

22/01/2024

Procédure SNORT

PROCÉDURE SNORT

Sommaire

Table des matières

Table des illustrations.....	1
1- Introduction	2
1.1– Schéma	2
2. Installation de SNORT su PfSense.....	3
3. configuration de SNORT su PfSense	4
4. Configuration de l'interface.....	6
5. Vérification avec KALI	9

Table des illustrations

Figure 1 - Schéma réseau	3
--------------------------------	---

1- Introduction

Cette procédure explique comment paramétrer SNORT sur pfSense.

Snort est un système de détection d'intrusion et de prévention d'intrusion gratuit et open-source créé en 1998 par Martin Roesch. Développé à l'origine par la société Sourcefire, il est aujourd'hui maintenu par Cisco Systems à la suite du rachat de Sourcefire en 2013.

PROCÉDURE SNORT

1.1– Schéma

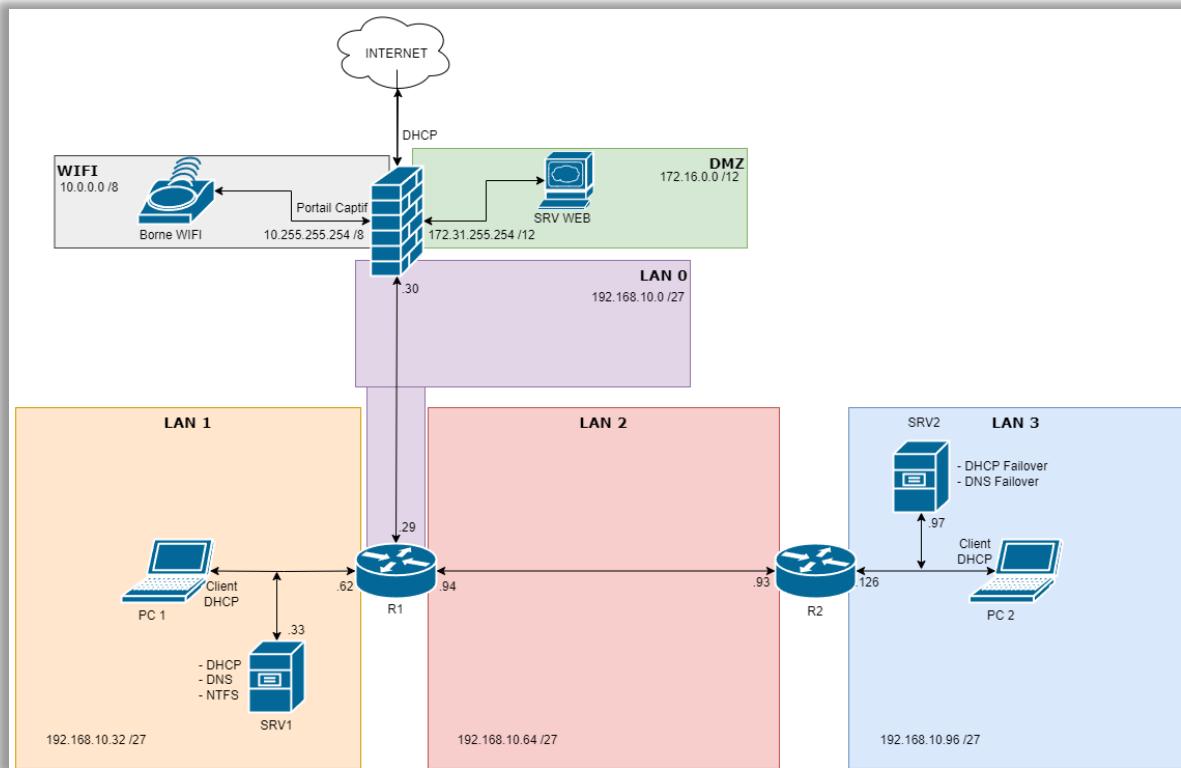
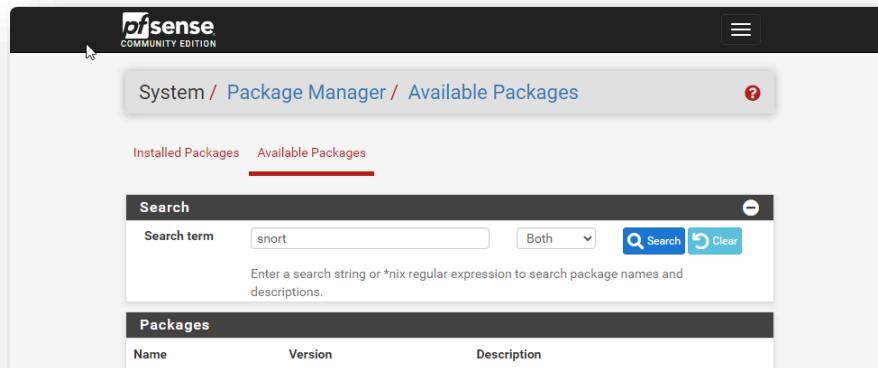


