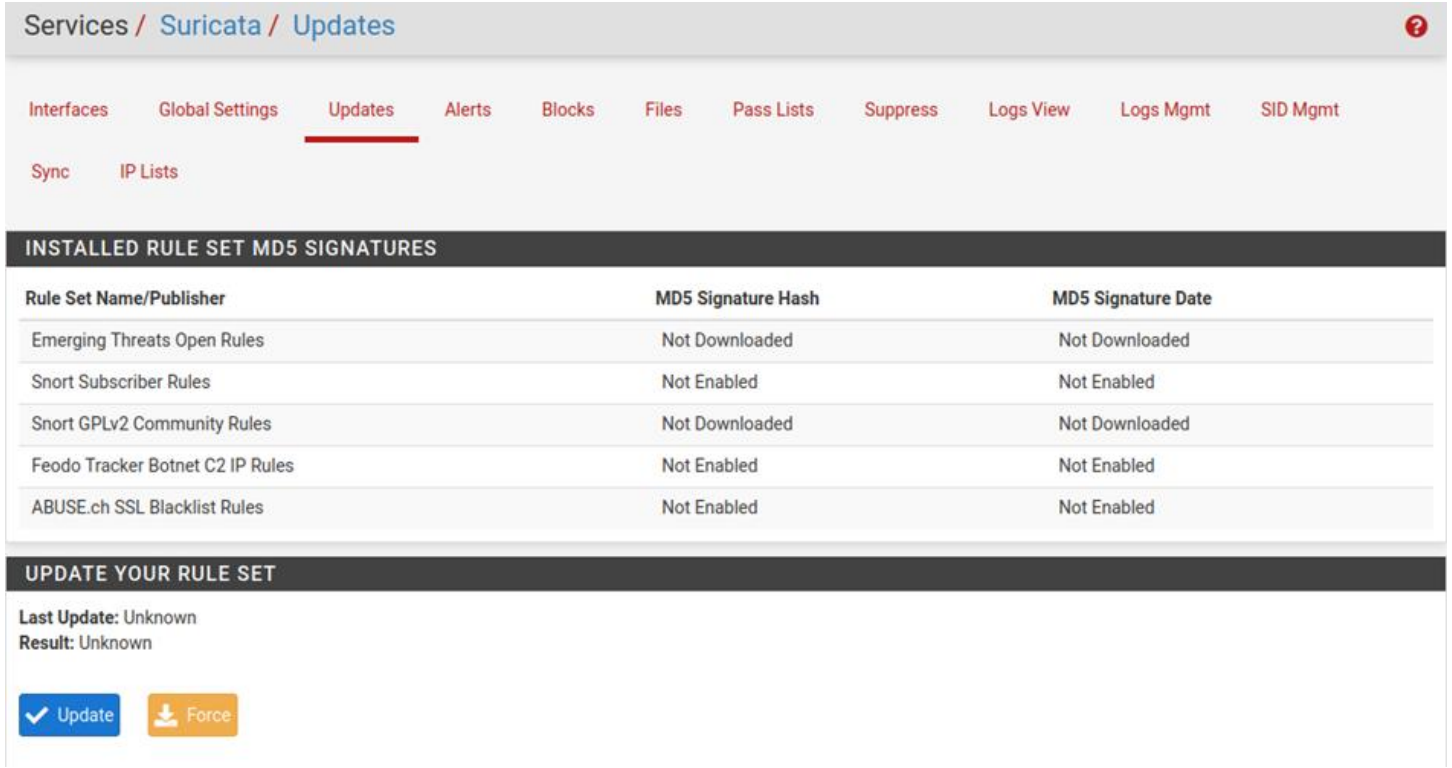






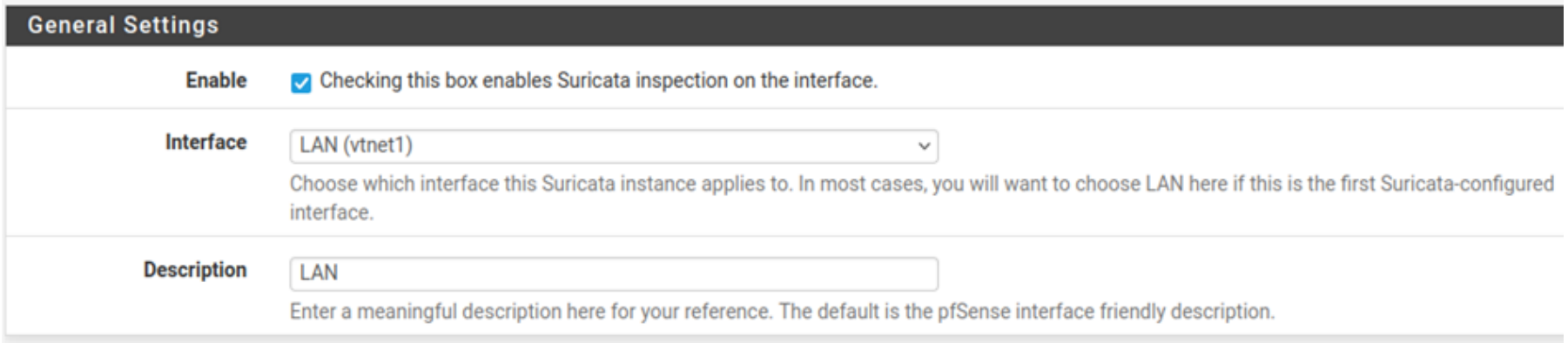
Configuration de Suricata

Se rendre ensuite dans l'onglet Updates. Dans cette partie, nous pouvons voir les paquets de règles, forcer les mises à jour et voir s'il y a des problèmes.



