PRÉSENTÉ PAR DRUELLE NICOLAS

TP-IDS/IPS

CAHIER DES CHARGES

-Installer Suricata

-Configurer l’interface LAN sur Suricata

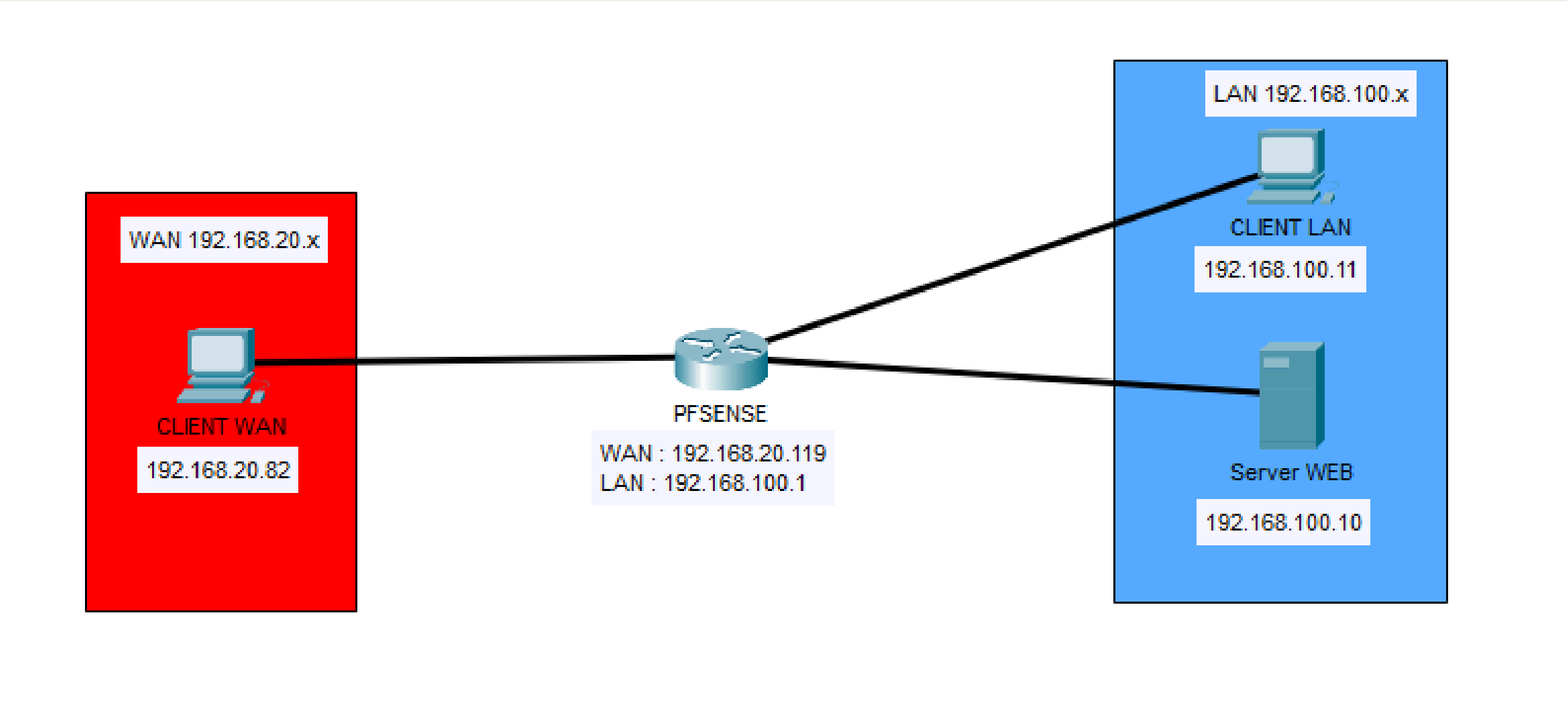
-Mettre en place les alertes

-Réalisations des tests pour les alertes

-Mettre en place les blocages

-Réalisations des tests pour les blocages

TOPOLOGIE

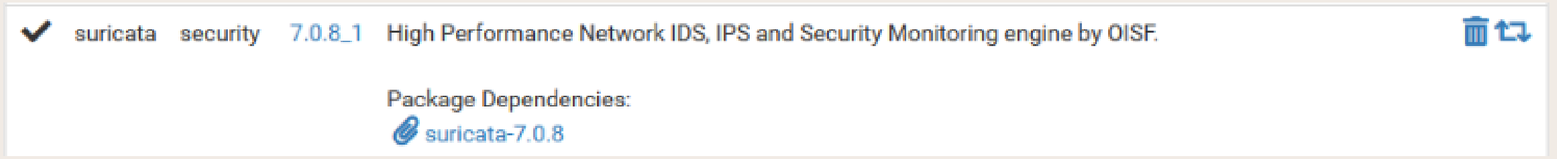

LAN 192.168.100.x
CLIENT LAN
192.168.100.11
WAN 192.168.20.x
CLIENT WAN
192.168.20.82
PFSENSE
WAN : 192.168.20.119
LAN : 192.168.100.1
Server WEB
192.168.100.10

QU’EST CE QUE L’IDS ET L’IPS

