

# Cours Virtualisation des réseaux

Nantes Ynov Campus – 2022-2023

## Activité Pratique 4

### Mise en place d'un IDS/IPS sur Pfsense

#### Objectifs :

⇒ Découvrir et essayer pratiquement un système de détection et prévention d'intrusion

#### Pré requis

Pour réaliser ce TP, vous devez avoir terminé l'activité pratique précédente et disposer d'au moins deux machines sur le réseau LAN afin de pouvoir suivre les étapes indiquées dans les copies d'écrans suivantes :

**pfSense** COMMUNITY EDITION

Système ▾ Interfaces ▾ Pare-feu ▾ Services ▾ VPN ▾ État ▾ Diagnostics ▾ Aide ▾

Système /

- Assistant de configuration
- Avancé
- Configuration générale
- Déconnexion (admin)
- Gestionnaire d'utilisateurs
- Gestionnaire de certificats
- Gestionnaire de paquets**
- Mettre à jour
- Routage
- Synchronisation à haute disponibilité

Ne pas utiliser ".local" comme la partie finale du domaine (TLD), le domaine ".local" est utilisé en mode large par mDNS (y compris Avahi et Apple OS X Bonjour / Rendezvous / Airprint / Airplay ), et certains systèmes Windows et périphériques en réseau. Ceux-ci ne se connecteront pas correctement si le routeur utilise ".local". Des alternatives telles que ".local.lan" ou ".mylocal" sont sécurisées.

### Paramètres du serveur DNS

Serveurs DNS	DNS Hostname	
192.168.232.104		Supprimer
8.8.8.8		Supprimer

Adresse  
Saisir les adresses IP des serveurs DNS utilisés par le système. Ceux-ci sont également utilisés pour le service DHCP, le DNS Forwarder et le serveur de résolution DNS lorsqu'il est activé.

Nom d'hôte  
Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).

Ajouter un serveur DNS [+ Ajouter un serveur DNS](#)

**pfSense** COMMUNITY EDITION

Système ▾ Interfaces ▾ Pare-feu ▾ Services ▾ VPN ▾ État ▾ Diagnostics ▾ Aide ▾

Système / Gestionnaire de paquets / Paquets disponibles

Paquets installés Paquets disponibles

### Recherche

Terme de recherche  Les deux [Recherche](#) [Effacer](#)

Entrer une phrase de recherche ou une expression régulière \*nix pour rechercher dans les noms et description de paquets.

### Paquets

Nom	Version	Description	
acme	0.6.9_3	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates. Dépendances du paquet: <a href="#">pecl-ssh2-1.2</a> <a href="#">socat-1.7.3.4_1</a> <a href="#">php74-7.4.15</a> <a href="#">php74-ftp-7.4.15</a>	<a href="#">+ Install</a>
apcupsd	0.3.91_9	"apcupsd" can be used for controlling all APC UPS models It can monitor and log the current power and battery status, perform automatic shutdown, and can run in network mode in order to power down other hosts on a LAN Dépendances du paquet: <a href="#">apcupsd-3.14.14_4</a>	<a href="#">+ Install</a>
arping	1.2.2.2	Broadcasts a who-has ARP packet on the network and prints answers. Dépendances du paquet: <a href="#">arping-2.21</a>	<a href="#">+ Install</a>

Système / Gestionnaire de paquets / Paquets disponibles

Paquets installés Paquets disponibles

Recherche

Terme de recherche

snort

Les deux ▾

Recherche

Effacer

Entrer une phrase de recherche ou une expression régulière \*nix pour rechercher dans les noms et description de paquets.

Paquets

Nom	Version	Description	
acme	0.6.9_3	Automated Certificate Management Environment, for automated use of LetsEncrypt certificates.  Dépendances du paquet: pecl-ssh2-1.2 socat-1.7.3.4_1 php74-7.4.15 php74-ftp-7.4.15	+ Install
apcupsd	0.3.91_9	"apcupsd" can be used for controlling all APC UPS models It can monitor and log the current power and battery status, perform automatic shutdown, and can run in network mode in order to power down other hosts on a LAN  Dépendances du paquet: apcupsd-3.14.14_4	+ Install
arping	1.2.2_2	Broadcasts a who-has ARP packet on the network and prints answers.  Dépendances du paquet: arping-2.21	+ Install

Système / Gestionnaire de paquets / Paquets disponibles

Paquets installés Paquets disponibles

Recherche

Terme de recherche

snort

Les deux ▾

Recherche

Effacer

Entrer une phrase de recherche ou une expression régulière \*nix pour rechercher dans les noms et description de paquets.

