République Algérienne Démocratique et Populaire Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université Abderrahmane Mira Béjaïa

Faculté des Sciences Exactes

Département Informatique

Mémoire de fin d'études

En vue de l'obtention du Diplôme de Master Professionnel en Informatique

Option : Administration et Sécurité des Réseaux

Thème

Mise en place d'un système de détection d'intrusion au niveau de l'Entreprise Portuaire de Béjaïa

Réalisé par :

MESSALTI Abdelhak et BOUCHAMA Rafik

Président :	Mme. **ELBOUHISSI** Houda	Université de Béjaïa
Encadreur :	Mme. **ADEL** Karima	Université de Béjaïa
Examinateur :	Mr. **MOKTEFI** Mohand	Université de Béjaïa

2020-2021

Dédicaces

On dédie ce travail :

A nos chers parents, pour tous leurs sacrifices, leurs amours, leurs tendresses, leurs soutiens et leurs prières tout au long de nos études.

A nos chères frères, nos chères sœurs pour leurs encouragements permanents, et leur soutien moral. A toute nos familles pour leur soutien tout au long de nos parcours universitaire.

A tous nos amis et tous ceux qui ont contribués de près ou de loin à la réalisation de ce travail.

Que Dieu les protège

Abdelhak et Rafik

Remerciements

Avant d'entamer ce projet de fin d'étude, nous rendons grâce à Dieu, le tout puissant et miséricordieux, de nous avoir donné le savoir, le courage et la force pour mener à bien et à terme ce modeste travail.

Au terme de ce projet de fin d'étude, nous adressons nos sincères remerciements à Madame ADEL, notre encadreur pour ses directives précieuses, et pour la qualité de son suivi durant le travail effectué pour ce projet.

Nous tenons à exprimer toute notre grande gratitude aux membres du jury qui ont accepté d'évaluer notre projet, nous leurs présentons toute nos gratitudes et nos profonds respects.

Par la même occasion, nous tenons à exprimer nos vifs remerciements à l'ensemble du personnels de l'entreprise EPB spécialement monsieur Hicham.

Pour finir, nous voulons exprimer nos reconnaissances envers les amis et collègues qui nous ont apporté leurs supports moraux tout au long de notre travail.

Table des Matières

Liste des figures

Liste des tableaux

Listes d'abréviation

ACID: Analysis Console for Intrusion Detection

AH: Authentication Header

ARP: Address Resolution Protocol

CERT: Computer Emergency Response Team

CNAN: Company National Algerian Navigation

CPU : Central Processing Unit

DC : Domain Controller

DHCP: Dynamic Host Configuration Protocol

DMZ : Demilitarised Zone

DNS : Domain Name System

ESP: Encapsulating Security Payload

EPE Entreprise Publique Economique

FTP: File Transfer Protocol

GED: Gestion Electronique de Documents

GUI: Graphical User Interface

HIDS: Host Intrusion Detection System

HIPS: Host Intrusion Prevention System

HSE: Hygiène Sécurité Environnement

HTTP: Hyper Text Transfer Protocol

HTTPS: Hyper Text Transfer Protocol Secure

ICMP: Internet Control Message Protocol

IDS: Intrusion Detection System

IETF: Internet Engineering Task Force

IP: Internet Protocol

IPS:	Intrusion Prevention System
IPSec:	Internet Protocol Security
ISP:	Internet Server Provider
LAN:	Local Area Network
LCP:	Link control Protocol
LLC:	Logical Link Control
L2F:	Layer 2 Forwarding
MAC:	Medium Access control
MAN:	Metropolitan Area Network
NCP:	Network Control Protocol
NIDS:	Network Intrusion Detection System
Nmap:	Network Mapper
ONP :	Office National des Ports
OSI:	Open System Interconnection
PAN:	Personnel Area Network
PHP:	Hypertext Preprocessor
PPP:	Protocol Point to Point
PPTP:	Point To Point Tunneling Protocol
RAID:	Redundant Array of Independent Disk
RIP:	Routing Information Protocol
SNM:	Société National de Manutention
SPA:	Société par Actions
SQL :	Structured Query Language
SSH:	Secure Shell
SSL:	Secure Socket Layer

TCP:	Transmission Control Protocol
UDP:	User Datagram Protocol
UTMS:	Universal Mobile Telecommunications System
VLAN	Virtual Local Area Network
VPN :	Virtual Private Network
WAN:	Wide Area Network
WIMAX:	Worldwide Interoperability for Microware Access

INTRODUCTION GENERALE

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 manne 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 étrangères pour essayer de pénétrer le réseau local de l'entreprise y accomplir des actions douteuses de destruction, vol d'informations confidentiels…etc.

Pour parer à ces attaques, doit être prendre une architecture sécurisée, Pour cela, les administrateurs déploient des solutions de sécurité efficace capable de protéger le réseau de l'entreprise. Dans le 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. Un IDS doit être conçu dans une politique globale de sécurité. 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 portuaire de Bejaia, c'est l'objet de ce mémoire de fin d'étude.

Nous avons structuré notre mémoire en quatre chapitres :

- Dans le premier chapitre, nous présentons l'organisme d'accueil de l'entreprise portuaire de Bejaia.
- Dans le deuxième chapitre, nous abordons les notions de base du réseau, et la sécurité informatique qui comprend les différentes attaques ainsi les mécanismes de sécurité mis-en-place.
- Le troisième chapitre est consacré à l'étude des systèmes de détection et de prévention d'intrusion, ses différentes variantes et ses méthodes de détection.
- Le dernier chapitre consiste à l'installation de pare-feu (Pfsense) équipé de Snort qui est un système open source pour réaliser une détection d'intrusion.

Chapitre 01

L'ORGANISME D'ACCUEIL DE L'EPB

1.1. Introduction:

Dans ce chapitre nous présenterons l'organisme d'accueil : l'entreprise portuaire de Bejaia en étalant en première partie son historique ainsi que ses activités principales, puis les différentes divisions qui la constituent. Nous nous intéresserons surtout à la division informatique afin de comprendre l'architecture réseau de cette entreprise et énumérer les problèmes rencontrés, pour énoncer en seconde partie, la problématique constatée au cours de notre stage puis proposer une solution pour pallier au manque constaté.

1.2. Présentation de l'entreprise portuaire de Bejaia:

Le port de Bejaia est un port Algérien situé dans la région de Kabylie dans le nord du pays. Il est notamment consacré au commerce international et aux hydrocarbures. Il joue un rôle très important dans les transactions internationales vu sa situation géographique [1].

Figure 1.1 : Port de Bejaia.

1.3. Création de l'EPB :

Le décret n°82-285 du 14 Août 1982 publié dans le journal officiel n° 33 porta création de l'Entreprise Portuaire de Bejaïa, entreprise socialiste à caractère économique, conformément aux principes de la charte de l'organisation des entreprises, aux dispositions de l'ordonnance n° 71-74 du 16 Novembre 1971 relative à la gestion socialiste des entreprises et les textes pris pour son application à l'endroit des ports maritimes.

L'entreprise, réputée commerçante dans ses relations avec les tiers, fut régie par la législation en vigueur et soumise aux règles édictées par le susmentionné décret. Pour accomplir ses missions, l'entreprise est substituée à l'ONP (Office National des Ports), à la SNM (Société Nationale de Manutention) et pour partie à la CNAN (Compagnie Nationale Algérienne de Navigation).

Elle fut dotée par l'Etat, du patrimoine, des activités, des structures et des moyens détenus par l'ONP, la SNM et de l'activité Remorquage, précédemment dévolue à la CNAN, ainsi que des personnels liés à la gestion et aux fonctionnements de celles-ci.

En exécution des lois n° 88.01, 88.03 et 88.04 du 02 Janvier 1988 s'inscrivant dans le cadre des réformes économiques et portant sur l'autonomie des entreprises, et suivant les prescriptions des décrets n°88.101 du 16 Mai 1988, n°88.199 du 21 Juin 1988 et n°88.177 du 28 Septembre 1988, l'Entreprise Portuaire de Bejaia entreprise socialiste est transformée en EPE (Entreprise Publique Economique), SPA (Société par Actions depuis) le 15 Février 1989, son capital social fut fixé à Dix millions (10.000.000) de dinars algérien, actuellement, il a été augmenté à 3.500.000.000 de DA [1].

1.4. Missions et activités de l'EPB:

1.4.1. Missions:

La gestion, l'exploitation et le développement du domaine portuaire sont les charges essentielles de la gestion de l'EPB (Entreprise Portuaire de Bejaia), cela dans le but de promouvoir les échanges extérieurs du pays. Elle est chargée des travaux d'entretien, d'aménagement, de renouvellement et de création d'infrastructures. L'EPB assure également des prestations à caractère commercial, à savoir : le remorquage, la manutention et l'acconage, le transite des passagers et leur véhicule par la gare maritime du port de Bejaia [1].

1.4.2. Activités:

Les principales activités de l'entreprise sont :

- L'exploitation de l'outillage et des installations portuaires**.**
- L'exécution des travaux d'entretien**,** d'aménagement et de renouvellement de la super structure portuaire**.**
- L'exercice du monopole des opérations d'acconage et de manutention portuaire.
- L'exercice du monopole des opérations de remorquage**,** de pilotage et d'amarrage**.**
- La police et la sécurité portuaire dans la limite géographique du domaine public portuaire [1].

1.5. Organisation générale de l'EPB :

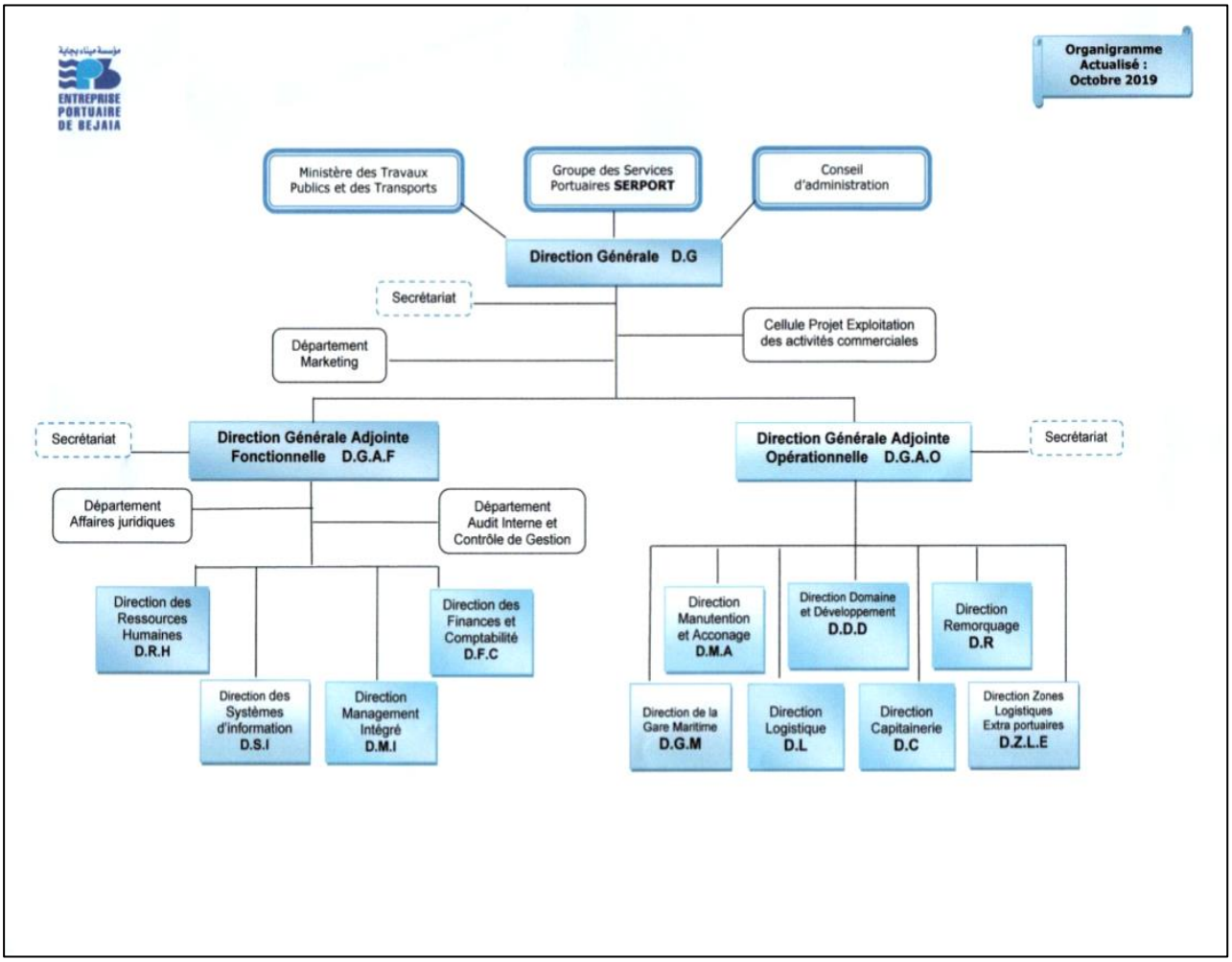


Figure 1.2 : Organigramme général de l'EPB.

1.5.1. Direction Générale (DG) :

Elle est chargée de concevoir, coordonner et contrôler les actions liées à la gestion et au développement de l'entreprise, elle est divisée en deux parties [1] :

1.5.1.1. Directions Générale Adjointe Opérationnelle DGAO:

Il s'agit des structures qui prennent en charge les activités sur le terrain et qui ont une relation directe avec les clients.

a. Direction Manutention et Acconage (D.M.A) : Elle est chargée de prévoir, organiser, coordonner et contrôler l'ensemble des actions de manutention et d'acconage liées à l'exploitation du port.

b. Direction Domaine et Développement (DDD) :

A pour tâches :

- Amodiation et location de terre-pleins, hangar, bureaux, immeubles, installations et terrains à usage industriel ou commercial.
- Enlèvement des déchets des navires et assainissement des postes à quai.
- Pesage des marchandises (pont bascule).
- Avitaillement des navires en eau potable.

c. Direction capitainerie (D.C) : Elle est chargée de la sécurité portuaire, ainsi que de la bonne régulation des mouvements des navires, et la garantie de sauvegarde des ouvrages portuaires.

d. Direction Remorquage (DR) :

Elle est chargée d'assister le pilote du navire lors de son entrée et de sa sortie du quai. Son activité consiste essentiellement à remorquer les navires entrants et sortants, ainsi que la maintenance des remorqueurs. Les prestations sont :

- Le Remorquage portuaire.
- Le Remorquage hauturier (haute mer).
- Le Sauvetage en mer.

e. Direction logistique (D.L) : Elle consiste à gérer tout ce qui concerne le transport et le stockage des produits de l'entreprise : véhicules nécessaires au transport, fournisseurs de l'entreprise, entrepôts, manutention, en optimisant leur exploitation pour minimiser les coûts et les délais.

f. Direction Zones Logistiques Extra Portuaire (D.Z.L.E) :

Elle a pour objet de gérer les flux physiques, informationnels et financiers d'une organisation, dans le but de mettre à disposition les ressources correspondantes aux besoins, aux conditions économiques et pour une qualité de service déterminées, dans des conditions de sécurité et de sûreté satisfaisantes.

1.5.1.2. Directions Générale Adjointe Fonctionnelle DGAF:

Cette direction est composée des structures de soutien aux structures opérationnelles.

a. Direction Management Intégré (D.M.I) :

Elle est chargée de :

- La mise en œuvre, le maintien et l'amélioration continue du Système de Management Intégré (plans projets et indicateurs de mesure).
- L'animation et la coordination de toutes les activités dans le domaine HSE (Hygiène Sécurité Environnement).
- La Contribution dans des actions de sensibilisation et de formation à la prévention des risques de pollution, à la protection de l'environnement, la santé des travailleurs et à l'intervention d'urgence.

b. Direction Finances et Comptabilité (DFC) :

Elle est chargée de :

- La tenue de la comptabilité.
- La gestion de la trésorerie (dépenses, recettes et placements).
- La tenue des inventaires.
- Le contrôle de gestion (comptabilité analytique et contrôle budgétaire).

c. Direction Ressources Humaines (DRH) :

Elle est chargée de prévoir, d'organiser et d'exécuter toutes les actions liées à la gestion des ressources humaines en veillant à l'application rigoureuse des lois et règlement sociaux. Elle assure les tâches suivantes :

- La mise en œuvre de la politique de rémunération, de recrutement et de la formation du personnel.
- La gestion des carrières du personnel (fichier).
- La gestion des moyens généraux (achats courants, parc automobile, assurances).

d. Direction des Systèmes d'Information (DSI) :

Elle est chargée de gérer l'ensemble des systèmes d'information et de télécommunication de l'entreprise.

1.5.2. Direction du système d'information (DSI):

1.5.2.1. Présentation:

Le système d'information (SI) est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information. La DSI est une direction de l'EPB rattachée directement à la direction générale, elle a pour mission l'automatisation des métiers de l'entreprise portuaire de Bejaia [1].

1.5.2.2. Missions:

Durant le stage effectué au niveau de la direction des systèmes d'information nous avons pu identifier les missions du système d'informations comme la montre la figure ci-dessous :

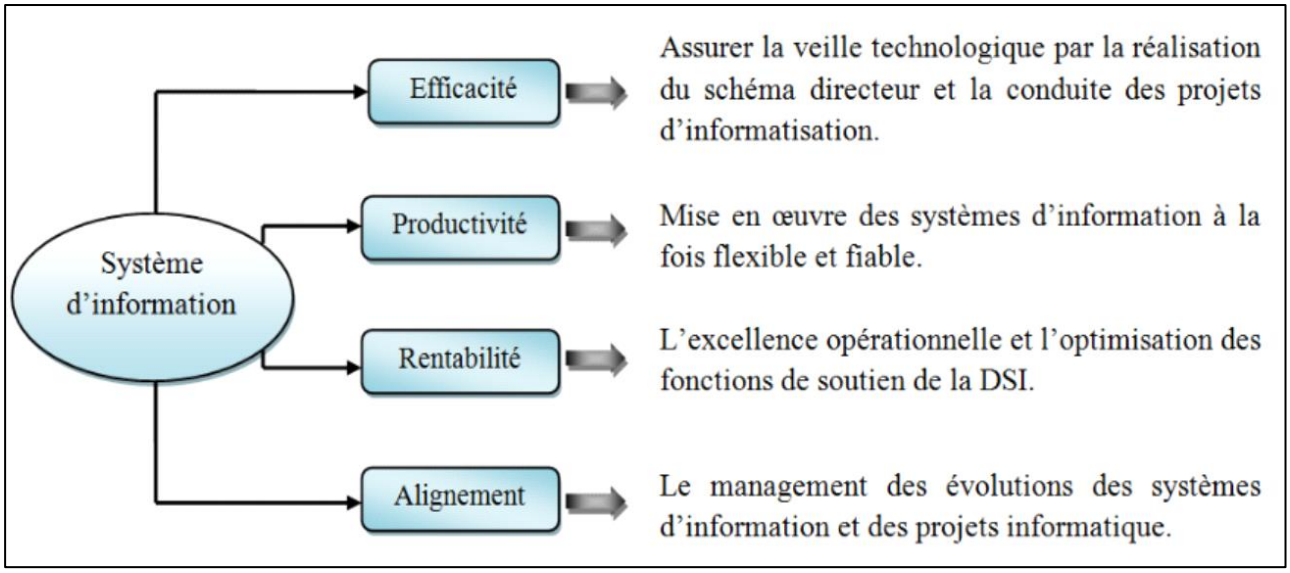


Figure 1.3 : Missions du système d'information de l'EPB.

1.5.2.3. Organisation humaine de la direction du système d'information :

La direction se compose de trois départements comme le montre l'organigramme suivant : [1]

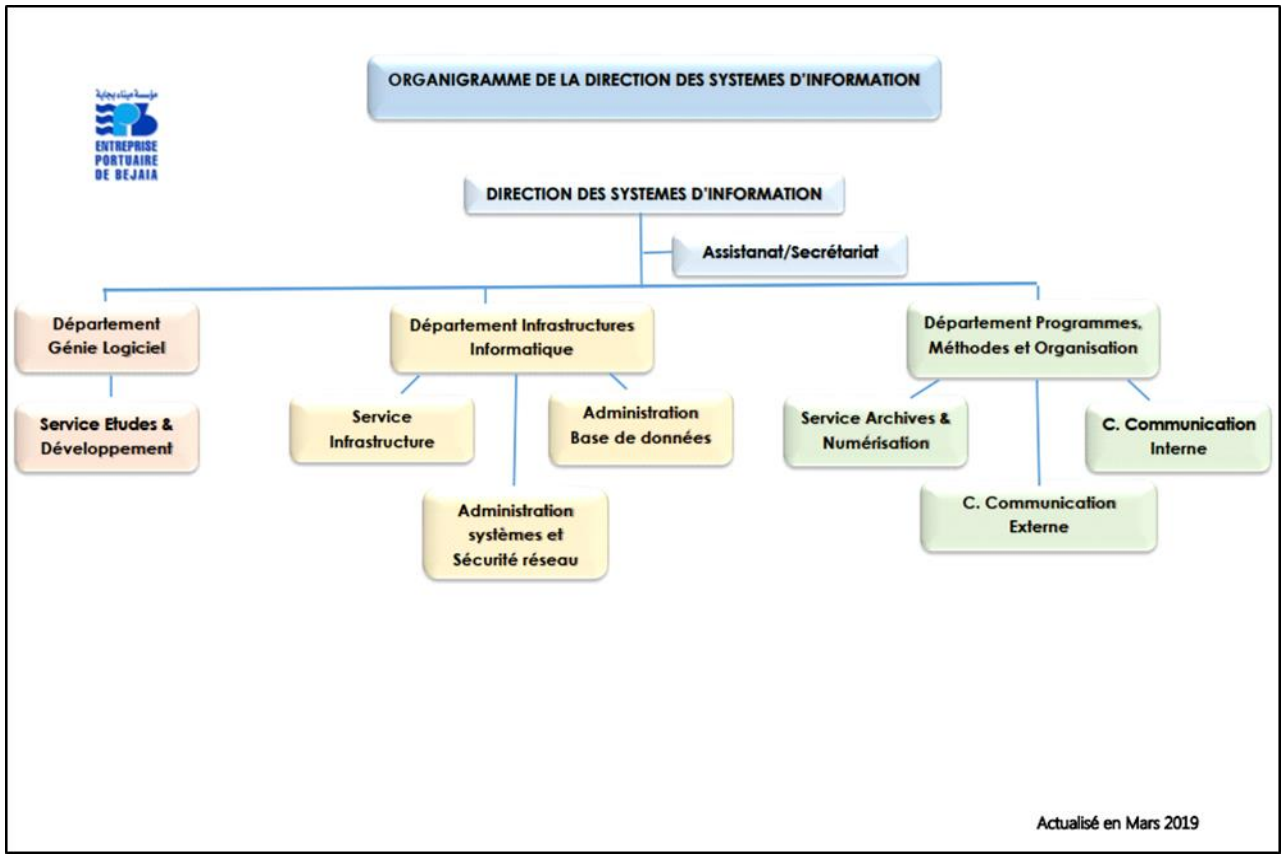


Figure 1.4 : Organigramme de la Direction du Système d'Information.

1.5.2.4. infrastructure informatique:

Le réseau du port de Bejaia s'étend du port pétrolier (n°16) aux ports 13 et 18 (parc à bois). La salle machine du réseau local de l'EPB contient principalement une armoire de brassage et une autre armoire optique de grande taille, ces deux armoires servent à relier les différents sites de l'entreprise avec le département informatique par fibres optiques de type 4, et 12 brins, comme l'illustre la figure (Fig. 1-5). Chaque site a une armoire de brassage contenant un/des convertisseur(s) media, un/plusieurs Switch où sont reliés les différents équipements par des câbles informatiques [1].

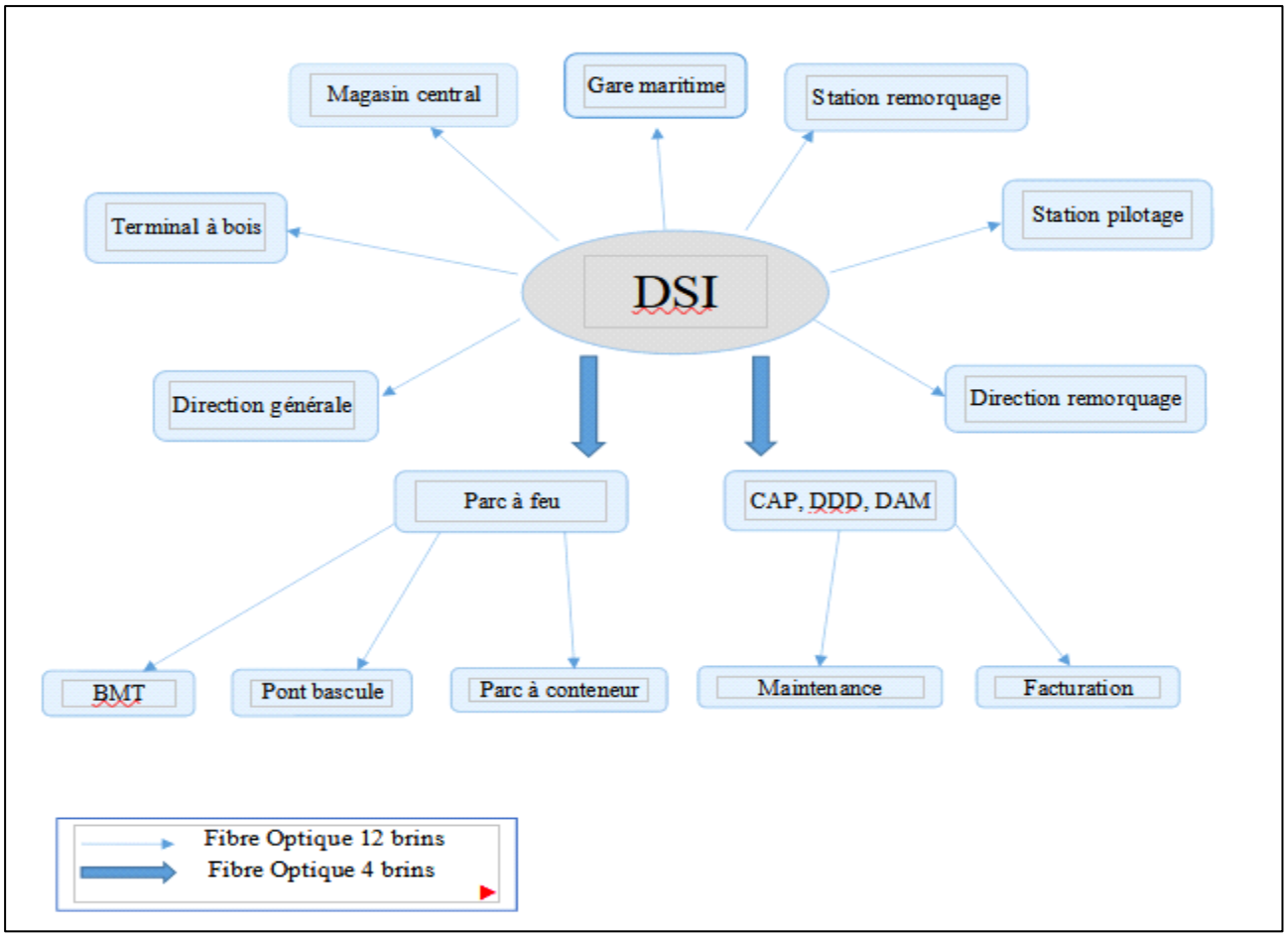


Figure 1.5 : Réseau fibre optique de l'EPB.

1.5.2.5. Le réseau local de l'EPB:

Le réseau local de l'EPB permet aux différents postes de travail d'échanger des informations, de se connecter vers l'extérieur et d'utiliser des applications hébergées en interne nécessaire à l'exécution des tâches quotidiennes des employées. Le réseau du port de Bejaia s'étend du port pétrolier (N16) aux ports 13 et 18 (port à bois).

