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

Université A/Mira de Béjaia
Faculté des Sciences Exactes
Département de Recherche Opérationnel

Mémoire de fin d'étude

En

Vue de l'obtention du diplôme de Master Professionnel en Informatique

Option

Adminisration et Sécurité des Réseaux

Thème

Sécurité et Monitoring d'un réseau informatique "Cas SARL RAMDY"

Présenté par : M^{lle} BELLILI Nabila

Encadré par : KABYL Kamal

Évalué par :
SAADI Mustapha. **U. A/Mira Béjaia.**
OUZEGGANE Redouane. **U. A/Mira Béjaia.**

Béjaia, Septembre 2021.

⁂ *Remerciements* ⁂

Je remercie tout d'abord, Allah qui m'a donné la force et le courage pour terminer mes études et élaborer ce modeste travail.

Je tiens à exprimer mes plus sincères remerciements à mon promoteur Mr K.KABYL, qui ma a aidés tout au long du travail.

Un grand merci à mon encadreur de stage au SARL RAMDY Mr.DJOUMER MHENNI pour les informations et ses orientations qui m'ont beaucoup aidés au cours de mon projet, ainsi ses encouragements.

J'adresse mes sincères remerciements pour les membres de jury d'avoir accepté d'examiner et d'évaluer mon travail.

Je tiens à remercier également ma familles et mes amis(es) pour leurs aides considérables.

Merci à tous ceux qui ont rendu service de prés ou de loin.

⁕ *Dédicaces* ⁕

"Louange à Dieu, le seul et unique"

Je dédie ce modeste travail à :

La mémoire de mon chére et tendre père, qui m'a toujours poussé à réaliser mes rêves. que son âme repose en paradis.

Ma très chére maman qui a était et elle est toujours à mes coté à me soutenir et à m'encourager.

Mes chére soeur et mon frère.

Tous mes amis.

M^{lle} BELLILI NABILA

Table des matières

Table des figures

Introduction générale

De nos jours, les entreprises exploitent un ou plusieurs moyens de sécurisation et de surveillance au niveau de leur réseau local. Et laissent simplement son serveur que ce soit linux ou Windows de gérer toutes les activités et les menaces. Ce qui entraine des problèmes de trafic réseau et des mauvais usages de l'internet. Cette situation provoque une augmentation du taux de consommation d'internet au sein des entreprises. De ce fais il devient indispensable de surveiller en permanence l'ensemble du réseau de l'entreprise afin que le personnel et les données ne soient pas affectée par les pannes de fonctionnement et que les pertes du système d'exploitation soit la plus faible possible. Pour cela les entreprises cherchent a investir dans les outils d'administration de réseau très couteuse et qui ne sont pas adapté à leur besoin.

La sécurité dans les réseaux informatiques est devenue une préoccupation importante des utilisateurs et des entreprises. Tous cherchent à se protéger contre une utilisation frauduleuse de leurs données ou contre des intrusions malveillantes dans les systèmes informatiques. Par ailleurs, les virus sont susceptibles de détruire des documents ou même de provoquer la perte totale des informations stockées dans les machines. La tendance actuelle est de mettre en place des mécanismes de contrôle d'accès et des protocoles sécurisés qui apportent plusieurs services : l'authentification, la confidentialité, l'intégrité, la non-répudiation.

Le monitoring est la surveillance en temps réel de l'évolution de l'utilisation de l'infrastructure technique (bande passante consommée, espace disque consommée, charge CPU). Il nécessaire de répartir un système d'administration dans les sous-réseaux de l'entreprise pour diminuer l'utilisation de la bande passante et gérer le trafic du réseau. Dans les réseaux d'entreprises l'administrateur doit surveiller et contrôler toutes activité circulant sur la bande passante, pour protéger le réseau des attaques et risques menacé ce qui donne a faire plus d'efforts mais on mettant un outils de monitoring adapté au réseau apportera une aide au administrateur par exemple analyser, surveiller et contrôler automatiquement.

Dans ce cadre s'inscrit mon projet de fin d'études intitulé "Sécurité et monitoring d'un réseau informatique CAS SARL RAMDY".

Ce mémoire est réparti en quatre chapitre :

Le premier est consacrée à la présentation de quelques généralité sur les réseaux informatiques, la sécurité informatique et les dispositifs de protections.

Le deuxième chapitre consiste à la présentation de l'entreprise d'accueille "RAMDY", et la solution proposer a notre problématique.

Dans le troisième chapitre nous avons défini le monitoring, le trafic réseau, et on a donné par la suite quelques outils de monitoring existants.

Le dernier chapitre fait partie de notre contribution(réalisation), il est consacré à configuration d'un pare-feu Pfsense sous virtuelBox et l'outil de monitoring Ntopng.

On terminera par une conclusion.

Chapitre 1

Généralités sur le réseau et la sécurité informatique

1.1 Introduction

La sécurité se place actuellement au premier plan de la mise en oeuvre d'un réseau. La difficulté que représente la sécurité dans son ensemble est de trouver un compromis entre deux besoins essentiels : le besoin d'ouvrir des réseaux pour profiter de nouvelles opportunités et le besoin de protéger des informations privées ou publiques.
Dans ce chapitre on va présenter quelques généralités sur les réseaux, la sécurité informatique, les dispositifs de protection et la virtualisation.

