

Nom : Kresser

Prénom : Alexis

N° Candidat : 02045540456

BTS Service Informatique aux organisation

Solution d'infrastructure système et réseaux

***Réalisation Professionnel n*1 :
Mise en place d'un système de détection d'intrusion de
SNORT***



Tables des matières

1. Description Réalisation Professionnel	3
2. Présentation GSB(Galaxy Swiss bourdin) et de son contexte	4
2.1 L'entreprise:	4
2.2 Réorganisation :	4
2.3 Besoin :	4
3. Matériel à disposition	6
3.1 Ressources documentaire :	6
3.2 Ressource matérielles:	6
3.3 Logiciel utilisées:	6
3.4 Table d'adressage IP :	6
3.5 Table des Vlans :	7
4. Présentation du projet	8
4.1 VirtualBox:	9
4.2 Pfsens:	10
4.3 Snort:	11
5. Mise en place	12
5.1 Le pare feu IDS, IPS avec Snort sur Pfsens	12
5. Test de Fonctionnement IDS	18
6. Test de fonctionnement IPS	20

1.Description Réalisation Professionnel

Propriétés	Description
Intitulé	Mise en place d'un système de détection d'intrusion avec architecture centralisée sur SNORT
Présentation rapide	Les systèmes de détection et intrusions (IDS) et de prévention des intrusions (IPS) sont des pare-feu qui sécurisent toutes les données entrant ou sortant d'un réseau.
Objectifs	<ul style="list-style-type: none"> - Automatiser les sécurité réseaux - Conformité des technologies et systèmes dédiés à la protection des données - Les IDS/IPS sont configurables, ce qui contribue à l'application des politiques de sécurité internes au niveau du réseau.
Compétences mobilisées	2.1 Concevoir une solution d'infrastructure réseau 2.2 Installer, tester et déployer une solution d'infrastructure réseau 2.3 Exploiter, dépanner et superviser une solution d'infrastructure réseau
Outils	L'application va s'appuyer sur l'infrastructure existante de GSB comportant : <ul style="list-style-type: none"> - Pfsens - réseau
Documents joints	Schéma réseau GSB (actuel et attendu), Procédure d'installation, Fiche technique des équipements ...
Modalités de réception	Présentation d'un système opérationnel - Documentation technique, Mode opératoire et compte rendu d'installation
Evolution possible	Mise en place d'un VLAN protéger à travers SNORT

2.Présentation GSB(Galaxy Swiss bourdin) et de son contexte

2.1 L'entreprise:

Le laboratoire Galaxy Swiss Bourdin est issu de la fusion entre le géant américain Galaxy et le conglomérat européen Swiss Bourdin, lui-même déjà union de trois petits laboratoires.

En 2009, les deux géants pharmaceutiques unissent leurs forces pour créer un leader de ce secteur industriel. L'entité GSB Europe a établi son siège administratif à Paris.

Le siège social de la multinationale est situé à Philadelphie, Pennsylvanie, aux Etats-Unis.

La France a été choisie comme témoin pour l'amélioration du suivi de l'activité de visite.

2.2 Réorganisation :

Une conséquence de cette fusion est la recherche d'une optimisation de l'activité du groupe en réalisant des économies d'échelle dans la production et la distribution des médicaments et d'augmenter la sécurité de cette fusion tout en prenant le meilleur des deux laboratoires sur les produits concurrents.

L'entreprise compte 480 visiteurs médicaux en France métropolitaine, et 60 dans les départements et territoires d'outre-mer.

2.3 Besoin :

Depuis la réorganisation de GSB l'entreprise fonctionne bien et a connu une hausse de son activité. Suite à cela Galaxy Swiss Bourdin a décidé de sécuriser son réseau en mettant en place un système de détection des intrusions et un système de prévention des intrusions en installant un pare-feu IDS/IPS. Pour réaliser cette mission, GSB nous a fourni un schéma de leur réseau actuel, grâce à celui-ci nous allons pouvoir étudier l'emplacement où l'IPS/IDS sera le plus efficace contre les attaques sans bloquer les autres connexions dans le réseau.

Schéma actuel :