Paquets

Nom	Version	Description	
snort	4.1.6	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.  Dépendances du paquet: snort-2.9.20	+ Install

Système / Gestionnaire de paquets / Installateur de paquets

Paquets installés Paquets disponibles Installateur de paquets

Confirmation requise pour installer le paquet pfSense-pkg-snort.

✓ Confirmer

Veillez patienter pendant que l'installation de **pfSense-pkg-snort** se termine.  
Cela peut prendre plusieurs minutes. Ne quittez pas et ne rafraîchissez pas la page !

Paquets installés   Paquets disponibles   Installateur de paquets

#### Installation du paquet

```
All repositories are up to date.
The following 5 package(s) will be affected (of 0 checked):

New packages to be INSTALLED:
  daq: 2.2.2_3 [pfSense]
  libdnet: 1.13_3 [pfSense]
  libpcap: 1.9.1_1 [pfSense]
  pfSense-pkg-snort: 4.1.3_2 [pfSense]
  snort: 2.9.17 [pfSense]

Number of packages to be installed: 5

The process will require 10 MiB more space.
2 MiB to be downloaded.
[1/5] Fetching pfSense-pkg-snort-4.1.3_2.txz: ..... done
```

**pfSense-pkg-snort** installé avec succès

Paquets installés   Paquets disponibles   Installateur de paquets

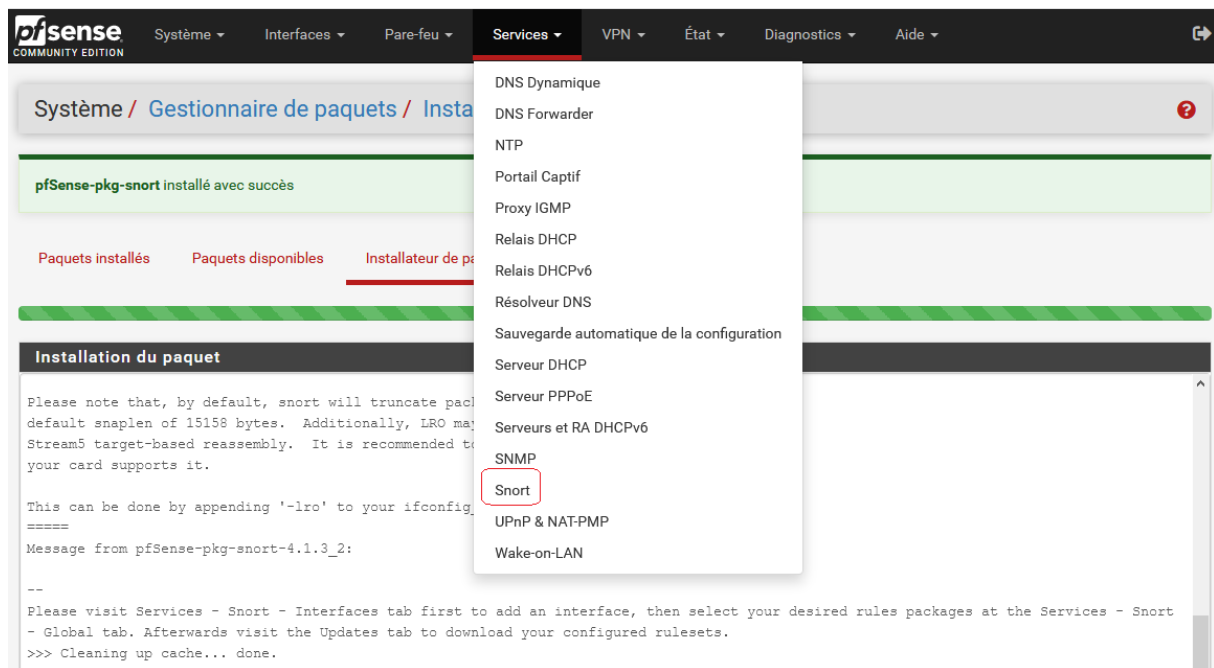
#### Installation du paquet

```
Please note that, by default, snort will truncate packets larger than the
default snaplen of 15158 bytes.  Additionally, LRO may cause issues with