1.2 Réseaux informatiques

Un réseau informatique est un ensemble d'équipements informatiques (ordinateurs, scanners, imprimantes...) reliés entre eux par des moyens de communications (avec câble et sans fil) pour partager des données, ressources matériels et logiciels et d'échanger des informations. La figure 1.1 présente un exemple d'un réseau informatique.

FIGURE 1.1 – Réseau informatique

1.2.1 Types de réseaux

Il existe différentes types de réseaux classifiés selon leur tailles, vitesses de transfert des donnés ainsi que leur étendus :

1. Réseau personnel (PAN ou Personal Area Network) : Petit réseau de quelques mètres d'étendus, permettant l'interconnexion de machines personnelles : Pc portables, mobile téléphonique, agenda électronique, etc

2. Réseau local (LAN ou Local Area Network) : Un réseau local, désigne une zone géographique, plus au moins délimitée par l'existence d'un mur ou d'une barrière plus au moins définie et qui sert à délimiter physiquement une étendu. Un LAN un réseau dont l'étendu s'arrête à partir d'un emplacement défini.

3. Réseau métropolitan (MAN ou Metropolitan Area Network) : Définit un type de réseau qui s'étend à une métropole ou à une zone géographique qui s'en approche, bien moins étendu qu'un WAN. Les MAN sont souvent utilisé par les fournisseur d'accès Internet pour relier les centres de données ou par les Administrateur/université qui ont besoin de connecter des sites géographiquement situé dans un périmètre relativement restent.

4. Réseau étendu (WAN ou Wide Area Network) : Par opposition au LAN, est l'ensemble des équipements sur lesquels l'entreprise n'a pas un contrôle direct en tant qu'entité. D'un point de vue géographique, l'acronyme WAN désigne les réseaux des opérateurs internet, qui sont bien plus étendus que les réseaux d'entreprise. Il peut s'étendre entre des villes, des pays voire des continent.

5.Réseau local sans fil (WLAN ou Wireless Local Area Network) : Désigne le réseau sans fil. Tous les équipements participant au réseau sans fil comme les bornes d'accès et les contrôleurs Wi-Fi sont désignés ainsi. Il fait partie du LAN mais a la particularité de ne nécessiter aucun fil. Considéré comme extension du LAN filaire et une solution d'appoint pour les utilisateurs mobiles dans l'entreprise.

6. Réseaux de stockage (SAN ou Storage Area Network) : Le réseau de stockage son principe est de laisser penser à un serveur, grâce à diffèrent technologies, que ses données sont situées sur un disque connecté localement. Il permet donc d'acheminer les données depuis un serveur vers les disques en passant par différents équipements. Traiter le SAN comme un réseau à part permet de mettre en oeuvre des moyens supplémentaire pour sa redondance et sa sécurité. Il peut fonctionner en mode cluster(un bloc de système de fichiers) et ainsi la perte d'une baie de stockage complète devient beaucoup moins critique. [1] La figure(1.2) montre les types des réseaux usuels.

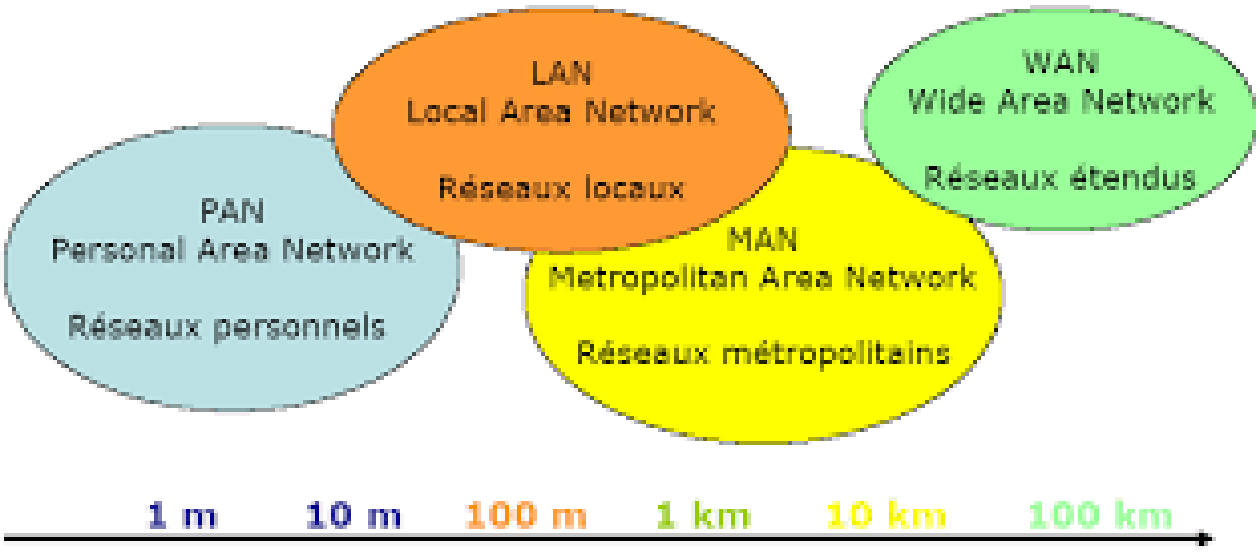

FIGURE 1.2 – Types des réseaux usuels

1.2.2 Caractéristiques de quelques types de réseaux

Il existe plusieurs types de réseaux, certains son caractérisés comme suit :

1.2.2.1 Réseau local (LAN)

Un réseau local se caractérise principalement par sa topologie (physique et logique), les médias utilisés pour le transport, ainsi que le mode transmission.

