République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université A/Mira de Béjaïa
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle

En vue d'obtention du diplôme de Master Professionnel en Informatique.
Spécialité : Adminstration et Sécurité des Réseaux.

Thème

Mise en place d'un système de détection d'intrusion au niveau de SONATRACH Béjaïa

---

Réalisé par :

Mlle. Medjdoub Kahina

Mlle. Mebarki Izdihar.

Evalué le 03/07/2023 devant le jury composé de :

Encadrant	**Dr. BACHIRI Lina**	**MCA**
Examinateur	**Dr.Zidani Feroudja**	**MCA**
Président	**Dr.Zamouche Djamila**	**MAB**

Année universitaire 2022/2023

Remerciements

Nous tonnons à remercier :

Le bon dieu de nous avoir donné la patience et la volonté pour accomplir ce travail.

Nos remerciements s'adressent également à :

Notre Encadreur Dr.Bachiri Lina pour ses conseils, ses orientations pour nous avoir transmit les renseignements nécessaires à la réalisation de ce travail.

Nous remercions également :

L'organisme d'accueil SONATRACH tout particulièrement le chef de service informatique, Mr Rehmani Seghir, pour avoir mit à notre disposition la place de déroulement de notre stage.

Nous tenons également à remercier :

Les membres de jury, pour l'honneur qu'ils nous font en acceptant de juger, de lire et d'évaluer ce mémoire.

Enfin, nous remercions toutes personne ayant contribué de près ou de loin à la réalisation de ce travail.

Dédicaces

Je tiens à dédier vivement ce modeste travail A nos chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de nos études.

A nos chères frères, nos chères soeurs pour leurs encouragements permanents, et leur soutien moral.

A toute nos famille pour leur soutien tout au long de mon parcours universitaire.

A tous nos amis(es).

A tous ceux qui ont contribué de prés ou de loin à la réalisation de ce travail.

Kahina et Izdihar

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

IDS	Intrusion detection System
IPS	intrusion prevention system
TCP	Transmission Control Protocols
UDP	User Datagram Protocol
IP	Internet Protocol
ARP	Address Resolution Protocol
DHCP	Dynamic Host Configuration Protocol
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
FTP	File Transfer Protocol
POP3	(Port Office Protocole version 3
CLI	Command Line Interface
GUI	Graphical User Interface
Web	World Wide Web
SNMP	Simple Network Management Protocol
SSH	Secure Shell
CPU	Central Processing Unit
MAC	Media Access Control
DNS	Domain Name System
SQL	Structured Query Language
MITM	man-in-the-middle
DoS	Denial of Service
USB	Universal Serial Bus
IPsec	Internet Protocole Security
AH	Authentification Header
ESP	Encapsulating Security Payload
SSL	Secure Sockets Layer
HTTPs	HTTP sécurisé
PKI	Public Key Infrastructure
CA	Certification Authority
VLAN	Virtual Local Area Network
IEEE	Institute of Electrical and Electronics Engineers
VPN	Virtual Private Network
NAT	Network Address Translation
ACL	Access Control List
IOS	International Organization for Standardization
FTP	File Transfer Protocol
DMZ	DeMilitarized Zone
OSI	Open Systems Interconnection
URL	Uniform Resource Locator
HIDS	Host Based IDS
NIDS	Network IDS
GNS	Graphical Network Simulator

LAN Local Area Network
WAN Wide Area Network
CD Compact Disc
DVD Digital Versatile Disc
UTM Unified Threat Management
CPU Central Processing Unit
HIPS Host-based Intrusion Prevention System
NIPS Network Intrusion Prevention System
KIPS Kernel Intrusion Prevention System
VRT Vulnerability Research Team

Introduction générale

De nos jours toutes les entreprises possèdent un réseau local et généralement possèdent aussi l'accès à l'internet, à fin d'accéder à la main d'information disponible sur les réseaux, et de pouvoir communiquer avec l'extérieur. Cette ouverture vers l'extérieur est indispensable et dangereuse au même temps. Ouvrir l'entreprise vers le monde signifie aussi laisser place ouverte aux étrangèrs pour essayer de pénétrer le réseau local de l'entreprise y accomplir des actions douteuses de destruction, vol d'informations confidentiels ... etc.

Pour éviter ces restrictions, les administrateurs déploient des solutions de sécurité efficace capable de protéger le réseau de l'entreprise. Dans ce contexte, les IDS (Systèmes de Détection d'Intrusion) constituent une bonne alternative pour mieux protéger le réseau informatique.

Cette technologie consiste à rechercher une suite de mots ou de paramètres caractérisant une attaque dans un flux de paquets. Son objectif est de détecter toute violation liée à la politique de sécurité, il permet ainsi de signaler les attaques. Une solution efficace doit être mise en place, d'où la mise en place d'un système de détection d'intrusion dont le nom est Snort au niveau de l'entreprise SONATRACH de Bejaia, c'est l'objet de ce mémoire de fin de cycle. Nous avons organisé le travail en quatre chapitres :

Dans le premier chapitre, nous présentons des généralités sur les réseaux informatiques et leurs systèmes de sécurité. le chapitre sera divisé en deux parties, dans la première nous allons parler uniquement sur les réseaux informatiques et la seconde sera consacrée pour la sécurité informatique .

Dans le deuxième chapitre, nous allons présenter l'organisme d'accueil, la société nationale des hydrocarbures (SONATRACH) généralement et la RTC de Bejaia. son activité, ses différentes directions.

Dans le troisième chapitre, nous allons donner une description bien détaillée des systèmes de détection et de prévention d'intrusion (leurs différents types, leurs principes de fonctionnement, une comparaison entre IDS et IPS).Le quatrième chapitre sera consacré à

la mise en oeuvre et le test de Snort, nous détaillerons l'installation de Snort sous le pare feu PFSense, ainsi tous les paramétrages nécessaires afin de le rendre fonctionnel. Enfin, nous testerons la fiabilité de notre solution en lançant quelques attaques réelles externe et interne dans le but de suivre son comportement.

Chapitre 1

Généralités sur la sécurité des réseaux informatiques

1.1 Introduction

Les réseaux informatiques sont nés d'un besoin d'échanger des informations de manière simple, sécurisée et rapide entre les machines.
Au cours de ce chapitre, nous aborderons principalement les différentes caractéristiques liées à la sécurité des réseaux informatiques et ces outiles, Nous allons définir dans un premier temps les notions de bases sur les réseaux informatiques tels que leurs types, leurs architectures, les différentes protocoles.

1.2 Réseau informatique

Un réseau informatique, est un ensemble d'équipements matériels et logiciels interconnectés les uns avec les autres, il permet de faire circuler les éléments ou l'échanger des informations, tel que le transfert des fichiers, le partage de ressources (imprimantes et données), la messagerie ou l'exécution de programmes à distance. [1]

1.2.1 Architecture des réseaux

On distingue également deux catégories de réseaux[2] :

a) Les réseaux Post à post (Peer to Peer) : Sur un réseau post à post, les ordinateurs sont connectés directement l'un à l'autre et il n'existe pas d'ordinateur central, comme présenté dans la figure 1.1.

L'avantage majeur d'une telle installation est son faible coût en matériel (les postes de travail et une carte réseau par poste). En revanche, si le réseau commence à comporter plusieurs machines il devient impossible à gérer.

b) Les réseaux client-serveur : Sur un réseau à architecture client/serveur, tous les ordinateurs (client) sont connectés à un ordinateur central (le serveur du réseau), une machine généralement très puissante en terme de capacité; Elle est utilisée surtout pour le partage de connexion Internet et de logiciels centralisés, ce type d'architecture est plus facile à administrer lorsque le réseau est important car l'administration est centralisé mais elle nécessite un logiciel couteux spécialisé pour l'exploitation du réseau (Voir la figure1.1).

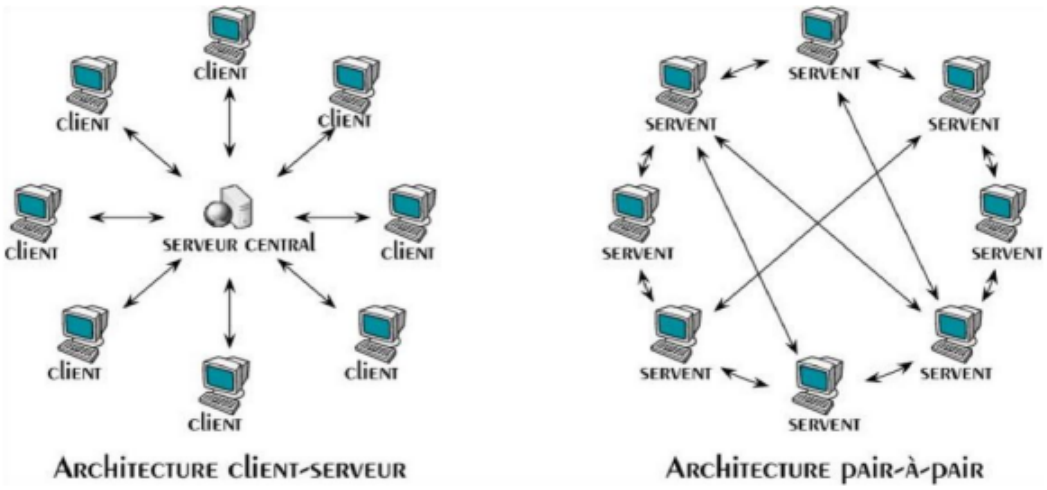


FIGURE 1.1 – Architecture des réseaux

1.2.2 Différents types de réseau

Il existe différentes types de réseaux classifiés selon leur tailles, vitesses de transfert des données ainsi que leur étendus [3] :

• **Réseau personnel :** Petit réseau de quelques mètres d'étendus, permettant l'interconnexion de machines personnelles : Pc portables, mobile téléphonique, agenda électronique, etc.

• **Réseau local :** Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie (la plus répondue étant Ethernet). La taille d'un réseau local peut atteindre jusqu'à 100 voire 1000 utilisateurs .

• **Réseau métro politan :** Interconnectent plusieurs LAN géographiquement proches (au maximum quelques dizaines de km) à des débits importants, supérieur à 100 Mbits/s. Ainsi Un MAN est formé de commutateurs ou de routeurs interconnectés par des liens hauts débits (en général en fibre optique).

• **Réseau étendu :** Interconnecte plusieurs LAN à travers de grandes distances géographiques. Les débits disponibles sur un WAN résultent d'un arbitrage avec le coût des liaisons (qui augmente avec la distance) et peuvent être faibles. Les WAN fonctionnent grâce à des routeurs qui permettent de choisir le trajet le plus approprié pour atteindre un noeud du réseau. Le plus connu des WAN est Internet .

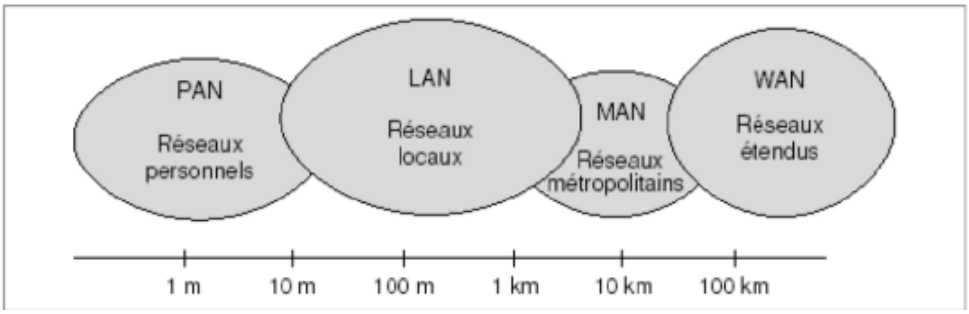


FIGURE 1.2 – Différents types de réseau

1.2.3 Modèle de référence OSI

Le modelé OSI (Operating System Interconnection) définit une sorte de langage commun. Il est devenu le socle de référence pour tout système de traitement de communication. Il est repartit les questions relatives au domaine des communications informatique selon sept couche classées par ordre décroissant. Son objectif est d'assuré que les protocoles spécifiques utilisés dans chacune des couches coopèrent pour assurer une communication efficaces. Décrivons succinctement le rôle de chaque couche [26] :

	PDU	Couche		Fonction
Couches hautes	Donnée	7	Application	Point d'accès aux services réseau
		6	Présentation	Gère le chiffrement et le déchiffrement des données, convertit les données machine en données exploitables par n'importe quelle autre machine
		5	Session	Communication Interhost, gère les sessions entre les différentes applications
	Segment (en) / Datagramme	4	Transport	Connexion de bout en bout, connectabilité et contrôle de flux ; notion de port (TCP et UDP)
Couches matérielles	Paquet	3	Réseau	Détermine le parcours des données et l'adressage logique (adresse IP)
	Trame	2	Liaison	Adressage physique (adresse MAC)
	Bit	1	Physique	Transmission des signaux sous forme numérique ou analogique

FIGURE 1.3 – Modèle OSI.

Les quatre couches inférieures (1, 2, 3 et 4) sont nécessaires à l'acheminement des informations entre les extrémités concernées et dépendent du support physique. Les trois couches supérieures (5, 6 et 7) sont responsables du traitement de l'information relative à la gestion des échanges entre systèmes informatiques. Par ailleurs, les couches 1 à 3 interviennent entre machines voisines, et non entre les machines d'extrémité qui peuvent être séparées par plusieurs routeurs.

Le modèle OSI comporte sept couches, chaque couche a des fonctions de manipulation de commandes ou de données significatives qui sont décrites et détaillées plus bas :

• **La Couche application :** C'est l'interface entre l'utilisateur et les applications et le réseau. Elle concerne la messagerie, le transfert et partage de fichiers, l'émulation de terminaux.

• **La Couche présentation :** Elle converti les données en information compréhensible par les applications et les utilisateurs : Syntaxe, sémantique, conversion des caractères graphique, format des fichiers, cryptage et compression.

• **La Couche session :** Son unité d'information est la translation. Elle s'occupe de la gestion et sécurisation du dialogue entre les machine connectes, les applications et les utilisateurs.

• **La couche transport :** Elle segmente les donnes de la couche session, prépare et contrôle les taches de la couche réseau. Elle peut multiplier les vois et corrige les erreurs de transport.

• **La couche réseau :** Elle traite la partie donnée utile contenu dans une trame. Elle connait l'adresse de toutes les destinations choisit par le meilleur itinéraire pour l'acheminement. Donc elle gère l'adressage logique et le routage.

• **La couche liaison de données :** Gère les communications entre deux machines directement connectées entre elles, ou connectées à un équipement qui émule une connexion directe (commutateur). Un rôle important de cette couche est la détection et la correction d'erreurs intervenues sur la couche physique. Elle est divisée en deux sous-couches : 1. Couche LLC (Logical Link Control) qui assure le transport des trame et gère l'adressage des utilisateurs. 2. Couche MAC (Medium Access Control) qui structure les de donnes en trame et gère l'adressage des carte réseaux.

• **La couche physique :** Elle convertit les signaux électrique en bits de données et inversement, selon qu'elle transmet ou reçoit les informations à la couche liaison de données.

1.2.4 Modèle de protocole TCP/IP :

Ce modèle suit la structure d'une suite de protocoles donnée. Le modèle TCP/IP est un modèle de protocole, car il décrit les fonctions qui interviennent à chaque couche de protocoles au sein de la suite TCP/IP. TCP/IP est également utilisé comme modèle de référence [26] :

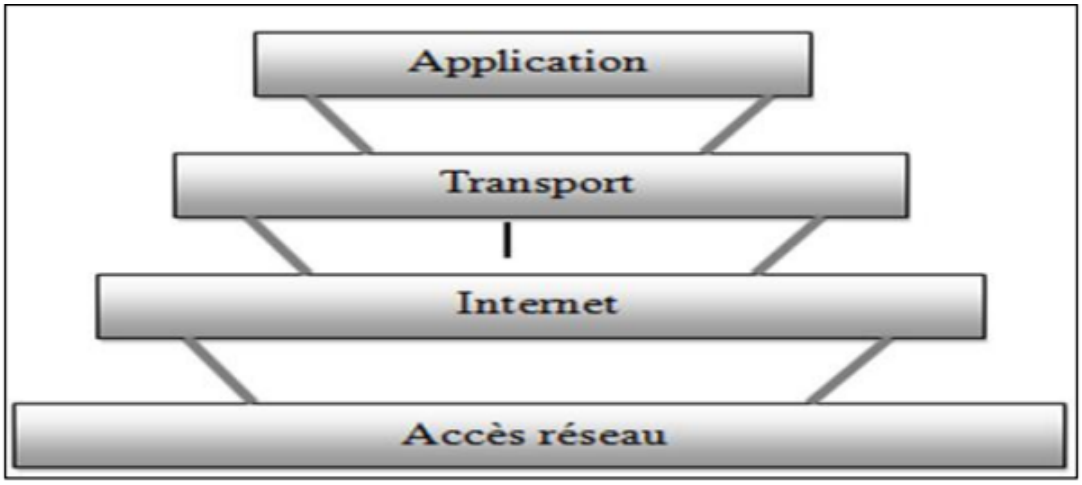


FIGURE 1.4 – Modèle TCP/IP.

• **La couche Application :** La couche application similaire de la couche homonyme de modèle OSI, correspond aux différentes applications utilisant les services réseaux pour communiquer à travers le réseau.

• **La couche Transport :** La couche transport gère le fractionnement et le réassemblage en paquet de flux de donnée à transmettre. Le routage ayant pour conséquence un arrivage des paquets dans un ordre incertain. Cette couche s'occupe aussi réagencement ordonnée de tous les paquets d'un même message.

• **La couche Internet :** La couche internet s'occupe de l'acheminement, à bonne destination, des paquets de données indépendamment les uns des autres, soit donc de leur routage à travers les différents nœuds par rapport le trafic et à la congestion du réseau. Le protocole IP assure intégralement les services de cette couche, et constitué donc l'un des points-clefs du modèle OSI/IP.

• **La couche Accès réseau :** La couche accès réseau, intégrant les services des couches physique et liaison du modèle OSI, a en charge la communication avec l'interface physique afin de transmettre ou de récupérer les paquets de donnes qui lui sont transmis de la couche supérieure.

1.2.5 Protocoles réseaux

1.2.5.1 Définition d'un protocole

Un protocole est une méthode standard qui permet la communication entre des processus (s'exécutant éventuellement sur différentes machines), c'est-à-dire un ensemble de règles et de procédures à respecter pour émettre et recevoir des données sur un réseau.

1.2.5.2 Les différents type de protocoles

Il en existe plusieurs selon ce que l'on attend de la communication. Certains protocoles seront par exemple spécialisés dans l'échange de fichiers, d'autres pourront servir à gérer simplement l'état de la transmission et des erreurs [4].

• **Le Protocole TCP :** est un protocole de la couche transport, utilisé sur le réseau Internet pour transmettre des données entre deux machines. TCP prend à sa charge l'ouverture et le contrôle de la liaison entre deux ordinateurs.

• **Protocole UDP :** est un protocole de la couche transport permettant l'envoi sans connexion de datagrammes dans des réseaux basés sur le protocole IP. Afin d'atteindre les services souhaités sur les hôtes de destination, le protocole utilise des ports qui constituent un élément essentiel de l'entête UDP.

• **Le protocole IP :** est un protocole de la couche internet, permet de gérer l'acheminement des paquets d'une machine à une autre ainsi que l'adressage. Au plus bas niveau (physique), on dispose alors d'interfaces pour communiquer d'un point à un autre.

•**Protocole DHCP :** Il s'agit d'un protocole de la couche application, qui permet à un ordinateur qui se connecte sur un réseau d'obtenir dynamiquement sa configuration .

• **Protocole HTTP :** un protocole de la couche application, fait la communication entre un client et un serveur pour le World Wide Web, le protocole http établit une liaison entre un ordinateur (client) et un serveur Web.

• **Protocole ARP :** Address Resolution Protocol est un protocole effectuant la traduction

d'une adresse de protocole de couche réseau (typiquement une adresse IPv4) en une adresse MAC (typiquement une adresse Ethernet), Il se situe à l'interface entre la couche réseau et la couche de liaison du modèle OSI.

• **Protocole ICMP :** est un protocole de la couche réseau,qui permet le contrôle des erreurs de transmission.

• **Protocole FTP :** File Transfer Protocol (protocole de transfert de fichier), est un protocole qui appartient à la couche application, destiné au partage de fichiers sur un réseau. Il permet depuis un ordinateur de transférer des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur.

1.3 Sécurité informatique

1.3.1 Définition

C'est la protection des données et des ressources matérielles ou logicielles (ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données), contre les attaques malveillantes en mettant en place des mécanismes de contrôle qui permettant d'assurer le bon fonctionnement du système [5].

1.3.2 Terminologie de la sécurité

La sécurité informatique utilise un ensemble de termes bien spécifique, que nous énumérons comme suit [7] :

• **La vulnérabilité :** Est une faiblesse de sécurité, qui peut découler, par exemple d'une erreur d'implémentation dans le développement d'une application, erreur susceptible d'être exploité pour nuire à l'application. Elle peut également provenir d'une mauvaise configuration. Elle peut enfin avoir pour origine une insuffisance de moyens de protection des biens critiques.

• **Menace :** Elle désigne l'exploitation d'une faiblesse de sécurité par un attaquant qu'il soit

interne ou externe à l'entreprise.

• **Risque :** Les menaces engendrent des risques et des coûts humains et financiers comme la perte de confidentialité de données sensibles et l'indisponibilité de l'infrastructure et des données. Les risques peuvent survenir si le système menacé présente des vulnérabilités.

• **Attaque :** Une attaque c'est le résultat de l'exploitation d'une faille d'un système informatique(système d'exploitation, logiciel, erreur de configuration, . . . etc) à des fins non connue par l'exploitant du système et il est généralement répudiable.

• **Intrusion :** Une intrusion c'est résultat d'une attaque qui a réussi à exploiter une vulnérabilité, dans le cas où l'attaque est réalisée le système informatique n'est plus en sécurité.

1.3.3 Types d'attaques

Il existe trois types d'attaques, les attaques réseaux , les attaques applicatives et les logiciels malveillants :

1.3.3.1 Les attaque réseaux

Ce type d'attaque se base principalement sur des failles liées aux protocoles ou à leur implémentation. Nous présenterons dans ce qui suit quelques attaques bien connues[8] :

• **Attaque par usurpation d'adresse IP (IP spooffing) :** L'usurpation d'adresse IP est une technique consistant à remplacer l'adresse IP de l'expéditeur d'un paquet IP par l'adresse IP d'une autre machine. Cette technique permet ainsi à un pirate d'envoyer des paquets anonymement. Il ne s'agit pas pour autant d'un changement d'adresse IP, mais d'une mascarade de l'adresse IP au niveau des paquets émis.