Stream5 target-based reassembly.  It is recommended to disable LRO, if
your card supports it.

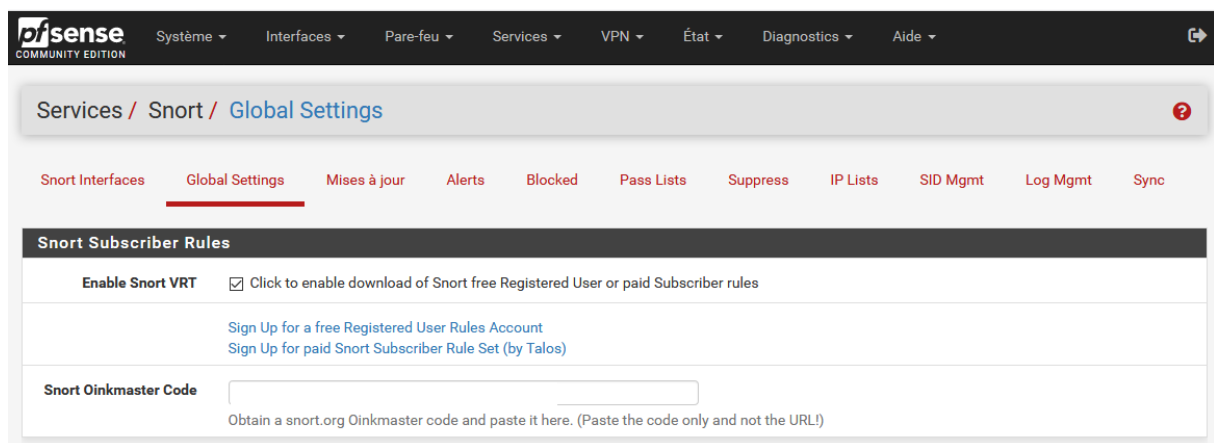
This can be done by appending '-lro' to your ifconfig_ line in rc.conf.
=====
Message from pfSense-pkg-snort-4.1.3_2:

--
Please visit Services - Snort - Interfaces tab first to add an interface, then select your desired rules packages at the Services - Snort
- Global tab. Afterwards visit the Updates tab to download your configured rulesets.
>>> Cleaning up cache... done.
Succès
```

Ensuite se rendre dans services -> Snort



Après l'installation procéder à la configuration des règles de détection d'intrusion



S'inscrire sur le site [https://snort.org/users/sign\\_up](https://snort.org/users/sign_up) de snort pour obtenir un code oinkmaster permettant de télécharger les règles disponible pour la communauté

## Email

Please enter your Email address

## Password

## Password confirmation


☐ Agree to [Snort license](#)

Subscribe to Snort mailing lists?

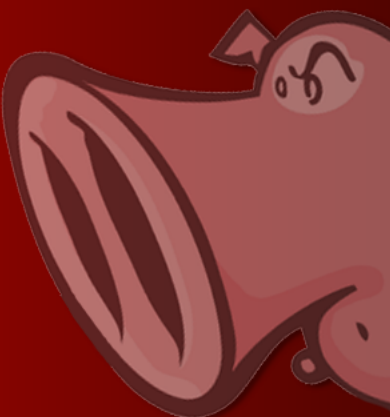
☒ Snort-users ☐ Snort-sigs ☐ Snort-devel ☐ Snort-openappid

You will receive an email confirmation that will require your action if you select any of these boxes

Checking one of above boxes will subscribe you to the respective mailing list. You will receive a confirmation email, (separate from your confirmation email from Snort.org to confirm your account) where you will need to confirm your subscription.

