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 de Cycle
**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

**Réalisé par :**

**BIR Khaled** et **SAOUDI Yanis**

**Presenté par :**

| | | |
|---|---|---|
| **Président :** | M. **ATMANI Mouloud** | Université de Béjaïa |
| **Encadreur :** | Mme. **LARBI-MEZEGHRANE Wahiba** | Université de Béjaïa |
| **co-encadreur :** | M. **LARBI Ali** | Université de Béjaïa |
| **Examinateur :** | M. **AKILAL abdellah** | Université de Béjaïa |

2016-2017

# 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.

Nous tenons à exprimer notre sincère gratitude envers tout ceux qui nous ont aidés ou ont participé au bon déroulement de ce projet.

Nous sommes particulièrement reconnaissants envers nos encadreurs : Monsieur LARBI et madame LARBI d'avoir accepté de nous encadrer et de diriger notre travail, nous les remercions pour leur qualités professionnelles, leur patience, leurs remarques constructives et leurs aides inestimables.

Nous tenons à exprimer toute notre grande gratitude aux membres du jury : Monsieur ATMANI, Monsieur AKILAL d'avoir accepté de juger notre travail.

Par la même occasion, nous tenons à exprimer nos vifs remerciements à l'ensemble du personnel de l'entreprise NAFTAL spécialement nourdine et souhila, et du departement informatique qui ont nous procuré l'environnement adéquat et les moyens nécessaires à la réalisation de ce mémoire.

Nous adressons également nos remerciements à nos parents, nos ami(e)s et toutes les personnes proches qui ont contribué grâce à leur aide à la construction de ce travail.
.

# Dédicaces

**On dédie ce travail :**

A nos chers parents, pour tous leurs sacrifices,
leur amour, leur tendresse, leur soutien et leurs prières tout au long de nos études.

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

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

A tous nos amis(es).

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

**Khaled et Yanis**

# Table des matières

# Table des figures

# Liste des abréviations

| | |
|---|---|
| **AMG** | **A**dministration **M**oyen **G**énéraux |
| **ARP** | **A**ddress **R**esolution **P**rotocol |
| **CERT** | **C**omputer **E**mergency **R**esponse **T**eam |
| **CPU** | **C**entral **P**rocessor **U**nit |
| **CGI** | **C**ommon **G**ateway **I**nterface |
| **DMZ** | **D**emilitarized **Z**one |
| **DNS** | **D**omain **N**ame **S**erver |
| **FTP** | **F**ile **T**ransfer **P**rotocol |
| **GPL** | **G**az **P**étrole **L**iquéfie |
| **GNS** | **G**raphical **N**etwork **S**imulator |
| **HIDS** | **H**ost **B**ased **I**ntrusion **D**etection**S**ystem |
| **HTTP** | **H**yper **T**exte **T**ransport **P**rotocol |
| **IP** | **I**nternet **P**rotocol |
| **ICMP** | **I**nernet **C**ontrol **M**essage **P**rotocol |
| **IDS** | **I**ntrusion **D**etection **S**ystem |
| **IPS** | **I**ntrusion **P**revention **S**ystem |
| **KIS** | **K**espesky **I**nternet **S**ecurity |
| **LAN** | **L**ocal **A**rea **N**etwork |
| **MAN** | **M**etropolitan **A**rea **N**etwork |
| **MAC** | **M**edia **A**ccess **C**ontrol |
| **NIDS** | **N**etwork **I**ntrusion **D**etection**S**ystem |
| **NAT** | **N**etwork **A**ddress **T**ranslation |
| **OSI** | **O**pen **S**ystem **I**nterconnexion |
| **OSC** | **O**euvre **S**ociales **C**ulturelles |
| **PAN** | **P**ersonnel **A**rea **N**etwork |
| **PHP** | **P**ersonnel **H**ome **P**age |
| **PME** | **P**etite **M**oyenne **E**ntreprise |
| **RPC** | **R**emote **P**rocedure **C**all |
| **SING** | **S**ervice **I**nformation **G**estion |
| **SQL** | **S**tructured **Q**uery **L**anguagel |
| **UDP** | **U**ser **D**atagramm **P**rotocol |
| **UND** | **U**nité **N**aftal **D**istribution |
| **UMTS** | **U**niversal **M**obile **T**elecommunications **S**ystem |
| **VPN** | **V**irtual **P**rivate **N**etwork |
| **VLAN** | **V**irtual **L**ocal **A**rea **N**etwork |
| **VRT** | **V**ulnerability **R**esearch **T**eam |
| **WAN** | **W**id **A**rea **N**etwork |

# Introduction générale

Les réseaux informatiques sont devenus des ressources vitales et déterministes pour le bon fonctionnement des entreprises. De plus, ces réseaux sont ouverts de fait qu'ils sont pour la plus part raccordés à l'internet. Cette ouverture qui permet de faciliter la communication, engendre malheureusement des risques importants dans le domaine de la sécurité informatique.

Les utilisateurs de l'internet ne sont pas forcements pleins de bonnes intentions, ils peuvent exploiter les vulnérabilités des réseaux et systèmes pour réaliser leurs attaques. Les conséquences de ces attaques peuvent être lourdes pour un particulier (pertes d'informations, ou pire encore vol d'informations, atteinte à la vie privée..) et pour une entreprise (perte du savoir-faire..). Pour cela, les administrateurs déploient des solutions de sécurité efficace capable de protéger le réseau de l'entreprise.

Dans ce contexte, nous allons tout d'abord rappeler quelques notions concernant la sécurité informatique et les attaques qu'un réseau d'entreprise peut subir, ajouter a cela les solutions les plus répondus dans le domaine informatique .

Puis nous nous pencherons sur l'organisme d'accueil (NAFTAL) pour présenter son service informatique et analyser sa sécurité, pour ensuite proposer des solutions à ses vulnérabilités si elles existent.

Nous présenterons ensuite le concept de pare-feux et leurs différents types, puis nous nous pencherons d'IDS, les différents types d'IDS, leur mode de fonctionnement et les critères de test de ces derniers, ce qui nous amènera à nous intéresser spécifiquement à l'IDS SNORT.

Pour finir nous mettrons en place la solution de sécurité qui est l'IDS SNORT jumelé à un pare-feu qui est en l'occurrence PfSense pour une amélioration future de la sécurité du réseau de NAFTAL.

# Chapitre I

# La sécurité des réseaux informatiques

## I.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, et les équipements d'interconnexions, puis dans un second temps nous survolerons les objectifs et les terminologies de la sécurité informatique, ainsi que les différents dispositifs existants.

## I.2 Généralité sur les réseaux informatiques

### I.2.1 Définition

Un réseau informatique est un ensemble d'équipements appelés des nœuds ou encore des stations qui peuvent être (un ordinateur, portable, imprimante, routeur...) reliés ensembles par un support de transmission (câblage) ou par transmission par ondes comme le wifi, afin d'établir une connexion pour pouvoir échanger et partager des informations entre eux.

### I.2.2 Typologie des réseaux informatiques

#### 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. [**18**]

#### 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. [**18**]

#### 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. [**18**]

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

C'est une infrastructure Interconnectent sur quelques mètres des équipements personnels (tels que les terminaux : UMTS, portables, organiseurs,... etc.) d'un même utilisateur. [**18**]

### I.2.3 Catégories des réseaux informatique

On distingue également deux catégories de réseaux :

#### a) Le réseau (Peer to Peer ou pair à pair)

Le logiciel client et le logiciel serveur sont généralement exécutés sur des ordinateurs distincts, mais un seul ordinateur peut tenir simultanément ces deux rôles. Dans le cas des réseaux de particuliers et de petites entreprises, il arrive souvent que les ordinateurs fassent à la fois office de serveur et de client sur le réseau. [**18**]

#### b) Le réseau Server/Client

Sur un réseau a architecture client-serveur, tous les ordinateur (client) sont connectés à un ordinateur central (le serveur de réseau), une machine généralement très puissante en terme de capacité, elle est utilisé pour le partage de connexion, les logiciels centralisés et les fichier.

### I.2.4 Topologie des réseaux informatique

#### a) Les topologies physiques

Une topologie physique correspond à la disposition physique d'un réseau, mais ne spécifie pas les types de périphérique, les méthodes de connectivité ou les adresses d'un réseau. Les principales topologies physiques sont :

• **La toplogie en bus**

Dans cette topologie un même câble relie tous les nœuds d'un réseau sans périphérique de connectivité intermédiaire.

• **La toplogie en étoile**

Dans cette topologie, chaque nœud du réseau est relié à un périphérique central, tel qu'un concentrateur (hub). Un même câble de réseau en étoile ne peut relier que deux périphérique, donc un problème de câblage ne touchera jamais plus de deux nœuds .Les nœuds transmettent des données au concentrateur, qui a son tour retransmet les informations au segment de réseau ou le nœud de destination pourra les ramasser.

• **La toplogie en anneau**

Dans une topologie en anneau, chaque nœud est relié aux deux nœuds les plus proches, et l'ensemble du réseau forme un cercle, les données sont transmises autour de l'anneau dans une seule direction chaque station de travail accepte et répond aux paquets qui lui sont adressés, puis les fait suivre à la prochaine station de l'anneau.

• **La toplogie en maille**

Une topologie maillée, est une évolution de la topologie en étoile, elle correspond à plusieurs liaisons Point à point. Une unité réseau peut avoir une connexion point à point vers plusieurs autres unités.

• **La toplogie en arbre**

Aussi connu sous le nom de topologie hiérarchique, le réseau est divisé en niveaux. Le sommet, le haut niveau, est connectée à plusieurs nœuds de niveau inférieur, dans la hiérarchie. Ces nœuds peuvent être eux-mêmes connectés à plusieurs nœuds de niveau inférieur. Le tout dessine alors un arbre, ou une arborescence.

**b) Les topologies logiques**

Le terme topologie logique désigne la façon par laquelle les données sont transmises entre les nœuds, plutôt que la disposition des voies ou chemins qu'empruntent les données. Une topologie logique s'appelle aussi un système de transport réseau.

### I.2.5 Les équipements d'interconnexions

**a) La carte réseau**

Une carte doit être installée dans chaque machine devant être raccordée au réseau. Chaque carte possède une adresse MAC (Media Access Control) unique.

**b) Le concentrateur (hub)**

Le hub permet de connecter plusieurs machines (ordinateurs ou autre périphériques) entre elles. Son rôle est de diriger les données émises par un PC vers tous les autres équipements connectés (PC ou autres).

**c) Le commutateur (switch)**

Le commutateur est un hub intelligent, Il prend des décisions en fonction des adresses MAC (Media Access Control). En raison des décisions qu'il prend, le commutateur rend le LAN beaucoup plus efficace.

**d) Le routeur**

Un routeur il permet d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter. Dans les réseaux Ethernet les routeurs opèrent au niveau de la couche 3 (Réseau) de l'OSI (Open Systems Interconnection).

**e) Les ponts**

Un pont est un dispositif matériel permettant de relier des réseaux travaillant avec le même protocole.

**f) Le répéteur**

Un répéteur est un équipement simple permettant de régénérer un signal entre deux nœuds du réseau, afin d'étendre la distance de câblage d'un réseau. Le répéteur travaille uniquement au niveau physique (couche 1 (Physique) du modèle OSI).

**g) La passerelle**

Une passerelle applicative (en anglais « Gateway ») est un système matériel et logiciel permettant de faire la liaison entre deux réseaux.

**g) Le modem**

Un modem est un Périphérique qui envoie et reçoit des données informatiques via une ligne téléphonique ou un câble à haut débit.

### I.2.6 Architecture des réseaux

Le modèle OSI (Open System Interconnexion) et le modèle TCP/IP (Transmission Control Protocol/Internet Protocol) sont les principaux modèles utilisés en matière de fonctionnalités réseau. Chacun représente un type basique de modèle de réseau en couches. **[18]**

### a) Le modèle de référence OSI :

Le modelé OSI (Open System Interconexion) 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 : [**8**]

√ **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 tous les destination choisit par le meilleur itinéraire pour l'acheminement. Donc elle gère l'adressage logique et le routage.

√ **La couche liaison de données :** Elle est divisée en deux sous-couches :

- Couche LLC (Link Control) qui assure le transport des trame et gère l'adressage des utilisateurs.
- 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 donneés.

### b) Le 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. [**11**]

√ **La couche Application :** La couche application similaire a la couche homonyme de modèle OSI, correspond aux différentes applications utilisant les services réseaux pour communiquer a 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.

## I.3 la sécurité informatique

### I.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. [**2**]

### I.3.2 Objectif de la sécurité

Une politique de sécurité réseau vise à satisfaire les objectifs suivants :

√ **La confidentialité :** : Ensemble des mécanismes permettant qu'une communication de données reste privée entre un émetteur et un destinataire. Les données ne doivent être visibles que pour les personnes autorisées.

√ **L'authentification :** A pour objectif de vérifier l'identité des processus communicants.

√ **L'intégrité :** Ensemble des mécanismes garantissant qu'une information n'a pas été

√ **La non-répudiation :** Mécanisme permettant de garantir qu'un message a bien été envoyé par un émetteur et reçu par un destinataire.

√ **La disponibilité :** Son objectif est de garantir l'accès à un service ou à des ressources.

### I.3.3 Terminologie de la sécurité

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

**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. [**3**]

**b) 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. [**3**]

**c) 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. [**4**]

**d) 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.

**e) Contre mesure :**

Les contre-mesures donnent au système la capacité à réagir aux tentatives d'intrusions. [**4**]

**f) Cryptographie et Cryptanalyse :**

- **Cryptographie :** Étude des méthodes permettant de transmettre des données de manière confidentielle.
- **Cryptanalyse :** À l'inverse de la cryptanalyse est l'étude des procédés cryptographiques permettant de décrypter les textes chiffrés.

### I.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**]

- **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.
- **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.
- **Persist (Persister) :** Consiste en la création d'un compte avec des droits de super utilisateurs pour pouvoir se ré-infiltre ultérieurement. Une autre technique consiste à installer une application de contrôle à distance capable de résister à un cheval de Troie.
- **Propagate (Propager) :** Cette étape consiste à observer ce qui est accessible et disponible sur le réseau local.
- **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.

### I.3.5 Les types d'attaques

#### a) Les attaque réseaux

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

- ✓ **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. [**5**]
- ✓ **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. [**3**]
- ✓ **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.

La finalité est la même que l'IP Spoofing mais celle-ci se déroule au niveau de la couche liaison de donnée. Pour effectuer cette usurpation, il faut corrompre le cache ARP de la victime. Ce qui signifie qu'il faut lui envoyer des trames ARP en lui indiquant que l'adresse IP d'une autre machine est la sienne. [5]

✓ **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. Il existe deux techniques pour effectuer cette attaque. [5]

✓ **Fragments attacks :** 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. [5]

✓ **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. [5]

**b) Les attaque 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.

✓**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.

✓ **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.

✓ **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.

### I.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. [**9**]

∼ **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 var 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.

∼ **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 mal-intentionnées à des fins malicieuses.

∼ **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.

### I.3.7 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. [**19**]

### b) Antivirus

Il s'agit d'un logiciel capable de détecter et de détruire les virus contenus sur un disque. Le logiciel a pour charge de surveiller la présence de virus et éventuellement de nettoyer, supprimer ou mettre en quarantaine le ou les fichiers infectés. Ils surveillent tous les espaces dans lesquels un virus peut se loger. [**10**]

### c) VPN (Virtual Private network)

Est un service qui permet à un ou plusieurs postes distants d'établir des connexions prive sécurise 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.

### d) 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. [**20**]

### e) 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. [**20**]

### f) 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.[**7**]

### g) 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...). [**21**]

### h) 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 executer ensuite à partir du proxy et non du serveur distant qui héberge le site. [**21**]

## I.4 Conclusion

Au cours de ce chapitre, nous avons pris connaissance des différents aspects liées aux réseaux informatique et à leur sécurité, ainsi que les différentes menaces et attaques pouvant corrompre le bon fonctionnement d'un réseau.

Dans ce contexte, les pare-feu et les IDS constituent une bonne alternative pour mieux protéger les réseaux informatiquesn, à condition qu'ils soient bien configurés. Ce que nous détaillerons dans le chapitre qui suit.

# Chapitre II

# Les systèmes de détection d'intrusions et les pare-feux

## II.1 Introduction

Afin de détecter les attaques que peut subir un système, il est nécessaire de disposer d'un logiciel spécialisé dont le rôle est de surveiller les données qui transitent sur ce système et qui serait capable de réagir si des données semblent suspectes. En effet, dans ce chapitre nous allons présenter en première partie la fonctionnalité d'un pare-feu, ses types, ainsi que ses catégorie, en second partie, nous abordons le principe des systèmes de détections d'intrusion IDS, tout en énonçant leur types, leur protocoles dont ils utilise, ainsi que les avantages et les inconvénients.

## II.2 Pare-feux

### II.2.1 Définition d'un pare-feux

Les pare-feu sont des mécanismes de sécurité efficaces pour protéger un réseau interne contre toute attaque extérieure. En effet, un pare feu est un dispositif de sécurité conçu pour examiner constamment le trafic entrant et sortant sur le réseau.

Il joue le rôle d'une barrière de sécurité qui bloque ou laisse passer les paquets en fonction des règles de sécurité établies. De plus, un pare-feu permet de journaliser le trafic réseau en enregistrant les tentatives de connexions afin de pouvoir mieux l'analyser.

La mise en œuvre d'un pare-feu nécessite un certain nombre de choix faits par l'administrateur réseau : type du pare-feu, l'emplacement du pare-feu, la politique de sécurité, et le coût financier du pare-feu. [**12**]

### II.2.2 Fonctions d'un pare-feux

Les fonctions du pare-feu les plus répondues sont : [**13**]

**a) Blocage de trafic entrant en fonction de l'origine et de la destination :**

il s'agit de contrôler le trafic entrant d'un réseau et empêcher certains nœuds extérieurs de se connecter à un réseau local.

**b) Blocage de trafic sortant en fonction de l'origine et de la destination :**

il s'agit de contrôler le trafic sortant d'un réseau en direction d'internet, et notamment éviter que les utilisateurs accèdent à certains sites inappropriés.

**c) Blocage de trafic en fonction du contenu :**

un pare-feu peut inspecter le contenu du paquet IP en utilisant par exemple un scanner de virus intégré. Il peut aussi intégrer un filtre pour empêcher les emails indésirables.

**d) Etablir des rapports sur les trafics et l'activité du pare-feu :**

un pare-feu doit incorporer un mécanisme de reporting. Ce mécanisme permet d'établir des rapports sur son activité et les archiver dans un journal pour pouvoir l'examiner ultérieurement.

### II.2.3 Les différentes catégories de pare-feux

Essentiellement, il existe trois catégories de pare-feux :

**a) Pare-feu sans état (stateless firewall) :**

Ce pare-feu applique un mode de filtrage statique. Il permet d'inspecter les paquets qu'il reçoit pour valider les règles de la politique de sécurité. Ces règles sont basées sur l'en-tête du paquet IP (l'adresse IP de source et de destination, le protocole, le port de source et de destination pour les protocoles TCP et UDP). Il traite chaque paquet indépendamment des autres et décide, en fonction des règles stipulées par la politique de sécurité, de bloquer ou laisser passer le paquet. Cependant, ce type de pare-feu est incapable de détecter plusieurs attaques potentielles telles que l'usurpation de l'adresse IP (IP Spoofing), et certaines attaques par déni de service (DoS) qui nécessitent une solution dynamique en se basant sur l'analyse du trafic sur le réseau.[**16**]

**b) Pare-feu a état (stateful firewall) :**

Ce pare-feu applique un mode de filtrage dynamique. Il a été conçu pour remédier aux limites des pare-feux sans état. En effet, il inclut un mécanisme de reporting permettant d'établir des rapports sur le trafic et conserver les tentatives de connexions. Cette fonction permet de renforcer la capacité d'un pare-feu à détecter les attaques. Ce pare-feu opère au niveau de la couche réseau. Par conséquent, il est incapable d'œuvrer sur les failles logicielles au niveau de la couche application.[**16**]

**c) Pare-feu applicatif :**

Ce type de pare-feu incarne une politique de sécurité beaucoup plus stricte qu'avec un pare-feu à filtrage de paquets. Il opère au niveau de la couche application. Ce pare-feu empêche tout trafic qui ne respecte pas les politiques de sécurité spécifiées. Par exemple le pare-feu d'application de proxy permet d'accepter seulement les applications dont le proxy est configuré conformément à la politique de sécurité.[**16**]

**d) Pare-feu authentifiant :**

Les firewalls authentifiant permettent de mettre en place des régles de filtrage suivant les utilisateurs et non plus uniquement suivant des machine a travers le filtre IP.Il est alors possible de suivre l'activité réseau par utilisateur. Pour que le filtrage puisse être possible, il y a une association entre l'utilisateur connecté et l'adresse IP de la machine qu'il utilise.[**14**]

**e) Pare-feu personnel :**

Les firewalls personnels sont installés directement sur les postes de travail. Leur principale but est de contrer les virus informatiques et logiciels espion. Leur principal atout est qu'ils permettent de contrôler les accès aux réseaux des applications installes sur les machine. Ils sont capables en effet de repérer et d'empêcher l'ouverture de ports par des applications non autorisé à utiliser le réseau.[**14**]

### II.2.4 Les different types de pare-feux

**a) Les firewalls bridge :**

Ces derniers sont relativement répandus. Ils agissent comme de vrais câbles réseau avec la fonction de filtrage en plus, d'où leur appellation de firewall. Leers interfaces ne possèdent pas d'adresse IP, et ne font que transférer les paquets d'une interface à une autre en leur appliquant les règles prédéfinies.