IDS (Intrusion Detection System) : Système de surveillance qui analyse le trafic réseau ou les activités système pour détecter des comportements suspects et générer des alertes.

IPS (Intrusion Prevention System) : Extension de l’IDS qui bloque activement les menaces en filtrant ou en stoppant le trafic malveillant avant qu’il n’atteigne sa cible.

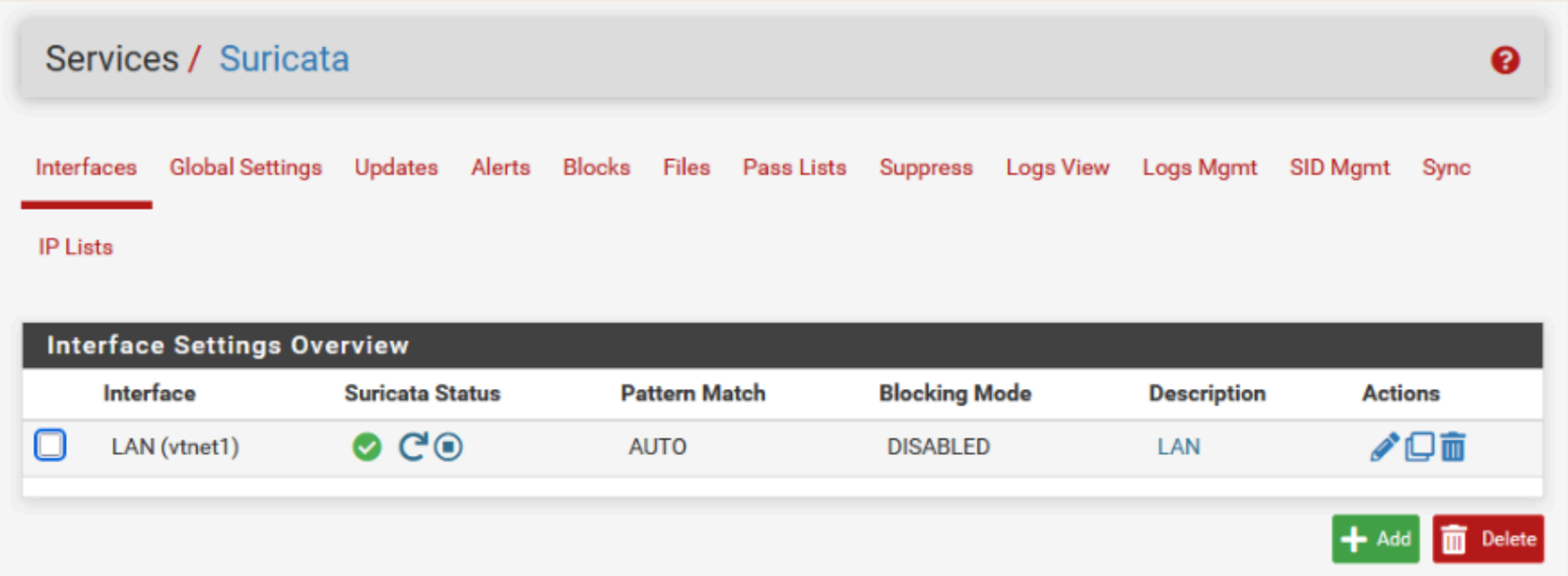
INSTALLATION SURICATA



Dans un premier temps je procède à l'installation de Suricata sur Pfsense en me rendant dans "System → Package Manger".