Figure 1 - Schéma réseau

2. Installation de SNORT su PfSense

2.1- Installer SNORT dans : System / Packet Manager / Available Packages

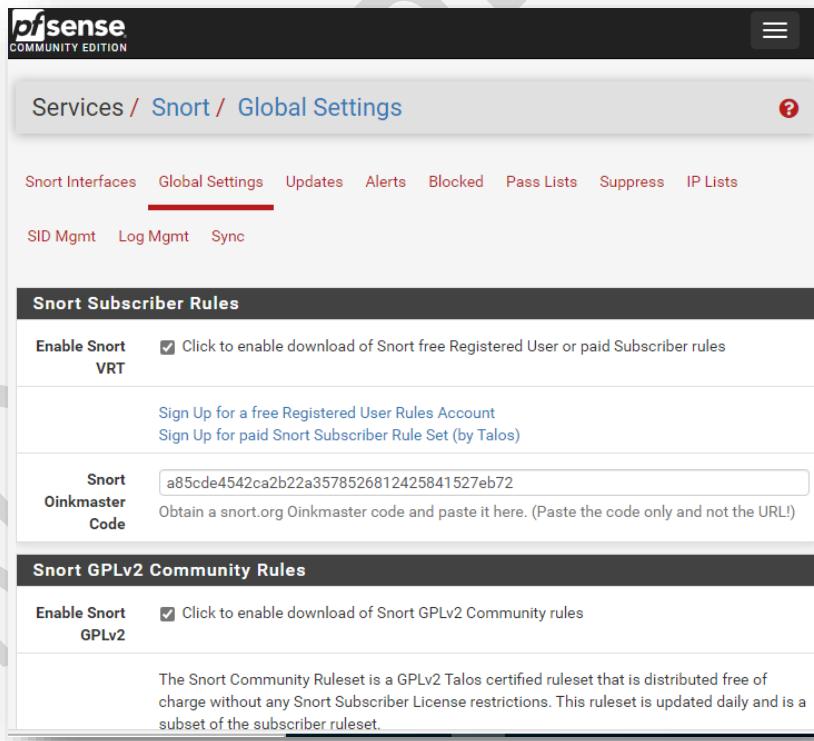
On clique ensuite sur **Install** puis **Confirm** et l'installation se lance !



3. configuration de SNORT su PfSense

3.1- Une fois installé, Snort apparaîtra dans l'onglet **Services**. Une fois rendu dessus, nous allons dans un premier temps aller sur l'onglet **Global Settings** :

2.2- La première étape est donc d'activer le téléchargement de règles gratuites, en cochant la première case (**Enable Snort VRT**). Il faudra renseigner une clé et pour l'obtenir il vous faudra créer un compte sur le site officiel de Snort.



2.4- Et ensuite nous pouvons cocher les cases :

- Enable Snort GPLv2, pour les règles communautaires ;
- Enable ET Open, qui sont des règles proposées par la société ET ;
- Enable OpenAppID, éventuellement, qui est une autre société ;

Procédure SNORT

The screenshot shows two main sections of the Snort configuration interface:

- Emerging Threats (ET) Rules**:
 - Enable ET Open**: Click to enable download of Emerging Threats Open rules. Description: ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.
 - Enable ET Pro**: Click to enable download of Emerging Threats Pro rules. Description: Sign Up for an ETPro Account. ETPro for Snort offers daily updates and extensive coverage of current malware threats.
- Sourcefire OpenAppID Detectors**:
 - Enable OpenAppID**: Click to enable download of Sourcefire OpenAppID Detectors. Description: The OpenAppID Detectors package contains the application signatures required by the AppID preprocessor and the OpenAppID text rules.
 - OpenAppID Version**: Installed Detection Package Version=366
 - Enable AppID Open Text Rules**: Click to enable download of the AppID Open Text Rules. Note: Note - the AppID Open Text Rules file is maintained by a volunteer contributor and hosted by the pfSense team. The URL for the file is https://files.netgate.com/openappid/appid_rules.tar.gz.