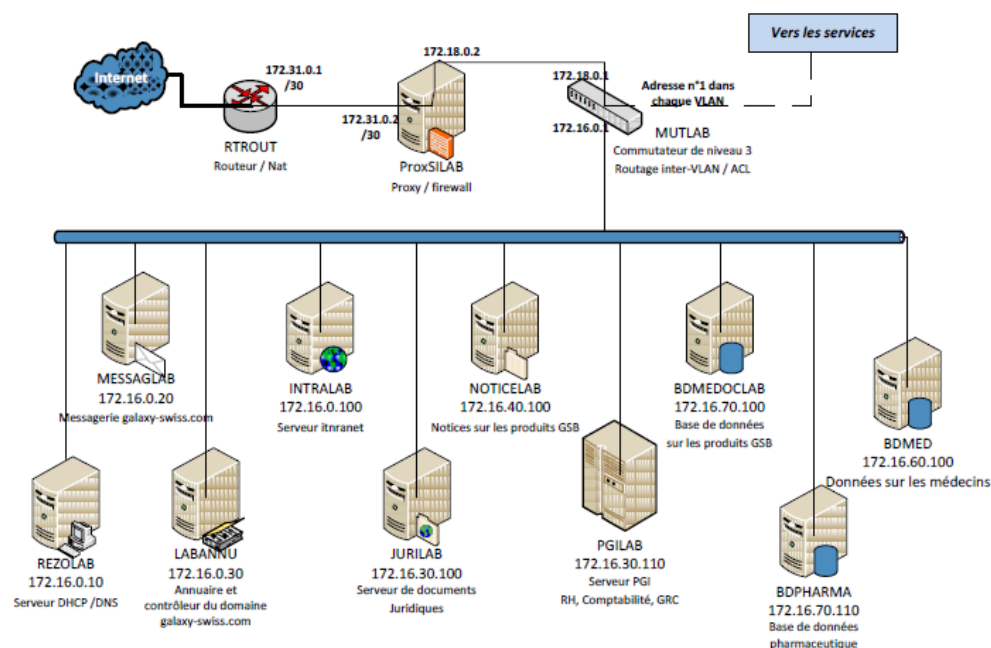
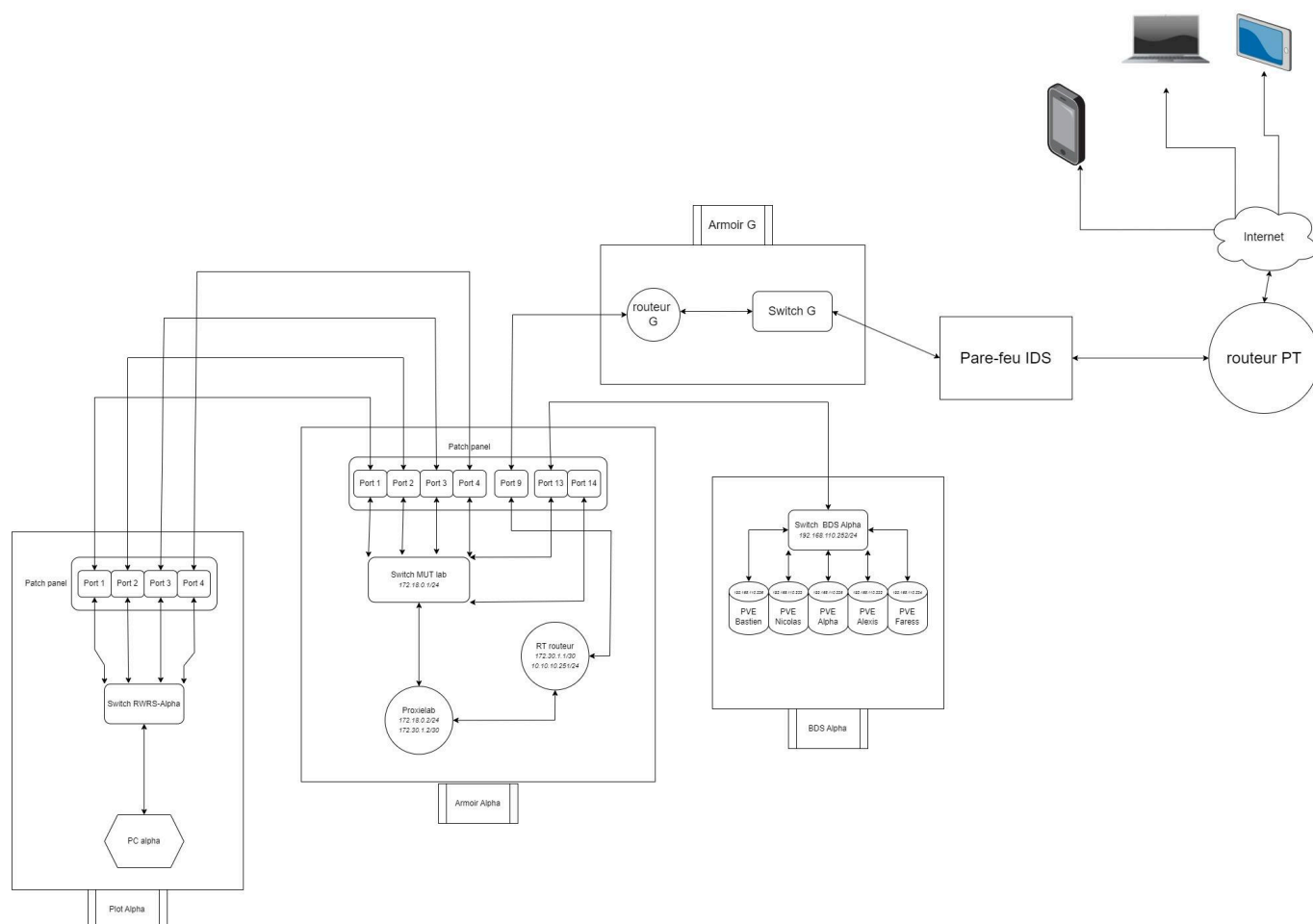


Schéma réseau attendu :



3. Matériel à disposition

3.1 Ressources documentaire :

- Contexte GSB
- Schéma réseau (contexte)