Cette absence est particulièrement utile, car cela signifie que le firewall est indétectable pour un hacker lambda. En effet, quand une requête ARP (Address Resolution Protocol) est émise sur le câble réseau, le firewall ne répondra jamais. Ses adresses Mac ne circuleront jamais sur le réseau, et comme il ne fait que « transmettre » les paquets, il sera totalement invisible sur le réseau. Cela rend impossible toute attaque dirigée directement contre le firewall, étant donné qu'aucun paquet ne sera traité par ce dernier comme étant sa propre destination. Donc, la seule façon de le contourner est de passer outre ses règles de suppression.

- **Les avantages**
  - Impossible de l'éviter (les paquets passeront par ses interfaces.
  - Peu coûteux.

• **Les inconvénients**
  - Possibilité de le contourner (il suffit de passer outre ses règles).
  - Configuration souvent contraignante.
  - Les fonctionnalités présentes sont très basiques (filtrage sur adresse IP, port, le plus souvent en Stateless).

**b) Les firewalls matériels :**

Ils se trouvent souvent sur des routeurs achetés dans le commerce par de grands constructeurs comme Cisco ou Nortel. Intégrés directement dans la machine, ils font office de « boite noire », et ont une intégration parfaite avec le matériel. Leur configuration est souvent relativement ardue, mais leur avantage est que leur interaction avec les autres fonctionnalités du routeur est simplifiée de par leur présence sur le même équipement réseau.

• **Les avantages**
  - Intégré au matériel réseau.
  - Administration relativement simple.
  - Bon niveau de sécurité.

• **Les inconvénients**
  - Dépendant du constructeur pour les mises à jour.
  - Souvent peu flexibles.

**c) Les firewalls logiciels :**

Présents à la fois dans les serveurs et les routeurs "faits maison", ils sont assez souvent commerciaux et ont pour but de sécuriser un ordinateur particulier, et non pas un groupe d'ordinateurs. Souvent payants, ils peuvent être contraignants et quelque fois très peu sécurisés. En effet, ils s'orientent plus vers la simplicité d'utilisation plutôt que vers l'exhaustivité, afin de rester accessible à l'utilisateur final.

• **Les avantages**
  - Sécurité en bout de chaîne (le poste client).
  - Personnalisable assez facilement.

• **Les inconvénients**
  - Facilement contournable.
  - Difficiles à départager de par leur nombre énorme.

# II.3 Système détection d'intrusion

## II.3.1 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. Par définition, un IDS n'a pas de vocation préventive ou réactive dans la mesure où il n'empêche pas une intrusion de se produire. 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. Toutefois, il y'a des IDS qui réagissent suite à la détection d'une intrusion en mettant fin par exemple à une connexion suspecte.[**15**]

### II.3.2 Les différents types de systèmes détection d'intrusions

#### a) Les systèmes détection d'intrusions réseau (NIDS)

Les IDS réseaux analysent en temps réel le trafic qu'ils aspirent à l'aide d'une sonde carte réseau en mode promiscuous1. 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.[**1**]

- **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 est capable d'identifier les attaques de /à multiples hôtes.
  - L'IDS basé réseau assure une grande sécurité contre les attaques parce qu'il est invisible aux attaquants.
  - Il peut capturer le contenu de tout les paquets envoyés à un système cible.
  - Les NIDS sont des systèmes à temps réels.[**1**]
- **Les inconvénient 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.[**1**]
- **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.

– Les capteurs IDS sont parfois situes a l'entrée de zones du réseau particulièrement sensible (parcs de serveurs, donnes confidentielles), de façon à surveiller tout trafic en direction de cette zone.[**1**]

### b) Les Systèmes 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. Toutefois, ce type d'IDS présente une limitation qui se traduit par la nécessité d'avoir un système sain pour vérifier l'intégrité des données et donc un HIDS devient inefficace dans le cas où il est implémenté sur un système déjà infecté.[**1**]

• **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).[**1**]

• **Les inconvénient 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.[**1**]

• **L'emplacement des HIDS :**

– Les HIDS sont en général places sur des machines sensibles, susceptible de subir des attaques et possédant des données sensible pour l'entreprise. Les serveurs, web et applicatifs, peuvent notamment être protèges par un HIDS.[**1**]

### c) Les Systèmes détection d'intrusions hybrides

Les IDS hybrides rassemblent les caractéristiques des 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 lier les informations d'origines multiples. Ainsi, nous comprenons que les IDS hybrides sont basés sur une architecture distribuée, où chaque composant unifie son format d'envoi. Cela permet de communiquer et d'extraire des alertes plus pertinentes.[**1**]

• **Les avantages des IDS hybrides :**
  – Moins de faux positifs.
  – Meilleure corrélation (elle permet de générer de nouvelles alertes à partir de celles existantes).
  – Possibilité de réaction sur les analyseurs.[**1**]

### II.3.3 Les méthodes de détection d'intrusions

En général, il existe deux types d'approches pour détecter les intrusions dans les systèmes informatiques : l'approche comportementale basée sur un modèle constitué des actions autorisées, l'approche par scénarios basée sur un modèle constitué des actions interdites dans le système d'informations.[**1**]

#### a) Approche par scénario (Misuse Detection)

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.[**1**]

⋆ **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 connues d'un système et qui sont, en général, publiées par des organismes internationaux (comme le CERT : Computer Emergency Response Team). Le dernier type est utilisé pour coder le savoir-faire de l'administrateur réseau.[**1**]

⋆ **Reconnaissance de formes (Pattern Matching) :** Cette méthode consiste à identifier dans les paquets analysés une suite d'événements ou de caractères 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.[**1**]

#### b) Approche par comportementale (Anomaly 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 déclencher 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 des 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.

Plusieurs approches peuvent être utilisées pour la méthode de détection comportementale :[**5**]

⋆ **Approche probabiliste :** Cette approche consiste à établir des probabilités permettant de représenter une utilisation courante d'une application ou d'un protocole. Une alerte est alors générée si une activité ne respecte pas le modèle probabiliste.[**5**]

⋆ **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 et le data mining pour tenter d'avoir des résultats convaincants.[**5**]

⋆ **Algorithmes génétiques :** Les algorithmes génétiques utilisent la notion de sélection naturelle et l'appliquent à une population de solutions potentielles à un problème difficile (dont on ne sait pas trouver la solution optimale) pour trouver une solution approchée dans un temps raisonnable.[**5**]

### II.3.4 Critères de test d'un système détection d'intrusions

Lors de la mise en place d'un IDS, il est nécessaire de prendre en considération plusieurs critères permettant de choisir au mieux l'IDS. Tester un IDS avec des scanners de vulnérabilité est une mesure nécessaire pour évaluer un IDS, mais est loin d'être suffisante. D'autres critères doivent être pris en compte :

⋆ **Méthodes et capacités de détection :** Estimer le taux de faux positifs et la qualité d'information fournie par l'IDS.

⋆ **Rapidité :** Tester l'IDS en condition de charge élevée. Il est important de tester cela de manière réaliste, et non pas en utilisant des générateurs de paquets.

⋆ **Ouverture :** Il faut que l'IDS permette de modi ?é les signatures afin d'éviter certains faux positifs, mais aussi d'ajouter de nouvelles signatures spécifiques à l'environnement.

⋆ **Résistance aux techniques d'évasion :** Utiliser des outils tels que Whisker, Nikto, Babelweb, Fragroute ou Mendax pour observer le comportement de l'IDS.

⋆ **Architecture logicielle :** Pour les grandes entreprises, il est intéressant de pouvoir séparer les fonctions d'administration.

⋆ **Exploitabilité des données :** Il faut disposer d'outils permettant de retrouver et analyser facilement les événements suspects, car le volume généré par les IDS est important. Afin de centraliser les données, il peut être intéressant de disposer de consoles de reporting ou de tableaux de bord.

⋆ **Ergonomie :** Il existe différents types d'interfaces dans les IDS. Les interfaces graphiques qui sont adaptées aux particuliers ou aux PME. Les interfaces de type Web ou encore les interfaces en ligne de commandes réservées aux spécialistes.

D'autres critères, comme la réactivité de l'éditeur (mises à jour des signatures, correctifs...), ou le prix (solution libre ou non) rentrent en jeu. Pour évaluer un IDS, il est intéressant de pondérer chacun de ces critères selon l'importance qu'on leur attribue, et donner une note à l'IDS pour chaque critère .[**5**]

### II.3.5 Présentation de SNORT

Nous allons maintenant nous intéresser au système de détection d'intrusions le plus répondu et le plus abouti, à savoir SNORT. SNORT est un système de détection d'intrusions réseau en open source, capable d'effectuer une analyse du trafic réseau en temps réel et est doté de différentes technologies de détection d'intrusions telle que l'analyse protocolaire. SNORT peut détecter de nombreux types d'attaques, comme : les buffers over ?ows, les scans de ports, etc.

#### a) Architecture de SNORT

L'architecture de SNORT est modulaire elle est composée de :

- **Noyau de base "Packet Decoder" :** Au démarrage, ce noyau charge, compile, optimise et classe un ensemble de règles. Durant l'exécution, son rôle principal est la capture des paquets. [**20**]
- **Série de préprocesseurs "Detection Engine" :** Ceux-ci améliorent les possibilités de SNORT en matière d'analyse et de recomposition du trafic capturé. Ils reçoivent les paquets directement capturés et décodés, éventuellement les retravaillent puis les fournissent au moteur de recherche de signatures .[**20**]
- **Une série de "Detection Plugins" :** Après la détection, cette série est appliquée aux paquets. Ces analyses se composent principalement de comparaisons de différents champs des headers des protocoles (IP, ICMP, TCP, UDP) par rapport à des valeurs précises.[**20**]
- **Série de "Output Plugins" :** Permet de traiter cette intrusion de plusieurs manières, à savoir : l'envoie d'alertes vers un fichier log, l'envoie d'un message d'alerte vers un serveur syslog, le stockage de cette intrusion dans une base de données SQL.[**20**]

#### b) Mode de fonctionnement de SNORT

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

- **mode sniffer :** Dans ce mode, SNORT lit les paquets circulant sur le réseau et les affiche d'une façon continue sur l'écran. [**20**]
- **Le mode "Packet logger" :** Ci SNORT journalise le trafic réseau dans des répertoires sur le disque à savoir le fichier de log (/var/log/snort/). [**20**]
- **Le mode détecteur d'intrusions réseau (NIDS) :** Est là, SNORT analyse le trafic du réseau, le compare à des règles déjà définie par l'utilisateur et établit des

actions à exécuter.[**20**]

- **Le mode prévention des intrusions réseau (IPS) :** C'est "SNORT-Inline" ; décide du comportement du Pare-feu ; bloquer ou laisser passer des paquets.[**20**]

### c) SNORT dans le réseau

√ **Positionnement :** L'emplacement physique de la sonde SNORT sur le réseau a un impact considérable sur son efficacité. Dans le cas d'une architecture classique, composée d'un Firewall et d'une DMZ, trois positions sont généralement envisageables :

- **Avant le Firewall ou le routeur filtrant :**dans cette position, la sonde occupe une place de premier choix dans la détection des attaques de sources extérieures visant l'entreprise. SNORT pourra alors analyser le trafic qui sera éventuellement bloqué par le Firewall.[**20**]
- **Sur la DMZ :** Dans cette position, la sonde peut détecter tout le trafic filtré par le Firewall et qui a atteint la zone DMZ. Cette position de la sonde permet de surveiller les attaques dirigées vers les différents serveurs de l'entreprise accessibles de l'extérieur.[**20**]
- **Dans le réseau interne** Le positionnement du NIDS à cet endroit, nous permet d'observer les tentatives d'intrusion parvenues à l'intérieur du réseau de l'entreprise, ainsi que les tentatives d'attaques à partir de l'intérieur.[**20**]

√ **Déploiement :** Bien que SNORT puisse s'utiliser dans un petit réseau ou dans le cadre d'une utilisation personnelle, son déploiement au sein des grandes entreprises peut s'avérer plus problématique. En effet, SNORT ne constitue que la brique de base d'un système globale de détections des intrusions et ne fournit nativement aucun mécanisme de stockage des données ou d'exploitation de la somme. Pour remédier à ceci, il est courant d'utiliser SNORT en association avec des bases de données SQL et des interfaces d'exploitation utilisant un frontal Web.[**20**]

### d) Règles de SNORT

Les règles de SNORT sont composées de deux parties distinctes : le header et les options. Le header permet de spécifier le type d'alerte à générer (alert, log et pass) et d'indiquer les champs de base nécessaires au filtrage : le protocole ainsi que les adresses IP et les ports sources et destination. Les options, spécifiées entre parenthèses, permettent d'affiner l'analyse, en décomposant la signature en différentes valeurs à observer parmi certains champs du header ou parmi les données.[**20**]

√ **Action :** Une règle nous permet tout d'abord de définir une action, SNORT exécute cette action lorsqu'il trouve une correspondance entre un paquet et les éléments dans une composition de règle. Les cinq principaux types d'actions définis par SNORT sont les suivants :

- **Alert :** Génère une alerte en utilisant la méthode d'alerte sélectionnée et journalise le paquet.

  - **Log :** Journalise le paquet.
  - **Pass :** Ignore le paquet.
  - **Activate :** alerte et active une autre règle dynamique.
  - **Dynamic :** Reste passive jusqu'à être activée par une règle activate, alors agit comme une règle log.[**21**]

√ **Protocoles :** Il faut spécifier ensuite le protocole que SNORT doit analyser, il est en mesure d'analyser les protocoles TCP, UDP, ICMP et IP. Il est en outre tout à fait possible de créer des règles se rapportant aux protocoles des couches supérieures, il suffit pour cela de spécifier le numéro de port correspondant dans le champ "any".[**21**]

√ **Les adresses IP :** La section suivante de l'entête de règle s'occupe comme information de l'adresse IP et du port pour une règle donnée. Le mot clé "any" peut être utilisé pour définir n'importe quelle adresse.[**7**]

√ **Les numéros de ports** Les numéros de ports peuvent être spécifie de plusieurs manières, en incluant"any", en définissant des ports statiques ou des intervalles et des négations. Les ports "any" sont les valeurs génériques, signifiant littéralement tous les ports. Les ports statiques sont indiqués par un seul numéro de port, les intervalles de ports sont indiqués avec l'opérateur d'intervalle. [**7**]

√ **Les options des règles :** Les options de règle forment le cœur du moteur de détection d'intrusions de SNORT. Toutes les options de règle de SNORT sont séparées les unes des autres par un caractère de point-virgule ";". Les mots clés des options de règle sont séparés de leurs arguments avec un caractère "deux options". [**7**]

## II.4 Conclusion

Ce chapitre nous a permis de constater que les IDS sont de plus en plus fiables, d'où le fait qu'ils soient souvent intégrés dans les solutions modernes de sécurité. Les avantages qu'ils présentent par rapport aux autres outils de sécurité les favorisent. nous a également permis de comprendre que ces derniers sont indispensables aux entreprises afin d'assurer leur sécurité informatique. Aussi, Le firewall est un des éléments mis en place dans le cadre de la politique globale de sécurité. En effet, un pare-feu ne peut pas protéger de toutes les attaques, en particulier des attaques dirigées vers les données. Mais il est très utile (et très efficace si celui-ci est bien configuré) dans le domaine du contrôle des flux. L'avantage de ces firewalls filtrants est qu'ils permettent d'éviter la mise en place d'une architecture matérielle souvent coûteuse, dépendante du constructeur et lourde à administrer. Dans le chapitre qui suit nous présenterons l'organisme d'acceuil.

# Chapitre III

# Organisme d'accueil

## III.1 Introduction

Dans ce chapitre nous présenterons l'organisme d'accueil en étalons en première partie son historique ainsi que ses activité principale, puis les différentes divisions qui la constituent. Nous nous intéresserons aussi à la division informatique afin de comprendre l'architecture réseau de cette entreprise et énumérez les problèmes rencontrés en matière de réseau et sécurité, pour énoncer en second partie la problématique constatée au cours de notre stage et enfin conclure avec la solution modélisée pour pallier au manque constaté.

## III.2 Présentation de l'organisme d'accueil

### III.2.1 Historique de NAFTAL

Issue de SONATRACH, (société nationale pour la recherche, transport, production, transformation, la commercialisation des hydrocarbures), l'entreprise nationale de raffinage et de distribution de produits pétroliers (ERDP) a été créé par le décret N°80-101 du 06 avril 1980.Et entrée en activité le 01 janvier1982, elle est chargée de l'industrie de raffinage et de la distribution de produits pétroliers.

En 1984 : les anciens districts (Carburants, lubrifiants, pneumatique et bitume) ont été regroupés sous le nom UND (unité NAFTAL de distribution).

En 1987 : est désormais chargé de la commercialisation et la distribution des produits pétrolières et dérivés.

A partir de 1998, elle change de statut et devient société par action filiale à 100% de SONATRACH, avec un capital de 15 650 000 000 DA.[**17**]

### III.2.2 Mission et objectifs de NAFTAL

La mission principale de NAFTAL est la commercialisation et la distribution des produits pétrolière raffiné sur le marché national, notamment ; les carburants et le GPL

(gaz de pétrole liquéfie), bitume et lubrifiants, solvant, aromatique, paraffinés et pneumatique...etc. Afin de mener à terme sa mission principale, NAFTAL s'est tracé les objectifs suivants :

- développer, organiser la commercialisation et la distribution de produit pétrolière .
- stocker, transporter, et/ou faire transporter tous produits pétroliers commercialiser sur le territoire national.
- développer les infrastructures de stockage et de distribution pour assure une meilleure couverture du marché .
- élaborer des plans en liaison avec l'organisme concerné visant la couverture du marché national en produits pétrolière.
- promouvoir, participer et veiller à l'application de la normalisation et du contrôle de la qualité des produits relevant de son objet .
- centraliser les informations relatives aux besoins en produits pétrolière en vue de planifier et d'assurer l'approvisionnement du marché.
- procéder à toute étude du marché de consommation.
- développé et mettre en œuvre les actions visant l'utilisation optimale et rationnelle des infrastructures et moyens .
- participer et veiller à la mise en œuvre des actions visant le renforcement de l'intégration économique .
- concourir à la formation, au recyclage et au perfectionnement des travailleurs .
- assurer la maintenance des équipements, matériels roulants relevant de son patrimoine.[**17**]

### III.2.3 NAFTAL District Carburants de Bejaia

Le District CBR Bejaia est organisé comme suit :

#### a)Direction

Sont rattachés : Une secrétaire, le responsable de la sécurité industrielle, le laboratoire, le juridique les différents départements et dépôts carburants.

