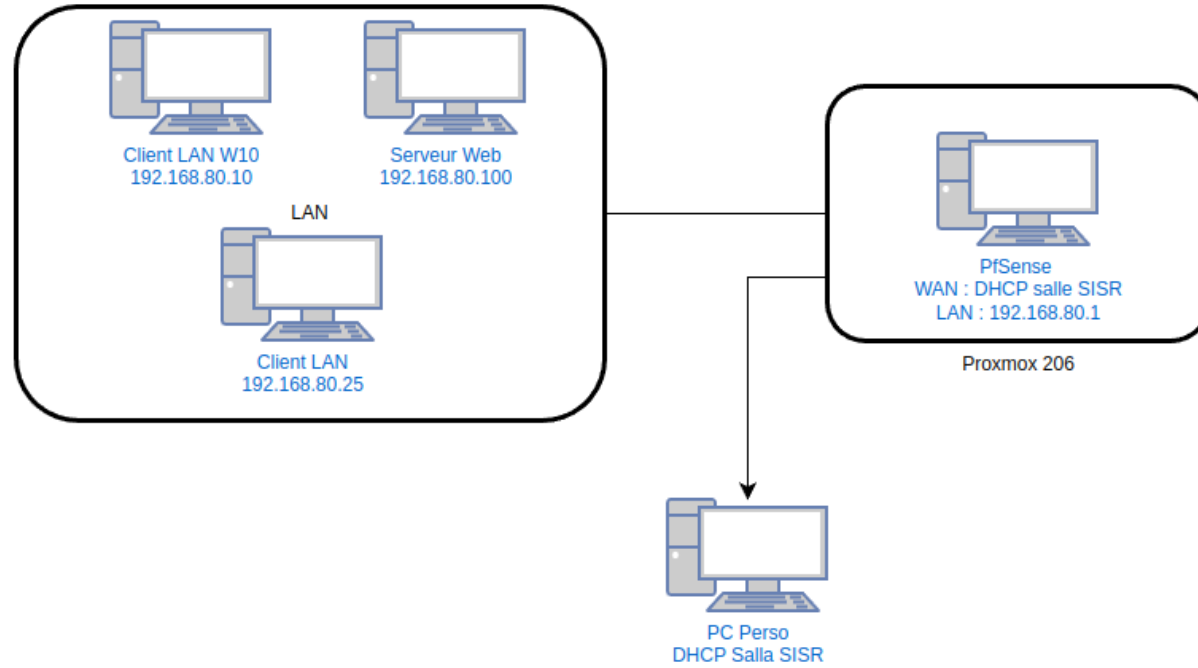


**TP – B3**  
**IDS / IPS**

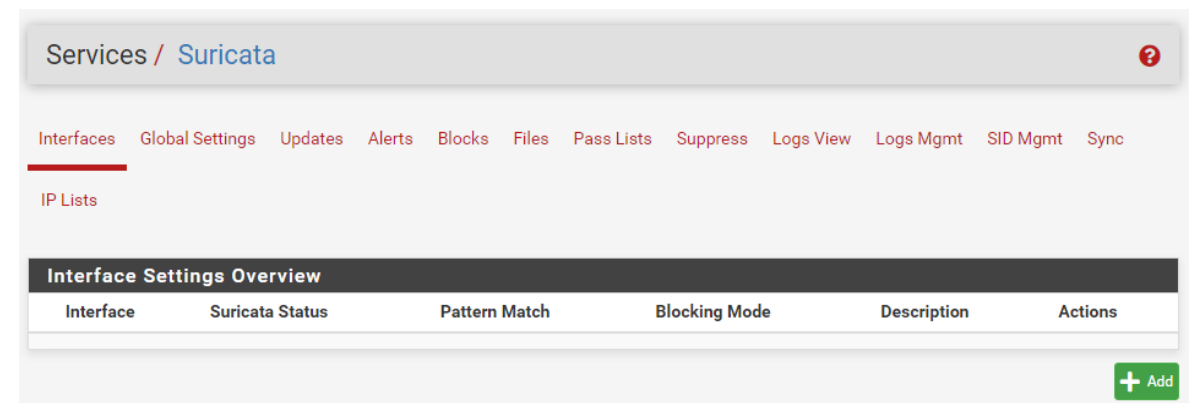
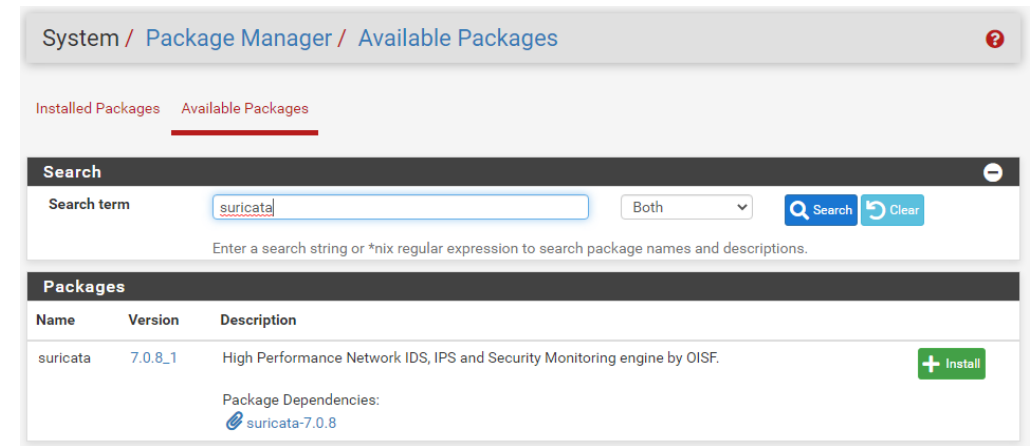