(a) Médias de transmission : Dans les réseaux locaux, nous pouvons trouver plusieurs médias de transport, et parmi ces médias nous citons :
- Câble coaxial(Câble à deux conducteurs de pôles opposés, séparés par un isolant).
- Paire torsadée(Ligne de transmission constituée de deux fils conducteurs enroulés en hélice l'un autour de l'autre).
- Fibre optique(Fil en verre ou en plastique dans le lequel passe l'internet).
- Ondes hertziennes(Ondes électromagnétiques, utilisées en particulier pour la télécommunication sans fil).

(b) Mode de transmission : Selon le sens des échanges, nous distinguons trois modes de transmission :
- Liaison simplex (Mode de communication unidirectionnel, dans lequel chaque appareil est soit émetteur ou récepteur).
- Liaison half-duplex (Deux système interconnecter, capable d'émettre et de recevoir chacun leur tour).
- Liaison full-duplex (Deux systèmes interconnecter, capable d'émettre et de recevoir simultanément).

1.2.2.2 Réseau étendu (WAN)

Un réseau étendu est un ensemble de LAN reliés entre-eux par des routeurs. Caractériser par

- les liaisons micro-ondes qui sont des supports de transmission d'informations utilisées pour relier différents réseaux, et des réseaux qui n'autorisent aucune connexion physique.
- La liaison point à point qui consiste à établir une connexion entre un opérateur et le réseau d'un client via une ligne louée.

1.2.2.3 Réseau métropolitaine (MAN)

Le réseau métropolitaine permet de :

- Relier deux réseaux local(LAN) sans que la vitesse de transfert ne soit affectée.
- Communiquer deux LAN distants comme si ils faisaient partie d'un même réseau local.

1.2.3 Topologie de réseau

Parmi ces topologies on a :

(a) **Topologie en BUS :** Repose sur un câblage, sur lequel viennent se connecter des noeuds (postes de travail, équipement d'interconnexion, périphériques). Il s'agit d'un support multipoints. Le câble est l'unique élément matériel constituant le réseau et seuls les noeuds génèrent les signaux. La figure 1.3 montre la topologie en Bus

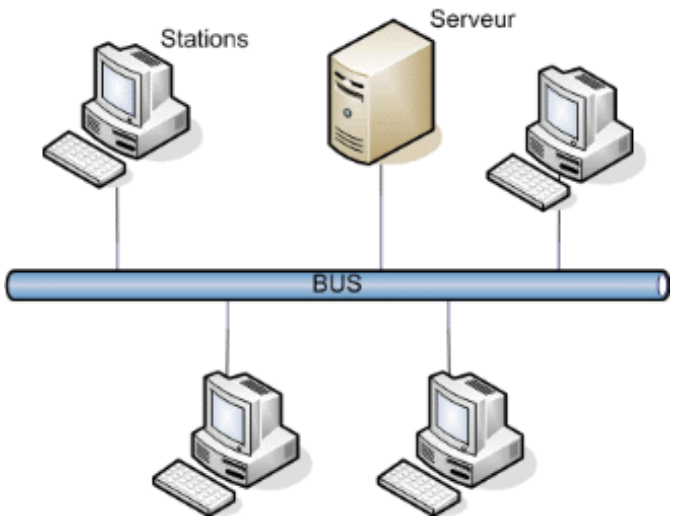

FIGURE 1.3 – Topologie en Bus

(b) **Topologie en Étoile :** Quant à elle, repose sur des matériels actifs. Ce dernier remet en forme les signaux et les régénère. Il intègre une fonction de répéteur. Ces points centraux sont appelés des concentrateurs (hubs). Il est possible de créer une structure hiérarchique en constituant un nombre limité de niveaux. La figure 1.4 montre la topologie en Étoile

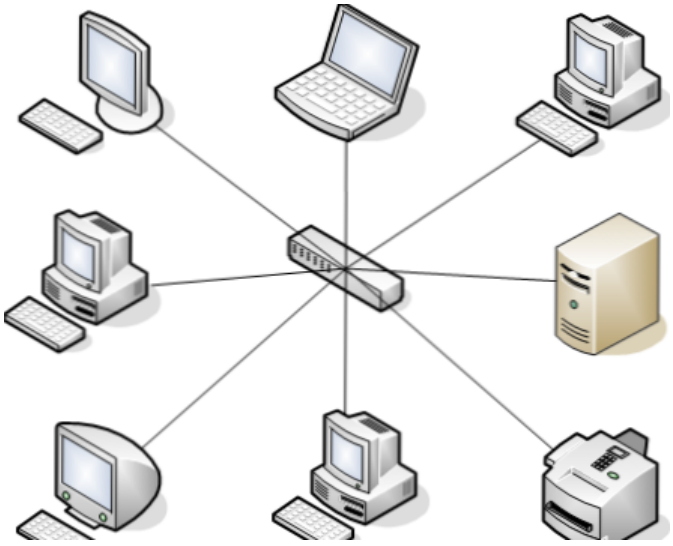

FIGURE 1.4 – Topologie en Étoile.