☐ Je ne suis pas un robot   
reCAPTCHA  
Confidentialité - Conditions

[Sign up](#)




Cliquez sur votre compte en haut à droite


[Rule Doc Search](#)

[Documents](#) [Downloads](#) [Products](#) [Community](#) [Talos](#) [Resources](#) [Contact](#)

Protect your network with the world's most powerful Open Source detection software.

[Get Started](#) [Download Rules](#) [Documents](#)





**Snort 3.0 is here!**

Upgrade to experience a slew of new features and improvements.

[Upgrade Now](#)

Ainsi vous obtiendrez votre code oinkmaster

Account

Oinkcode

Subscription

Receipts

False Positive

Oinkcode

Regenerate

Documentation

How to use your oinkcode

Ensuite cocher la case permettant d'activer un ensemble de règles distribuées gratuitement par la communauté

Snort GPLv2 Community Rules	
Enable Snort GPLv2	<input checked="" type="checkbox"/> Click to enable download of Snort GPLv2 Community rules
The Snort Community Ruleset is a GPLv2 Talos certified ruleset that is distributed free of charge without any Snort Subscriber License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.	
Emerging Threats (ET) Rules	
Enable ET Open	<input checked="" type="checkbox"/> Click to enable download of Emerging Threats Open rules
ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.	
Enable ET Pro	<input type="checkbox"/> Click to enable download of Emerging Threats Pro rules
<a href="#">Sign Up for an ETPro Account</a> ETPro for Snort offers daily updates and extensive coverage of current malware threats.	

Paramétrage du dernier block concerne la périodicité de téléchargement des règles. Indiquer la durée de rétention d'une adresse bloquée

Rules Update Settings	
Update Interval	<div>1 DAY</div> <div>Please select the interval for rule updates. Choosing NEVER disables auto-updates.</div>
Update Start Time	<div>23:00</div> <div>Enter the rule update start time in 24-hour format (HH:MM). Default is 00 hours with a randomly chosen minutes value. Rules will update at the interval chosen above starting at the time specified here. For example, using a start time of 00:08 and choosing 12 Hours for the interval, the rules will update at 00:08 and 12:08 each day. The randomized minutes value should be retained to minimize the impact to the rules update site from large numbers of simultaneous requests.</div>
Hide Deprecated Rules Categories	<input checked="" type="checkbox"/> Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.
Disable SSL Peer Verification	<input type="checkbox"/> Click to disable verification of SSL peers during rules updates. This is commonly needed only for self-signed certificates. Default is not checked.
Paramètres généraux	
Remove Blocked Hosts Interval	<div>1 HOUR</div> <div>Please select the amount of time you would like hosts to be blocked. In most cases, one hour is a good choice.</div>
Remove Blocked Hosts After Deinstall	<input type="checkbox"/> Click to clear all blocked hosts added by Snort when removing the package. Default is checked.
Keep Snort Settings After Deinstall	<input checked="" type="checkbox"/> Click to retain Snort settings after package removal.
Startup/Shutdown Logging	<input checked="" type="checkbox"/> Click to output detailed messages to the system log when Snort is starting and stopping. Default is not checked.

Ensuite procéder à la mise à jour des règles

Snort InterfacesGlobal SettingsMises à jourAlertsBlockedPass ListsSuppressIP ListsSID MgmtLog MgmtSync

Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	Not Downloaded	Not Downloaded
Snort GPLv2 Community Rules	Not Downloaded	Not Downloaded
Emerging Threats Open Rules	Not Downloaded	Not Downloaded
Snort OpenAppID Detectors	Not Enabled	Not Enabled
Snort AppID Open Text Rules	Not Enabled	Not Enabled

Update Your Rule Set

Last UpdateInconnuResult: Inconnu

Update Rules

Force Update

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

Manage Rule Set Log

View Log

Clear Log

The log file is limited to 1024K in size and is automatically cleared when that limit is exceeded.