Configuration de Suricata

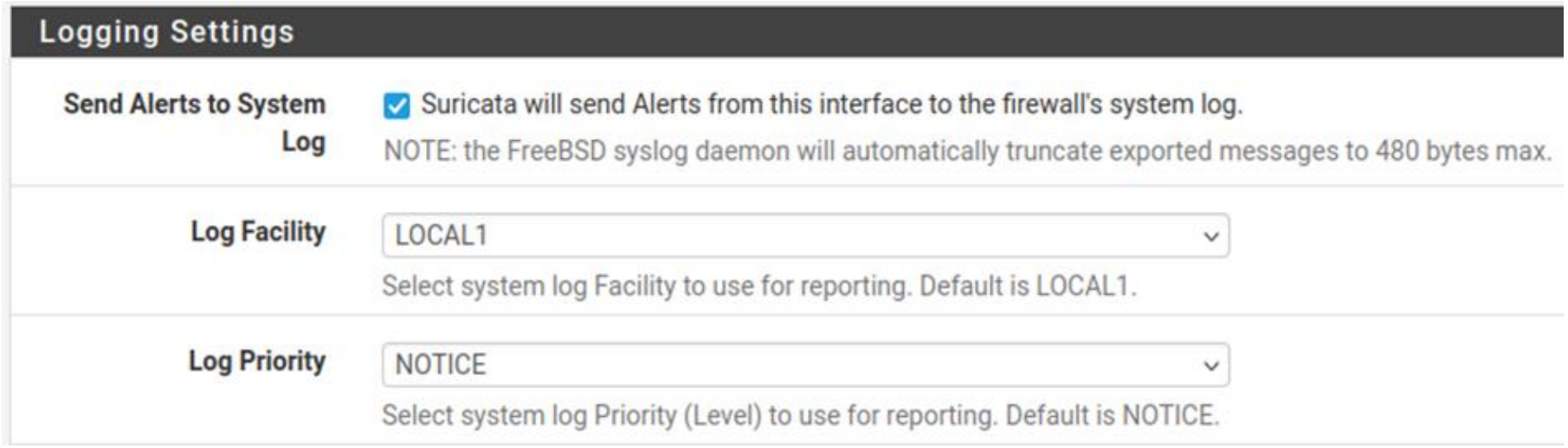
Pour configurer Suricata, se rendre dans services, puis Suricata, dans Interfaces en dessous de General Settings, cocher la case enable pour activer Suricata et sélectionner l'interface LAN.