(c) **Topologie en Anneau :** Cette topologie repose sur une boucle fermée, constituée de liaisons point à point entre périphérique. Les trames transitent par chaque noeud qui se comporte comme un répéteur (élément actif). Les concentrateurs en anneau permettent l'insertion de stations dans un réseau. La figure 1.5 montre la topologie en Anneau

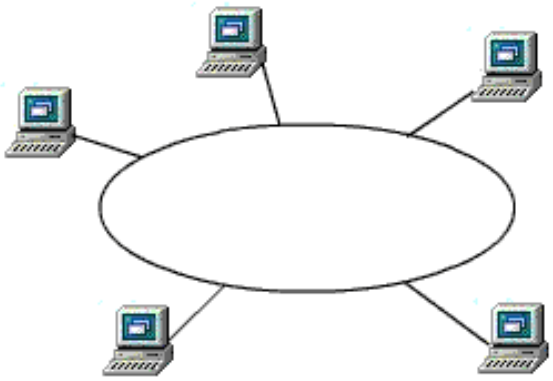

FIGURE 1.5 – Topoogie en Anneau

(d) **Topologie en Arbre :** Dans cette architecture, les postes sont reliés entre eux de manière hiérarchique, à l'aide des concentrateurs cascadables. La figure 1.6 montre la topologie en Arbre

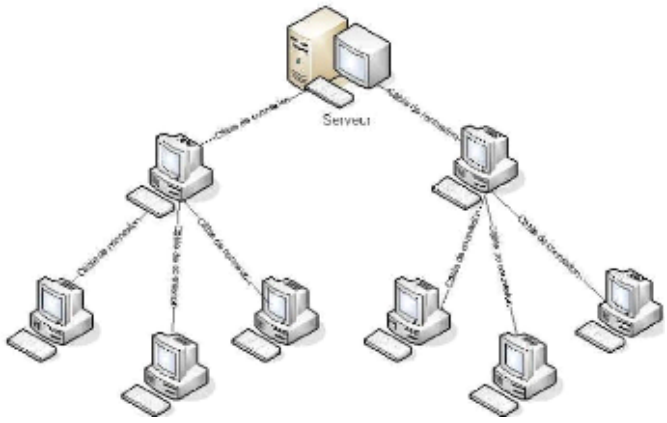

FIGURE 1.6 – Topologie en Arbre

1.3 Protocole de communication réseau

Un protocole de communication est un ensemble de règles qui rendent les communications possibles, ces règles peuvent être modélisés et catégorisés selon divers critères.

1.3.1 Modèle OSI

L'ISO (International Organization for Standardization) a développé, en 1978, le modèle OSI (Open Systems Interconnection) qui décrit les concepts mis en oeuvre pour normaliser l'interconnexion entre systèmes hétérogènes ce modèle permet de :

— Échanger des fichiers.
— Échanger des messages électroniques.
— Se connecter à d'autres systèmes (Terminal virtuel).
— Faire coopérer des applications se trouvant sur des systèmes différents.
— Faire travailler d'autres systèmes.

La norme OSI est basée sur sept couches, la plus haute présente les programmes d'applications la plus basse présente l'électronique de modulation et chaque couche fourni des services à la couche supérieure et utilise des services de la couche inférieure.

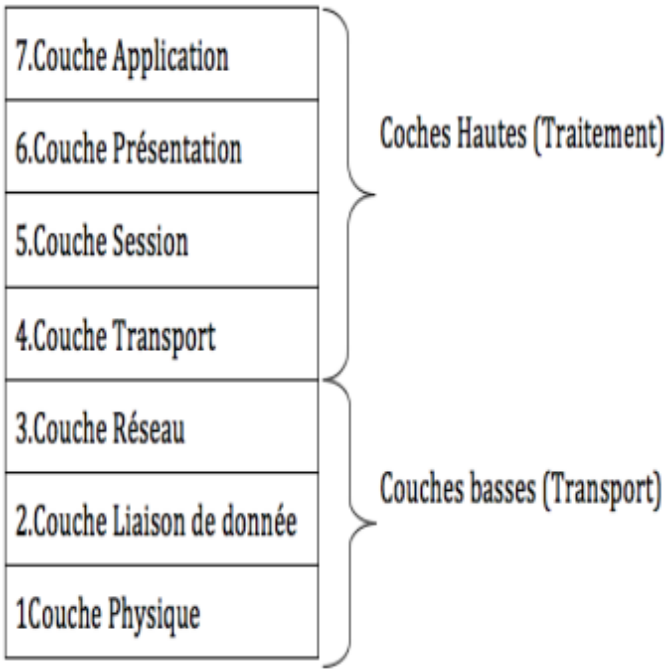

FIGURE 1.7 – Norme OSI

Le rôle de chacune des couches de la figure 1.7 est :

- **Couche Physique**
  Elle assure le transfert des bits sur le support de transmission. À cet effet, elle définit les spécifications mécaniques (connecteur), électriques (niveau de tension), et les spécifications fonctionnelles des éléments de raccordement nécessaires à l'établissement, au maintien et à la libération de la ligne.

