Procédure
Snort

Sommaire

Table des matières

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 réussie 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 paramétrerons les interfaces dans le but d'analyser tout le trafic entrant sur notre réseau.

Présentation de Snort

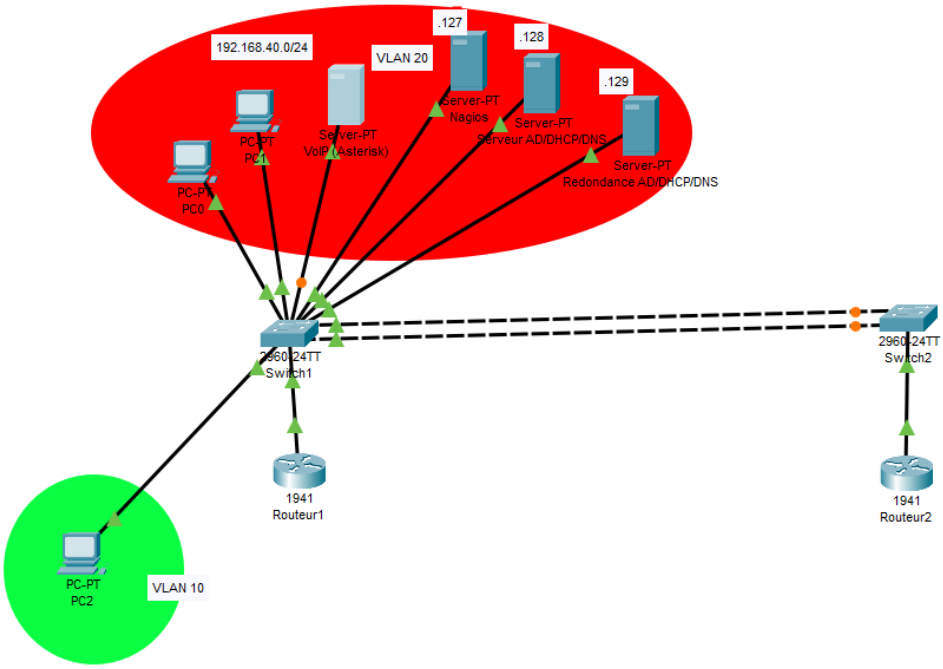
Snort est un système de détection d'intrusion (IDS) et de prévention d'intrusion (IPS) gratuit et open-source[1] créé en 1998 par Martin Roesch.

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.

