

PRÉSENTÉ PAR DRUELLE NICOLAS

TP-IDS/IPS

CAHIER DES CHARGES

-Installer Suricata

-Configurer l'interface LAN sur Suricata

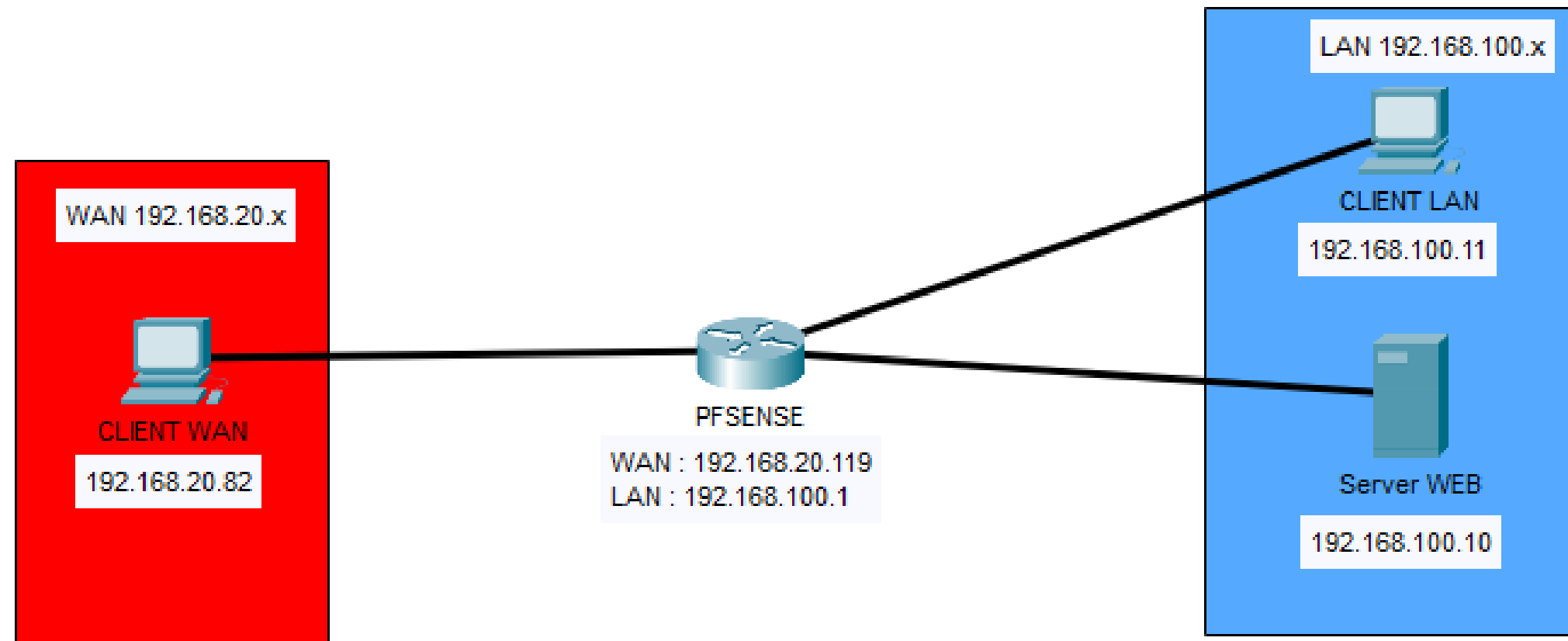
-Mettre en place les alertes

-Réalisations des tests pour les alertes

-Mettre en place les blocages

-Réalisations des tests pour les blocages

TOPOLOGIE



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

System / Package Manager / Installed Packages

✓	suricata	security	7.0.8_1	High Performance Network IDS, IPS and Security Monitoring engine by OISF.	 
Package Dependencies:					
 suricata-7.0.8					

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

CONFIGURATION INTERFACE

LAN SUR SURICATA

CONFIGURATION LAN

Services / Suricata

Interfaces

Global Settings

Updates

Alerts

Blocks

Files

Pass Lists

Suppress

Logs View

Logs Mgmt

SID Mgmt

Sync

IP Lists

Interface Settings Overview

Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions
LAN (vtnet1)		AUTO	DISABLED	LAN	

+ Add

Delete

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

CONFIGURATION LAN

Services / Suricata / LAN - Interface Settings

Interfaces

Global Settings

Updates

Alerts

Blocks

Files

Pass Lists

Suppress

Logs View

Logs Mgmt

SID Mgmt

Sync

IP Lists

LAN Settings

LAN Categories

LAN Rules

LAN Flow/Stream

LAN App Parsers

LAN Variables

LAN IP Rep

General Settings

Enable

☒ Checking this box enables Suricata inspection on the interface.