- **Couche Liaison**
  Elle assure un service de transfert de blocs de données (trames) entre deux systèmes adjacents en assurant le contrôle, l'établissement, le maintien et la libération du lien logique entre les entités. Elle permet en outre, de détecter les erreurs incohérentes aux supports physiques.

- **Couche Réseau**
  La couche réseau doit permettre d'acheminer correctement les paquets d'informations jusqu'à l'utilisateur final. Pour aller de l'émetteur au récepteur, il faut passer par des noeuds de transfert intermédiaire interconnectant deux ou plusieurs réseaux. Cette couche assure trois fonctionnalités principales :
  - Le contrôle de flux,
  - Le routage
  - L'adressage.

- **Couche Transport**
  Elle est la couche pivot du modèle OSI. Elle assure le contrôle du transfert de bout en bout lors du transfert des informations (messages) entre les deux extrémités communicantes. Elle est la dernière couche de contrôle des informations, elle doit assurer aux couches supérieures un transfert fiable quelle que soit la qualité du sous-réseau de transport utilisé.

- **Couche Session**
  Elle gère l'échange de données entre les applications distantes. La fonction essentielle de cette couche est la synchronisation des échanges et la définition de points de reprise.

- **Couche Présentation**
  Cette couche assure la mise en forme des données pour qu'elles soient accessibles à l'utilisateur. Elle effectue les fonctions de codage, compression, cryptage, décryptage, etc.

- **La couche Application**
  Cette couche est le point de contact entre l'utilisateur et le réseau, c'est donc elle qui apporte à l'utilisateur les services de base offerts par le réseau, comme par exemple le transfert de fichiers, la messagerie, etc.

1.3.2 Modèle TCP/IP

Un protocole crée dans les années 70 par Bob Kahn, du Defense ARPA. La famille TCP/IP comporte plusieurs dizaine de protocoles, définit un modèle en quatre couches réseau. Il s'agit des protocoles de communication et d'application les plus populaire pour connecter des systèmes hétérogènes, indépendamment de la couche physique. Transmission Control Protocol (TCP) est un protocole de transport qui assure un service fiable, orienté connexion pour un flot d'octets. Par opposition avec TCP, User Datagram Protocol (UDP) est le protocole de transport non orienté connexion. Il est donc très rapide mais surtout peu fiable.
Internet Protocol (IP) fournit un système de livraison de paquets, sans connexion et non fiable. Il gère des adresses logiques, qui décomposent l'identifiant de chaque noeud en un numéro de périphérique sur quatre octets (en IP version 4 (IPV4). La figure 1.8 présente un modèle TCP/IP.[2]

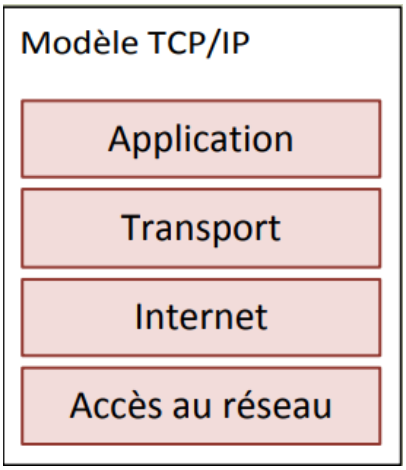

FIGURE 1.8 – Modèle de référence TCP/IP

Le modèle de référence TCP/IP comporte quatre couches ; Chaque couche illustre une fonction réseau bien précise. Cette répartition des fonctions réseau est appelée organisation en couches.

- **Couche de liens ou accès au réseau**
  L'interface avec le réseau, constituée d'un driver du système d'exploitation et d'une carte d'interface avec le réseau.
- **Couche réseau ou couche IP (Internet Protocol)**
  Cette couche gère la circulation des paquets à travers le réseau en assurant leur routage.
- **Couche transport**
  La couche transport assure tout d'abord une communication de bout en bout en faisant abstraction des machines intermédiaires entre l'émetteur et le destinataire.
  Elle s'occupe de réguler le flux de données et assure un transport fiable (données transmises sans erreur et reçues dans l'ordre de leur émission) dans le cas de TCP (Transmission Control Protocol).
  Non fiable dans le cas de UDP (User Datagram Protocol). Pour UDP, il n'est pas garanti qu'un paquet (appelé dans ce cas datagramme) arrive à bon port, c'est à la couche application de s'en assurer.

- **Couche application**
  Est celle des programmes utilisateurs comme telnet("terminal network", connexion à un ordinateur distant), FTP (File Transfert Protocol), SMTP (Simple Mail Transfert Protocol), etc ...

La capacité de fonctionnement sur toutes tailles de réseau, son efficacité et l'évolution de TCP/IP ont séduit les entreprises. Elles ont interconnectés leurs réseaux par internet, surtout pour des applications de messagerie et WEB.

