

---

---

**GSB**

**IDS**

**Version <2.0>**



**Mise en place d'un système de détection d'intrusions**

<b>GSB</b>	Version: <1.0>
IDS	Date: 08/03/2016

## Historique des révisions

<b>Date</b>	<b>Version</b>	<b>Description</b>	<b>Auteur</b>
08/03/2016	<1.0>	Installation du package «Snort» et mise en place des règles	Legrand Julien Harismendy Brice
10/03/2016	<1.5>	Configuration du Pare-Feu	Legrand Julien Harismendy Brice
11/03/2016	<2.0>	Création de la liste blanche puis des règles de détection	Legrand Julien Harismendy Brice

<b>GSB</b>	Version: <1.0>
<b>IDS</b>	Date: 08/03/2016

## Table des matières

### 1. Introduction

- 1.1 Contexte du projet
- 1.2 Objectifs du document
- 1.3 Portée
- 1.4 Références

### 2. Éléments de configuration

- 2.1 Installation de “Snort” et mise à jour des règles
- 2.2 Configuration du Pare-Feu pour le réseau local
- 2.3 Création d'une “liste blanche” de l'IDS
- 2.4 Mise en place des dernières règles
  - 2.4.1 Configuration et activation des règles 9
  - 2.4.2 Démarrage du service “Snort” 10

### 3. Tests / Validations

- 3.1 Test par lancement de scan
- 3.2 Vérification des alertes

### 4. Conclusion

GSB	Version: <1.0>
IDS	Date: 08/03/2016

# Mise en place d'un système de détection d'intrusions

## 1. Introduction

Nous allons maintenant mettre en place un IDS, c'est à dire un système de détection des intrusions sur notre Pfsense, avec un package du nom de «Snort». Celui-ci aura pour fonction d'analyser les communications entrantes ET sortantes du réseau pour se prémunir d'éventuelles attaques et aussi afin de créer une base de connaissance sur les attaques réussies pour ne pas qu'elles soient réitérées.

### 1.1 Contexte du projet

Nous reprenons ici le contexte du Pare-Feu / Proxy Pfsense, (cf. Compte-Rendu du sujet) et allons y ajouter un IDS pour prévenir plus efficacement des intrusions.

### 1.2 Objectifs du document

Le document à pour but de compléter celui du TP précédent sur les Pare-Feu / Proxy, et de démontrer la place que doit avoir une solution de supervision comme celle-ci.

### 1.3 Portée

Ce document est adressé ici aussi aux équipes techniques en charge de la sécurité d'un réseau et aux administrateurs qui souhaiteraient mettre en place la même solution.

### 1.4 Références

<http://www.snort.org> (Site officiel du package)

GSB	Version: <1.0>
IDS	Date: 08/03/2016

## 2. Éléments de configuration

### 2.1 Installation de "Snort" et mise à jour des règles

- Allez dans "**System**" > "**Packages**" > onglet "**Available Packages**" puis sélectionner "**Snort**" cliquez sur confirmer avant l'installation.

#### System: Package Manager: Install Package



Available packages

Installed packages

Package Installer

```

snort installation completed.

Beginning package installation for snort .
Downloading package configuration file... done.
Saving updated package information... done.
Downloading snort and its dependencies...
Checking for package installation...
  Downloading https://files.pfsense.org/packages/10/All/snort-2.9.7.6-amd64.pbi
... (extracting)
Loading package configuration... done.
Configuring package components...
Loading package configuration... done.
Additional files... done.
Loading package instructions...
Custom commands...
Executing custom_php_install_command()...done.
Executing custom_php_resync_config_command()...done.
Menu items... done.
Services... done.
Writing configuration... done.

Installation completed.
snort setup instructions:
Please visit Services - Snort - Interfaces tab first and select your desired
rules. Afterwards visit the Updates tab to download your configured rulesets.

```

- Allez dans "**Services**" > "**Snort**" > onglet "**Global Settings**" > cochez "**Install Snort VRT Rules**" et "**Install Snort Community Rules**" (pour les installations, il vous faut créer un compte sur snort.org et dans le profil du compte allez dans le menu "**Oinkcode**" afin d'obtenir le code de téléchargement).

GSB	Version: <1.0>
IDS	Date: 08/03/2016

## Snort: Global Settings



Snort Interfaces
Global Settings
Updates
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync

Please Choose The Type Of Rules You Wish To Download

Install **Snort VRT** rules
☒

Snort VRT free Registered User or paid Subscriber rules  
[Sign Up for a free Registered User Rule Account](#)  
[Sign Up for paid Sourcefire VRT Certified Subscriber Rules](#)

**Snort VRT Oinkmaster Configuration**  
Code:   
Obtain a snort.org Oinkmaster code and paste it here.

Install **Snort Community** rules
☒

The Snort Community Ruleset is a GPLv2 VRT certified ruleset that is distributed free of charge without any VRT License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.  
  
**Note:** If you are a Snort VRT Paid Subscriber, the community ruleset is already built into your download of the Snort VRT rules, and there is no benefit in adding this rule set.