1.6. Architecture du réseau local de l'entreprise :

L'architecture du réseau LAN de l'entreprise est représentée dans la figure ci-dessous [1] :

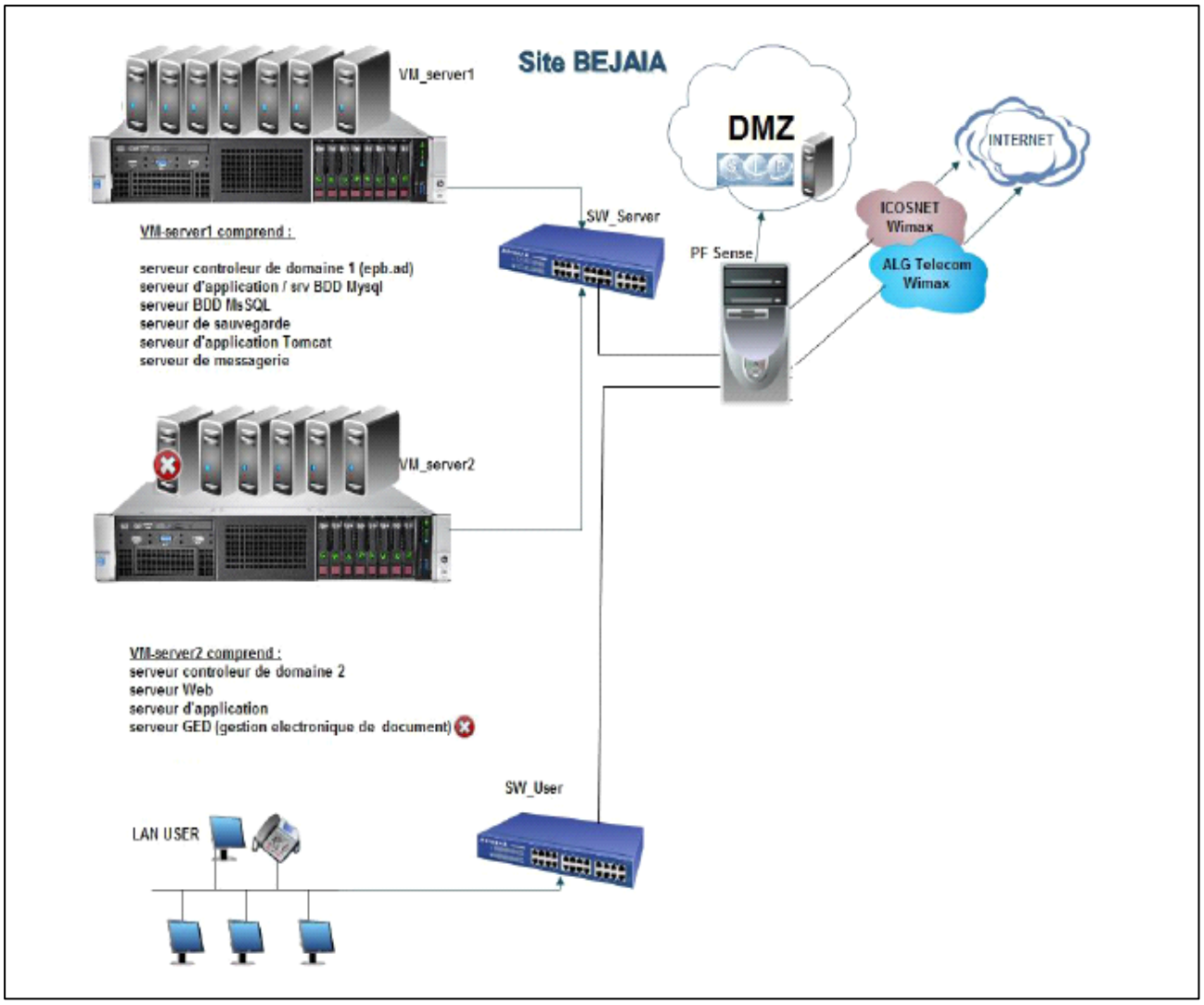


Figure 1.6 : Architecture actuelle du réseau local de l'entreprise.

a. Connexion Internet :

L'entreprise portuaire de Bejaia est dotée de deux connexions internet, Icosnet et Algérie télécom. En utilisant l'accès haut débit sans fil WIMAX (Worldwide Interopérabilité for Microware Access) qui est une solution alternative pour le déploiement des réseaux haut débit, l'entreprise se connecte à une internet sans-fil à partir d'un poste fixe qui communique par ondes hertziennes via une antenne-relais appelée station de base.

b. Sécurité :

La sécurité est assurée par un pare-feu pour appliquer les stratégies d'accès et les règles de routages déterminant la manière dont les clients accèdent à Internet.

- **Pfsense (pare- feu) :** La sécurité est assurée par deux serveurs virtuel pare-feu qui agissent comme un filtre afin de définir les règles d'accès à un réseau comme Internet à cause des risques que peut représenter une connexion normal dans certains cas.
- **DMZ** : une zone démilitarisée qui consiste à créer une « zone » de telle sorte que l'échange entre le réseau interne et le réseau externe transite par cette dernière, dont l'objectif principale et que tous les échanges passent par cette zone qui offre les différents services de sécurité tels le filtrage réseaux entre les différents réseaux ainsi interconnecter mais aussi des serveurs relais dans la DMZ pour gérer tous le trafic interne et externe.
- **VPN (Virtuel Private Network) :** Pour répondre aux besoins d'interconnexion de l'entreprise portuaire de Bejaia aux différents sites distants (BORDJ BOU ARRERIDJ et IGHIL OUBEROUAK -TALA HAMZA).

c. Salle machine:

Les activités du port se rattachent à cette salle, qui rassemble tous les serveurs nécessaires pour répondre aux attentes des utilisateurs afin d'aboutir à un réseau qui accompagne la croissance de l'entreprise. En plus des switches elle comporte une armoire de brassage qui contient des différents serveurs tels que :

- **Serveur de base de données (SQL server and MARIA DB) :** un serveur de base de données répond à des demandes de manipulation de données stockées dans une ou plusieurs bases de données. Il s'agit de demande de recherche, de tri, d'ajout, de modification ou de suppression de données. Ces données sont utilisées par des serveurs web et des utilisateurs.
- **Serveur de contrôleur de domaine DC1 (Active Directory)** : Sous Windows Server 2012 R2 l'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateur utilisant le système Windows. Il répertorie les éléments de ce réseau administré tel que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes … etc.
- **Serveur de contrôleur de domaine redondant DC2 (Active Directory) :** Il permet de conserver des réplicas de données de l'annuaire sur un autre contrôleur de domaine, cela garantie la disponibilité et la continuité.
- **Un serveur de messagerie électronique(Exchange):** est un serveur qui est connecté à internet, il permet à ses utilisateurs d'envoyer et de recevoir des courriers électroniques. Pour se connecter au serveur de messagerie, l'utilisateur a recours à un logiciel client, capable de

gérer l'adressage (ou envoi) du courriel mais aussi sa réception tel que Outlook de Ms office, ou via navigateur web (Web mail).

- **Serveur application/fichier :** C'est un serveur sur lequel sont installées les applications utilisées par les usagers. Ces applications sont chargées sur le serveur d'application pour y accéder à distance. Un serveur d'application peut être un serveur qui centralise toutes les applications utilisées par les postes clients.
- **Serveur antivirus (Eset) :** est un outil de gestion centralisé de protection contre les programmes malveillants dans l'entreprise et d'administration de l'antivirus chez les utilisateurs.
- **Serveur DNS** (Domain Name System) : est le service de résolution de nom d'hôte, il permet d'associer un nom d'une machine à un adresse IP.
- **Serveur DHCP :** pour un adressage dynamique, afin d'avoir une configuration fiable des paramètres de connexion et d'assurer la réduction de gestion de configuration.
- **Serveur web** : est spécifiquement un serveur multiservices utilisé pour publier des sites web sur Internet ou un intranet. L'expression « serveur Web » désigne également le logiciel utilisé sur le serveur pour exécuter les requêtes HTTP, le protocole de communication employé sur le World Wide Web.
- **Serveur d'impression :** est un serveur qui permet de partager une ou plusieurs imprimantes entre plusieurs utilisateurs (ou ordinateurs) situés sur un même réseau informatique ainsi la centralisation de l'administration.
- **La Technologie de stockage avec les RAID : (**Redundant Array of Independent Disk) pour une meilleure gestion de stockage et de disponibilité des données l'entreprise EPB s'est dotée de la technologie RAID et plus précisément le RAID de niveau 5.

1.7. Parc informatique de l'EPB:

L'EPB dispose de 250 PC HP et ACER répartis travers les différentes directions de l'entreprise et un réseau informatique interconnecté par fibre optique et de câbles paires torsadés. Les systèmes d'exploitation utilisés sur les postes de travail sont Windows et Linux sous différentes distributions [1].

- ✓ La majorité des PC est reliée à des imprimantes de plusieurs types (matricielle, laser et à jet d'encre couleur).

- ✓ Chaque ordinateur est branché à un onduleur APC de 400 à 1000 VA.
- ✓ Tous les PC sont dotés d'un anti-virus ESET END point.
- ✓ Tous les PC sont connectés à l'internet.

1.8. Présentation du projet:

Dans cette partie, nous allons définir les imperfections du système actuel. Ce qui nous permettra de détecter les insuffisances et les difficultés rencontrées.

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. Au cours de nos visites au sien de l'entreprise portuaire de Bejaia, nous avons constatés deux anomalies au niveau de la sécurisation du réseau de l'entreprise, nous les énumérons comme suit :

- Aucun système de détection d'intrusion n'est mis en place pour donner un maximum d'information sur l'attaque détectée et de préparer la réaction.
- Aucun système de protection contre la divulgation de donné interne.

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.

1.9. Conclusion :

Dans ce chapitre nous avons pris connaissance de l'organisme d'accueil de l'entreprise (EPB) ainsi que l'architecture réseau la constituant dont on a relevé quelques failles de sécurité, pour y remédier, nous avons fini par proposer une solution qui consiste à mettre en place un pare-feu équipé d'un IDS.

Dans le chapitre qui suit, nous allons présenter les principes de bases des réseaux informatiques (architectures, types, topologies, modèles de standardisation, protocoles… etc). Le développement

de ce dernier a posé des conflits majeurs aux utilisateurs qui restent confrontés à une augmentation et à une complexité croissante d'intrusions et attaques informatiques dans leurs réseaux. Cependant, dans le même chapitre, nous allons étudions les vulnérabilités et proposer des précautions qu'il faut entreprendre.

Chapitre 02

LA SECURITE DES RESEAUX INFORMATIQUES

2.1. 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. Nous allons définir dans un premier temps les notions de bases sur les réseaux informatiques tels que leurs types, leurs architectures, les différentes topologies, ensuite nous donnons un aperçu sur les différentes couches du modèle OSI et TCP/IP, nous citons aussi les protocoles de communication amenés à faire le routage des données entre les réseaux. Puis nous passons à la sécurité informatique où nous allons définir les différentes attaques et les moyens mit à la disposition pour sécuriser les données informatiques.

2.2. Généralité sur les réseaux informatiques:

2.2.1. Définition:

Un réseau informatique est un moyen de communication qui permet à des individus ou à des groupes de partager des informations et des services. Il est constitué d'un ensemble d'équipements appelés nœuds qui sont interconnectés entre eux à travers des protocoles de communication, ou des langages compréhensibles par tous. Il sert à l'échange d'informations et des ressources (Imprimantes, disques, …) [2].

2.2.2. Classification des réseaux:

Les réseaux informatiques peuvent être divisés en plusieurs types : selon leurs étendues, leurs architectures et leurs topologies [2].

2.2.2.1. Classification selon l'étendue géographique :

a) LAN (Local Area Network) ou réseau local:

C'est une Infrastructure réseau reliant les utilisateurs et les périphériques finaux dans une zone

géographique peu étendue, il s'agit généralement d'un réseau de petite ou moyenne entreprise ou d'un réseau domestique, dont le propriétaire et le gestionnaire est un individu ou un service.

b) MAN (Metropolitan Area Network):

C'est une infrastructure réseau qui couvre une zone plus vaste qu'un LAN, mais moins étendue qu'un WAN (par exemple, une ville). Les MAN sont généralement gérées par une seule entité, comme une grande entreprise.

c) WAN (Wide Area Network) ou réseau étendu:

C'est une Infrastructure réseau permettant d'accéder à d'autres réseaux au sein d'une zone géographique étendue, qui appartient généralement à un prestataire de services et dont la gestion est assurée par ce dernier.

d) PAN (Personnel Area Network) ou Réseaux personnel:

C'est une infrastructure Interconnectent sur quelques mètres des équipements personnels (tels que les terminaux : UMTS (Universal Mobile Telecommunication System), portables, organiseurs,... etc.) d'un même utilisateur.

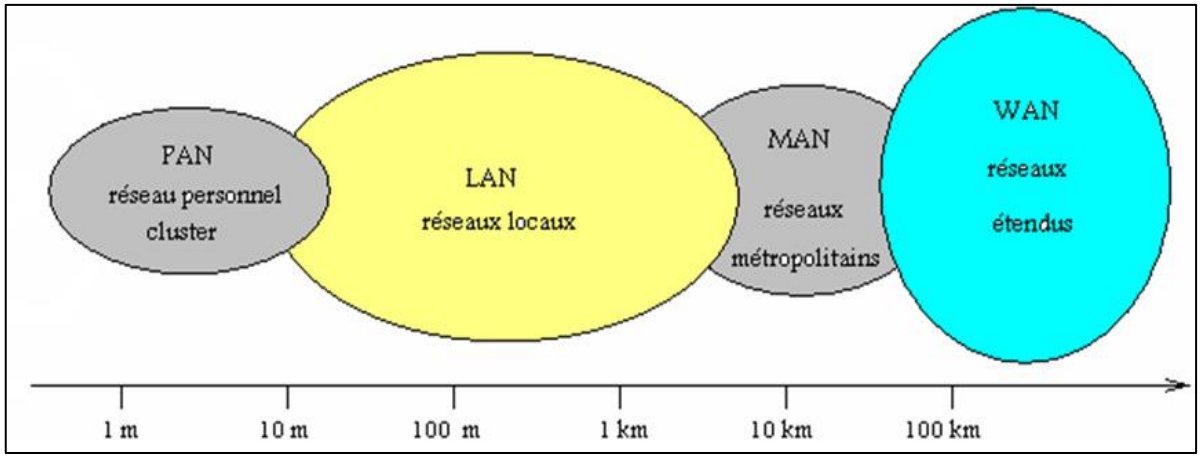


Figure 2.1 : Les différents réseaux.

2.2.2.2. Classification selon l'architecture:

On distingue généralement deux types de réseaux locaux [2] :

a) Réseau poste à poste (Peer to Peer) :

Les ordinateurs sont reliés par un support physique, chaque poste connecté peut mettre ses données et ses ressources à disposition du réseau, il peut être à la fois client et serveur; il est plus adapté aux petites structures.

Sur un réseau poste à poste, les ressources telles que les imprimantes, les fax et les modems sont généralement connectés à un même ordinateur qui les partage avec les autres ordinateurs du réseau.

Avec ce type de réseau, chaque utilisateur doit apprendre à administrer son propre ordinateur pour permettre aux autres d'y accéder ; en plus y'a un problème de sécurité des données et la personne n'aura pas accès au réseau distant ni à la messagerie internet.

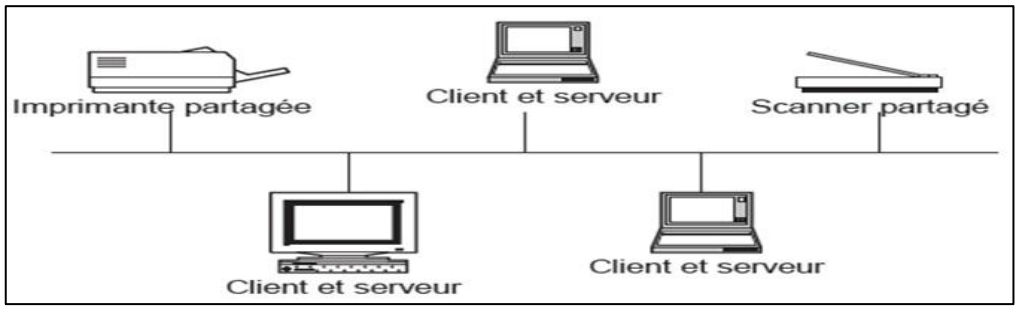


Figure 2.2 : Réseau poste à poste.

b) Réseau Client/serveur :

Dans une architecture client/serveur, parmi les machines du réseau, il y a une qui est considérée comme un serveur, elle est généralement très puissante et c'est elle qui délivre les informations (tels que la connexion) aux autres ordinateurs qui sont considérés comme des postes clients.

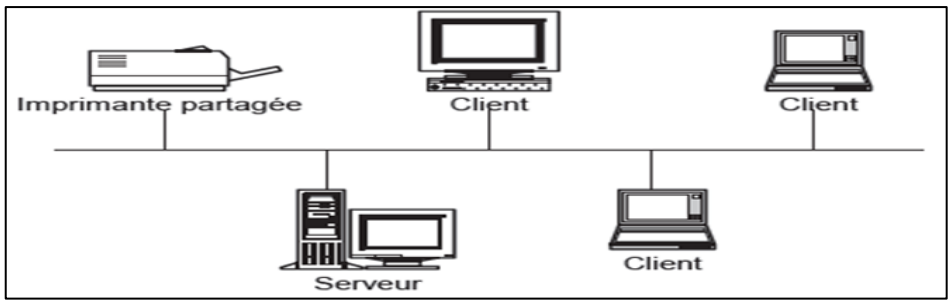


Figure 2.3 : Réseau client/serveur.

2.2.2.3. Classification selon la topologie:

On distingue deux types de topologie qui sont différentes à l'utilisation [2]:

- **Topologie physique:** Une topologie physique est en fait la structure physique de votre réseau. C'est donc la forme, l'apparence du réseau. Il existe plusieurs topologies physiques : le bus, l'étoile (la plus utilisée), le Mesh (topologie maillée), l'anneau, hybride, etc.

- **Topologie logique:** Une topologie logique est la structure logique d'une topologie physique, c'est à dire que la topologie logique définit comment se passe la communication dans la topologie physique.

2.2.3. 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 [2] :

	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 2.4 : 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.

2.2.4. 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 [2] :

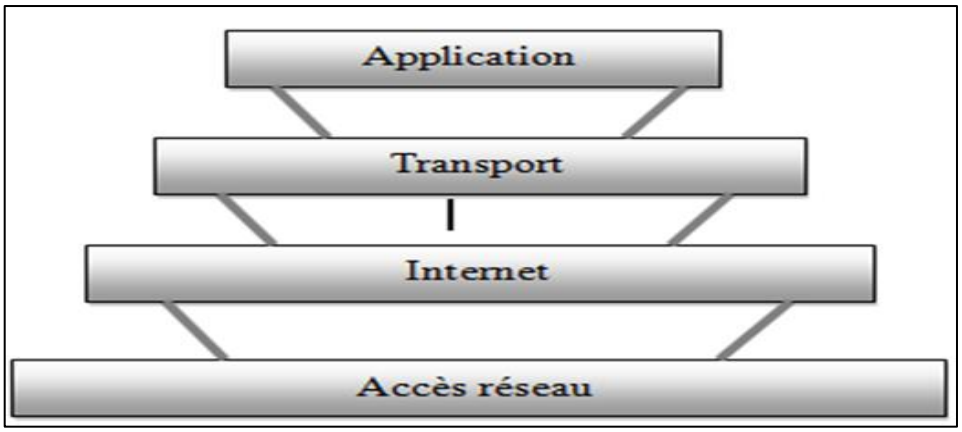


Figure 2.5 : Modèle TCP/IP.

- **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.

2.2.5. Encapsulation des données :

Lors d'une transmission, les données traversent chacune des couches au niveau de la machine émettrice. A chaque couche, une information est ajoutée au paquet de données, il s'agit d'une entête, ensemble d'informations qui garantissent la transmission. Au niveau de la machine réceptrice, lors du passage dans chaque couche, l'entête est lu, puis supprimé. Ainsi, à la réception, le message est dans son état original [2].

2.2.6. Routage IP:

C'est une fonction qui permet de déterminer le meilleur chemin dans un réseau maillé vers une destination identifiée par une adresse IP. Le routage est divisé en deux grandes familles [2]:

- **Le routage direct :**
  - Il s'agit de délivrer un datagramme à une machine raccordée au même LAN.
  - L'émetteur trouve l'adresse physique du correspondant (ARP : Address Resolution Protocol), encapsule le datagramme dans une trame et l'envoie.
- **Le routage indirect :**
  - Le destinataire n'est pas sur le même LAN comme précédemment. Il est absolument nécessaire de franchir une passerelle connue d'avance ou d'employer un chemin par défaut.
  - En effet, toutes les machines à atteindre ne sont pas forcément sur le même réseau physique. C'est le cas le plus courant, par exemple sur l'Internet qui regroupe des centaines de milliers de réseaux différents.

Cette opération est beaucoup plus délicate que la précédente, car il faut sélectionner une passerelle.

Il existe deux modes de routages bien distincts lorsque nous souhaitons aborder la mise en place d'un protocole de routage, il s'agit du routage statique et du routage dynamique.

- **Routage statique:** Dans le routage statique, les administrateurs vont configurer les routeurs un à un au sein du réseau afin d'y saisir les routes (par l'intermédiaire de port de sortie ou d'IP de destination) à emprunter pour aller sur tel ou tel réseau. Concrètement, un routeur sera un pont entre deux réseaux et le routeur d'après sera un autre pont entre deux autres réseaux.
- **Routage dynamique:** Le routage dynamique permet quant à lui de se mettre à jour de façon automatique. La définition d'un protocole de routage va permettre au routeur de se comprendre et d'échanger des informations de façon périodique ou événementielle afin que chaque routeur

soit au courant des évolutions du réseau sans intervention manuelle de l'administrateur du réseau. Concrètement, le protocole de routage fixe la façon dont les routeurs vont communiquer mais également la façon dont ils vont calculer les meilleures routes à emprunter.

2.2.7. Protocoles de communication:

Un protocole réseau est un ensemble de règles et de procédures de communication utilisées d'une part et d'autre par toutes les stations qui échangent des données sur le réseau [2].

Il existe de nombreux protocoles réseaux, mais ils n'ont pas tous, ni le même rôle, ni la même façon de procéder. Certains protocoles réseaux fonctionnent au niveau de plusieurs couches du modèle OSI, d'autres peuvent être spécialisés dans la réalisation d'une tâche correspondant à une seule couche du modèle OSI. Un paquet transmis sur le réseau est constitué de plusieurs couches d'informations correspondant aux différents traitements de chacun des protocoles de la pile [2].

- **Le 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), ou même de tout matériel de couche de liaison.

Il se situe à l'interface entre la couche réseau et la couche de liaison du modèle OSI).

- **Le protocole DHCP :**

Dynamic Host Configuration Protocol est un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station, notamment en lui affectant automatiquement une adresse IP et un masque de sous-réseau.

- **Le protocole FTP :**

File Transfer Protocol (protocole de transfert de fichier), est un protocole de communication destiné au partage de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur.

- **Le protocole HTTP :**

L'HyperText Transfer Protocol, est un protocole de la couche application. Il peut fonctionner sur n'importe quelle connexion fiable, il permet l'échange de données de différents types. Les clients HTTP les plus connus sont les navigateurs Web permettant à un utilisateur d'accéder à un serveur contenant les données.

- **Le protocole RIP :**

Routing Information Protocol est un protocole de routage IP de type vecteur de distances. Il permet à chaque routeur de communiquer aux routeurs voisins la métrique. Pour chaque réseau IP connu, chaque routeur conserve l'adresse du routeur voisin dont la métrique est la plus petite.

- **Le protocole DNS:**

Domain Name System (ou système de noms de domaine) est un service permettant d'établir une correspondance entre une adresse IP et un nom de domaine. Autrement dit, il permet aux utilisateurs d'ordinateurs clients d'utiliser des noms plutôt que des adresses IP numériques pour identifier les hôtes distants.

- **Le protocole UDP:**

User Datagram Protocol (en français protocole de datagramme utilisateur) est un des principaux protocoles de télécommunication utilisés par Internet. Il fait partie de la couche transport du modèle OSI, il appartient à la couche 4, comme TCP. Le rôle de ce protocole est de permettre la transmission de données de manière très simple entre deux entités, chacune étant définie par une adresse IP et un numéro de port.

2.3. Sécurité informatique:

2.3.1. Définition:

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Elle s'occupe de la prévention d'actions non autorisées par les utilisateurs d'un système informatique, afin d'assurer certaines notions que nous allons définir dans ce qui suit. [3]

2.3.2. Critères de la sécurité informatique :

Les objectifs d'une politique de sécurité sont de garantir la sécurité des informations et des réseaux d'entreprise. Ces impératifs peuvent être définis à plusieurs niveaux: [2]

a) L'intégrité: Consiste à déterminer si les données n'ont pas été altérées durant la communication. C'est-à-dire garantir que les données sont bien celles que l'on croit être.

b) La confidentialité: Consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées.

c) La disponibilité: L'objectif de la disponibilité est de garantir l'accès à un service ou à des ressources, permettant de maintenir le bon fonctionnement du système d'information quand les informations sont accessibles au moment voulu.

d) Non répudiation: Permettant de garantir qu'une transaction ne peut être niée. La non-répudiation de l'origine prouve que les données ont été envoyées, et la non-répudiation de l'arrivée prouve qu'elles ont été reçues.

e) L'authentification : Consistant à assurer que seules les personnes autorisées aient accès aux ressources. Elle consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre l'accès à des ressources uniquement aux personnes autorisées.

2.3.3. Terminologie de la sécurité :

La sécurité informatique utilise un ensemble de termes bien spécifique, que nous énumérons comme suit [4] :

a) 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.

b) Menace : Elle désigne l'exploitation d'une faiblesse de sécurité par un attaquant qu'il soit interne ou externe à l'entreprise.

c) 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.

d) 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.

e) 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.

2.3.4. Anatomie d'une attaque:

Fréquemment appelés "les 5P" dans la littérature, ces cinq verbes anglophones constituent le squelette de toute attaque informatique. Nous avons [5] :

1) Probe (Analyser) :

Consiste en la collecte d'information par le biais d'outils comme whois, Arin, DNS look up. La collecte d'information sur le système cible peut s'effectuer de plusieurs manières, comme un scan de ports grâce au programme Nmap ou encore un scan de vulnérabilité à l'aide du programme Nessus.

2) Penetrate (Pénétrer) :

Consiste en l'utilisation des informations récoltées pour pénétrer un réseau. Des techniques comme le brut force ou les attaques par dictionnaires peuvent être utilisées pour outrepasser les protections par mot de passe.

3) Persist (Persister) :

Consiste en la création d'un compte avec des droits de super utilisateurs pour pouvoir se réinfiltre ultérieurement. Une autre technique consiste à installer une application de contrôle à distance capable de résister à un cheval de Troie.

4) Propagate (Propager) : Cette étape consiste à observer ce qui est accessible et disponible sur le réseau local.

5) Paralyse (Paralyser) : Cette étape peut consister en plusieurs actions. Le pirate peut utiliser un serveur pour mener une attaque sur une autre machine; détruire des données ou encore endommager le système d'exploitation.

2.3.5. Types d'attaques :

Il existe deux types d'attaques, les attaques réseaux et les attaques applicatives :

2.3.5.1. Attaques 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 [5] :

- **Les techniques de scan :** Le scan de ports est une méthode pour déterminer le type d'attaque que l'on peut lancer sur une machine cible. Cette technique consiste à rapporter des informations sur la machine scannée, et en particulier le système d'exploitation et les services installés. On peut donc déterminer avec précision les failles de sécurité et donc les types d'attaques possibles sur la machine.

- **IP Spoofing :** Le Spoofing consiste à se faire passer pour un autre système en falsifiant son adresse IP. Le pirate commence par choisir le système qu'il veut attaquer. Après avoir obtenu le maximum de détails sur ce système cible, il détermine les systèmes ou adresses IP autorisés à se connecter au système cible. Le pirate attaque ensuite le serveur cible en utilisant l'adresse IP falsifiée.

- **ARP Spoofing :** Le but de cette attaque est de rediriger le trafic d'une machine vers une autre. Grace à cette redirection, une personne mal attentionnée peut se faire passer pour une autre. De plus, le pirate peut ré-router les paquets qu'il reçoit vers les véritables destinataires, ainsi l'utilisateur usurpé ne se rendra compte de rien.

- **DNS Spoofing :** Le but de cette attaque est de fournir de fausses réponses aux requêtes DNS c'est-à-dire indiquer une fausse adresse IP pour un nom de domaine afin de rediriger, à leur insu, des internautes vers des sites pirates. Grace à cette fausse redirection, l'utilisateur peut envoyer ses informations en toute confiance telle que les identifiants.

- **Fragments attaques :** Le but de cette attaque est de passer outre les protections des équipements de filtrage IP. Dans ce cas un pirate peut s'infiltrer dans un réseau pour effectuer des attaques ou récupérer des informations confidentielles.

- **Sniffing :** Le Sniffing ou reniflement de trafic constitue l'une des méthodes couramment utilisée par les pirates informatiques pour espionner le trafic sur le réseau. Dans la pratique, les hackers font généralement recours à ce procédé, pour détecter tous les messages circulant sur le réseau en récupérant des mots de passe et des données sensibles.

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

2.3.5.2. Attaques applicatives:

- **Injection SQL :** Les attaques par injection de command SQL sont des attaques visant les sites web, elles s'appuient sur des bases de données, 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 (Ex : des mots de passe) ou encore de détruire des données [5] :

- **Scripts :** Principalement Web (Ex : PHP HyperText Preprocessor), ils s'exécutent sur un serveur et renvoient un résultat au client. Cependant, lorsqu'ils sont dynamiques (i.e. Qu'ils utilisent des entrées saisies par un utilisateur), des failles peuvent apparaître si les entrées ne sont pas correctement contrôlées. [5]

- **Les problèmes de configuration :** Il est très rare que les administrateurs réseau configurent correctement un programme. En général, ils se contentent d'utiliser les configurations par défaut. Celles-ci sont souvent non sécurisées afin de faciliter l'exploitation du logiciel [5] :

- **Les bugs :** Liés à un problème dans le code source, ils peuvent amener à l'exploitation de failles. Il n'est pas rare de voir l'exploitation d'une machine bloquée suite à une simple erreur de programmation. On ne peut toutefois rien faire contre ce type de problèmes, si ce n'est attendre un correctif de la part du développeur.