# Infrastructure



# Installation et configuration de Suricata sur PfSense

- Dans notre PfSense, nous allons dans le package manager et nous recherchons le package Suricata.
- Ensuite dans l'onglet Service, nous retrouvons Suricata.



# Installation et configuration de Suricata sur PfSense

- Ajout des règles pour IDS, pour alerter sur les connexions HTTP et ping.

<b>Règle n°1</b>	Alert	tcp	Any	Any	->	80	Any
<b>Regle n°2</b>	Alert	icmp	Any	Any	->	Any	Any
<b>Description</b>	Alerte	Protocol	Source	Source	Destination	Port / source	source

## Available Rule Categories

Category

Select the rule category to view and manage.


## Defined Custom Rules


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

```
alert icmp any any -> any any (msg:"Tentative de ping"; sid:100002; rev:1;)
```

# Installation et configuration de Suricata sur PfSense

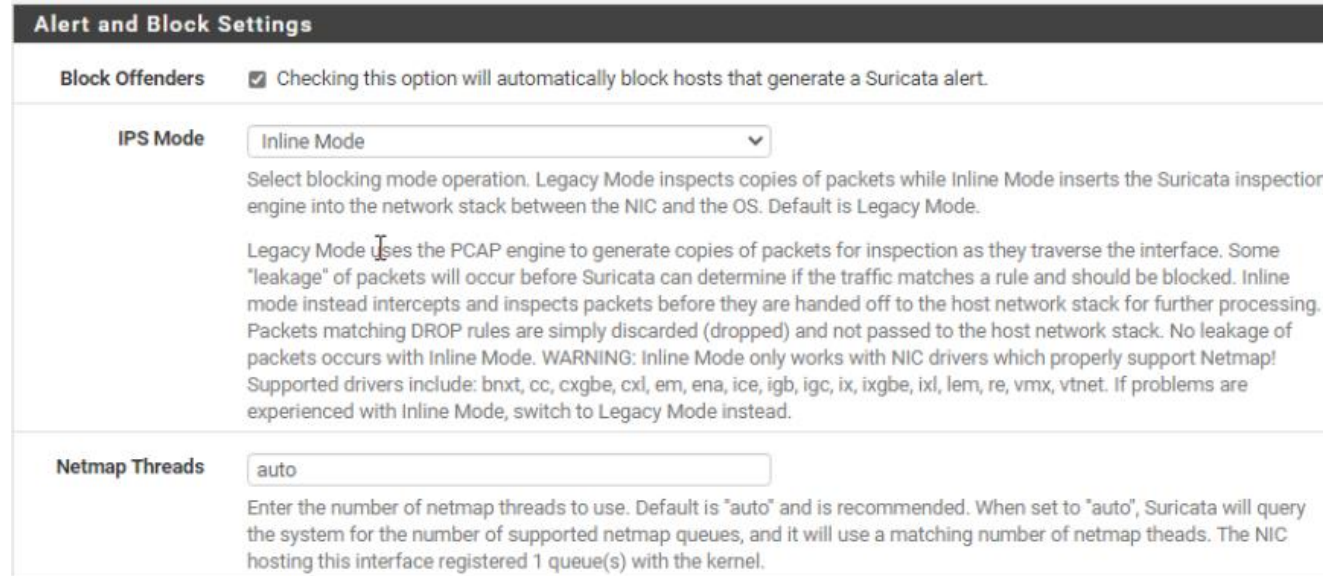
- Après avoir ajouté notre règle LAN dans l'onglet LAN rules, nous allons tester cela.
- Nous tapons l'adresse de notre serveur Web afin de le consulter et nous voyons que la règle remonte en nous indiquant que nous passons par le protocole TCP
- Ping depuis le client LAN vers notre serveur web
- On remarque qu'un message apparaît à la suite des pings indiquant une requête 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 14:49:39		3	TCP	Not Assigned	192.168.80.10	60401	192.168.80.100	80	1:100001	Tentative de connexion HTTP détectée

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 14:36:22		3	ICMP	Not Assigned	192.168.80.25	8	192.168.80.100	0	1:100002	Requete ICMP détectée

# Passage en mode IPS

- Dans la configuration de Suricata, nous allons cocher la case **Block Offenders**, cela aura pour effet de bloquer les différents éléments offensifs qui seront ajoutés à nos règles.