3.2 Ressource matérielles:

- un hyperviseur de type 1 : Proxmox hébergeant les machine virtuelle du contexte
- Un Hyperviseur de type 1 : Proxmox hébergeant les machine virtuelle de mes réalisation professionnel
- un routeur (RT-ROUT)
- Un par-feu ProxSilab (PFSENSE)
- Plusieurs switch de niveau 3 (Cisco-3750G)
- Un switch niveau 2 (Cisco 2960)
- Un Switch BDS
- plusieurs ordinateur pour effectuer les simulations et les tests

3.3 Logiciel utilisées:

- PFSense
- virtualBox

3.4 Table d'adressage IP :

Matériel	IP de connexion	ID de connexion	Mot de passe	Protocol
Switch RWRS 3750G	192.168.110.253	admin	Aristee.2022	SSH2
MUTLAB	192.168.110.1	admin	Aristee.2022	SSH2
RT-ROUT	172.30.0.1		Aristee.2024	Telnet
PFSENSE	192.168.110.100	admin	Aristee.2024	SSH2
Switch BDS	192.168.110.252	admin	Aristee.2022	SSH2
Proxmox Alpha	192.168.110.235	root	Aristee.2024	SSH2
Proxmox Alexis	192.168.110.232	root	Aristee.2024	SSH2
SRV-DC01	192.168.110.101	a.kresser	Aristee.2024	SSH2
JURILAB	172.16.30.100	root	Aristee.2024	SSH2

Matériel	IP de connexion	ID de connexion	Mot de passe	Protocol
MESSAGELAB	172.16.0.20	root	Aristee.2024	SSH2
NOTICELAB	172.16.40.100	root	Aristee.2024	SSH2
BDMED	172.16.60.100	root	Aristee.2024	SSH2
BDMEDCOLAB	176.16.70.100	root	Aristee.2024	SSH2
BDPHARMA	176.16.70.110	root	Aristee.2024	SSH2
REZOLAB	176.16.0.10	root	Aristee.2024	SSH2
PC Student	X	1133941414	Aristee.2024	Anydesk

3.5 Tableau des Vlan :

Numéro Vlan	Services(s)	Adressage IP
20	Direction / DSI	192.168.20.0/24
30	RH / Compta / Juridique / Secrétariat / Administratif	192.168.30.0/24
40	Communication / Rédaction	192.168.40.0/24
50	Développement	192.168.50.0/24
60	Commercial	192.168.60.0/24
70	Labo-Recherche	192.168.70.0/24
100	Accueil	192.168.100.0/24
110	Réseau et système	192.168.110.100/24
150	Visiteurs	192.168.150.0/24
200	Démonstration	192.168.200.0/24
300	Serveurs	172.16.0.0/17
400	Sortie	172.18.0.0/30

4.Présentation du projet

Dans le cadre de notre mission pour Galaxy Swiss Bourdin et de la sécurisation de leur équipement, nous allons mettre en place un système de détection des intrusions (IDS) et de prévention des intrusions (IPS).

Leur fonctionnement est simple, les IDS/IPS comparent les paquets de réseau à une base de données de cybermenaces contenant des signatures connues de cyberattaques et repèrent tous les paquets qui concordent avec ces signatures.

La principale différence entre les deux tient au fait que l'IDS est un système de surveillance, alors que l'IPS est un système de contrôle.

L'IDS ne modifie en aucune façon les paquets réseau, alors que l'IPS empêche la transmission du paquet en fonction de son contenu, tout comme un pare-feu bloque le trafic en se basant sur l'adresse IP.

Les IDS (Intrusion Detection Systems) : analysent et surveillent le trafic réseau pour détecter des signes indiquant que des hackers utilisent une cybermenace connue afin de s'infiltrer dans votre réseau ou y voler des données. Les systèmes d'IDS comparent l'activité réseau en cours avec une base de données d'attaques connues afin de détecter divers types de comportements tels que les violations de la politique de sécurité, les malwares et les scanners de port.

Les IPS (Intrusion Prevention Systems) agissent dans la même zone du réseau qu'un pare-feu, entre le monde extérieur et le réseau interne. Les IPS *rejetent* de façon proactive les paquets réseau en fonction d'un profil de sécurité si ces paquets représentent une menace connue.

Les équipes de sécurité sont confrontées à un risque croissant de fuite de données et d'amendes pour non-conformité. Parallèlement, elles continuent d'être confrontées à des problèmes de contraintes budgétaires et de politique d'entreprise. La technologie IDS/IPS recouvre des tâches spécifiques et importantes en matière de **stratégie de cybersécurité** :

Automatisation : les systèmes IDS/IPS sont dans une large mesure automatiques, ce qui

en fait des candidats parfaits à l'intégration à la pile de sécurité actuelle. Les IPS procurent la tranquillité d'esprit que le réseau est protégé contre les menaces connues, et ce avec des besoins limités en ressources.

Conformité : dans le cadre du respect de la conformité, il est souvent nécessaire de prouver que vous avez investi dans des technologies et systèmes dédiés à la protection de vos données. La mise en œuvre d'une solution d'IDS/IPS permet de satisfaire une condition de conformité et de réaliser un certain nombre de contrôles de sécurité du CIS. Surtout, les données d'audit constituent un élément essentiel des enquêtes en matière de conformité.