- **Man in the middle :** L'attaque « man in the middle » littéralement « attaque de l'homme au milieu », est un scénario d'attaque dans lequel un pirate écoute une communication entre deux interlocuteurs et falsifie éventuellement les échanges à leur insu [5].

2.3.6. Logiciels malveillants :

- **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 [6].

- **Ver :** 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 [6].

- **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 [6].

- **Les logiciels d'espions :** Ce sont des logiciels qui facilitent la collecte d'informations, ils peuvent surveiller et consigner les activités se déroulant sur un système cible [6].

- **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 (par exemple les options qu'il a coché) afin de lui éviter de les ressaisir. Mais certain cookies sont utilisés par des personnes malintentionnées à des fins malicieuses [6].

- **Porte dérobé :** Une porte dérobé (backdoor) est un logiciel de communication cachée, Il permet à un utilisateur externe de prendre le contrôle d'une ordinateur à distance, Les portes dérobées sont effectuées par les chevaux de Troie une fois lancés pour ouvrir toutes grandes les portes de l'ordinateur attaqué [6].

2.3.7. Protocoles de sécurité :

a. Le protocole PPP:

Le protocole le plus utilisé pour les accès à Internet par modem. Le protocole Point à Point (PPP) propose une méthode standard pour le transport de datagrammes multi-protocoles sur une liaison simple point à point [7].

Il comprend trois composants principaux:

- Une méthode pour encapsuler les datagrammes de plusieurs protocoles.
- Un protocole de contrôle du lien "Link Control Protocol" (LCP) destiné à établir, configurer, et tester la liaison de données.
- Une famille de protocoles de contrôle de réseau "Network Control Protocol" (NCP) pour l'établissement et la configuration de plusieurs protocoles de la couche réseau.

b. Le protocole PPTP:

Le protocole PPTP (Point To Point Tunneling Protocol) est issu des travaux de Microsoft et 3Com. PPTP permet aux connexions PPP d'être convoyées au travers d'un réseau IP. Microsoft a implémenté ses propres algorithmes et protocoles afin d'intégrer PPTP dans ses systèmes d'exploitation [7].

c. Le protocole IPSec:

IPSec (Internet Protocol Security) est un standard de l'IETF (Internet Engineering Task Force) qui définit une extension de sécurité pour le protocole IP afin de permettre la sécurisation des données échangées sur les réseaux basés sur ce protocole. Basé sur des mécanismes cryptographiques, IPSec s'insère dans la pile protocolaire TCP / IP au niveau d'IP. Cela signifie qu'il agit sur chaque paquet émis ou reçu et peut soit le laisser passer sans traitement particulier, soit le rejeter, soit lui appliquer un mécanisme de sécurisation.

IPSEC fournit trois principaux mécanismes de sécurité :

- Confidentialité et protection contre l'analyse du trafic.
- Authenticité des données et contrôle d'accès continu.
- Protection contre le rejeu.

Les services de sécurité d'IPSEC sont fournis au travers de deux extensions du protocole IP appelées AH (*Authentication Header*) et ESP (*Encapsulating Security Payload*).

- **Authentication Header AH:** est conçu pour assurer l'authenticité des paquets IP sans chiffrement des données. Le principe d'AH est d'adjoindre aux paquets IP un champ supplémentaire permettant à la réception de vérifier l'authenticité des données. Un numéro de séquence permet de détecter les tentatives de rejeu.

- **Encapsulation Security Payload ESP:** a pour rôle premier d'assurer la confidentialité des données mais peut aussi être utilisé pour assurer l'authenticité de celles-ci. Le principe d'ESP consiste à encapsuler dans un nouveau paquet IP le paquet d'origine mais sous une forme chiffrée. L'authenticité des données peut être obtenue par l'ajout d'un bloc d'authentification et la protection contre le rejeu par celui d'un numéro de séquence [7].

d. Le protocole HTTPS :

L'HyperText Transfer Protocol Secure est la combinaison du HTTP avec une couche de chiffrement comme SSL.

HTTPS permet au visiteur de vérifier l'identité du site web auquel il accède, grâce à un certificat d'authentification émis. Il garantit théoriquement la confidentialité et l'intégrité des données envoyées par l'utilisateur (notamment des informations entrées dans les formulaires) et reçues du serveur. Pour cela, il fait usage de méthodes de cryptographie asymétrique pour l'authentification et de méthode de cryptographie symétrique pour le chiffrement des échanges [7].

e. Le protocole SSH :

Secure Shell est un protocole qui facilite les connexions sécurisées entre deux systèmes à l'aide d'une architecture client/serveur et permet aux utilisateurs de se connecter à distance à des systèmes hôte de serveurs. Toutefois, contrairement à d'autres protocoles de communication à distance, tels que FTP ou Telnet, SSH crypte la session de connexion et empêche ainsi tout agresseur de recueillir des mots de passe non-cryptés [7].

2.3.8. Dispositif de Sécurité:

a) Firewall (pare-feu): Un firewall est outil informatique (matériel et/ou logiciel) conçu pour protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet par exemple, ou protection d'un réseau d'entreprise).Il permet d'assurer la sécurité des informations d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur [8].

b) VPN (Virtual Private network) : Est un service qui permet à un ou plusieurs postes distants d'établir des connexions privées sécurisées dans le réseau publique comme internet pour

communiquer de manière sure. Ce type de liaison est apparu suite à un besoin croissant des entreprises de relier les différents sites.

c) IDS (Intrusion Detection System): Nous appelons un 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 [9].

d) IPS (Intrusion Prevention System): Les systèmes de prévention d'intrusions sont des systèmes de détection d'intrusions particuliers qui permettent, en plus de repérer les tentatives d'intrusion à un système, d'agir pour contrer ces tentatives. En effet, les IPS constituent des IDS actifs qui tentent de bloquer les intrusions [9].

e) DMZ (Demilitarized Zone): DMZ est une interface située entre un segment de réseau connu (réseau interne) et un segment inconnu (réseau internet) .Une série de règles de connexion configurées sur le pare-feu de cette interface ; une zone physiquement isolée entre les deux réseaux. Cette séparation physique permet d'autoriser les accès internet à destination des serveurs placés dans la DMZ et non à ceux destinés au réseau privé.

f) VLAN (Virtual Local Area Network): Un VLAN est un réseau local regroupant un ensemble de machines de façon logique et non physique. Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc...) [10].

g) Proxy : Le proxy est un ordinateur faisant office de passerelle entre le réseau d'un particulier ou d'une entreprise et internet, il fait office de firewall pour tout le réseau, ce qui en fait une sécurité de plus en cas d'attaque, il sert de mémoire cache, téléchargeant les pages web visitées par les utilisateurs du réseau local, ce qui permet de les exécuter ensuite à partir du proxy et non du serveur distant qui héberge le site [10].

2.4. Conclusion :

Dans ce chapitre, nous avons donnés en premier lieu les différentes notions de base de réseau informatique. En second lieu nous avons exposés certains types d'attaques qui s'introduire dans le système, ainsi les contre-mesures et les protocoles de sécurité du réseau.

Dans le chapitre suivant, nous allons étudier les méthodes et techniques des systèmes de détection et de prévention d'intrusions qui permettent de prendre le contrôle d'une machine et assurer sa protection.

Chapitre 03

LES SYSTEMES DE DETECTION ET DE PREVENTION D'INTRUSION

3.1. Introduction:

C'est bien d'avoir un système qui joue un rôle pour surveiller la circulation des données échangées entre le réseau de l'entreprise et le réseau externe, et qui serait capable de réagir en temps réel si des données semblent suspectes. Les systèmes de détection et de prévention d'intrusions (IDS/IPS) conviennent parfaitement pour réaliser ces tâches.

Dans ce chapitre nous donnerons d'abord un aperçu sur les systèmes de détection et de prévention d'intrusion telle que leurs types, leurs fonctionnements ainsi que leurs architectures, ensuite nous évoquerons quelques points forts et faibles et les différences majeur entre ces deux systèmes. Enfin, nous allons choisir Snort comme un système de sécurité pour détecter et répondre aux attaques et intrusions prévenantes de l'extérieur, et c'est bien sûr pour plusieurs raisons qui le distinguent et en font un moyen efficace de protéger les réseaux internes.

3.2. Système de détection d'intrusion:

3.2.1. Définition:

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 [11].

3.2.2. Différents types de systèmes détection d'intrusions :

3.2.2.1. Systèmes de détection d'intrusions réseau (NIDS):

Les IDS réseaux (Network IDS) analysent en temps réel le trafic qu'ils aspirent à l'aide d'une sonde (carte réseau en mode "promiscuous 1 "). Ensuite, les paquets sont décortiqués puis analysés. Il est

fréquent de trouver plusieurs IDS sur les différentes parties du réseau. On trouve souvent une architecture composée d'une sonde placée à l'extérieur du réseau afin d'étudier les tentatives d'attaques et d'une sonde en interne pour analyser les requêtes ayant traversé le pare-feu [12].

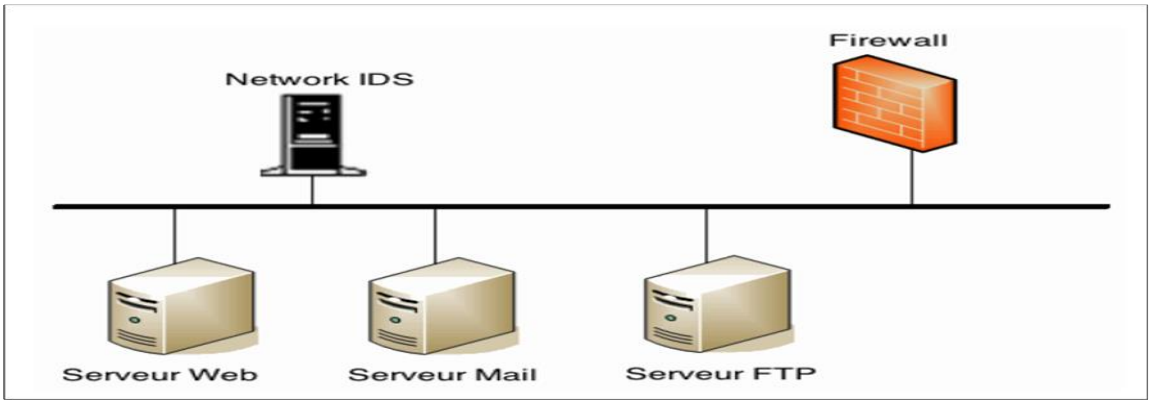


Figure 3.1 : l'architecture de NIDS.

- **Les avantages des NIDS :**
  - ✓ L'IDS basé réseau est capable de contrôler un grand nombre d'hôtes avec un petit coût de déploiement.
  - ✓ Il n'influence pas sur les performances des entités surveillées.
  - ✓ L'IDS basé réseau assure une grande sécurité contre les attaques parce qu'il est invisible aux attaquants.
  - ✓ Il peut capturer le contenu de tous les paquets envoyés à un système cible.
  - ✓ Les NIDS sont des systèmes à temps réels [12].
- **Les inconvénients des NIDS:**
  - ✓ L'IDS basé réseau ne peut pas fonctionner dans des environnements cryptés. Sauf si l'on dispose des clés de déchiffrement, ce qui reste probable.
  - ✓ Ce type d'IDS ne permet pas d'assurer si une tentative d'attaque est couronnée de succès.
  - ✓ Il faut des configurations spéciales sur les réseaux pour que les NIDS puissent voir tout le trafic [12].
- **L'emplacement des NIDS:**

Les capteurs places à l'extérieure du pare-feu servent à détecter toutes les attaques en direction du réseau, leur tâche ici est donc plus de contrôler le fonctionnement et la configuration du firewall que

d'assurer une protection contre toutes les intrusions détectées (certaines étant traitées par le firewall). Il est également possible de placer un capteur avant le firewall et un autre après le firewall [12].

Quelques exemples des NIDS: Net Ranger, Dragon, NFR, Snort, DTK…etc.

3.2.2.2. Systèmes de détection d'intrusions hôte (HIDS):

Les IDS hôte permet d'analyser, non seulement, le trafic réseau, mais aussi l'activité se passant sur la machine. Le but de ce type d'IDS est d'assurer l'intégrité des données d'un système et analyser le flux relatif à une machine ainsi que ces journaux. Il existe plusieurs solutions qui proposent cette fonctionnalité, par exemple les HIDS Samhain ou Tripwire [2].

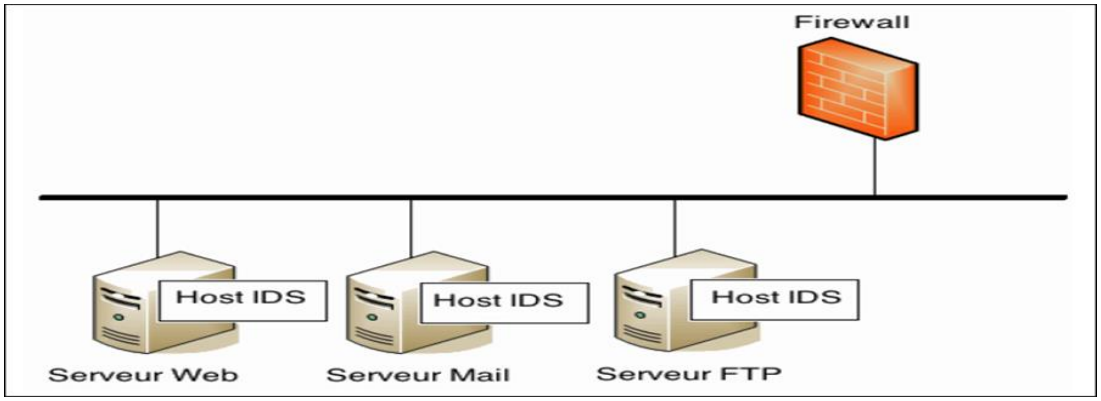


Figure 3.2 : l'architecture de HIDS.

- **Les avantages des HIDS:**
  - ✓ La capacité de contrôler les activités locales des utilisateurs avec précision.
  - ✓ Capable de déterminer si une tentative d'attaque est couronnée de succès.
  - ✓ La capacité de fonctionnement dans des environnements cryptés.
  - ✓ L'IDS basé hôte fonctionne sur les traces d'audit des systèmes d'exploitation, ce qui lui permet de détecter certains types d'attaques (Ex : Cheval de Troie) [12].
- **Les inconvénients des HIDS :**
  - ✓ La vulnérabilité aux attaques de type déni de service, puisque l'IDS peut résider dans l'hôte cible par les attaques.
  - ✓ La difficulté de déploiement et de gestion, surtout lorsque le nombre d'hôtes qui ont besoin de protection est large.
  - ✓ Ces systèmes sont incapables de détecter des attaques contre de multiples cibles dans le réseau.

- ✓ Ils peuvent être identifié et mis hors service par un attaquant [12].

- **L'emplacement des HIDS:**

Les HIDS sont en général places sur des machines sensibles, susceptibles de subir des attaques et possédantes des données sensibles pour l'entreprise. Les serveurs web et applicatifs, peuvent notamment être protèges par un HIDS [12].

3.2.2.3. IDS hybrids (NIDS+HIDS):

Les IDS hybrides rassemblent les caractéristiques de plusieurs IDS différents. En pratique, on ne retrouve que la combinaison de NIDS et HIDS. Ils permettent, en un seul outil, 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 agréger ou lier les informations d'origines multiples.[12]

3.3. Architecture d'un IDS:

Cette section décrit les trois composants qui constituent classiquement un système de détection d'intrusions. La figure suivante illustre les interactions entre ces trois composants :

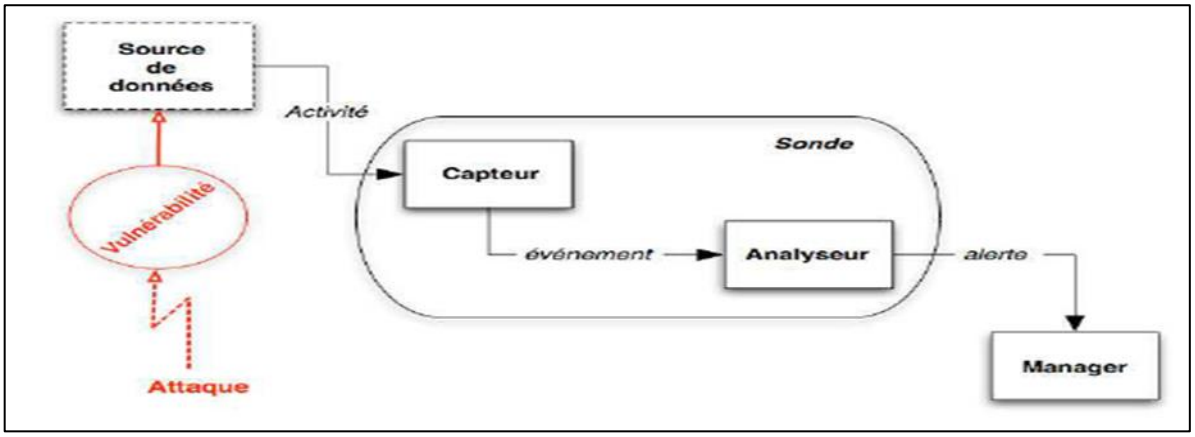


Figure 3.3 : L'architecture de l'IDS.

3.3.1. Capteur :

Les capteurs transmettent des informations aux agents (parfois également appelés analyseurs), qui surveillent les activités intrusives sur leurs hôtes individuels. Sont généralement (mais pas toujours) les composants les plus bas de gamme. En d'autres termes, les capteurs n'ont généralement pas de fonctionnalités très sophistiquées. Ils sont généralement conçus uniquement pour obtenir certaines données et les transmettre [13].

On distingue classiquement 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 applicative.

3.3.2. Agent (Analyseur):

Leur fonction principale est d'analyser les entrées fournies par les capteurs. Un agent est un groupe de processus qui s'exécutent indépendamment et qui sont programmés pour analyser le comportement du système ou les événements du réseau ou les deux pour détecter les événements anormaux et les violations de la politique de sécurité d'une organisation.

Un agent doit intégrer trois fonctions ou composants :

- Une interface de communication pour communiquer avec d'autres composants des IDS.
- Un écouteur qui attend en arrière-plan les données des capteurs et les messages des autres agents, puis les reçoit.
- Un expéditeur qui transmet des données et des messages à d'autres composants, tels que d'autres agents et le composant gestionnaire [13].

3.3.3. Manager (Gestionnaire):

Le manager est responsable de la présentation des alertes à l'opérateur (fonction de console de management). Il peut également réaliser les fonctions de corrélation d'alertes, dans la mesure de leur disponibilité. Enfin, il peut assurer le traitement de l'incident, par exemple au travers des fonctions suivantes:

- Confinement de l'attaque, qui a pour but de limiter les effets de l'attaque.
- éradication de l'attaque, qui tente d'arrêter l'attaque.
- Recouvrement, qui est l'étape de restauration du système dans un état sain.
- Diagnostic, qui est la phase d'identification du problème, de ses causes et qui peut éventuellement être suivi d'actions contre l'attaquant (fonction de réaction) [13].

3.4. Mode de fonctionnement :

Le mode de fonctionnement d'un IDS est basé sur deux aspects: le mode de détection utilisé et la réponse apportée par l'IDS lors de la détection d'une intrusion.

Il existe deux modes de détection, la détection d'anomalies et la reconnaissance de signatures. D'eux-mêmes, deux types de réponses existent, la réponse passive et la réponse active [14].

3.4.1. Mode de détection:

Nous notons deux modes de détection qui sont :

→ La détection d'anomalies.

→ La reconnaissance de signature.

Il faut noter que la reconnaissance de signature est le mode de fonctionnement le plus implémenté par les IDS du marché. Cependant, les nouveaux produits tendent à combiner les deux méthodes pour affiner la détection d'intrusion.

A. La détection d'anomalies :

Elle consiste à détecter des anomalies par rapport à un profil "de trafic habituel". La mise en œuvre comprend toujours une phase d'apprentissage au cours de laquelle les IDS vont découvrir le fonctionnement normal des éléments surveillés. Les modèles comportementaux peuvent être élaborés à partir d'analyses statistiques. Ils présentent l'avantage de détecter des nouveaux types d'attaques. Cependant, de fréquents ajustements sont nécessaires afin de faire évoluer le modèle de référence de sorte qu'il reflète l'activité normale des utilisateurs et réduire le nombre de fausses alertes générées.

B. La reconnaissance de signatures :

Cette approche consiste à rechercher dans l'activité de l'élément surveillé les empreintes (ou signatures) d'attaques connues. Ce type d'IDS est purement réactif ; il ne peut détecter que les attaques dont il possède la signature. De ce fait, il nécessite des mises à jour fréquentes. De plus, l'efficacité de ce système de détection dépend fortement de la précision de sa base de signature. C'est pourquoi ces systèmes sont contournés par les pirates qui utilisent des techniques dites "d'évasion" qui consistent à maquiller les attaques utilisées. Ces techniques tendent à faire varier les signatures des attaques qui ainsi ne sont plus reconnues par l'IDS.

Il est possible d'élaborer des signatures plus génériques, qui permettent de détecter les variantes d'une même attaque, mais cela demande une bonne connaissance des attaques et du réseau.

Une signature permet de définir les caractéristiques d'une attaque, au niveau des paquets (jusqu'à TCP ou UDP) ou au niveau des protocoles (HTTP, FTP...).

- **Au niveau paquet :** l'IDS va analyser les différents paramètres de tous les paquets transitant et les comparer avec les signatures d'attaques connues.

- **Au niveau protocole:** l'IDS va vérifier au niveau du protocole si les commandes envoyées sont correctes ou ne contiennent pas d'attaque. Cette fonctionnalité a surtout été développée pour HTTP actuellement.

Il faut savoir que les signatures sont mises à jour en fonction des nouvelles attaques identifiées. Néanmoins, plus il y a de signatures différentes à tester, plus le temps de traitement sera long. L'utilisation de signatures plus élaborées peut donc procurer un gain de temps appréciable. Cependant, une signature mal élaborée peut ignorer des attaques réelles ou identifiées du trafic normal comme étant une attaque.

Une fois une attaque détectée, un IDS a le choix entre plusieurs types de réponses, que nous allons maintenant détailler.

3.4.2. Réponses actives et passives :

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

A. Réponse passive:

La réponse passive d'un IDS consiste à enregistrer les intrusions détectées dans un fichier de log qui sera analysé par le responsable de sécurité. Certains IDS permettent de logger l'ensemble d'une connexion identifiée comme malveillante. Ceci permet de remédier aux failles de sécurité pour empêcher les attaques enregistrées de se reproduire, mais elle n'empêche pas directement une attaque de se produire.

B. Réponse active:

La réponse active au contraire a pour but de stopper une attaque au moment de sa détection. Pour cela on dispose de deux techniques : la reconfiguration du firewall et l'interruption d'une connexion TCP.

La reconfiguration du firewall permet de bloquer le trafic malveillant au niveau du firewall, en fermant le port utilisé ou en interdisant l'adresse de l'attaquant. Cette fonctionnalité dépend du modèle de firewall utilisé, tous les modèles ne permettant pas la reconfiguration par un IDS. De plus, cette reconfiguration ne peut se faire qu'en fonction des capacités du firewall. L'IDS peut également interrompre une session établie entre un attaquant et sa machine cible, de façon à empêcher le transfert de données ou la modification du système attaqué.

Pour cela l'IDS envoie un paquet TCP reset aux deux extrémités de la connexion (cible et attaquant). Un paquet TCP reset a le flag RST de positionné, ce qui indique une déconnexion de deux extrémités

de la connexion. Chaque extrémité en étant destinataire, la cible et l'attaquant pensent que l'autre extrémité s'est déconnectée et l'attaque est interrompue.

3.5. Points forts et faibles d'un IDS:

3.5.1. Points forts:

Le positionnement des sondes réseaux de l'IDS et la configuration des interfaces réseaux, joue un rôle majeur sur l'étude de l'efficacité des protections mises en place, et avoir des avantages indispensable, comme [15] :

- ✓ L'invisibilité des dispositifs pour les attaquants.
- ✓ Conçu pour la surveillance continue sur le réseau.
- ✓ Diminue le travail manuel de la sécurité, en réduisant le coût dans les entreprises.
- ✓ Les systèmes de détection d'intrusions peuvent analyser tout le trafic.
- ✓ 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.
- ✓ Contient des outils de filtrage très intéressants qui nous permettent de faire du contrôle par protocole (ICMP (Internet Control Message Protocol), TCP, UDP), adresse IP, suivi de connexion.

3.5.2. Points faible:

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.

Nous trouvons d'autres points faibles, et sont classées comme suit [15] :

- ➢ **Besoin de connaissances en sécurité:**
  - ◆ La mise en place de sonde sécurité fait appel à de bonnes connaissances en sécurité.
  - ◆ L'exploitation des remontées d'alertes nécessite des connaissances plus pointues.

- La configuration, et l'administration des IDS nécessitent beaucoup de temps, et de connaissances.

➢ **Problème de positionnement des sondes :**

- Avec fonctionnement en mode promiscuité. Les sondes captent tout le trafic, et même si un Ping flood, les sondes NIDS le captureront aussi et donc en subiront les conséquences, comme si l'attaque leur était directement envoyée.
- L'archivage de contenu des trames ayant levées une alerte, vont faire exploser la taille des fichiers de logs des sondes en quelques minutes.

➢ **Problèmes intrinsèques à la plateforme :**

- Beaucoup d'IDS sont des logiciels reposant sur un système d'exploitation non dédié aux IDS.
- Une saturation de la mémoire, de la carte réseau, ou du processeur porte atteinte directement au bon fonctionnement de tout le système.

3.6. Méthodes de détections :

Plusieurs approches de détection d'intrusion sont utilisées par l'IDS (conjointement ou exclusivement). Les méthodologies qui vont être traitées dans le cadre de ce projet sont les méthodes basées signatures et les méthodes comportementales:

3.6.1. Approche par scénario (mésuse détection):

Une signature représente le scénario d'une attaque. Cette approche consiste à rechercher dans l'activité de l'élément surveillé (un flux réseau) les empreintes d'attaques connues, à l'instar des anti-virus. Trois familles de méthodes sont utilisées par les IDS à signature qui se basent tous sur la recherche d'un profil connu d'attaque [12] :

Plusieurs analyses peuvent être utilisées pour la méthode de détection par scénario:

- **Systèmes Experts:**

  Un système expert est un système basé sur trois types de règles. Le premier type sert à coder ce qui est suspect à priori (par rapport à la politique de sécurité mise en œuvre). Un deuxième type qui concerne les failles et les vulnérabilités connus d'un système et qui sont, en général, publiés par des organismes internationaux (comme le CERT ou Computer Emergency Response Team). Le dernier type est utilisé pour coder le savoir-faire de l'administrateur réseau [12] :

- **Recherche de motifs (Pattern Matching):**

Cette méthode consiste à identifier dans les paquets analysés une suite d'événements ou de caractéristiques d'une attaque connue. En fait, Le trafic réseau peut être vu comme une chaîne de caractères principale et les scénarios d'attaque comme des sous-suites qu'on veut identifier [12].

3.6.2. Approche comportementale (Anomalie Detection) :

Cette technique consiste à détecter une intrusion en fonction du comportement passé de l'utilisateur. Pour cela, il faut préalablement dresser un profil utilisateur à partir de ses habitudes et déclenche une alerte lorsque des événements hors profil se produisent. Cette technique peut être appliquée non seulement à des utilisateurs, mais aussi à des applications et services. Plusieurs métriques sont possibles : la charge CPU, le volume de données échangées, le temps de connexion sur des ressources, la répartition statistique des protocoles et applications utilisés, les heures de connexion...etc. Cependant elle possède quelques inconvénients :

- ✓ **Peu fiable:** tout changement dans les habitudes de l'utilisateur provoque une alerte.
- ✓ **Nécessite une période de non-fonctionnement:** pour mettre en œuvre les mécanismes d'auto-apprentissage: si un pirate attaque pendant ce moment, ses actions seront assimilées à un profil utilisateur, et donc passeront inaperçues lorsque le système de détection sera complètement mis en place.
- ✓ **L'établissement du profil doit être souple:** afin qu'il n'y ait pas trop de fausses alertes : le pirate peut discrètement intervenir pour modifier le profil de l'utilisateur afin d'obtenir après plusieurs jours ou semaines, un profil qui lui permettra de mettre en place son attaque sans qu'elle ne soit détectée [12].

Plusieurs approches peuvent être utilisées pour la méthode de détection comportementale [12] :

- **Approche probabiliste :**

  Des probabilités sont établies permettant de représenter une utilisation courante d'une application ou d'un protocole. Toute activité ne respectant pas le modèle probabiliste provoquera la génération d'une alerte.

- **Approche statistique :**

  Le but est de quantifier les paramètres liés à l'utilisateur : taux d'occupation de la mémoire, utilisation des processeurs, valeur de la charge réseau, nombre d'accès à l'Intranet par jour, vitesse de frappe au clavier, sites les plus visités… etc

Cette méthode est très difficile à mettre en place. Elle n'est actuellement présente que dans le domaine de la recherche, où les chercheurs utilisent des réseaux neuronaux pour tenter d'avoir des résultats convaincants.