• **ARP Spoofing :** Cette attaque consiste à rediriger le trafic d'une machine vers une autre. Grâce à cette redirection, une personne mal intentionnée peut se faire passer pour une autre. De plus, le pirate peut rerouter les paquets qu'il reçoit vers le véritable destinataire, ainsi l'utilisateur usurpé ne se rendra compte de rien. La finalité est la même que l'IP spoofing, mais ARP Spoofing (ARP Redirect) travaille au niveau de la couche liaison de données.

• **Déni de service :** Le déni de service est une attaque visant à rendre indisponible un ser-

vice. Ceci peut s'effectuer de plusieurs manières : par le biais d'une surcharge réseau, rendant ainsi la machine totalement injoignable; ou bien de manière applicative en crashant l'application à distance.

• **Les techniques de scan :** Elle consiste à préciser quels ports sont ouverts afin de déterminer les vulnérabilités du système. Le firewall va dans tous les cas bloquer ces scans en annonçant le port comme fermé.

1.3.3.2 Les attaques applicatives

Les attaques applicatives se basent sur des failles dans le programme utilisées, ou encore sur des erreurs de configuration. Toutes fois, il est possible de classifier ces attaques selon leur provenance [8].

• **les problèmes de configurations :** En général les administrateurs réseau se contente d'utilisé les configurations par défaut. Celles-ci sont souvent non sécurisées afin de faciliter l'exploitation du logiciel. De plus, des erreurs peuvent apparaitre lors de la configuration d'un logiciel. Une mauvaise configuration d'un serveur peut entrainer l'accès à des fichiers important ou mettre en jeu l'intégrité du système d'exploitation.

• **Les scripts :** Les scripts s'exécutent sur un serveur et renvoient un résultat au client. Cependant lorsqu'ils sont dynamiques ils utilisent des entrées saisies par un utilisateur. Des failles peuvent apparaitre si les entrées ne sont pas correctement contrôlées. L'exemple classique est l'exploitation de fichier à distance, tel que l'affichage du fichier mot de passe du système en remontant l'arborescence depuis le répertoire web.

• **Les injections SQL :** Tout comme les attaques de scripts, les injections SQL profitent de paramètres d'entrée non vérifiés. Le but des injections SQL est d'injecter du code SQL dans une requête de base de données. Ainsi, il est possible de récupérer des informations se trouvant dans la base (exemple : des mots de passe) ou encore de détruire des données.

• **Man in the middle :** L'attaque MITM est une attaque contre l'intégrité. L'attaque MITM est une redirection complète d'une connexion entre deux machines. [1] Chacun des deux interlocuteurs croit dialoguer directement avec l'autre, mais en réalité, il adresse ses données à

une troisième machine qui joue le rôle d'un routeur et renvoie les trames modifiées vers le véritable destinataire.

1.3.3.3 Logiciels malveillants

Il existe plusieurs logiciels malveillants pour cella on peut citer [9] :

• **Les virus :** Est un programme capable d'infecter d'autres programmes en les modifiant pour y inclure une copie de lui-même qui pourra avoir légèrement évolué.

• **Les Vers :** Un ver est une variété de virus qui se propage par le réseau .Il se reproduit en s'envoyant à travers un réseau (e-mail, Bluetooth, chat. . .). Le ver contrairement aux virus, n'a pas besoin de l'interaction humaine pour pouvoir se proliférer.

• **Le cheval de Troie :** Un cheval de Troie est un logiciel qui se présente utile ou préalable, et qui une fois installe sur un ordinateur y effectue des actions cachées et pernicieuse. La différence essentielle entre un cheval de Troie et un ver réside dans le fait que le ver tente de se multiplier. Ce que ne fait pas un cheval de Troie.

• **Cookies :** Un cookie est en réalité un fichier stocké sur le disque dur de l'utilisateur, afin de permettre au serveur web de le reconnaître d'une page web à l'autre. Les cookies sont notamment utilisés par les sites de commerce électronique afin de conserver les préférences de l'utilisateur afin de lui éviter de les ressaisir. Mais certain cookies sont utilisés par des personnes malintentionnées à des fins malicieuses.

1.3.4 Protocoles de sécurité

parmi les protocoles de sécurité on trouve[10] :

• **Protocole IPsec :** IPSec (Internet Protocole Security) est un protocole de niveau 3. Il est très utilisé lors de la création de réseaux privés virtuels et pour la sécurisation des accès distants à un intranet. Les services IPSec sont basés sur des mécanismes cryptographiques qui leur confèrent un niveau de sécurité élevé. La sécurisation se faisant au niveau IP, IPSec peut être mis en œuvre sur tous les équipements du réseau et fournir un moyen de protection unique pour les échanges de données.

IPSec s'insère dans la pile de protocoles TCP/IP au niveau d'IP. Ceci présente l'avantage de le rendre exploitable par les niveaux supérieurs et d'offrir un moyen de protection unique pour toutes les applications .

IPSec distingue deux niveaux de protection à travers deux protocoles :

— Authentification Header (AH) qui ne prend en charge que l'authentification, le contrôle d'intégrité et l'anti-rejeu. Le rejeu est une technique, utilisable par un intrus, qui consiste à renvoyer des paquets capturés lors d'une communication réseau légale.

— Encapsulating Security Payload (ESP) qui ajoute la fonction de confidentialité.

• **Protocole HTTPs :** HTTPs (HTTP sécurisé) est un procédé de sécurisation des transactions HTTP utilisé pour la navigation sécurisée. Il offre des possibilités d'authentification et de chiffrement pour les sites web nécessitant un certain niveau de sécurité dans leurs échanges avec les navigateurs web. Pour garantir cette sécurité, il fait usage de méthodes de cryptographie asymétrique pour l'authentification et de méthodes de cryptographie symétrique pour le chiffrement des échanges.

Contrairement à SSL au niveau de la couche de transport, HTTPs procure une sécurité basée sur des messages au dessus du protocole HTTP, en marquant individuellement les documents html à l'aide de certificats.

• **Le protocole SSH :** Le SSH (Secure Shell) permet de répondre à la principale problématique posée par la sécurité des informations, la confidentialité. En effet, grâce à ce protocole, il est possible de chiffrer des données par un système de clés privées et publiques. Ces données transitent dans un tunnel, une sorte de canal sécurisé où il est impossible de savoir ce qui se passe à l'intérieur. Dans le protocole SSH, un ordinateur client peut initier une connexion avec un ordinateur serveur .

1.4 Outils de sécurité des réseaux informatiques

1.4.1 VLAN (Virtual Local Area Network)

Un VLAN ou réseau local virtuel est un regroupement de stations de travails indépendamment de la localisation géographique sur le réseau. Ces dernières pourront communiquer comme si elles étaient sur le même segment. Un VLAN permet de crever des domaines de diffusion (domaines de broadcast) gérés par les commutateurs indépendamment de l'emplacement où se situent les noeuds, ce sont des domaines de diffusion gérés logiquement[13].(voir la figure 1.3)

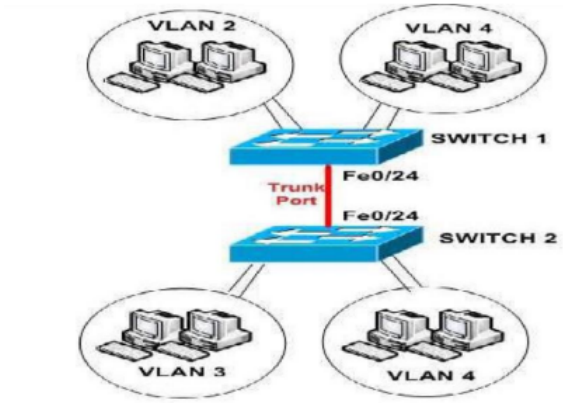


FIGURE 1.5 – Exemple de VLAN

1.4.2 VPN (Virtual Private Network)

Un VPN est un système permettant de créer un lien direct entre des ordinateurs distants. On utilise notamment ce terme dans le travail à distance notamment, ainsi que pour l'accès à des structures de type cloud computing. Un VPN permet d'accéder à des ordinateurs distants comme si l'on était connecté au réseau local.(voir la figure 1.4)

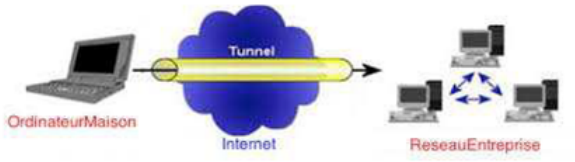


FIGURE 1.6 – principe de VPN

1.4.3 IDS (Intrusion detection System)

Un mécanisme permettant d'écouter le trafic réseau et de contrôler les activités réseau afin de repérer toutes activités anormales ou suspectes et ainsi remonter des alertes sur les tentatives d'intrusion à un système informatique. C'est un outil complémentaire aux firewall[12].

1.4.4 IPS (intrusion prevention system)

Un IPS est un outil des spécialistes en sécurité des systèmes d'information, permettant de détecter une attaque sur le système surveillé et de mettre en place des mécanismes de défense permettant de mitiger l'attaque [12],

1.4.5 NAT (Network Address Translation)

On dit qu'un routeur fait du (NAT) (« traduction d'adresse réseau »lorsqu'il fait correspondre les adresses IP internes non uniques et souvent non routables d'un intranet à un ensemble d'adresses externes uniques et routables. Ce mécanisme permet notamment de faire correspondre une seule adresse externe publique visible sur Internet à toutes les adresses d'un réseau privé, et pallie ainsi l'épuisement des adresses IPv4,il existe deux type de NAT statique et dynamique.

FIGURE 1.7 – Network address translation

1.4.6 Proxy

Un serveur proxy est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local et internet. La plupart du temps le serveur proxy est utilisé pour le web, il s'agit alors d'un proxy HTTP. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP, ...)[13].

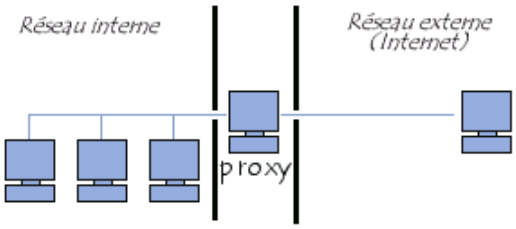


FIGURE 1.8 – Proxy

1.4.7 Par-feux

Un pare-feu est un système logiciel ou matériel placé entre un réseau fiable et un autre non fiable comme le montre la figure 1.7 . L'objectif principal de son implémentation est de filtrer et d'empêcher le trafic indésirable de traverser la limite du pare-feu. Pour ce faire, un pare-feu doit assurer les recommandations suivantes[11] :

— être résistant aux attaques.

— être le seul point de transit entre deux réseaux.

FIGURE 1.9 – Placement d'un firewall

1.4.8 DMZ (DeMilitarized Zone)

Une DMZ est une zone tampon d'un réseau d'entreprise, située entre le réseau local et Internet, derriére le pare-feu. Il s'agit d'un réseau intermédiaire regroupant des serveurs publics (HTTP, DHCP, mails, DNS, etc.). Ces serveurs devront être accessibles depuis le réseau interne de l'entreprise et, pour certains, depuis les réseaux externes. Le but est ainsi d'éviter toute connexion directe au réseau interne. La figure 1.8 illustre l'architecture DMZ.

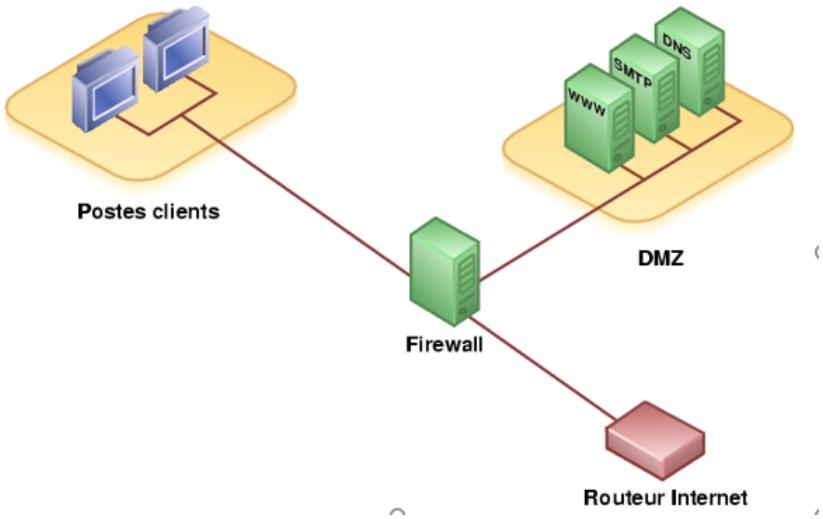


FIGURE 1.10 – DMZ

1.5 Conclusion

Au cours de ce chapitre, nous avons pris connaissance des différents aspects liées aux réseaux informatique et à leur sécurité, ainsi que les différentes attaques pouvant corrompre

le bon fonctionnement d'un réseau.

Dans le chapitre qui suit, nous allons présenter l'organisme d'accueil de l'entreprise SONATRACH .

Chapitre 2

Présentation de l'organisme d'accueil

2.1 Introduction

L'étude de l'organisme d'accueil est une étape importante qui sert à représenter les contraintes sous lesquelles se réalisera notre projet. Dans ce chapitre, nous allons présenter l'entreprise SONATRACH, citer les différents départements qui la constituent et donner quelques informations qui nous seront utiles dans notre travail, tout en posant la problématique autours de laquelle tournera notre mémoire.

2.2 Présentation générale de l'organisme d'accueil

SONATRACH est un Groupe pétrolier et gazier intégré sur toute la chaine des hydrocarbures. Il détient en totalité ou en majorité absolue, plus de vingt entreprises importantes sur tous les métiers connexes à l'industrie pétrolière tel que le forage, le raffinage... Il possède aussi des participations significatives dans près de 50 entreprises implantées tant en Algérie qu'à l'étranger.

2.3 Historique et missions

L'entreprise "SONATRACH" (Société Nationale pour le Transport et la Commercialisation des Hydrocarbures) a été crée le 31 Décembre 1963 par le décret n°63/491, les statuts ont été modifiés par le décret n°66/292 du 22 Septembre 1966, et SONATRACH devient "Société nationale pour la recherche, la production, le transport, la transformation et la commercialisation des hydrocarbures", cela a conduit à une restructuration de l'entreprise dans le cadre d'un schéma directeur approuvé au début de l'année 1981 pour une meilleure efficacité organisationnelle et économique, de ces principes SONATRACH a donné naissance à 17 entreprises : (NAFTAL, ENIP, ENAC,...etc.)
Après sa restructuration en 1982, et sa réorganisation en 1985, SONATRACH s'est recentrée sur ses métiers de base que constituent les activités suivantes :

— Exploration et recherche.

— Exploration des gisements d'hydrocarbures.

— Le transport par canalisation.

— La liquéfaction et la transformation de GAZ.

— La commercialisation.

Pour la réalisation de ces objectifs, SONATRACH est divisé en cinq branches différentes représentées dans la figure 2.1 :

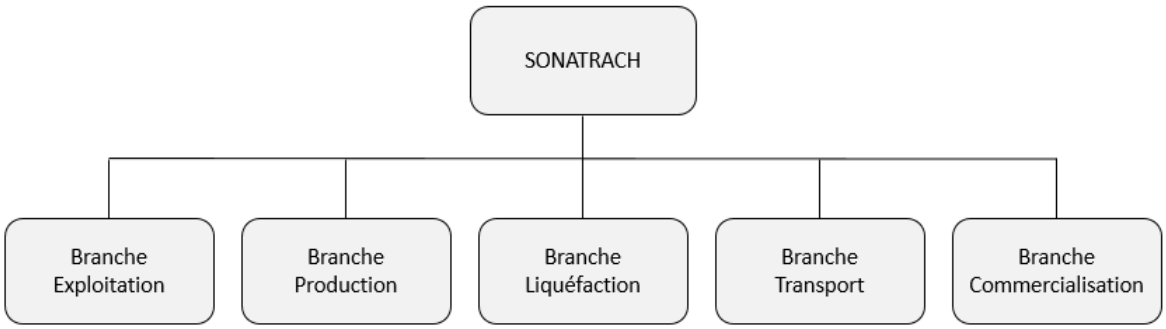


FIGURE 2.1 – Organigramme de la RTC

à travers cette transformation structurelle et fractionnelle, un schéma de groupes a évolué en constituant des branches d'activités autonomes et leurs filiations. De la branche (Activité de transport par canalisation), se trouve la Direction Régionale de Bejaia (DRGB) où s'est déroulé notre stage pratique.

2.4 Activités de la branche transport par canalisation (TRC)

L'activité de transport par canalisation (TRC) est en charge de l'acheminement des hydrocarbures pétroles brut, gaz et condensat vers les ports pétroliers, les zones de stockages et les pays d'exploitation. Les missions affectées à la branche transport par canalisation sont :

— La gestion et l'exploitation des ouvrages et canalisations de transport d'hydrocarbures.

— La coordination et le contrôle de l'exécution des programmes de transport arrêtés en fonction des impératifs de production et de commercialisation.

— La maintenance, l'entretien et la protection des ouvrages et canalisations.

— L'exécution des révisions générales, des machines tournantes et équipements.

— La gestion de l'interface transport des projets internationaux du groupe ou en partenariat.

La SONATRACH possède cinq directions régionales de transport des hydrocarbures :

— La direction régionale Est (Skikda).

— La direction régionale Centre (Béjaia).

— La direction régionale Ouest (Arzew).

— La direction régionale de Haoud-El-Hamra.

— La direction régionale d'Ain Amenas.

2.5 Présentation de la direction régionale de Bejaia (DRGB)

La DRGB est l'une des cinq directions chargée du transport, du stockage et de la livraison des hydrocarbures liquides et gazeux. Les hydrocarbures transportés à travers les canalisations gérées et exploitées par la DRGB sont :

— Le GAZ naturel.

— Le pétrole brut.

— Le condensat.

2.6 Structure de la DRGB

Nous illustrons les directions et sous-directions dans le diagramme de la figure 2.2 comme suit :

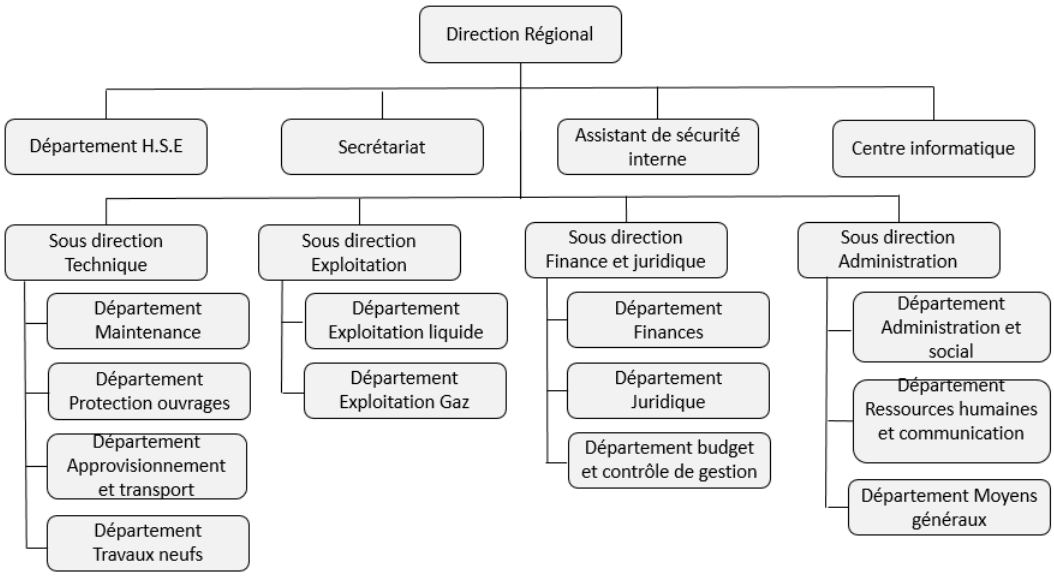


FIGURE 2.2 – Organigramme de la RTC

• **Direction régionale :** Elle est dirigée par un directeur régional aidé par des assistants et un secrétariat.

• **Secrétariat.**

• **Assistant de sûreté interne :** Sa mission est de protéger et de sauvegarder le patrimoine humain et matériel de la DRGB.

• **Centre informatique :**Il regroupe les moyens d'exploitation et de développement des applications informatiques pour l'ensemble des structures de la DRGB, ainsi que la gestion du réseau informatique interne.

• **Sous direction technique :** Elle a pour mission d'assurer la maintenance et la protection des ouvrages. Elle est organisée en quatre départements : département maintenance, département protection des ouvrages, département approvisionnement et transport et département des travaux neufs.

• **Sous direction Exploitation :** Elle est chargée de l'exploitation des installations de la région, et de maintenir le fonctionnement de trois ouvrages en effectuant des réparations en cas de fuite, de sabotage ou de panne pour les stations de pompage. Elle est composée de deux départements : le département exploitation liquide et le département exploitation gaz.

• **Sous direction Finances et Juridique :** Elle a pour mission d'effectuer la gestion financière,

le budget et le contrôle de gestion et de prendre en charge les affaires juridiques de la DRGB. Elle est organisée en trois départements : département finances, département juridique, département budget et contrôle de gestion.

• **Sous direction Administration :** Elle a pour mission la gestion des ressources humaines et les moyens généraux. Elle est organisée en trois départements : département administration et social, département ressources humaines et communication et département moyens généraux.

• **Présentation du centre informatique :** Le centre informatique est chargé du développement et de l'exploitation des applications informatiques de gestion pour le compte de la direction régionale de Béjaia (DRGB) et des autres régions.

2.7 Organisation structurelle

L'organisation du centre ne cesse de subir des changements et l'évolution rapide de l'informatique pousse le centre à adopter des actions nouvelles à chaque fois afin de subvenir aux nouveaux besoins de l'entreprise.

Pour mener à bien sa mission, le centre informatique s'organise en trois services tels qu'ils sont schématisés dans la figure 2.3 :

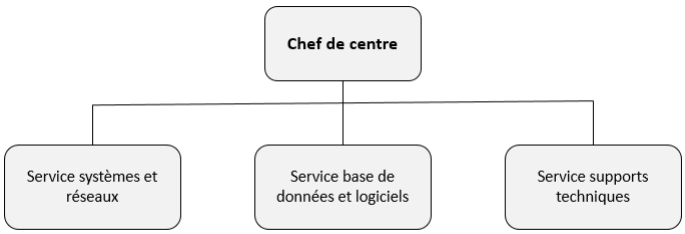


FIGURE 2.3 – Organigramme du centre informatique

2.8 Organisation fonctionnelle

Chaque service a sa propre fonction, nous allons définir et citer les différentes tâches de chacun ci-dessous :

2.8.1 Service systèmes et réseaux

• Système :

— Choix des équipements informatiques et logiciels de base.

