

Procédure Snort

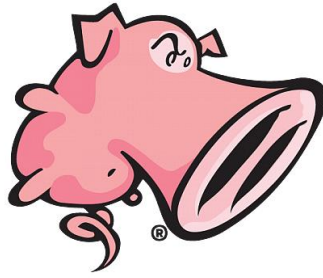


Sommaire

Table des matières

Sommaire	1
Contexte	2
Solution proposée	3
Présentation de Snort	3
Architecture du réseau	3
Mise en place	4
Configuration du PFSense.	4
Installation de Snort	5
Installation des règles	7
Paramétrage de l'interface WAN sur Snort	7
Test des alertes Snort	9

Procédure Snort



Contexte

Dans le cadre d'un projet réalisé durant notre formation, on nous demande de mettre en place un système de détection d'intrusion. Cette solution nous permet de repérer des activités anormales ou suspectes sur notre réseau. Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions.

Procédure Snort



Solution proposée

La solution consiste à utiliser une machine basée sur Pfsense, sur laquelle nous installerons les paquets nécessaires tel que Snort. Ensuite, nous paramètrons les interfaces dans le but d'analyser tout le trafic entrant sur notre réseau.

Présentation de Snort

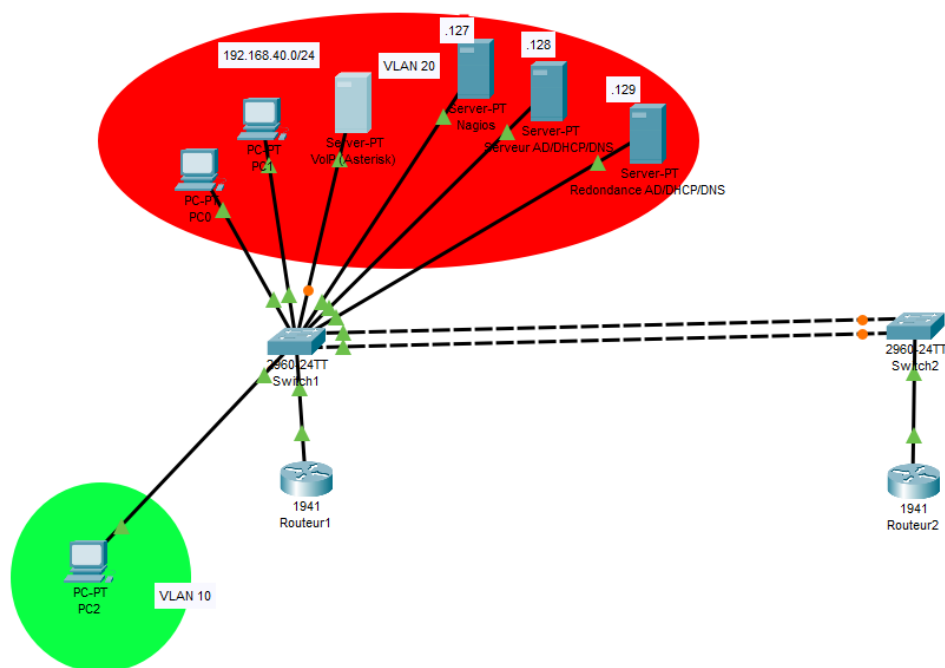
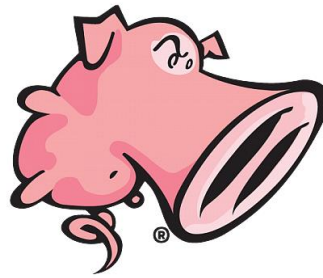
Snort est un [système de détection d'intrusion](#) (IDS) et de [prévention d'intrusion](#) (IPS) gratuit et open-source¹ créé en 1998 par [Martin Roesch](#).

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^{2,3}.

Le système de détection et de prévention des intrusions (IDS/IPS) Snort a la capacité d'effectuer une analyse du trafic en temps réel et un enregistrement des paquets sur les réseaux [IP](#). Snort effectue l'analyse des protocoles, la recherche et la mise en correspondance des contenus.

Architecture du réseau

Procédure Snort



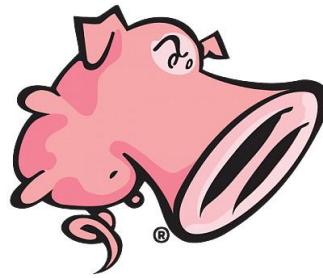
Mise en place

Configuration du PFSense.

System Information	
Name	pfSense.m2i3.lan
User	admin@172.25.31.128 (Local Database)
System	VMware Virtual Machine Netgate Device ID: e49c43d0fa7214de17b4

Configuration des interfaces WAN & LAN

Procédure Snort



Interfaces			
WAN	↑	1000baseT <full-duplex>	192.168.0.21 2a01:e0a:59:d780:20c:29ff:fe83:50b2
LAN	↑	1000baseT <full-duplex>	172.25.31.5

Enter an option: 7

Enter a host name or IP address: 1.1.1.1

PING 1.1.1.1 (1.1.1.1): 56 data bytes

64 bytes from 1.1.1.1: icmp_seq=0 ttl=57 time=22.292 ms

64 bytes from 1.1.1.1: icmp_seq=1 ttl=57 time=24.564 ms

64 bytes from 1.1.1.1: icmp_seq=2 ttl=57 time=22.312 ms

--- 1.1.1.1 ping statistics ---

3 packets transmitted, 3 packets received, 0.0% packet loss

round-trip min/avg/max/stddev = 22.292/23.056/24.564/1.067 ms




Press ENTER to continue.