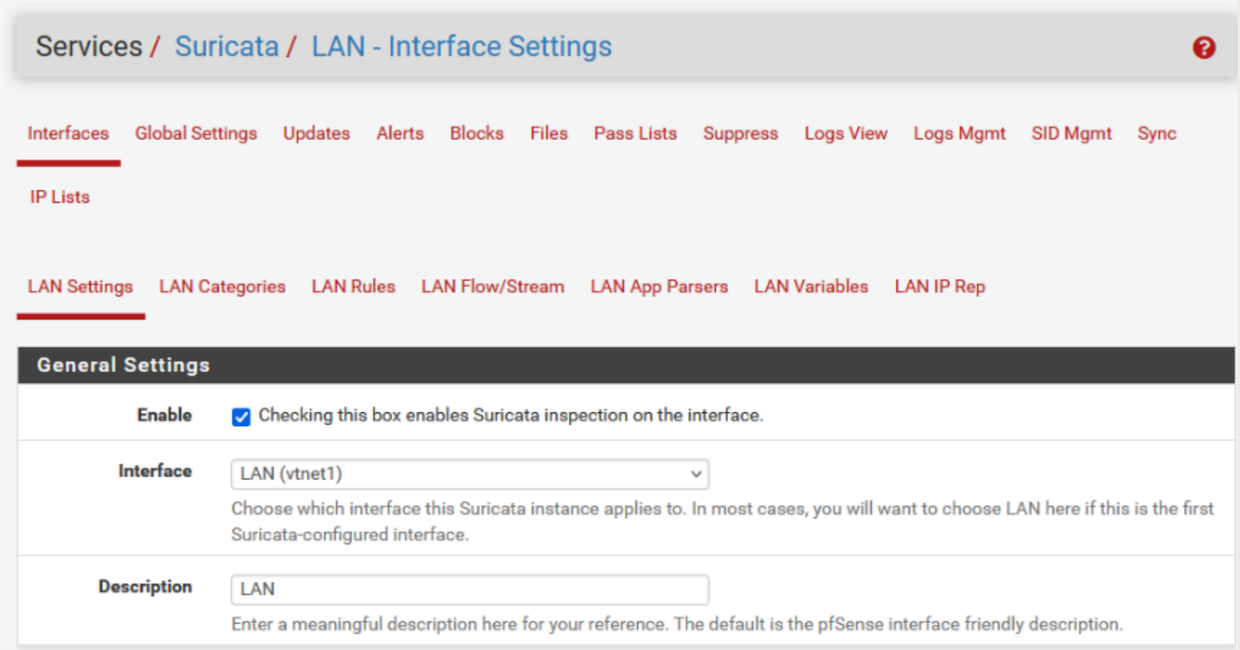
CONFIGURATION INTERFACE LAN SUR SURICATA