— Mise en oeuvre des solutions matérielles et logicielles retenues.

— Installation et configuration des systèmes.

— Mise en oeuvre des nouvelles versions de logiciels.

• Réseau :

— Assurer le bon fonctionnement et la fiabilité des communications.

— Assurer l'administration du réseau et organiser l'évolution de sa structure.

— Etude et choix de l'architecture du réseau à installer et la participation à sa mise en place.

— Définition des droits d'accès à l'utilisation du réseau.

— Assurer la surveillance permanente pour détecter les pannes.

— Traitement des incidents survenant sur le réseau.

2.8.2 Service base de données et logiciels :

• Base de données

— Conception des bases de données, optimisation et suivi des données informatiques.

— Installation, configuration et exploitation du système de gestion de bases de données et ses bases.

— Mise en oeuvre et gestion des procédures de sécurité.

— Gestion de la sauvegarde, la restauration et la migration des données.

• Logiciels :

— Etude et conception des systèmes d'information.

— Développement et maintenance des applications informatiques pour TRC.

— Déploiement des applications et formation des utilisateurs.

2.8.3 Service supports techniques :

— Assistance aux utilisateurs en cas de problèmes software et hardware.

— Installation des logiciels de gestion, technique et bureautique.

— Formation aux nouveaux produits installés.

2.9 Aspect réseau

Le réseau de la DRGB est constitué de deux parties connectées entre elle (le réseau de l'ancien bâtiment et le réseau du nouveau bâtiment). En effet, il a subit une extension après la construction du nouveau bâtiment.

2.9.1 Les commutateurs utilisés dans le réseau de la DRGB

Le réseau de la DRGB utilise deux types de commutateurs :

• **Les commutateurs intelligents :** En plus de leur fonction ils peuvent faire le routage. Dans le réseau de la DRGB, on trouve trois exemples de ce type qui sont :

— Catalyst Cisco 6509 : La gamme Catalyst 6509 représentée sur la figure 2.4 offre des moyens pour soutenir la capacité de la bande passante du système et des capacités améliorées de gestion des câbles. Elle fournit également des flux d'air d'avant en arrière qui est optimisé pour les conceptions allée chaude et froide dans le centre de données co-localisées et les déploiements de services. En outre elle offre une protection exceptionnelle des investissements en soutenant plusieurs générations de produits sur le même châssis, réduisant ainsi les coûts totaux de propriété. Le cadre Cisco Catalyst 6509 supporte à la fois la gamme Cisco Catalyst 6500 Supervisor Engine 32 et Cisco Catalyst 6500 Series Supervisor Engine 720 familles, avec LAN associés, WAN, et des modules de services .

FIGURE 2.4 – Gamme Catalyst Cisco 6509

— Catalyst Cisco 3750 : La gamme Cisco Catalyst 3750 représentée dans la figure 2.5 est une ligne de commutateurs innovants qui améliorent l'efficacité de l'exploitation des réseaux locaux grâce à leur simplicité d'utilisation et leur résilience la plus élevée disponibles pour des commutateurs empilables. Cette gamme de produits dispose de la technologie Cisco StackWise, interconnectant les commutateurs au sein d'une même pile à 32 Gbps qui permet de construire un système unique de commutation à haute disponibilité. En outre, elle est optimisée pour les déploiements Gigabit Ethernet haute densité et comprend un large éventail de commutateurs qui répondent aux exigences en matière d'accès, d'agrégation ou de connectivité dorsale pour de petits réseaux .

FIGURE 2.5 – Gamme Catalyst Cisco 3750

• **Les commutateurs non intelligents :** Ce type de commutateurs ne permet pas de faire le routage. Le réseau de la DRGB contient le type suivant :

— Catalyst Cisco 3550 : C'est une gamme de commutateurs CISCO empilables, il fournit une haute disponibilité et des fonctionnalités avancées de qualité de service et de la sécurité afin d'améliorer l'exploitation de réseau (Figure 2.6) .

FIGURE 2.6 – Gamme Catalyst Cisco 3550

2.10 Aspect sécurité

• **Serveur antivirus :** Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants. Ceux-ci peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de programme modifiant ou supprimant des fichiers, que ce soit des documents infectés de l'utilisateur ou des fichiers nécessaires au bon fonctionnement de l'ordinateur. Un antivirus vérifie les fichiers et courriers électroniques, les secteurs de boot (pour détecter les virus de boot), mais aussi la mémoire vive de l'ordinateur, les médias amovibles (clés USB, CD, DVD etc), les données qui transitent sur les éventuels réseaux (dont Internet) etc .

• **Serveur filtrage Web :**Permet d'interdire l'accès à des sites au contenu répréhensible ou plus simplement de bloquer les bannières publicitaires. Les règles de filtrage sont mises à jour automatiquement dans l'établissement à partir d'une base de données. Les sites filtrés sont classés par catégories (adultes, piratages, publicités) modifiables, ainsi c'est l'établissement qui maîtrise sa politique de filtrage .

• **Serveur reporting :** C'est un outil complet et de rapport facile à utiliser qui permet d'évaluer l'utilisation de l'Internet par des employés de l'entreprise, identifier tous les problèmes possibles avec accès à l'Internet ou à la consommation de la bande passante réseau en générant des rapports détaillés, des résumés ou des graphiques. Il est utilisé pour montrer comment la connexion Internet est utilisée et pour affiner les stratégies de filtrage afin de maximiser les ressources du réseau .

• **Firewall juniper ssg 550 :** : Représente une nouvelle classe de dispositif de sécurité construite à cet effet qui offre un parfait mélange de haute performance, de sécurité et de connectivité LAN/WAN pour les déploiements de bureau régional et de leurs branches. Avec un réseau éprouvé et la protection au niveau application, le SSG 550 peut être mis en oeuvre comme dispositif de sécurité autonome pour arrêter les vers, les logiciels espions, cheval de trois, les logiciels malveillants et autres attaques émergentes (Figure 2.7).

FIGURE 2.7 – Firewall Juniper ssg 550

Firewall juniper ssg 550 représenté dans la figure 2.7 contient un ensemble de règles structurées en trois zones qui se présentent comme suit :

• **La zone strust :** C'est la zone la plus confiante, car elle autorise le trafic sortant et interdit le trafic entrant et c'est pour cela que la RTC lui a confiée son réseau LAN.

• **La zone untrust :** C'est une zone qui autorise de trafic entrant et interdit le trafic sortant.

• **La DMZ (Demilitarized Zone) :** C'est une zone tampon d'un réseau d'entreprise, située entre le réseau local et Internet derrière le par-feu. Il s'agit d'un réseau intermédiaire regroupant des serveurs publics (DNS, HTTP, DHCP). Ces serveurs devront être accessibles depuis le réseau interne de l'entreprise et, pour certains, depuis le réseau externe. Le but est ainsi d'éviter toute connexion directe au réseau interne.

2.11 Problématique

Aujourd'hui l'internet apporte une réelle valeur ajoutée aux entreprises, en permettant la communication avec de nombreux partenaires, fournisseurs et clients, ceux-ci expose les

systèmes des entreprises à de nouvelles formes de menaces. Le véritable défi est La sécurisation du réseau informatique pour conserver un haut degré de fiabilité du trafic sur le réseau. vu que Firewall et d'autres antivirus ne suffisent pas à garantir la sécurité des réseaux informatiques, des systémes de détction et de prévention d'intrusion sont mis en place. De ce fait, durant notre stage au sein de SONATRACH nous avons constaté des anomalies relatives à la sécurité de leur réseau, à savoir le manque d'un mécanisme de détection et de prévention d'intrusion.

2.12 Propositions

Pour pallier les problèmes énumérés, le firewall (Pfsense) n'est pas suffisant à l'avenir car ce dernier ne permet pas de signaler les actions malveillantes venant de stations non protégées.
De ce fait, nous allons proposer la mise en place d'un système de détection d'intrusion (IDS) qui s'appelle Snort au sein du firewall, car il joue un rôle de complément a ce dernier, en lui permettant une analyse plus intelligente des paquets constituant les données circulantes, en détectant toute activité suspecte.

2.13 Conclusion

Dans ce chapitre, nous avons appris à mieux comprendre la structure et l'organisation du réseau de la RTC de Béjaia, et d'étudier notre problématique afin de proposer les solutions adéquates et les objectifs à atteindre.

Chapitre 3

Système de détection et prévention de l'intrusion informatique IDS/IPS

3.1 Introduction

Afin de détecter les attaques que peut subir un système, il est nécessaire de disposer d'un logiciel spécialisé dont le rôle est de surveiller les données qui transitent sur ce système et qui serait capable de réagir si des données semblent suspectes. En effet, dans ce chapitre nous allons présenter en première partie la Fonctionnement d'un pare-feu, ses types, en second partie, nous abordons le principe des systèmes de détections et prévention d'intrusion IDS/IPS, tout en énonçant leur types, leur architecture et leur fonctionnement, ainsi que les avantages et les inconvénients,et la dernier partier une petite présentation de SNORT.

3.2 Les firewalls

3.2.1 Définition

un firewalls est un élément du réseau informatique, logiciel et/ou matériel qui permet de protéger une machine ou un réseau quelconque et contrôle le trafic intérieur/extérieur qui le traverse, selon une politique d'accès aux ressources informatiques[14].

Il comporte au minimum deux interfaces réseau :

• Une interface pour le réseau à protéger (réseau interne).

•Une interface pour le réseau externe.

3.2.2 Différents types de filtrages

Essentiellement, il existe trois type de filtrage [15] :

3.2.2.1 Filtrage simple de paquet

C'est le filtrage sans état est la méthode de filtrage la plus simple, elle opère au niveau de la couche réseau et transport du modèle OSI. Il analyse les en-têtes de chaque paquet de données (datagramme) indépendamment des autres en se basant sur les règles prédéfinies par l'administrateur (généralement appelées ACL, Access Control List). Cela consiste à accorder ou refuser le passage de paquet d'un réseau à un autre en se basant sur l'adresse IP Source/Destination, le numéro de port Source/destination et le protocole de niveau 3 ou 4(type de paquet TCP, UDP, ICMP . . . etc.).

3.2.2.2 Filtrage dynamique

C'est le filtrage avec état, est une évolution des pare-feu sans états. L'amélioration est par rapport à la conservation de la trace des sessions et des connexions dans des tables d'états internes au Firewall pour appliquer les règles de filtrage. De cette manière, L'application des règles est alors possible sans lire les ACL à chaque fois, car l'ensemble des paquets appartenant à une connexion active seront acceptés.

3.2.2.3 Filtrage applicatif

(Aussi nommé pare-feu de type proxy ou passerelle applicative) fonctionne sur la couche 7 du modèle OSI et analyse le trafic échangé au niveau de cette couche. Cela suppose que le firewall connaisse l'ensemble des protocoles utilisés par chaque application. Chaque pro-

tocole dispose d'un module spécifique à celui-ci. C'est à dire que, par exemple, le protocole HTTP sera filtré par un processus proxy http.

3.2.3 Déférentes type de pare-feu

3.2.3.1 Pare-feu bridge

Agissent comme des câbles réseau avec la fonction de filtrage en plus, leurs interfaces ne possèdent pas d'adresse IP et ne font que transférer les paquets d'une interface à une autre en leur appliquant les règles prédéfinies. Cette absence d'adresse IP est particulièrement utile, car cela signifie que le pare-feu est indétectable pour un hacker.
En effet, quand une requête ARP est émise sur le câble réseau, le pare-feu ne répondra jamais. Ses adresses Mac ne circuleront jamais sur le réseau, et comme il ne fait que « transmettre » les paquets, il sera totalement invisible sur le réseau. Cela rend impossible toute attaque dirigée directement contre le pare-feu. Ces types de pare-feu se trouvent typiquement sur les switchs.

3.2.3.2 Pare-feu matériels

Est un périphérique physique installé entre un réseau informatique et Internet ou à la périphérie du réseau pour surveiller les paquets de données, possédant, au minium deux interfaces réseau, qui va analyser les données qui transitent par lui (tout trafic entrant et sortant par réseau passe à travers celui-ci avant d'atteindre des ordinateurs individuels), et vérifier si elles correspondent aux règles de politique de sécurité ou bien non comme par exemple de rejeter systématiquement toutes les requêtes provenant d'un domaine précis, ou bien toutes les requêtes utilisant un protocole spécifique, ou bien encore toutes celles relatives à tel ou tel numéro de port. Il est d'habitude intégré dans un router/modem.

3.2.3.3 Pare-feu logiciel

Est un programme qui peut être installés sur un ordinateur en le téléchargé directement à partir d'un site Web ou les charger à partir d'un CD ou d'un DVD. Il s'exécute sur un ordina-

teur local, et répondre aux besoins d'un utilisateur individuel (Hardware Firewall), mais en principe, il accomplit les mêmes tâches qu'un pare-feu matériel. Les pare-feu logiciel surveillent les paquets de données entrant et sortant par réseau et décident, selon des règles, s'il faut les bloquer ou autoriser. Nous pouvons les classer en deux catégories : les pare-feu personnels et les pare-feu plus sûr.

3.3 Système de détection d'intrusion IDS

3.3.1 Déffinition

Il s'agit d'un équipement permettant de surveiller l'activité d'un réseau ou d'un hôte donné, afin de détecter toute tentative d'intrusion. Un IDS est un système informatique, composé généralement de logiciel et éventuellement de matériel, dont le rôle est la détection d'intrusions. Il se contente plutôt d'analyser certaines informations en vue de détecter d'éventuelles activités malveillantes qu'il aura à notifier dans les plus brefs délais au responsable de la sécurité du système. C'est pour cette raison que la majorité des IDS opèrent en temps réel

3.3.2 Les différents types d'IDS

Les différents IDS se caractérisent par leur domaine de surveillance. Il existe trois grandes familles distinctes d'IDS[16] :

3.3.2.1 La détection d'intrusion basée sur l'hôte

L'HIDS (Host Based IDS) surveille le trafic sur une seule machine. Il analyse les journaux systèmes, les appels, et enfin vérifie l'intégrité des fichiers. Un HIDS a besoin d'un système sain pour vérifier l'intégrité des données. Si le système a étécompromis par un pirate, le HIDS ne sera plus efficace.

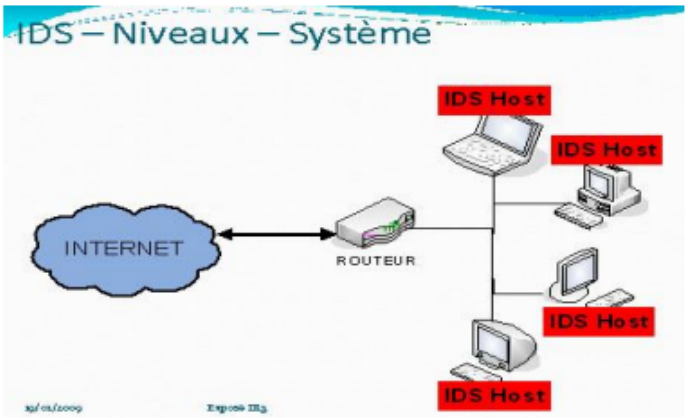


FIGURE 3.1 – Exemple de HIDS

3.3.2.2 La détection d'intrusion réseau NIDS

Les NIDS sont des IDS utilisés pour protéger un réseau. Ils comportent généralement une sonde (machine par exemple) qui écoute et surveille en temps réel tout le trafic réseau, puis analyse et génère des alertes s'il détecte des intrusions ou des paquets semblent dangereux.

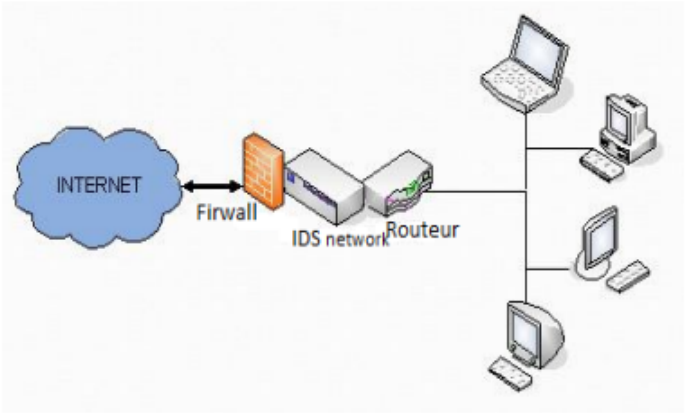


FIGURE 3.2 – Exemple de NIDS

3.3.2.3 Détection d'intrusion Hybride

IDS hybrides rassemblent les caractéristiques des NIDS et HIDS. Ils permettent, de surveiller le réseau et les terminaux. Les sondes sont placées en des points stratégiques, et agissent comme NIDS et/ou HIDS suivant leurs emplacements. Toutes ces sondes remontent alors les alertes à une machine qui va centraliser le tout, et lier les informations d'origines

multiples.

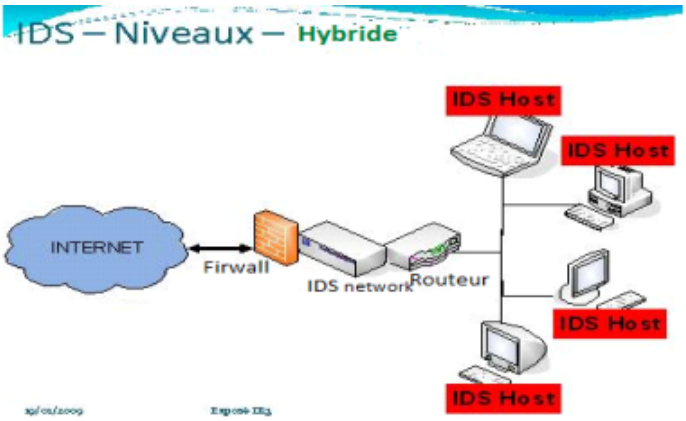


FIGURE 3.3 – Exemple d'Hybride

3.3.3 Architecture des IDS

Nous décrivons dans cette section les trois composants qui constituent classiquement un système de détection d'intrusion[17].

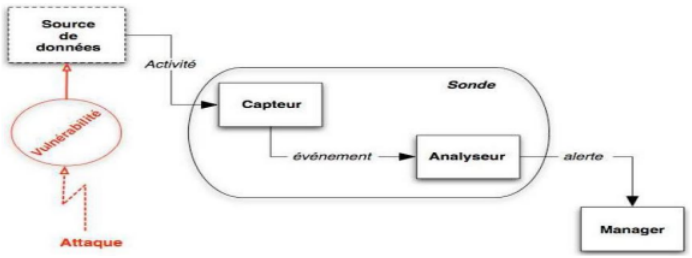


FIGURE 3.4 – architecture d'un IDS

• **Capteur :** Le capteur observe l'activité du système par le biais d'une source de donnée et fournit à l'analyseur une séquence d'événements qui renseignent de l'évolution de l'état du système. Le capteur peut se contenter de transmettre directement ces données brutes, mais en général un prétraitement est effectué. Et pour cela on distingue trois types de capteurs en fonction des sources de données utilisées pour observer l'activité du système : les capteurs système, les capteurs réseau et les capteurs applicatifs.

• **Analyseur :** L'objectif de l'analyseur est de déterminer si le flux d'événements fourni par le

capteur contient des éléments caractéristiques d'une activité malveillante.

• **Manager :** Le manager collecte les alertes produites par le capteur, les met en forme et les présente à l'administrateur. Éventuellement, le manager est chargé de la réaction à adopter qui peut être :

— Isolement de l'attaque, qui a pour but de limiter les effets de l'attaque.

— Suppression d'attaque, qui tente d'arrêter l'attaque.

— Recouvrement, qui est l'étape de restauration du système dans un état sain.

— Recouvrement, qui est l'étape de restauration du système dans un état sain.

3.3.4 Fonctionnement d'un IDS

3.3.4.1 Méthodes de détection des IDS

Il existe deux méthodes de détection :

• **Approche par scénario ou par signature :** Cette technique s'appuie sur les connaissances des techniques utilisées par les attaquants contenues dans la base de donnée, elle compare l'activité de l'utilisateur à partir de la base de donnée, ensuite elle déclenche une alerte lorsque des événements hors profil se produisent.

• **L'approche comportementale :** Cette technique consiste à détecter une intrusion en fonction du comportement de l'utilisateur ou d'une application, autrement dit c'est créer un modèle basé sur le comportement habituel du système et surveiller toute déviation de ce comportement.

3.3.4.2 Comportement après la détection d'intrusion

Il existe deux types de réponses, suivant les IDS utilisés. La réponse passive est disponible pour tous les IDS, la réponse active est plus ou moins implémentée.

• **Réponse passive :** Lorsqu'une attaque est détectée, le système d'intrusion ne prend aucune action, il génère seulement une alarme en direction de l'administrateur système sous

forme d'une alerte lisible qui contient les informations à propos de chaque attaque. Les réponses passives se traduisent la plupart du temps par des opérations de reconfiguration automatique d'un firewall afin de bloquer les adresses IP source impliquées dans les intrusions. Mais si le pirate prend une adresse IP sensible telle qu'un routeur d'accès ou un serveur DNS, l'entreprise qui implémente une reconfiguration systématique d'un firewall risque tout simplement de se couper du monde extérieur.

• **Réponse active :** La réponse active consiste à répondre directement à une attaque, elle implique des actions automatisées prises par un IDS qui permet de couper rapidement une connexion suspecte quand le système détecte une intrusion. Par exemple interrompre le progrès d'une attaque pour bloquer ensuite l'accès suivant de l'attaquant. Mais cella risque de se voir exposer à une contre attaque part le pirate.

3.3.5 Positionnement de l'IDS

Il existe trois endroits stratégiques où il convient de placer un IDS. Le schéma suivant illustre un réseau local ainsi que les trois positions que peut y prendre un IDS[18].

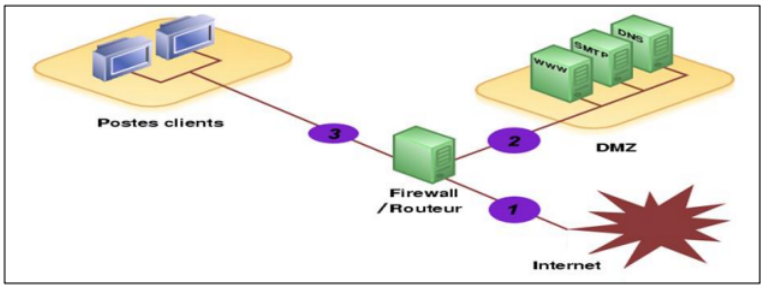


FIGURE 3.5 – Positionnement de L'IDS.

• **Position (1) :** Sur cette position, l'IDS va pouvoir détecter l'ensemble des attaques frontales, provenant de l'extérieur, en amont du firewall. Ainsi, beaucoup d'alertes seront remontées ce qui rendra les logs difficilement consultables.