#### b)Département AMG (Administration et Moyen Généraux)

Le Département AMG Est subdivisé en quatre services ;

- **Service administration :** Il contient trois section, à savoir ; Section gestion du personnel, Section gestion paie, Section prestations sociales.
- **Services ressources humaines .**
- **Services du moyen généraux :** Ses activités sont assurées par trois sections ; Section bureau d'ordre, Section entretien bâtiment, Section économat.
- **Cellule OSC (Ouvre sociales et culturelles).**

### c) Département finances et comptabilité

Il comprend trois services à savoir :

- **Service trésorerie :** Il est composé de deux sections, la Section recettes et la Section dépense.
- **Service comptabilité :** Il est composé de deux sections, la Section SVCD et la Section comptabilité.
- **Service budgets et coûts .**

### d)Département Transport et Technique

Ce département comporte les services suivants :

- **Service exploitation et maintenance.**
- **Service études et réalisation.**

### e)Département Informatique

Le département est divisé en deux services :

- **Service Système Et Réseaux .**
- **Service Information De Gestion (ING).** [17]

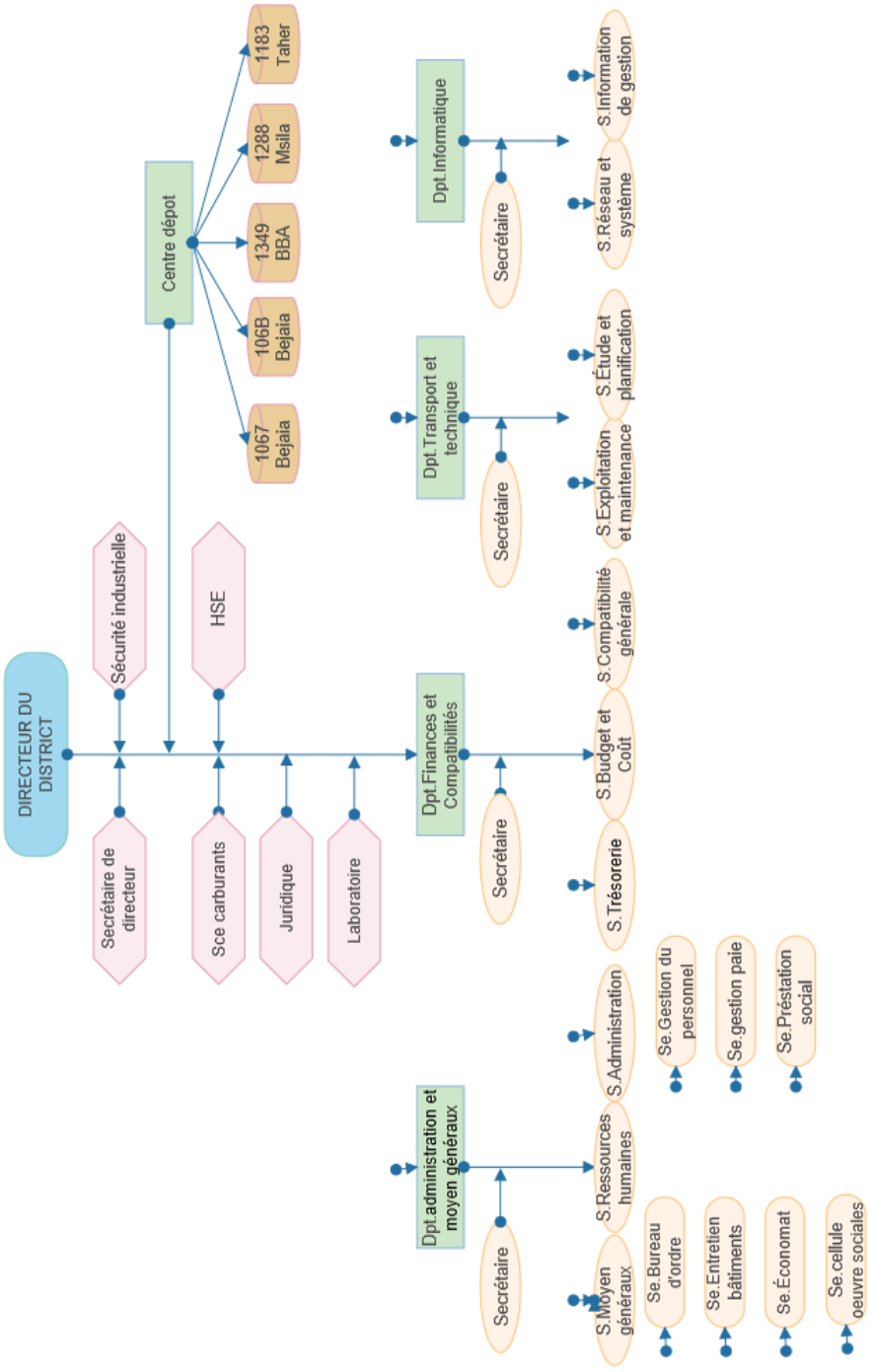



FIGURE III.1 – Organigramme du district carburant Bejaïa

### III.2.4 Infrastructure réseau du district carburant Bejaïa

#### a) Réseau local(LAN)

Le réseau local du district CBR de Bejaïa possède un service DHCP pour la distribution des adresses IP, un serveur DNS, un domaine active directory. Les machines du parc ont deux systèmes d'exploitation.Windows7, et Windows Serveur 2012 pour leur serveur, des switch.

Des imprimantes sont mises en réseau pour être partagées entre les employer afin que ceux-ci puissent y accéder sans avoir à transporter les documents d'un poste a un autre. Des onduleurs sont également mis à contribution en cas de coupures brusque du courant électrique. On dénombre un dans chacun des deux services informatique et d'autre dans les services cités plus haut,un swiche pour chaque etage.[**17**]

#### b) Réseau internet

Pour permettre la connexion des travailleurs à l'extérieur, NAFTAL se dote de deux connexions internet, connexion 3G de mobilis et une connexion d'une bande passante de 2Mo pour le fournisseur d'accès (Algérie télécom).

Ce réseau se compose d'un réseau filaire et d'un réseau wifi pour permettre l'accès à internet aux visiteurs.[**17**]

#### c) Parc informatique

- **Environnement client :** le district dispose d'un parc informatique composé :

| Equipements | Nombre | Modèle |
|---|---|---|
| PC Bureau | 89 | HP Compact 8300 I7 |
| PC Portable | 04 | HP Compact 600pro I7 |
| Imprimantes | 15 | EPSON ACULASER M2000 |
| Serveurs | 01 | Fujitsu Primergy D24529 |
| Photocopieuse | 04 | Xerox Work Centre 5020DN |

FIGURE III.2 – Tableau de l'équipement informatique du district carburant Bejaïa

- **Environnement serveur :** Le district dispose d'un serveur Windows 2012 qui permet de gérer et configurer les différents équipements de leurs réseaux.
- **Matériels d'interconnexion :** Les équipements d'interconnexion représentés le cœur du réseau dans une architecture. Ils pourront avoir des effets négatifs sur le trafic du réseau, pouvant entrainer la détérioration de celui-ci. Dans notre cas d'étude, l'infrastructure du réseau de district embryonnaire, comporte 13 commutateurs CISCO CATALYSE 2960 de 24 ports et un commutateur fibre optique CISCO 3750 pour l'interconnexion des différents clients et d'un routeur CISCO 2911.[**17**]

### d)Architecture réseau du district carburant Bejaïa

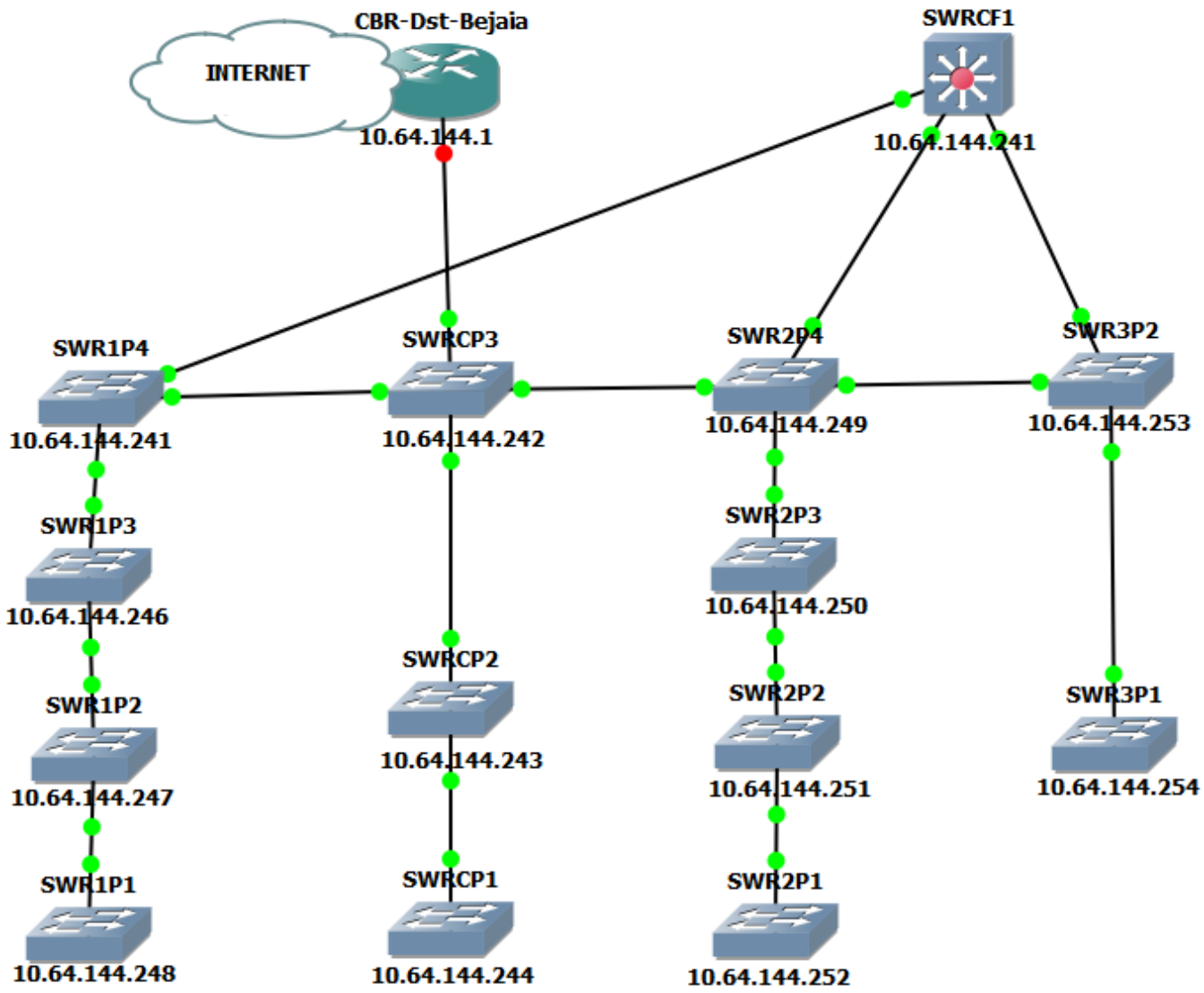



FIGURE III.3 – Architecture réseau de l'entreprise NAFTAL

### e)la sécurité au niveau du réseau NAFTAL

L'entreprise NAFTAL utilise une application de sécurité (Kaspersky Internet Security) sur chaque machine pour les surveiller et bloquer quelques actions malveillantes, ainsi que l'utilisation des VPN pour communiquer avec d'autres sites distants en tout sécurité.[**17**]

## III.3 Problématique

Aujourd'hui l'internet apporte une réelle valeur ajoutée aux entreprises, en permettant la communication avec de nombreux partenaires, fournisseurs et clients, ceux-ci expose les systèmes des entreprises à de nouvelles formes de menaces. Le véritable défi est La sécurisation du réseau informatique pour conserver un haut degré de fiabilité du trafic sur le réseau. Au cours de nos visites au sien de l'entreprise NAFTAL nous avons constaté des anomalies au niveau de la sécurisation du réseau de l'entreprise, nous les énumérons comme suit :

- Les seuls systèmes de sécurité utilisée sont des antivirus installés sur les machines.
- Absence d'utilisation de pare-feu permettant de filtrer le flux de données circulants sur le réseau.
- Aucun système de détection d'intrusion n'est mis en place.
- Aucun système de protection contre la divulgation de donné interne.

## III.4 Solution proposée

Pour pallier au problème énuméré dans la problématique, nous proposons d'implémenté un firewall afin de filtrer le flux de données traversant le réseau, mais le firewall n'est pas suffisant à l'avenir car ce dernier ne permet pas d'interdire les actions malveillantes venant de stations non protégées.

De ce fait en plus du pare-feu, nous allons proposer la mise en place d'un système de détection d'intrusion (IDS) connue sous Snort car il joue un rôle de complément aux firewalls en lui permettant une analyse plus intelligente des paquets constituant les données circulantes en détectant toute activité suspecte.

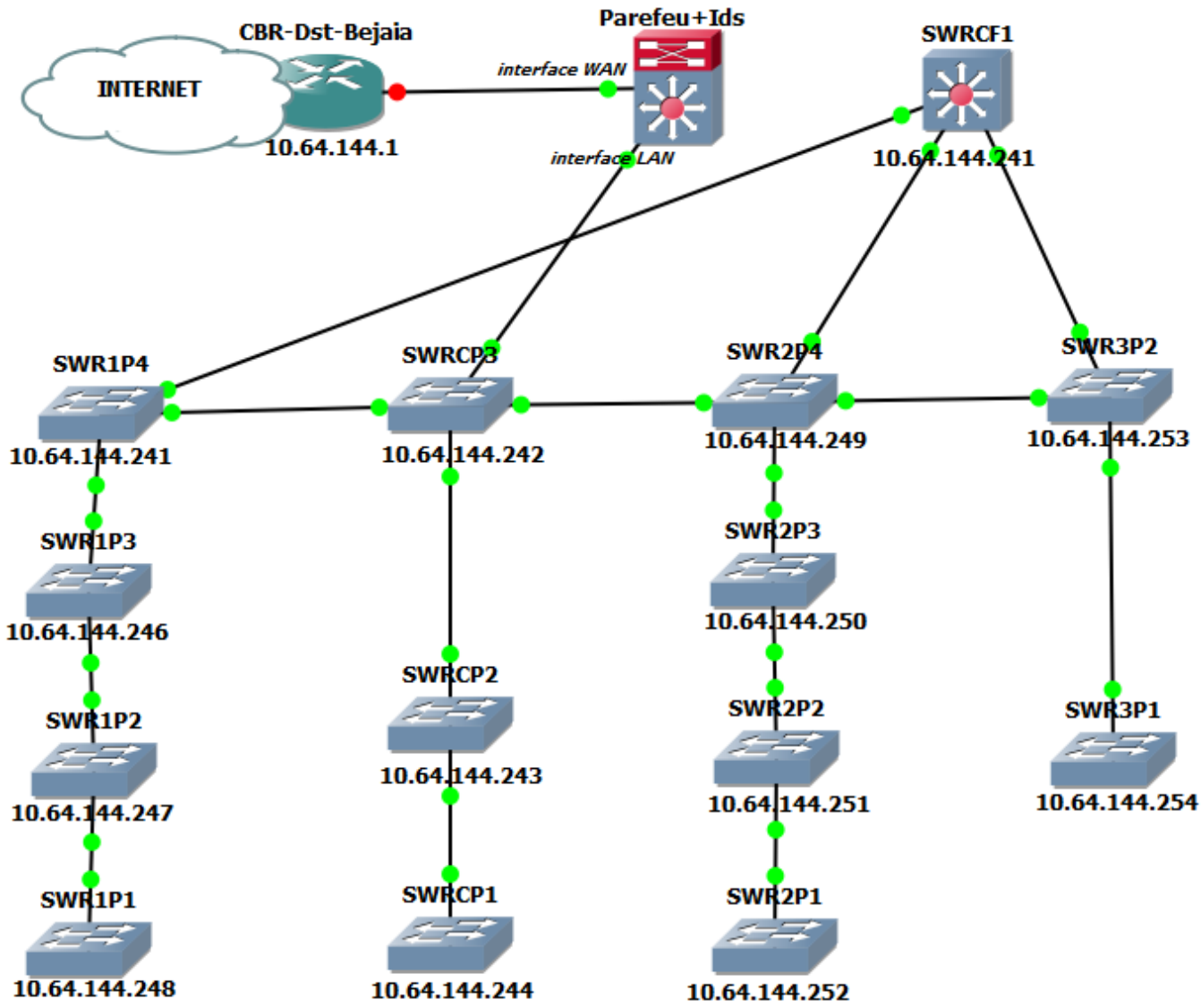



FIGURE III.4 – Architecture réseau proposeé pour l'entreprise

# Conclusion

Dans ce chapitre nous avons pris connaissance du système d'information de l'entreprise NAFTAL ainsi que l'architecture réseau la constituant dont on a relevé quel que faille de sécurité, pour y remédier, nous avons fini par proposer une solution qui consiste à mettre en place une nouvelle architecture comportant un pare-feu équipé d'un IDS, dont on va détaillé l'implémentation dans le chapitre suivant.

# Chapitre IV

# Test et mise en œuvre de la solution

## IV.1 Introduction

Dans ce dernier chapitre, nous allons voir un cas pratique concernant pfsense et l'implémentation de la plateforme de snort, nous allons voir comment installer ses différents composants, ainsi que toutes les configurations nécessaires. Enfin, nous allons donner quelque tests que nous avons réalisés en lançant quelques attaques et voir comment ces derniéres sont détectées et bloquées.

## IV.2 Présentation de l'environnement

### IV.2.1 VMware Workstation

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.[**23**]

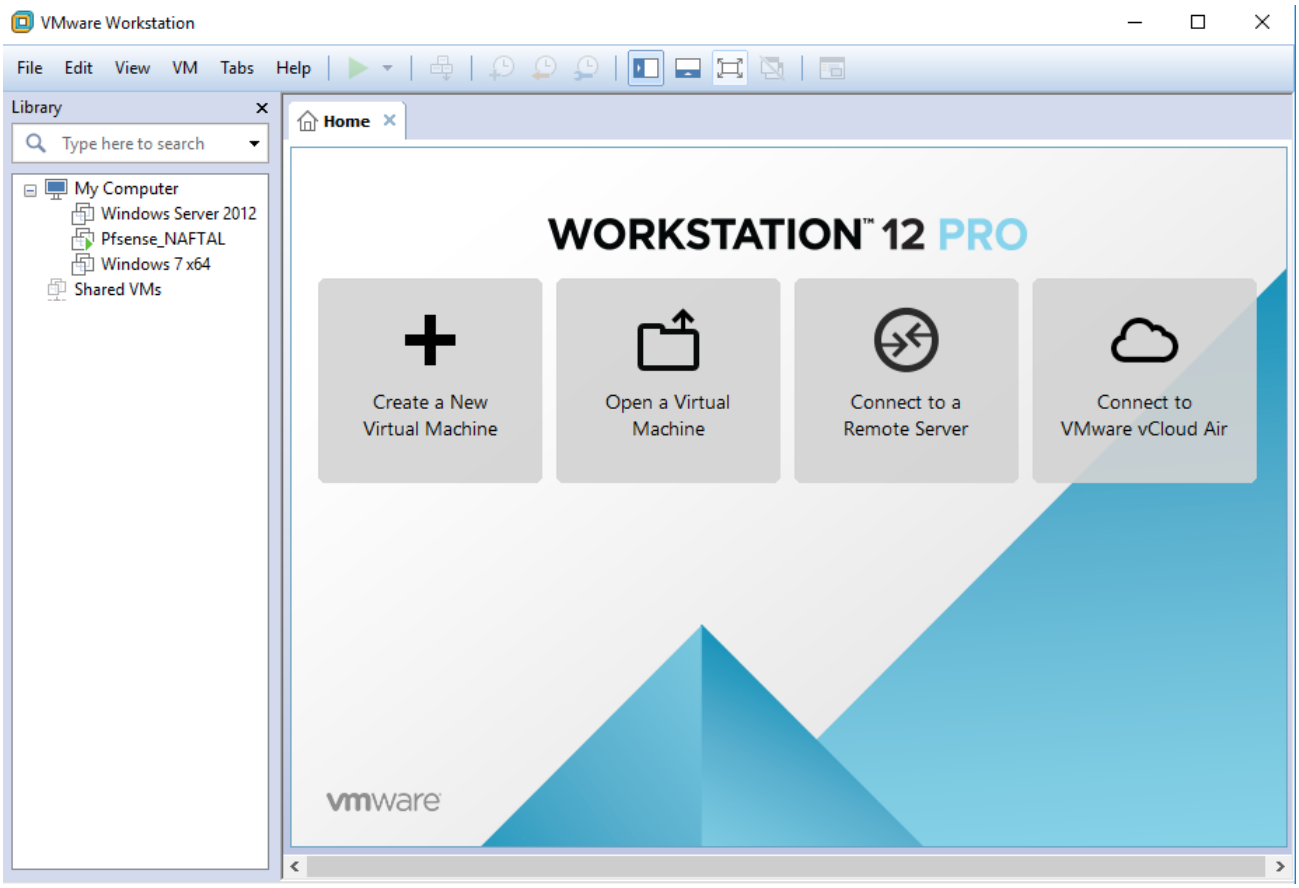



FIGURE IV.1 – VMware workstation 12.0 professionnel

### IV.2.2 Pfsense

pfSense est libre, une distribution personnalisée de FreeBSD adapté pour être utilisé comme routeur et pare-feu. En plus d'être une plate-forme puissante, flexible de routage et de pare-feu, il comprend une longue liste de caractéristiques connexes et un système de package permettant en outre l'évolutivité sans ajouter de ballonnement et de failles de sécurité potentielles à la distribution de base. pfSense est un projet populaire avec plus de 1 million de téléchargements depuis sa création et approuvé dans d'innombrables installations allant des petits réseaux domestiques pour protéger un ordinateur unique, pour les grandes entreprises, les universités et d'autres organisations protégant des milliers de périphériques réseau.[**24**]