Interface

LAN (vtnet1)

Choose which interface this Suricata instance applies to. In most cases, you will want to choose LAN here if this is the first Suricata-configured interface.

Description

LAN

Enter a meaningful description here for your reference. The default is the pfSense interface friendly description.

Logging Settings

Send Alerts to System Log

☒ Suricata will send Alerts from this interface to the firewall's system log.
NOTE: the FreeBSD syslog daemon will automatically truncate exported messages to 480 bytes max.

Log Facility

LOCAL1

Select system log Facility to use for reporting. Default is LOCAL1.

Log Priority

NOTICE

Select system log Priority (Level) to use for reporting. Default is NOTICE.

Enable Stats Collection

☐ Suricata will periodically gather performance statistics for this interface. Default is Not Checked.

Enable HTTP Log

☒ Suricata will log decoded HTTP traffic for the interface. Default is Checked.

HTTP Log File Type

Regular

Select "Regular" to log to a conventional file, or choose UNIX "Datagram" or "Stream" Socket to log to an existing UNIX socket. Default is "Regular"

Append HTTP Log

☒ Suricata will append-to instead of clearing HTTP log file when restarting. Default is Checked.

Log Extended HTTP Info

☒ Suricata will log extended HTTP information. Default is Checked.

Une fois l’interface LAN créée 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