Application de la politique : les IDS/IPS sont configurables, ce qui contribue à l'application des politiques de sécurité internes au niveau du réseau. Par exemple, si vous n'utilisez qu'un VPN, vous pouvez utiliser l'IPS pour bloquer le trafic provenant d'un autre VPN

Afin de mettre IDS/IPS en place nous allons avoir besoin de certains outils déjà présents ou non dans notre réseau, les voici:

4.1 VirtualBox:

C'est un logiciel libre de virtualisation, une solution pour pouvoir exécuter d'autres systèmes d'exploitation sur une seule machine et faire un test d'un réseau réel dans un seul ordinateur.. Il marche sur les trois plateformes (Linux, Windows, macOS).

4.2 Pfsens:

C'est une distribution de pare-feu réseau gratuite, il intègre aussi un gestionnaire de paquets pour installer (logiciels) supplémentaires, désinstaller des paquets et d'autres fonctionnalités. Plusieurs services peuvent être gérés par pfSense, et ces services peuvent être arrêtés ou activés depuis une interface graphique. Voici une liste des services proposés par Pfsense :

- VPN client PPTP, VPN site à site OpenVPN et IPSec.
- Gestion des VLAN.
- Filtrage d'URL.
- Serveur DHCP.
- Partage de bande passante Traffic Shaper (régulation de flux est le contrôle du volume des échanges sur un réseau informatique dans le but d'optimiser ou de garantir les performances).

- Répartition de charge (Load Balancer).
- IDS-IPS Snort.

pour réaliser cette installation nous pouvons utiliser 2 services différents, voici un petit comparatif, Les 4 principales différence entre Snort et Suricata:

1. Architecture : Suricata utilise une architecture multi thread, ce qui lui permet de tirer parti du matériel moderne doté de plusieurs cœurs. Snort, en revanche, fonctionne principalement sur un seul thread.
2. Prise en charge du protocole : Suricata offre une prise en charge étendue des protocoles, notamment HTTP, SMTP, FTP, SSH, etc. Bien que complet, Snort n'a peut-être pas le même niveau de couverture protocolaire que Suricata.
3. Performances : l'architecture multithread et le traitement optimisé de Suricata offrent un débit et une évolutivité plus élevés, ce qui le rend adapté aux réseaux à haut débit. La nature monothread de Snort peut limiter ses performances sur de tels réseaux.
4. Langage de règles : Suricata utilise son langage de règles, Suricata Rule Language (SRL), conçu pour être expressif et puissant. Snort utilise son langage de règles appelé Snort Rules Language (SRL), mais prend également en charge un sous-ensemble compatible de règles Suricata.

Pour notre projet nous allons choisir de prendre Snort car il comporte tous les services dont nous avons besoin en restant assez léger à installer et configurer.

4.3 Snort:

C'est un hybride d'IPS et d'IDS efficace et le projet Open Source le plus avancé au monde. Il utilise une série de règles qui aident à définir l'activité réseau malveillante et utilise ces règles pour trouver les paquets qui leur correspondent et génère des alertes pour les utilisateurs. Snort peut être téléchargé et configuré pour une utilisation personnelle et professionnelle, c'est un outil multi-plateformes (Linux, Windows, FreeBSD). Snort a trois utilisations principales:

- Un détecteur de paquets (renifleur)
- Un enregistreur de paquets - ce qui est utile pour le débogage du trafic réseau.
- Un système de prévention des intrusions réseau à part entière.

5. Mise en place

5.1 Le pare feu IDS, IPS avec Snort sur Pfsens

Pour commencer nous allons installer Snort sur le pfsens, pour se faire nous allons sur l'adresse suivante avec notre Vlan: 192.168."Vlan".100

The screenshot displays the pfSense Community Edition dashboard. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. The main content area is divided into two panels: System Information and Interfaces.

System Information

Name	pfSense.gsb.lan
User	admin@192.168.110.63 (Local Database)
System	pfSense Serial: CZC9155XZC Netgate Device ID: 049421d44dacbfa8172d
BIOS	Vendor: Hewlett-Packard Version: 786G1 v01.16 Release Date: Thu Mar 5 2009
Version	2.4.5-RELEASE-p1 (amd64) built on Tue Jun 02 17:51:17 EDT 2020 FreeBSD 11.3-STABLE The system is on the latest version. Version information updated at Tue Nov 28 14:33:12 CET 2023
CPU Type	Intel(R) Core(TM)2 Duo CPU E8400 @ 3.00GHz 2 CPUs: 1 package(s) x 2 core(s) AES-NI CPU Crypto: No
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	00 Hour 19 Minutes 33 Seconds
Current date/time	Tue Nov 28 14:48:25 CET 2023