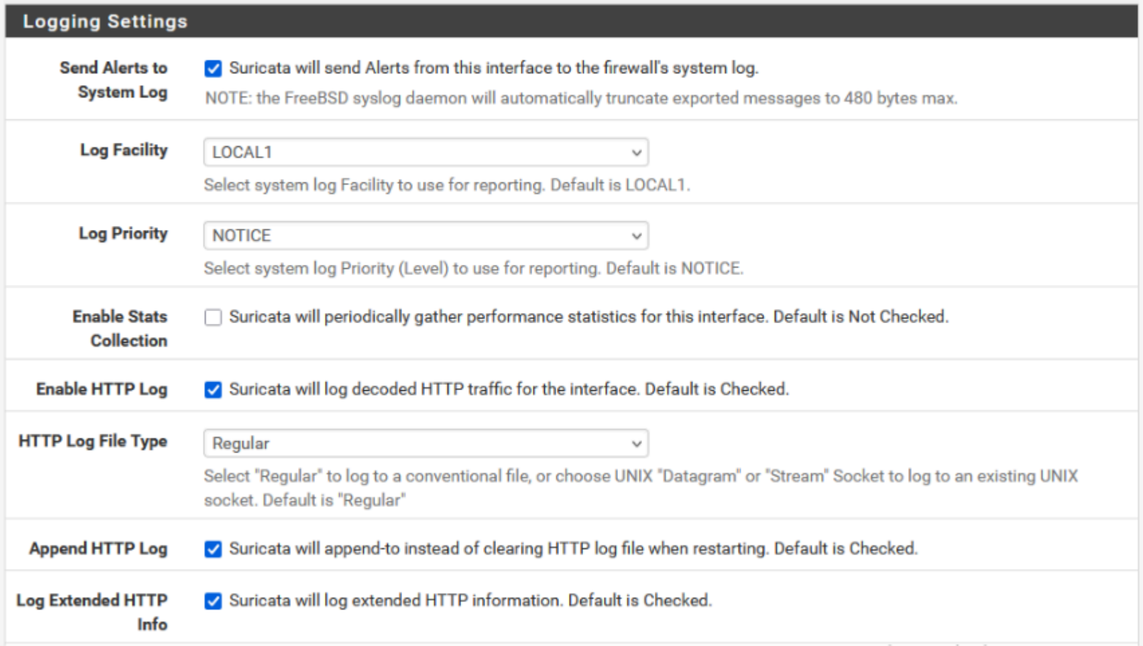
CONFIGURATION LAN



Une fois suricata installé j’ajoute mon interface LAN sur celui-ci.

CONFIGURATION LAN





Une fois l'interface LAN créee je vais dans "LAN Settings" et coche la case "Enable". Je vérifie aussi si la case "Send Alert to System Log" est cochée.

MISE EN PLACE DES ALERTES

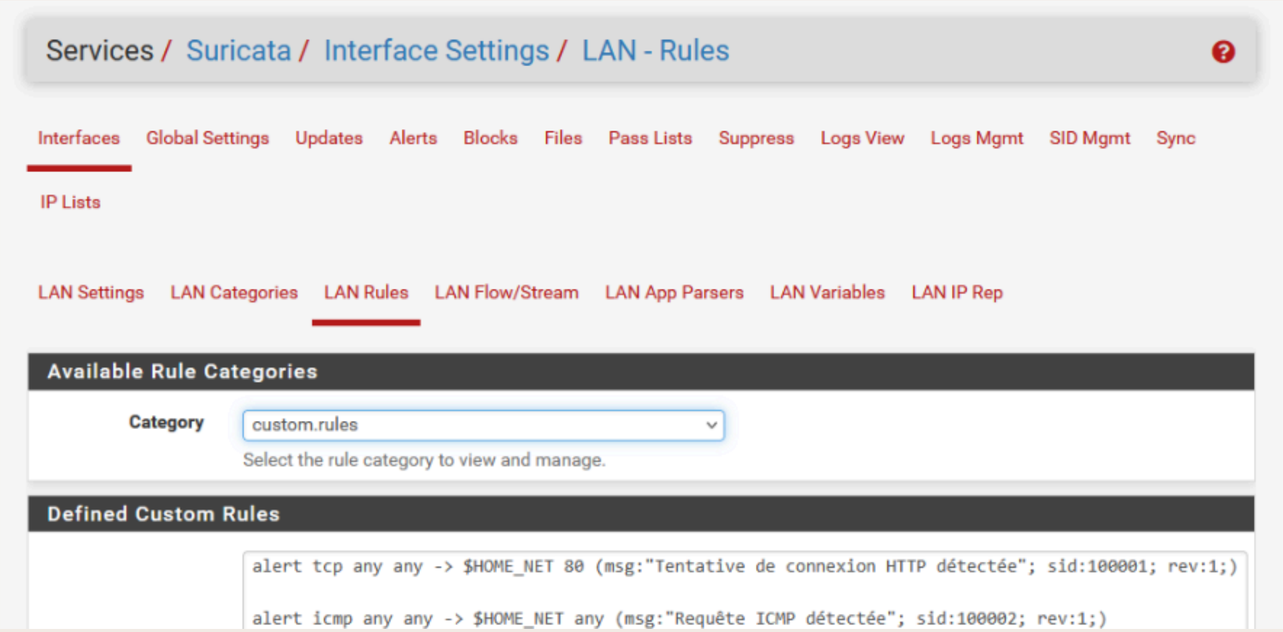
EXPLICATION DES RÉGLES

Pour les règles la mise en forme est la suivante :

“action” “protocole” “source_ip” “source_port” → “destination_ip” “destination_port” “options pour les logs et l’identification”

Différentes actions	alert (Déclenche une alerte sans bloquer) drop (Bloque et enregistre dans les logs) pass (Autorise et ignore le trafic) reject (Bloque et renvoie un message au client)
Protocoles	ICMP, TCP, UDP
Source	Any = N’importe quelle IP IP de réseau ou spécifique
->	Direction du flux
Destination	Any ou IP
Options	« msg : « ... » » = Message affiché dans les logs « sid :100001 ; » = Identifiant unique à la règle « rev :1 ; » = Version de la règles

MISE EN PLACE DES ALERTES



Ensuite en me rendant dans “LAN Rules” j’établis une règle permettant de détecter le passage de ping en ICMP ainsi que le passage de trame TCP.