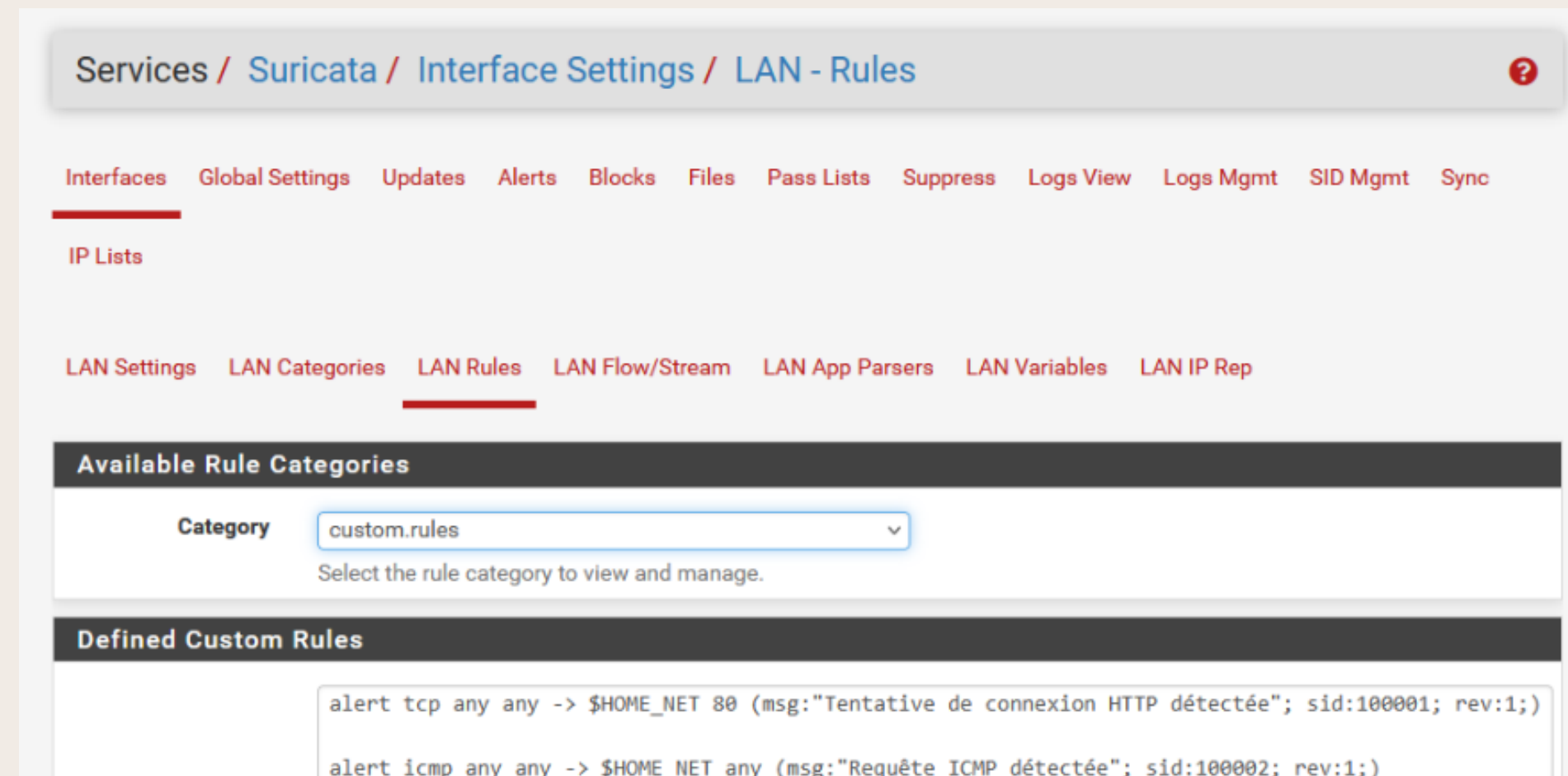
EXPLICATION DES RÉGLES

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 (Bloquent et enregistrent dans les logs) pass (Autorise et ignore le trafic) reject (Bloquent 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 règle

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

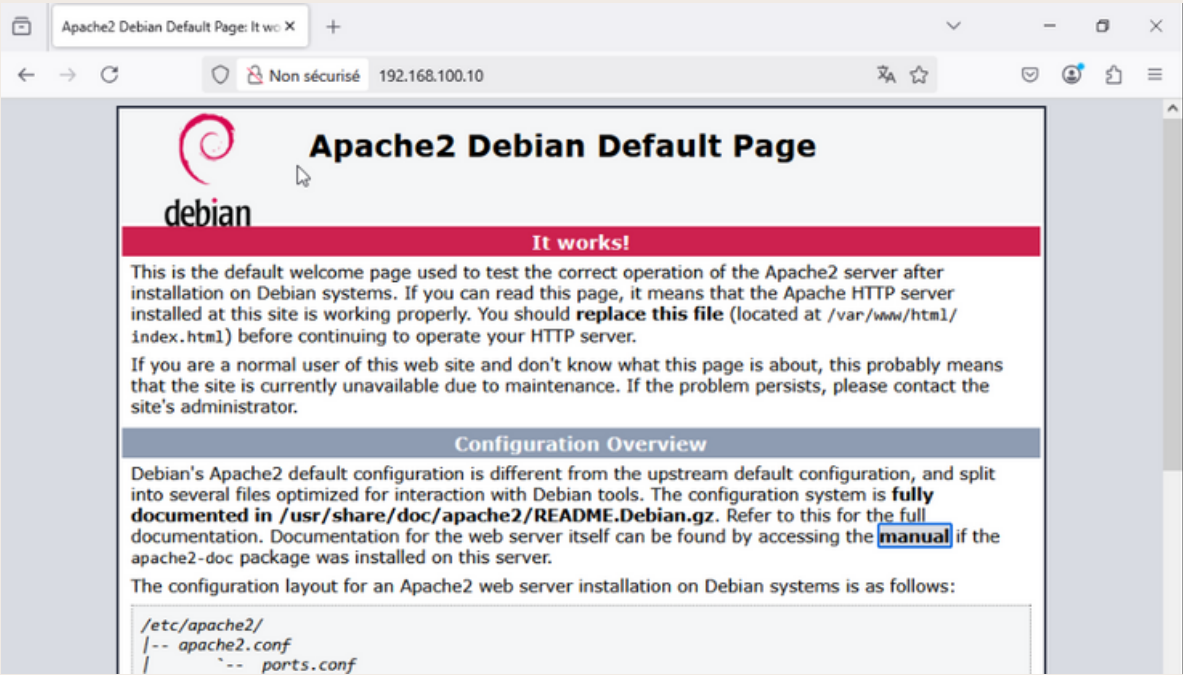
Last 250 Alert Entries. (Most recent entries are listed first)										
Date	Action	Pri	Proto	Class	Src	SPort	Dst	DPort	GID:SID	Description
03/29/2025 22:32:46		3	ICMP	Not Assigned	192.168.20.82  	0	192.168.100.10  	0	1:100002  	Requête ICMP détectée

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

TEST ALERTE HTTP

1189	243.041706	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

Alert and Block Settings

Block Offenders

☒ Checking this option will automatically block hosts that generate a Suricata alert.