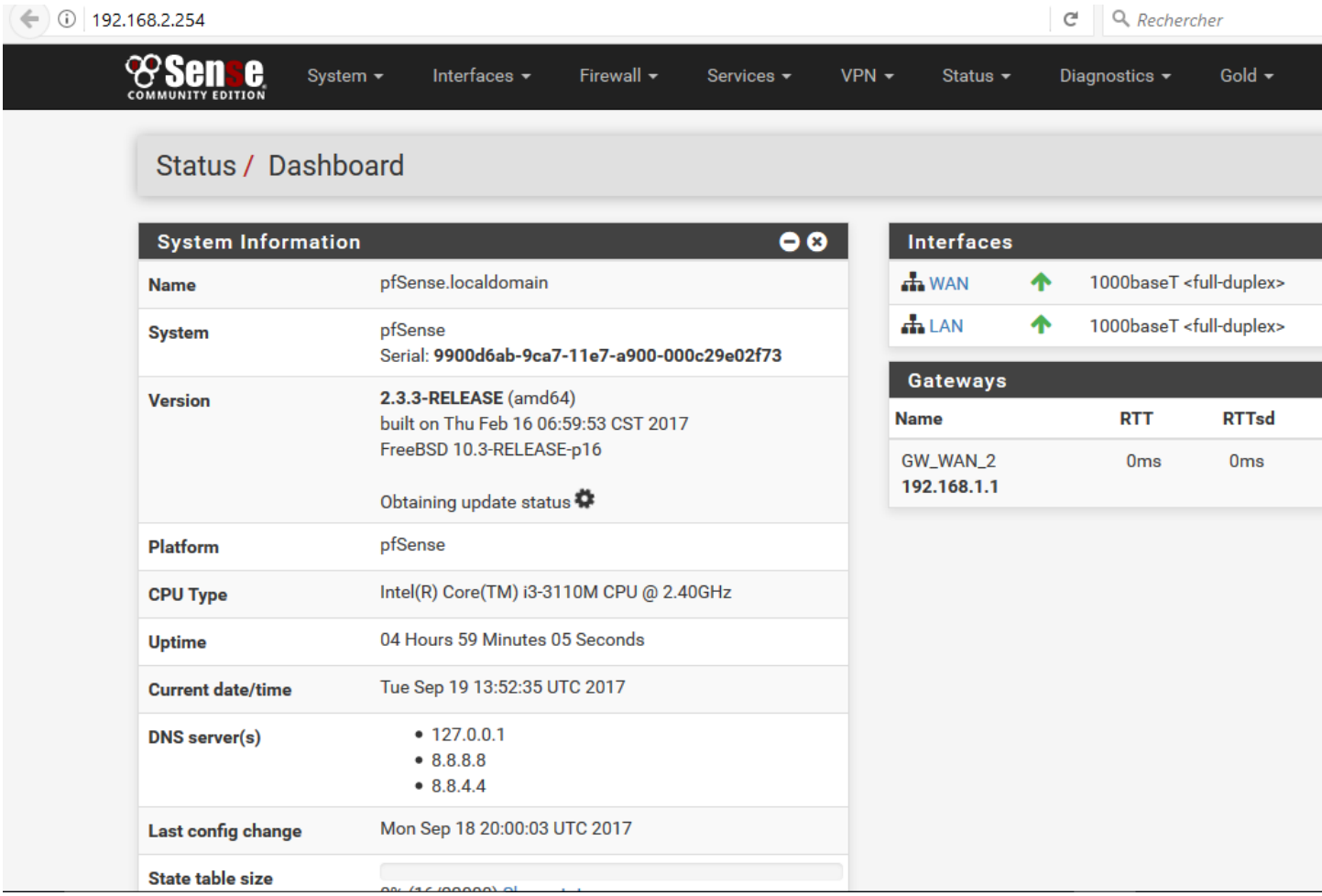



FIGURE IV.2 – Pfsense 2.3.3-release

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

- Pare-feu : indispensable pour une distribution "firewall" ;).
- Table d'état : La table d'état ("State Table") contient les informations sur les connexions réseaux. Cela permet d'avoir un aperçu des connexions et surtout de créer des régles par exemple sur le nombre de connexion maximum pour un hôte.
- Traduction d'adresses réseaux (NAT).
- VPN : permet la création de VPN IpSec, OpenVPN ou PPTP.
- Serveur DHCP.
- Serveur DNS et DNS dynamiques.
- Portail Captif.
- Proxy et Blacklist SQUIDGUARD.
- Gestion des VLAN.
- IDS-IPS SNORT.

### IV.2.3 Package SNORT

Snort est un système de détection d'intrusion de réseau open source (NIDS) créé par Martin Roesch. Snort est un sniffer de paquets qui surveille le trafic réseau en temps réel, scrutant chaque paquet de manière étroite pour détecter une charge utile dangereuse ou des anomalies suspectes. Snort est basé sur libpcap (pour la capture de paquets de bibliothèque), un outil largement utilisé dans les sniffers et les analyseurs de trafic TCP / IP. Grâce à l'analyse du protocole et à la recherche de contenu, Snort détecte les méthodes d'attaque, y compris le déni de service, le dépassement de tampon, les attaques CGI, les balayages de port furtif et les sondes SMB. Lorsque des comportements suspects sont détectés, Snort envoie une alerte en temps réel à syslog, à un fichier d'alertes distinct ou à une fenêtre contextuelle.**[25]**

### IV.2.4 Simulateur graphique de réseau(GNS3)

#### a) Définition

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

#### b) Les composants du logiciel

Afin de fournir une simulation précise et complète, GNS3 est fortement lié à [27] :
- 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.

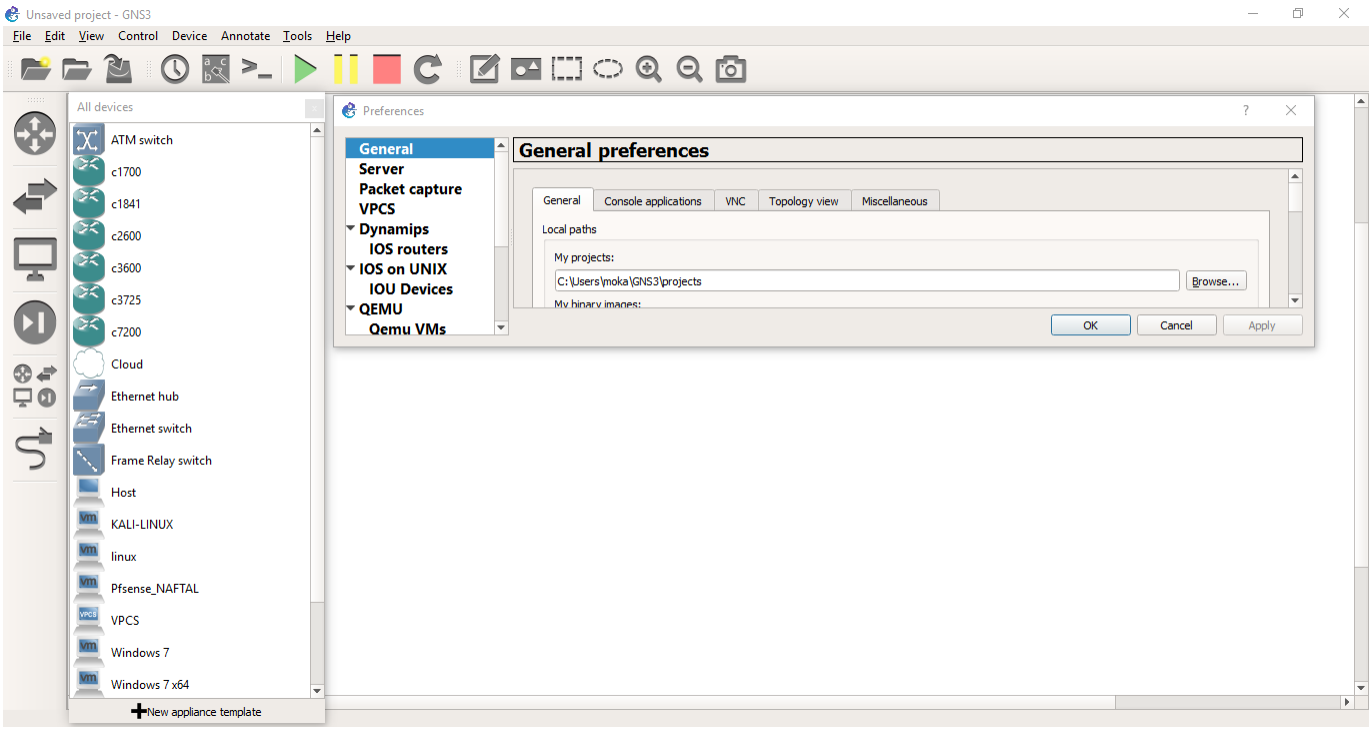



FIGURE IV.3 – GNS3 Graphical Network Simulator version 1.5.2

# IV.3 Configuration du pare-feu

## IV.3.1 Installation de pfsense

Pour commencer,il faut disposer d'une image iso de Pfsense version 2.3.3-RELEASE Basé sur FreeBSD, cette images est disponible sur https ://Pfsense.org/dowlnload.

On utilise une machine virtuelle disposant de cartes réseaux une reliée au réseau local et l'autre branchée au réseau WAN. cette capture montre l'ajout des deux cartes réseaux que nous allons utiliser.

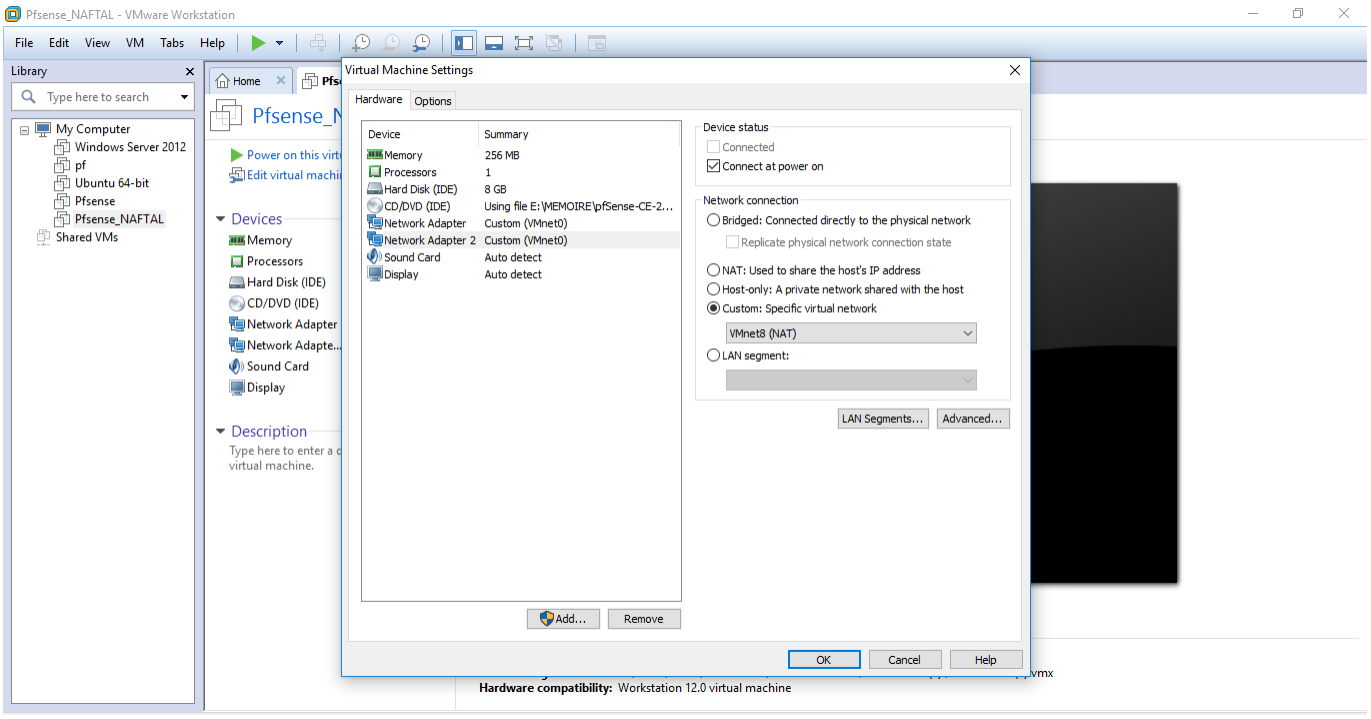
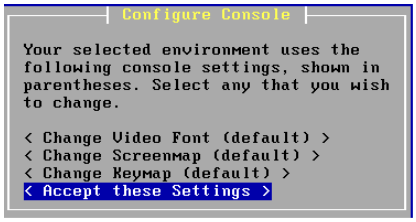
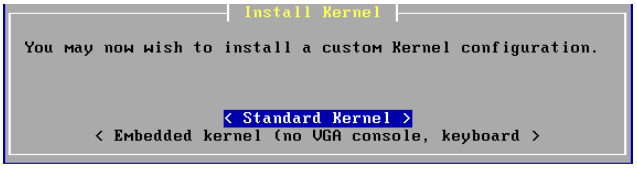
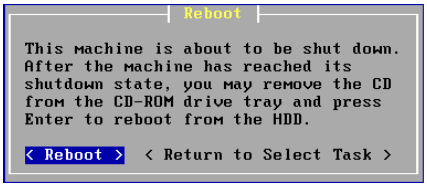



FIGURE IV.4 – Configuration des cartes réseau de pfsense

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



### IV.3.2 Configuration des interfaces

Une fois l'installation terminée, nous allons maintenant configurer les interfaces , en choisissant l'option 2 puis les numéros correspondants a l'interfaces souhaiter configurer, par exemple pour l'interface LAN c'est le numéro 2, on affecte une adresse IP et un masque sous réseau tel que le montre la capture suivante :

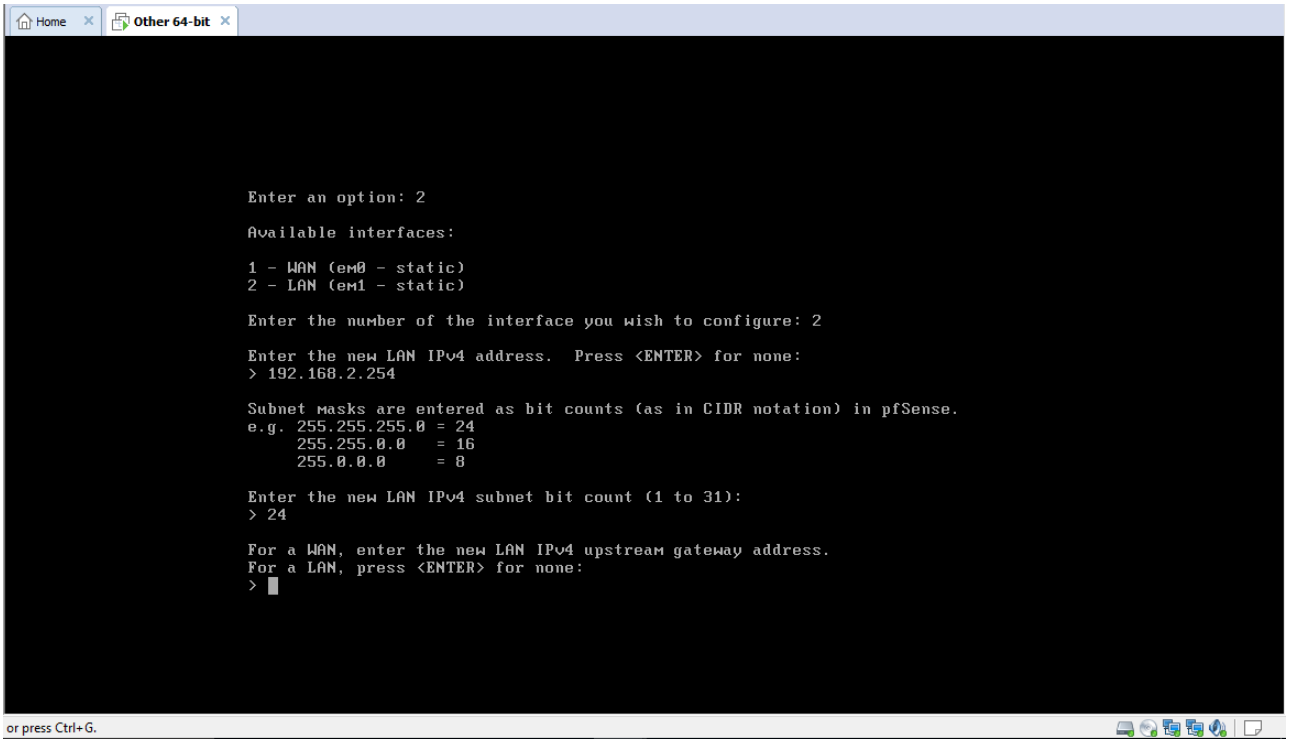



FIGURE IV.5 – Configuration de l'interface LAN

Et pour l'interface WAN c'est le numéro 1, on affecte une adresse IP et un masque sous réseau puis une paserelle par defaut comme suit :

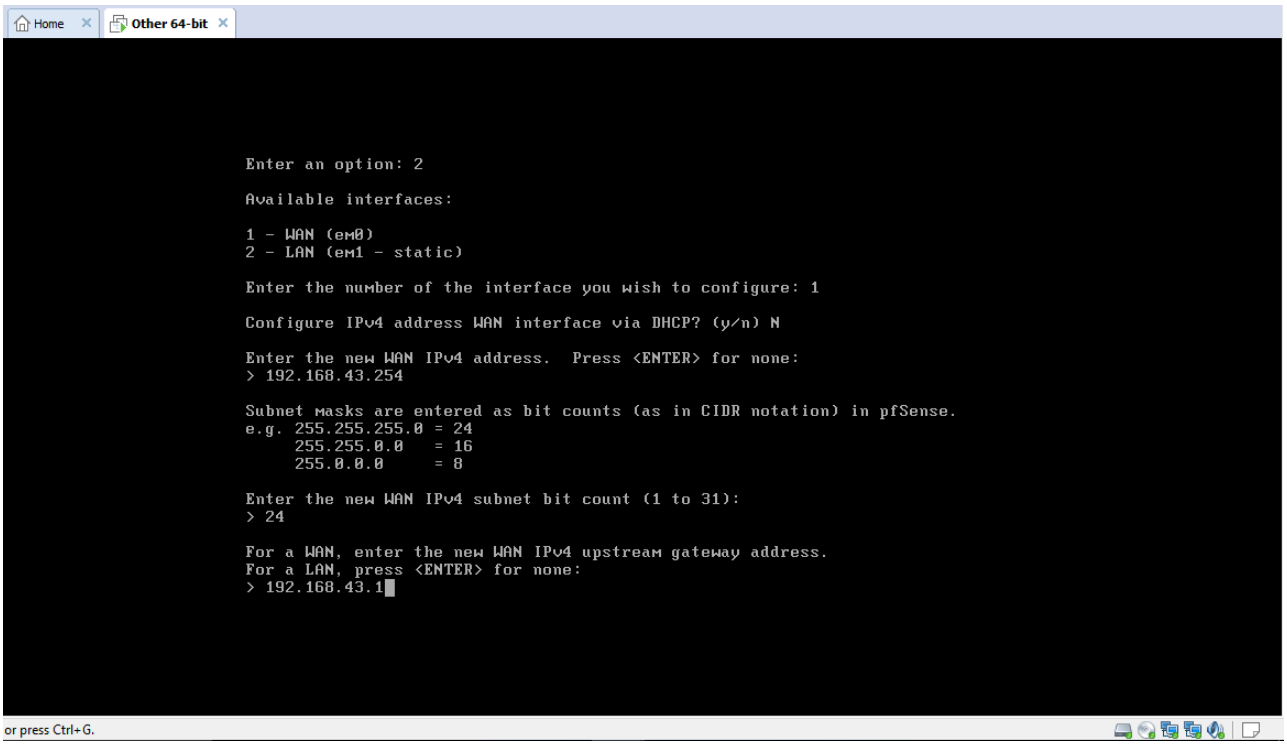



FIGURE IV.6 – Configuration de l'interface WAN

### IV.3.3 Activation des interfaces

Pour activer une interface nous devons d'abord accéder à l'interface web de pfsense et pour le faire,nous allons taper l'adresse IP de l'interface LAN dans le navigateur on obtient cette capture

**Username** : admin / **Password** : pfsense

Cette étape quand en rentre pour la première fois dans pfsense, aprés en peut changer le mot de passe.

Pour activer l'interface WAN, on doit accéder à : **interfaces**/ **WAN**/, et on coche la case "enable interface".

l'interface LAN est activée par défaut.