TEST DES ALERTES

COMMENT LIRE UNE RÈGLES SUR SURICATA

Sur une règle, on peut y retrouver divers éléments qui sont tous représentés dans le tableau suivant :

Champ	Description
Date	Indique quand l'alerte a été déclenchée
Action	Affiche l'action appliquée : alert / drop, etc..
Pri (Priorité)	Indique la gravité de l'alerte (1= critique, 4 = faible)
Proto (Protocole)	Indique le protocole utilisé
Class	Montre la classification de l'alerte (peut rester vide)
Src (Source IP)	Affiche l'adresse IP qui a initié la connexion
Sport (Source Port)	Indique le port source
Dst (Destination IP)	Affiche l'adresse IP cible de la connexion
Dport (Destination port)	Indique le port de destination
GID : SID	GID = Groupe ID et SID = Signature ID qui permet d'identifier la règle qui a déclenché l'alerte
Description	Affiche le message défini dans la règle

TEST ALERTE ICMP

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

Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
03/29/2025 22:32:46	⚠	3	ICMP	Not Assigned	192.168.20.82	0	192.168.100.10	0	1:100002	Requête ICMP détectée

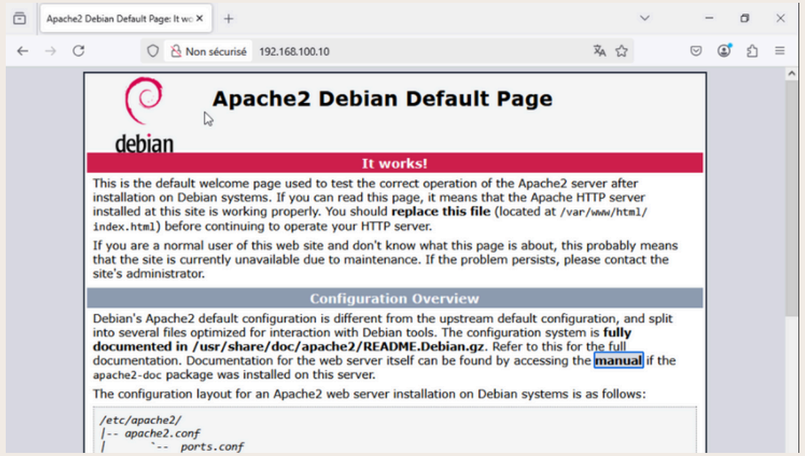
Lorsque je lance un ping on voit bien qu’une règle est créée sur Suricata.

TEST ALERTE HTTP

```
1189 243.043706    192.168.20.82     192.168.100.10    HTTP     419 GET / HTTP/1.1
1193 243.104289    192.168.100.10    192.168.20.82     HTTP     514 HTTP/1.1 200 OK  (text/html)
1196 243.571016    192.168.20.82     192.168.100.10    HTTP     449 GET /icons/openlogo-75.png HTTP/1.1
1202 243.686618    192.168.100.10    192.168.20.82     HTTP     254 HTTP/1.1 200 OK  (PNG)
1205 244.225873    192.168.20.82     192.168.100.10    HTTP     436 GET /favicon.ico HTTP/1.1
1207 244.249149    192.168.100.10    192.168.20.82     HTTP     546 HTTP/1.1 404 Not Found  (text/html)
```