Interfaces

WAN	100baseTX <full-duplex>	172.31.0.2
LAN	autoselect	172.18.0.2
VLAN110	1000baseT <full-duplex>	192.168.110.100
VLAN20	1000baseT <full-duplex>	192.168.20.100
VLAN30	1000baseT <full-duplex>	192.168.30.100
VLAN40	1000baseT <full-duplex>	192.168.40.100
VLAN50	1000baseT <full-duplex>	192.168.50.100
VLAN60	1000baseT <full-duplex>	192.168.60.100
VLAN70	1000baseT <full-duplex>	192.168.70.100
VLAN80	1000baseT <full-duplex>	192.168.80.100
VLAN90	1000baseT <full-duplex>	192.168.90.100
VLAN100	1000baseT <full-duplex>	192.168.100.100
VLAN150	1000baseT <full-duplex>	192.168.150.100
VLAN200	1000baseT <full-duplex>	192.168.200.100
VLAN300	1000baseT <full-duplex>	172.16.0.100
VLAN400	1000baseT <full-duplex>	172.19.0.100
VLAN22	1000baseT <full-duplex>	192.168.22.100

Puis se rendre sur Système > Package manager > Available package, rechercher Snort et l'installer:

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

System / Package Manager / Available Packages

Installed Packages Available Packages

Search

Search term Both ▾

Enter a search string or *nix regular expression to search package names and descriptions.

Packages

Name	Version	Description
snort	4.1.2_3	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-2.9.16.1](#)

Une fois installé il doit apparaître dans “ installed package” comme ceci:

Installed Packages Available Packages

Installed Packages

Name	Category	Version	Description	Actions
✓ snort	security	4.1.2_3	Snort is an open source network intrusion prevention and detection system (IDS/IPS). Combining the benefits of signature, protocol, and anomaly-based inspection.	<input type="button" value="Update"/> <input checked="" type="button" value="Current"/> <input type="button" value="Remove"/> <input type="button" value="Information"/> <input type="button" value="Reinstall"/>

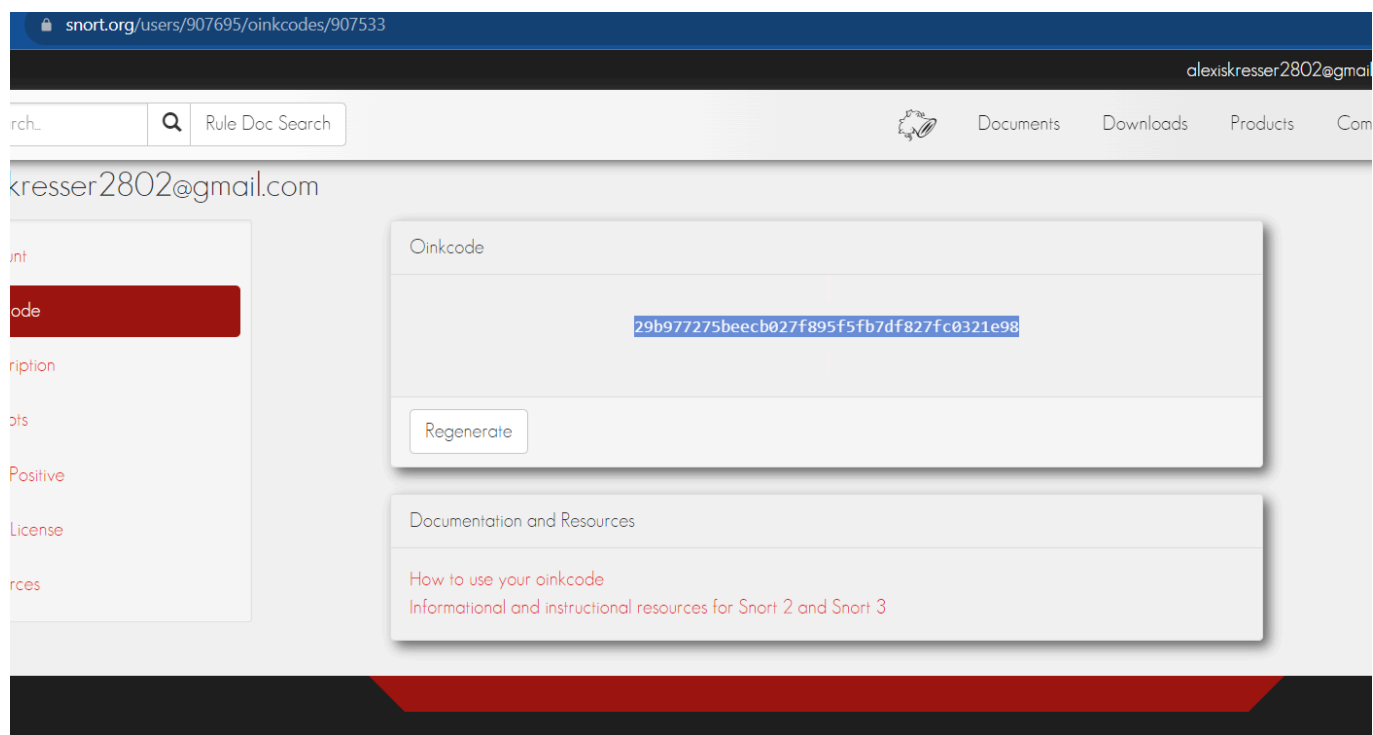
Package Dependencies:
[snort-2.9.16.1](#)

= Update = Current
 = Remove = Information = Reinstall
 Newer version available
 Package is configured but not (fully) installed or deprecated