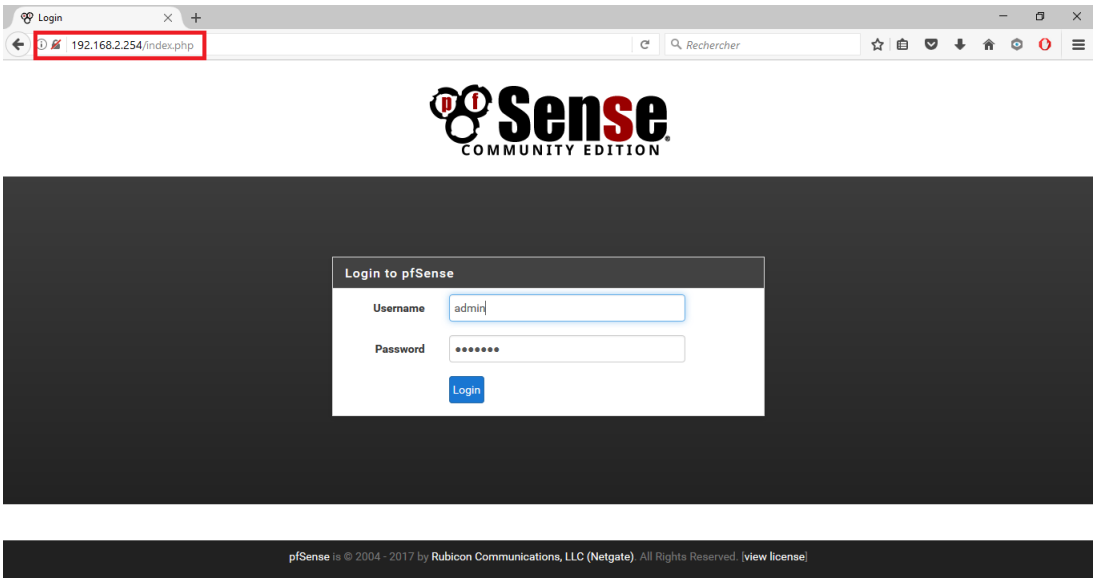



FIGURE IV.7 – Page d'authentification de pfsense

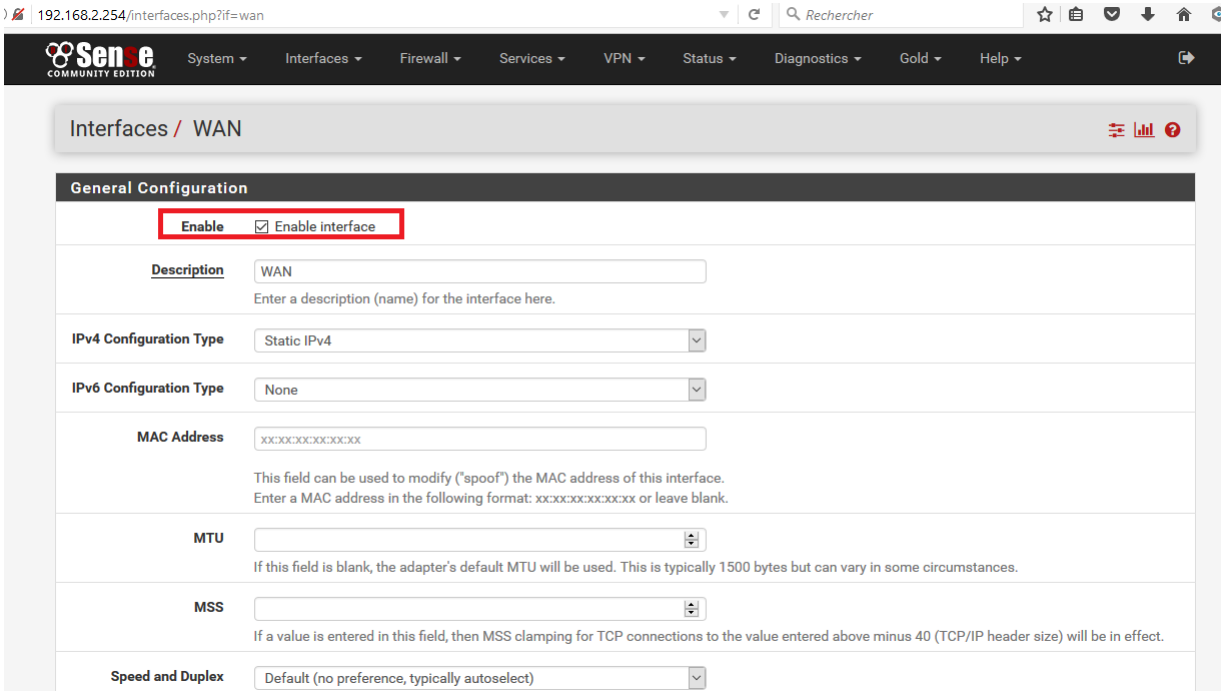



FIGURE IV.8 – Activation de l'interface WAN

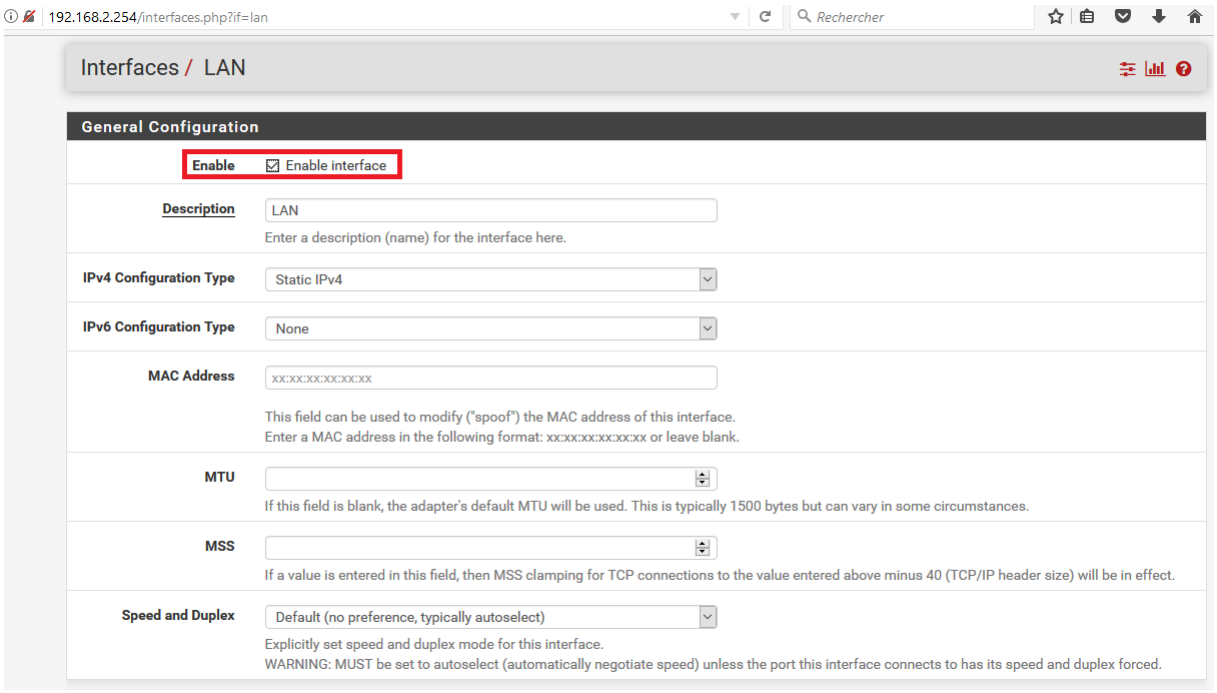
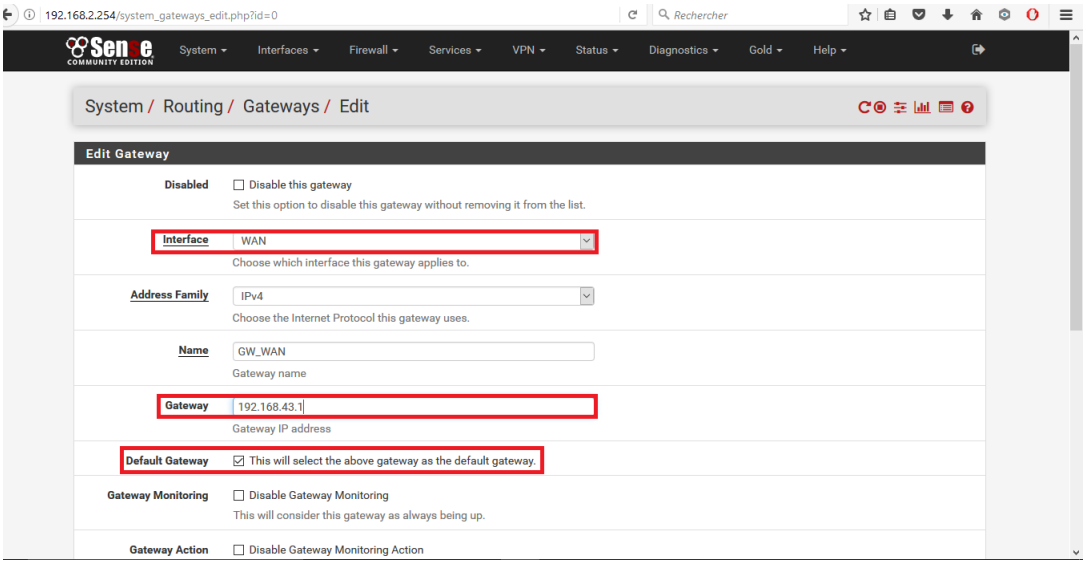



FIGURE IV.9 – Activation de l'interface LAN

### IV.3.4 Configuration de la passerelle

Pour configurer une passerelle il faut accéder à : **System/Routing/Add** est sélectionner l'interface pour lequel on souhaite configurer une passerelle (geteway) et taper son adresse comme représente cette figure et cocher aussi passerelle par défaut (default getway).



### IV.3.5 Configuration du protocole de configuration dynamique des hôtes

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 : **services/ DHCP server/LAN** 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.

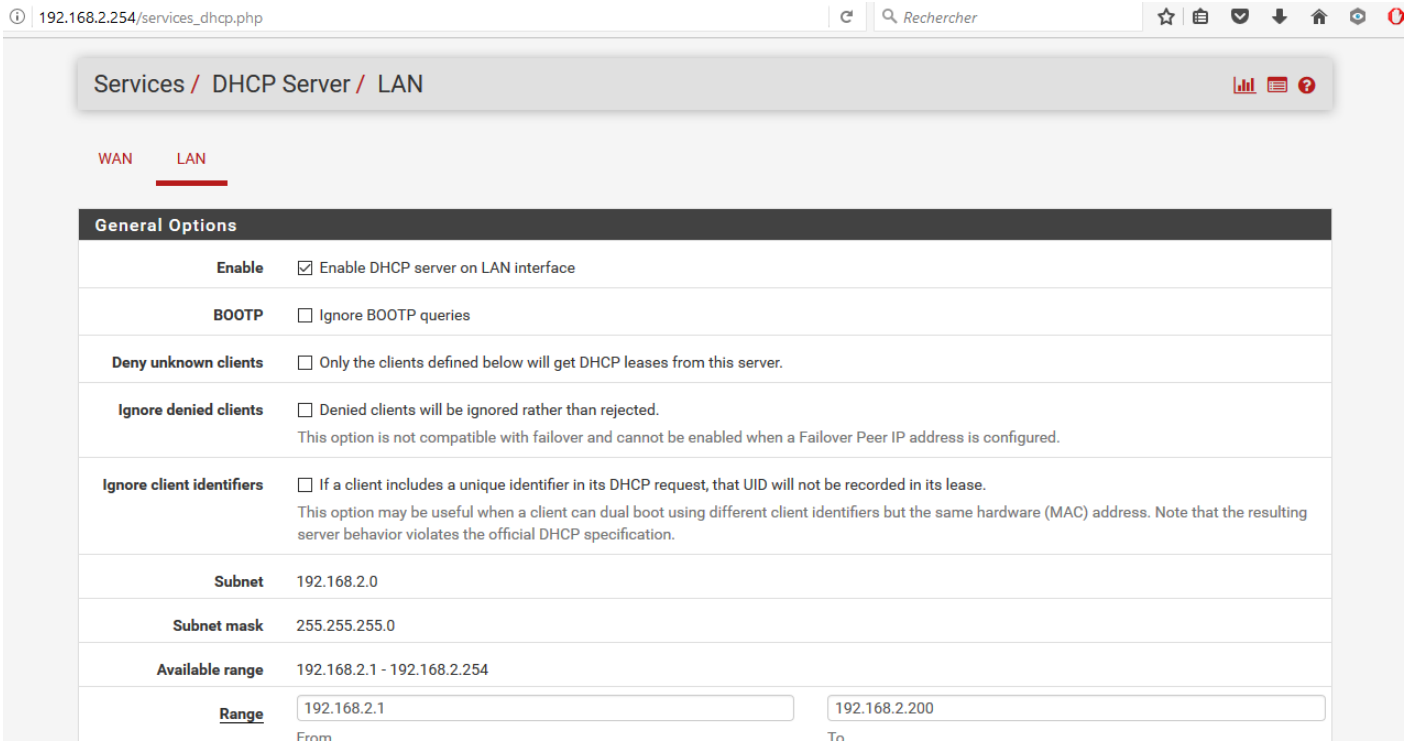



FIGURE IV.10 – configuration du protocole de configuration dynamique des hôtes

## IV.4 Configuration de SNORT

### IV.4.1 Installation du package SNORT

Nous commençons par l'installation des packages, pour cela nous allons dans : **System/ Package Manager/ Available Packages** pour télécharger et installer les deux paquets Open-VM-Tools il inclut des utilitaires de virtualisation permettant d'améliorer le fonctionnement et la gestion de la machine virtuelles de pfsense, puis le package SNORT.

les deux prochaines figure expliquent l'installation du package open-VM-Tools version 10.1.0.

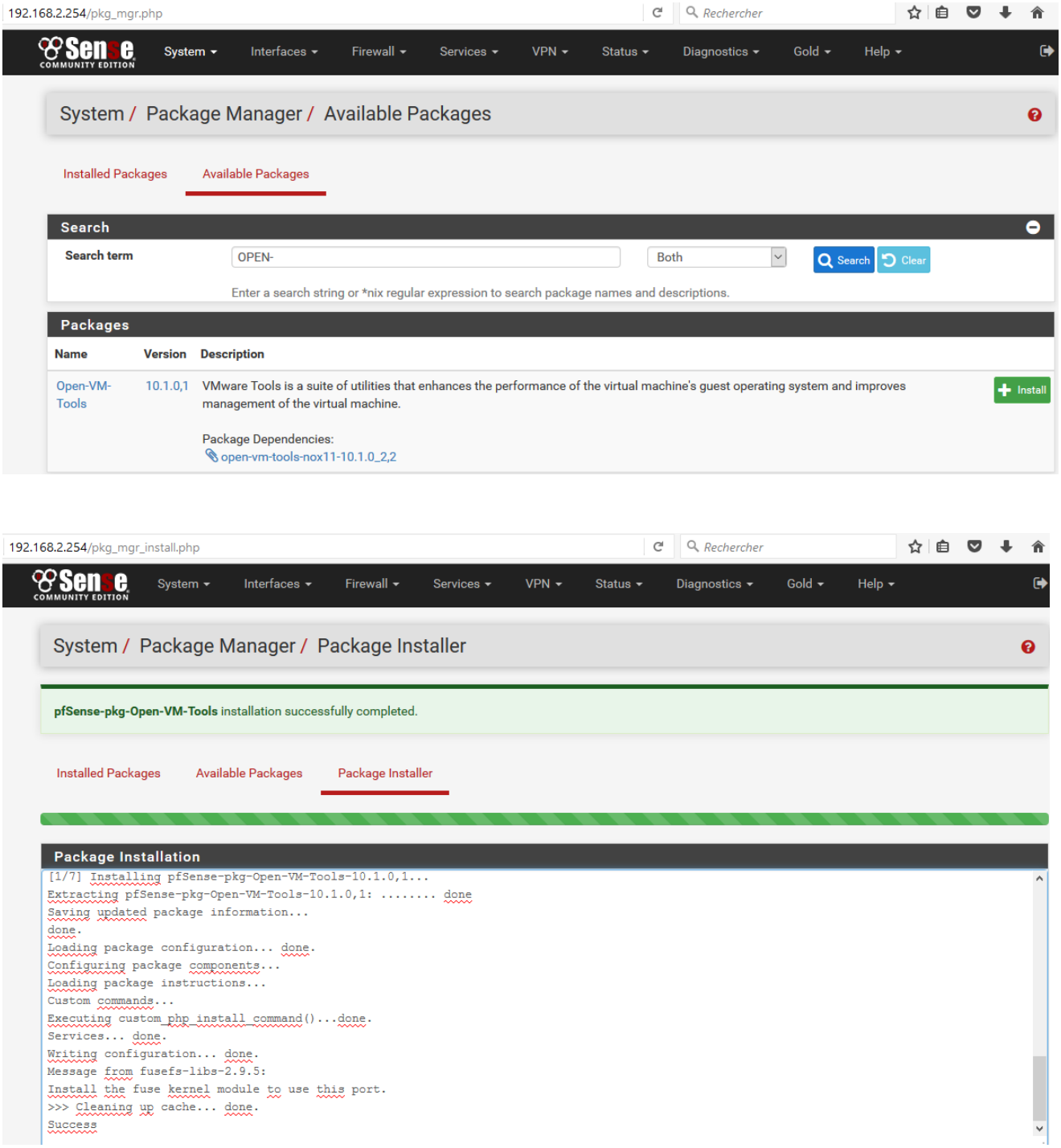



FIGURE IV.11 – installation du package open-VM-tools

Maintenant on passe a l'installation du package SNORT version 3.2.9.3 qui sera expliquée dans les deux prochaines captures.

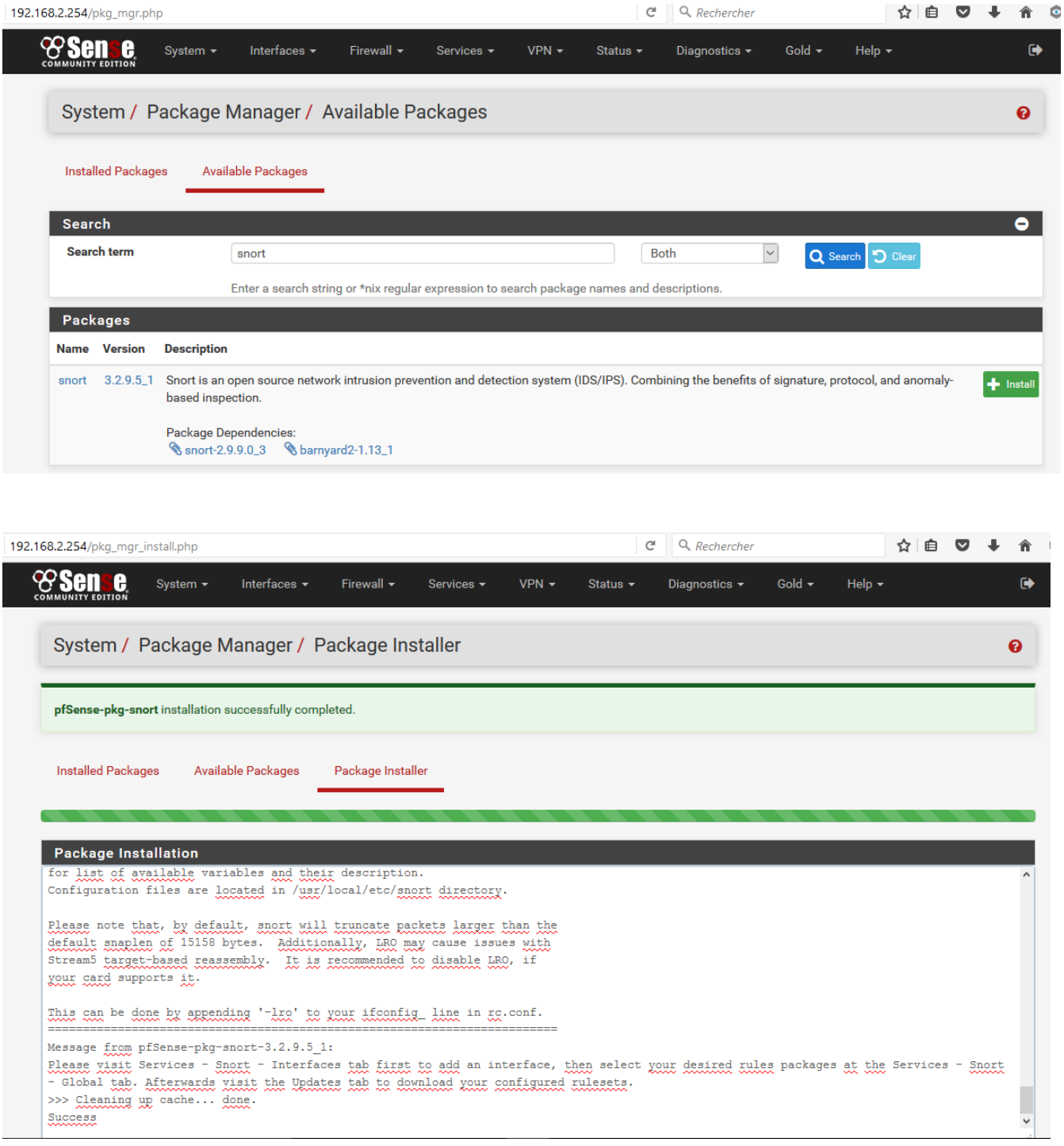



FIGURE IV.12 – installation du package snort

### IV.4.2 Configuration des outils et mise à jour de SNORT

Pour mettre a jour notre SNORT, il est nécessaire de cocher les cinq 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 régles 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.