• **Position (2) :** Si l'IDS est placé sur la DMZ, il détectera les attaques qui n'ont pas été filtrées par le firewall et qui relèvent d'un certain niveau de compétence. Les logs seront ici plus clairs à consulter puisque les attaques bénines ne seront pas recensées.

• **Position (3) :** L'IDS peut ici rendre compte des attaques internes, provenant du réseau local de l'entreprise. Il peut être judicieux d'en placer un à cet endroit étant donné le fait que 80 pour cente des attaques proviennent de l'intérieur.

3.3.6 Les avantages

— Détection et réponse en temps réel : l'emplacement des capteurs réseaux dans les endroits stratégiques permet de donner la réponse en temps réel, car les capteurs détectent les attaques puis il envoie un message d'alerte à l'administrateur réseau.

— Ils contient des outils de filtrage très intéressants qui nous permettent de faire du contrôle par protocole (ICMP, TCP, UDP), adresse IP, suivi de connexion.

— Les IDS détectent les intrusions et renvoient des alertes et notifications avec nombreuses informations détaillées (type supposé d'attaque, la source, la destination), tout cela permet une bonne compréhension sur les attaques.

3.3.7 Les inconvénients

— Les IDS basés sur une bibliothèque de signatures d'attaque connues, cette bibliothèque devra être mise à jour à chaque nouvelle attaque sera affichées. Si l'attaque ne contient pas la signature d'une attaque spécifique et récente, cette dernière passera au travers des mailles du filet et la sécurité des données et le réseau en général sera menacé

— L'intervention humaine est toujours indispensable, pour prendre les décisions critiques et finales.

— La faiblesse d'un IDS est liée à la faiblesse de la plate-forme.

— Une saturation de la mémoire, de la carte réseau, ou du processeur porte atteinte directement au bon fonctionnement de tout le système.

3.4 Système de prévention d'intrusion

3.4.1 Définition

L'IPS est un outil de protection et sécurité des systèmes d'information contre les intrusions, similaire aux IDS, permettant de prendre des mesures afin de diminuer les impacts d'une attaque. C'est un IDS actif, il empêche toute activité suspecte détectée au sein d'un système.

3.4.2 Types de L'IPS

3.4.2.1 La détection d'intrusion basée sur l'hôte HIPS

Les HIPS sont des IPS permettant de surveiller le poste de travail à travers différentes techniques, ils surveillent les processus, les drivers... etc. En cas de détection de processus suspect, le HIPS peut le tuer pour mettre fin à ses agissements .

3.4.2.2 La prévention d'intrusion basée sur le NIPS

Le NIPS permet de surveiller le trafic réseau, identification et blocage du trafic malicieux, et parfois utilisé pour évoquer la protection des réseaux sans-fil.

3.4.3 Architecture foncionnelle d'un IPS

Le fonctionnement d'un IPS est similaire à celui d'un IDS. Il capture le trafic du réseau puis l'analyse. Mais au lieu d'alerter l'utilisateur d'une intrusion ou d'une attaque, l'IPS bloque directement les intrusions en supprimant les paquets illégitimes. Pour informer l'utilisateur, l'IPS peut aussi remplir un fichier de journalisation qui contiendra la liste des paquets supprimés et éventuellement un message indiquant la raison de cette suppression

3.4.4 Les avantages

— Cette approche fait interagir des technologies hétérogènes : pare-feu, VPN, IDS, anti-virus, anti-spam, etc.

— La liberté de création des règles pour les actions à exécuter.

— La plupart des logiciels IPS sont multi-plateforme (Linux, FreeBSD, Windows ... etc.).

— Un dispositif simple peut analyser le trafic pour une grande échelle des centres serveurs sur le réseau, qui fait au NIPS une bonne solution qui diminue le coût d'entretien et de déploiement.

— Empêche la transmission des paquets en fonction de ses règles tous comme un pare-feu bloque le trafic en se basant sur les adresses IP.

3.4.5 Les inconvénients

— Ils bloquent toute activité qui lui semble suspecte, mais n'étant pas fiable à 100 ils peuvent donc bloquer incorrectement des applications ou des trafics légitimes.

— Ils laissent parfois passer certaines attaques sans les repérer, et permettent donc aux pirates d'attaquer un PC.

— Ils sont peu discrets et peuvent être découverts lors de l'attaque d'un pirate une fois qu'il aura découvert l'IPS s'empressera de trouver une faille dans ce dernier pour le détourner et arriver à son but.

3.4.6 Différence entre IPS et IDS

la différence principale entre IDS et IPS est que IDS fonctionne comme un système de surveillance et de détection tandis qu'IPS fonctionne comme un système de prévention en dehors de la surveillance et de la détection. Certaines différences sont :

• **Réponse :** Les solutions IDS sont des systèmes de sécurité passifs qui surveillent et détectent uniquement les réseaux pour les activités malveillantes. Ils peuvent vous alerter mais

ne prennent aucune mesure par eux-mêmes pour empêcher l'attaque. L'administrateur du réseau ou le personnel de sécurité affecté doit prendre des mesures immédiatement pour atténuer l'attaque. D'autre part, les solutions IPS sont des systèmes de sécurité actifs qui surveillent et détectent votre réseau pour les activités malveillantes, alertent et empêchent automatiquement l'attaque de se produire.

• **placement :** l'IDS est placé à la périphérie d'un réseau pour collecter tous les événements, enregistrer et détecter les violations. Ce positionnement donne à l'IDS une visibilité maximale pour les paquets de données. Le logiciel IPS est placé derrière le pare-feu du réseau et communique en ligne avec le trafic entrant pour mieux prévenir les intrusions.

• **Mécanisme de détection :** IDS utilise la détection basée sur les signatures, la détection basée sur les anomalies pour les activités malveillantes. Sa détection basée sur les signatures n'inclut que les signatures face aux exploits. D'autre part, IPS utilise une détection basée sur les signatures avec des signatures orientées exploit et vulnérabilité. En outre, IPS utilise une détection statistique basée sur les anomalies et une détection d'analyse de protocole avec état.

• **risques digitaux :**Si vous êtes menacé, l'IDS pourrait être moins utile car votre personnel de sécurité doit trouver comment sécuriser votre réseau et nettoyer le système ou le réseau immédiatement. IPS peut effectuer une prévention automatique par lui-même.

• **Faux positifs :** Si IDS donne un faux positif, vous pouvez trouver une certaine commodité. Mais si IPS le fait, l'ensemble du réseau en souffrira car vous devrez bloquer tout le trafic - entrant et sortant du réseau.

3.5 SNORT

3.5.1 Définition

SNORT est un système de détection d'intrusions réseau en open source, capable d'effectuer une analyse du trafic réseau en temps réel et doté de différentes technologies de

détection d'intrusions telle que l'analyse protocolaire. SNORT peut détecter de nombreux types d'attaques, comme :les scans de ports, etc.

3.5.2 Architecture de SNORT

L'architecture de SNORT est modulaire elle est composée de[20] :

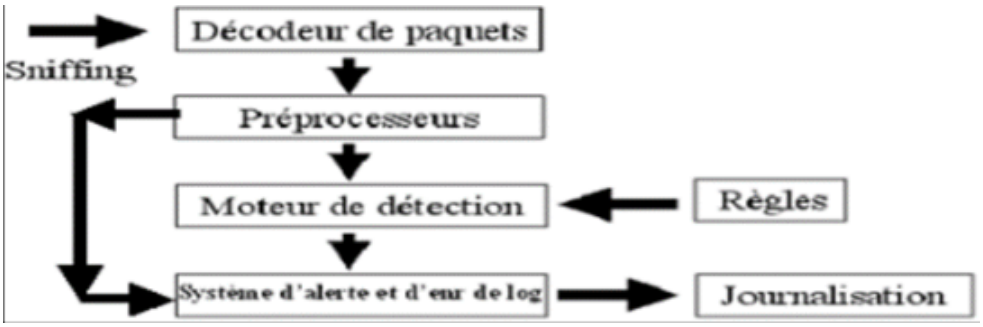


FIGURE 3.6 – Architecture de SNORT

• **Décodeur de paquet (Packet Decoder) :** il capture les paquets de données des interfaces réseaux, les prépare afin d'être prétraitées ou envoyées au moteur de détection.

• **Pré processeur (Pre processor) :** ce sont des composants utilisés avec SNORT afin d'améliorer les possibilités d'analyse, et de recomposition du trafic capturé. Ils reçoivent les paquets, les retraitent et les envoient au moteur de détection.

•**Moteur de détection (Detection Engine) :** c'est le composant le plus important de SNORT. Son rôle consiste à détecter les éventuelles intrusions qui existent dans un paquet. Pour se faire, le moteur de recherche se base sur les règles de SNORT. En effet, ce moteur consulte ces règles et les compare une à une avec le paquet de données. S'il y a conformité, le détecteur l'enregistre dans le fichier log et/ou génère une alerte. Sinon le paquet est laissé tomber.

• **Système d'alerte et d'enregistrement des logs (Logging and Alerting System) :** il permet de générer les alertes et les messages log suivant ce que le moteur de détection a trouvé dans le paquet analysé.

3.5.3 Mode de fonctionnement de SNORT

SNORT permet d'analyser le trafic réseau de type IP, il peut être configuré pour fonctionner en trois modes [25] :

• **mode sniffer :**Dans ce mode, SNORT lit les paquets circulant sur le réseau et les affiche d'une façon continue sur l'écran.

• **Le mode "Packet logger" :** Ci SNORT journalise le trafic réseau dans des répertoires sur le disque à savoir le fichier de log (/var/log/snort/).

• **Le mode détecteur d'intrusions réseau (NIDS) :** Est là, SNORT analyse le trafic du réseau, le compare à des règles déjà définie par l'utilisateur et établit des actions à exécuter.

• **Le mode prévention des intrusions réseau (IPS) :** C'est "SNORT-Inline" ;décide du comportement du Pare-feu ; bloquer ou laisser passer des paquets.

3.5.4 Raison de choix du Snort

Nous avons opté le logiciel SNORT pour les raisons suivantes :

— C'est un logiciel libre (open source) et qu'il est beaucoup utilisé dans les entreprises.

— Il est capable d'effectuer une analyse en temps réel et du trafic entrant et sortant.

— Il est disponible pour la plupart des systèmes d'exploitation (Windows et linux comme Ubuntu, Debian, CentOS).

— Les mises à jour des règles sont gratuites.

— La détection et la notification des attaques sont déjà connues.

— Possède une base de signatures qui va être mise à jour quotidiennement, via ses règles.

3.6 Conclusion

Dans ce chapitre, nous avons présenté les concepts de détection des intrusions, leurs architectures et leur fonctionnement. ils complètent les taches des autres équipements de sécurité comme les pare-feux ...etc.

le chapitre suivant nos renseigne comment réussir la configuration, après installation, du système de détection d'intrusion afin de mieux sécuriser le réseau, Nous allons montrer également un test permettant la confermation les bonnes installation et configuration de notre systéme.

Chapitre 4

Test et mise en œuvre de la solution

4.1 Introduction

Dans ce chapitre nous présentons notre projet avec ces architecture et son environnement de travail et différente configurations de base de réseaux .
En plus de ça nous donnons les techniques de sécurisation convenable à chaque type d'attaque que nous testons.

4.2 Présentation de l'environnement

4.2.1 Simulateur graphique de réseau(GNS3)

GNS3 signifie (Graphical Network Simulator), est un simulateur graphique de réseau qui permet l'émulation de réseaux complexes. Il est utilisé pour reproduire différents systèmes d'exploitation dans un environnement virtuel. Il permet l'émulation en exécutant un IOS Cisco (Internetwork Operating Systems) [21].

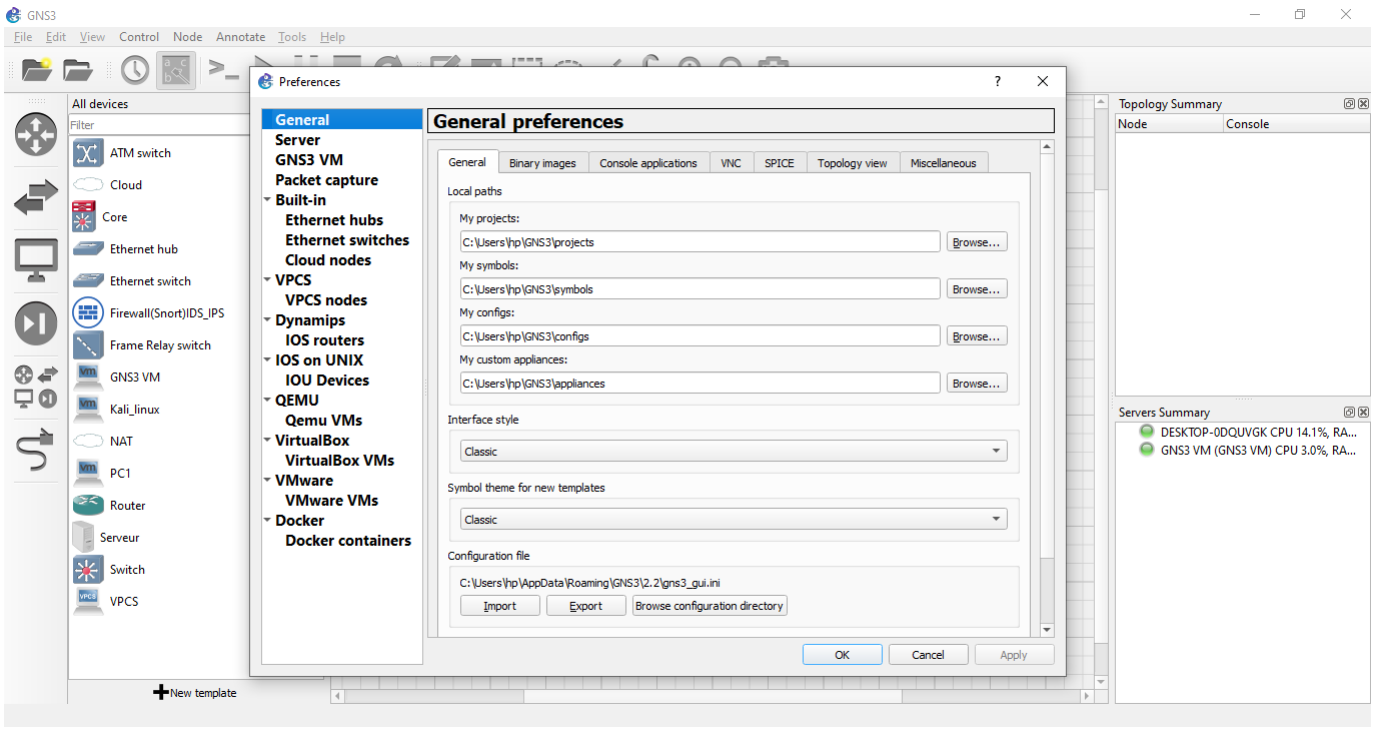


FIGURE 4.1 – GNS3 Graphical Network Simulator version 2.2.32

4.2.2 VMware Workstation

C'est la version station de travail du logiciel. Il permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation (généralement Windows ou Linux), ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique (machine existant réellement). Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspondant aux performances de l'ordinateur hôte. [22].

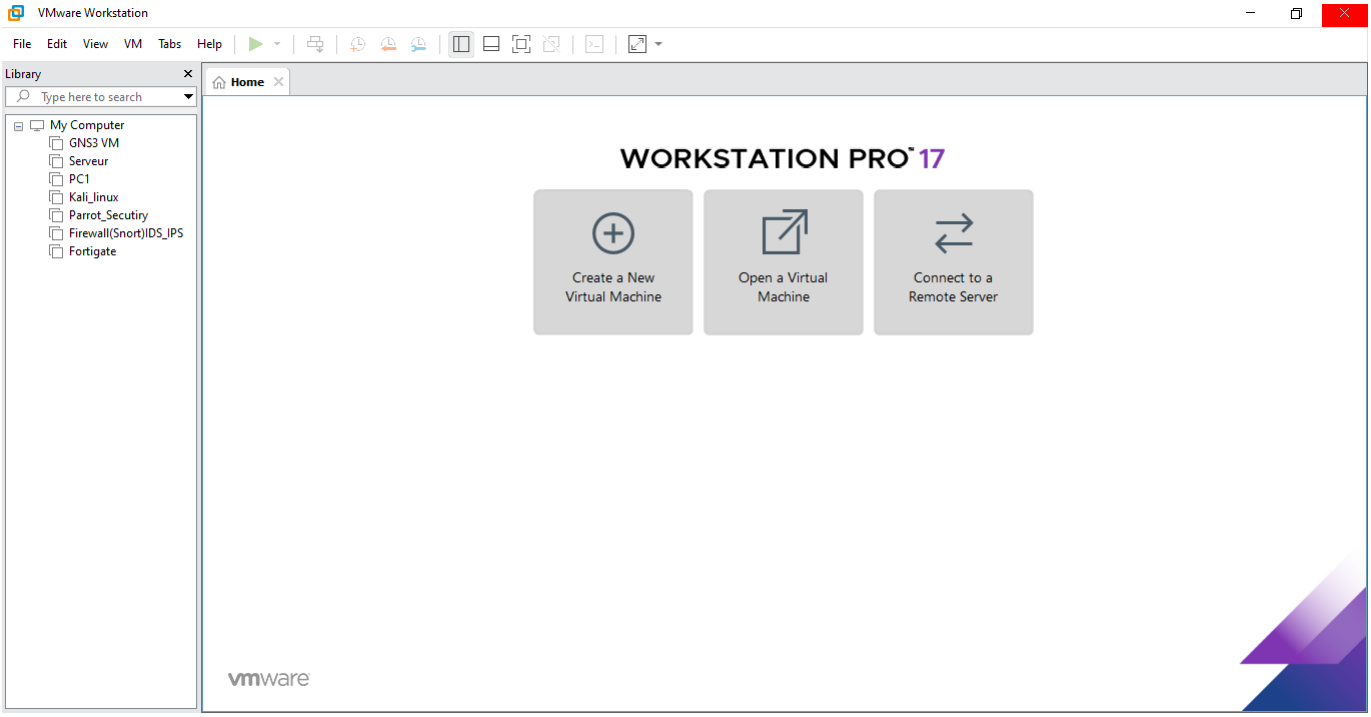


FIGURE 4.2 – VMware workstation 17.0 professionnel

4.2.3 Pfsense

PfSense est libre, une distribution personnalisée de FreeBSD adapté pour être utilisé comme routeur et pare-feu. En plus d'être une plate-forme puissante, flexible de routage et de pare-feu, il comprend une longue liste de caractéristiques connexes et un système de package permettant en outre l'évolutivité sans ajouter de ballonnement et de failles de sécurité potentielles à la distribution de base. Pfpense est un projet populaire avec plus de 1 million de téléchargements depuis sa création et approuvé dans d'innombrables installations allant des petits réseaux domestiques pour protéger un ordinateur unique, pour les grandes entreprises, les universités et d'autres organisations protégant des milliers de périphériques réseau [23].

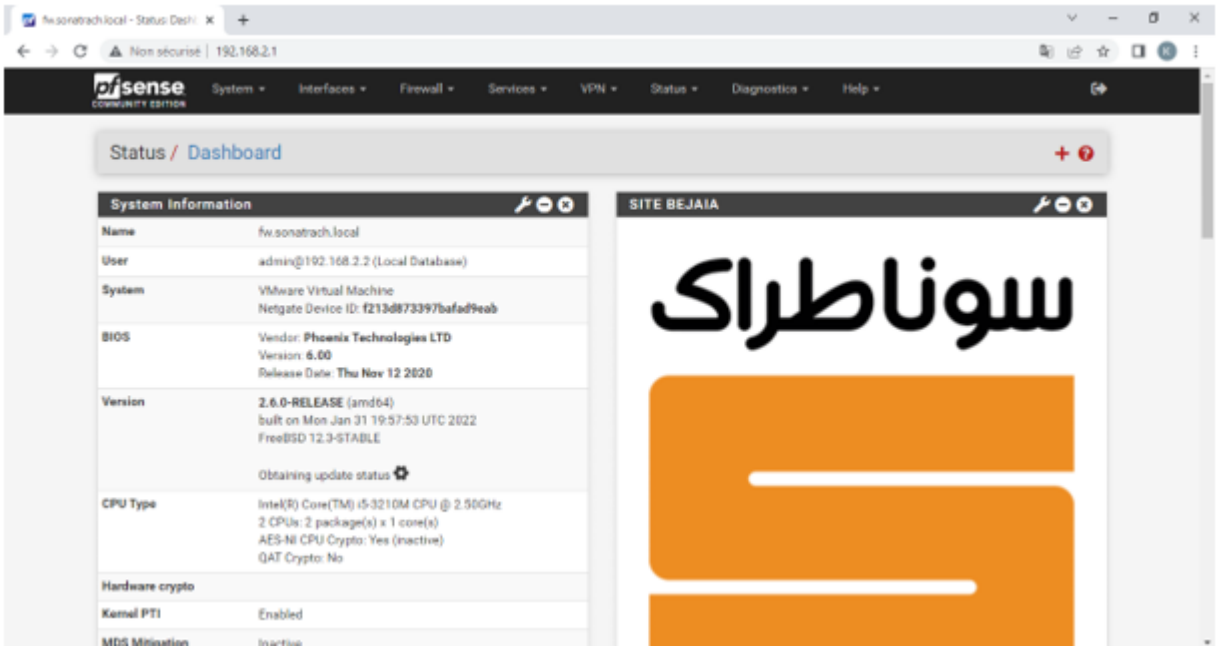


FIGURE 4.3 – Pfsense 6.0.0

pfSense ne fait pas seulement firewall, il offre toute une panoplie de services réseaux. Voici une partie qui semble interessante :

— Pare-feu : indispensable pour une distribution "firewall".

— Table d'état : La table d'état ("State Table") contient les informations sur les connexions réseaux. Cela permet d'avoir un aperçu des connexions et surtout de créer des régles par exemple sur le nombre de connexion maximum pour un hôte.

— Traduction d'adresses réseaux (NAT).

— VPN : permet la création de VPN IpSec, OpenVPN ou PPTP.

— Serveur DHCP.

— Serveur DNS et DNS dynamiques.

— Portail Captif.

— Proxy et Blacklist SQUIDGUARD.

— Gestion des VLAN.

— IDS-IPS SNORT.

4.2.4 Package SNORT

Snort est un système de détection d'intrusion de réseau open source (NIDS) créé par Martin Roesch. Snort est un sniffer de paquets qui surveille le trafic réseau en temps réel, scrutant chaque paquet de manière étroite pour détecter une charge utile dangereuse ou des anomalies suspectes. Snort est basé sur libpcap (pour la capture de paquets de bibliothèque), un outil largement utilisé dans les sniffers et les analyseurs de trafic TCP / IP. Grâce à l'analyse du protocole et à la recherche de contenu, Snort détecte les méthodes d'attaque, y compris le déni de service, le dépassement de tampon, les attaques CGI, les balayages de port furtif et les sondes SMB. Lorsque des comportements suspects sont détectés, Snort envoie une alerte en temps réel à syslog, à un fichier d'alertes distinct ou à une fenêtre contextuelle [24].