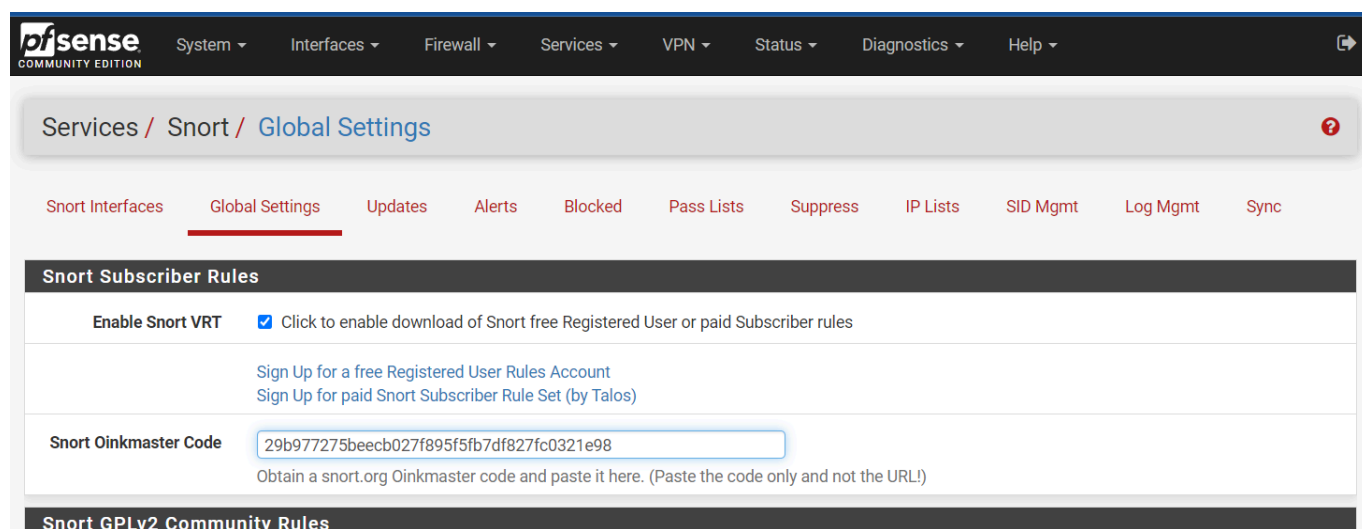
Maintenant nous pouvons nous rendre dans l'onglet service > Snort pour le configurer.

La première étape est 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.

Récupération du code:



Mettre le code dans “Snort Oinkmaster Code”



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 Open AppID**, éventuellement, qui est une autre société

Puis, 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:

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
Sign Up for an ETPro Account ETPro for Snort offers daily updates and extensive coverage of current malware threats.	
Sourcefire OpenAppID Detectors	
Enable OpenAppID	<input checked="" type="checkbox"/> Click to enable download of Sourcefire OpenAppID Detectors
The OpenAppID Detectors package contains the application signatures required by the AppID preprocessor and the OpenAppID text rules.	
OpenAppID Version	
Enable AppID Open Text Rules	<input type="checkbox"/> Click to enable download of the AppID Open Text Rules
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.pfsense.org/openappid/appid_rules.tar.gz .	
Rules Update Settings	
Update Interval	<div>12 HOURS</div> <div>Please select the interval for rule updates. Choosing NEVER disables auto-updates.</div>
Update Start Time	<div>1:00</div>

Dans notre cas l'intervalles des mise à jour sera de 12h minimum et l'heure de mise à jour sera 1h du matin pour ne pas gêner l'activité des collaborateurs

Ne pas oublier de sauvegarder le paramétrage

Une fois sauvegarder, nous pouvons nous rendre sur l'onglet Updates et manuellement mettre à jour les différentes règles que nous avons cochées précédemment en cliquant sur "update rules" (dans notre cas cela prendra un peu de temps, car nous allons toutes les télécharger une première fois).

[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 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 Downloaded	Not Downloaded
Snort AppID Open Text Rules	Not Enabled	Not Enabled

Update Your Rule Set

Last Update

Unknown

Result: Unknown

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.

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.

Close

Update Your Rule Set

Last Update

Nov-28 2023 15:30

Result: Success

Maintenant que Snort est bien installé et configuré nous pouvons nous rendre sur “Snort interfaces” pour choisir l’interface (ou les interfaces) sur laquelle Snort va écouter et analyser le trafic et appuyer sur “add” pour ajouter:

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
<div>+ Add</div>					

Ici nous choisissons donc l'interface que nous voulons surveiller, puis une description du réseau et ensuite nous cochons simplement le fait d'envoyer les alertes sur le système de log interne, pour les analyser en cas de tentative d'intrusion

Services / Snort / Edit Interface / LAN ?

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

LAN Settings

LAN Categories

LAN Rules

LAN Variables

LAN Preprocs

LAN IP Rep

LAN Logs

General Settings

Enable

☒ Enable interface

Interface

WAN (em0)

Choose the interface where this Snort instance will inspect traffic.

Description

interface WAN

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

Send Alerts to System Log

☒ 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

A partir de ces options nous avons mis en place notre IDS car ils nous envoient les informations du pare-feu dans des logs consultables.