The screenshot displays the 'Alert and Block Settings' section of a configuration interface. It features three main settings:

- Block Offenders:** A checkbox is checked, with the text: "Checking this option will automatically block hosts that generate a Suricata alert."
- IPS Mode:** A dropdown menu is set to "Inline Mode". Below it, a detailed explanation states: "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." A further note explains: "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:** A text input field contains the value "auto". Below it, the text reads: "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."

# Passage en mode IPS

- Modifications des règles pour bloquer les connexions suspectes.
- Ajout d'une règle dans l'onglet Firewall pour que la connexion soit rejetée par IPS

<b>Règle 1</b>	Reject	Tcp	Any	Any	->	80	Any
<b>Regle 2</b>	reject	Icmp	Any	Any	->	Any	Any
<b>Description</b>	Rejet	Protocol	Source	Source	Destination	Port / source	source

**Available Rule Categories**

Category:    
Select the rule category to view and manage.

---

**Defined Custom Rules**

```

alert tcp any any -> 80 any (msg:"Tentative de connexion HTTP détectée"; sid:100001; rev:1;)
alert icmp any any -> any any (msg:"Tentative de ping"; sid:100002; rev:1;)
reject tcp any any -> 80 any (msg:"Connexion HTTP rejetée"; sid:100005; rev:1;)
reject icmp any any -> any any (msg:"Requete ICMP rejetée"; sid:100006; rev:1;)
    
```

Firewall / Rules / LAN

Floating WAN LAN

**Rules (Drag to Change Order)**

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
<input checked="" type="checkbox"/>	0/21.78 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule
<input type="checkbox"/>	0/82 KiB	IPv4 TCP	*	*	*	80 (HTTP)	*	none		Block HTTP

# Test des règles

- Nous voyons que la règle du rejet HTTP remonte bien ainsi que celle du Ping.
- Le Ping ne passe plus vers le PfSense.
- Et lorsqu'on se rend sur notre navigateur, nous voyons que nous ne pouvons plus accéder à notre serveur web.

## 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
04/01/2025 14:26:37		3	TCP	Not Assigned	192.168.80.10 	61199	2.23.22.11 	80	1:100005 	Connexion HTTP rejetée

## 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
04/01/2025 13:26:51		3	ICMP	Not Assigned	192.168.80.10 	8	192.168.80.1 	0	1:100006 	Requete ICMP rejetée

ERROR: The requested URL could not be retrieved

The following error was encountered while trying to retrieve the URL: /

**Invalid URL**

Some aspect of the requested URL is incorrect.

Some possible problems are:

- Missing or incorrect access protocol (should be "http://" or similar)
- Missing hostname
- Illegal double-escape in the URL-Path
- Illegal character in hostname; underscores are not allowed.

Your cache administrator is [admin@localhost](mailto:admin@localhost).

Generated Tue, 01 Apr 2025 14:53:07 GMT by localhost (squid/6.3)