4.2.5 Kali linux

Kali Linux est une distribution Linux basée sur Debian largement utilisée par les professionnels de la sécurité, les testeurs d'intrusion et les hackers éthiques. C'est un système d'exploitation libre et open-source qui est spécialement conçu pour la forensique numérique, les tests d'intrusion et l'audit de sécurité.
L'objectif de Kali Linux est de fournir une distribution regroupant l'ensemble des outils nécessaires aux tests de sécurité d'un système d'information, notamment le test d'intrusion.

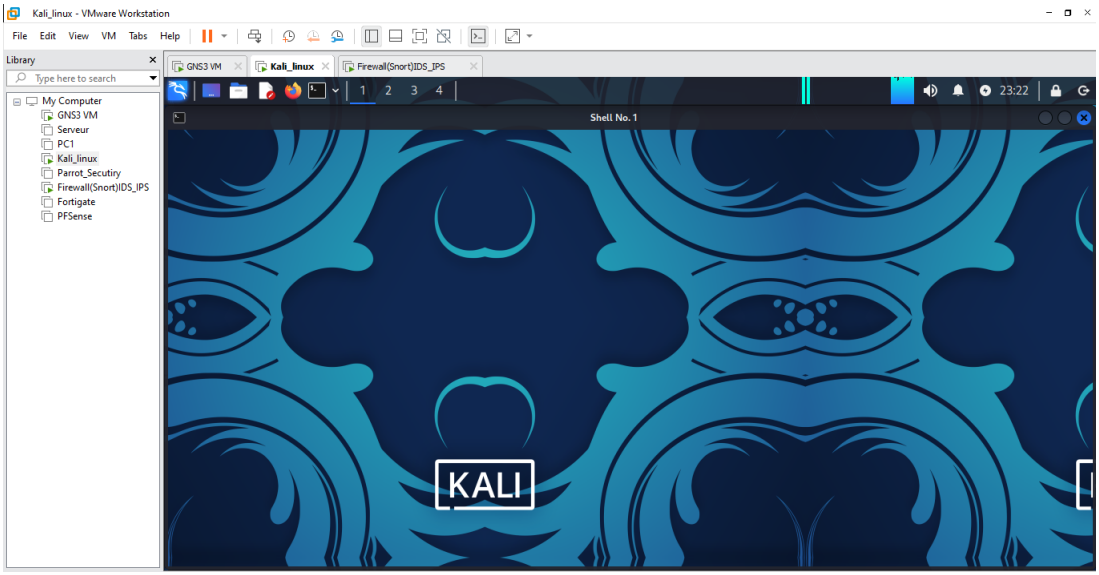


FIGURE 4.4 – Kali linux.

4.2.6 Nmap

Nmap a été conçu pour détecter en scannant les portes ouvertes sur le réseau et obtenir des informations sur l'OS d'un systéme distant, il utlise plusieurs protocoles pour générer un audit de sécurité.

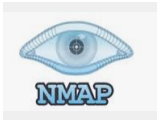


FIGURE 4.5 – Nmap.

4.2.7 La topologie de simulation

Afin de réaliser ce test, nous avons utilisé la topologie visible sur la figure 4.6 :

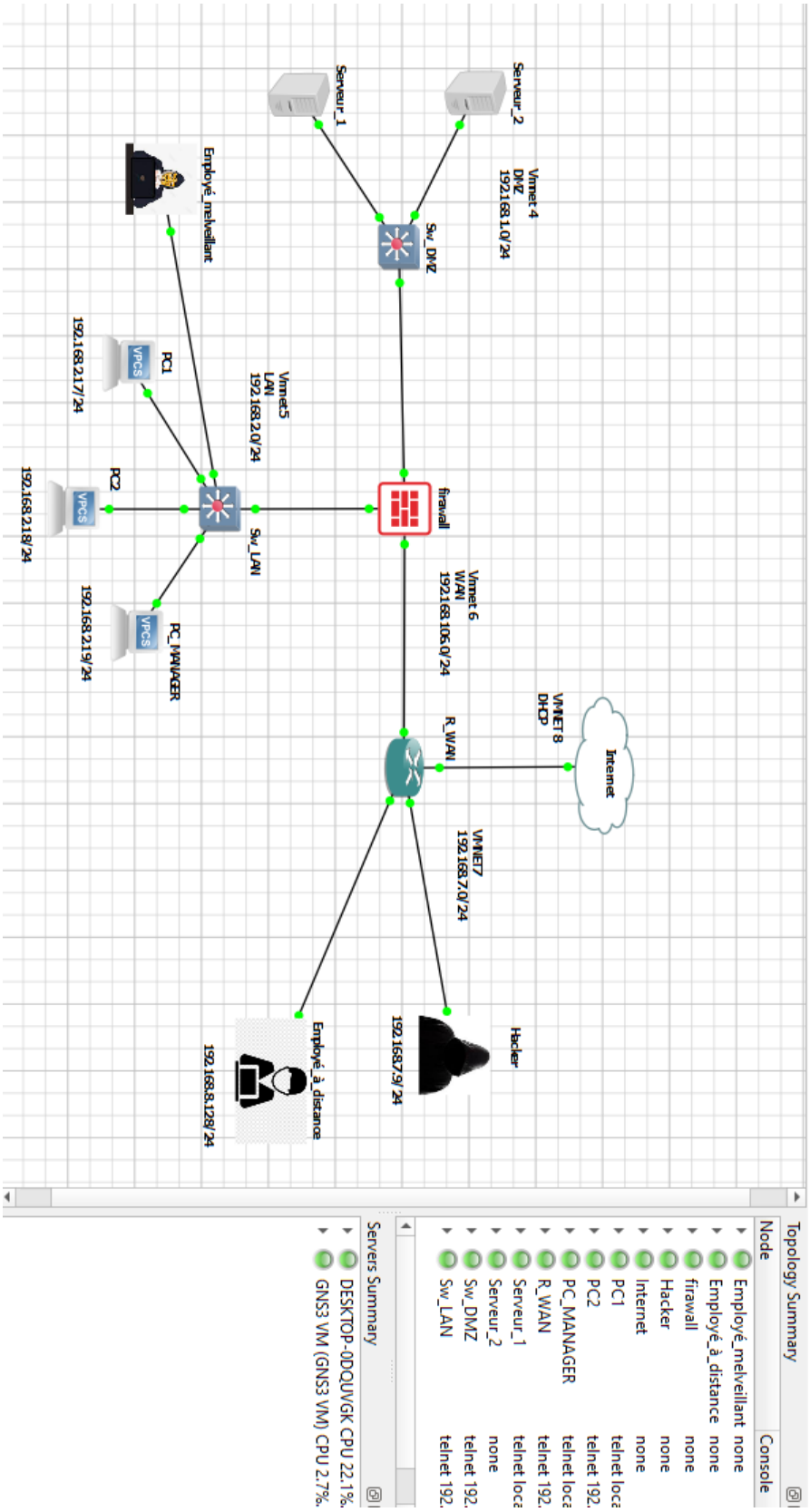


FIGURE 4.6 – La topologie utilisée.

- La table d'adressage suivi dans ce projet :

Sous réseau	Adresse de sous réseau	Mask	Adresse de Diffusion	Passerelle
WAN	192.168.106.0	/24	192.168.106.255	192.168.106.2
LAN	192.168.2.0	/24	192.168.2.255	/
DMZ	192.168.1.0	/24	192.168.1.255	/
Attaquant externe	192.168.7.0	/24	192.168.7.255	192.168.7.1

TABLE 4.1 – Un tableau simple dans le second chapitre.

- La configuration les interface d'un routeur :

```
R1#show ip interface brief
Interface                  IP-Address      OK? Method Status
    Protocol
Ethernet0/0                192.168.106.2   YES NVRAM  up
    up
Ethernet0/1                192.168.7.1     YES NVRAM  up
    up
Ethernet0/2                192.168.3.131   YES DHCP   up
    up
```

FIGURE 4.7 – La configuration les interface d'un routeur

4.3 Configuration du pare-feu

4.3.1 Installation de pfsense

Pour commencer, il faut disposer d'une image iso de Pfsense version 2.6.0 Basé sur FreeBSD, cette image est disponible sur https ://Pfsense.org/dowlnload. On utilise une machine virtuelle disposant de cartes réseaux une reliée au réseau local et l'autre branchée au réseau WAN et une treizième pour la zone DMZ. Cette capture montre l'ajout des deux cartes réseaux que nous allons utiliser.

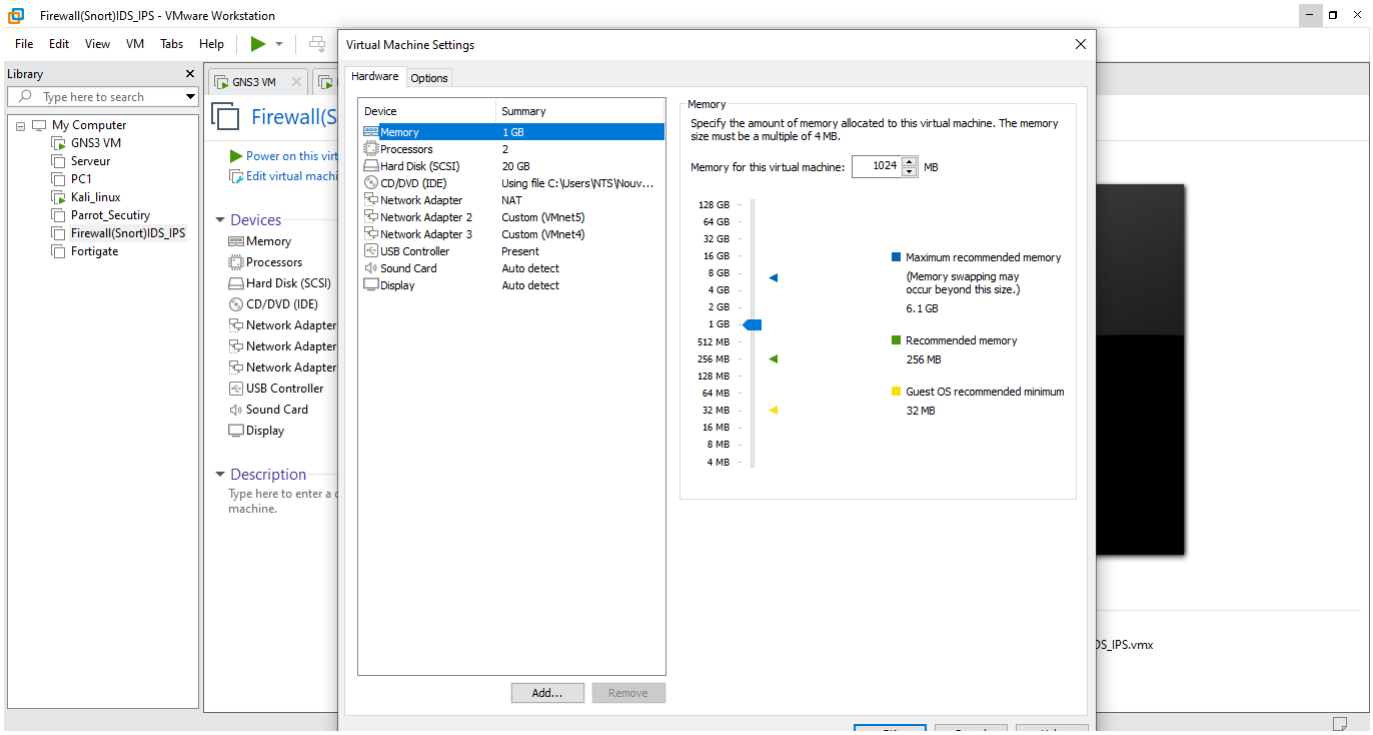
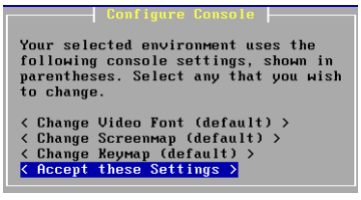
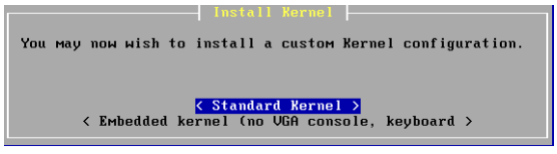
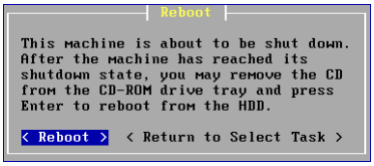


FIGURE 4.8 – Configuration des cartes réseau de pfsense

Pour aboutir à une installation complète et correcte de pfsense suivre les étapes dans les trois prochaines captures.







4.3.2 Configuration des interfaces

Une fois l'installation terminée, nous allons maintenant configurer les interfaces, en choisissant l'option 2 puis les numéros correspondants a l'interfaces souhaiter configurer, par exemple pour l'interface LAN c'est le numéro 2, on affecte une adresse IP et un masque sous réseau ,Et pour l'interface WAN c'est le numéro 1, on affecte une adresse IP et un masque sous réseau .

Une fois la configuration est terminée au aura cet affichage pour Pfsense :

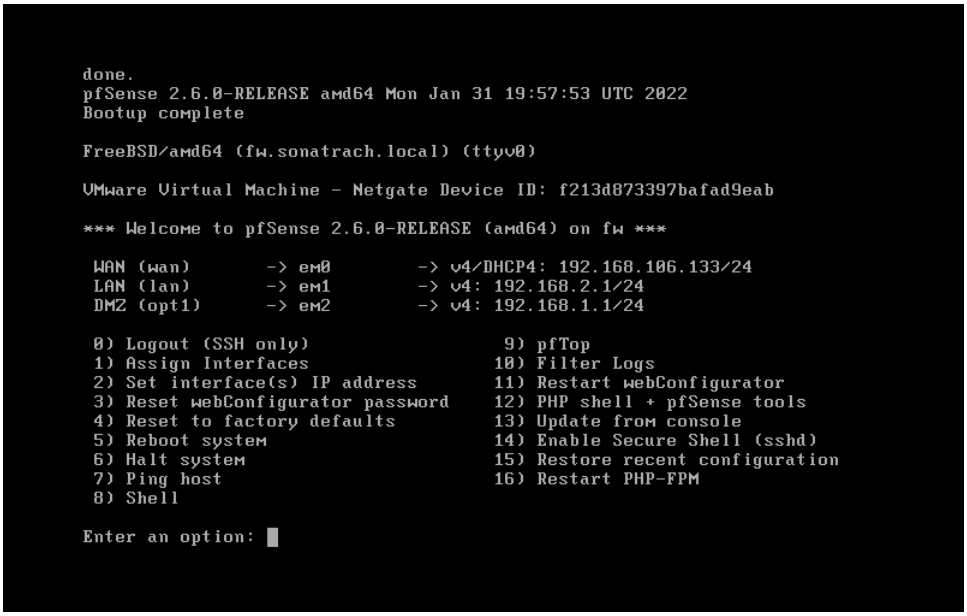


FIGURE 4.9 – Pfsense SONATRACH l'installation terminée.

• Les adresses IP des interfaces sont attribuées statiquement par le choix de l'option 2.

• Pour se connecter à l'interface web de configuration de Pfsense on utilise l'adresse IP de l'interface LAN : https ://192.168.2.1

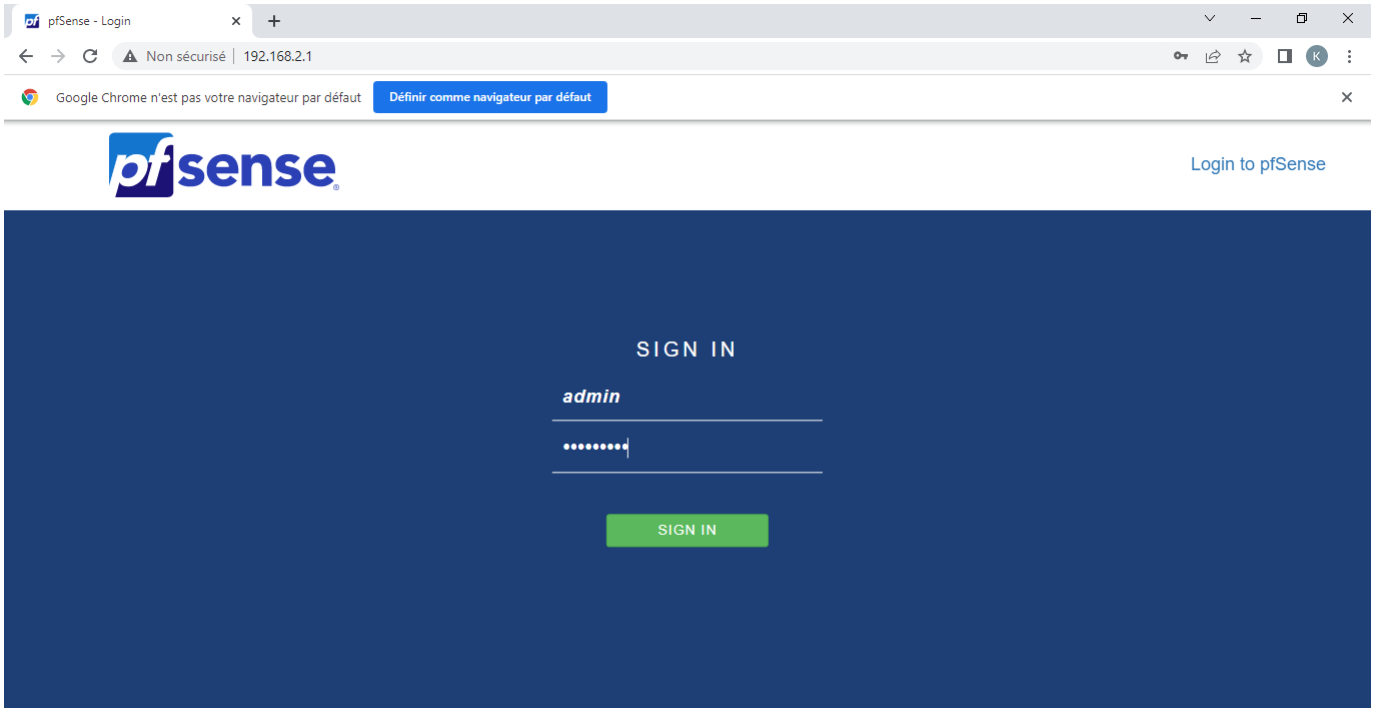


FIGURE 4.10 – Page d'authentification de Pfsense.

- Le couple «Username/Password» par défaut est «admin/pfsense».

Cette étape quand en rentre pour la première fois dans Pfsense, après on peut changer le mot de passe.

- Pour activer l'interface WAN où bien l'interface DMZ, on doit accéder à : interfaces/ WAN/ (interfaces/DMZ/), et on coche la case "enable interface".

l'interface LAN est activée par défaut.

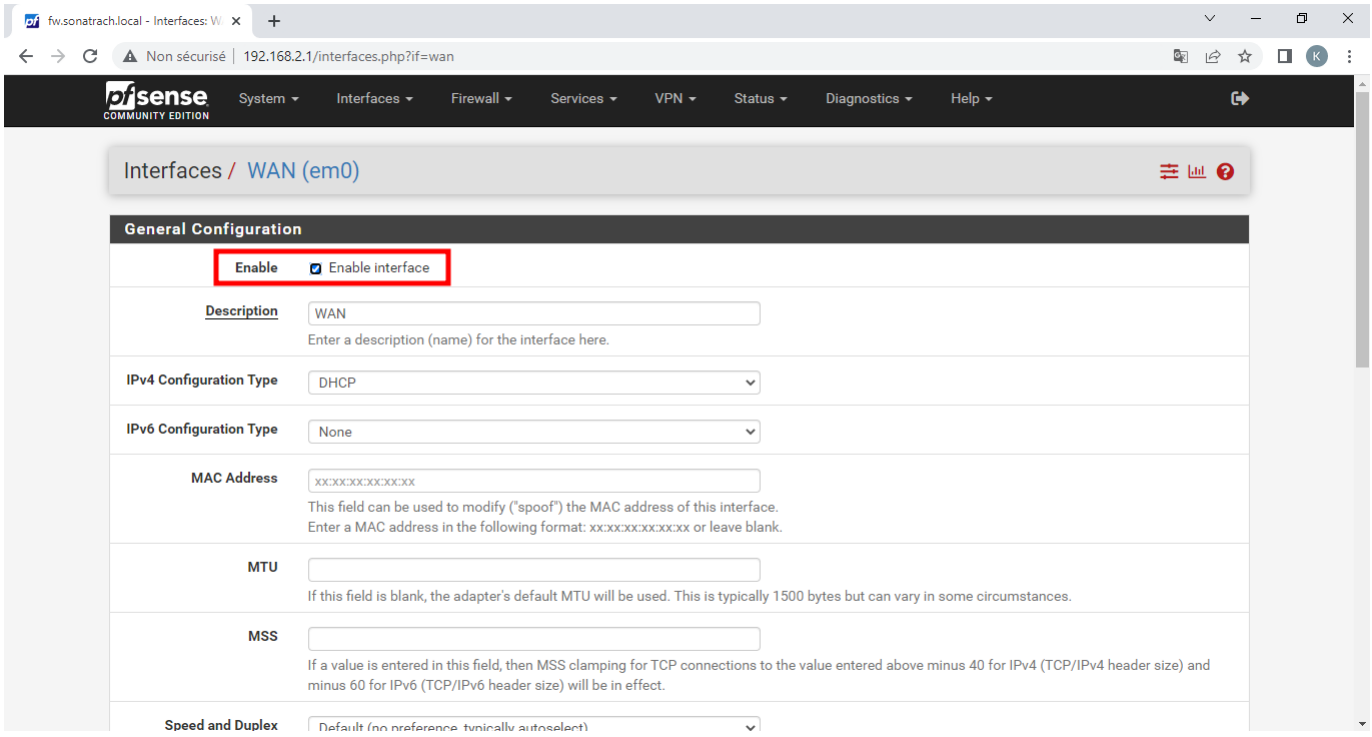


FIGURE 4.11 – L'activation de l'interface WAN.