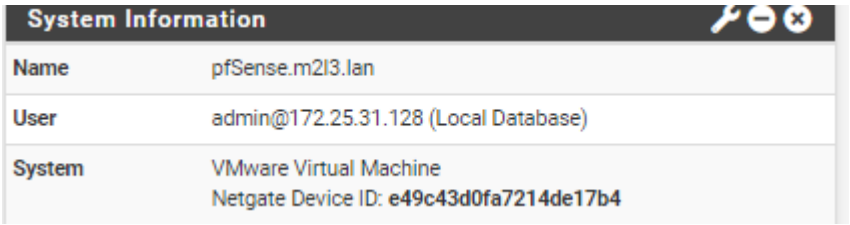
Architecture du réseau

Procédure Snort



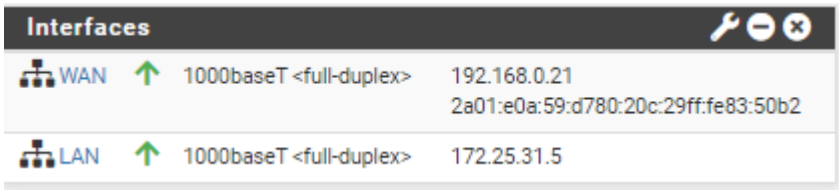
Mise en place

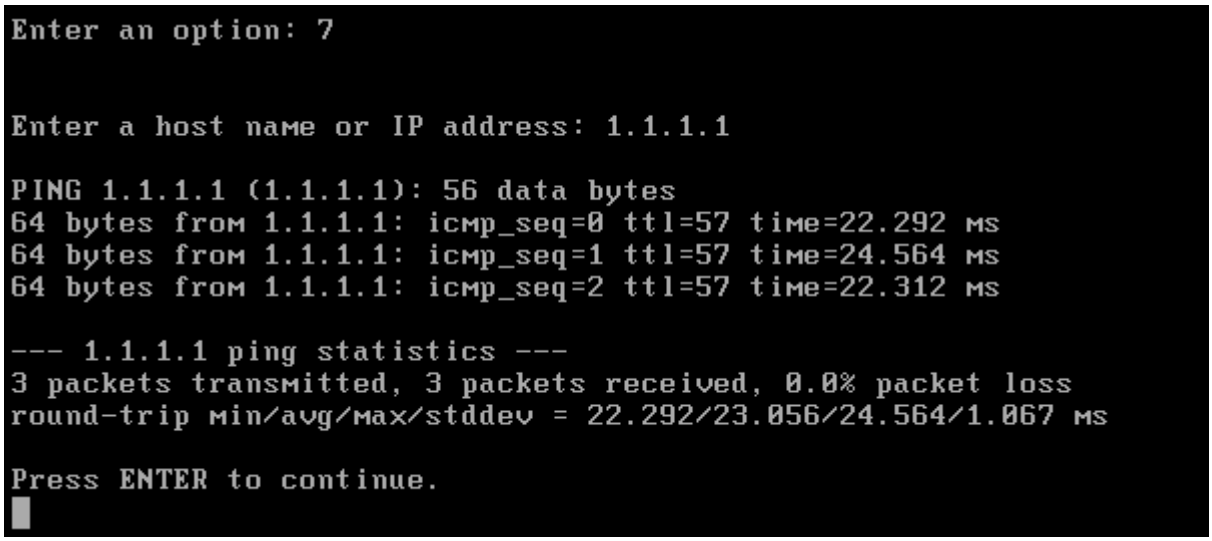
Configuration du PFSense.