- Cliquez sur "**Save**" en bas de page.
- Allez enfin dans l'onglet "**Update**" et cliquez sur "**Update**"

## Snort: Updates



Snort Interfaces
Global Settings
**Updates**
Alerts
Blocked
Pass Lists
Suppress
IP Lists
SID Mgmt
Log Mgmt
Sync

INSTALLED RULE SET MD5 SIGNATURE

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

UPDATE YOUR RULE SET

Last Update: Unknown  
Result: Unknown

MANAGE RULE SET LOG

GSB	Version: <1.0>
IDS	Date: 08/03/2016

## 2.2 Configuration du Pare-Feu pour le réseau local

- Ajoutez une règle sur l'interface WAN du Pare-Feu en allant dans "**FireWall**" > "**Rules**" > et dans l'onglet "**WAN**", créez une règle permettant les requêtes ICMP dans le réseau local.

Edit Firewall rule

Action	<div>Pass</div> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.</p>
Disabled	<input type="checkbox"/> <b>Disable this rule</b> Set this option to disable this rule without removing it from the list.
Interface	<div>WAN</div> <p>Choose which interface packets must be sourced on to match this rule.</p>
TCP/IP Version	<div>IPv4</div> <p>Select the Internet Protocol version this rule applies to</p>
Protocol	<div>ICMP</div> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>
ICMP type	<div>any</div> <p>If you selected ICMP for the protocol above, you may specify an ICMP type here.</p>
Source	<input type="checkbox"/> <b>not</b> Use this option to invert the sense of the match. Type: <div>any</div> Address: <div></div> / <div>127</div>
Destination	<input type="checkbox"/> <b>not</b> Use this option to invert the sense of the match. Type: <div>any</div> Address: <div></div> / <div>127</div>
Log	<input type="checkbox"/> <b>Log packets that are handled by this rule</b> Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the <a href="#">Diagnostics: System logs: Settings</a> page).
Description	<div></div> <p>You may enter a description here for your reference.</p>

Save

Cancel

- Cliquez ensuite sur "**Save**" et "**Apply Changes**" (dans l'onglet "**WAN**").  
- Allez enfin dans "**FireWall**" > "**Aliases**" > onglet "**IP**" > puis créez l'alias du nom du réseau (contenant ici notre VM) :

GSB	Version: <1.0>
IDS	Date: 08/03/2016

## Firewall: Aliases: Edit



**Alias Edit**

**Name**


The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and \_".

**Description**


You may enter a description here for your reference (not parsed).

**Type**

**Network(s)**

Networks are specified in CIDR format. Select the CIDR mask that pertains to each entry. /32 specifies a single IPv4 host, /128 specifies a single IPv6 host, /24 specifies 255.255.255.0, /64 specifies a normal IPv6 network, etc. Hostnames (FQDNs) may also be specified, using a /32 mask for IPv4 or /128 for IPv6. You may also enter an IP range such as 192.168.1.1-192.168.1.254 and a list of CIDR networks will be derived to fill the range.

Network or FQDN	CIDR	Description
172.16.0.0	16	The_Awesome_Network

## 2.3 Création d'une "liste blanche" de l'IDS

- Allez dans "Services" > "Snort" > "Pass Lists" > créez une passlist et entrez l'alias crée précédemment.

### Snort: Pass List Edit - passlist\_57429



**Snort Interfaces**
**Global Settings**
**Updates**
**Alerts**
**Blocked**
**Pass Lists**
**Suppress**
**IP Lists**
**SID Mgmt**
**Log Mgmt**
**Sync**

**Add the name and description of the file.**

**Name**


The list name may only consist of the characters "a-z, A-Z, 0-9 and \_". **Note:** No Spaces or dashes.

**Description**


You may enter a description here for your reference (not parsed).

**Add auto-generated IP Addresses.**

Local Networks ☒ Add firewall Local Networks to the list (excluding WAN).

WAN Gateways ☒ Add WAN Gateways to the list.

WAN DNS servers ☒ Add WAN DNS servers to the list.

Virtual IP Addresses ☒ Add Virtual IP Addresses to the list.

VPNs ☒ Add VPN Addresses to the list.

**Add custom IP Addresses from configured Aliases.**

Assigned Aliases:



GSB	Version: <1.0>
IDS	Date: 08/03/2016

- Créez ensuite une interface à surveiller dans **"Snort Interfaces"** affectée au WAN. Puis mettre le nom de la "passlist" en bas dans **"Home Net"**.

## Snort: Interface - Edit Settings



Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Iface Settings Iface Categories Iface Rules Iface Variables Iface Preprocs Iface Barnyard2 Iface IP Rep Iface Logs

**General Settings**

**Enable** ☒ Enable or Disable

**Interface** WAN Choose which interface this Snort instance applies to.  
Hint: In most cases, you'll want to use WAN here.

**Description** WAN  
Enter a meaningful description here for your reference.

**Alert Settings**

**Choose the networks Snort should inspect and whitelist**

**Home Net**    
Choose the Home Net you want this interface to use.  
Note: Default Home Net adds only local networks, WAN IPs, Gateways, VPNs and VIPs.  
Hint: Create an Alias to hold a list of friendly IPs that the firewall cannot see or to customize the default Home Net.