5. Test de Fonctionnement IDS

Maintenant que nous l'avons activé, en allant dans l'interface Service > Snort > Alerte on peut observer les logs qui arrivent et qui nous prévient de toute connexion suspecte sur le réseau sans bloquer la connexion au réseau qu'il tente d'accéder.

The screenshot displays the pfSense web interface, specifically the 'Services / Snort / Alerts' section. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below this, a sub-navigation bar highlights 'Alerts' among other options like Snort Interfaces, Global Settings, Updates, Blocked, Pass Lists, Suppress, IP Lists, SID Mgmt, Log Mgmt, and Sync.

The 'Alert Log View Settings' section shows the 'Interface to Inspect' set to 'WAN (em0)', with an option for 'Auto-refresh view' and a limit of '250' alert lines to display. Below this, 'Alert Log Actions' include 'Download' and 'Clear' buttons.

The 'Alert Log View Filter' section is currently empty. Below it, the '98 Entries in Active Log' table is shown, displaying a list of alerts. The table has columns for Date, Action, Pri, Proto, Class, Source IP, SPort, Destination IP, DPort, GID:SID, and Description. The alerts are categorized as 'Not Suspicious Traffic' and 'Unknown Traffic', with descriptions indicating issues like 'BARE BYTE UNICODE ENCODING' and 'PROTOCOL-OTHER HTTP server response before client request'.


Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-01-30 13:14:14	⚠	3	TCP	Not Suspicious Traffic	172.31.0.2	12623	57.128.101.77	80	119:4	(http_inspect) BARE BYTE UNICODE ENCODING
2024-01-30 13:14:14	⚠	3	TCP	Unknown Traffic	57.128.101.77	80	172.31.0.2	12623	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request
2024-01-30 13:14:14	⚠	3	TCP	Unknown Traffic	57.128.101.77	80	172.31.0.2	12623	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request
2024-01-30 13:14:14	⚠	3	TCP	Unknown Traffic	57.128.101.77	80	172.31.0.2	12623	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request
2024-01-30 13:13:52	⚠	3	TCP	Not Suspicious Traffic	172.31.0.2	2096	51.178.65.231	80	119:4	(http_inspect) BARE BYTE UNICODE ENCODING
2024-01-30 13:13:52	⚠	3	TCP	Unknown Traffic	51.178.65.231	80	172.31.0.2	2096	120:18	(http_inspect) PROTOCOL-OTHER HTTP server response before client request

Maintenant nous allons faire de Snort un IPS, en cochant la case "Block Offenders"

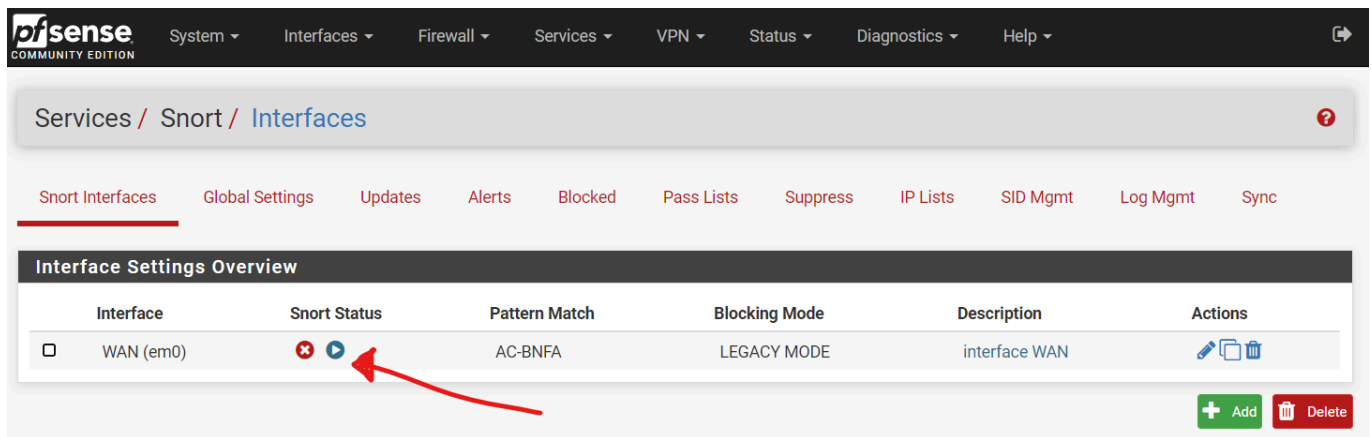
En faisant cela, Snort va donc bloquer les hôtes générant des alertes automatiquement

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	<div>Legacy Mode</div> <p>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.</p> <p>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: cc, cxl, cxgbe, em, igb, em, lem, ix, ixgbe, ixl, re, vtnet. If problems are experienced with Inline Mode, switch to Legacy Mode instead.</p>
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	<div>BOTH</div> <p>Select which IP extracted from the packet you wish to block. Default is BOTH.</p>