Mais pour avoir la règle Enable snort VRT, il nous demande un code oinkmaster pour l'obtenir il faut se connecter au cite officiel du snort avec l'utilisation d'un compte E-mail. Cette capture représente comment avoir le code :

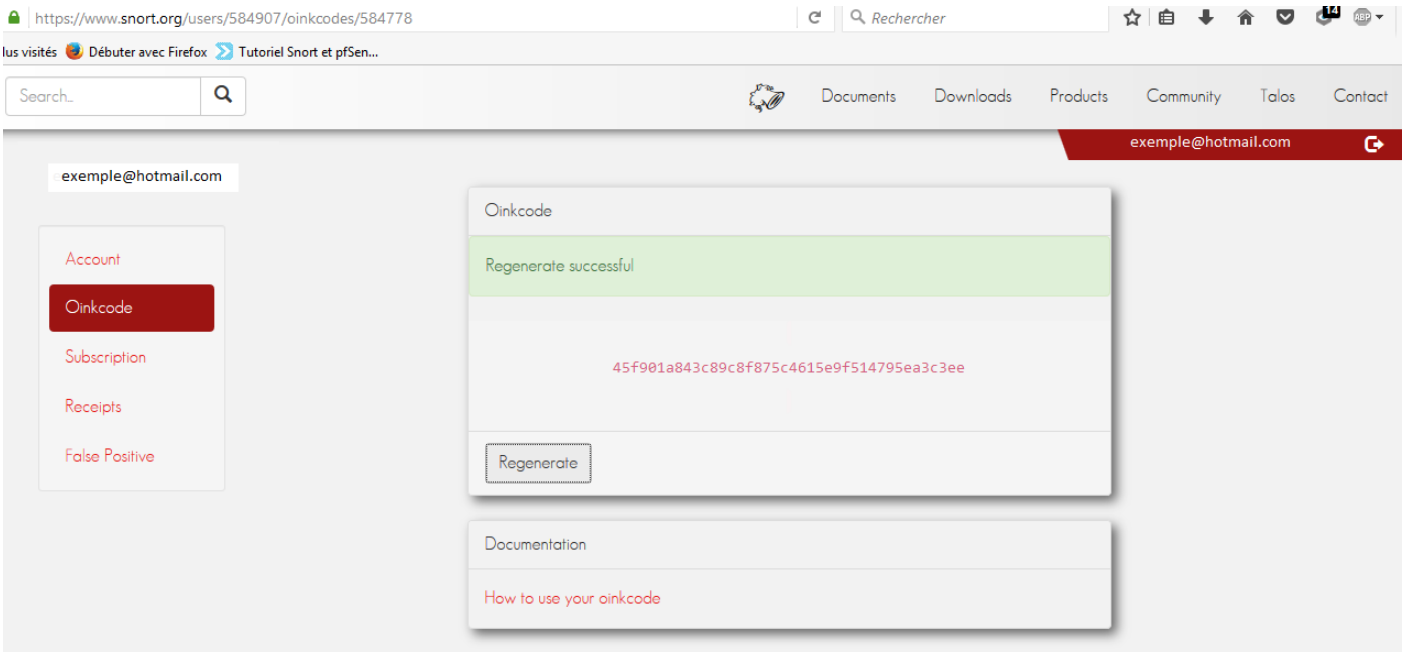



FIGURE IV.13 – Oinkmaster code de snort

les captures suivantes montrent les régles de snort à cocher.

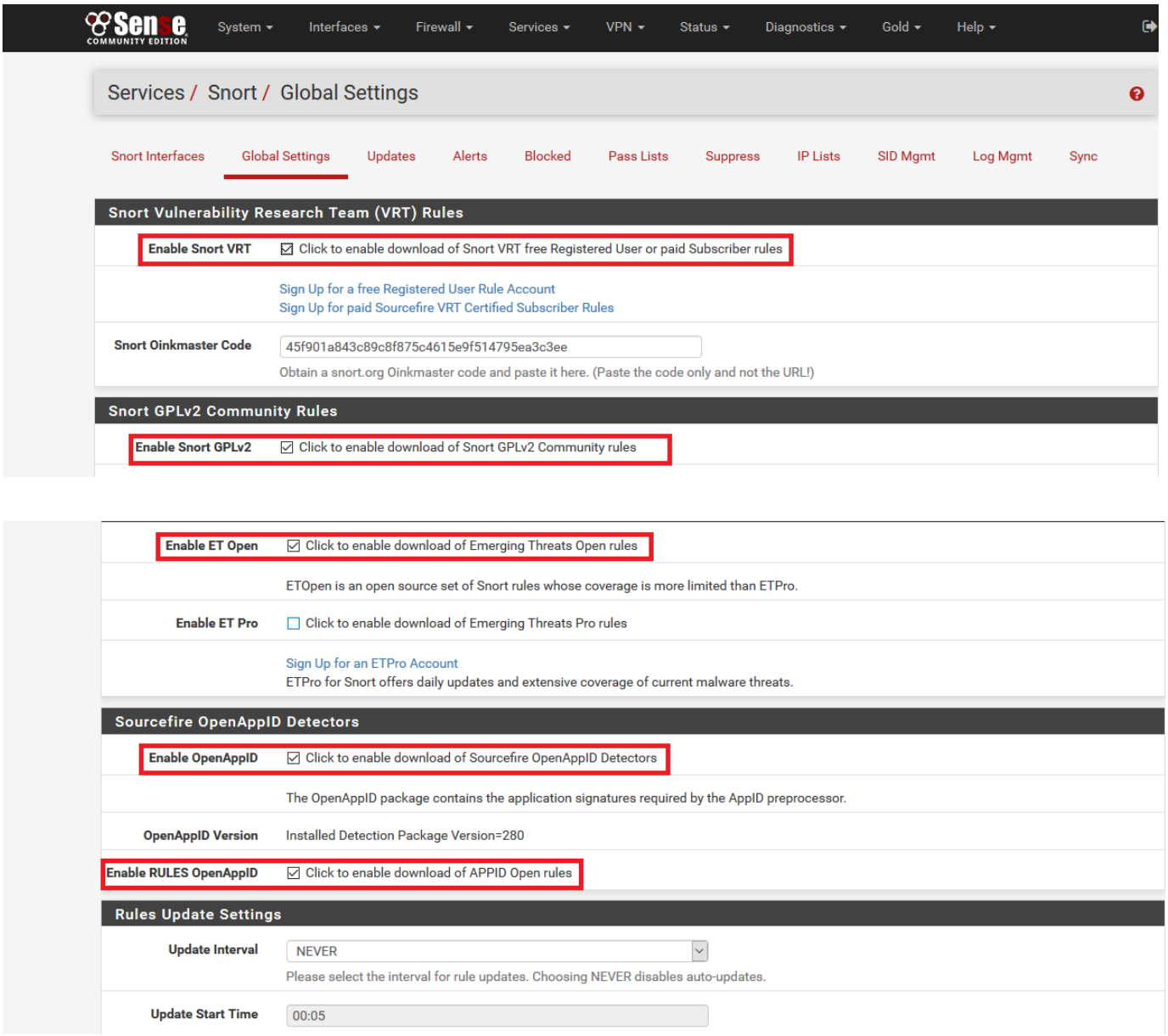



FIGURE IV.14 – les régle de snort à sélectionées

Cette image montre comment on met à jour les cinq règles afin de pouvoir utiliser le SNORT, on va dans : **Services/Snort/ Update**, puis on clique dans (update rules).

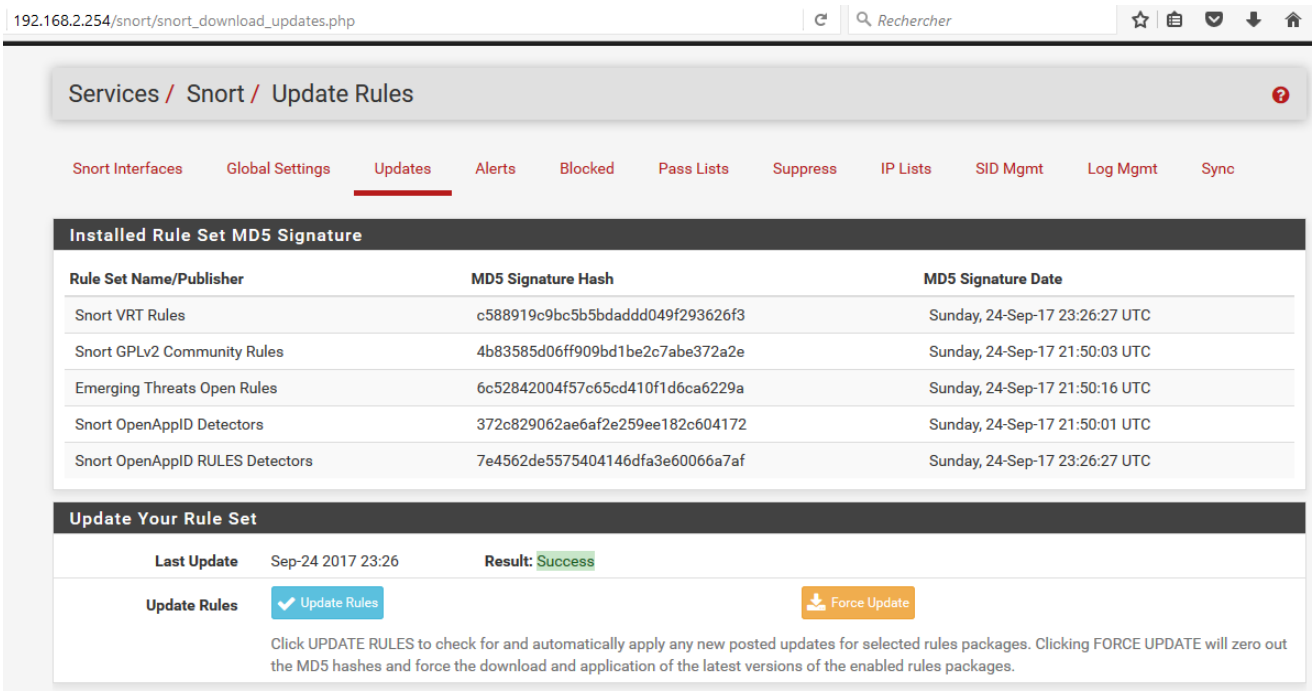



FIGURE IV.15 – Mise à jour des régles de snort

### IV.4.3 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**, on coche la case (enable) et la case (send alerts to system), puis on sélection l'interface WAN.

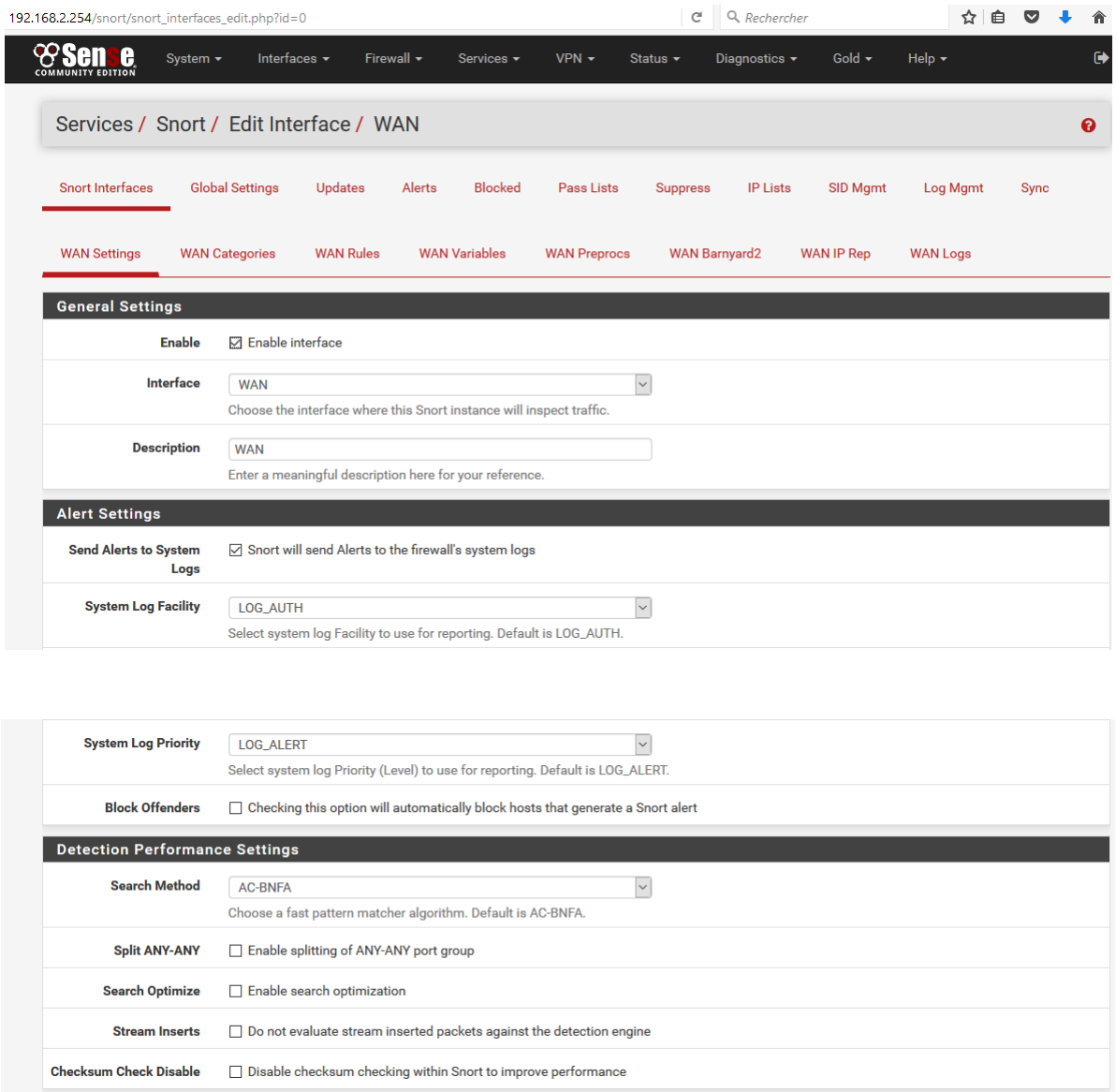



FIGURE IV.16 – Activation du Snort sur l'interface WAN

Et pour activer snort sur l'interface LAN, on suit la même procédure que la précédante.

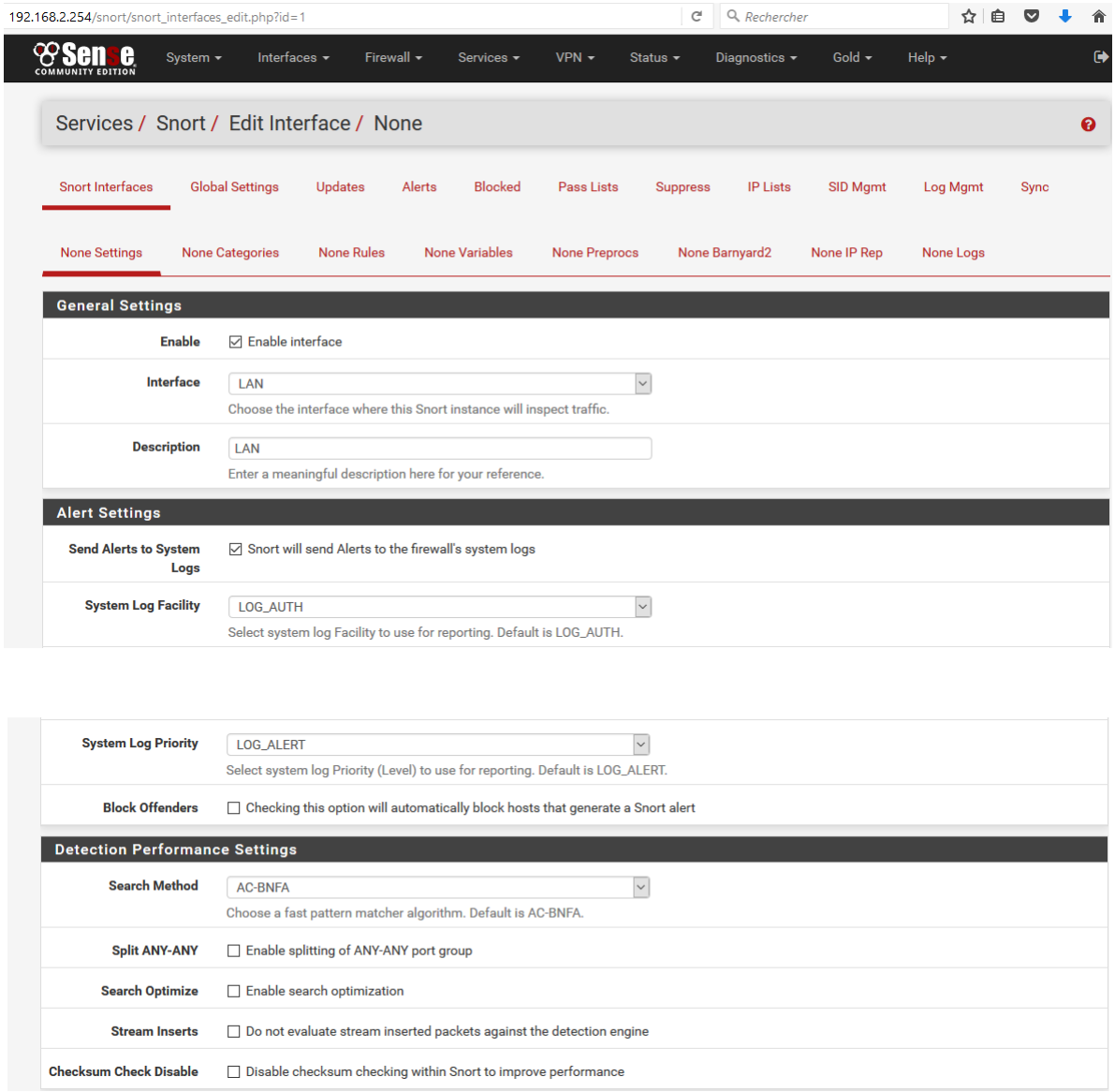



FIGURE IV.17 – Activation du Snort sur l'interface LAN

### IV.4.4 Activation des catégories

Les catégories peuvent s'appliquer à partir d'un simple clique, pour le cas de l'interface WAN. nous allons dans : **Services/ Snort/ Edit interface/ WAN Categories**, et activez les catégories qui vous semblent le plus appropriées pour votre cas de figure.