**External Net**    
Choose the External Net you want this interface to use.  
Note: Default External Net is networks that are not Home Net. Most users should leave this setting at default.  
Hint: Create a Pass List and add an Alias to it, and then assign the Pass List here for custom External Net settings.

**Pass List**    
Choose the Pass List you want this interface to use.  
Note: This option will only be used when block offenders is on.  
Hint: The default Pass List adds local networks, WAN IPs, Gateways, VPNs and VIPs. Create an Alias to customize.

## 2.4 Mise en place des dernières règles

### 2.4.1 Configuration et activation des règles

- Allez dans **"WAN Categories"** et choisir **"snort\_scan.rules"**

- Allez dans **"WAN Preprocs"** et cocher **"Enable"** dans **"Portscan Detecion"**. Enfin, mettre **"high"** dans **"Sensitivity"**.

<input type="checkbox"/>	snort_rservices.rules
<input type="checkbox"/>	snort_scada.rules
<input checked="" type="checkbox"/>	snort_scan.rules
<input type="checkbox"/>	snort_server-apache.rules
<input type="checkbox"/>	snort_server-iis.rules

GSB	Version: <1.0>
IDS	Date: 08/03/2016

**Portscan Detection**

Enable ☒ Use Portscan Detection to detect various types of port scans and sweeps. Default is **Not Checked**.

Protocol  Choose the Portscan protocol type to alert for (all, tcp, udp, icmp or ip). Default is **all**.

Scan Type  Choose the Portscan scan type to alert for. Default is **all**.  
 PORTSCAN: one->one scan: one host scans multiple ports on another host.  
 PORTSWEEP: one->many scan: one host scans a single port on multiple hosts.  
 DECOY\_PORTSCAN: one->one scan: attacker has spoofed source address inter-mixed with real scanning address.  
 DISTRIBUTED\_PORTSCAN: many->one scan: multiple hosts query one host for open services.  
 ALL: alerts for all of the above scan types.

Sensitivity  Choose the Portscan sensitivity level (Low, Medium, High). Default is **Medium**.  
 LOW: alerts generated on error packets from the target host; this setting should see few false positives.  
 MEDIUM: tracks connection counts, so will generate filtered alerts; may false positive on active hosts.  
 HIGH: tracks hosts using a time window; will catch some slow scans, but is very sensitive to active hosts.

Memory Cap  Maximum memory in bytes to allocate for portscan detection. Default is **10000000** (10 MB).  
 The maximum number of bytes to allocate for portscan detection. The higher this number, the more nodes that can be tracked. Default is **10,000,000** bytes. (10 MB)

Ignore Scanners  Leave blank for default. Default value is **\$HOME\_NET**. Aliases  
 Ignores the specified entity as a source of scan alerts. Entity must be a defined alias.

## 2.4.2 Démarrage du service "Snort"

- Allez dans "Status" > "Services" puis démarrer le service.

snort	Snort IDS/IPS Daemon	<span>✖ Stopped</span>	
-------	----------------------	------------------------	---

GSB	Version: <1.0>
IDS	Date: 08/03/2016


### 3. Tests / Validations

#### 3.1 Test par lancement de scan

- On lance un test avec un scan sur "Zenmap" et on peut voir que l'IDS détecte le portscan.

#### 3.2 Vérification des alertes

-Allez dans l'onglet "Alerts" de Snort ( "Services" > "Snort" ), on peut constater qu'il a bien détecté le portscan de "zenmap".


**Snort: Snort Alerts** 

Snort Interfaces Global Settings Updates **Alerts** Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

**Alert Log View Settings**

Instance to inspect (WAN) WAN Choose which instance alerts you want to inspect.









Save or Remove Logs **Download** All log files will be saved. **Clear** **Warning:** all log files will be deleted.

Auto Refresh and Log View **Save** Refresh ☐ Default is ON.  250 Enter number of log entries to view. Default is 250.

**Alert Log View Filter**

Alert Log Filter Options **Show Filter** Click to display advanced filtering options dialog

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

Date	Pri	Proto	Class	Source	SPort	Destination	DPort	SID	Description
03/08/16 10:41:39	3	TCP	Not Suspicious Traffic	192.168.2.51 	18336	213.41.212.217 	80	119:2  	(http_inspect) DOUBLE DECODING ATTACK
03/08/16 10:41:32	2		Attempted Information Leak	192.168.2.151 		192.168.2.51 		122:5  	(portscan) TCP Filtered Portscan

### 4. Conclusion

Nous avons mis en place un IDS qui permettra de vérifier la conformité des paquets et ainsi avoir un réseau plus sécurisé et une meilleure supervision. Un IDS permet de bloquer certaines attaques (portscan, arp, etc) couplé avec "squidguard" et un Pare-feu correctement configuré, on obtient un réseau très sécurisé, il faut maintenant se poser la question de l'emplacement du Pare-Feu sur ce dit réseau.