1.3.3 Comparaison entre la norme OSI et le protocole TCP/IP

La norme OSI différe du protocole TCP/IP dans plusieurs niveaux, on cite quelques différences :

— TCP / IP est un modèle client-serveur, c'est-à-dire lorsque le client demande un service, il est fourni par le serveur. Tandis que, le modèle OSI est un modèle conceptuel.
— TCP / IP est un protocole standard utilisé pour tous les réseaux, y compris Internet, tandis que OSI n'est pas un protocole mais un modèle de référence utilisé pour comprendre et concevoir l'architecture du système.
— TCP / IP est un modèle à quatre couches, tandis que OSI a sept couches.
— TCP / IP suit l'approche verticale. Alors, le modèle OSI prend en charge l'approche horizontale.
— TCP / IP est réel, par contre OSI est conceptuel.
— TCP / IP suit une approche de haut en bas, tandis que le modèle OSI suit une approche ascendante(de bas en haut). [3]

1.4 Utilité d'un réseau informatique d'entreprise

Le réseau d'entreprise permet de relier chaque ordinateur entre eux via un serveur qui va gérer l'accès à Internet, les e-mails, les droits d'accès aux documents partagés et le travail collaboratif. Chaque utilisateur du réseau se connecte avec un nom d'utilisateur et un mot de passe authentifié par le serveur. L'utilisateur peut accéder à ses données et au partage de fichiers. le réseau d'entreprise permet de centralisé les données de l'entreprise, les sécurisés et de travailler en équipe .[4]

1.5 Sécurité informatique

La sécurité informatique est un ensemble de moyens techniques, organisationnels, juridiques et humains utilisés pour garantir la sécurité des systèmes manipulés, notamment la sécurité des données et des communications.

1.5.1 Objectifs de sécurité

Le système d'information est généralement défini par l'ensemble des données et des ressources matérielles et logicielles de l'entreprise permettant de les stocker ou de les faire circuler. Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger.

La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

La sécurité informatique vise généralement cinq principaux objectifs :

- **Confidentialité :** Elle consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction.

- **Authentification :** L'authentification consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.

- **Intégrité :** Vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).

- **Disponibilité :** L'objectif de la disponibilité est de garantir l'accès à un service ou à des ressources.

- **Non répudiation :** La non répudiation de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction.

1.5.2 Terminologie de la sécurité informatique

La sécurité informatique utilise un vocabulaire bien défini, pour mieux comprendre les risques possibles des attaques informatiques et définir certains termes comme :

- **Vulnérabilités :** Ce sont les failles de sécurité dans un ou plusieurs systèmes. Tout système vu dans sa globalité présente des vulnérabilités, qui peuvent être exploitables ou non.
- **Attaques (exploits) :** Elles représentent les moyens d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables.
- **Contre-mesures :** Ce sont les procédures ou techniques permettant de résoudre une vulnérabilité ou de contrer une attaque spécifique (auquel cas il peut exister d'autres attaques sur la même vulnérabilité).
- **Menaces :** Ce sont des adversaires déterminés capables de monter une attaque exploitant une vulnérabilité.[5]

1.5.3 Politique de sécurité

La sécurité des systèmes informatiques se cantonne généralement à garantir les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des ressources possèdent uniquement les droits qui leur ont été octroyés.

Les mécanismes de sécurité mis en place peuvent néanmoins provoquer une gêne au niveau des utilisateurs et les consignes et règles deviennent de plus en plus compliquées au fur et à mesure que le réseau s'étend. Ainsi, la sécurité informatique doit être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance.

C'est la raison pour laquelle il est nécessaire de définir dans un premier temps une politique de sécurité, dont la mise en oeuvre se fait selon les quatre étapes suivantes :

- Identifier les besoins en terme de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences ;
- Elaborer des règles et des procédures à mettre en oeuvre dans les différents services de l'organisation pour les risques identifiés ;
- Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés ;
- Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace ;

La politique de sécurité est donc l'ensemble des orientations suivies par une organisation (à prendre au sens large) en terme de sécurité. A ce titre elle se doit d'être élaborée au niveau de la direction de l'organisation concernée, car elle concerne tous les utilisateurs du système.

1.6 Types d'attaques

Il existe deux grandes catégories d'attaques :

- **Attaques passives :** Consistent à écouter sans modifier les données ou le fonctionnement du réseau. Elles sont généralement indétectables mais une prévention est possible.
- **Attaques actives :** Consistent à modifier des données ou des messages, à s'introduire dans des équipements réseau ou à perturber le bon fonctionnement de ce réseau. Noter qu'une attaque active peut être exécutée sans la capacité d'écoute. De plus, il n'y a généralement pas de prévention possible pour ces attaques, bien qu'elles soient détectables (permettant ainsi une réponse adéquate). La figure 1.9 présente un exemple d'attaque passive et d'attaque active.[6]

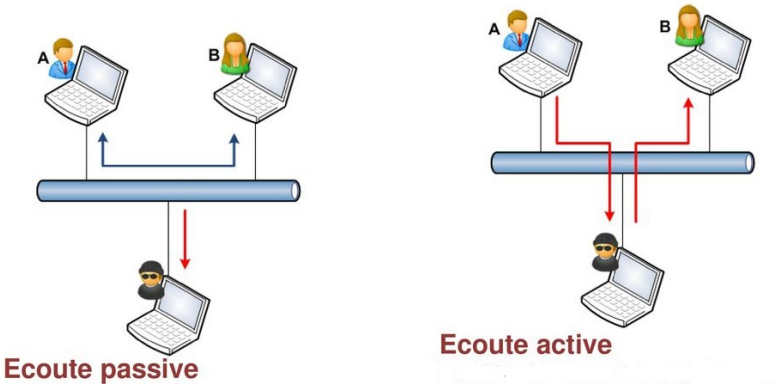

FIGURE 1.9 – Attaques passives et actives

1.6.1 Type d'insécurités

On distingue généralement deux types d'insécurités :