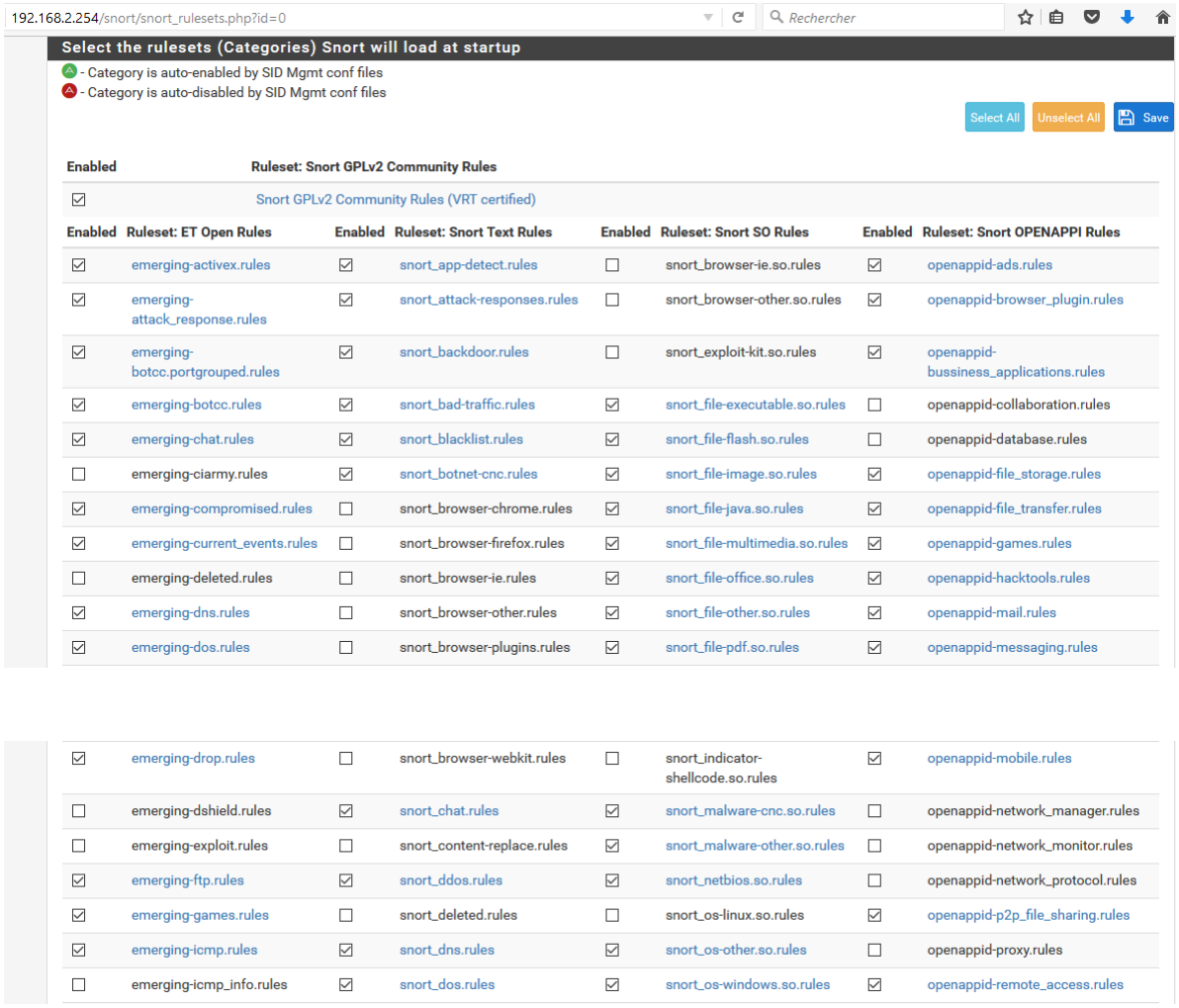
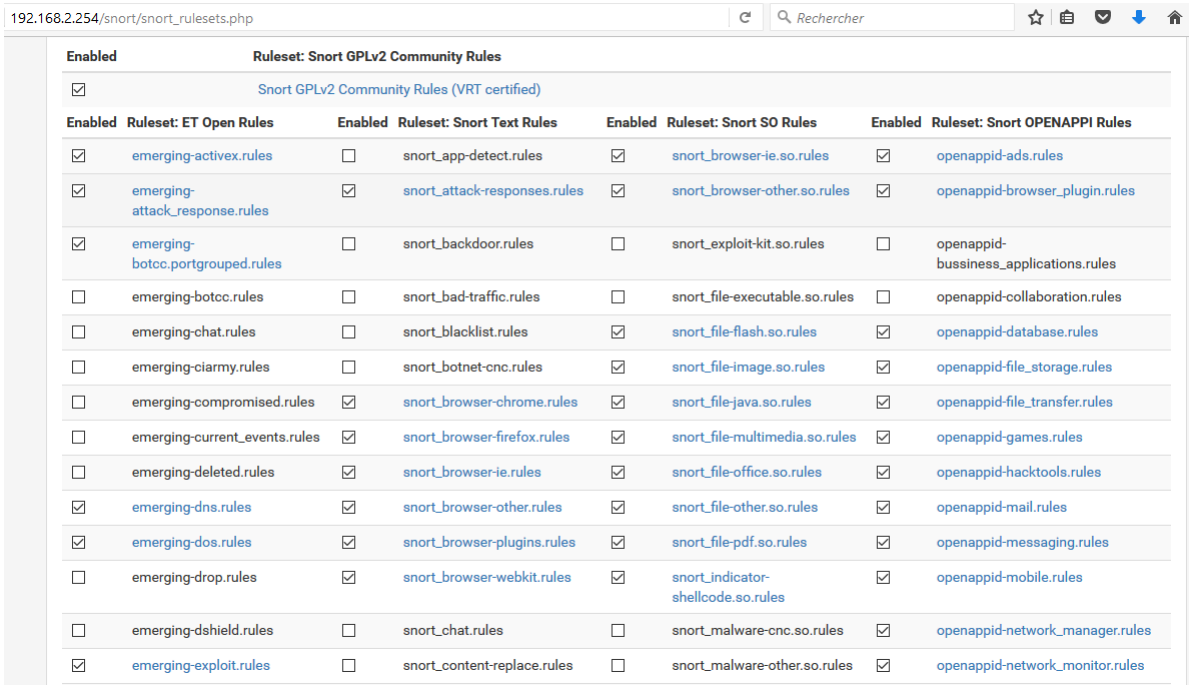



FIGURE IV.18 – Activation des catégories sur l'interface WAN

En ce qui concerne l'interface LAN on va dans : **Services/ Snort/ Edit interface/ LAN Categories**./
L'opération est similaire à la précédente. Les détails des catégories appliqués sont mentionnés dans Annexe.




| Enabled | Ruleset: Snort GPLv2 Community Rules |
|---|---|
| ☑ | Snort GPLv2 Community Rules (VRT certified) |

| Enabled | Ruleset: ET Open Rules | Enabled | Ruleset: Snort Text Rules | Enabled | Ruleset: Snort SO Rules | Enabled | Ruleset: Snort OPENAPPI Rules |
|---|---|---|---|---|---|---|---|
| ☑ | emerging-activex.rules | ☐ | snort_app-detect.rules | ☑ | snort_browser-ie.so.rules | ☑ | openappid-ads.rules |
| ☑ | emerging-attack_response.rules | ☑ | snort_attack-responses.rules | ☑ | snort_browser-other.so.rules | ☑ | openappid-browser_plugin.rules |
| ☑ | emerging-botcc.portgrouped.rules | ☐ | snort_backdoor.rules | ☐ | snort_exploit-kit.so.rules | ☐ | openappid-bussiness_applications.rules |
| ☐ | emerging-botcc.rules | ☐ | snort_bad-traffic.rules | ☐ | snort_file-executable.so.rules | ☐ | openappid-collaboration.rules |
| ☐ | emerging-chat.rules | ☐ | snort_blacklist.rules | ☑ | snort_file-flash.so.rules | ☑ | openappid-database.rules |
| ☐ | emerging-ciarmy.rules | ☐ | snort_botnet-cnc.rules | ☑ | snort_file-image.so.rules | ☑ | openappid-file_storage.rules |
| ☐ | emerging-compromised.rules | ☑ | snort_browser-chrome.rules | ☑ | snort_file-java.so.rules | ☑ | openappid-file_transfer.rules |
| ☐ | emerging-current_events.rules | ☑ | snort_browser-firefox.rules | ☑ | snort_file-multimedia.so.rules | ☑ | openappid-games.rules |
| ☐ | emerging-deleted.rules | ☑ | snort_browser-ie.rules | ☑ | snort_file-office.so.rules | ☑ | openappid-hacktools.rules |
| ☑ | emerging-dns.rules | ☑ | snort_browser-other.rules | ☑ | snort_file-other.so.rules | ☑ | openappid-mail.rules |
| ☑ | emerging-dos.rules | ☑ | snort_browser-plugins.rules | ☑ | snort_file-pdf.so.rules | ☑ | openappid-messaging.rules |
| ☐ | emerging-drop.rules | ☑ | snort_browser-webkit.rules | ☑ | snort_indicator-shellcode.so.rules | ☑ | openappid-mobile.rules |
| ☐ | emerging-dshield.rules | ☐ | snort_chat.rules | ☐ | snort_malware-cnc.so.rules | ☑ | openappid-network_manager.rules |
| ☑ | emerging-exploit.rules | ☐ | snort_content-replace.rules | ☐ | snort_malware-other.so.rules | ☑ | openappid-network_monitor.rules |

FIGURE IV.19 – Activation des catégories sur l'interface LAN

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

### IV.4.5 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'alerts),nous allons également cocher la case (auto-refresh view) pour actualiser la liste des notification.

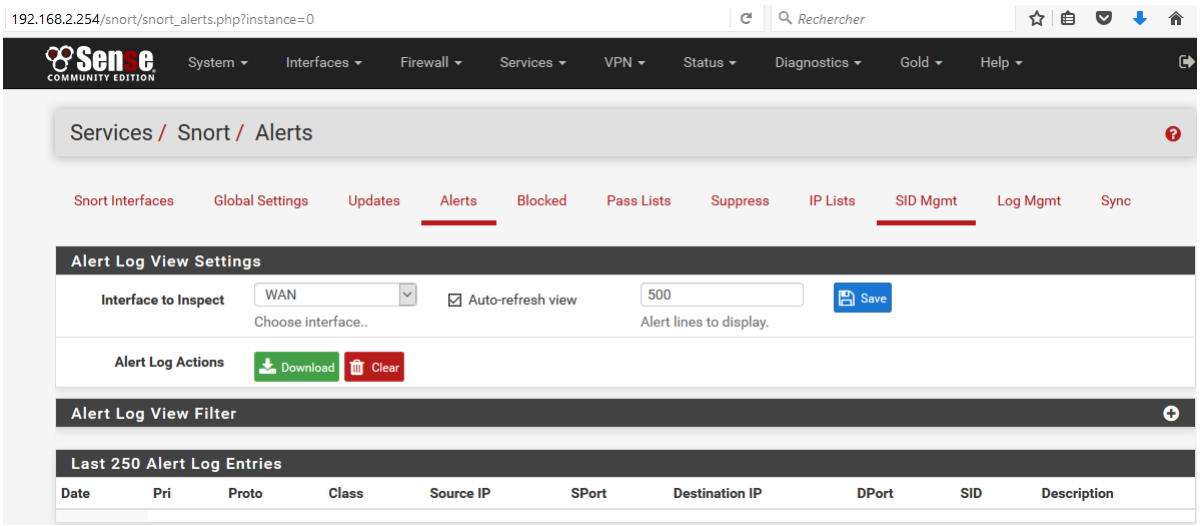



FIGURE IV.20 – Configuration des alerts

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

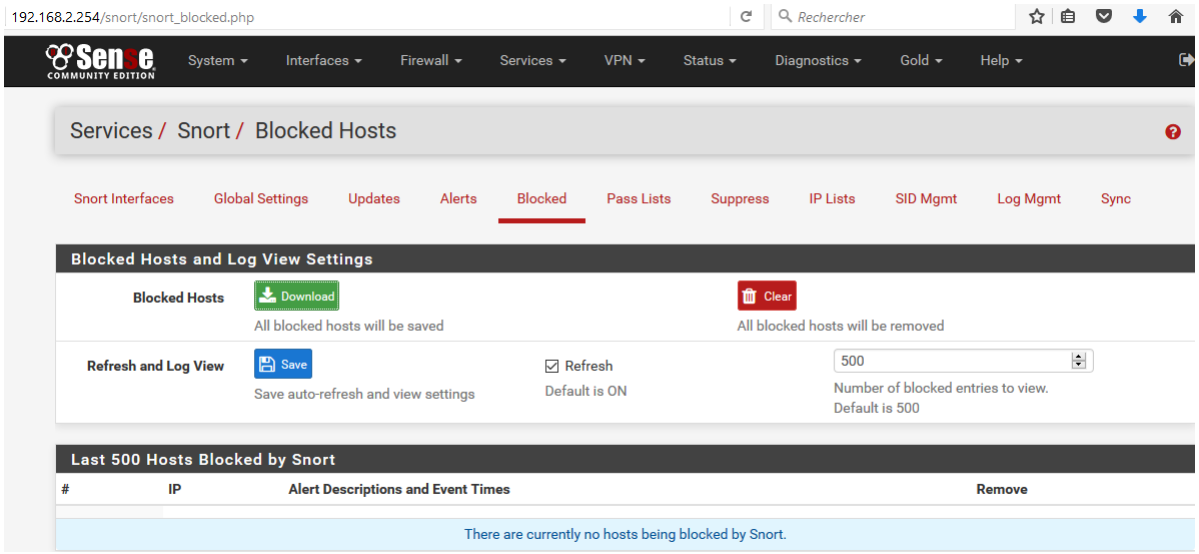
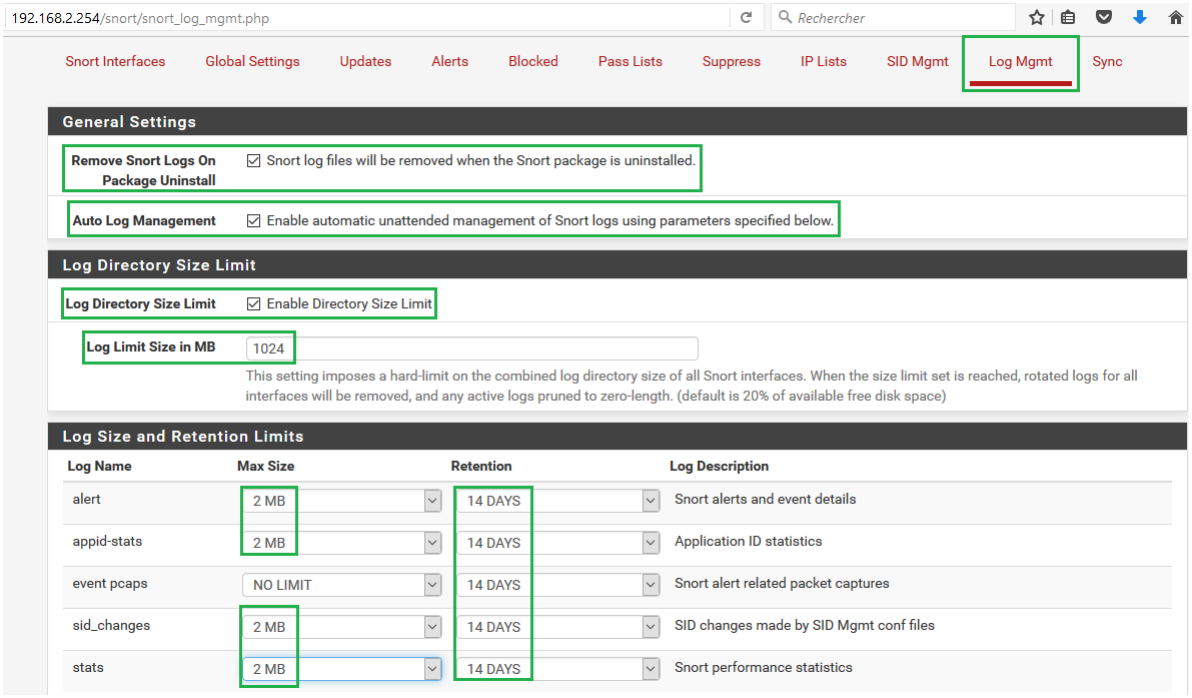
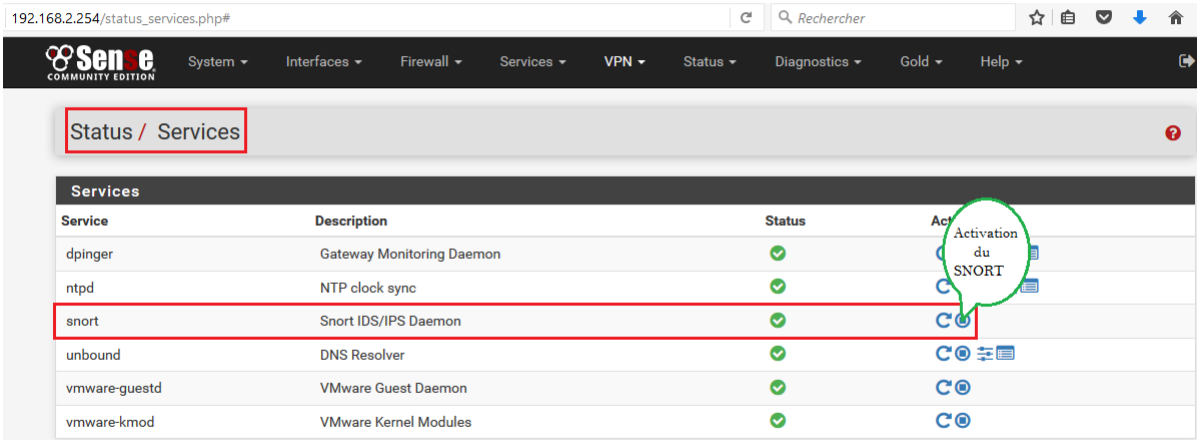



FIGURE IV.21 – Configuration des blocages

La capture suivante montre les configuration à appliquer sur le fichier log selon nos besoin, on se positionne dans :**Services/Snort/Log Mgmt**, on coche d'abord les deux case (Remove Snort Logs On Package Uninstall) et (Auto Log Management), Pour la taille (Max Size) on a choisi 2MB, et pour la retention on a choisi 14 jours (DAYS), parce que après 14 jour le système il va faire la mise à jour.




Le service snort est par défaut est désactivé, la figure suivante montre comment l'activer : on clique sur le bouton qu'on a précisé sur l'image.



### IV.4.6 Test de SNORT

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

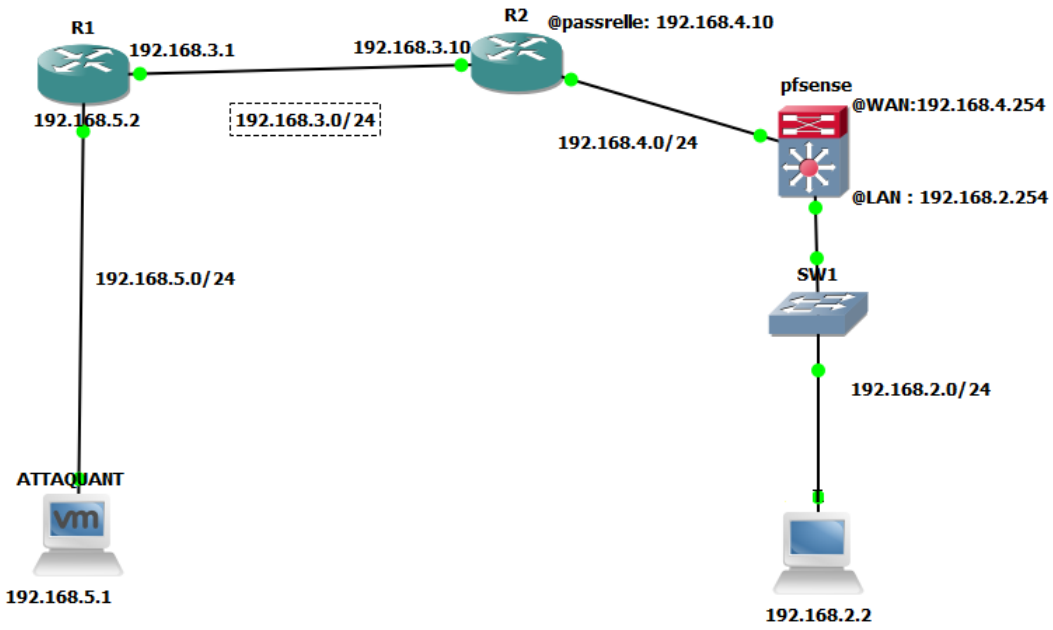



FIGURE IV.22 – La topologie utilisée

configuration des deux routeurs est affichée sur les captures suivantes : on remarque que sur les routeur les interfaces fastethernet0/0 et fastethernet1/0 sont activée et bien configurer, et on a utilisée le routage dynamique (router rip).

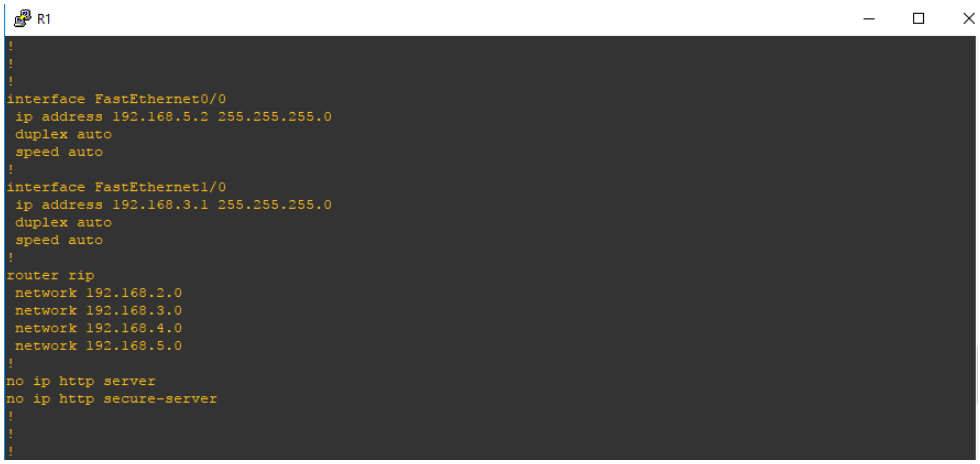



FIGURE IV.23 – La configuration de routeur 1

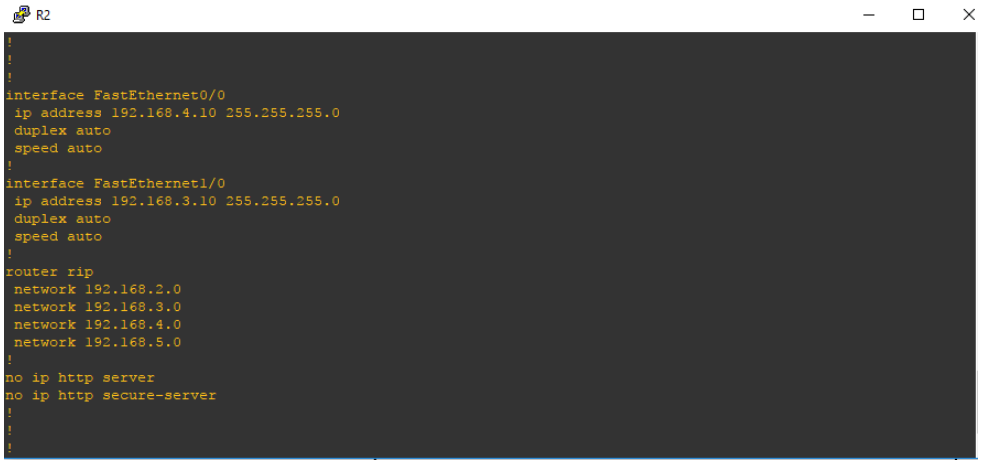



FIGURE IV.24 – La configuration de routeur 2

Afin d'exécuter l'attaque, nous devons installer l'outil NMAP sur la machine attaquante 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).