3.7. 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 [16]:

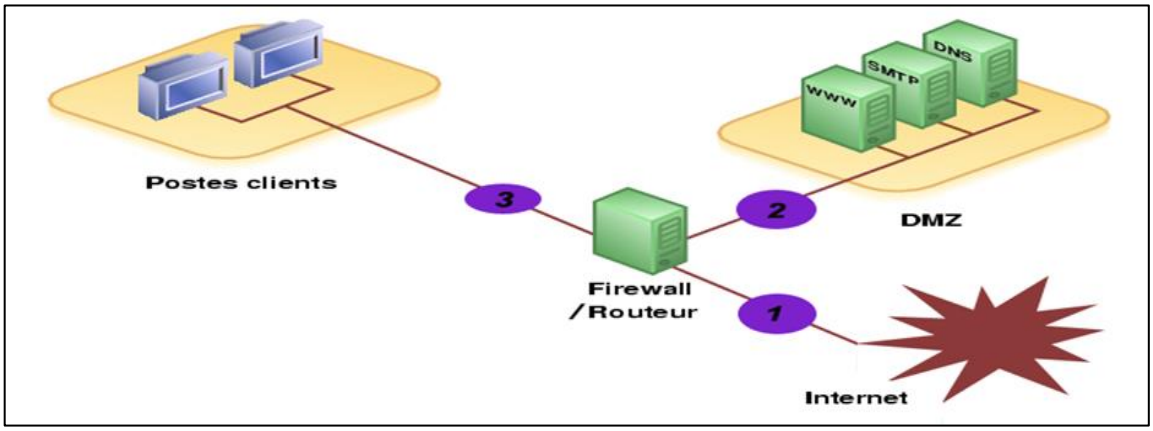


Figure 3.4 : Positionnement de L'IDS.

- **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% des attaques proviennent de l'intérieur.

3.8. Critères de choix d'un IDS:

Les systèmes de détection d'intrusion sont devenus indispensables lors de la mise en place d'une infrastructure de sécurité opérationnelle. Ils s'intègrent donc toujours dans un contexte et dans une architecture imposants des contraintes très diverses. Certains critères (toujours en accord avec le contexte de l'étude) peuvent être dégagés:

- ✓ **Fiabilité :** Les alertes générées doivent être justifiées et aucune intrusion ne doit pouvoir lui échapper [17].
- ✓ **Réactivité:** Un IDS doit être capable de détecter les nouveaux types d'attaques le plus rapidement possible, pour cela il doit rester constamment à jour [17].
- ✓ **Facilité de mise en œuvre et adaptabilité :** Un IDS doit être facile à mettre en œuvre et surtout s'adapter au contexte dans lequel il doit opérer ; il est inutile d'avoir un IDS émettant des alertes en moins de 10 secondes si les ressources nécessaires à une réaction ne sont pas disponibles pour agir dans les mêmes contraintes de temps [17].
- ✓ **Performance:** la mise en place d'un IDS ne doit en aucun cas affecter les performances des systèmes surveillés. De plus, il faut toujours avoir la certitude que l'IDS a la capacité de traiter toute l'information à sa disposition car dans le cas contraire il devient trivial de masquer les attaques en augmentant la quantité d'information [17].
- ✓ **Multicanal:** Un bon IDS doit pouvoir utiliser plusieurs canaux d'alerte (email, pager, téléphone, fax...) afin de pouvoir garantir que les alertes seront effectivement émises [12].
- ✓ **Classification:** il doit être aisé de hiérarchiser la gravité des attaques détectées afin d'adapter le mode d'alerte [12].

3.9. Définition d'IPS:

Un système de prévention d'intrusions (IPS) est un composant logiciel et/ou matériel dont la fonction principale est d'empêcher toute activité suspecte détectée au sein d'un système. Les IPS rejettent de façon proactive les paquets réseau en fonction d'un profil de sécurité si ces paquets représentent une menace connue. En effet, le concept d'IPS avant tout été conçu pour lever les limitations des IDS en matière de réponses passives à des attaques. Il ne s'agit plus seulement de détecter une attaque en cours, mais d'empêcher que celle-ci puisse seulement débuter [18].

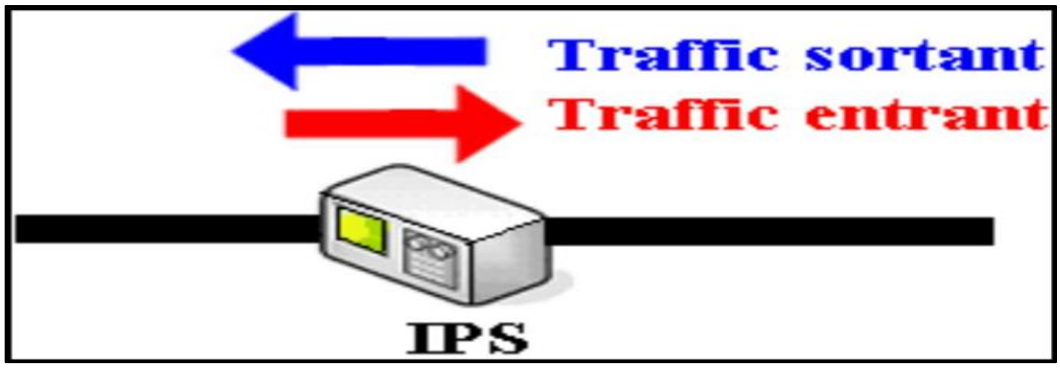


Figure 3.5 : Emplacement d'un IPS au niveau d'un système informatique.

3.9.1. Différents types d'IPS:

Comme pour les IDS, les IPS peuvent être orientés hôtes (Host IPS) ou réseaux (Network IPS). Mais, il n'existe pas d'IPS destiné à surveiller une application.

- **IPS orienté hôte (HIPS) :** un IPS basé hôte est un agent installé sur le système bloquant les comportements anormaux tels que la lecture ou l'écriture de fichiers protégés, l'accès à des ports non autorisés, une tentative de débordement de pile, un accès à certaines zones de la base de registres. Les HIPS sont en général placés sur des machines sensibles, susceptibles de subir des attaques et possédantes des données importantes pour l'entreprise [18].
- **IPS orienté réseau (NIPS) :** Le rôle d'un IPS basé réseau est d'analyser les paquets circulant dans le réseau. La principale différence entre un NIDS et NIPS tient principalement en deux caractéristiques. Le positionnement en coupure sur le réseau du NIPS, et non plus seulement en écoute comme pour le NIDS et la possibilité de bloquer immédiatement les intrusions quel que soit le type de protocole de transport utilisé et sans reconfiguration d'un équipement tierce. Ce qui induit que le NIPS est constitué d'une technique de filtrage de paquets et de moyens de blocage [18].

3.9.2. Architecture fonctionnelle d'IPS:

Le fonctionnement d'un IPS est similaire à celui d'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 réagit automatiquement sans l'intervention de l'utilisateur, et 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 [19].

L'IPS détecte et produit des alertes en raison d'un certain nombre des facteurs qui sont classifiées dans une des limites suivantes [19] :

- **Vrai positif :** Une situation dans laquelle une signature met le feu correctement quand le trafic intrusif est détecté sur le réseau, ceci représente l'opération normale et optimale.
- **Faux positif :** Une situation dans laquelle d'utilisation d'une activité normale déclenche une alerte ou une réponse, ceci représente une erreur.
- **Vrai négatif :** Une situation dans laquelle une signature ne met pas un signe pendant l'utilisation normal de trafic sur le réseau. Aucune activité malveillante. Ceci représente une opération normale et optimale.

- **Faux négatif :** Une situation dans laquelle le système de détection ne détecte pas le trafic intrusif bien qu'il y a une activité malveillante, mais le système de sécurité ne réagit pas, dans ce cas représente une erreur.

3.9.3. Points forts :

- ✓ La plupart des logiciels IPS sont multiplateformes (Linux, FreeBSD, Windows ... etc.).
- ✓ 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.
- ✓ La liberté de création des règles pour les actions à exécuter.
- ✓ Cette approche fait interagir des technologies hétérogènes : pare-feu, VPN (Virtual Protocol Network), IDS, antivirus, anti-spam, etc.
- ✓ Peut détecter des attaques sur plusieurs différents types des logiciels d'exploitation et d'applications, selon l'ampleur de sa base de données.
- ✓ Un simple dispositif peut analyser le trafic et sécurisé un large réseau [19].

3.9.4. Points faibles:

- ✓ L'IPS peuvent couper les connexions suspectes ou même, pour une attaque externe, reconfigurer le pare-feu pour qu'il refuse tout ce qui vient du site incriminé. Toutefois, il apparaît que ce type de fonctionnalité automatique est potentiellement dangereux car il peut mener à des dénis de service provoqués par l'IDS. Il est préférable de proposer une réaction facultative à un opérateur humain (qui prend la décision finale).
- ✓ La consommation des ressources (mémoire, CPU).
- ✓ Paralyse le réseau (Faux positif) [20].

3.10. Différence entre IDS et IPS :

Les IDS et IPS lisent tous les deux les paquets réseau et comparent le contenu à une base de menaces connues. La principale différence entre les deux tient à ce qui se passe ensuite.

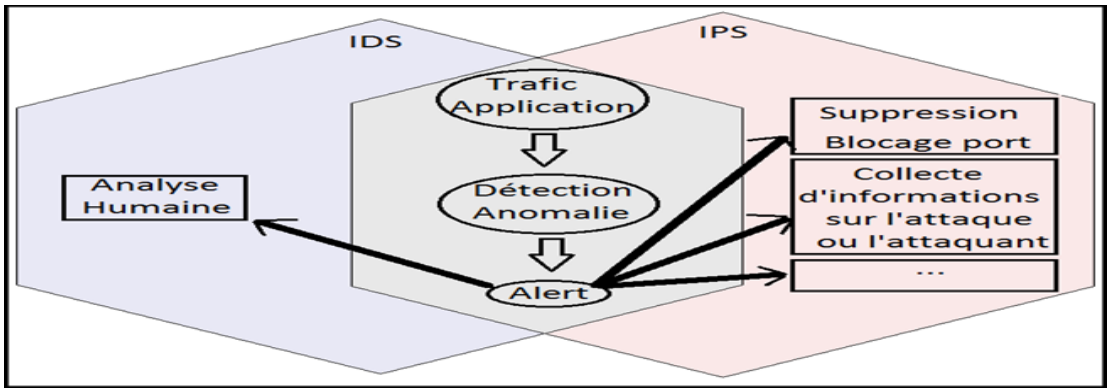


Figure 3.6 : Différence entre IDS et IPS.

IDS	IPS
• Les IDS sont des outils de détection et de surveillance qui n'engagent pas d'action de leur propre fait. • Il est nécessaire qu'un humain ou un autre système prenne ensuite le relais pour examiner les résultats et déterminer les actions à mettre en œuvre, ce qui peut représenter un travail à temps complet selon la quantité quotidienne de trafic généré. • L'IDS ne modifie en aucune façon les paquets réseau.	• Les IPS constituent un système de contrôle qui accepte ou rejette un paquet en fonction d'un ensemble de règles. • L'IPS constitue un très bon outil, qui pourra l'utiliser dans le cadre de ses enquêtes sur les incidents de sécurité. • l'IPS empêche la transmission du paquet en fonction de son contenu, tout comme un pare-feu bloque le trafic en se basant sur l'adresse IP.

Tableau 1 : La différence entre IDS/IPS.

De nombreux fournisseurs d'IDS/IPS ont intégré de nouveaux systèmes IPS à des pare-feu, afin de créer une technologie appelée UTM (Unified Threat Management). Cette technologie combine en une seule entité les fonctionnalités de ces deux systèmes similaires. Certains systèmes intègrent dans une même entité les fonctionnalités d'un IDS et d'un IPS [21].

3.11. Snort:

3.11.1. Définition:

Snort est le premier système hybride (IDS/IPS) Open Source le plus avancé au monde. Il utilise une série de règles qui aident à définir l'activité réseau malveillante et utilise ces règles pour trouver les paquets qui leur correspondent à eux et génère des alertes pour les utilisateurs. Il peut également être déployé en ligne pour arrêter ces paquets [22].

Snort a trois utilisations principales:

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

3.11.2. Architecture de Snort :

L'architecture de SNORT est organisée en modules, elle est composée de quatre grands modules : Le décodeur de paquets, les préprocesseurs, le moteur de détection et le système d'alerte et d'enregistrement de log [23].

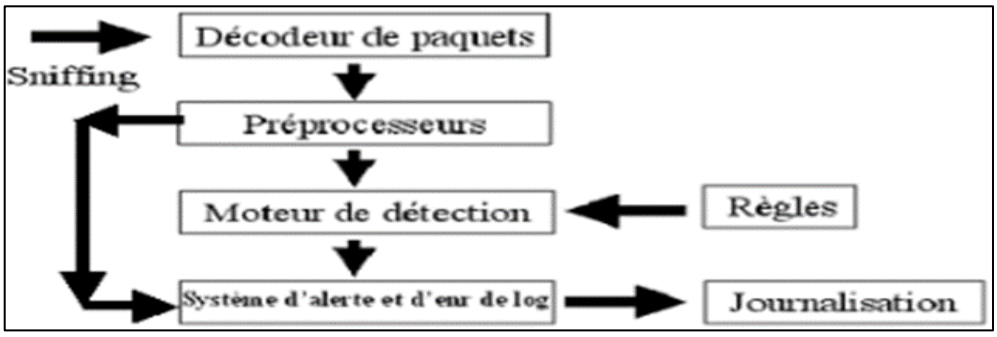


Figure 3.7 : L'architecture de Snort.

- **Le décodeur de paquets :**

Un système de détection d'intrusion active un ou plusieurs interfaces réseau de la machine en mode espion (promiscuous mode), ceci va lui permettre de lire et d'analyser tous les paquets qui passent par le lien de communication. SNORT utilise la bibliothèque libpcap pour faire la capture des trames. Un décodeur de paquets est composé de plusieurs sous décodeurs qui sont organisés par protocole (Ethernet, IP, TCP..), ces décodeurs transforme les éléments des protocoles en une structure de données interne.

- **Les préprocesseurs :**

Les préprocesseurs s'occupent de la détection d'intrusion en cherchant les anomalies. Un préprocesseur envoie une alerte si les paquets ne respectent pas les normes des protocoles utilisées. Un préprocesseur est différent d'une règle de détection, il est un programme qui vise à aller plus en détail dans l'analyse de trafic.

- **Moteur de détection :**

C'est la partie la plus importante dans un IDS. Le moteur de détection utilise les règles pour faire la détection des activités d'intrusion. Si un paquet correspond à une règle, alors une alerte est générée. Les règles sont groupées en plusieurs catégories sous forme de fichiers. SNORT vient avec un ensemble de règles prédéfini.

- **Système d'alerte et d'enregistrement des logs :**

Le système d'alerte et d'enregistrement des logs s'occupe de la génération des logs et des alertes.

Dès que le système devient opérationnel, on pourra consulter les alertes générées directement dans les fichiers textes ou bien utiliser une console de gestion (ACID) ou une version améliorer (BASE). ACID (Analysis Console for Intrusion Detection) est une application qui fournit une console de gestion et qui permet la visualisation des alertes en mode graphique.

3.11.3. 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.

3.12. Conclusion :

Comme tous les outils technologiques, les IDS ont des limites et des faiblesses que seule une analyse humaine peut compenser, et les IPS ont des limites et des faiblesses que ne peut pas empêcher toutes

les attaques non connues, et ils peuvent paralyser tout un système. Mais avec le temps, ces outils deviennent chaque jour meilleurs grâce à l'expérience acquise.

Dans ce chapitre, nous avons montré les notions des systèmes de détection et prévention d'intrusions, et leurs architectures, ainsi que leurs fonctionnements. Nous avons compris que les IDS/IPS sont des outils indispensables à la bonne sécurité d'un réseau, et capables de satisfaire les besoins de presque tous les types d'utilisateurs.

Dans le chapitre suivant nous allons détailler l'implémentation de la solution proposé qui consiste de mettre en place une architecture réseau comportant un tunnel IPSec site à site et un pare-feu équipé d'un IDS Snort ensuite nous allons réaliser quelques attaques pour voir comment Snort va réagir.

Chapitre 04

TEST ET MISE EN ŒUVRE DE LA SOLUTION

4.1. Introduction :

Ce dernier chapitre, nous allons voir un cas pratique concernant Pfsense et l'implémentation de la plateforme de Snort en plus un tunnel IPSec site à site, nous allons voir comment installer ses différents composants, ainsi que toutes les configurations nécessaires. Enfin, nous allons donner quelques tests que nous avons réalisés en lançant quelques attaques et voir comment Snort va détecter et bloquer ces derniers.

4.2. Présentation de l'environnement :

4.2.1. 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. La version Linux présente l'avantage de pouvoir sauvegarder les fichiers de la machine virtuelle (*.vmsd) pendant son fonctionnement [24].

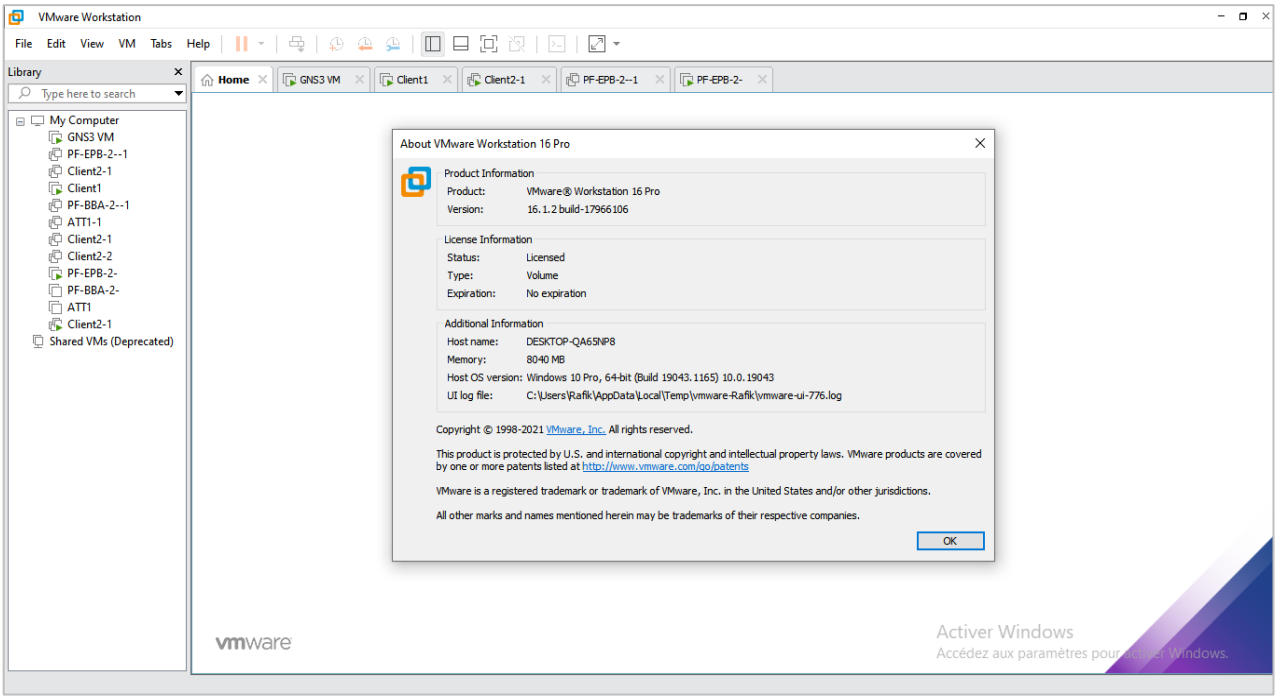


Figure 4.1 : VMware Workstation 16.1.2 professional.

4.2.2. Pfsense :

Pfsense est une distribution personnalisée open source gratuite de FreeBSD, conçue pour être utilisée comme pare-feu et routeur entièrement gérée par une interface Web facile à utiliser. Cette interface Web est connue sous le nom de configurateur d'interface graphique Web, ou Web GUI (Graphical User Interface) en abrégé. En plus d'être une plate-forme de pare-feu et de routage puissante et flexible, ce logiciel comprend une longue liste de fonctionnalités connexes.

Le système de package Pfsense permet une évolutivité supplémentaire sans ajouter de surcharge et de vulnérabilités de sécurité potentielles à la distribution de base. Pfsense est un projet populaire avec des millions de téléchargements depuis sa création et des centaines de milliers d'installations actives [25].

Pfsense ne fait pas seulement firewall, il offre toute une panoplie de services réseaux.

Voici une partie qui semble intéressante :

- 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 règles 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 L2TP.
- Serveur DHCP.
- Serveur DNS et DNS dynamiques.
- Portail Captif.
- Proxy et Blacklist SQUIDGUARD.
- Gestion des VLAN.
- IDS-IPS SNORT.

4.2.3. 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 System) [26].

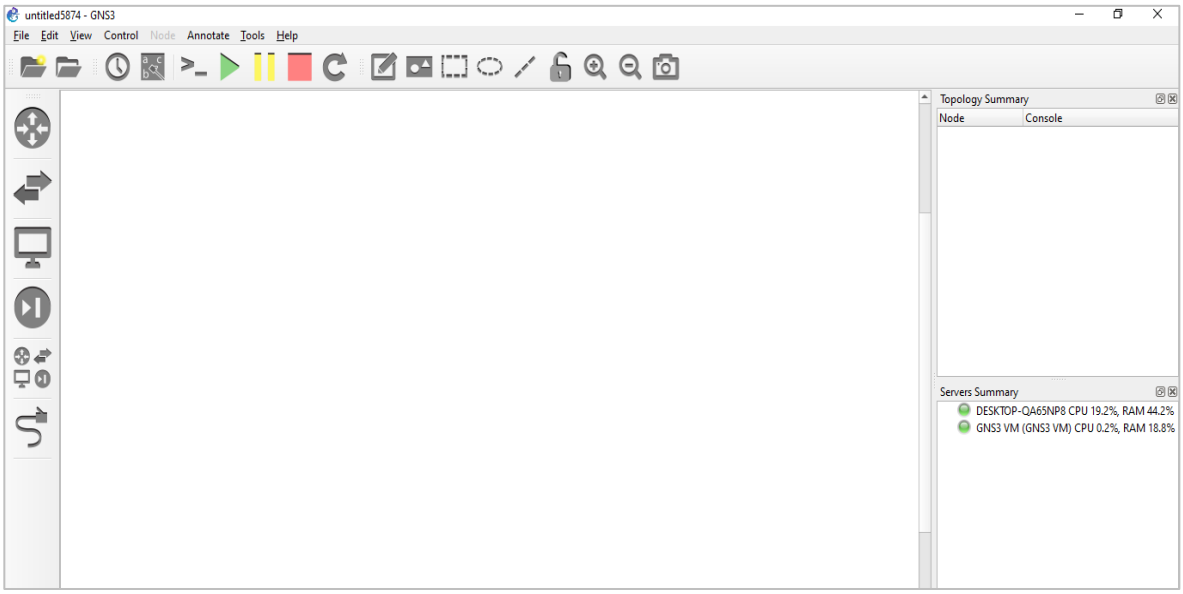


Figure 4.2 : GNS3 Graphical Network Simulator version 2.2.24.

a) Les composants du logiciel :

Afin de fournir une simulation précise et complète, GNS3 est fortement lié à :

– Dynamips : Emulateur d'IOS Cisco.

– Dynagen : Interface écrite en python et permettant l'interconnexion de plusieurs machines émulées.

– Qemu : Emulateur de système.

– VMware : Logiciel permettant la création de machines virtuelles.

– Wireschark : est un logiciel pour analyser les trames.

b) Avantages:

- Logiciel gratuit.
- Logiciels open source.
- Pas de frais de licence mensuels ou annuels.
- Aucune limitation sur le nombre d'appareils pris en charge (la seule limitation est votre matériel : CPU et mémoire).
- Appliances téléchargeables, gratuites, préconfigurées et optimisées disponibles pour simplifier le déploiement.
- Logiciels de plusieurs fournisseurs disponibles gratuitement.
- Grande communauté active (plus de 800 000 membres).

c) Désavantages:

- Les images Cisco doivent être fournies par l'utilisateur (téléchargement depuis Cisco.com, ou achat d'une licence VIRL, ou copie depuis un périphérique physique).
- Pas un package autonome, mais nécessite une installation locale de logiciel (GUI).
- GNS3 peut être affecté par la configuration et les limitations de votre PC en raison de l'installation locale (paramètres de pare-feu et de sécurité, politiques d'ordinateur portable de l'entreprise, …etc.).

4.3. Installation et Configuration basique de Pfsense sous VMware :

4.3.1. Installation de Pfsense :

Pour commencer, il faut disposer d'une image iso de Pfsense version 2.5.2-RELEASE Basé sur FreeBSD, cette images est disponible sur https://www.pfsense.org/download/ . On créer une Machine Virtuelle sous VMware avec les spécifications suivantes :

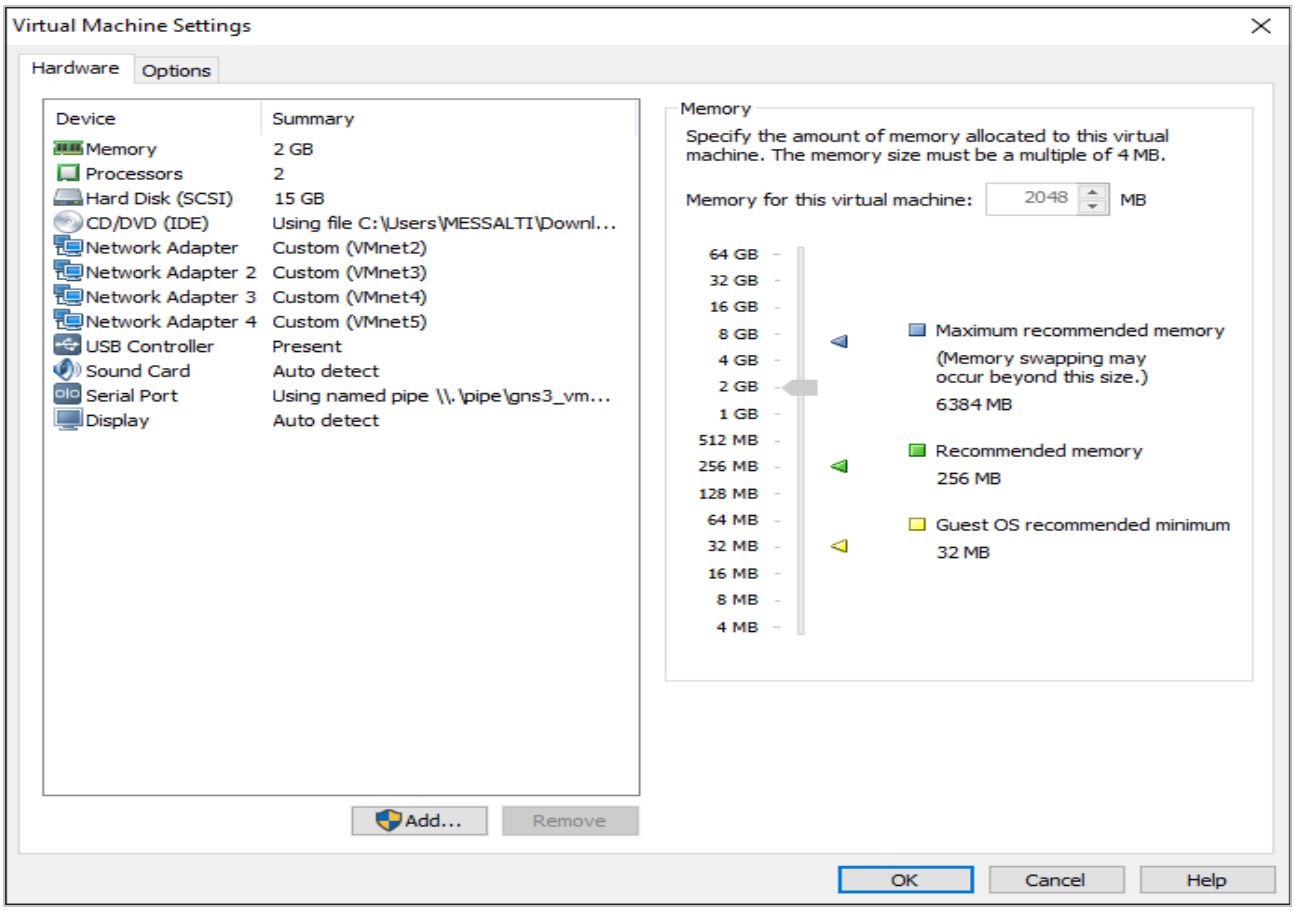


Figure 4.3 : Configuration des cartes réseau de Pfsense.