- **État actif d'insécurité**, c'est-à-dire la non connaissance par l'utilisateur des fonctionnalités du système, dont certaines pouvant lui être nuisibles (par exemple le fait de ne pas désactiver des services réseaux non nécessaires à l'utilisateur).
- **État passif d'insécurité**, c'est-à-dire la méconnaissance des moyens de sécurité mis en place, par exemple lorsque l'administrateur (ou l'utilisateur) d'un système ne connaît pas les dispositifs de sécurité dont il dispose.

1.7 Dispositifs de protection

La méthodologie généralement employée par le pirate informatique consiste à scruter le réseau (en envoyant des paquets de données de manière aléatoire) à la recherche d'une machine connectée, puis à chercher une faille de sécurité afin de l'exploiter et d'accéder aux données s'y trouvant. Cette menace est d'autant plus grande que la machine est connectée en permanence à internet pour plusieurs raisons :

- La machine cible est susceptible d'être connectée sans pour autant être surveillée.
- La machine cible est généralement connectée avec une plus large bande passante.
- La machine cible ne change pas (ou peu) d'adresse IP.

Ainsi, il est nécessaire, autant pour les réseaux d'entreprises que pour les internautes possédant une connexion de type câble ou ADSL, de se protéger des intrusions réseaux en installant un dispositif de protection.

1.7.1 Pare-feu

Un pare-feu (appelé aussi coupe-feu, garde-barrière ou firewall en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

- une interface pour le réseau à protéger (réseau interne).
- une interface pour le réseau externe.

La figure 1.10 montre une architecture d'un pare-feu.

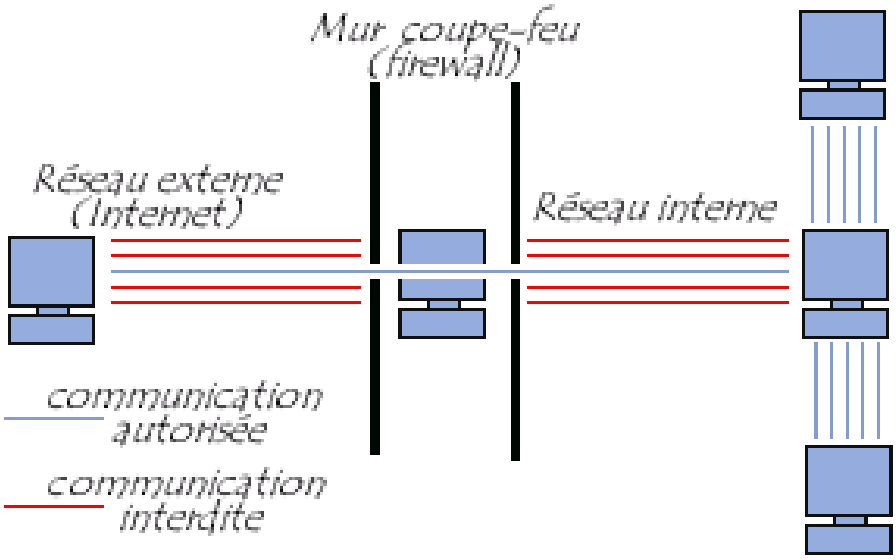

FIGURE 1.10 – Architecture d'un pare-feu.

1.7.1.1 Objectifs d'un pare-feu

Le pare-feu permet de :

> **Protéger un environnement :** (vis à vis de l'extérieur)

- Tout n'est pas bien administré.
- Des machines ne doivent pas être accessibles par tous.
- Certaines doivent être "accessibles" (serveur WWW, FTP, Courriel).

> **Contrôler les accès entrant et sortant :**

- Contrôler et/ou espionner.
- Autoriser certains services seulement :
  - Dans un sens pas dans l'autre.
  - Vers/depuis certaines machines seulement.

Barrière de Sécurité, Introduction Serveur de proximité, pare-feu IP, filtrage, architecture

1.7.1.2 Fonctionnement d'un système pare-feu

Un système pare-feu contient un ensemble de règles prédéfinies permettant :

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

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

- Soit d'autoriser uniquement les communications ayant été explicitement autorisées : "Tout ce qui n'est pas explicitement autorisé est interdit".
- Soit d'empêcher les échanges qui ont été explicitement interdits. La première méthode est sans doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

1.7.1.3 Type de filtrage

Il existe quatre types de filtrage :

(a) **Filtrage simple de paquets**

Un système pare-feu fonctionne sur le principe du filtrage simple de paquets (en anglais : stateless packet filtering). Il analyse les en-têtes de chaque paquet de données (datagramme) échangé entre une machine du réseau interne et une machine externe.