Configuration de Suricata

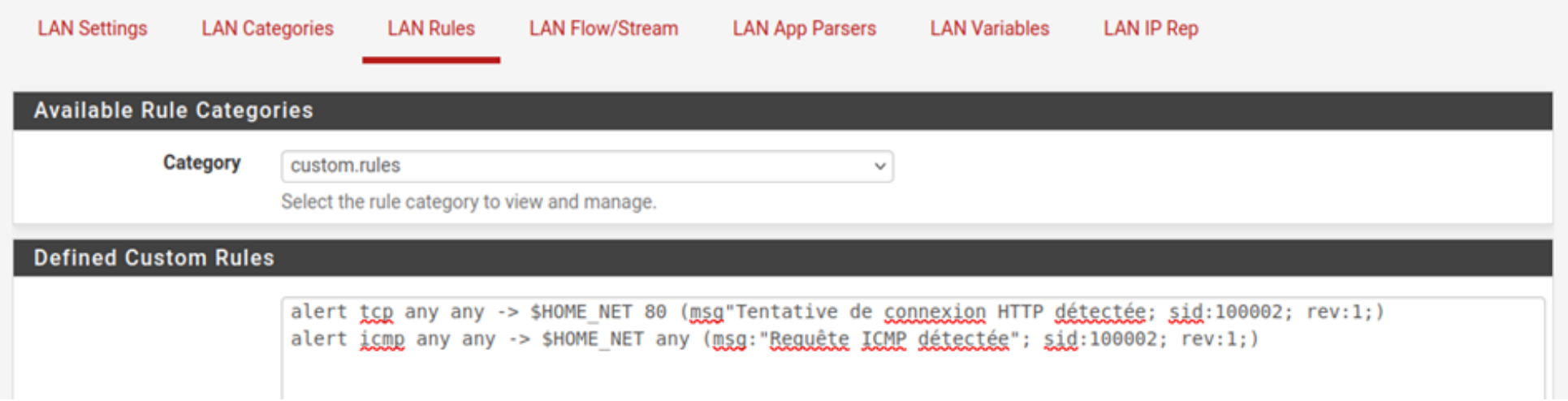
Passage en mode IDS

Dans Logging Settings cacher la case Send Alerts to System Log, penser à cliquer sur save pour enregistrer les modifications



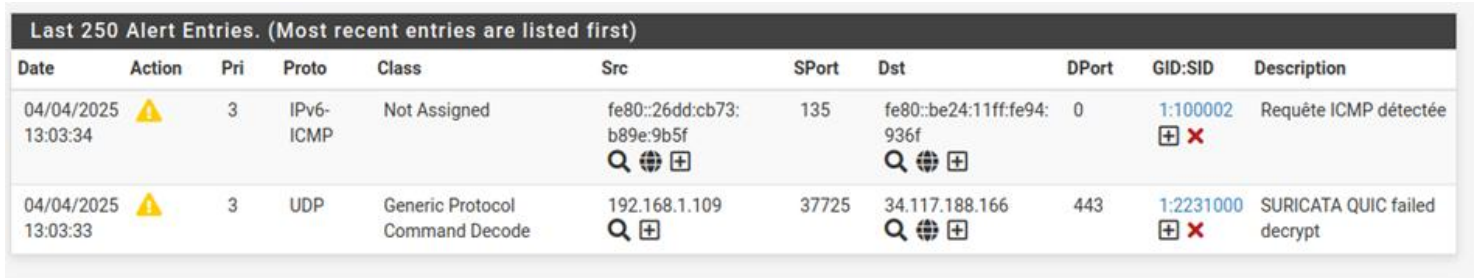
Configuration de Suricata

Dans LAN Rules, dans la catégorie custom.rules, créer les règles suivantes



Test

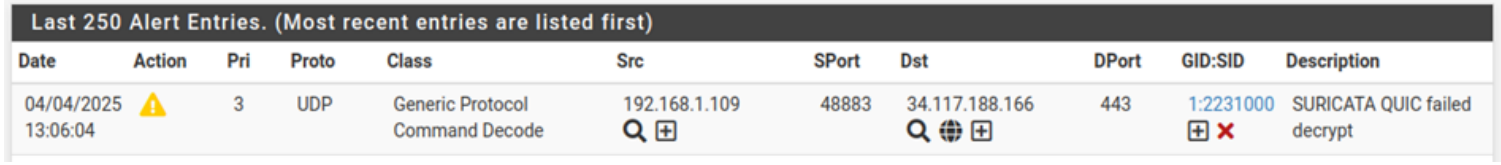
Test suricata ping serveur :