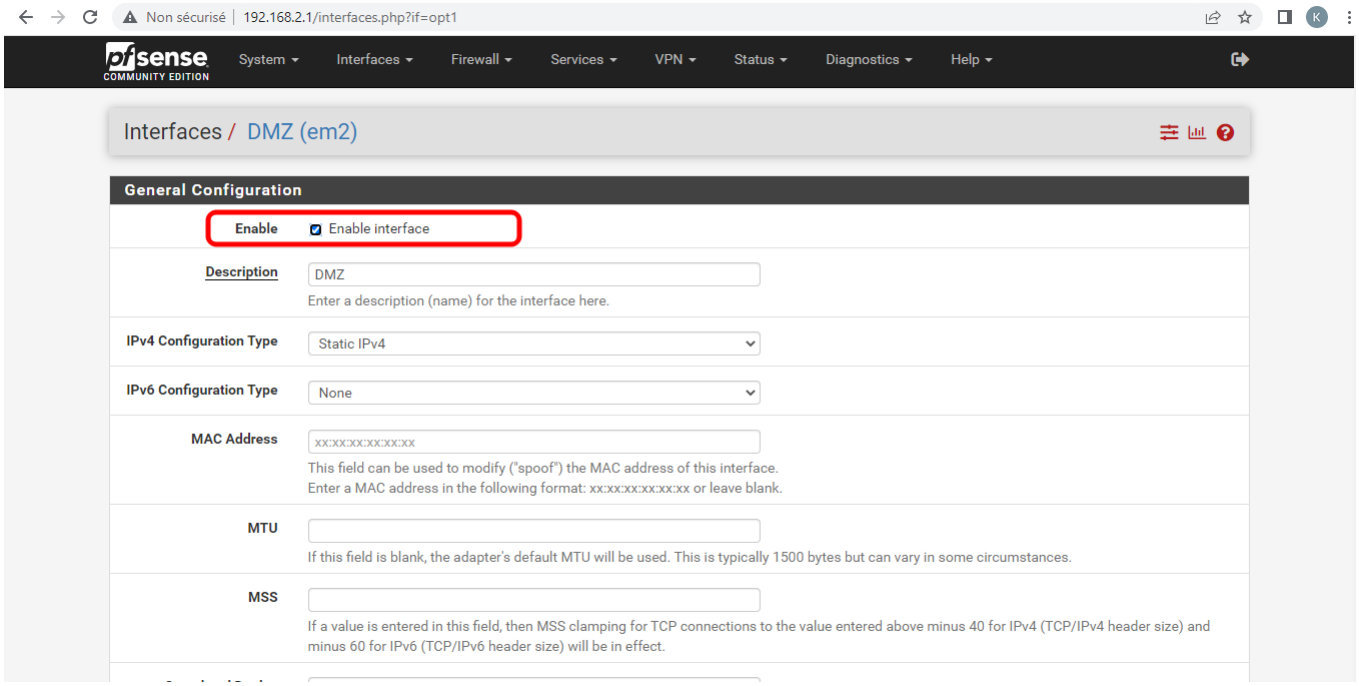


FIGURE 4.12 – L'activation de l'interface DMZ.

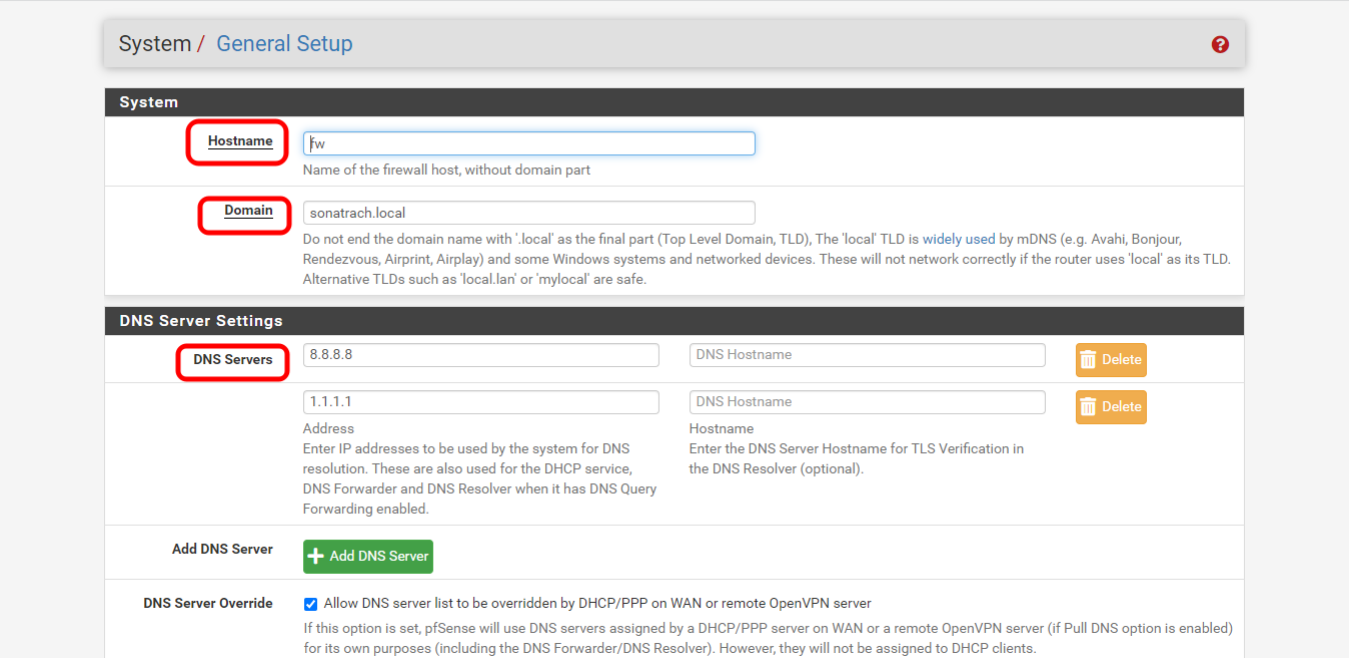
• Après l'activation on va passer à la configuration générale du serveur Pfsense :

— Hostname : le nom d'Host (fw).

— Domain : le domaine si c'est déjà établi, sinon on laisse le choix par défaut.

— Primary (Secondary) DNS Server : l'adresse primaire (secondaire) du serveur DNS à utiliser (on a utilisé ici les serveurs DNS de Google : 8.8.8.8 et 1.1.1.1).

— Timeservers : Ici on déclare le serveur d'horloge avec lequel on doit se synchroniser, par défaut c'est 0.pfsence.pool.ntp.org (on le laisse par défaut).



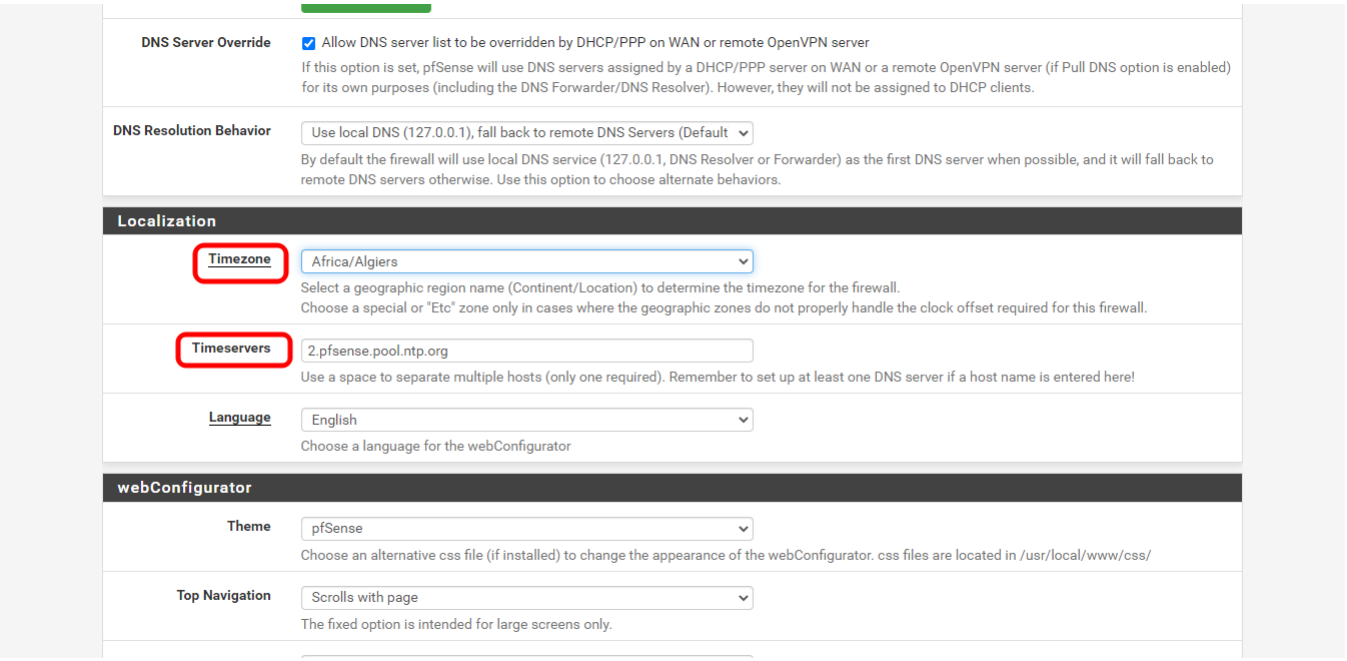


FIGURE 4.13 – L'interface web pour la configuration générale du serveur Pfsense.

• Nous avons configuré un serveur protocole contrôle dynamique des hôtes(DHCP) pour gérer l'allocation des adresses IP via Pfsense, lui permettant ainsi de s'intégrer à l'ensemble de ses hôtes. pour le faire, nous allons dans services/ DHCP server/LAN puis on coche la case « enable » et on ajoute : l'adresse réseau local dans (subnet), le masque sous réseau dans (subnet mask), puis le pool d'adresses duquel le DHCP tire les adresses pour les affecter aux hôtes .

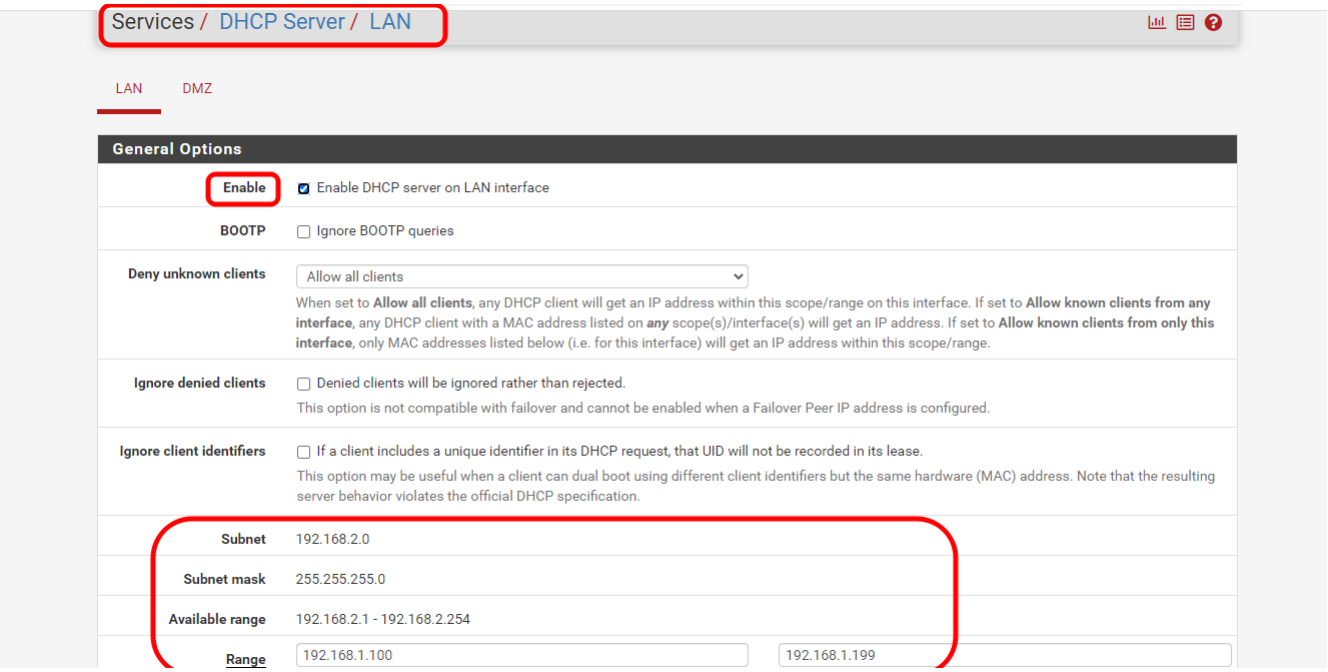


FIGURE 4.14 – configuration du protocole DHCP des hôtes.

4.3.3 Règles de filtrage du Pfsense

Une fois le réseau est prêt on passe à la configuration des règles du pare-feu car c'est la plus importante étape. Tout d'abord on accède à l'interface web de Pfsense avec l'adresse 192.168.2.1 puis nous allons dans : System/Rules. On commence à mettre en place les règles de filtrage propre pour chaque interface du pare-feu, donc chaque règle appliquée sur une des trois interfaces s'applique aussi sur l'ensemble du réseau local relié à cette interface. Un système pare-feu contient un ensemble de règles prédéfinies permettant D'autoriser (allow), de bloquer la connexion (deny) et de rejeter la demande de connexion sans avertir l'émetteur (drop).

Ces règles de filtrages nous aident beaucoup pour la sécurisation de notre réseau local contre les intrusions distante en filtrant toutes les flux de communication.

• **Interface LAN :** la figure suivante nous montre la liste des règles associée à l'interface LAN.

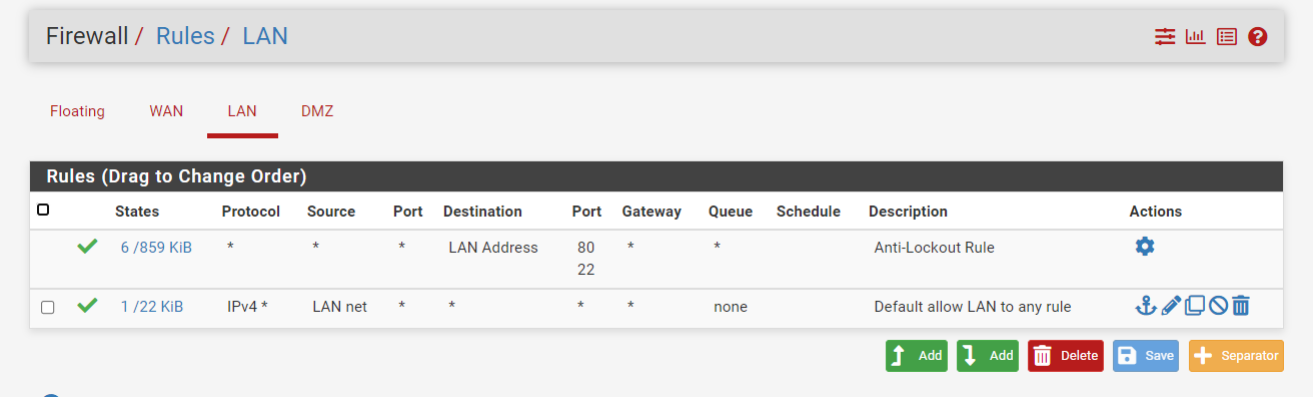


FIGURE 4.15 – La liste des règles associées à l'interface LAN.

On remarque que dans la figure il existe deux règles pour l'interface LAN :

— La 1ère règle : Autoriser n'importe quelle flux d'accéder au LAN .

— la 2 ème règle : Autoriser le LAN d'accéder à tous les réseaux.

• **Interface WAN :** la figure suivante nous montre la liste des règles associée à l'interface WAN.

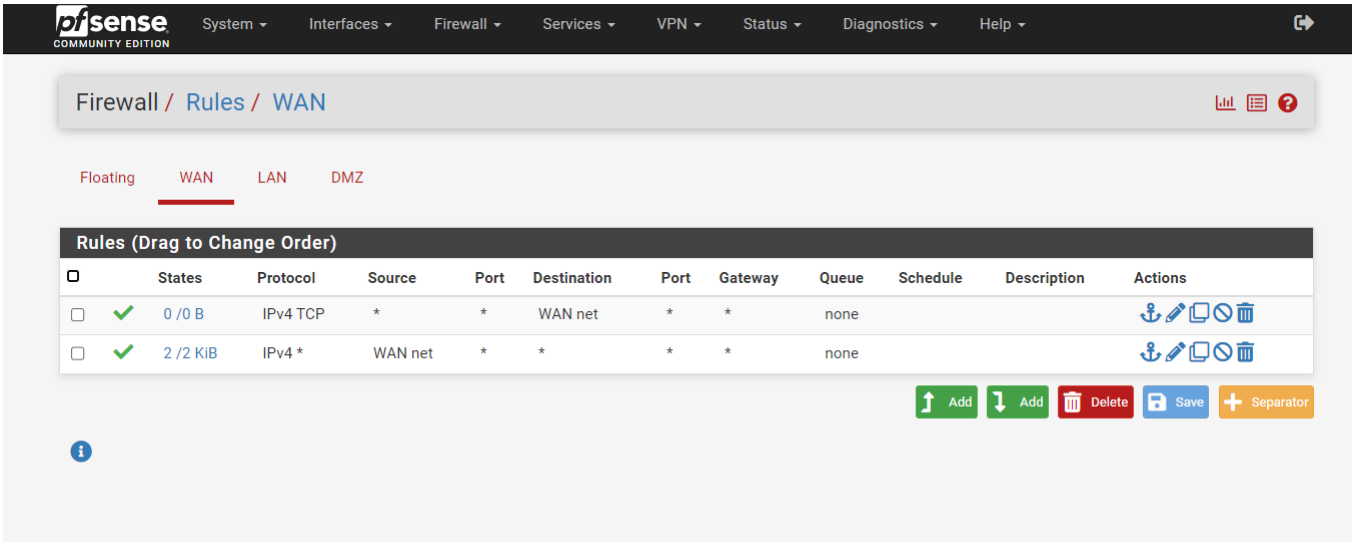


FIGURE 4.16 – La liste des règles associées à l'interface WAN.

On remarque que dans la figure il existe deux règles pour l'interface WAN :

— La 1ère règle : Autoriser n'importe quelle flux d'accéder au WAN.

— la 2 ème règle : Afin d'autoriser le flux sortant du WAN d'accéder à tous les réseaux.

• **Interface DMZ :** la figure suivante nous montre la liste des règles associée à l'interface DMZ.

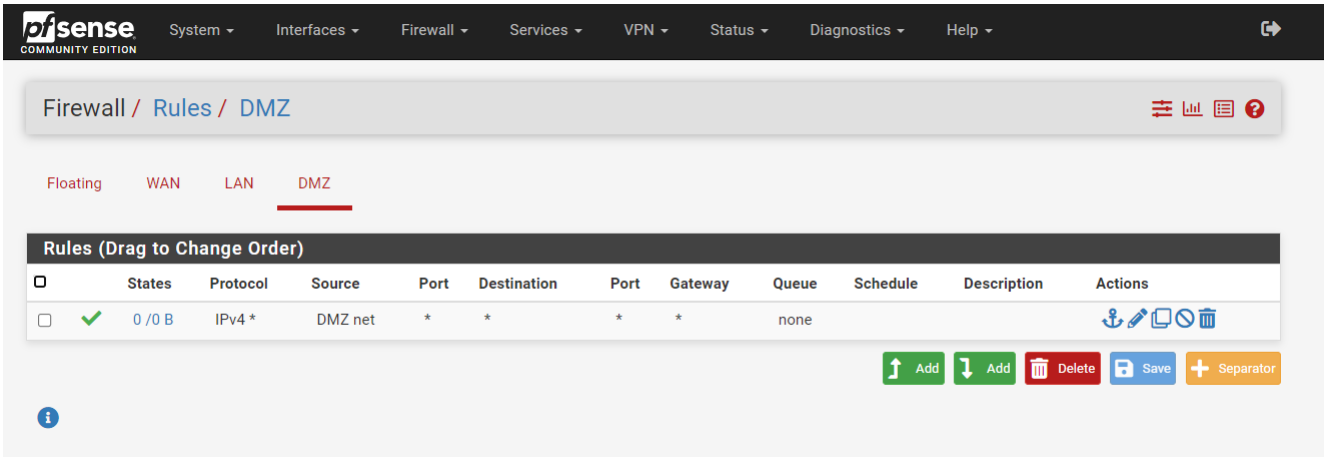


FIGURE 4.17 – La liste des règles associées à l'interface DMZ.

On remarque que dans la figure il existe une seul règle pour l'interface DMZ :

— La 1ère règle : Autoriser la DMZ d'accéder à tous les réseaux.

4.4 Configuration du SNORT

4.4.1 Installation du package SNORT

Pour installer le package SNORT, nous allons dans : System/ Package Manager/Available Packages, on cherche SNORT puis on clique sur installer.

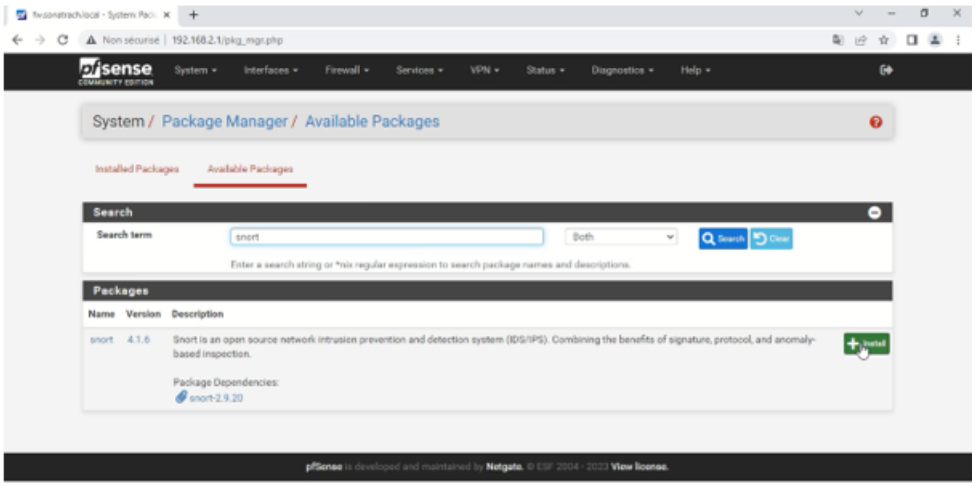


FIGURE 4.18 – Installation de package Snort.

4.4.2 Configuration des outils et mise à jour de SNORT

Pour mettre à jour notre SNORT, il est nécessaire de cocher les six règles proposées par Snort qu'on trouve dans : Services/Snort/ Global Settings. On coche :

— Enable Snort VRT : qui représente les règles de l'équipe de recherche sur la vulnérabilité Snort (VRT).