- Avant de commencer l'installation, notre machine doit être équipée en minimum de quatre cartes réseaux. Pour ce projet on va utiliser quatre interfaces (4 cartes réseaux) :

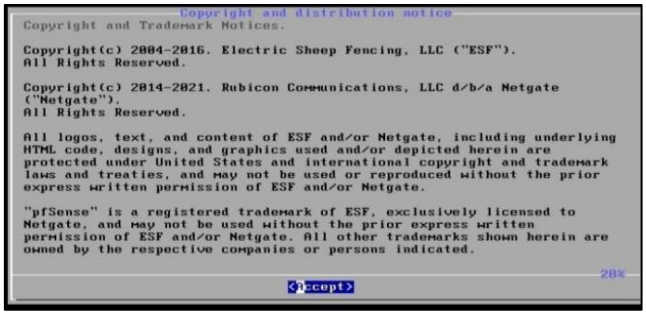
  – WAN (VMnet2): pour qu'on puisse se connecter à l'internet.

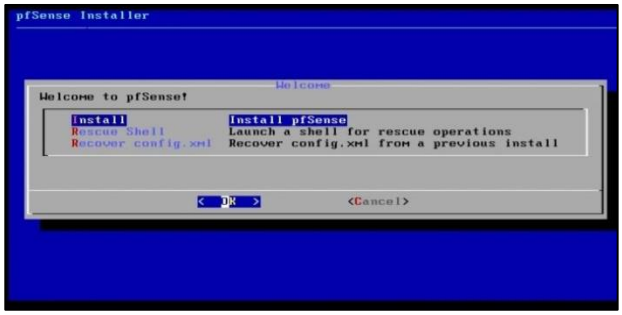
  – LAN (VMnet3) : passerelle du réseau locale.

  – Serveur (VMnet4) : passerelle du réseau Serveur.

  – DMZ (VMnet5) : passerelle du réseau DMZ.

Pour aboutir à une installation complète et correcte de Pfsense, suivre les étapes dans captures suivantes :





- La première question que nous rencontrons durant l'installation est la suivante :

On répond par n (No) car on n'aura pas besoin des VLANs.

- Pfsense demande d'affecter chaque interface (ici vmx0, vmx1, vmx2, vmx3) à une interface WAN ou bien à une LAN, DMZ ou le Serveur.

- Une fois les affectations son faite, Pfsense détecte automatiquement les cartes réseaux disponibles, puis on attribue pour chaque interface une adresse IP.

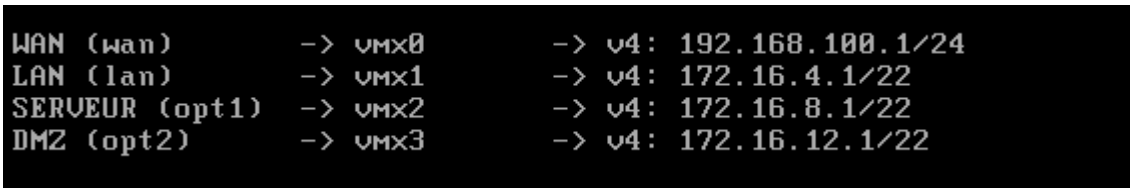


Figure 4.4 : Assignation de l'interface WAN et LAN et DMZ et Serveur.

Une fois l'installation est terminée au aura cet affichage pour Pfsense :

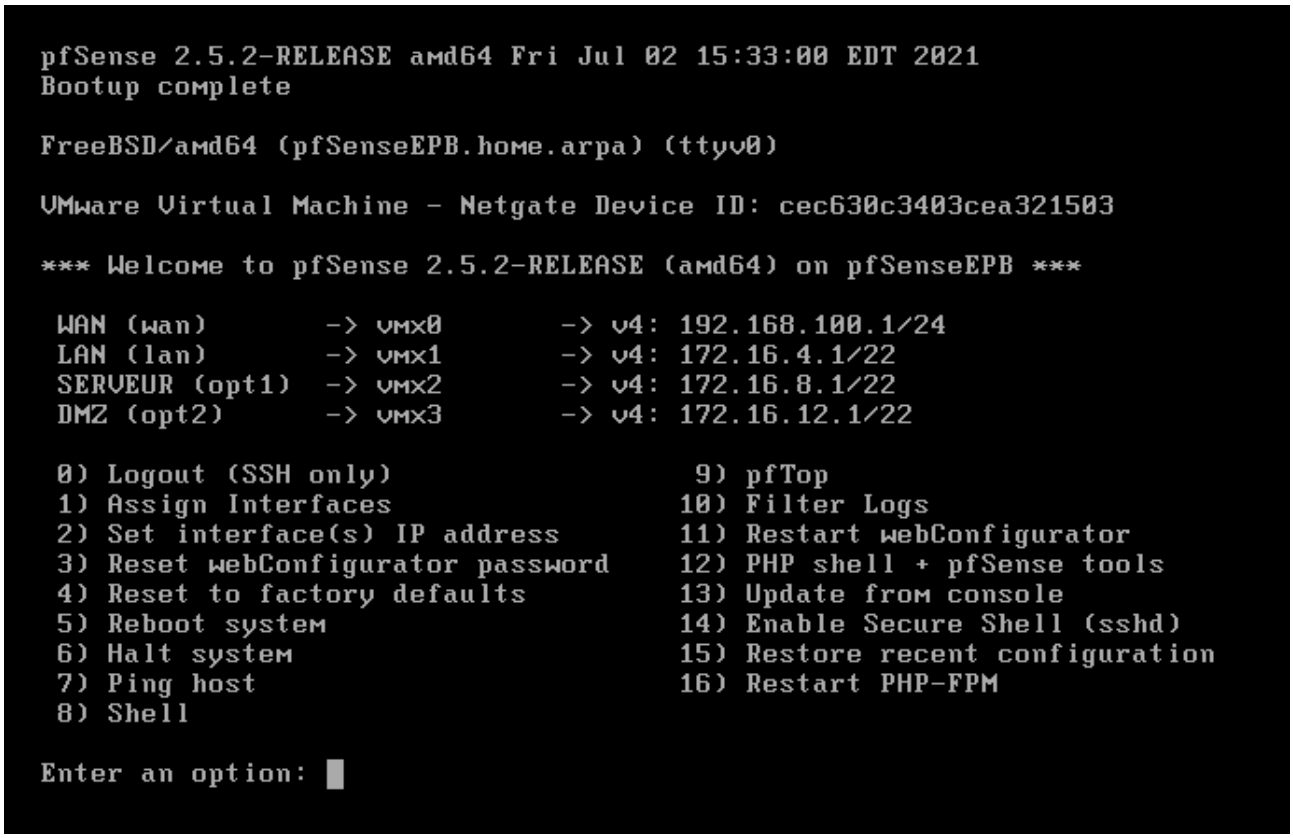


Figure 4.5 : Pfsense EPB l'installation terminée.

- Les adresses IP des interfaces sont attribuées statiquement par le choix de l'option 2.
- La table d'adressage suivi dans ce projet est la suivante :

Sous réseau	Adresse de sous réseau	Mask	Adresse de Diffusion	Passerelle
WAN	192.168.100.0	/24	192.168.100.255	192.168.100.1
LAN	172.16.4.0	/22	172.16.7.255	172.16.4.1
Serveur	172.16.8.0	/22	172.16.11.255	172.16.8.1
DMZ	172.16.12.0	/22	172.16.15.255	172.16.12.1

Tableau 2 : Table d'adressage de Pfsense de EPB.

- Pour se connecter à l'interface web de configuration de Pfsense on utilise l'adresse IP de l'interface LAN : https://172.16.4.1.

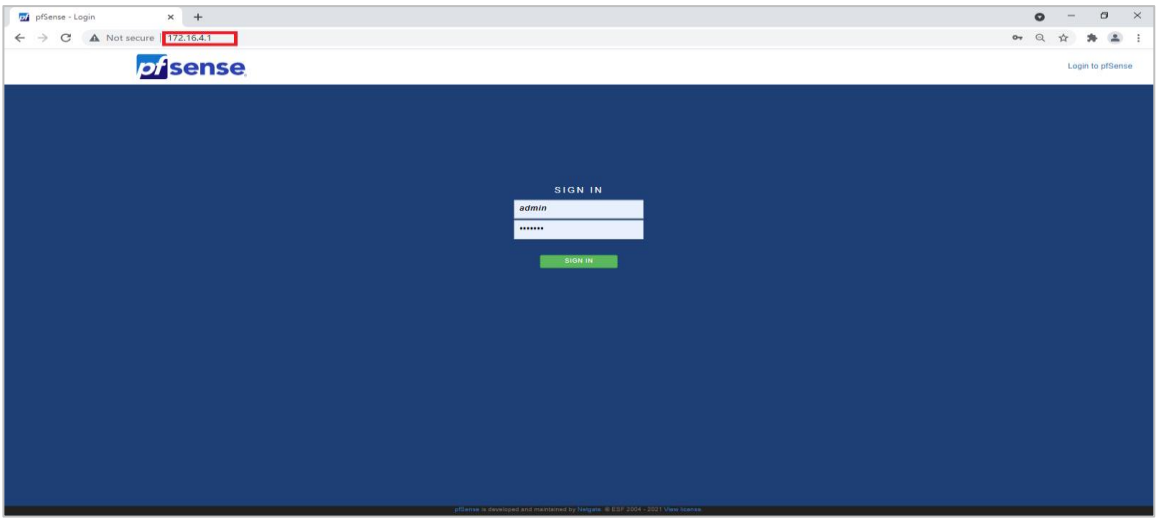


Figure 4.6 : Page d'authentification de Pfsense.

- 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.

4.3.2. Configuration basique de Pfsense :

Pour activer les interfaces, on doit accéder à : « interfaces » puis on choisit l'interface (Serveur ou DMZ) après on coche la case "enable interface". Les interfaces LAN et WAN sont activées par défaut.

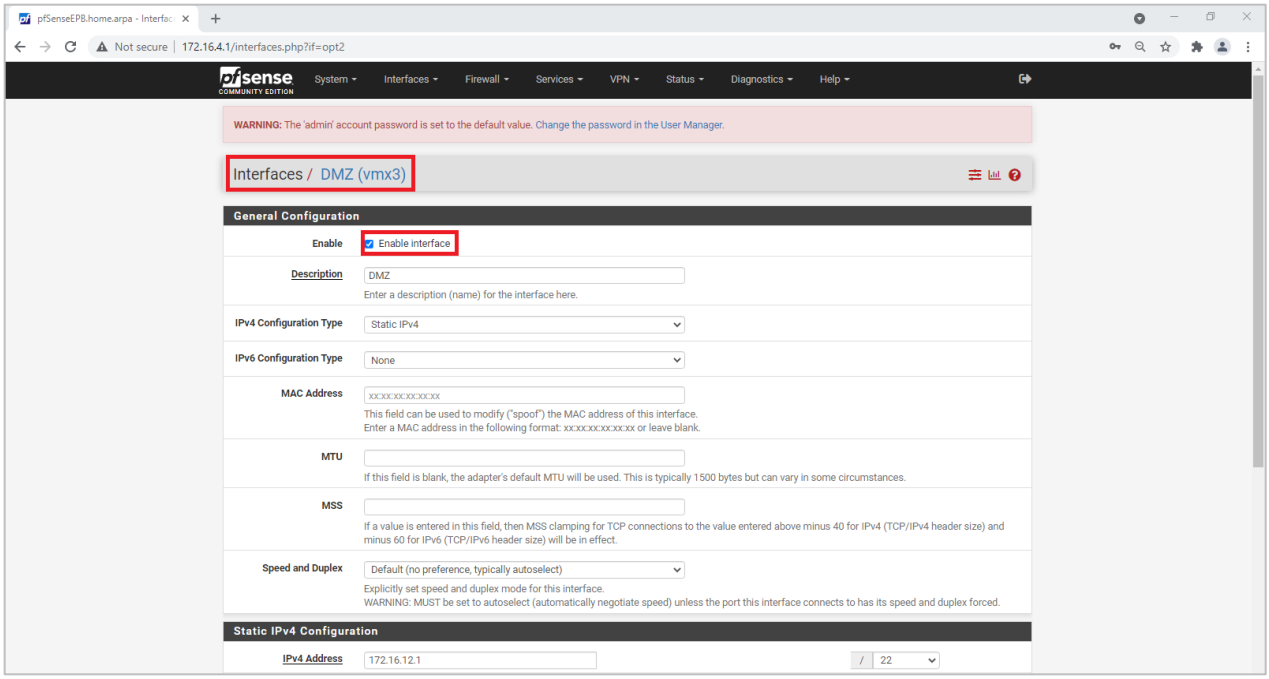


Figure 4.7 : L'activation de l'interface DMZ.

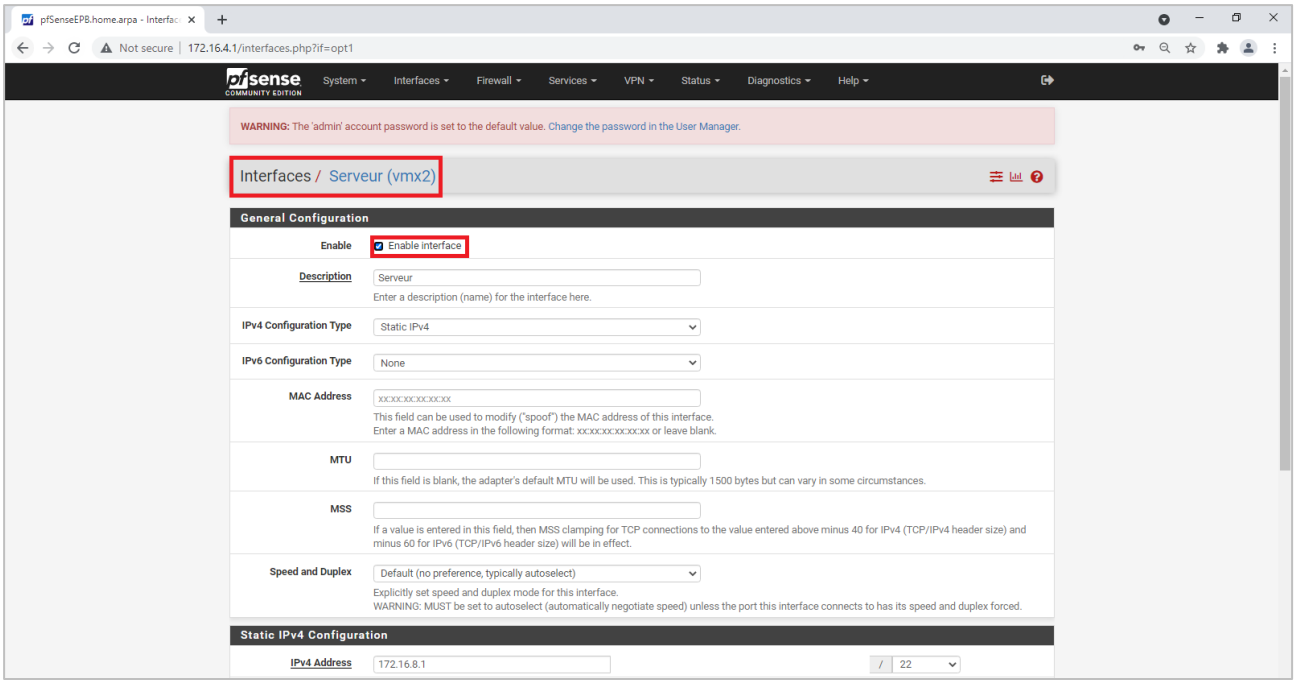


Figure 4.8 : L'activation de l'interface Serveur.

- Après l'activation on va passer à la configuration générale du serveur Pfsense:
  - **Hostname** : le nom d'Host.
  - **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 8.8.4.4).
  - **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).

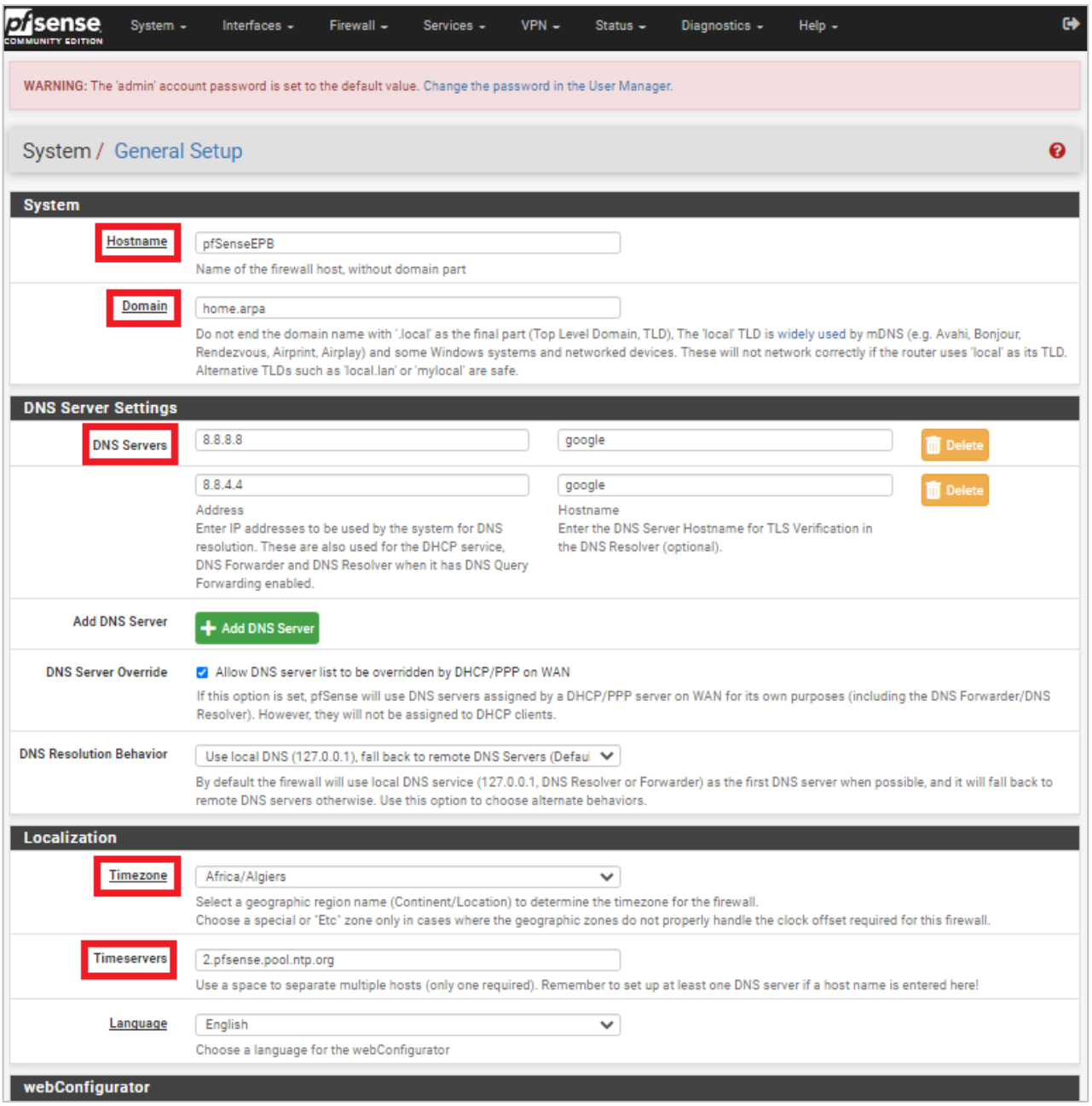


Figure 4.9 : L'interface web pour la configuration générale du serveur Pfsense.

- 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.

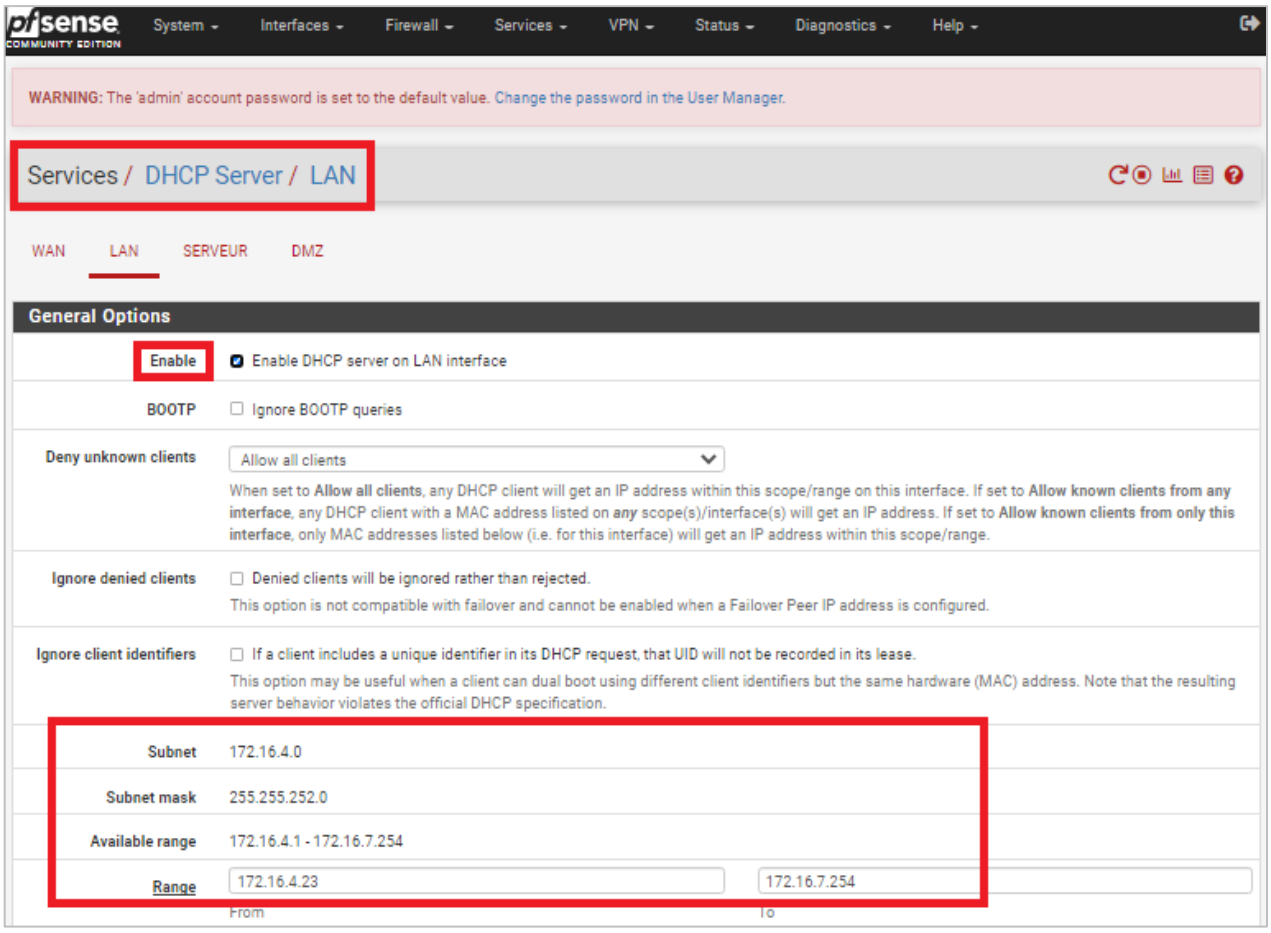


Figure 4.10 : configuration du protocole DHCP des hôtes.

4.4. 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 172.16.4.1 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 [24] :

- D'autoriser la connexion (allow) ;
- De bloquer la connexion (deny) ;
- De rejeter la demande de connexion sans avertir l'émetteur (drop).

L'ensemble de ces règles permet de mettre en œuvre une méthode de filtrage dépendant de la politique de sécurité adoptée par l'entité. On distingue habituellement deux types de politiques de sécurité permettant :

- soit d'autoriser uniquement les communications ayant été explicitement autorisées
- soit d'empêcher les échanges qui ont été explicitement interdits.

Un système pare-feu fonctionne sur le principe du filtrage simple de paquets (en anglais « stateless packet filtering »).

Il analyse les en-têtes de chaque paquet de données (datagramme) échangé entre une machine du réseau interne et une machine extérieure.

Ainsi, les paquets de données échangées entre une machine du réseau extérieur et une machine du réseau interne transitent par le pare-feu et possèdent les en-têtes suivants, systématiquement analysés par le firewall :

- Adresse IP de la machine émettrice ;
- Adresse IP de la machine réceptrice ;
- type de paquet (TCP, UDP, etc.) ;
- numéro de port (rappel: un port est un numéro associé à un service ou une application réseau).

Les adresses IP contenues dans les paquets permettent d'identifier la machine émettrice et la machine cible, tandis que le type de paquet et le numéro de port donnent une indication sur le type de service utilisé.

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.

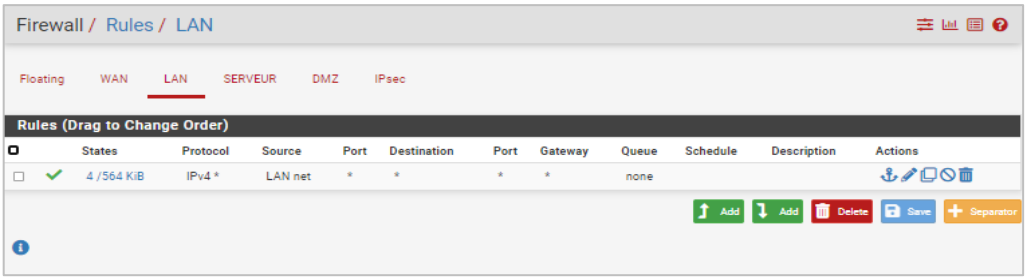


Figure 4.11 : La liste des règles associées à l'interface LAN.

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

✓ Autoriser le LAN d'accéder à tous les réseaux.

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

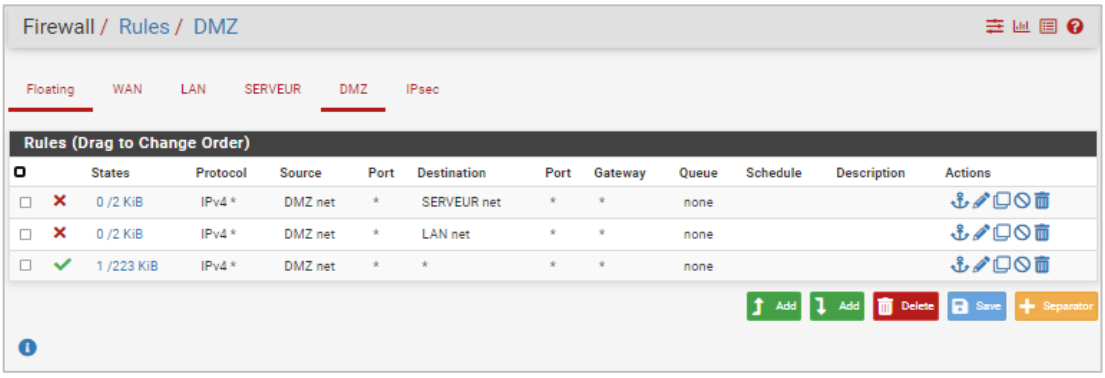


Figure 4.12 : La liste des règles associées à l'interface DMZ.

Pour les règles de DMZ, on remarque qu'il y a 3 règles :

- ✓ 1ère règle: c'est pour bloquer le flux sortant de DMZ vers les serveurs de l'entreprise.
- ✓ 2ème règle: c'est pour bloquer le flux sortant de DMZ vers le LAN ce qui empêcher un intrus dans les serveurs situés dans la DMZ d'accéder au réseau locale.
- ✓ La 3ème règle : Autoriser la DMZ d'accéder à tous les réseaux.

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

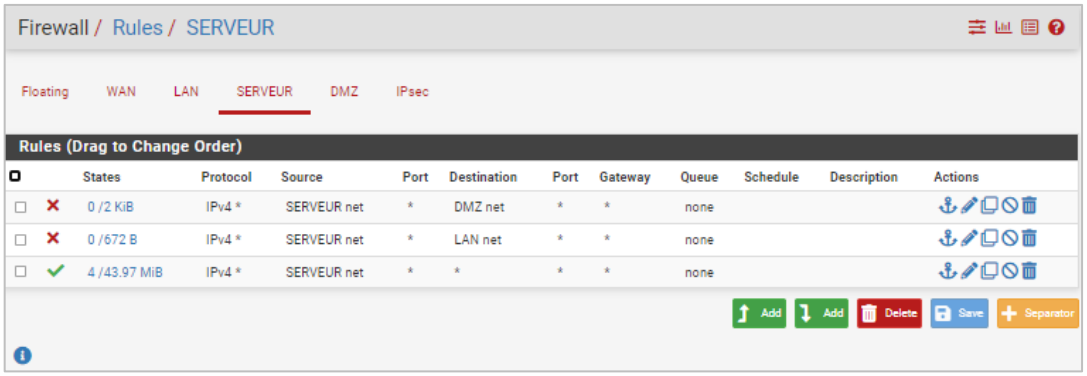


Figure 4.13 : La liste des règles associées à l'interface Serveur.

On remarque que dans la figure il existe 3 règles pour l'interface Serveur :

- ✓ Les deux premiers règles : c'est pour bloquer le flux sortant de Serveur vers la DMZ et le réseau locale de l'entreprise.
- ✓ 3ème règle : Autoriser le Serveur d'accéder à tous les réseaux.