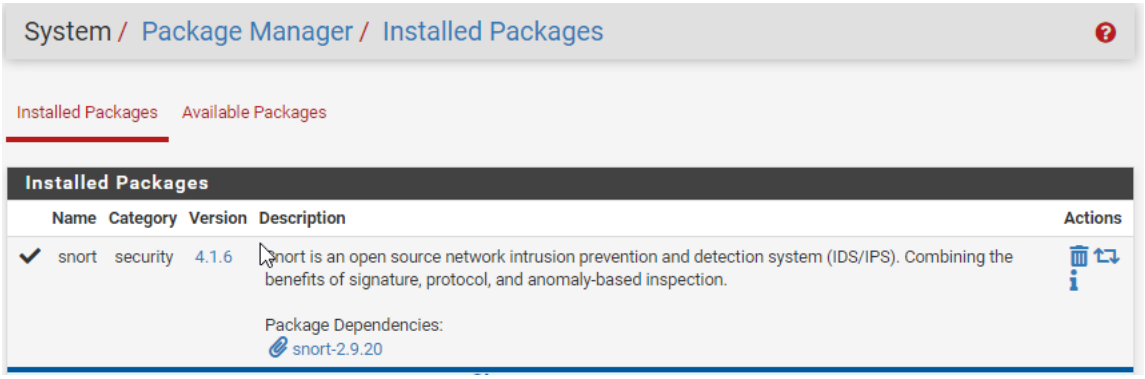
Configuration des interfaces WAN & LAN

Procédure Snort

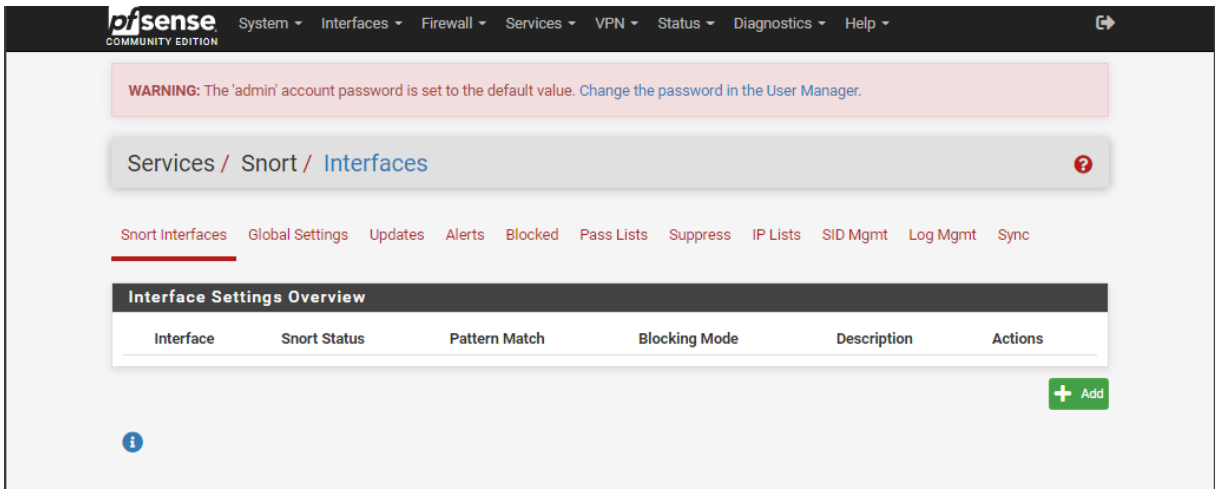


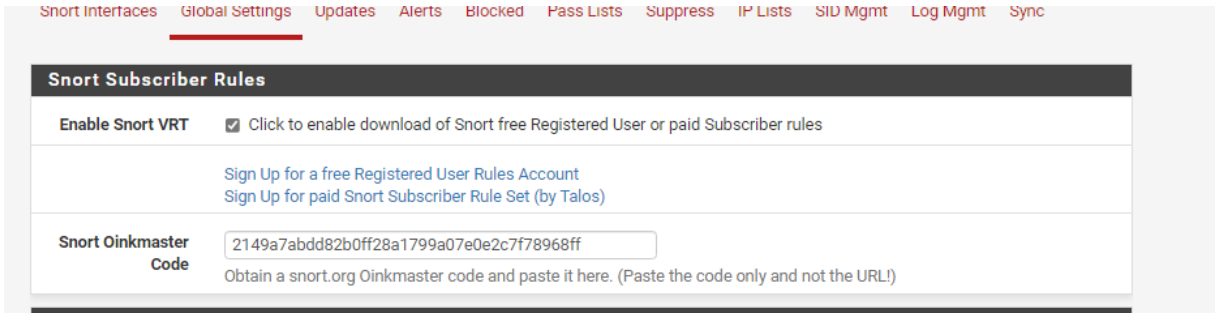


Installation de Snort

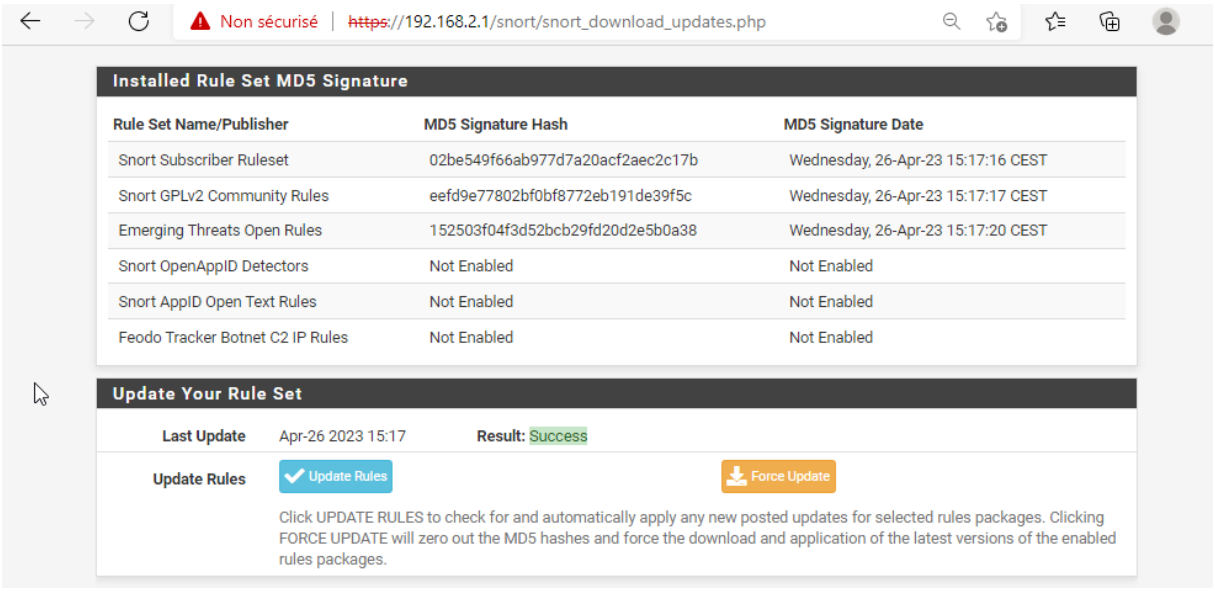


Procédure Snort



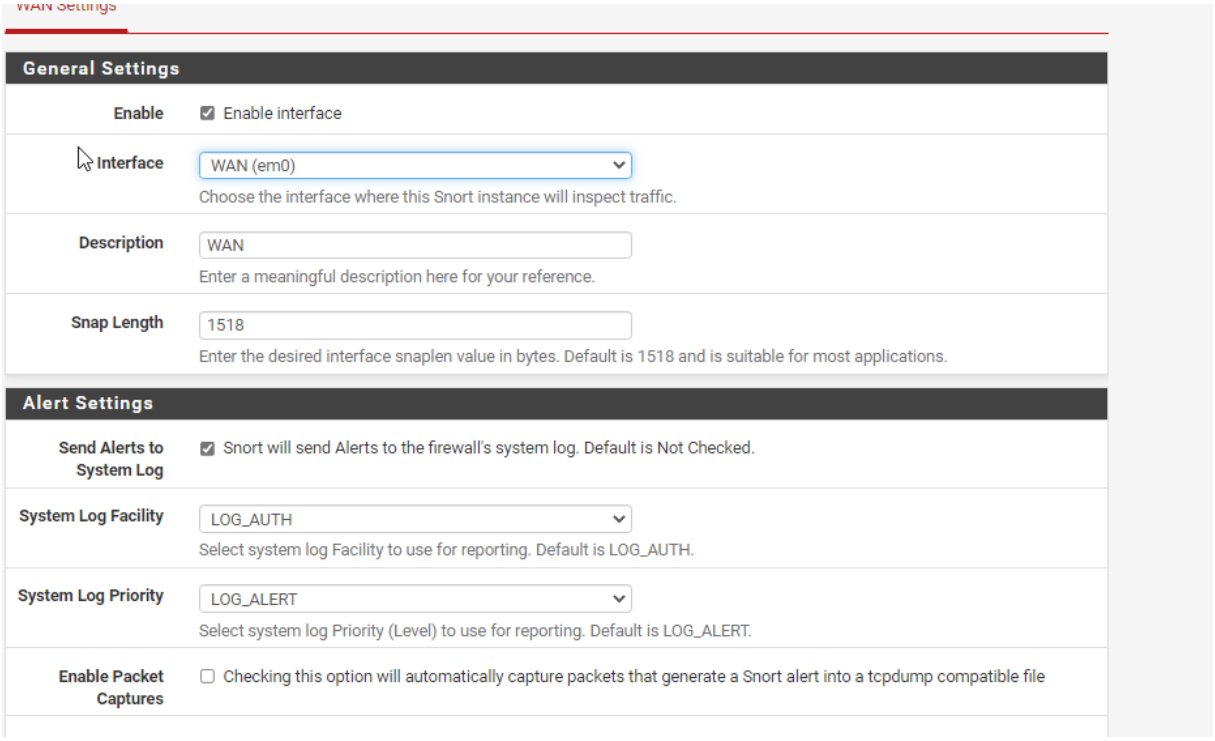