2.5- Et ensuite, pour les derniers paramètres il convient simplement de configurer l’update pour les différentes règles, c'est-à-dire le délai avant de vérifier les mises à jour pour les différentes règles ou pour de nouvelles : 12H est suffisant, mais en entreprise il conviendra de mettre 6H par précaution. Et pour l'heure de début de vérification pour les updates, j'ai choisi 01:00 (à vous de choisir l'heure qui vous convient).

The screenshot shows two main sections of the Snort configuration interface:

- FEODO Tracker Botnet C2 IP Rules**:
 - Enable FEODO Tracker Botnet C2 IP Rules**: Click to enable download of FEODO Tracker Botnet C2 IP rules. Description: Feodo Tracker tracks certain families that are related to, or that evolved from, Feodo. Originally, Feodo was an ebanking Trojan used by cybercriminals to commit ebanking fraud. Since 2010, various malware families evolved from Feodo, such as Cridex, Dridex, Geodo, Heodo and Emotet.
- Rules Update Settings**:
 - Update Interval**: NEVER. Description: Please select the interval for rule updates. Choosing NEVER disables auto-updates.
 - Update Start Time**: 00:12. Description: 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.
 - Hide Deprecated Rules Categories**: Click to hide deprecated rules categories in the GUI and remove them from the configuration. Default is not checked.
 - Disable SSL**: Click to disable verification of SSL peers during rules updates. This is commonly needed.

3.6- Une fois cliqué sur **Save**, nous pouvons nous rendre sur l'onglet **Updates** et manuellement mettre à jour les différentes règles que nous avons cochées juste avant (ici cela prendra un peu plus de temps, car nous allons toutes les télécharger une première fois, forcément) :

4. Configuration de l'interface

4.1- Une fois la mise à jour terminé, nous approchons de la fin ! Rendons-nous donc sur **Snort interfaces** pour choisir l'interface (ou les interfaces) sur laquelle Snort va écouter et analyser le trafic :

The screenshot shows the pfSense interface under the Services / Snort / Interfaces section. The 'Snort Interfaces' tab is selected. A table titled 'Interface Settings Overview' lists one interface: 'DMZ (em2)' with status 'AC-BNFA', pattern match 'LEGACY MODE', and description 'DMZ'. There are 'Add' and 'Delete' buttons at the bottom.

4.2- Ici nous choisissons donc l'interface de notre choix (DMZ ici), puis une courte description, et ensuite nous cochons simplement le fait d'envoyer les alertes sur le système de log interne, ce qui est toujours bien.

The screenshot shows the pfSense interface under the Services / Snort / DMZ - Interface Settings section. The 'Snort Interfaces' tab is selected. A table lists several categories: DMZ Settings, DMZ Categories, DMZ Rules, DMZ Variables, DMZ Preprocs, and DMZ IP Rep. Below these, the 'General Settings' section is shown with fields for 'Enable' (checked), 'Interface' (set to 'DMZ (em2)'), 'Description' (set to 'DMZ'), and 'Snap Length' (set to '1518').

4.3- A noter qu'ici, nous pouvons justement faire **de Snort un IPS**, en cochant la case **Block Offenders** :

Procédure SNORT

Alert Settings

Send Alerts to System Log	<input checked="" type="checkbox"/> Snort will send Alerts to the firewall's system log. Default is Not Checked.
System Log Facility	LOG_AUTH Select system log Facility to use for reporting. Default is LOG_AUTH.
System Log Priority	LOG_ALERT Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.
Enable Packet Captures	<input type="checkbox"/> Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file
Enable Unified2 Logging	<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

Block Offenders	<input checked="" type="checkbox"/> Checking this option will automatically block hosts that generate a Snort alert. Default is Not Checked.
IPS Mode	Legacy Mode 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. 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: bnx, cc, cxgbe, cxl, em, em, ena, ice, igb, igo, ix, ixgbe, ixl, lem, re, vmx, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.
Kill States	<input checked="" type="checkbox"/> Checking this option will kill firewall established states for the blocked IP. Default is checked.
Which IP to Block	BOTH Select which IP extracted from the packet you wish to block. Default is BOTH.