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

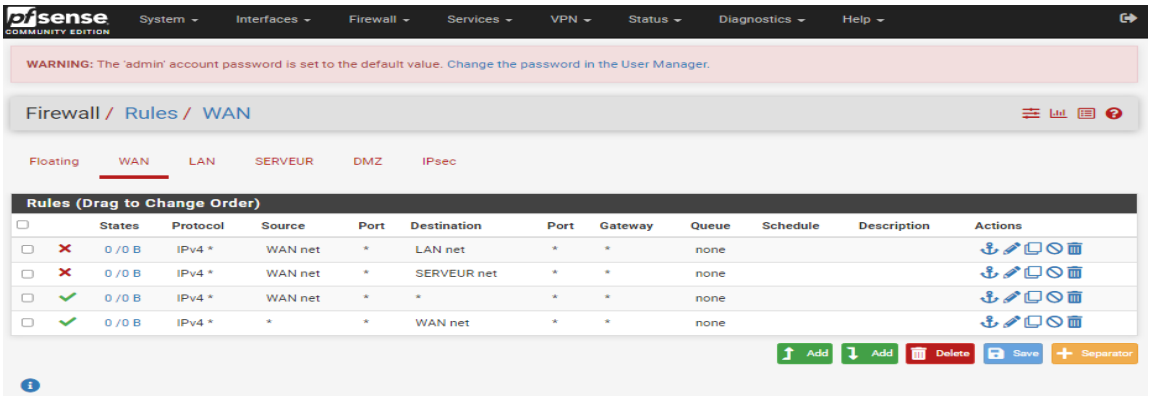


Figure 4.14 : La liste des règles associées à l'interface WAN.

On remarque qu'il existe 4 règles pour le WAN :

- ✓ La 1ère et la 2ème règle : c'est pour bloquer le flux sortant du WAN vers le Serveur et le réseau locale ce qui empêcher un intrus dans le WAN d'accéder au réseau locale et le Serveur de l'entreprise.
- ✓ 3ème règle : Afin d'autoriser le flux sortant du WAN d'accéder à tous les réseaux.
- ✓ 4ème règle : Autoriser n'importe quelle flux d'accéder au WAN.

4.5. Configuration de SNORT :

4.5.1. 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.

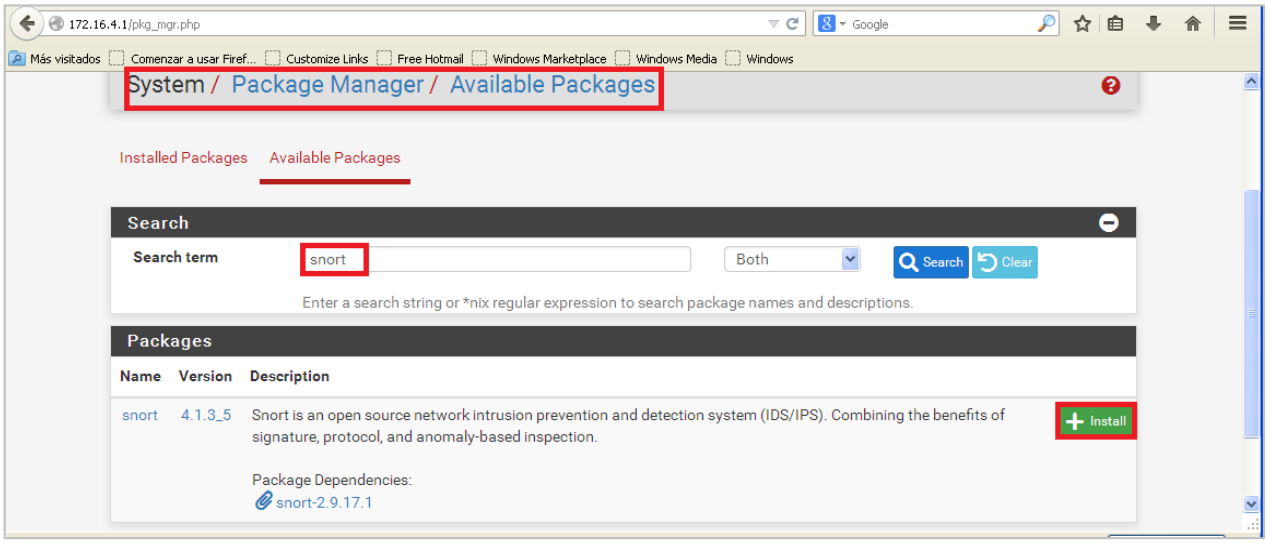


Figure 4.15 : Installation de package Snort.

4.5.2. 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.
- Enable OpenAppID : qui est un plugin de sécurité réseau pour la couche application. Il s'ajoute à Snort pour permettre d'avoir une remontée d'alerte sur les utilisations des applicatifs sur un réseau.
- Feodo Tracker Botnet C2 IP Rules : Cet ensemble de règles sont utilisées pour détecter et/ou bloquer les connexions réseau vers les serveurs hotline (combinaison adresse IP:port).

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. Cette capture représente comment avoir le code :

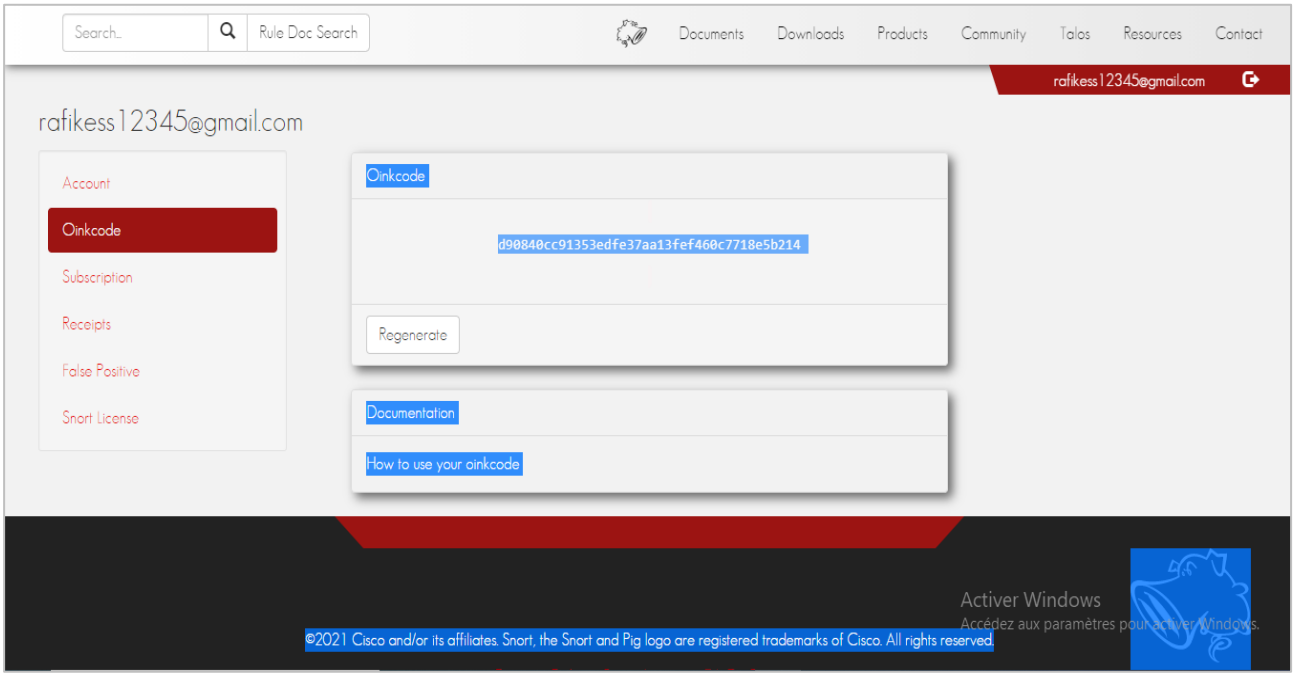


Figure 4.16 : Oinkmaster code de Snort.

La capture suivante montre les paramètres généraux de Snort et les règles à cocher :

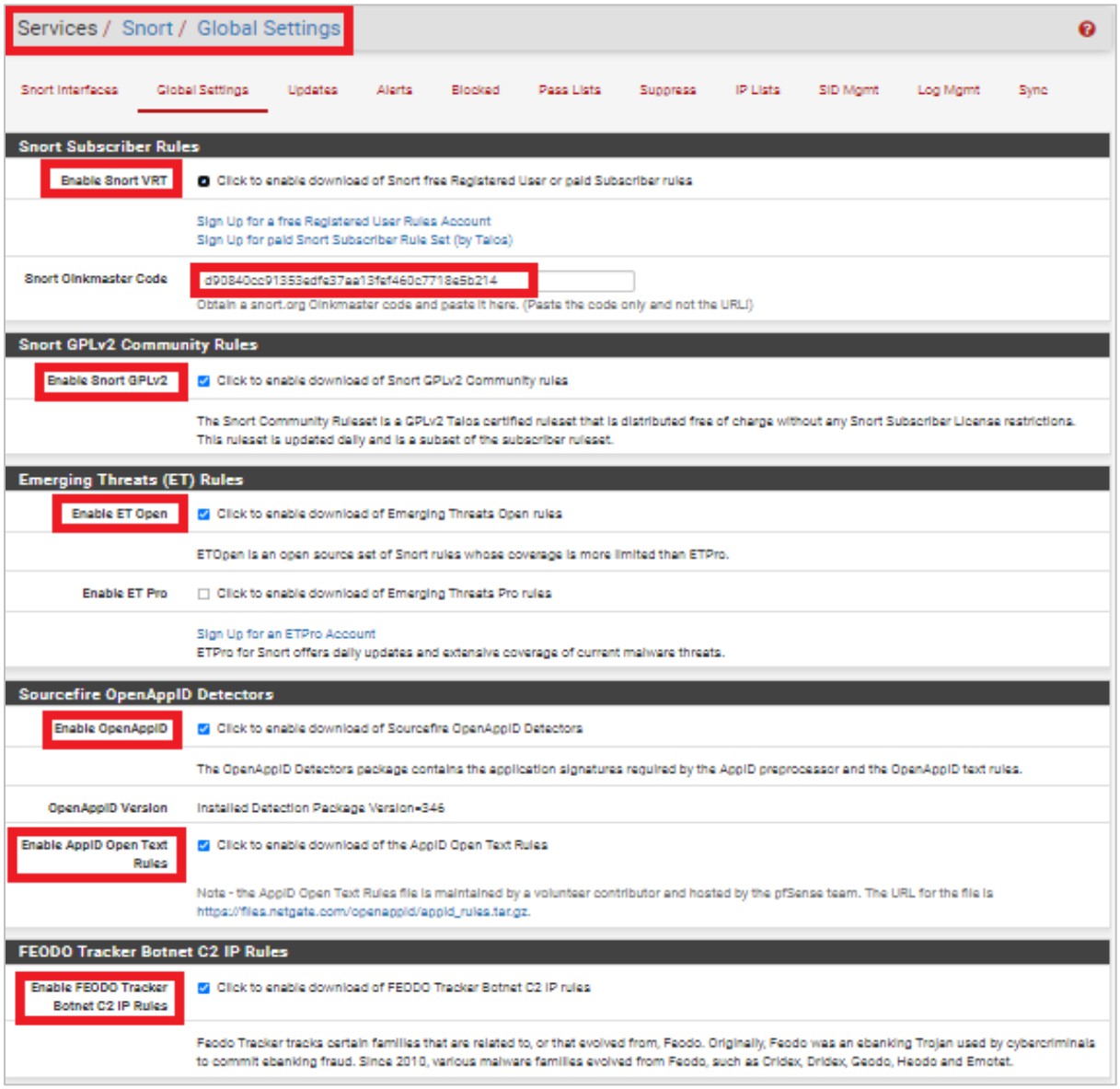


Figure 4.17 : Les règles de Snort a sélectionnées.

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 :

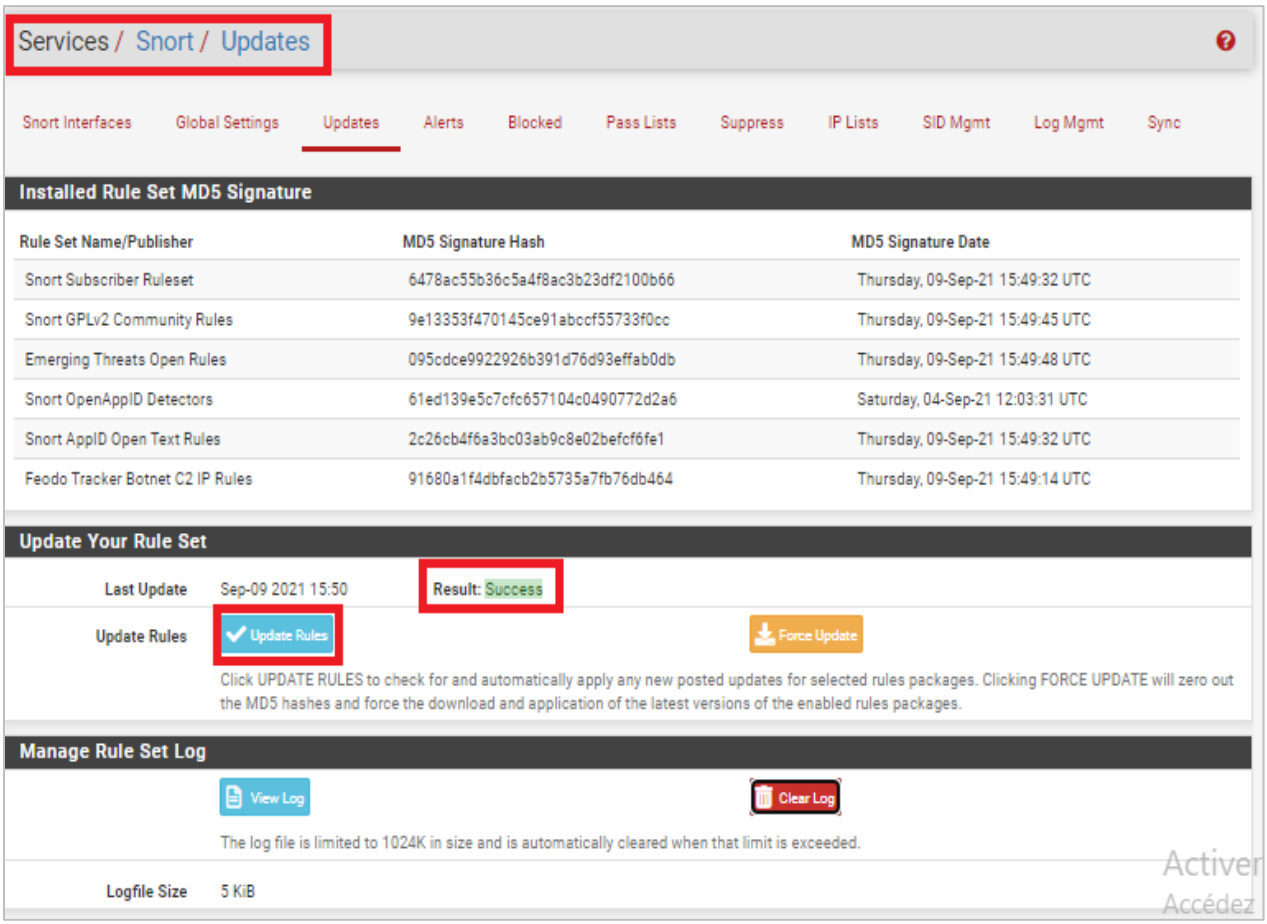


Figure 4.18 : Mise à jour des règles de Snort.

4.5.3. Activation et ajout de SNORT aux interfaces :

Afin de pouvoir utiliser nos règles, il est nécessaire de les appliquer sur une interface de notre pare-feu. Le WAN est le plus exposée aux attaques 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**. La figure prochaine explique comment activer Snort sur l'interface WAN :

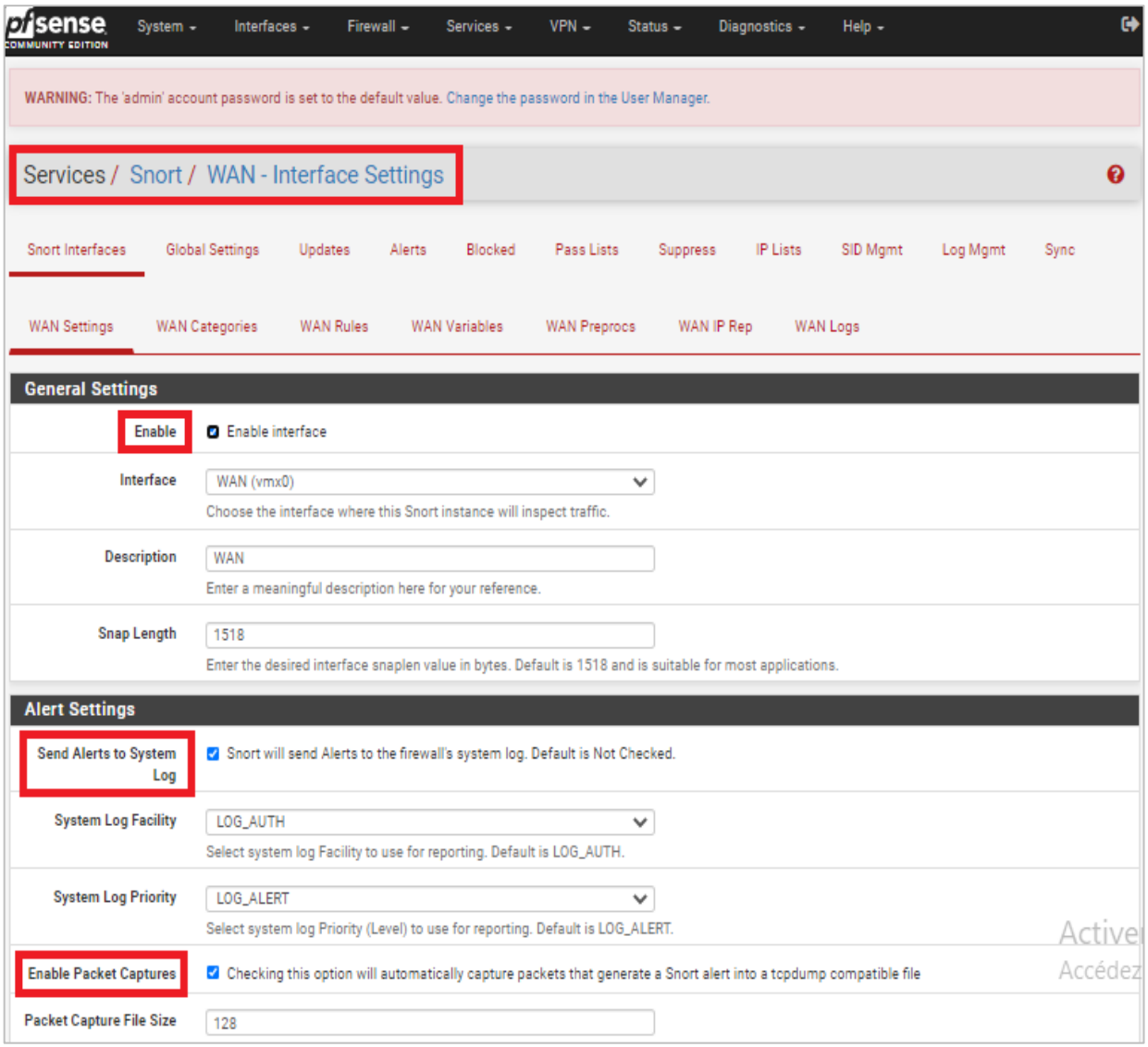


Figure 4.19 : Activation du Snort sur l'interface WAN.

4.5.4. 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** » :

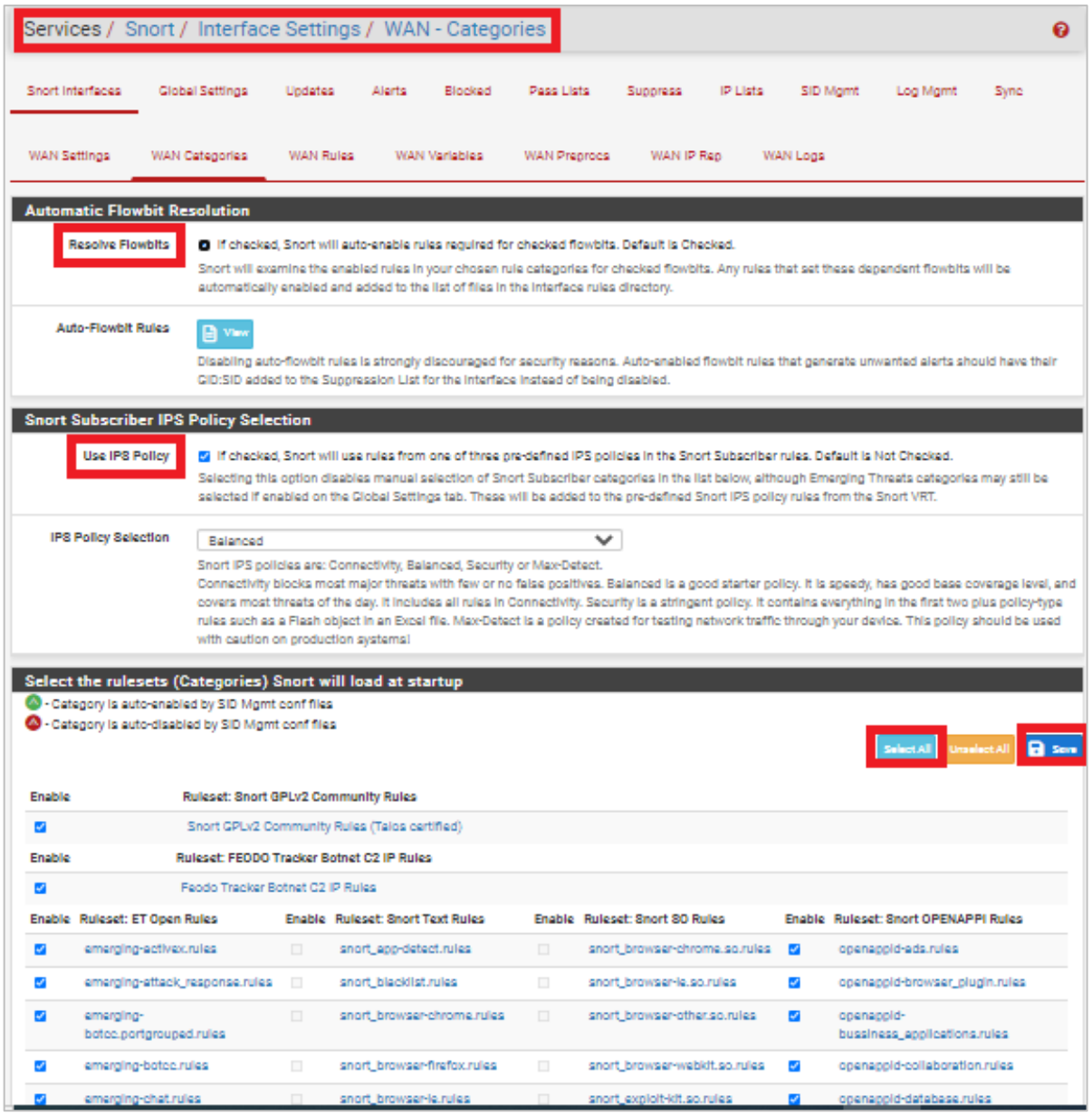


Figure 4.20 : Activation des catégories sur l'interface WAN.

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

4.5.5. 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'alertes), nous allons également cocher la case (auto-refresh view) pour actualiser la liste des notifications.

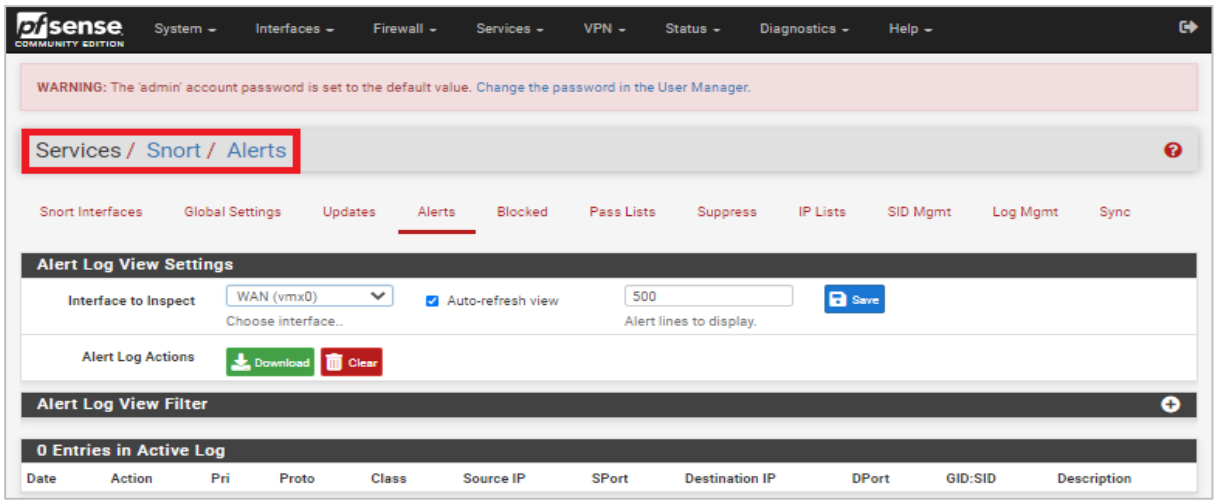


Figure 4.21 : Configuration des alertes.

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

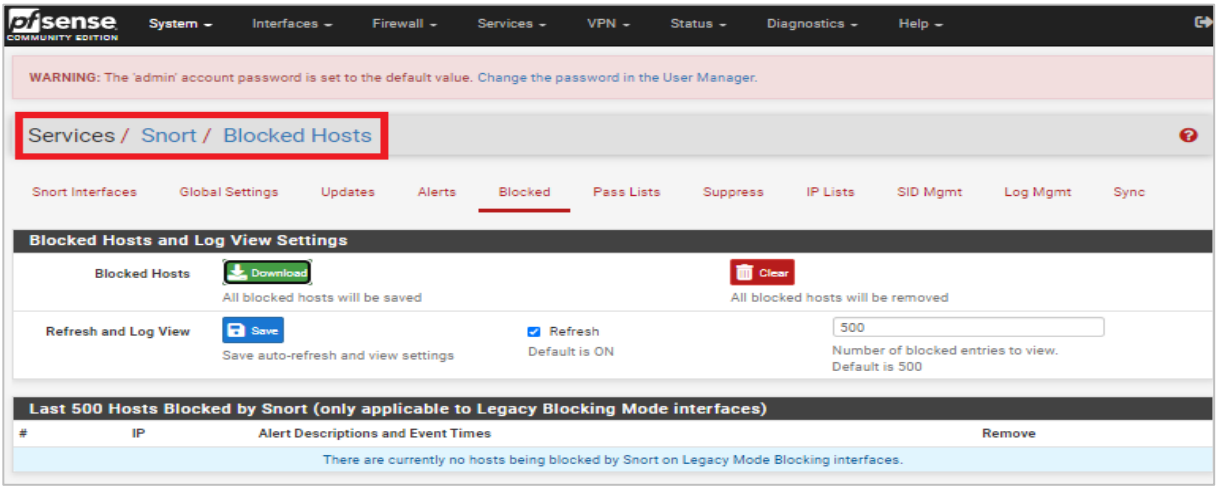


Figure 4.22 : Configuration des blocages.

La capture suivante montre les configurations à appliquer sur le fichier log selon nos besoin, on se positionne dans : **Services/Snort/Log Mgmt**, on active d'abord les trois cases suivantes :

- **Remove Snort Logs On Package Uninstall :** supprimer le fichier journal de Snort lorsque le paquet Snort sera désinstallé.
- **Auto Log Management :** activer la gestion automatique sans surveillance des journaux de Snort en utilisant les paramètres spécifiés ci-dessous.
- **Log Directory Size Limit :** limiter la taille du répertoire des logs (1024 MB).

Ensuite, on a choisi 1 MB pour La taille « Max Size» de chaque fichier log, et pour la rétention on a choisi 14 jours (DAYS), parce qu'après 14 jours le système il va faire la mise à jour.