Logfile Size

Log file is empty

Patienter pendant le téléchargement des règles

Services / Snort / Update Rules

Snort InterfacesGlobal SettingsMises à jourAlertsBlockedPass ListsSuppressIP ListsSID MgmtLog MgmtSync

Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	Not Downloaded	Not Downloaded
Snort GPLv2 Community Rules	Not Downloaded	Not Downloaded
Emerging Threats Open Rules	Not Downloaded	Not Downloaded
Snort OpenAppID Detectors	Not Enabled	Not Enabled
Snort AppID Open Text Rules	Not Enabled	Not Enabled

Update Your Rule Set

Last UpdateInconnuResult: Inconnu

Update Rules

Force Update

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

Manage Rule Set Log

View Log

Clear Log

The log file is limited to 1024K in size and is automatically cleared when that limit is exceeded.

Rules Update Task

Updating rule sets may take a while ... please wait for the process to complete.

This dialog will auto-close when the update is finished.

Fermer



Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	f2a458153bf300d93e9b08a705305e4c	Friday, 20-Jan-23 20:31:43 CET
Snort GPLv2 Community Rules	27f9018a8f628613ee849fab665c1a59	Friday, 20-Jan-23 20:31:43 CET
Emerging Threats Open Rules	c2f61094211cfc8c7fb8072b715cd173	Friday, 20-Jan-23 20:31:43 CET
Snort OpenAppID Detectors	Not Enabled	Not Enabled
Snort AppID Open Text Rules	Not Enabled	Not Enabled
Feodo Tracker Botnet C2 IP Rules	Not Enabled	Not Enabled

Update Your Rule Set

Last Update

Jan-20 2023 20:31

Result: Success

Update Rules

Update Rules

Force Update

Click UPDATE RULES to check for and automatically apply any new posted updates for selected rules packages. Clicking FORCE UPDATE will zero out the MD5 hashes and force the download and application of the latest versions of the enabled rules packages.

Maintenant que les règles sont disponibles, ajouter l'interface permettant de se connecter au réseau

pfSense

COMMUNITY EDITION

Système ▾ Interfaces ▾ Pare-feu ▾ Services ▾ VPN ▾ État ▾ Diagnostics ▾ Aide ▾

Services / Snort / Interfaces

Snort Interfaces

Global Settings

Mises à jour

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
-----------	--------------	---------------	---------------	-------------	---------

Ajouter

Sélectionner l'interface sur lequel sera effectué l'écoute

Snort Interfaces

Global Settings

Mises à jour

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

None Paramètres

None Categories

None Règles

None Variables

None Preprocs

None IP Rep

None Journaux

Paramètres généraux

Activer

☒ Activer interface

Interface

LAN (em1)

Choose the interface where this Snort instance will inspect traffic.

Description

LAN

Enter a meaningful description here for your reference.

Snap Length

1518

Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.

Alert Settings	
<b>Send Alerts to System Log</b>	<input checked="" type="checkbox"/> Snort will send Alerts to the firewall's system log. Default is Not Checked.
<b>System Log Facility</b>	<div>LOG_AUTH</div> <div>Select system log Facility to use for reporting. Default is LOG_AUTH.</div>
<b>System Log Priority</b>	<div>LOG_ALERT</div> <div>Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.</div>
<b>Enable Packet Captures</b>	<input checked="" type="checkbox"/> Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file
<b>Packet Capture File Size</b>	<div>128</div> <div>Enter a value in megabytes for the packet capture file size limit. Default is 128 megabytes. When the limit is reached, the current packet capture file in directory /var/log/snort/snort_em057231 is rotated and a new file opened.</div>
<b>Enable Unified2 Logging</b>	<input type="checkbox"/> Checking this option will cause Snort to simultaneously log alerts to a unified2 binary format log file in the logging subdirectory for this interface. Default is Not Checked. Log size and retention limits for the Unified2 log should be configured on the LOG MGMT tab when this option is enabled.