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

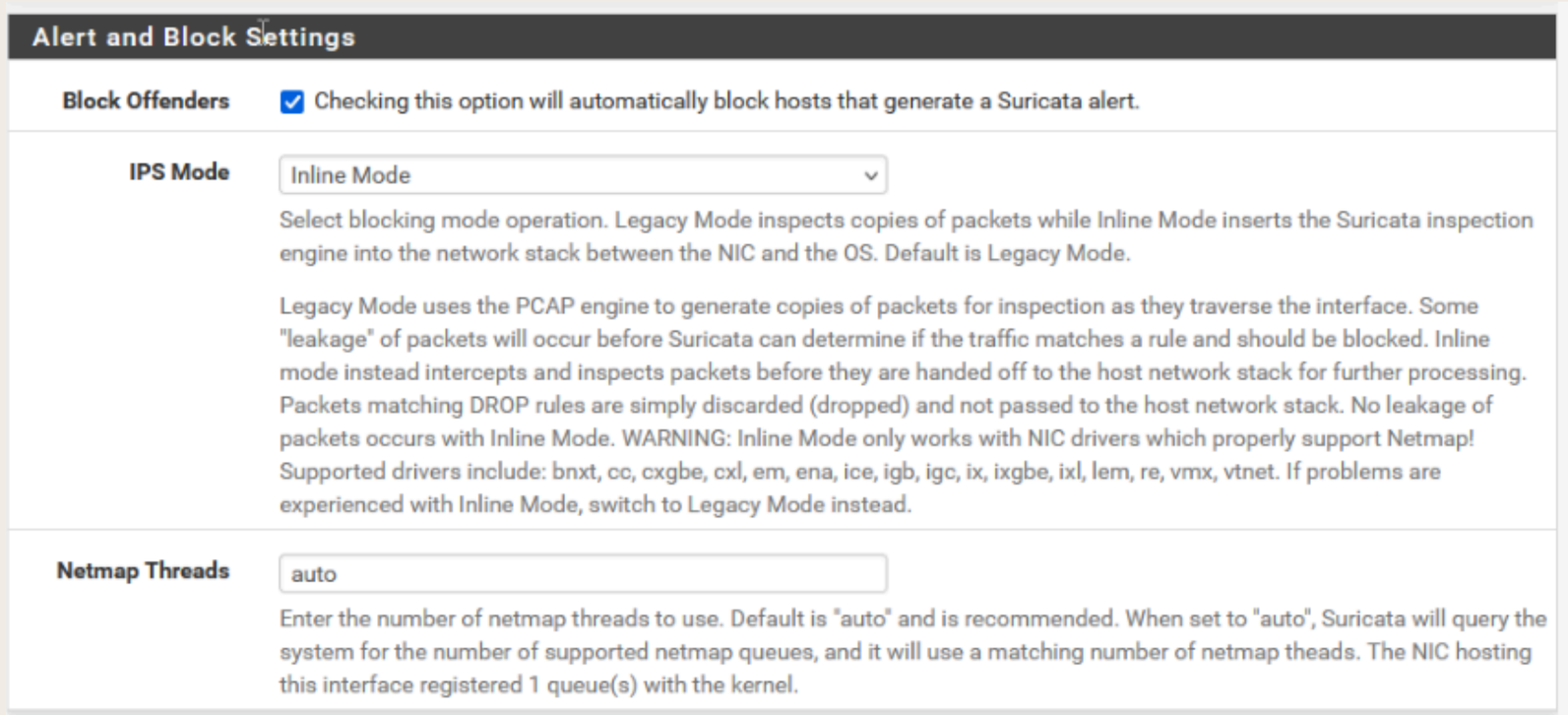
Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
03/29/2025 22:38:22	⚠	3	TCP	Not Assigned	192.168.20.82	51329	192.168.100.10	80	1:100001	Tentative de connexion HTTP détectée



Même chose pour l'alerte pour TCP, on voit ici que la connexion au serveur web a généré une alerte.

MISE EN PLACE DES BLOCAGES

ACTIVATION IPS



Pour activer l’ips je me rends dans les paramètres de l’interface LAN et coche la case “Block Offenders”.

MISE EN PLACE DES RÈGLES

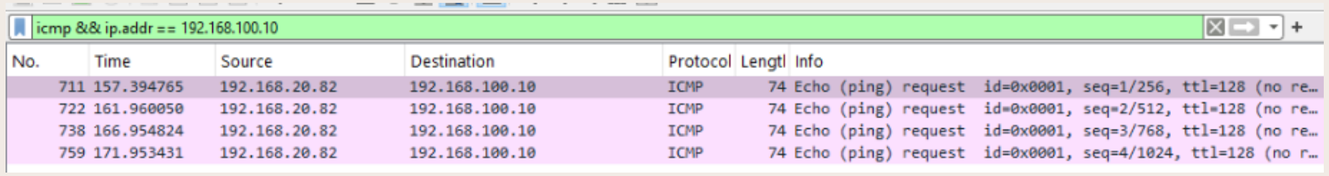
```
alert tcp any any -> $HOME_NET 80 (msg:"Tentative de connexion HTTP détectée"; sid:100001; rev:1;)

alert icmp any any -> $HOME_NET any (msg:"Requête ICMP détectée"; sid:100002; rev:1;)

pass tcp $HOME_NET any -> 192.168.100.1 any (msg:"HTTP autorisé pour IP"; sid:200003; rev:1;)

pass icmp $HOME_NET any -> 192.168.100.1 any (msg:"Ping autorisé pour IP"; sid:200004; rev:1;)

drop tcp any any -> $HOME_NET any (msg:"Connexion HTTP bloquée"; sid:100003; rev:1;)

drop icmp any any -> $HOME_NET any (msg:"Ping bloqué"; sid:100004; rev:1;)
```