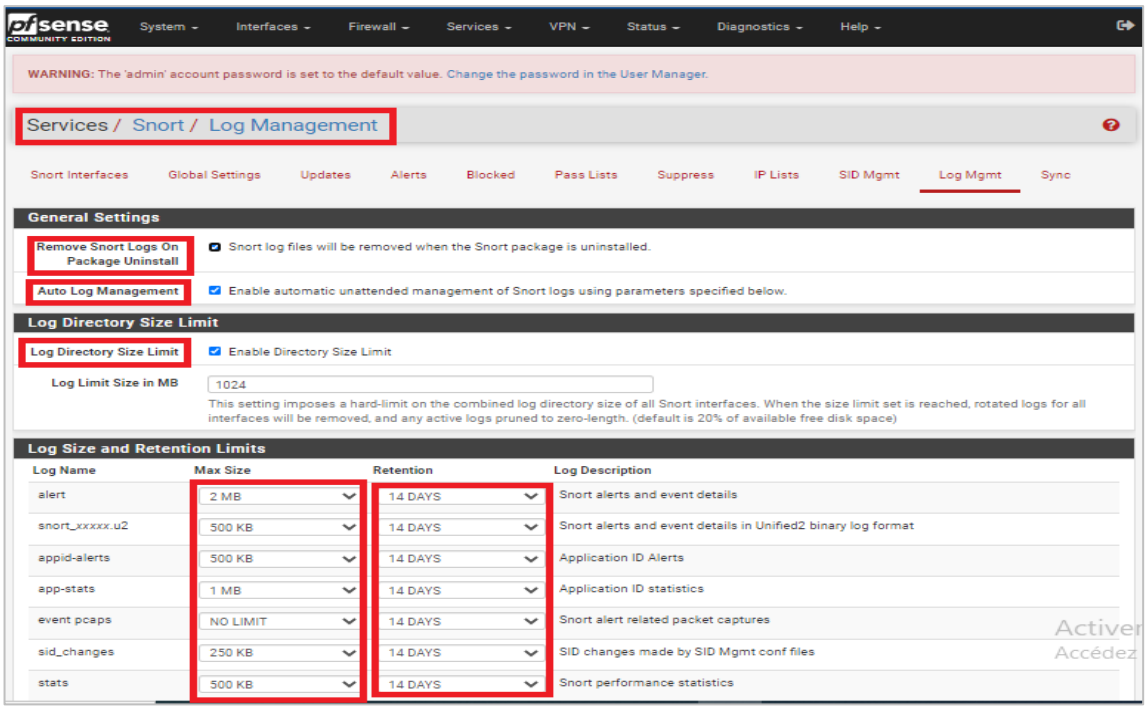


Figure 4.23 : Configuration de fichier Log Mgmt.

Le service Snort est par défaut désactivé, pour l'activer on va aller dans : **Status/Services**. On cherche Snort puis on clique sur le bouton d'activation.

4.6. Configuration de VPN site à site :

Un VPN Site-to-Site (aussi appelé **LAN-to-LAN)** est un VPN qui permet de joindre deux réseaux de type LAN distants de manière à faire en sorte qu'ils puissent communiquer comme s'ils étaient sur le même réseau et qu'un simple routeur les séparait. On peut trouver ce genre de VPN entre des agences et un siège d'entreprise par exemple. Les agences doivent pouvoir se connecter aux ressources du siège de manière transparente malgré leur distance. On établit alors un VPN au travers Internet afin de joindre les deux réseaux mais également de manière à sécuriser ces flux au travers un chiffrement.

Il existe plusieurs outils et technologies permettant de faire du VPN **LAN-to-LAN**. Nous allons ici travailler avec IPSEC **(Internet Protocol Security)** qui est un ensemble de protocoles utilisant des algorithmes permettant le transport de données sécurisées sur un réseau. Il se caractérise comme étant un standard ouvert travaillant sur la couche 3 du modèle OSI et supportant de multiples algorithmes de chiffrement et d'authentification.

Pour illustrer la mise en place de notre VPN Site-to-Site, nous allons utiliser le Pfsense.

Nous aurons donc une interface WAN (192.168.100.0/24,192.168.200.0/24) et LAN (172.16.4.0/22,172.18.4.0/22) sur chacun de nos Pfsense, le but final sera donc que les deux clients puissent communiquer entre eux via ce tunnel. Les clients seront des simples machines Windows XP. On part donc du principe que les Pfsense et les clients sont déjà en place et que ces derniers ont déjà un accès au WAN via un simple NAT des Pfsense.

On commence donc par accéder à l'interface d'administration de notre premier Pfsense (EPB) (172.16.4.1). On se rend directement dans le menu **"VPN"** puis on clique sur le "**add**" pour ajouter une nouvelle configuration **IPSec (phase 1)**. On se retrouve alors avec beaucoup d'options, toutes ont leur importance et leur pertinence mais il n'est pas utile de toute les modifier. La configuration des champs expliquera dans la figure suivante :

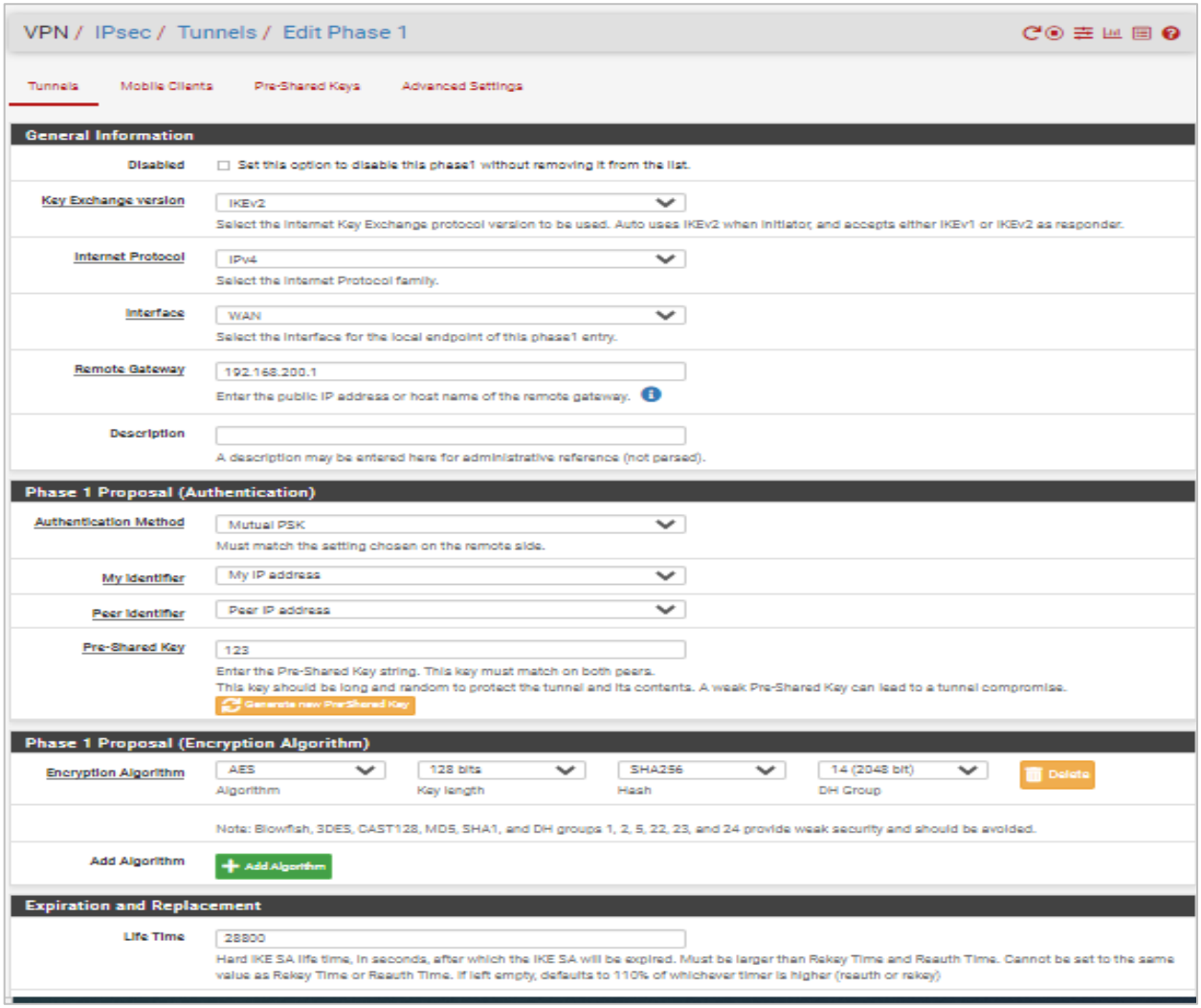


Figure 4.24 : Configuration de l'IPSec phase_1.

On finit par cliquer sur **"Save"** puis sur **"Apply changes**" sur la page suivante. On va alors cliquer en dessous de la première ligne du tableau puis à nouveau sur le "**add**" au bout de cette nouvelle

ligne. On arrive sur une nouvelle page de configuration **(phase_2)** sur laquelle nous allons remplir le champ **"Remote Network"** dans lequel nous allons mettre la plage IP du LAN distant :

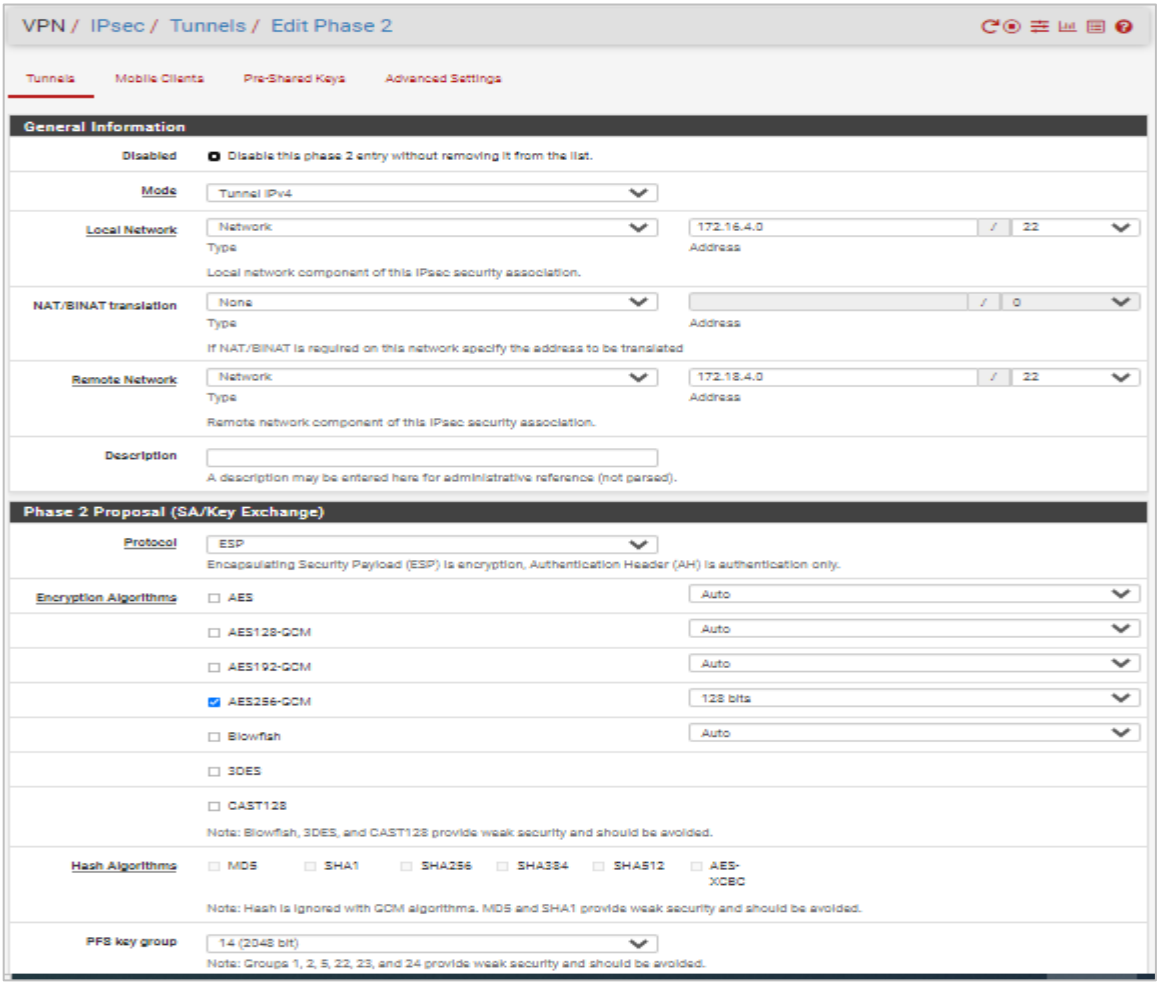
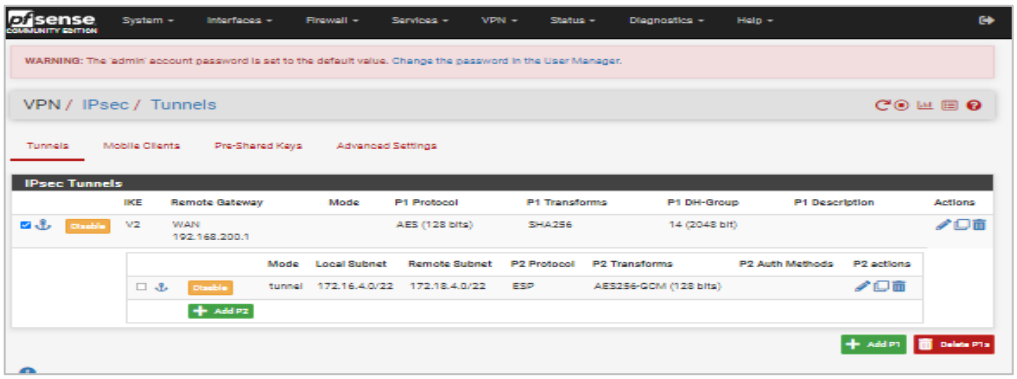


Figure 4.25 : Configuration de l'IPSec phase_2.

On clique sur **"Save"** puis sur **"Apply changes"** sur la page suivante. Si on redéveloppe le tableau principal, nous aurons quelque chose qui ressemble à cela :



Nous avons donc un résumé de notre configuration VPN. Il faut maintenant effectuer exactement la même configuration du coté de notre deuxième Pfsense (Bordj Bouarreridj) en adaptant bien entendu

les adresses IP et les plages IP précisées dans l'annexe. L'installation de ce dernier est similaire à la précédente.

Maintenant nous allons dans **Firewall/rules/IPSec** et cliquer sur le **add** à droite du tableau pour ajouter une règle qui va autoriser tous les flux à arriver depuis l'interface **IPSec** (ceci est bien entendu à adapter selon nos besoins) la configuration de la règle doit ressembler à cela :

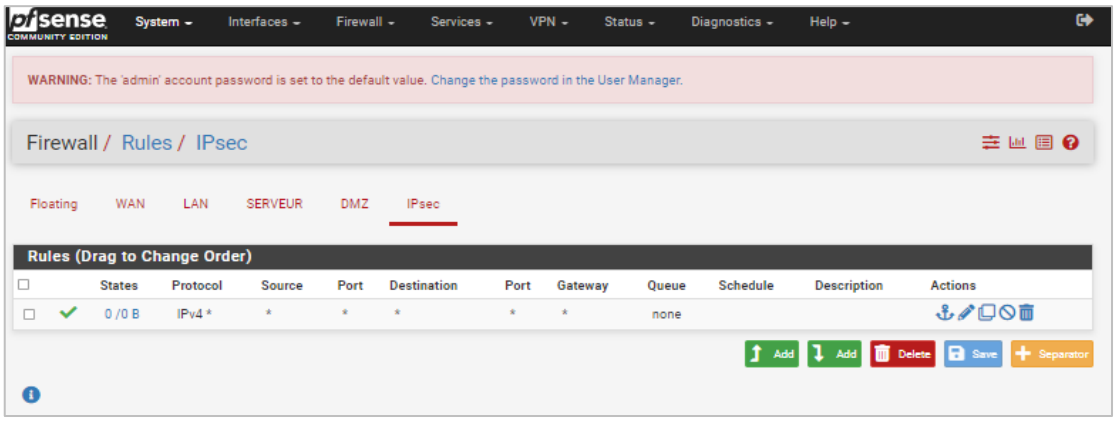
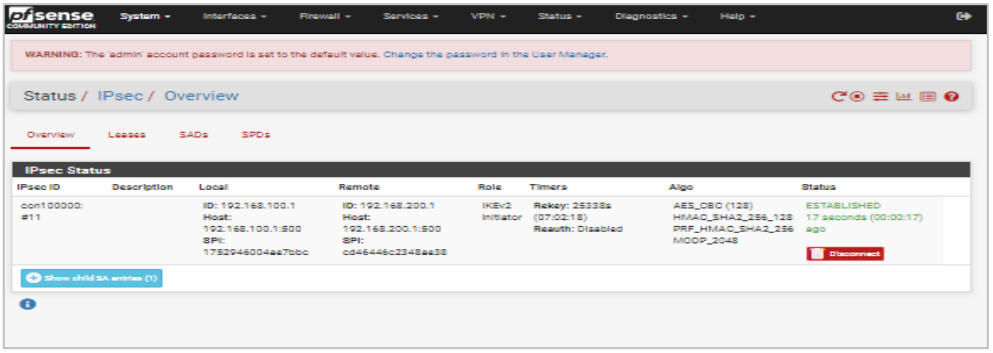


Figure 4.26 : La règle associée à l'interface IPSec.

4.7. Test de fonctionnement :

4.7.1. Test de VPN :

Pour tester le fonctionnement de notre VPN, nous pouvons dans un premier temps aller à la partie **Status/IPSec** puis on clique sur la case « connecte » afin de rendre le VPN active :



Maintenant on peut également effectuer un Ping entre les deux machines clientes pour vérifier leurs bonnes communications via ce tunnel IPSec:

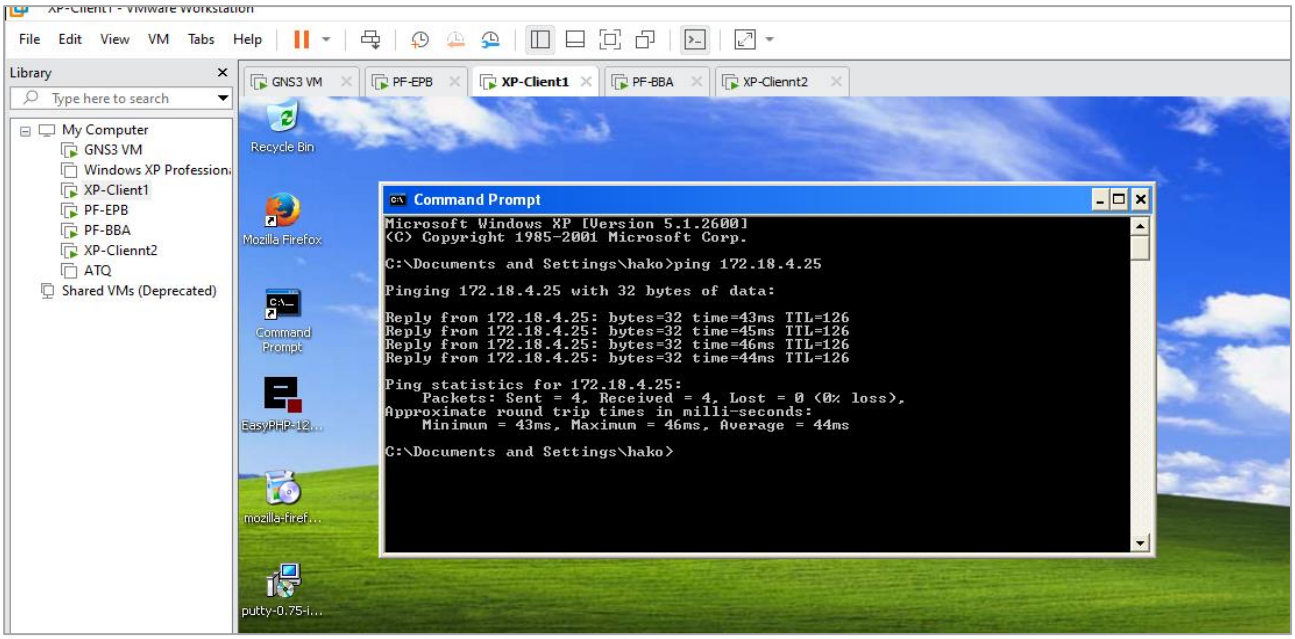


Figure 4.27 : Client1 au Client2.

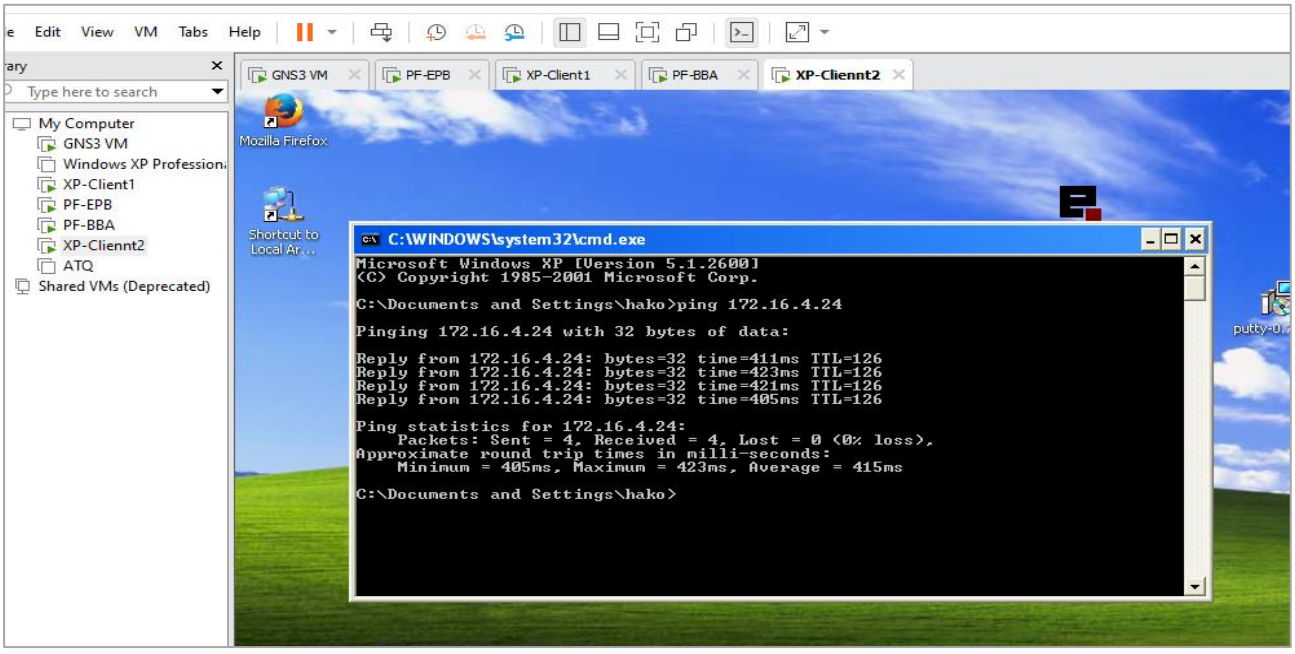


Figure 4.28 : Client2 au Client1.

Notre VPN est donc bien fonctionnel et les deux LAN arrivent désormais à communiquer au travers de notre tunnel IPSec.

4.7.2. Nmap :

Nmap ("Network Mapper") est un utilitaire gratuit et open source (licence) pour la découverte de réseau et l'audit de sécurité. De nombreux administrateurs système et réseau le trouvent également utile pour des tâches telles que l'inventaire du réseau, la gestion des programmes de mise à niveau

des services et la surveillance de la disponibilité de l'hôte ou du service. Nmap utilise des paquets IP bruts de manière innovante pour déterminer quels hôtes sont disponibles sur le réseau, quels services (nom et version de l'application) ces hôtes offrent, quels systèmes d'exploitation (et versions de système d'exploitation) ils exécutent, quel type de filtres de paquets, et des dizaines d'autres caractéristiques. Il a été conçu pour analyser rapidement les grands réseaux, mais fonctionne bien contre des hôtes uniques.

Nmap fonctionne sur tous les principaux systèmes d'exploitation informatiques et des packages binaires officiels sont disponibles pour Linux, Windows et Mac OS X. En plus de l'exécutable classique en ligne de commande Nmap, la suite Nmap comprend une interface graphique avancée et une visionneuse de résultats (Zenmap), un outil flexible de transfert de données, de redirection et de débogage (Ncat), un utilitaire de comparaison des résultats d'analyse (Ndiff) et un outil de génération de paquets et d'analyse de réponse (Nping) [27].

4.7.3. Test de SNORT :

Afin de réaliser ce test, nous avons utilisé la topologie visible sur l'image suivante :

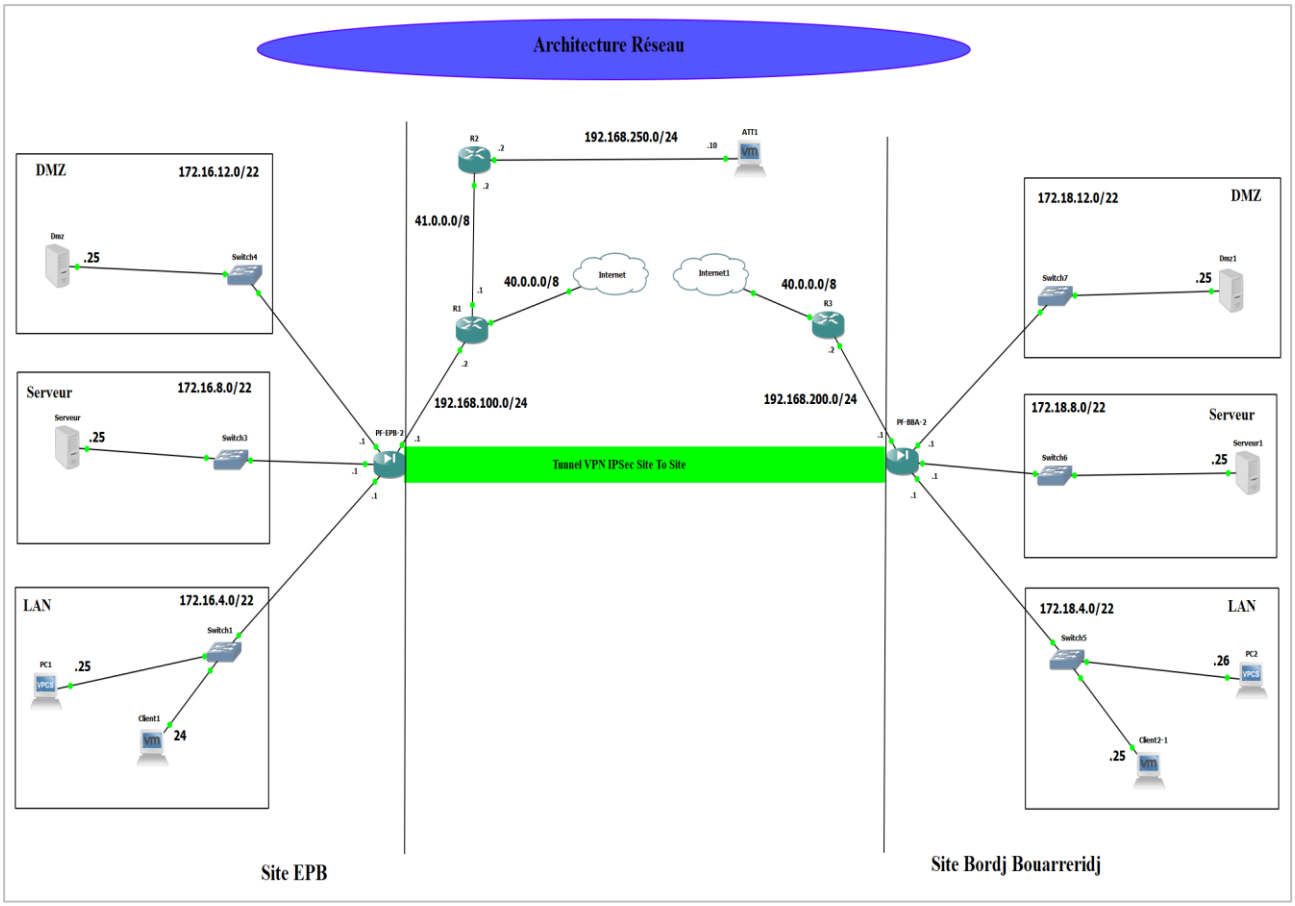


Figure 4.29 : La topologie utilisée.

Afin d'exécuter l'attaque, 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).