— Enable Snort GPLv2 : qui est un jeu de règles certifié et qui est distribué gratuitement sans aucune restriction de licence VRT (Vulnerability Research Team).

— Enable ET Open : ces règles ouvertes de menace émergente sont un ensemble open source de règles Snort dont la couverture est plus limitée que ETPro.

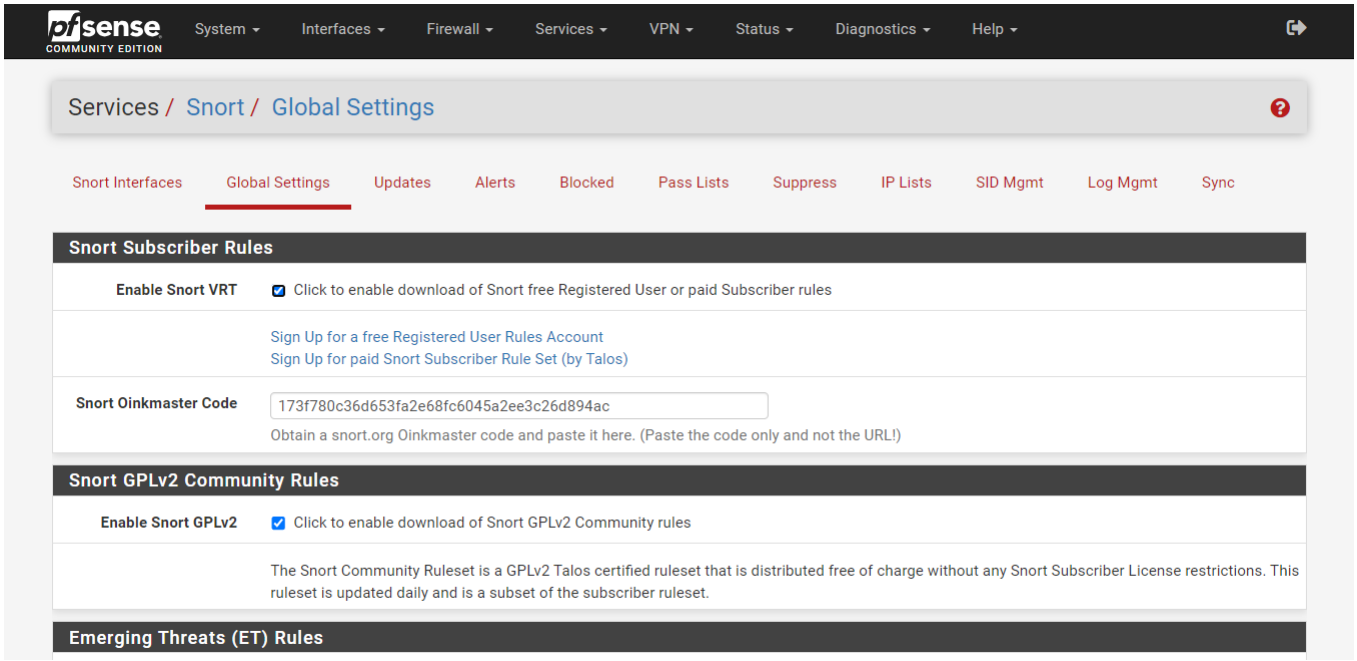
— Hide Deprecated Rules Categories : permet de manquer les régles absolète dansl'interface graphique et les supprimerde la configuration.

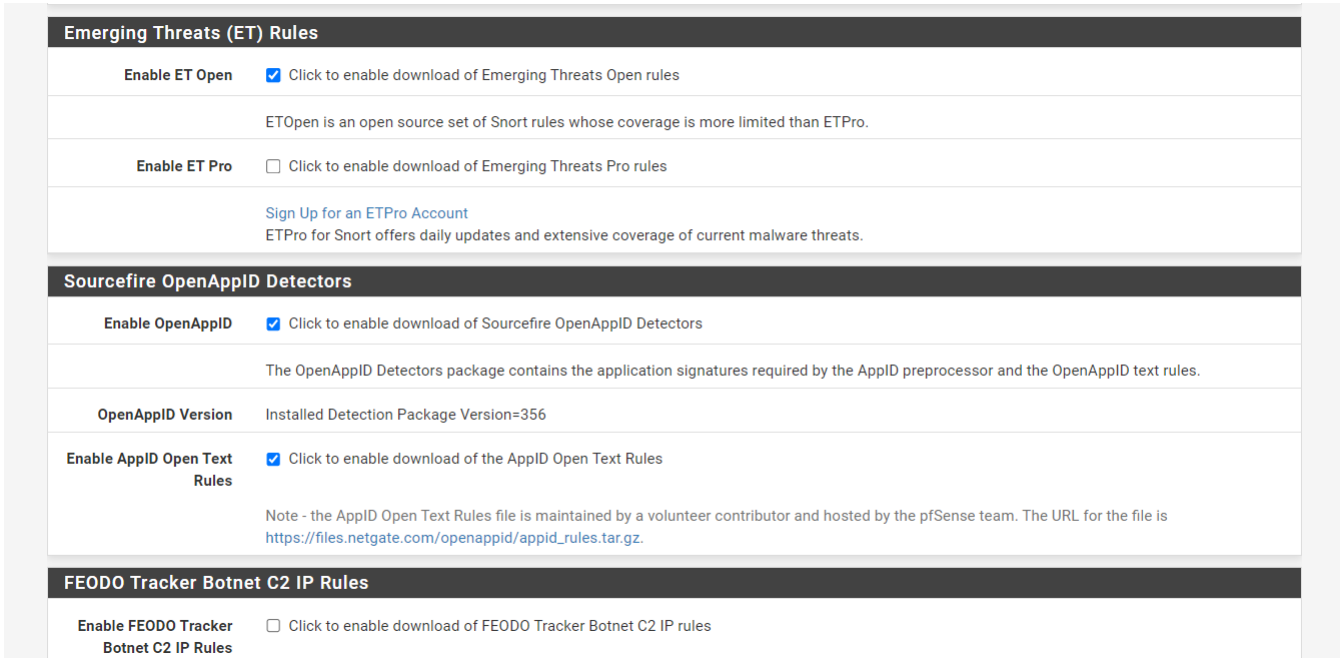
— Keep Snort Settings After Deinstall :permet de garder les paramètres apré la désinstallation de snort.

— Startup/Shutdown Logging : permet de journaliser quand snort démare et s'arrete.

Mais pour avoir la règle Enable Snort VRT, il nous demande un code Oinkmaster pour l'obtenir il faut se connecter au site officiel du Snort « Snort - Network Intrusion Detection Prevention System » avec l'utilisation d'un compte E-mail.

Les trois captures suivantes montrent les paramètres généraux de Snort et les règles à cocher.





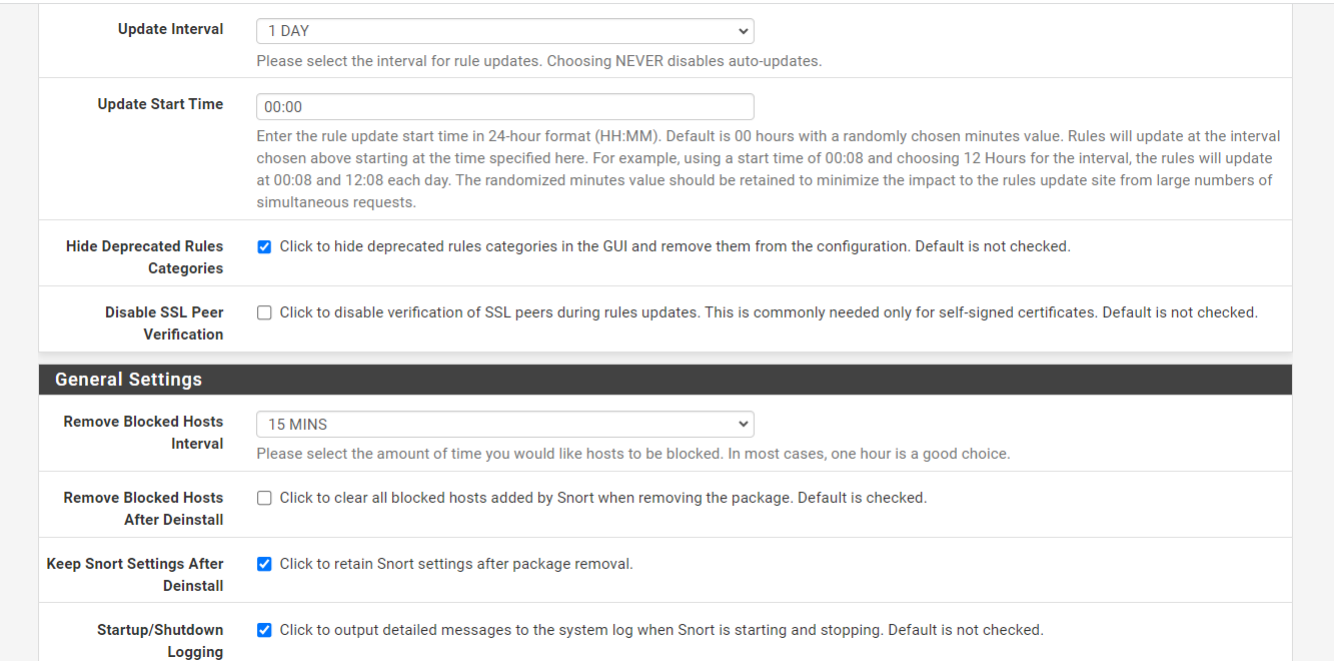


FIGURE 4.19 – Les règles de Snort a sélectionnées.

• Cette image montre comment on met à jour les six règles afin de pouvoir utiliser le SNORT, on va dans : Services/Snort/ Update, puis on clique dans (update rules). la figure suivante montre que la mise à jour des règles sont indiquées par succès :

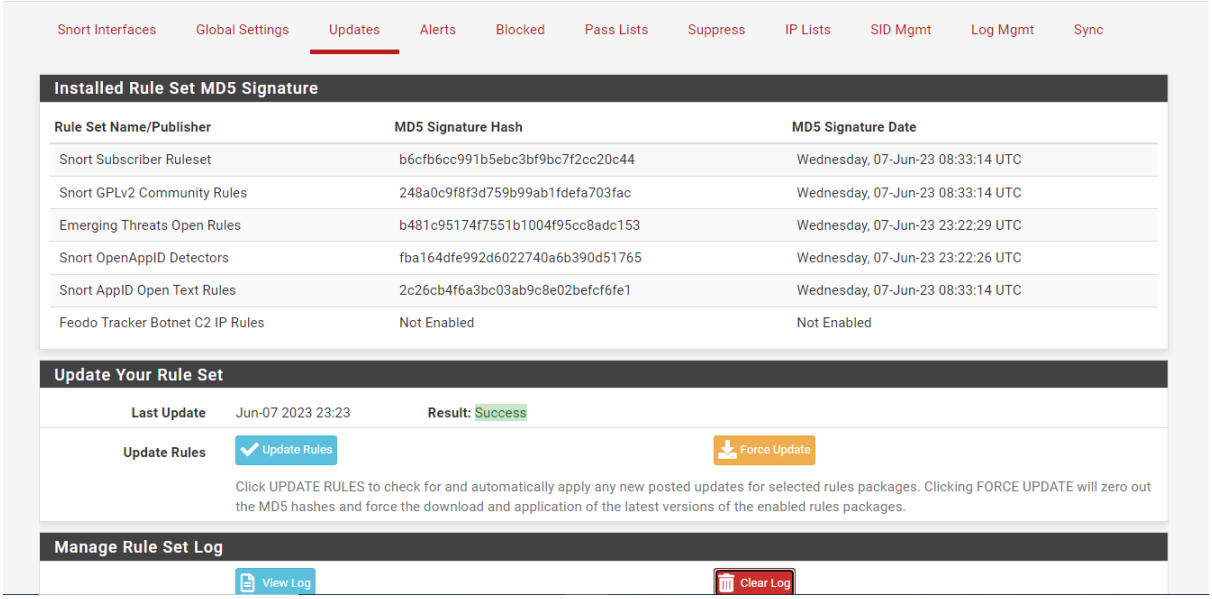


FIGURE 4.20 – Mise à jour des règles de Snort.

4.4.2.1 Activation et ajout de SNORT aux interfaces

Afin de pouvoir utiliser nos règles, il est nécessaire de les appliquer sur les interfaces de notre pare feu. Le WAN est le plus exposée aux attaques externe et nous devons empêcher ces attaques de se produire, d'abord il faut ajouter et activer SNORT pour cette interface, pour cela nous allons dans Services/Snort/Snort interfaces. Et il est nécessaire de ajouter et activer Snort pour l'interface LAN afin de détecter les attaques interne. Les deux figures prochaines expliquent comment activer Snort sur l'interface WAN qui sont les même étape a suivi pour activer Snort sur l'interface LAN :

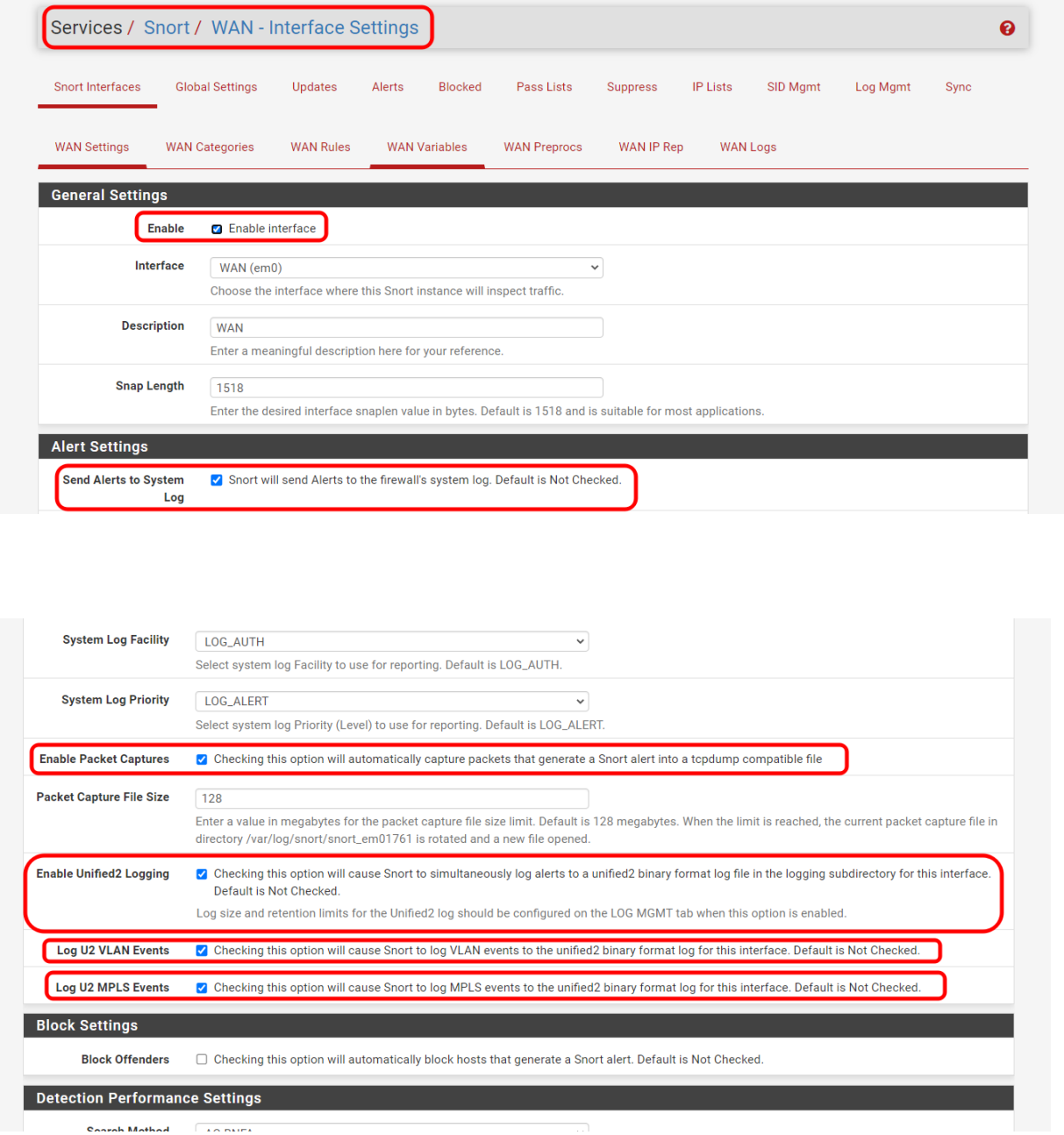


FIGURE 4.21 – Activation du Snort sur l'interface WAN

4.4.2.2 Activation des catégories

Les catégories peuvent s'appliquer à partir d'une simple clique, pour le cas de l'interface WAN. Nous allons dans : Services/ Snort/ Edit interface/ WAN Categories, on cochant l'option Use IPS Policy puis on clique en bas sur « Select all » et en finir par la sauvegarde « Save » :

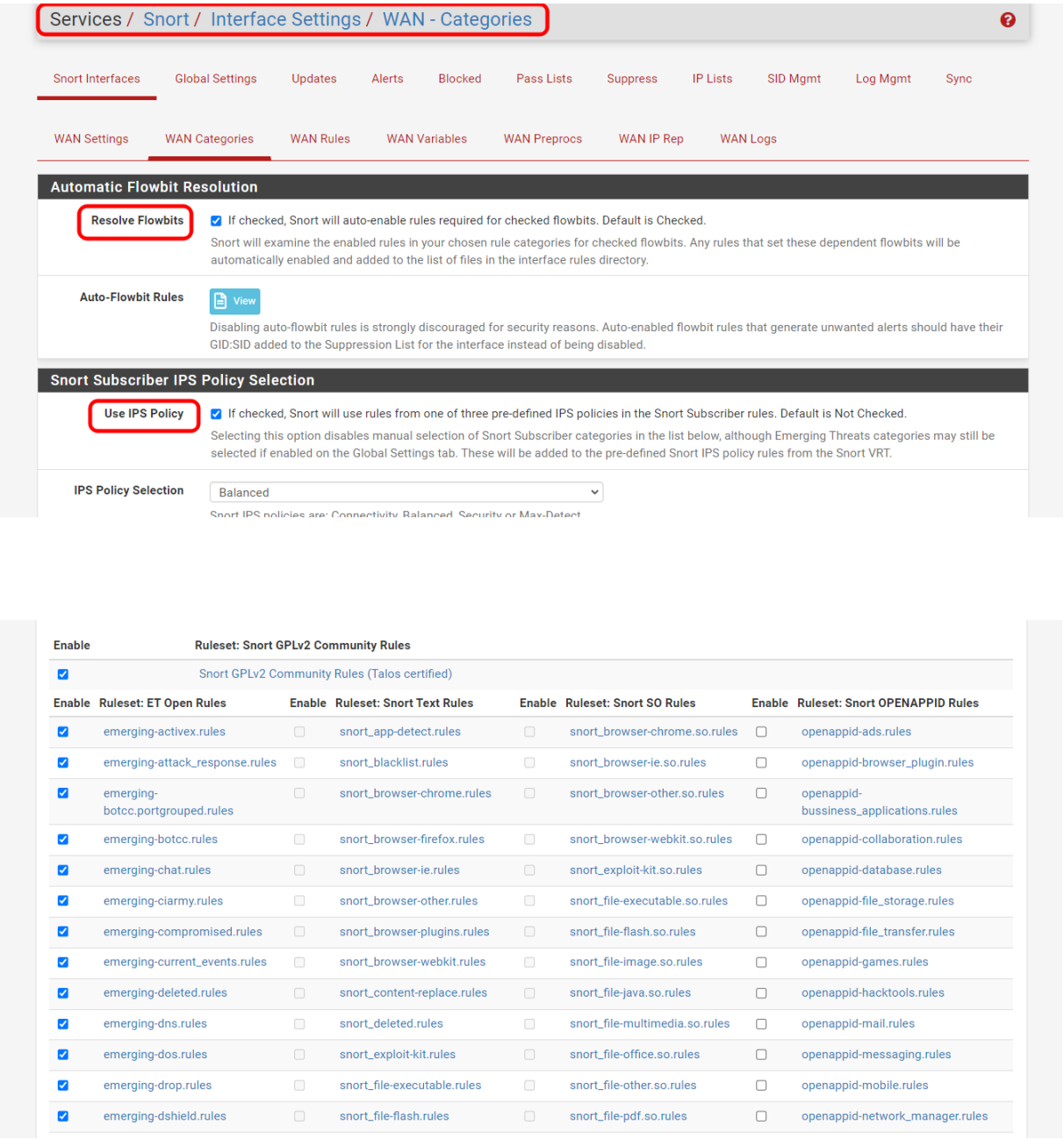


FIGURE 4.22 – Activation des catégories sur l'interface WAN.

Une fois les catégories activées, vous pourrez simplement y accéder et les configurer de façon plus fine à partir de l'onglet « WAN Rules » pour L'interface WAN et « LAN Rules » pour l'interface LAN. Chaque catégorie dispose de ses propres règles qui sont activées/désactivées par défaut.

Comme nous le voyons sur la figure 4.22 Snort est activé sur les deux interfaces WAN et LAN.

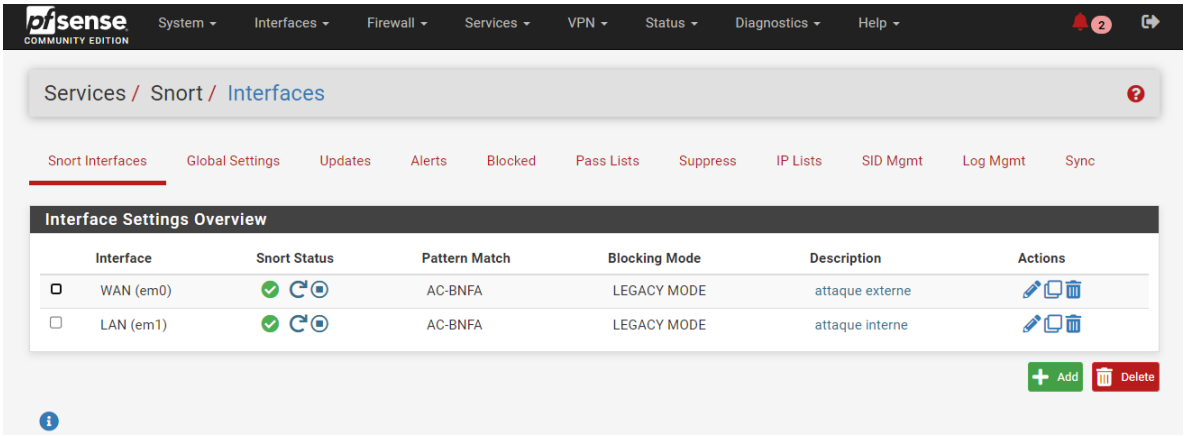


FIGURE 4.23 – Activation de Snort sur l'interfaces WAN et LAN.