Installation des règles



Procédure Snort

Paramétrage de l'interface WAN sur Snort



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 — View

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

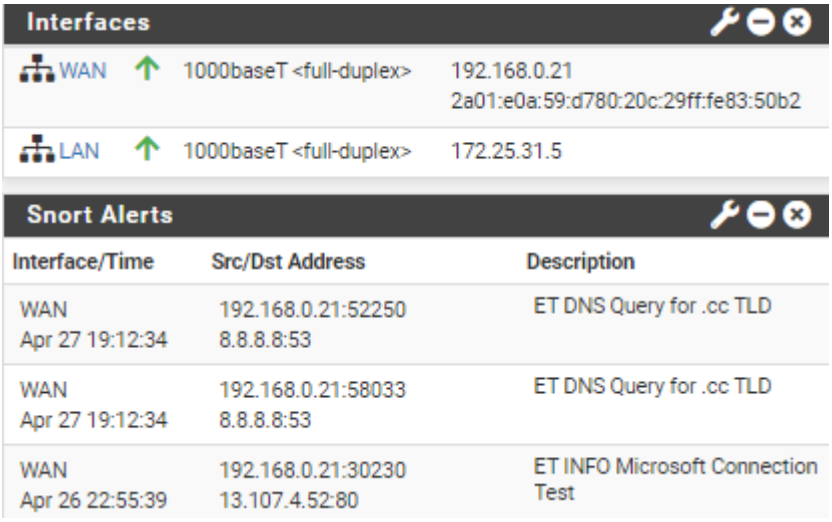
Snort GPLv2 Com

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