Block Settings	
<b>Block Offenders</b>	<input checked="" type="checkbox"/> Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.
<b>IPS Mode</b>	<div>Legacy Mode</div> <div>Select blocking mode operation. Legacy Mode inspects copies of packets while Inline Mode inserts the Snort inspection engine into the network stack between the NIC and the OS. Default is Legacy Mode.</div> <div>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 Snort 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: bnxt, cc, cxgbe, cxl, em, em, ice, igb, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.</div>
<b>Supprimer les états</b>	<input checked="" type="checkbox"/> Checking this option will kill firewall established states for the blocked IP. Default is checked.
<b>Which IP to Block</b>	<div>BOTH</div> <div>Select which IP extracted from the packet you wish to block. Default is BOTH.</div>

Puis valider le reste des paramètres par défaut

## Paramétrer les catégories

LAN Paramètres	LAN Categories	LAN Règles	LAN Variables	LAN Preprocs	LAN IP Rep	LAN Journaux
<b>Automatic Flowbit Resolution</b>						
<b>Resolve Flowbits</b>		<input checked="" type="checkbox"/> If checked, Snort will auto-enable rules required for checked flowbits. Default is Checked. Snort will examine the enabled rules in your chosen rule categories for checked flowbits. Any rules that set these dependent flowbits will be automatically enabled and added to the list of files in the interface rules directory.				
<b>Snort Subscriber IPS Policy Selection</b>						
<b>Use IPS Policy</b>		<input checked="" type="checkbox"/> If checked, Snort will use rules from one of three pre-defined IPS policies in the Snort Subscriber rules. Default is Not Checked. Selecting this option disables manual selection of Snort Subscriber categories in the list below, although Emerging Threats categories may still be selected if enabled on the Global Settings tab. These will be added to the pre-defined Snort IPS policy rules from the Snort VRT.				
<b>IPS Policy Selection</b>		<div>Balanced</div> <div>Snort IPS policies are: Connectivity, Balanced, Security or Max-Detect.            Connectivity blocks most major threats with few or no false positives. Balanced is a good starter policy. It is speedy, has good base coverage level, and covers most threats of the day. It includes all rules in Connectivity. Security is a stringent policy. It contains everything in the first two plus policy-type rules such as a Flash object in an Excel file. Max-Detect is a policy created for testing network traffic through your device. This policy should be used with caution on production systems!</div>				

Sélectionner toutes les règles pour les appliquer

**Select the rulesets (Categories) Snort will load at startup**

- Category is auto-enabled by SID Mgmt conf files  
 - Category is auto-disabled by SID Mgmt conf files

Activator	Ruleset: Snort GPLv2 Community Rules
<input checked="" type="checkbox"/>	Snort GPLv2 Community Rules (Talos certified)

Activator	Ruleset: ET Open Rules	Activator	Ruleset: Snort Text Rules	Activator	Ruleset: Snort SO Rules	Snort OPENAPPID rules are not enabled.
<input checked="" type="checkbox"/>	emerging-activex.rules	<input checked="" type="checkbox"/>	snort_app-detect.rules	<input checked="" type="checkbox"/>	snort_browser-chrome.so.rules	
<input checked="" type="checkbox"/>	emerging-attack_response.rules	<input checked="" type="checkbox"/>	snort_blacklist.rules	<input checked="" type="checkbox"/>	snort_browser-ie.so.rules	
<input checked="" type="checkbox"/>	emerging-botcc.portgrouped.rules	<input checked="" type="checkbox"/>	snort_browser-chrome.rules	<input checked="" type="checkbox"/>	snort_browser-other.so.rules	
<input checked="" type="checkbox"/>	emerging-botcc.rules	<input checked="" type="checkbox"/>	snort_browser-firefox.rules	<input checked="" type="checkbox"/>	snort_browser-webkit.so.rules	
<input checked="" type="checkbox"/>	emerging-chat.rules	<input checked="" type="checkbox"/>	snort_browser-ie.rules	<input checked="" type="checkbox"/>	snort_exploit-kit.so.rules	
<input checked="" type="checkbox"/>	emerging-ciarmy.rules	<input checked="" type="checkbox"/>	snort_browser-other.rules	<input checked="" type="checkbox"/>	snort_file-executable.so.rules	
<input checked="" type="checkbox"/>	emerging-compromised.rules	<input checked="" type="checkbox"/>	snort_browser-plugins.rules	<input checked="" type="checkbox"/>	snort_file-flash.so.rules	