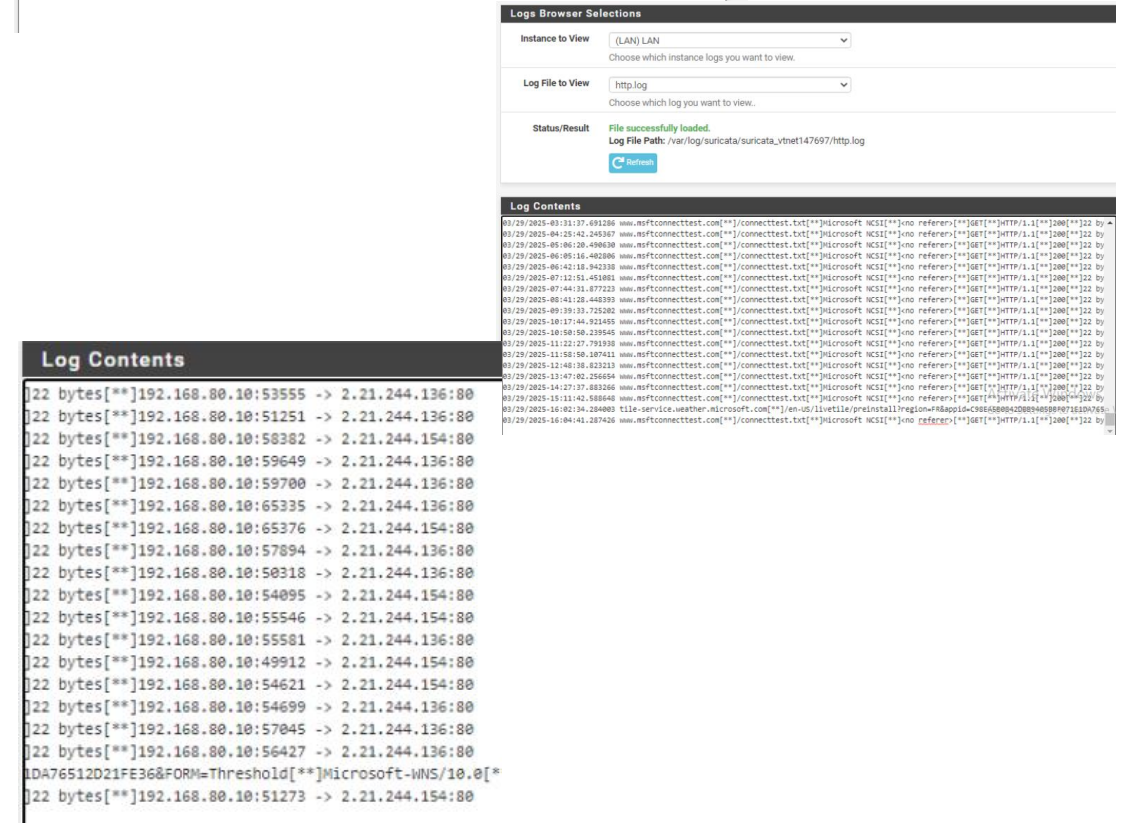
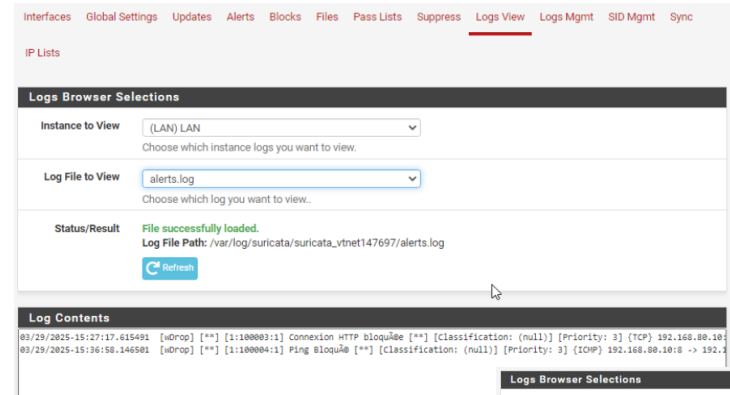
```
C:\Users\sio>ping 192.168.80.1
Pinging 192.168.80.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.80.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```



# Analyse des logs

- Dans suricata, il est possible de consulter les fichiers de log directement via l'interface PfSense.
- Nous voyons dans le fichier alerts.log les informations précédentes qui remontent.
- Sur le fichier http.log, nous pouvons voir en détail les sites consultés, principalement par le client Windows 10 pour de la récupération de mise à jour.



# Amélioration des règles

- alert tcp any any -> any 80 (msg:"Tentative de connexion HTTP détectée"; **flow:to\_server,established;** **content:"GET "; http\_method;** sid:1000001; rev:2;)
- alert icmp any any -> any any (msg:"Tentative de ping détectée"; **itype:8;** sid:1000002; rev:2;)
- reject tcp any any -> any 80 (msg:"Connexion HTTP rejetée"; **flow:to\_server,established;** **content:"Host:";** **http\_header;** sid:1000005; rev:2;)
- reject icmp any any -> any any (msg:"Requête ICMP rejetée"; **itype:8;** sid:1000006; rev:2;)

# Amélioration des règles - Explications

- **Flow: to\_server, established** : seules les connexions actives et complètes sont prises en compte.
- **content:"GET "; http\_method** : grâce à GET qui recherche une chaîne, http method complète le contenu : "GET" en indiquant le champ de méthode à rechercher et donc permet d'éviter les faux positifs.
- **Content:"host:"** ; : recherche "host:" dans le paquet et permet d'identifier une requête http contenant un champ host pouvant être utilisé pour spécifier le serveur cible.
- **Http\_header** ; : assure que "host:" ; est bien situé dans les en-têtes http et permet d'empêcher les faux positifs qui pourraient apparaître ailleurs dans un paquet.
- **Itype:8** ; : filtre précisément les pings avec uniquement les paquets ICMP echo request pris en compte, cela évite les alertes ou blocages d'autres types de messages ICMP ( Destination Unreachable) et sans itype:8, cela déclenche des alertes sur n'importe quel trafic ICMP.