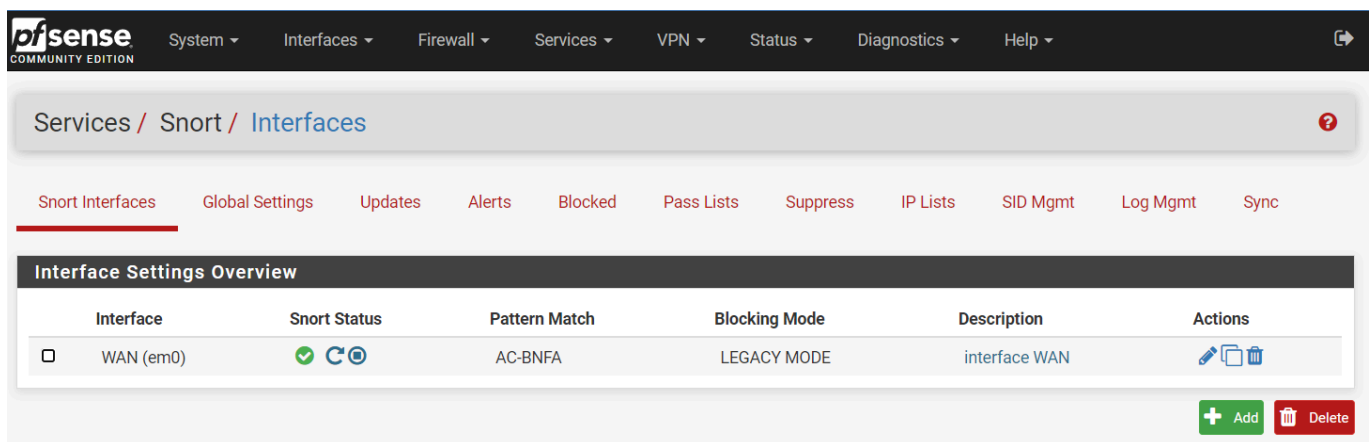
Maintenant nous pouvons activer toutes les règles précédemment téléchargées en nous rendant sur Snort Interfaces, LAN catégorie et cocher l'option Use IPS Policy. Bien penser à sauvegarder les paramètres.

<div>  System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾ </div>										
Services / Snort / Categories / LAN										
<div> Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync </div>										
<div> LAN Settings LAN Categories LAN Rules LAN Variables LAN Preprocs LAN IP Rep LAN Logs </div>										
Automatic Flowbit Resolution										
Resolve Flowbits	<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.									
Snort Subscriber IPS Policy Selection										
Use IPS Policy	<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.									
IPS Policy Selection	<div>Connectivity</div> <p>Snort IPS policies are: Connectivity, Balanced, Security or Max-Detect.</p>									

Une fois les règles activer et sauvegarder nous pouvons retourner sur Snort l'interface et le démarrer:



Une fois démarré il est dans cette état:



Voilà l'IPS est en place, nous pouvons voir les logs dans alerte et les différentes options nous permettent de gérer en temps réel les entrées et sorties de notre réseau WAN.

6. Test de fonctionnement IPS

Maintenant que nous avons mis en place l'IPS nous pouvons vérifier qu'il fonctionne en allant dans Service > Snort > blocked Hosts. Ici on retrouve tous les host qui se sont fait bloquer par l'IPS, c'est hosts bloquer ont également créer des logs dans l'interface "Alerte" mais cela ne nous intéresse pas car ils sont

directement bloquer et ne peuvent donc pas entrer sur le réseau.

Services / Snort / Blocked Hosts

Snort Interfaces

Global Settings

Updates

Alerts

Blocked

Pass Lists

Suppress

IP Lists

SID Mgmt

Log Mgmt

Sync

Blocked Hosts and Log View Settings

Blocked Hosts

Download

Clear

All blocked hosts will be saved

All blocked hosts will be removed

Refresh and Log View

Save

☒ Refresh

500

Save auto-refresh and view settings

Default is ON

Number of blocked entries to view.

Default is 500

Last 500 Hosts Blocked by Snort (only applicable to Legacy Blocking Mode interfaces)

#	IP	Alert Descriptions and Event Times	Remove
1	13.39.208.199 Q	(spp_ssl) Invalid Client HELLO after Server HELLO Detected -- 2024-01-30 13:57:48	X
2	51.178.65.231 Q	(http_inspect) PROTOCOL-OTHER HTTP server response before client request -- 2024-01-30 13:13:52 (http_inspect) BARE BYTE UNICODE ENCODING -- 2024-01-30 13:13:52	X
3	57.128.101.77 Q	(http_inspect) PROTOCOL-OTHER HTTP server response before client request -- 2024-01-30 13:14:14 (http_inspect) BARE BYTE UNICODE ENCODING -- 2024-01-30 13:14:14	X
4	141.95.145.210 Q	(http_inspect) PROTOCOL-OTHER HTTP server response before client request -- 2024-01-30 13:26:27 (http_inspect) BARE BYTE UNICODE ENCODING -- 2024-01-30 13:26:27	X
5	162.19.169.41 Q	(http_inspect) PROTOCOL-OTHER HTTP server response before client request -- 2024-01-30 13:26:28 (http_inspect) BARE BYTE UNICODE ENCODING -- 2024-01-30 13:26:28	X
6	138.199.36.111 Q	(http_inspect) PROTOCOL-OTHER HTTP server response before client request -- 2024-01-30 13:44:23 (http_inspect) BARE BYTE UNICODE ENCODING -- 2024-01-30 13:44:23	X