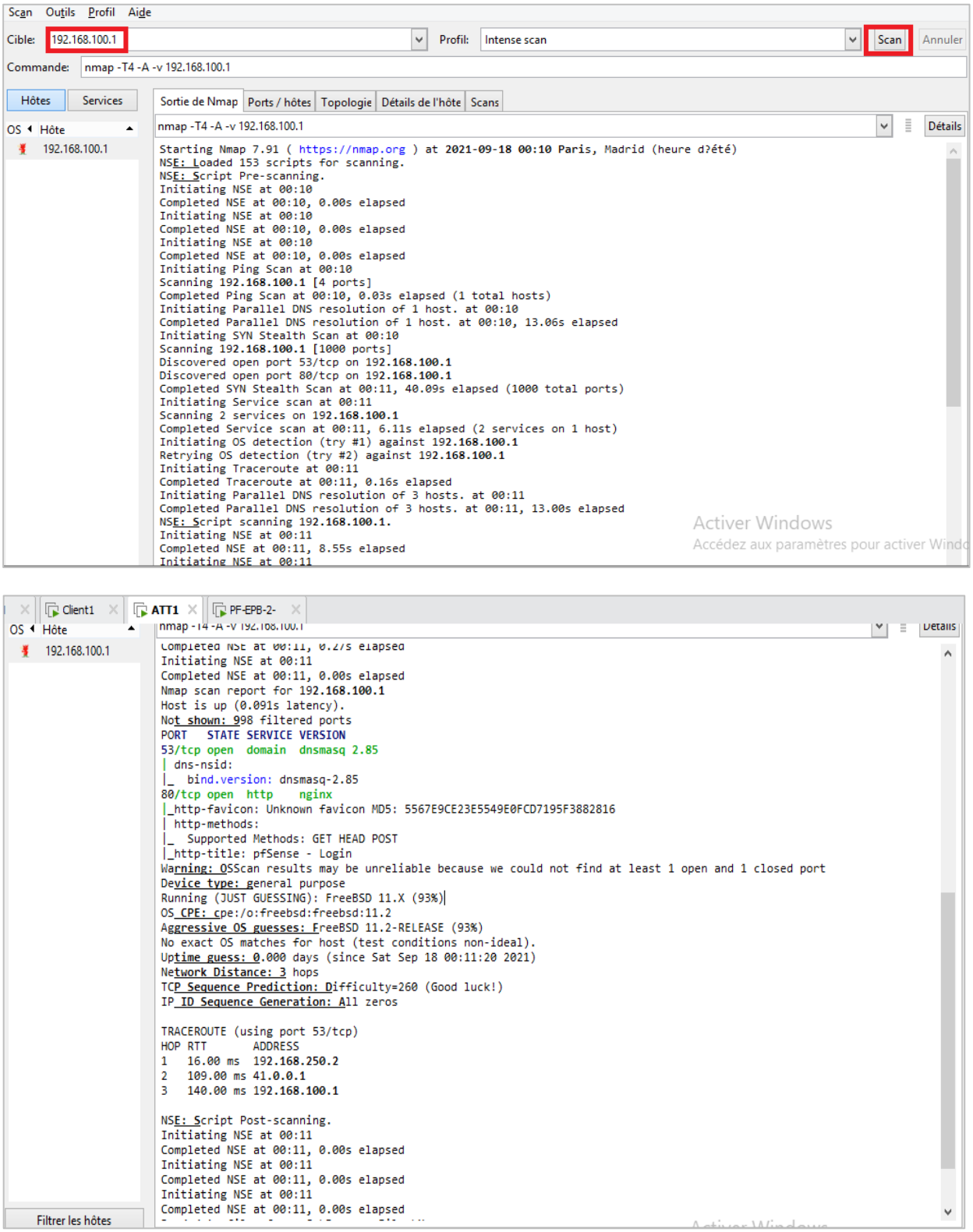


Figure 4.30 : Lancement de l'attaque.

Nous constatons clairement que SNORT détecte l'attaque, et affiche même l'adresse de l'attaquant.

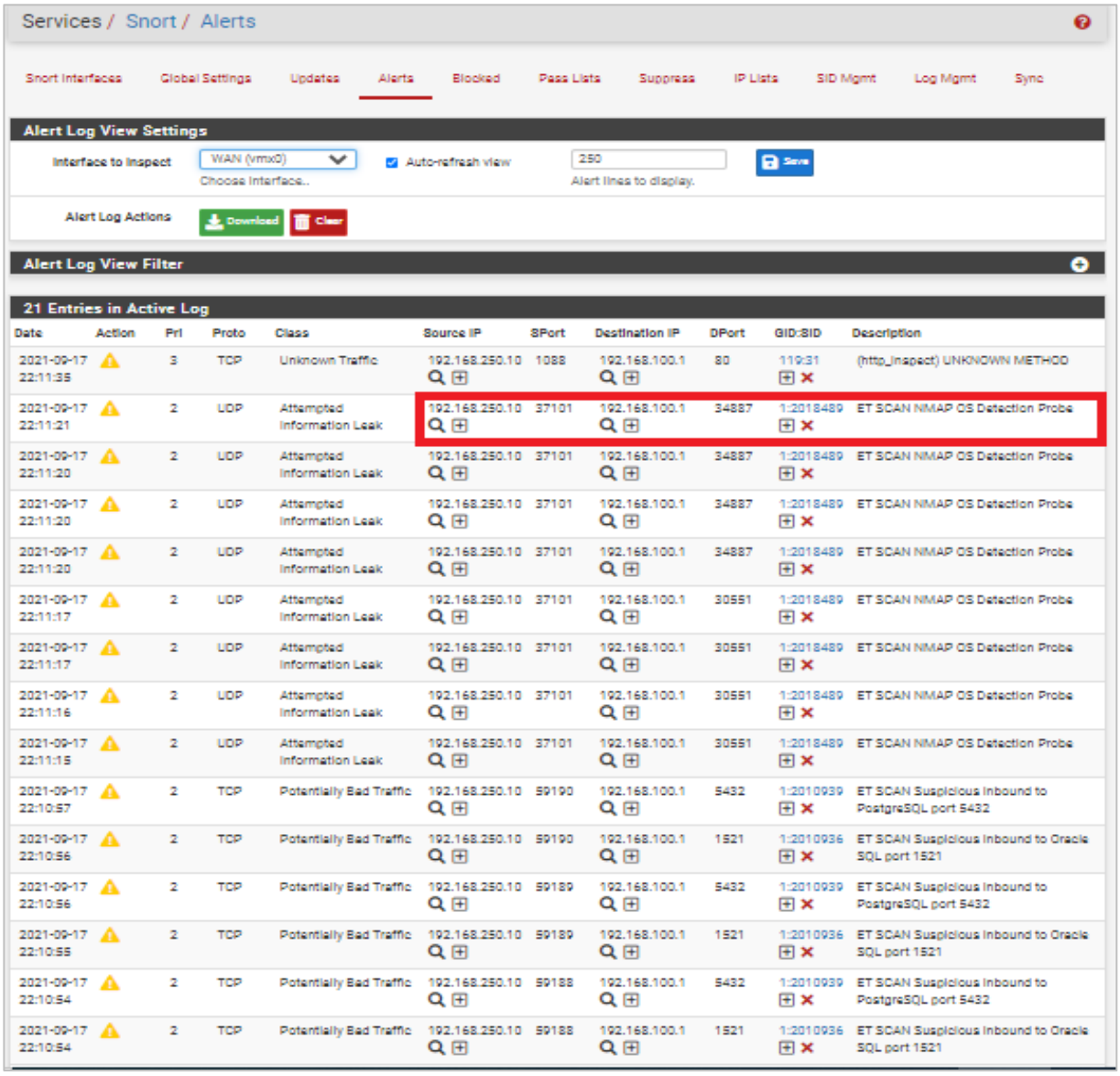


Figure 4.31 : Détection de l'attaque par Snort.

4.8. Conclusion :

Dans ce chapitre, nous avons présenté des outils importants pour la mise en place de Pfsense et SNORT. Ensuite nous avons donné toutes les étapes d'installation et configuration de ces derniers. On a rajouté aussi le VPN IPSec site à site qui permettant de connecter les deux sites d'une manière plus sécurisé. 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 GENERALE

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 la présentation de l'organisme d'accueil afin de prendre connaissance de l'entreprise ainsi que son environnement et l'architecture de son réseau, pour ensuite évaluer le niveau de vulnérabilité et établir un processus d'audit de sécurité pour ce dernier, pour ensuite présenter la sécurité des réseaux informatiques et ce en définissant entre autres les notions fondamentales du réseau informatique, les différentes attaques et contre-mesures de sécurité, Nous nous sommes par la suite penchés sur la présentation de système de détection et de prévention d'intrusion ainsi que l'environnement de travail.

Finalement, nous avons mis en place un VPN IPSec site à site et un Pfsense équipé de Snort afin d'améliorer le réseau de l'entreprise dans le but de renforcer sa sécurité.

Le stage effectué au sein de l'entreprise portuaire de Béjaïa nous a énormément apporté autant au niveau des connaissances sur le domaine qu'au niveau de l'expérience sur la manière de s'organiser et de travailler en groupe, ce qui sera bénéfique pour notre parcours professionnel.

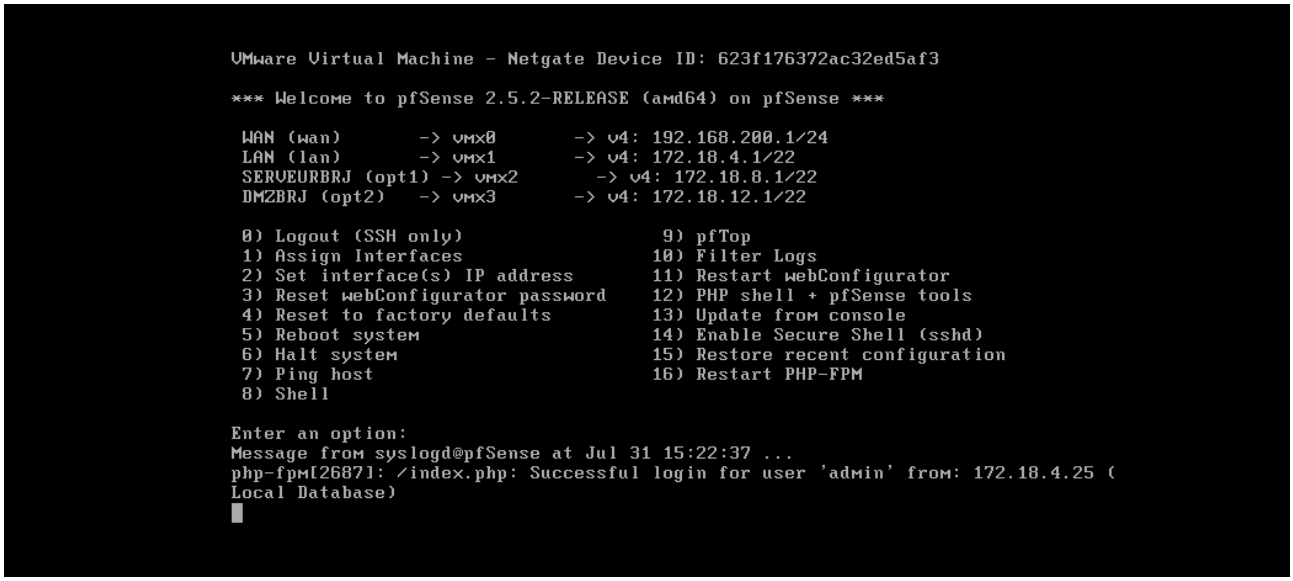
Annexe

Annexe-A. Configuration de Pfsense Bordj Bouarreridj :

1. La table d'adressage suivi dans ce projet :

Sous réseau	Adresse de sous réseau	Mask	Adresse de Diffusion	Passerelle
WAN	192.168.200.0	/24	192.168.200.255	192.168.200.1
LAN	172.18.4.0	/22	172.18.7.255	172.18.4.1
Serveur	172.18.8.0	/22	172.18.11.255	172.18.8.1
DMZ	172.18.12.0	/22	172.18.15.255	172.18.12.1

2. Configuration des quatre interfaces (WAN ,LAN, Serveur, DMZ) :

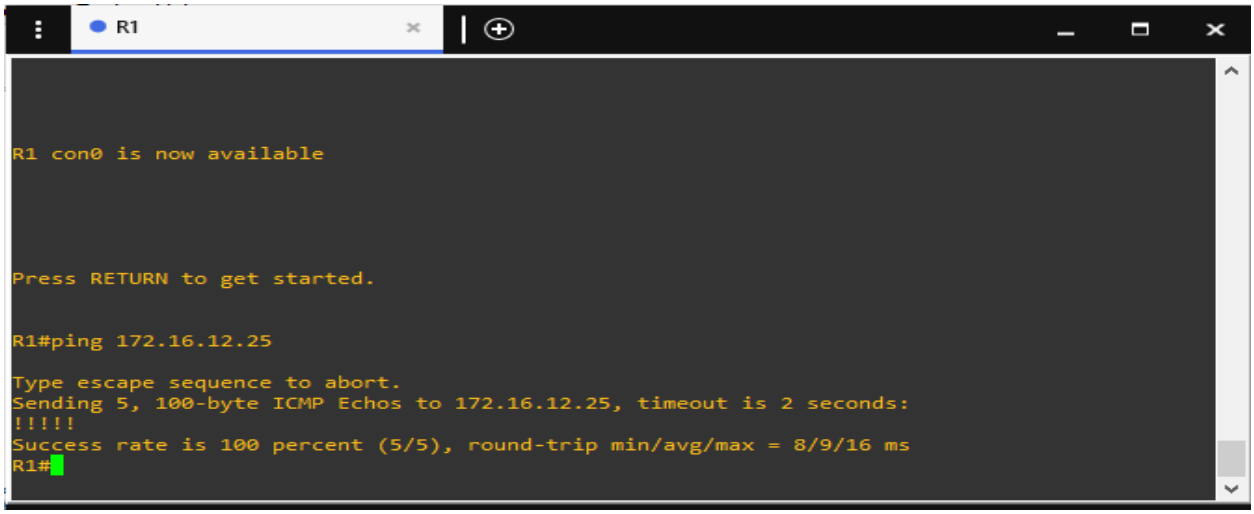


Annexe-B. Teste de connexion entre les réseaux après la configuration du Pfsense EPB :

Ici on va montrer la bonne communication entre les différents réseaux de notre entreprise et l'accès internet.

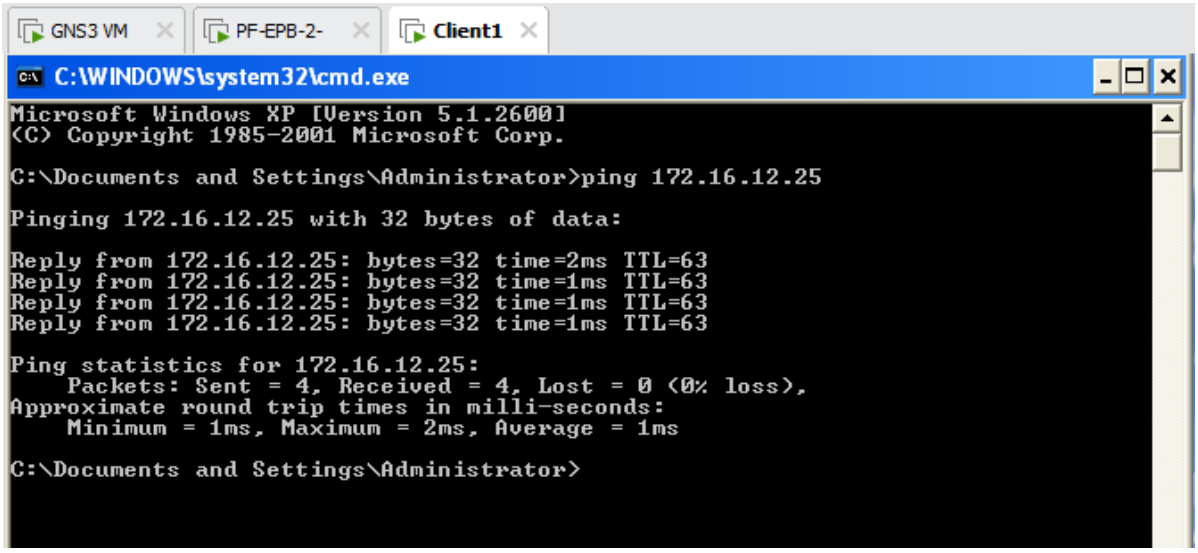
- **WAN vers DMZ :**

Cette figure illustre que les machines de WAN peuvent accéder aux serveurs de DMZ :



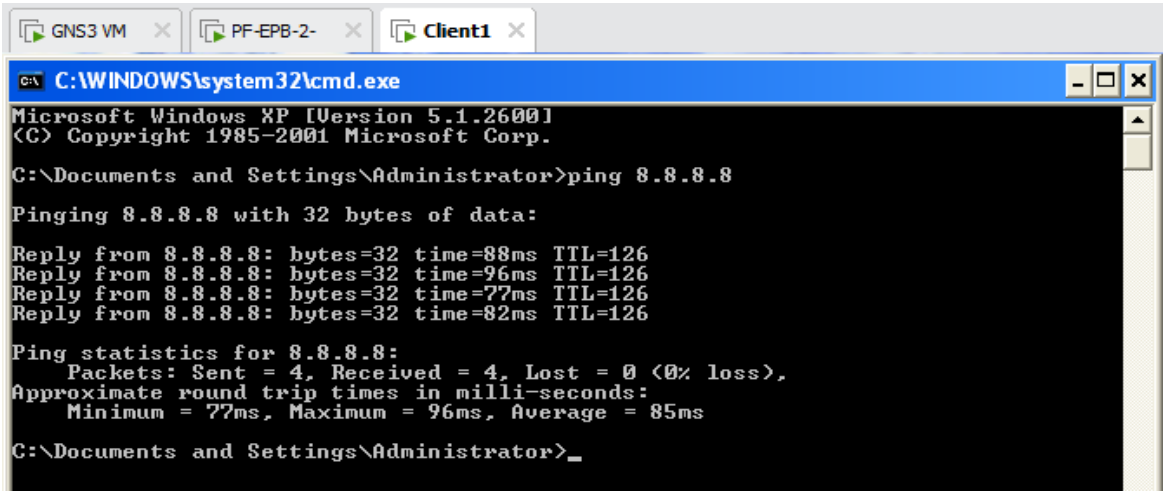
- **LAN vers DMZ :**

Cette figure illustre que les machines qui se trouvent sur le réseau local de gestion peuvent accéder aux serveurs qui se trouvent sur la DMZ :



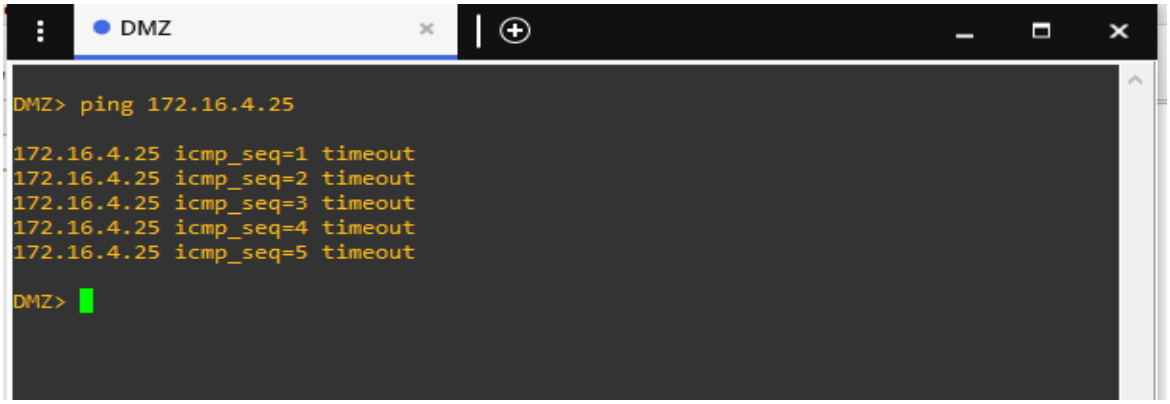
- **LAN vers WAN :**

Cette figure illustre que les machines qui se trouvent sur le réseau local peuvent accéder à internet et que le serveur DNS est bien configuré, car cette requête fait appelle en premier lieu au serveur DNS pour recevoir l'IP du serveur 8.8.8.8 puis on teste notre connexion à ce serveur :



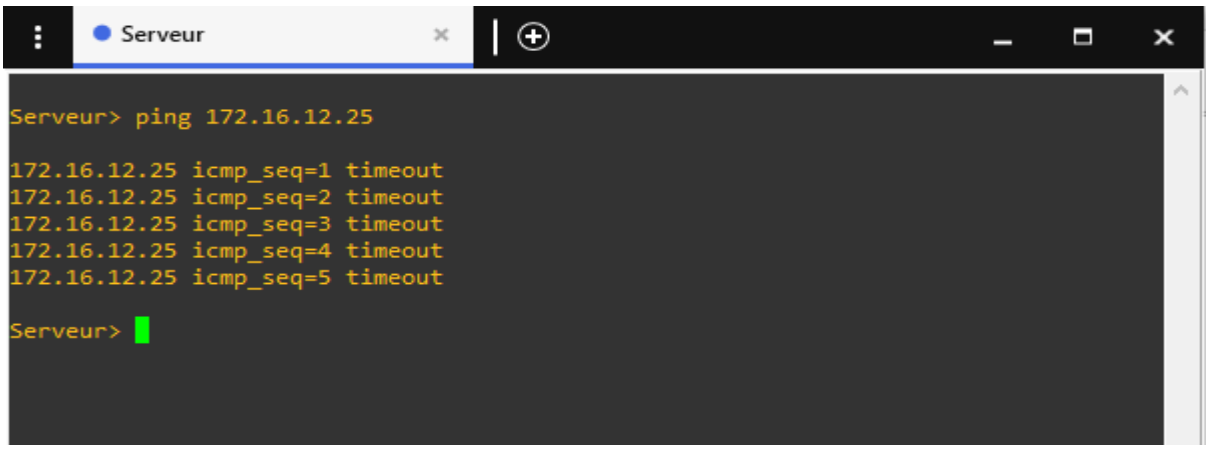
➢ **DMZ vers LAN :**

Cette figure illustre que les machines qui s'infiltrent dans la DMZ ne peuvent pas accéder au réseau local de l'entreprise (timeout) :



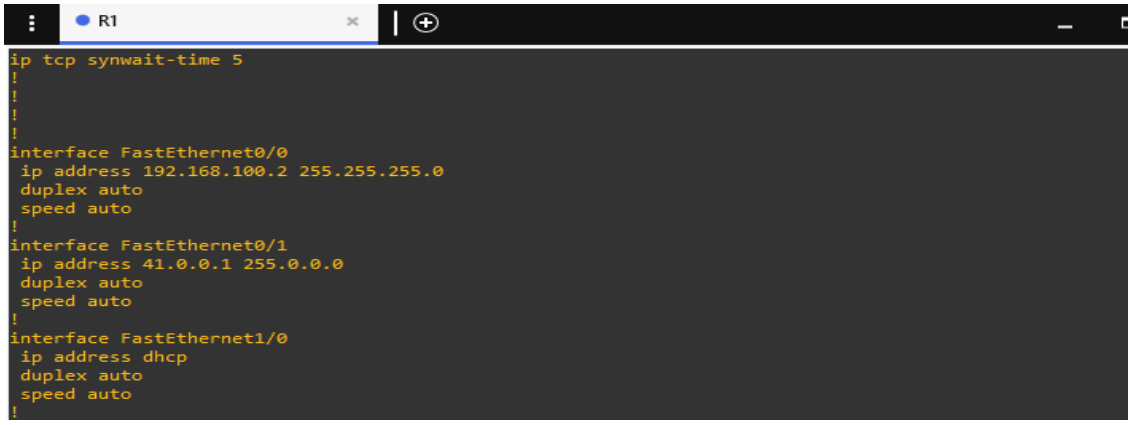
➢ **Serveur vers DMZ :**

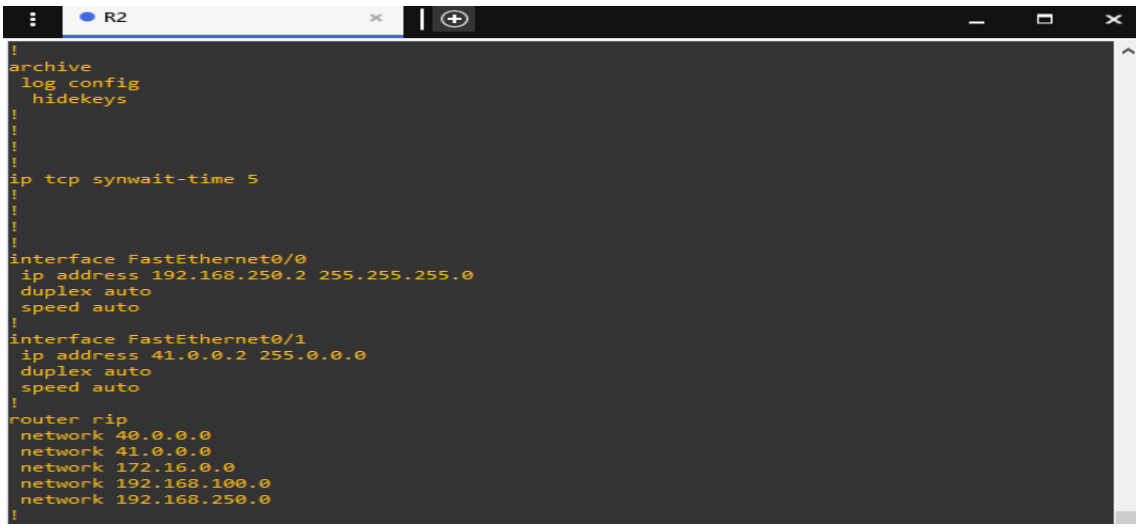
Cette figure illustre que les machines qui s'infiltrent dans le Serveur ne peuvent pas accéder au DMZ (timeout) :



Annexe-C. La configuration des routeurs :

La configuration des deux routeurs (R1, R2) est affichée sur les captures suivantes : on remarque que sur les interfaces fastethernet sont activées et bien configurées, et on a utilisé le routage dynamique (router rip) :





Références Bibliographiques

[1] EPB, (2019). Documentation de l'entreprise.

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

[3] Mme Claire. « Service AAA dans les réseaux ad hoc mobiles ».Thèse de Doctorat. Université Télécom Paris sud. 2012.

[4] https://www.networklab.fr/introduction-a-la-securite/. Consulté le 05/2021

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

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

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

[8] http://www.futura-sciences.com/tech/definitions/internet-firewall-474/. Consulté le 05/2021

[9] https://www.nbs-system.com/blog/howto-idsips.html#intro_ids. Consulté le 06/2021

[10] https://www.nbs-system.com/blog/howto-idsips.html#intro_ids. Consulté le 06/2021

[11] Gunadiz Safia. « Algorithmes d'intelligence artificielle pour la classification d'attaquer réseau à partir de 2donnée TCP ».Thèse de Doctorat. Université de Boumerdès-Mouhamed Bougara. 2011.

[12] AMAND Michaël et NSIRI Mohamed. « Etude d'un système de détection d'intrusion comportemental pour l'analyse du trafic aéroportuaire ».Rapport de projet LENAC. Janvier 2011.

[13] https://flylib.com/books/en/2.352.1/ids_and_ips_architecture.html#fastmenu_6. Consulté le 06/2021

[14] Miage kenitra et Hamzata Gueye. « Mise en place d'un IDS en utilisant Snort ». 2010.

[15] Nicolas Baudoin, Marion Karle. « NT Réseaux IDS et IPS ». 2003-2004.

[16] http://www-igm.univ-mlv.fr/~dr/XPOSE2004/IDS/IDSSnort.html. Consulté le 06/2021.

[17] http://lehmann.free.fr/RapportMain/node10.html. Consulté le 06/2021.

[18] SOUROUR Meharouech. « Optimisation de la Fiabilité et la Pertinence des Systèmes de Détection et Prévention d'intrusions ». Thèse de Doctorat. Ecole supérieure des Communications de Tunis Université 7 Novembre à Carthage. 2009/2010.

[19] BELKHTMI Keltouma, BENAMARA Ouarda. « Mise en place d'un système de détection et de prévention d'intrusion ». Mémoire de fin d'étude Master. Université A/Mira de Béjaïa. 2015/2016.

[20] Cédric MICHEL. «Langage de description d'attaque pour la détection d'intrusion par corrélation d'évènements ou d'alertes en environnement réseau hétérogène». Thèse de doctorat. Université de Rennes 1. Décembre 2003.

[21] https://blog.varonis.fr/ids-et-ips-en-quoi-sont-ils-differents/. Consulté le 06/2021.

[22] https://www.snort.org/. Consulté le 06/2021.

[23] https://eventus-networks.blogspot.com/2014/07/les-idsips-snort.html. Consulté le 06/2021.

[24] https://www.techno-science.net/glossaire-definition/VMware.html. Consulté le 07/2021.

[25] https://docs.netgate.com/pfsense/en/latest/general/index.html. Consulté le 07/2021.

[26] https://docs.gns3.com/docs/. Consulté le 06/2021.

[27] https://nmap.org. Consulté le 06/2021.

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 à la sécurité informatique et les attaques menaçant le réseau, présenter les différents mécanismes de sécurité (firewalls, proxy. . .), ensuite configurer un VPN IPSec site à site et 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 l'EPB. 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. Pfsense quant à lui est un pare-feu qui a gagné la confiance d'énormément d'entreprises partout dans le monde grâce notamment à sa simplicité d'utilisation et son efficacité.

Mots clés : Sécurité, Attaques, Détection, Intrusion, Menaces, VPN IPSec, Snort, Pfsense, Firewall, IDS.

Abstract:

Nowadays, computing networks increasingly exposed to attacks and intrusions due to the evolutions of the tools used by hackers. This is why it is said that a totally secure network is simply impossible to devise. Nevertheless, detecting and blocking intrusion attempts remains an important asset in the process of securing a computing network. This is made possible especially thanks to firewalls and IDS. The work achieved in this dissertation consists in studying the different aspects related to computing security and the attacks threatening the network, presenting the different security mechanisms (firewalls, proxy, . . .), then operating an VPN IPSec site to site and intrusion detection system called SNORT, which is associated with the firewall Pfsense, and implement all this at the level of the network architecture of EPB. SNORT imposed itself as the most performant and used intrusion detection system; it can perform an analysis of the network traffic in real time and thus detect numerous types of attacks. As for Pfsense, it is a firewall that won the trust of many companies all over the world especially thanks to its simplicity of use and efficiency.

Key words: security, attacks, detection, intrusion, threats, VPN IPSec, SNORT, Pfsense, firewall, IDS.