Ensuite aller tout en bas des règles pour valider leur application

<input checked="" type="checkbox"/>	snort_server-apache.rules
<input checked="" type="checkbox"/>	snort_server-iis.rules
<input checked="" type="checkbox"/>	snort_server-mail.rules
<input checked="" type="checkbox"/>	snort_server-mssql.rules
<input checked="" type="checkbox"/>	snort_server-mysql.rules
<input checked="" type="checkbox"/>	snort_server-oracle.rules
<input checked="" type="checkbox"/>	snort_server-other.rules
<input checked="" type="checkbox"/>	snort_server-samba.rules
<input checked="" type="checkbox"/>	snort_server-webapp.rules
<input checked="" type="checkbox"/>	snort_sql.rules
<input checked="" type="checkbox"/>	snort_x11.rules

Ensuite aller démarrer snort pour commencer l'écoute

**pfSense** COMMUNITY EDITION

Système ▾ Interfaces ▾ Pare-feu ▾ Services ▾ VPN ▾ État ▾ Diagnostics ▾ Aide ▾

Services / Snort / Interfaces

[Snort Interfaces](#)
[Global Settings](#)
[Mises à jour](#)
[Alerts](#)
[Blocked](#)
[Pass Lists](#)
[Suppress](#)
[IP Lists](#)
[SID Mgmt](#)
[Log Mgmt](#)
[Sync](#)

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/> LAN (em1)		AC-BNFA	LEGACY MODE	LAN	

pfSense  
COMMUNITY EDITION

Système ▾ Interfaces ▾ Pare-feu ▾ Services ▾ VPN ▾ État ▾ Diagnostics ▾ Aide ▾

Services / Snort / Interfaces

Snort Interfaces Global Settings Mises à jour Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

### Interface Settings Overview

Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/> LAN (em1)	<span style="color: green;">✓</span>	AC-BNFA	LEGACY MODE	LAN	

+ Ajouter Supprimer

Se rendre ensuite dans l'onglet « Alerts » pour vérifier s'il y'a des données qui remontent

pfSense  
COMMUNITY EDITION

Système ▾ Interfaces ▾ Pare-feu ▾ Services ▾ VPN ▾ État ▾ Diagnostics ▾ Aide ▾

Services / Snort / Alerts

Snort Interfaces Global Settings Mises à jour Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

### Alert Log View Settings

Interface to Inspect: LAN (em1) ▾ ☐ Auto-refresh view 250 Enregistrer  
Choose interface.. Alert lines to display.

Alert Log Actions Téléchargement Effacer

### Alert Log View Filter

+

### 0 Entries in Active Log

Date	Action	Pri	Proto	Class	IP Source	SPort	IP de destination	DPort	GID:SID	Description
------	--------	-----	-------	-------	-----------	-------	-------------------	-------	---------	-------------

Lancer un scan d'une machine sur le LAN puis vérifier que les alertes remontent bien

Services / Snort / Alerts

Snort Interfaces Global Settings Mises à jour Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

### Alert Log View Settings

Interface to Inspect: LAN (em1) ▾ ☐ Auto-refresh view 250 Enregistrer  
Choose interface.. Alert lines to display.

Alert Log Actions Téléchargement Effacer

### Alert Log View Filter

+

### 4 Entries in Active Log

Date	Action	Pri	Proto	Class	IP Source	SPort	IP de destination	DPort	GID:SID	Description
2021-04-03 20:57:37		1	TCP	Web Application Attack	192.168.232.188	40966	192.168.232.187	80	1:2024364	ET SCAN Possible Nmap User-Agent Observed
2021-04-03 20:57:37		1	TCP	Web Application Attack	192.168.232.188	40964	192.168.232.187	80	1:2024364	ET SCAN Possible Nmap User-Agent Observed
2021-04-03 20:57:37		1	TCP	Web Application Attack	192.168.232.188	40960	192.168.232.187	80	1:2024364	ET SCAN Possible Nmap User-Agent Observed
2021-04-03 20:57:37		1	TCP	Web Application Attack	192.168.232.188	40958	192.168.232.187	80	1:2024364	ET SCAN Possible Nmap User-Agent Observed