IPS Mode

Inline Mode

Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Suricata inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.

Legacy Mode uses the PCAP engine to generate copies of packets for inspection as they traverse the interface. Some "leakage" of packets will occur before Suricata can determine if the traffic matches a rule and should be blocked. Inline mode instead intercepts and inspects packets before they are handed off to the host network stack for further processing. Packets matching DROP rules are simply discarded (dropped) and not passed to the host network stack. No leakage of packets occurs with Inline Mode. WARNING: Inline Mode only works with NIC drivers which properly support Netmap! Supported drivers include: bnxt, cc, cxgbe, cxl, em, ena, ice, igb, igc, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.

Netmap Threads

auto

Enter the number of netmap threads to use. Default is "auto" and is recommended. When set to "auto", Suricata will query the system for the number of supported netmap queues, and it will use a matching number of netmap threads. The NIC hosting this interface registered 1 queue(s) with the kernel.

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 BLOCCAGE 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
					 		 		  	

icmp && ip.addr == 192.168.100.10						
No.	Time	Source	Destination	Protocol	Length	Info
711	157.394765	192.168.20.82	192.168.100.10	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=128 (no re...
722	161.960050	192.168.20.82	192.168.100.10	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=128 (no re...
738	166.954824	192.168.20.82	192.168.100.10	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=128 (no re...
759	171.953431	192.168.20.82	192.168.100.10	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=128 (no r...

```
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 BLOCCAGE 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

Capture en cours de Ethernet										
Fichier Editer Vue Aller Capture Analyser Statistiques Telephonie Wireless Outils Aide										
ip.addr == 192.168.100.10 && tcp.port == 80										
No.	Time	Source	Destination	Protocol	Length	Info				
78	25.466722	192.168.20.82	192.168.100.10	TCP	66	53762 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SA...				
79	25.580816	192.168.20.82	192.168.100.10	TCP	66	53763 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SA...				
80	25.733241	192.168.20.82	192.168.100.10	TCP	66	53764 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SA...				
84	26.468190	192.168.20.82	192.168.100.10	TCP	66	[TCP Retransmission] 53762 → 80 [SYN] Seq=0 Win=64240 Len...				
85	26.592340	192.168.20.82	192.168.100.10	TCP	66	[TCP Retransmission] 53763 → 80 [SYN] Seq=0 Win=64240 Len...				
86	26.738183	192.168.20.82	192.168.100.10	TCP	66	[TCP Retransmission] 53764 → 80 [SYN] Seq=0 Win=64240 Len...				
95	28.482332	192.168.20.82	192.168.100.10	TCP	66	[TCP Retransmission] 53762 → 80 [SYN] Seq=0 Win=64240 Len...				
96	28.605346	192.168.20.82	192.168.100.10	TCP	66	[TCP Retransmission] 53763 → 80 [SYN] Seq=0 Win=64240 Len...				
97	28.747109	192.168.20.82	192.168.100.10	TCP	66	[TCP Retransmission] 53764 → 80 [SYN] Seq=0 Win=64240 Len...				
130	32.489984	192.168.20.82	192.168.100.10	TCP	66	[TCP Retransmission] 53762 → 80 [SYN] Seq=0 Win=64240 Len...				
132	32.606427	192.168.20.82	192.168.100.10	TCP	66	[TCP Retransmission] 53763 → 80 [SYN] Seq=0 Win=64240 Len...				
133	32.751277	192.168.20.82	192.168.100.10	TCP	66	[TCP Retransmission] 53764 → 80 [SYN] Seq=0 Win=64240 Len...				
151	40.493484	192.168.20.82	192.168.100.10	TCP	66	[TCP Retransmission] 53762 → 80 [SYN] Seq=0 Win=64240 Len...				
152	40.608776	192.168.20.82	192.168.100.10	TCP	66	[TCP Retransmission] 53763 → 80 [SYN] Seq=0 Win=64240 Len...				
153	40.760898	192.168.20.82	192.168.100.10	TCP	66	[TCP Retransmission] 53764 → 80 [SYN] Seq=0 Win=64240 Len...				

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.