4.4.2.3 Finalisation de la configuration

Maintenant nous allons dans : Services/Snort/Alerts/, et nous allons choisir nombre de ligne à afficher sur le fichier log de snort(nombre d'alerts),nous allons également cocher la case (auto-refresh view) pour actualiser la liste des notification.

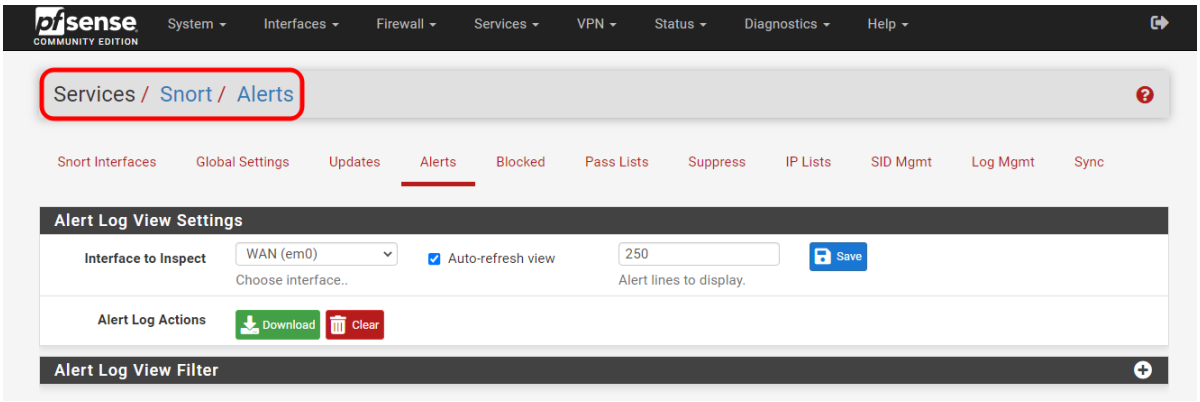


FIGURE 4.24 – Configuration des alerts.

Et pour la configuration des blocages on va dans : Services/Snort/Blocked/ même étape que la capture précedente

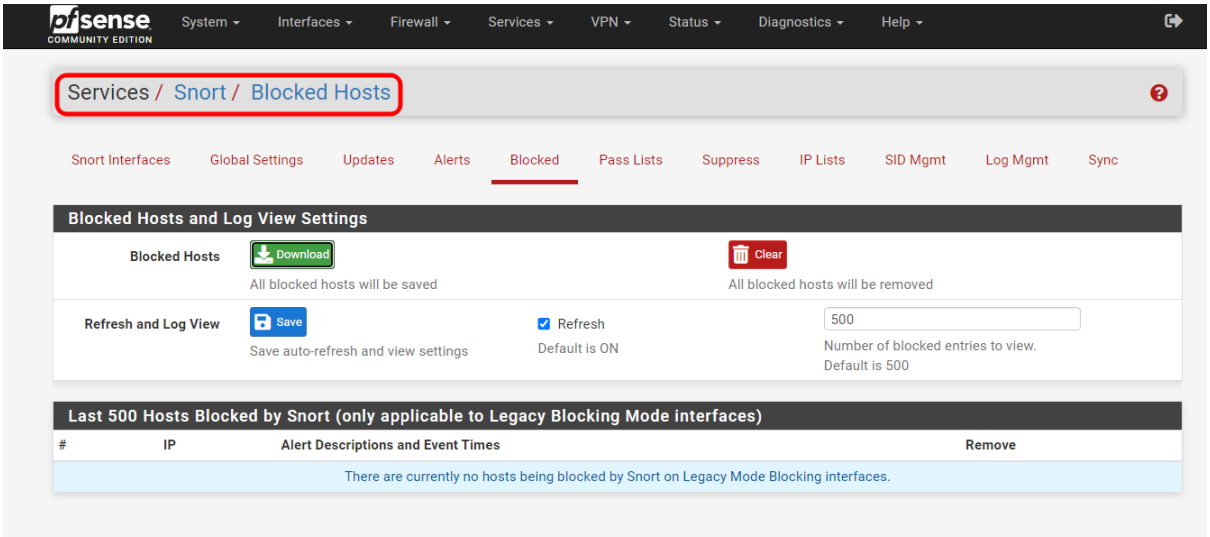


FIGURE 4.25 – Configuration des blocages.

4.5 Test de SNORT

• Attaque externe

Afin d'exécuter l'attaque, nous devons installer un attaquant (on a utilisé Kali linux avec l'adresse ip 192.168.7.9) qui représente pour nous l'intrus, puis on tape la commande nmap suivi par l'adresse IP de la machine ciblé (adresse de interface WAN du pare feu 192.168.106.1), et on lance l'attaque (scan de ports).

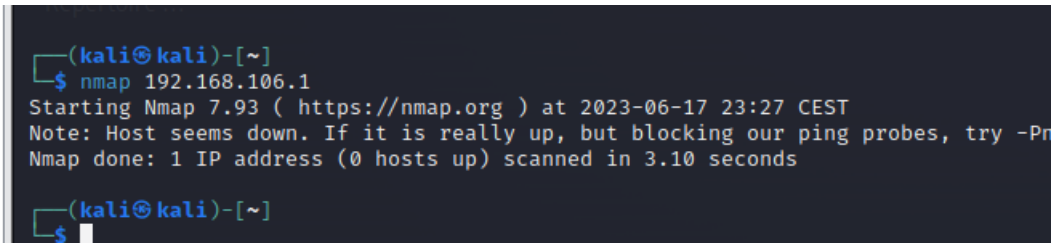


FIGURE 4.26 – Lancement de l'attaque externe .

Une fois l'attaque lancé, nous constatons clairement que SNORT détecte très rapidement l'attaque,et la bloqué et sera débloquer aprés 15 minute.

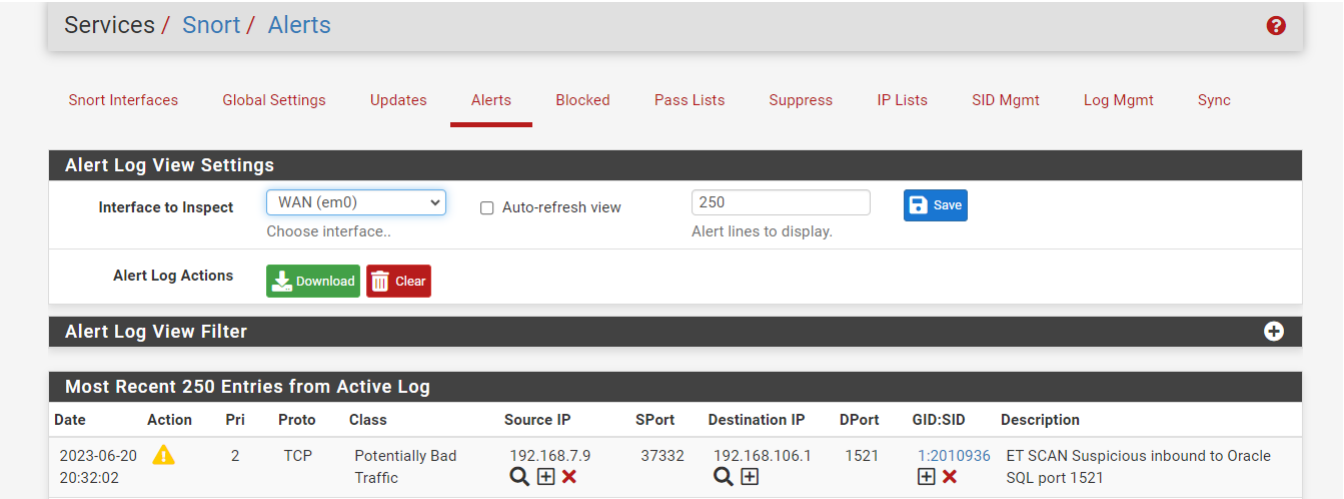


FIGURE 4.27 – Détection de l'attaque externe par Snort.

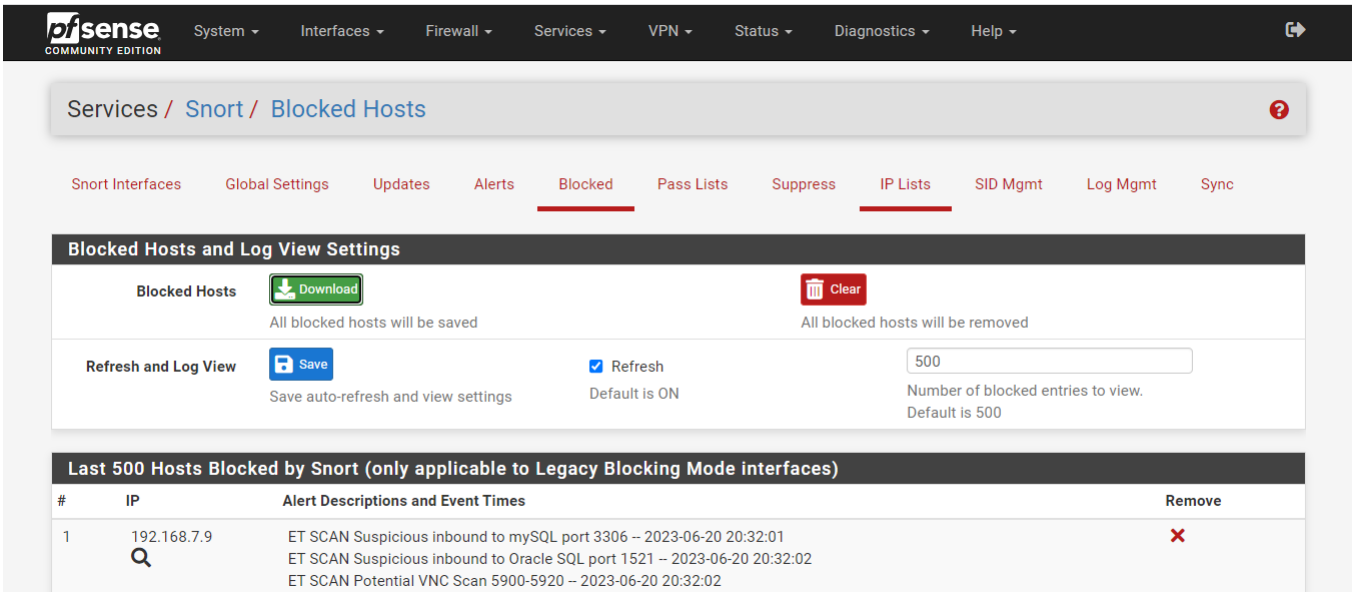


FIGURE 4.28 – La liste des adresses ip bloquées aprés le test.

• Attaque interne

Afin d'exécuter l'attaque interne, nous devons installer l'outil NMAP sur la machine attaquante qui représente pour nous l'intrus , puis on tape l'adresse IP de la machine ciblé, et on lance l'attaque (scan de ports).

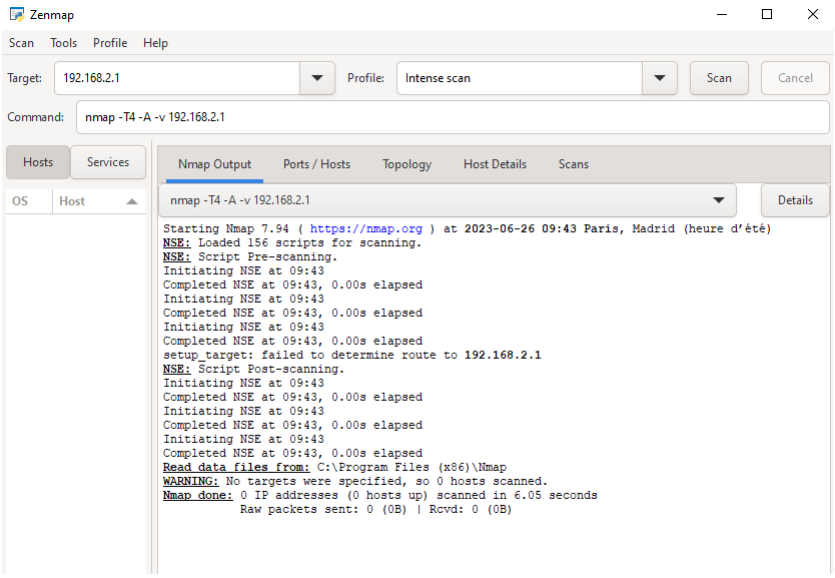


FIGURE 4.29 – Lancement de l'attaque interne.

Une fois l'attaque lancé, nous constatons clairement que SNORT détecte les l'attaque interne.

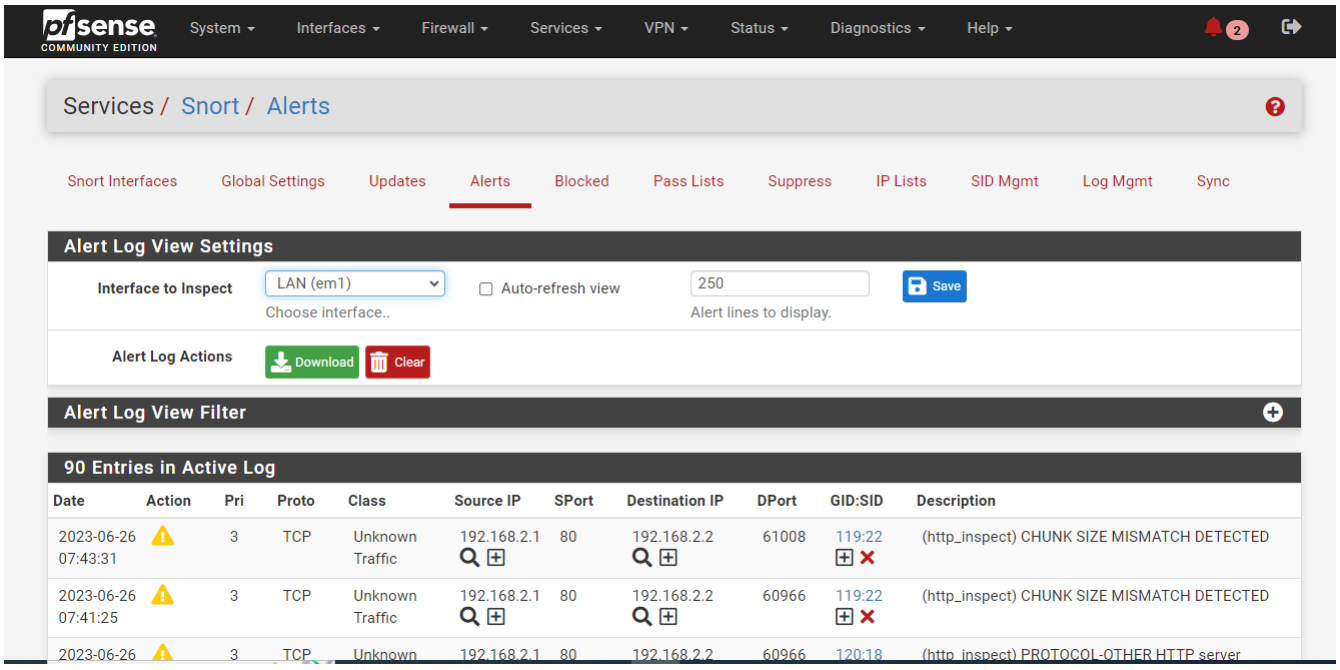


FIGURE 4.30 – Détection de l'attaque interne par Snort.

4.6 Conclusion

Tout au long de ce chapitre, nous avons presenté des outils importants pour la détection d'intrusion. A savoir pfsense et SNORT. Ensuite nous avons donné toutes les étapes d'installation et configuration de ces derniers. Enfin, pour tester notre produit Snort, nous avons procédé à un test d'intrusions avec le scanner de ports Nmap pour simuler une attaque et confirmer ainsi son bon fonctionnement .

Conclusion générale

Afin de garantir la sécurité des réseaux informatiques devant la multitude des risques et menaces qui deviennent de plus en plus complexes, il devient indispensable d'imaginer et de réaliser des solutions efficaces de protection, qui garantissent la continuité des différentes activités de l'entreprise. Pour ce faire, les solutions basiques de sécurité sont insuffisantes pour détecter les intrusions qui visent à accéder aux données confidentielles de l'entreprise.

Nous avons donc opté pour l'utilisation des systèmes de détections et de prévention d'intrusions aidés par un pare-feu, qui sont un complément idéal aux solutions de sécurité basiques tels que les pare-feu et les Antivirus. En effet, suivant leurs types (NIDS, HIDS, Hybrides), les IDS offrent une réelle plus-value aux dispositifs de sécurité.

Notre projet a donc commencé par un présentation de réseaux informatiques et leurs systèmes de sécurité. Nous allons présenter l'organisme d'accueil, la société nationale des hydrocarbures (SONATRACH) et la RTC de Bejaia. son activité, ses différentes directions. Nous allons donner une description bien détaillée sur des systèmes de détection et de prévention d'intrusion (leurs différents types, leurs principes de fonctionnement, une comparaison entre IDS et IPS).

Finalement, nous avons mis en place de Snort, nous détaillerons l'installation de Snort sous le pare feu PFSense, ainsi tous les paramétrages nécessaires afin de le rendre fonctionnel. Enfin, nous testerons la fiabilité de notre solution en lançant quelques attaques réelles dans le but de suivre son comportement. Le résultat des tests de notre système est satisfaisant, mais cela ne veut pas dire que notre système est parfaitement efficace, car aucun système de sécurité informatique permettant de garantir une sécurité fiable à cent pour cent.

Bibliographie

[1] Guy PUJOLLE, les réseaux, livre de l'édition EYROLLES, (2008).

[2] Http//mtyas.com/2009/05/11/pourquoi-le-web-30-sera-p2p-ou-ne-sera-pas. consulté le 04/2023.

[3] Dean .T « Réseaux Informatique, 2ème édition. les Editions RYNALD GOULET» 2001.

[4] https ://cisco.goffinet.org/ccna/services-infrastructure/. consulté le 04/2023.

[5] ELIE MABO, «la sécurité des systèmes informatique (théorie), support de cours » 2010.

[6] José Dordoinge. «Réseaux Informatique Notion Fondamentales (Normes, Architecture, Modèle OSI, TCP/IP, Ethernet, WIFI) ». Editions ENI. 6ème édition. Mars 2015.

[7] https ://www.networklab.fr/introduction-a-la-securite/. Consulté le 04/2023

[8] David Burgermeister, Jonathan Krier. « Les systèmes de détection d'intrusions ». 2006.

[9] Laurent Bloch et Christophe Wolfhugel. « Sécurité informatique : Principe et méthodes ». Juin 2011.

[10] Jean-Christophe GALLARD. «Sécurité et réseaux ». CNAM. Octobre 2005.

[11] http ://www.futura-sciences.com/tech/definitions/internet-firewall-474/. Consulté le 04/2023

[12] https ://www.nbs-system.com/blog/howto idsips.htmlintro-ids. Consulté le 05/2023.

[13] https ://www.nbs-system.com/blog/howto-idsips.htmlintro-ids. Consulté le 05/2023

[14] http ://deptinfo.cnam.fr/Enseignement/CycleProbatoire/SECURITE/cours-parefeux.pdf. Consulté le 05/2023

[15] HITMAN, M. et MATTORD, H. «Principales of information security. Cengage learning» (2011).

[16] http ://igm.univ-mlv.fr/dr/XPOSE2009/Sonde-de-securite-IDS-IPS/IPS.html. Consulté le 05/2023

[17] J. Timmis «Artificial immune systems : A novel data analysis technique inspired by the immune network theory» 1999.

[18] http ://www-igm.univ-mlv.fr/ dr/XPOSE2004/IDS/IDSSnort.html. Consulté le 04/2023.

[19] https ://www.snort.org/. Consulté le 03/2023.

[20] https ://eventus-networks.blogspot.com/2014/07/les-idsips-snort.html. Consulté le 04/2023.

[21] https ://docs.gns3.com/docs/. Consulté le 03/2023.

[22] https ://www.techno-science.net/glossaire-definition/VMware.html. Consulté le 04/2023.

[23] https ://www.calexium.com/fr/pfsense-le-logiciel.html, consulté le 04/2023

[24] http ://searchmidmarketsecurity.techtarget.com/definition/Snort. consulté le 05/2023.

[25] https ://www.nbs-system.com/blog/howto-idsips.htmlintro-ids, consulté le 05/2023.

[26] José Dordoinge. «Réseaux Informatique Notion Fondamentales (Normes, Architecture, Modèle OSI, TCP/IP, Ethernet, WIFI) ». Editions ENI. 6ème édition. consulter le 06/2023.

Résumé

De nos jours, les réseaux informatiques sont de plus en plus exposés à des attaques et intrusions de par l'évolution des outils utilisés par les pirates modernes. C'est pourquoi il est dit qu'un réseau totalement sécurisé est simplement impossible à concevoir. Cependant, détecter et bloquer les tentatives d'intrusions reste un atout non négligeable dans le processus de sécurisation d'un réseau informatique. Cela est possible grâce notamment aux pare-feux et aux IDS. Le travail réalisé dans ce mémoire consiste à étudier les différents aspects relatifs aux réseaux et la sécurité informatique et les attaques menaçant le réseau, et aprésenter les différents outils de sécurité (firewalls, proxy, VPN ...), ensuite configurer un système de détection d'intrusions qui est en l'occurrence SNORT, qui a été associé au pare-feu PfSense, et mettre tout ça en œuvre au niveau de l'architecture réseau de SONATRACH Bejaia. SNORT s'est imposé comme le système de détection d'intrusions le plus performant et utilisé, il peut effectuer une analyse du trafic réseau en temps réel et détecter ainsi de nombreux types d'attaques.

Mots clés : Sécurité, Attaques, Intrusion, Snort, PfSense, Firewall, IDS, , SONATRACH.

Abstract

Today, computer networks are increasingly exposed to attacks and intrusions due to the evolution of tools used by modern hackers. This is why it is said that a completely secure network is simply impossible to design. However, detecting and blocking intrusion attempts remains a significant asset in the process of securing a computer network. This is possible thanks to firewalls and IDS. The work carried out in this brief consists in studying the various aspects related to networks and computer security and attacks threatening the network, presenting the various security tools (firewalls, proxy, VPN, etc.), then configure an intrusion detection system that is in this case SNORT, which has been associated with the PfSense firewall, and implement all this at the level of the SONATRACH Bejaia network architecture. SNORT has established itself as the most efficient and used intrusion detection system, it can perform real-time network traffic analysis and thus detect many types of attacks.

Keywords : Security, Attacks, Intrusion, Snort, PfSense, Firewall, IDS, SONATRACH.