Installation de Snort

System / Package Manager / Installed Packages

Installed Packages Available Packages

Installed Packages

Name	Category	Version	Description	Actions
✓ snort	security	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. Package Dependencies: snort-2.9.20	  

Procédure Snort



piSense COMMUNITY EDITION System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

WARNING: The 'admin' account password is set to the default value. [Change the password in the User Manager.](#)

Services / Snort / Interfaces ?

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

Interface Settings Overview

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

[+ Add](#)

[i](#)

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

Snort Subscriber Rules

Enable Snort VRT ☒ Click to enable download of Snort free Registered User or paid Subscriber rules

[Sign Up for a free Registered User Rules Account](#)
[Sign Up for paid Snort Subscriber Rule Set \(by Talos\)](#)

Snort Oinkmaster Code
Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)

Installation des règles

← → ↻ ⚠ Non sécurisé | https://192.168.2.1/snort/snort_download_updates.php 🔍 ⭐ ⚙ 👤

Installed Rule Set MD5 Signature

Rule Set Name/Publisher	MD5 Signature Hash	MD5 Signature Date
Snort Subscriber Ruleset	02be549f66ab977d7a20acf2aec2c17b	Wednesday, 26-Apr-23 15:17:16 CEST
Snort GPLv2 Community Rules	eefd9e77802bf0bf8772eb191de39f5c	Wednesday, 26-Apr-23 15:17:17 CEST
Emerging Threats Open Rules	152503f04f3d52bcb29fd20d2e5b0a38	Wednesday, 26-Apr-23 15:17:20 CEST
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 Apr-26 2023 15:17 **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.

Procédure Snort



Paramétrage de l'interface WAN sur Snort

WAN Settings

General Settings

Enable	<input checked="" type="checkbox"/> Enable interface
Interface	<div>WAN (em0) ▼</div> <p>Choose the interface where this Snort instance will inspect traffic.</p>
Description	<div>WAN</div> <p>Enter a meaningful description here for your reference.</p>
Snap Length	<div>1518</div> <p>Enter the desired interface snaplen value in bytes. Default is 1518 and is suitable for most applications.</p>

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	<div>LOG_AUTH ▼</div> <p>Select system log Facility to use for reporting. Default is LOG_AUTH.</p>
System Log Priority	<div>LOG_ALERT ▼</div> <p>Select system log Priority (Level) to use for reporting. Default is LOG_ALERT.</p>
Enable Packet Captures	<input type="checkbox"/> Checking this option will automatically capture packets that generate a Snort alert into a tcpdump compatible file

Procédure Snort



Automatic Flowbit Resolution

Resolve Flowbits ☒ 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.

Auto-Flowbit Rules



Disabling auto-flowbit rules is strongly discouraged for security reasons. Auto-enabled flowbit rules that generate unwanted alerts should have their GID:SID added to the Suppression List for the interface instead of being disabled.

Snort Subscriber IPS Policy Selection

Use IPS Policy ☒ 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.

IPS Policy Selection

Balanced

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!

Select the rulesets (Categories) Snort will load at startup

- Category is auto-enabled by SID Mgmt conf files

☒ Snort GPLv2 Com

Enable Ruleset: ET Open Rules

☒ emerging-activex.rules

☒ emerging-attack_response.rules

☒ emerging-botcc.portgrouped.rules

☒ emerging-botcc.rules

☒ emerging-chat.rules

☒ emerging-ciarmy.rules

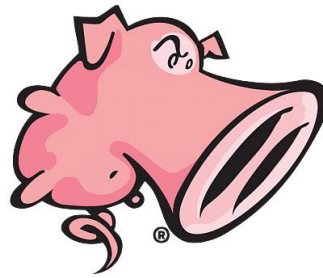
☒ emerging-compromised.rules

☒ emerging-current_events.rules

☒ emerging-deleted.rules





☒ emerging-dns.rules

Procédure Snort



Test des alertes Snort

Les alertes sélectionnées remontent bien grâce à notre IDS.

Interfaces			
 WAN		1000baseT <full-duplex>	192.168.0.21 2a01:e0a:59:d780:20c:29ff:fe83:50b2
 LAN		1000baseT <full-duplex>	172.25.31.5

Snort Alerts		
Interface/Time	Src/Dst Address	Description
WAN Apr 27 19:12:34	192.168.0.21:52250 8.8.8.8:53	ET DNS Query for .cc TLD
WAN Apr 27 19:12:34	192.168.0.21:58033 8.8.8.8:53	ET DNS Query for .cc TLD
WAN Apr 26 22:55:39	192.168.0.21:30230 13.107.4.52:80	ET INFO Microsoft Connection Test