Detection Performance Settings

Search Method	AC-BNFA Choose a fast pattern matcher algorithm. Default is AC-BNFA.
Split ANY-ANY	<input type="checkbox"/> Enable splitting of ANY-ANY port group. Default is Not Checked.
Search Optimize	<input type="checkbox"/> Enable search optimization. Default is Not Checked.
Stream Inserts	<input type="checkbox"/> Do not evaluate stream inserted packets against the detection engine. Default is Not Checked.
Checksum Check Disable	<input type="checkbox"/> Disable checksum checking within Snort to improve performance. Default is Not Checked.

Procédure SNORT

Choose the Networks Snort Should Inspect and Whitelist

Home Net	<input type="text" value="default"/> <input type="button" value="View List"/>
Choose the Home Net you want this interface to use. Default Home Net adds only local networks, WAN IPs, Gateways, VPNs and VIPs. Create an Alias to hold a list of friendly IPs that the firewall cannot see or to customize the default Home Net.	
External Net	<input type="text" value="default"/> <input type="button" value="View List"/>
Choose the External Net you want this interface to use. External Net is networks that are not Home Net. Most users should leave this setting at default. Create a Pass List and add an Alias to it, and then assign the Pass List here for custom External Net settings.	
Pass List	<input type="text" value="default"/> <input type="button" value="View List"/>
Choose the Pass List you want this interface to use. The default Pass List adds local networks, WAN IPs, Gateways, VPNs and VIPs. Create an Alias to customize. This option will only be used when block offenders is on and IPS Mode is set to Legacy Mode.	

Choose a Suppression or Filtering List (Optional)

Alert	<input type="text" value="default"/> <input type="button" value="View List"/>
Suppression and Filtering	Choose the suppression or filtering file you want this interface to use.

Custom Configuration Options

Advanced Configuration Pass-Through	<input type="text"/>
Enter any additional configuration parameters to add to the Snort configuration here, separated by a newline	
<input type="button" value="Save"/>	

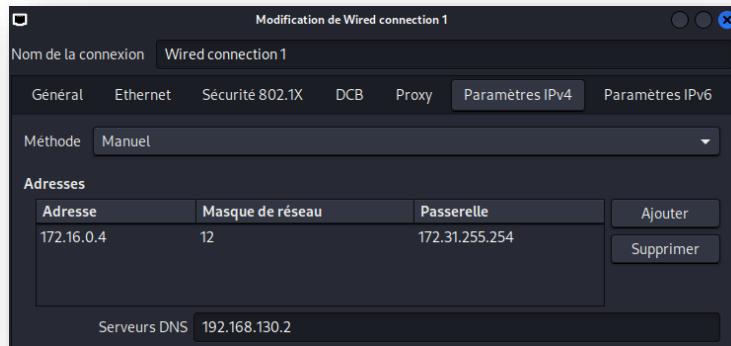
On valide et le tour est joué !

4.4- L'avant dernière étape est d'activer toutes les règles précédemment téléchargées en nous rendant dans **LAN Categories**, sur **Snort Interfaces**, **LAN** en cochant l'option **Use IPS Policy** :

4.5- On valide donc le tout, et on retourne à la liste des interfaces de Snort pour cliquer sur **Start** :

5. Vérification avec KALI

5.1- Installer KALI, configurer l'interface DMZ



5.2- Dans le terminal, faire un nmap de la passerelle de la DMZ.

```
(alex㉿kali)-[~]
$ nmap -sV 172.16.0.2
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-22 09:45 CET
Stats: 0:00:16 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 69.70% done; ETC: 09:45 (0:00:01 remaining)
Stats: 0:00:23 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 0.00% done
Nmap scan report for 172.16.0.2
Host is up (0.002s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     FileZilla ftpd
80/tcp    open  http   Microsoft IIS httpd 10.0
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.47 seconds
```

5.3- Dans l'interface du pare-feu, Services / Snort / Alerts. Les alertes s'affichent

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:
2024-01-22 11:25:46	⚠️	3	TCP	Unknown Traffic	172.16.0.7	48644	172.31.255.254	80	119
2024-01-22 11:24:23	⚠️	3	TCP	Unknown Traffic	172.16.0.4	41416	172.31.255.254	80	119
2024-01-22 11:20:15	⚠️	3	TCP	Unknown Traffic	172.16.0.4	51414	172.31.255.254	80	119