Last 250 Alert Entries. (Most recent entries are listed first)

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
04/04/2025 13:03:34	⚠	3	IPv6-ICMP	Not Assigned	fe80::26dd:cb73:b89e:9b5f	135	fe80::be24:11ff:fe94:936f	0	1:100002	Requête ICMP détectée
04/04/2025 13:03:33	⚠	3	UDP	Generic Protocol Command Decode	192.168.1.109	37725	34.117.188.166	443	1:2231000	SURICATA QUIC failed decrypt

Test suricata ouverture page web http :

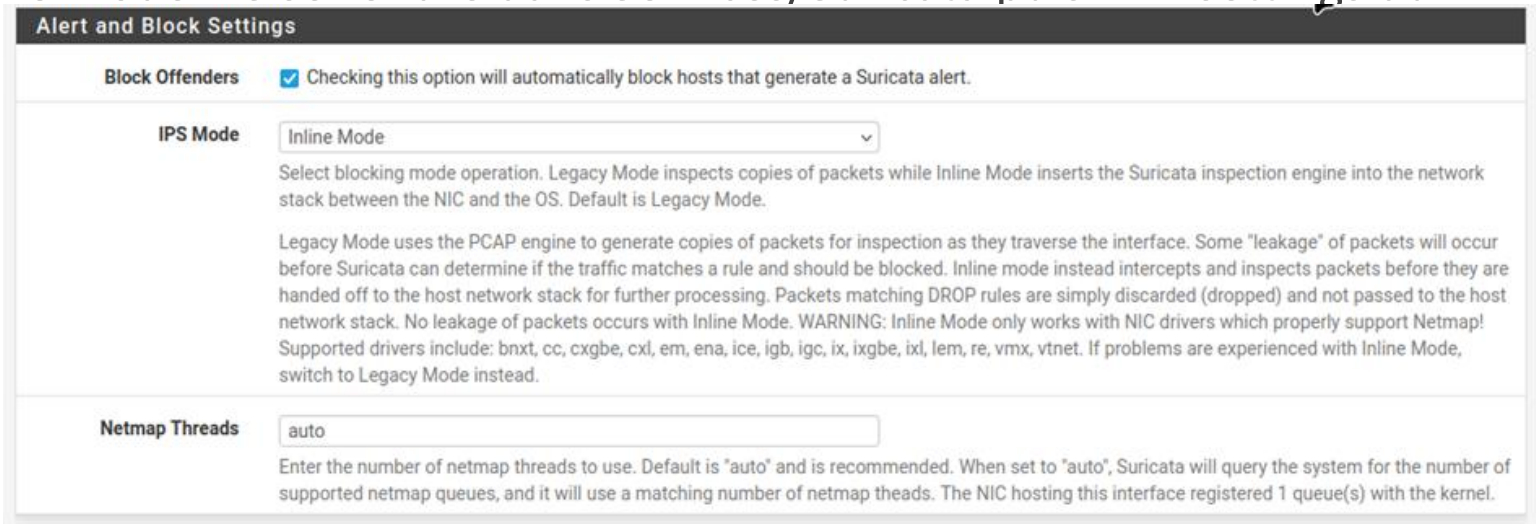


Last 250 Alert Entries. (Most recent entries are listed first)

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
04/04/2025 13:06:04	⚠	3	UDP	Generic Protocol Command Decode	192.168.1.109	48883	34.117.188.166	443	1:2231000	SURICATA QUIC failed decrypt