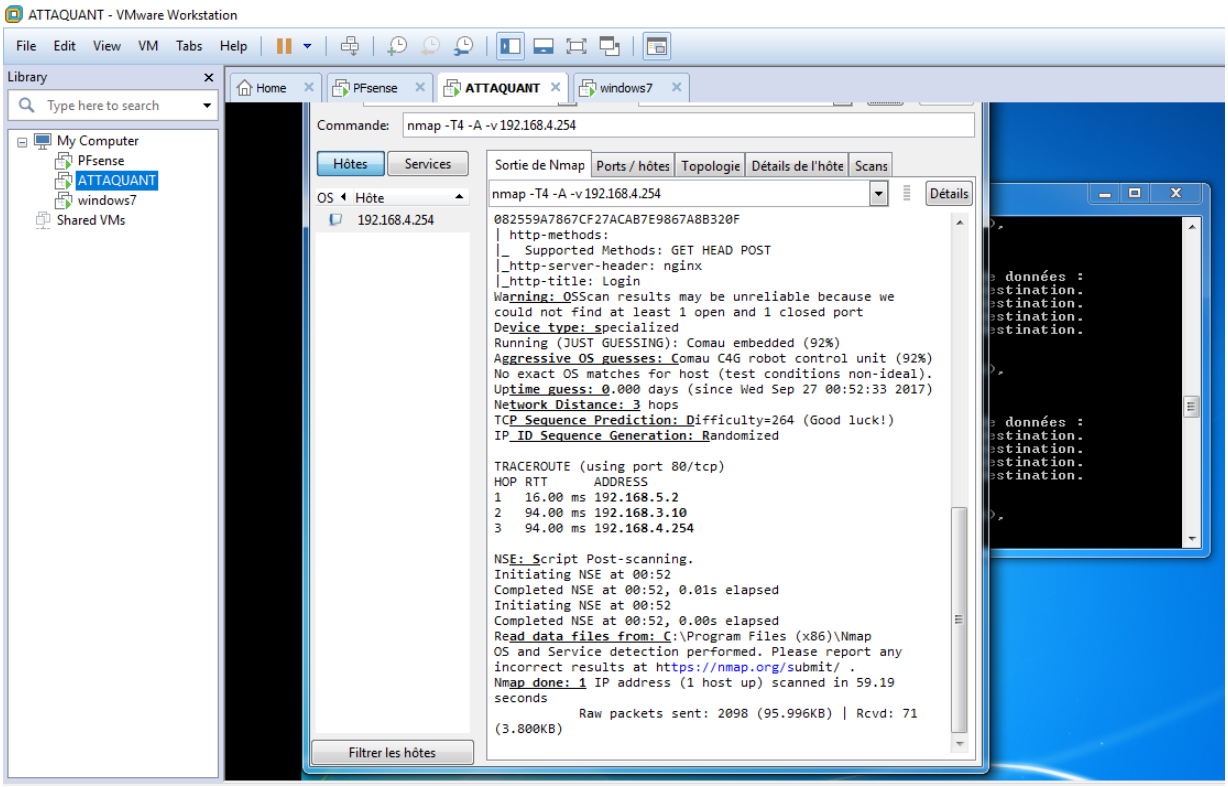



FIGURE IV.25 – Lancement de l'attaque

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

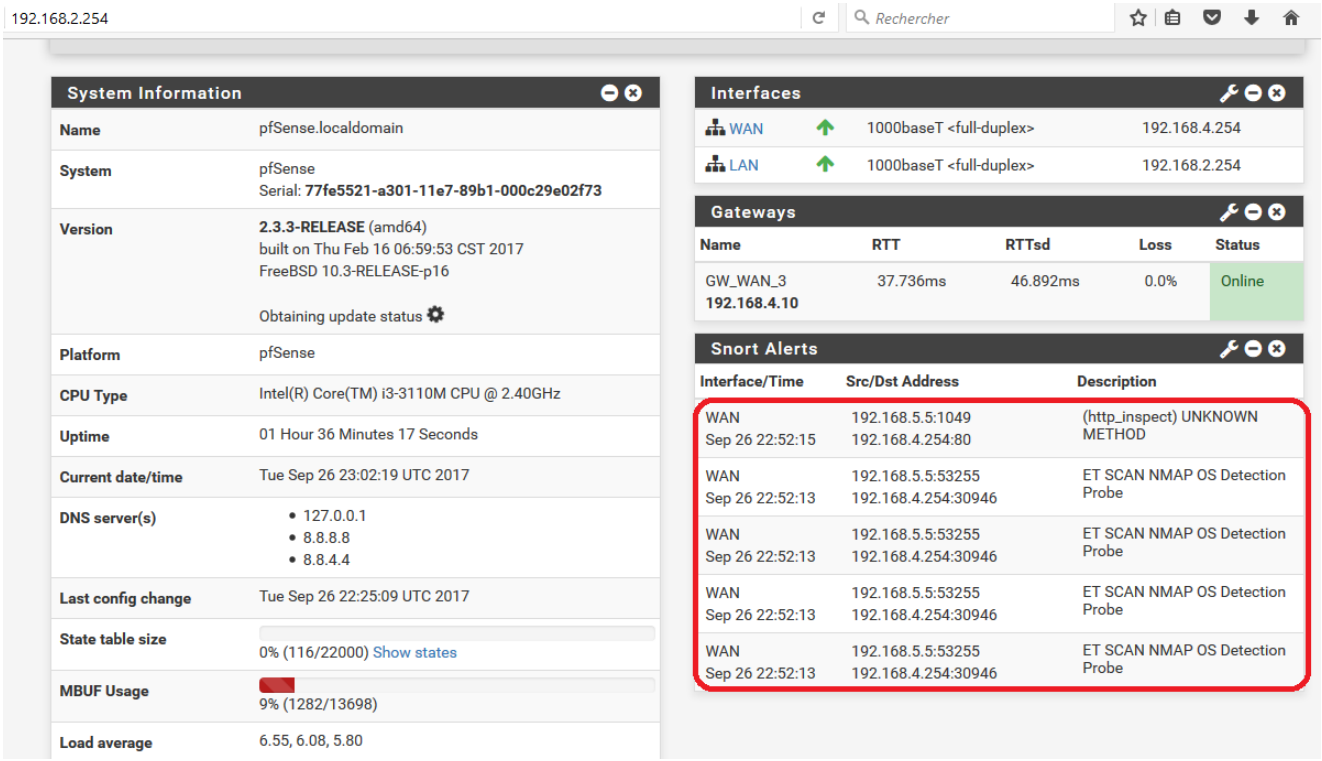



FIGURE IV.26 – Détection de l'attaque

# Conclusion

Dans ce chapitre, nous avons présenté des outils importants pour la détection et la prévention d'intrusion. A savoir pfsense et SNORT. En suite nous avons donné toutes les étapes d'installation et configuration de ces outils.

Enfin, pour tester notre produit, nous avons procédé à un test d'intrusions avec le scanner de ports Nmap pour simuler une attaque et confirmer ainsi le bon fonctionnement de SNORT.

# Conclusion générale

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

Nous avons donc opté pour l'utilisation des systèmes de détections 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 une présentation de la sécurité des réseaux informatiques et ce en définissant entre autres les différentes attaques et contre-mesures de sécurité, pour ensuite présenter le système de détection d'intrusion ainsi que l'environnement de travail. Nous nous sommes par la suite penchés sur 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.

Finalement, nous avons défini une politique de sécurité et avons mis en place Snort en plus de PfSense afin d'améliorer le réseau de l'entreprise et ce dans le but de renforcer sa sécurité.

Le stage effectué au sein de NAFTAL 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 de notre parcours professionnel.

# Annexes

Définition de certain catégories de Snort appliquées pour notre implémentation :
**-App-detect.rules :** Cette catégorie contient des régles qui recherchent et contrôlent le trafic de certaines applications qui génèrent une activité réseau. Cette catégorie sera utilisée pour contrôler différents aspects de la façon dont une application se comporte.
**-Blacklist.rules :** Cette catégorie contient des régles URI, USER-AGENT, DNS et adresse IP qui ont été déterminées comme des indicateurs d'activités malveillantes. Ces régles sont basées sur l'activité des sandboxes du virus Talos, la liste publique des URL malveillantes et d'autres sources de données.
**-Browser-chrome.rules :** Cette catégorie contient la détection des vulnérabilités présentes dans le navigateur Chrome. (Ceci est séparé de la catégorie "navigateur-webkit", car Chrome a suffisamment de vulnérabilités pour être exclus, et alors qu'il utilise le moteur de rendu Webkit, il existe beaucoup d'autres fonctionnalités pour Chrome).
**-Browser-firefox.rules :** Cette catégorie contient la détection des vulnérabilités présentes dans le navigateur Firefox ou des produits équipés du moteur "Gecko"(Client de messagerie Thunderbird,... etc).
**-Browser-ie.rules :** Cette catégorie contient la détection des vulnérabilités présentes sur le navigateur Internet Explorer (moteurs Trident ou Tasman).
**-Browser-webkit :** Cette catégorie contient la détection des vulnérabilités présentes dans le moteur de navigateur Webkit (à part Chrome), y compris le Safari d'Apple, le navigateur mobile RIM, Nokia, KDE, Webkit lui-même et Palm.
**-Browser-other :** Cette catégorie contient la détection de vulnérabilités dans d'autres navigateurs non listés ci-dessus.
**-Browser plugings :** Cette catégorie contient la détection des vulnérabilités dans les navigateurs qui traitent des plugins vers le navigateur. (Exemple : Active-x).
**-File-executable :** Cette catégorie contient des régles pour les vulnérabilités trouvées ou livrées via des fichiers exécutables, quelle que soit la plate-forme.
**-File-flash :** Cette catégorie contient des régles pour les vulnérabilités trouvées ou livrées via des fichiers flash. Soit comprimé soit non compressé, quelle que soit la plate-forme de méthode de livraison attaquée.
**-File-image :** Cette catégorie contient des régles pour les vulnérabilités qui se trouvent dans les fichiers d'images. Indépendamment de la méthode de livraison, du logiciel attaqué ou du type d'image. (Les exemples incluent : jpg, png, gif, bmp, etc.).
**-File-java :** Cette catégorie contient des régles pour les vulnérabilités présentes dans les fichiers Java (.jar).
**-File-multimédia :** Cette catégorie contient des régles pour les vulnérabilités présentes dans les fichiers multimédias (mp3, films, wmv).
**-File-offfice :** Cette catégorie contient des régles pour les vulnérabilités présentes dans

les fichiers appartenant à la suite de logiciels Microsoft Office. (Excel, PowerPoint, Word, Visio, Access, Outlook, etc.).
**-File-pdf :** Cette catégorie contient des régles pour les vulnérabilités trouvées dans les fichiers PDF. Indépendamment de la méthode de création, de la méthode de livraison ou du logiciel que le PDF affecte (par exemple Adobe Reader et FoxIt Reader) .
**-File-other :** Cette catégorie contient des régles pour les vulnérabilités présentes dans un fichier, qui ne correspond pas aux autres catégories ci-dessus.
**-Indicator-compromise :** Cette catégorie contient des régles qui ne doivent être utilisées que pour la détection d'un système à compromis positif, des faux positifs peuvent survenir.
**-Indicator-obfuscatio :** Cette catégorie contient des régles qui sont clairement utilisées uniquement pour la détection de contenu obscurci. Comme les régles JavaScript encodées.
**-Malware-backdoor :** Cette catégorie contient des régles pour la détection du trafic destiné aux canaux de commande d'écoute connus. Si un morceau de soft malicieux ouvre un port et attend des commandes entrantes pour ses fonctions de contrôle, ce type de détection sera ici. Un exemple simple serait la détection de BackOrifice alors qu'il écoute sur un port spécifique, puis exécute les commandes envoyées.
**-Malware-cnc :** Cette catégorie contient des activités de commande et de contrôle malveillantes connues pour le trafic de botnet identifié. Cela inclut l'appel à la maison, le téléchargement de fichiers abandonnés et l'exfiltration des données. Les commandes réelles issues du genre "Master to Zombie" seront également disponibles.
**-Malware-tools :** Cette catégorie contient des régles qui traitent des outils qui peuvent être considérés comme malveillants. Par exemple, LOIC.
**-Malware-other :** Cette catégorie contient des régles liées au malware, mais ne correspondent pas à l'une des autres catégories de logiciels malveillants.
**-Os-windows :** Cette catégorie contient des régles qui recherchent des vulnérabilités dans les systèmes d'exploitation basés sur Windows. Pas pour les navigateurs ou aucun autre logiciel sur le système d'exploitation.
**-Os-mobile :** Cette catégorie contient des régles qui recherchent des vulnérabilités dans les systémes d'exploitation mobiles. Pas pour les navigateurs ou tout autre logiciel en haut du systéme d'exploitation.
**-Os-other :** Cette catégorie contient des régles qui recherchent des vulnérabilités dans un OS qui n'est pas listé ci-dessus.
**-Policy-multimedia :** Cette catégorie contient des régles qui détectent les violations potentielles de la politique pour le multimédia. Des exemples comme la détection de l'utilisation d'iTunes sur le réseau. Ce n'est pas pour les vulnérabilit´es trouvées dans les fichiers multimédia, comme cela se fera dans le fichier multimédia.
**-Policy-sociale :** Cette catégorie contient des régles pour la détection de violations potentielles de la politique sur les réseaux d'entreprises pour l'utilisation des médias sociaux. (P2P, chat, etc.).
**-Policy-spam :** Cette catégorie concerne les régles qui peuvent indiquer la présence de spams sur le réseau.
**-Policy-other :** Cette catégorie est pour les régles qui peuvent enfreindre le poteau de politique d'entreprise des utilisateurs finaux. Ne relèvent d'aucune autre catégorie de poli-

tique.
**- Protocol-dns :** Cette catégorie concerne les régles qui peuvent indiquer la présence du protocole dns ou des vulnérabilités dans le protocole dns sur le réseau.
**-Protocol-finger :** Cette catégorie concerne les régles qui peuvent indiquer la présence du protocole finger ou des vulnérabilités dans ce protocole sur le réseau.
**-Protocol-ftp :** Cette catégorie concerne les régles qui peuvent indiquer la présence du protocole ftp ou des vulnérabilités dans le protocole ftp sur le réseau.
**-Protocol-icmp :** Cette catégorie concerne les régles qui peuvent indiquer la présence de trafic icash ou de vulnérabilités dans icmp sur le réseau.
**-Protocol-imap :** Cette catégorie concerne les régles qui peuvent indiquer la présence du protocole imap ou des vulnérabilités dans le protocole imap sur le réseau.
**-Protocol-nntp :** Cette catégorie concerne les régles qui peuvent indiquer la présence du protocole nntp ou des vulnérabilités dans le protocole nntp sur le réseau.
**-Protocol-pop :** Cette catégorie concerne les régles qui peuvent indiquer la présence du protocole pop ou des vulnérabilités dans le protocole pop sur le réseau.
**-Protocol-rpc :** Cette catégorie concerne les régles qui peuvent indiquer la présence du protocole rpc ou des vulnérabilités dans le protocole rpc sur le réseau.
**-Protocol-scada :** Cette catégorie concerne les régles qui peuvent indiquer la présence de protocoles scada ou de vulnérabilités dans les protocoles Scada sur le réseau.
**-Protocol-services :** Cette catégorie concerne les régles qui peuvent indiquer la présence du protocole services ou des vulnérabilités dans les protocoles services sur le réseau.
**-Protocol-snmp :** Cette catégorie concerne les régles qui peuvent indiquer la présence du protocole snmp ou des vulnérabilités dans le protocole snmp sur le réseau.
**-Protocol-telnet :** Cette catégorie concerne les régles qui peuvent indiquer la présence du protocole telnet ou des vulnérabilités dans le protocole telnet sur le réseau.
**-Protocol-tftp :** Cette catégorie concerne les régles qui peuvent indiquer la prsence du protocole tftp ou des vulnérabilités dans le protocole tftp sur le réseau.
**-Protocol-voip :** Cette catégorie concerne les régles qui peuvent indiquer la présence de services Voip ou de vulnérabilités dans le protocole VoIP sur le réseau.
**-Protocol-other :** Cette catégorie concerne les régles qui recherchent des protocoles ou des vulnérabilités dans les protocoles, mais ne correspondent pas à l'un des autres fichiers de régles "protocole".
**-Pua-adware :** Cette catégorie traite des applications "pua" ou potentiellement indésirables qui traitent de l'adware ou des logiciels espions.
**-Pua-p2p :** Cette catégorie traite de "pua" ou des applications potentiellement indésirables qui traitent de p2p.
**-Pua-toolbars :** Cette catégorie traite des applications "pua" ou potentiellement indésirables qui traitent des barres d'outils install"es sur le système client. (Google Toolbar, Yahoo Toolbar, Hotbar, etc.)
**-Server-oracle :** Cette catégorie traite des vulnérabilités ou des attaques contre Oracle DB Server d'Oracle.
**-Server-other :** Cette catégorie contient des régles qui détectent les attaques.

# 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 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 NAFTAL Bejaia. SNORT s'est imposé comme le système de détection d'intrusions le plus performant et utilisé, il peut effectuer une analyse du trafic réseau en temps réel et détecter ainsi de nombreux types d'attaques. 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, Politique de sécurité, Attaques, Détection, Intrusion, Menaces, 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 SDI [Strategic Defense Initiative]. 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 intrusion detection system called SNORT, which is associated with the firewall pfSense, and implement all this at the level of the network architecture of NAFTAL Bejaia. 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. Keywords : security, security policy, attacks, detection, intrusion, threats, SNORT, pfSense, firewall, SDI [Strategic Defense Initiative]

# Références bibliographique


[1] Michaël AMAND Mohamed NSIRI, "Etude d'un système de détection d'intrusion comportemental pour l'analyse du trafic aéroportuaire", rapport de projet tutoyé, janvier 2011.

[2] Mme Claire, "service AAA dans les réseaux ad hoc mobiles", thèse de doctorat, université Télécom Paris sud, 2012.

[3] Cédric Lorens, Denis Valoiset Laurent Levier, Tableau de bord de la sécurité réseau, groupe Eyrolles, 2éme édition, 2006.

[4] Jean-Christophe GALLARD, "sécurité et réseaux 2.0".

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

[6] Laurent Bloch et Christophe Wolfhugel, « securité informatique : principe et méthode », juin 2011

[7] Stéphane Lohier, Auréie Quidelleur, Le réseau Internet, des services aux infrastructures, Edition dunod, Paris, 2010.

[8] P.ATELIN, "Réseaux Informatique Notion Fondamentales (Normes, Architecture, Modelé OSI, TCP/IP, Ethernet, WIFI)", Editions ENI, 2009.

[9] Fred Cohen, Michel BERTIN et al, Espace Menaces groupe-virus "LES VIRUS INFORMATIQUE", Edition 2005.

[10] J. Legrand, Gestion d'Entreprises et Organisation des Systèmes d'Information "Virus et Antivirus", 2002.

[11] GATEAU GUILLAUME, le minimum sur TCP/IP, UFTI-IUFM Toulouse, 1997.

[12] CHESWICK, W. R., BELLOVIN, S. M. et RUBIN, A. D. (2003). Firewalls and Internet security : repelling the wily hacker. Addison-Wesley Longman Publishing Co., Inc.

[13] TOM, T. (2005). La sécurité réseaux first step. Pearson Education France.

[14] M. M. PRONZATO, « les firewalls », 3eme année ingénieure en informatique et réseaux, 2000 .

[15] Gunadiz Safia, algorithme d'intelligence artificielle pour la classification d'attaque réseau à partir de données TCP, Mémoire de magistère, université m'hamed BOUGARA de Boumerdes, 2011

[16] WHITMAN, M. et MATTORD, H. (2011). Principales of information security. Cengage learning.

[17] NAFTAL, (2017). Documentation de l'établisement

[18] https://1288702.netacad.com/courses/485246, consulté le 20 mai 2017.

[19] http://www.futura-sciences.com/tech/definitions/internet-firewall-474/, consulté le 26 mai 2017.

[20] https://www.nbs-system.com/blog/howto-idsips.html#intro_ids, consulté le 26 mai 2017.

[21] http://www.clashinfo.com/dico/definition-p/art90-proxy.html, consulté le 26 mai 2017.

[22] http://www.amoks.com/rep-lexique/ido-237/vlan.html, consulté le 26 mai 2017.

[23] http://www.formations-virtualisation.fr/vmware-definition-vmware.php, consulté le 26 mai 2017.

[24] https://www.calexium.com/fr/pfsense-le-logiciel.html, consulté le 18 août 2017

[25] http://searchmidmarketsecurity.techtarget.com/definition/Snort