Pour la mise en place des règles de blocage je mets d'abord en place des règles qui permettent de faire exception à l'IP "192.168.100.1" qui est l'interface LAN de mon Pfsense et la bloquer enlèverait l'accès au Web du serveur. Ensuite je mets en place une règle de blocage pour le TCP ainsi que ICMP.

RÉALISATION TEST

TEST BLOCAGE ICMP

03/30/2025 15:57:09	⚠	3	ICMP	Not Assigned	192.168.20.82	8	192.168.100.10	0	1:100002	Requête ICMP détectée
03/30/2025 15:57:09	👎	3	ICMP	Not Assigned	192.168.20.82	8	192.168.100.10	0	1:100004	Ping bloqué

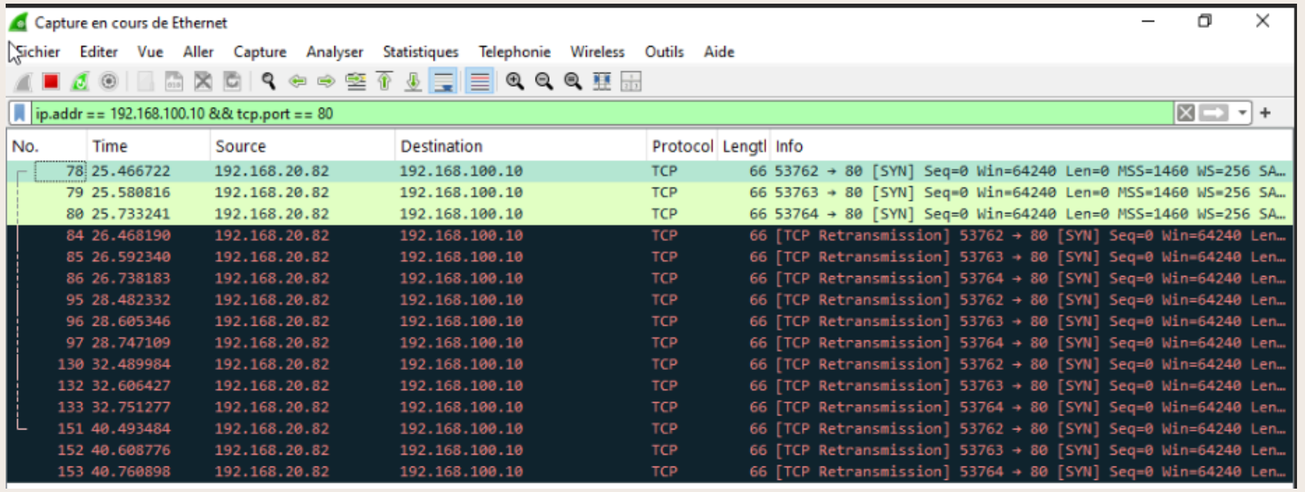



```
C:\Windows\system32>ping 192.168.100.10

Envoi d'une requête 'Ping'  192.168.100.10 avec 32 octets de données :
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.
Délai d'attente de la demande dépassé.

Statistiques Ping pour 192.168.100.10:
    Paquets : envoyés = 4, reçus = 0, perdus = 4 (perte 100%),
```

On peut ici voir que le ping ne passe plus et que cela a généré une alerte de ping ainsi que celle du ping bloqué.

TEST BLOCAGE HTTP

03/30/2025 03:09:17	⚠	3	TCP	Not Assigned	192.168.20.82	53817	192.168.100.10	80	1:100001	Tentative de connexion HTTP détectée
03/30/2025 03:09:17	👎	3	TCP	Not Assigned	192.168.20.82	53817	192.168.100.10	80	1:100003	Connexion HTTP bloquée



Pour le blocage TCP j’essaie de me connecter à mon serveur WEB depuis l’extérieur. On peut ici voir que la communication ne fonctionne plus et que les alertes se sont bien générées.