Passage en mode IPS

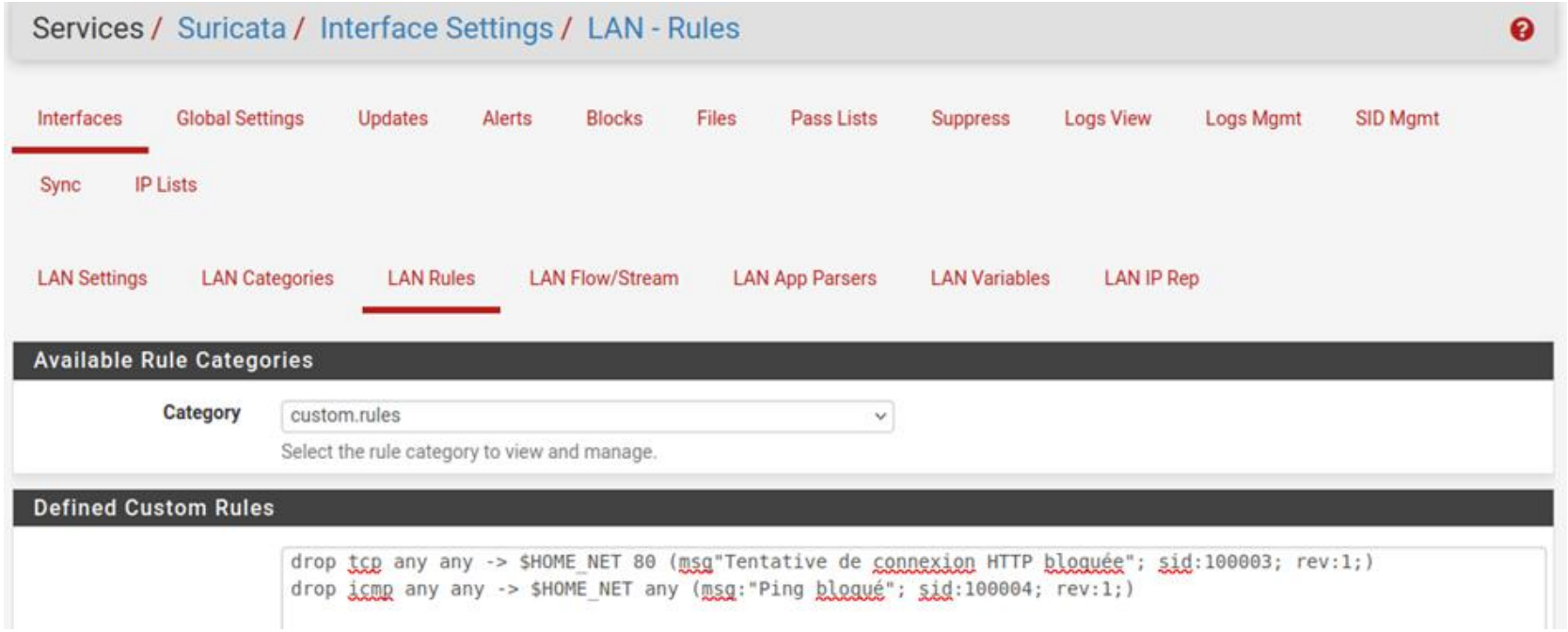
Pour activer le mode IPS se rendre dans Services/Suricata puis LAN settings du LAN



Penser à cliquer sur save pour enregistrer les modifications

Modifications des règles

Modifier les règles pour bloquer certaines activités



Vérification

Last 250 Alert Entries. (Most recent entries are listed first)

Note: Alerts triggered by DROP rules that resulted in dropped (blocked) packets are shown with highlighted rows below.

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
04/06/2025 17:48:34		3	IPv6-ICMP	Not Assigned	fe80::26dd:cb73:b89e:9b5f	135	fe80::be24:11ff:fe94:936f	0	1:100004	Ping bloqué
04/06/2025 17:43:34		3	IPv6-ICMP	Not Assigned	fe80::26dd:cb73:b89e:9b5f	135	fe80::be24:11ff:fe94:936f	0	1:100004	Ping bloqué
04/06/2025 17:42:28		3	UDP	Generic Protocol Command Decode	192.168.1.109	39916	34.117.188.166	443	1:2231000	SURICATA QUIC failed decrypt
04/06/2025 17:38:34		3	IPv6-ICMP	Not Assigned	fe80::26dd:cb73:b89e:9b5f	135	fe80::be24:11ff:fe94:936f	0	1:100002	Requête ICMP détectée
04/06/2025 17:33:20		3	IPv6-ICMP	Not Assigned	fe80::26dd:cb73:b89e:9b5f	135	fe80::be24:11ff:fe94:936f	0	1:100002	Requête ICMP détectée
04/06/2025 17:32:22		3	IPv6-ICMP	Not Assigned	fe80::26dd:cb73:b89e:9b5f	135	fe80::be24:11ff:fe94:936f	0	1:100002	Requête ICMP détectée

Sources

https://www.ctechmat.fr/pfsense-paquet-suricata/