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

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

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

(b) **Filtrage dynamique**

Le filtrage simple de paquets ne s'attache qu'à examiner les paquets IP indépendamment les uns des autres, ce qui correspond au niveau 3 du modèle OSI. Or, la plupart des connexions reposent sur le protocole TCP, qui gère la notion de session, afin d'assurer le bon déroulement des échanges. D'autre part, de nombreux services (le FTP par exemple) initient une connexion sur un port statique, mais ouvrent dynamiquement (c'est-à-dire de manière aléatoire) un port afin d'établir une session entre la machine faisant office de serveur et la machine cliente.

Un dispositif pare-feu de type inspection d'état (en anglais stateful inspection), est ainsi capable d'assurer un suivi des échanges, c'est-à-dire de tenir compte de l'état des anciens paquets pour appliquer les règles de filtrage. De cette manière, à partir du moment où une machine autorisée initie une connexion à une machine située de l'autre côté du pare-feu ; l'ensemble des paquets transitant dans le cadre de cette connexion seront implicitement acceptés par le pare-feu.

Si le filtrage dynamique est plus performant que le filtrage de paquets basique, il ne protège pas pour autant de l'exploitation des failles applicatives, liées aux vulnérabilités des applications. Or ces vulnérabilités représentent la part la plus importante des risques en terme de sécurité.

(c) **Filtrage applicatif**

Le filtrage applicatif permet de filtrer les communications application par application. Le filtrage applicatif opère donc au niveau 7 (couche application) du modèle OSI, contrairement au filtrage de paquets simple (niveau 4). Le filtrage applicatif suppose donc une connaissance des protocoles utilisés par chaque application. Le filtrage applicatif suppose donc une bonne connaissance des applications présentes sur le réseau, et notamment de la manière dont elle structure les données échangées (ports, etc.).

Un firewall effectuant un filtrage applicatif est appelé généralement passerelle applicative, (ou proxy), car il sert de relier entre deux réseaux en s'interposant et en effectuant une validation fine du contenu des paquets échangés. Le proxy représente donc un intermédiaire entre les machines du réseau interne et le réseau externe, subissant les attaques à leur place. De plus, le filtrage applicatif permet la destruction des en-têtes précédant le message applicatif, ce qui permet de fournir un niveau de sécurité supplémentaire.
La figure 1.11 montre le pare-feu avec filtrage dynamique et applicatif.

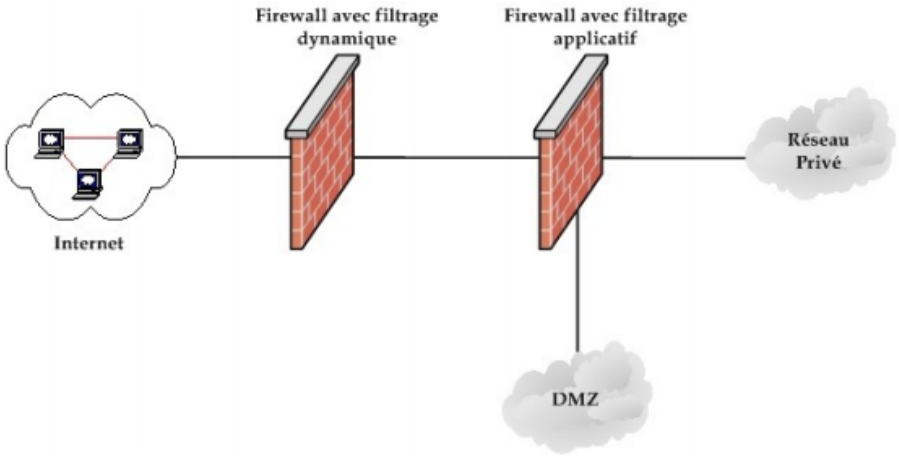

FIGURE 1.11 – Différent filtre d'un pare-feu

1.7.1.4 Différents catégories de pare-feu

Il existe différentes catégories de pare-feu. Chacune d'entre-elles disposent d'avantages et d'inconvénients qui lui sont propre.

(a) **Pare-feu sans états (ou stateless)** Ce sont les pare-deu les plus anciens mais surtout les plus basiques qui existent. Ils font un contrôle de chaque paquets indépendamment des autres en se basant sur les règles prédéfinies par l'administrateur (généralement appelées ACL(Access Control Lists)). Ces pare-feux interviennent sur les couches réseau et transport. Les règles de filtrages s'appliquent alors par rapport à une adresses IP sources ou destination, mais aussi par rapport à un port source ou destination.

(b) **Pare-feu à états (ou stateful)** Les pare-feux à états sont une évolution des pare-feux sans états. La différence entre ces deux types de pare-feu réside dans la manière dont les paquets sont contrôlés. Les pare-feux à états prennent en compte la validité des paquets qui transitent par rapport aux paquets précédemment reçus. Ils gardent alors en mémoire les différents attributs de chaque connexions, de leur commencement jusqu'à leur fin, c'est le mécanisme de stateful inspection. De ce fait, ils seront capables de traiter lespaquets non plus uniquement suivant les règles définies par l'administrateur, mais également par rapport à l'état de la session :

- NEW : Un client envoie sa première requête.
- ESTABLISHED : Connexion déjà initiée. Elle suit une connexion NEW.
- RELATED : Peut être une nouvelle connexion, mais elle présente un rapport direct avec une connexion déjà connue.
- INVALID : Correspond à un paquet qui n'est pas valide.

(c) **Pare-feu applicatif** Les pare-feux applicatif (aussi nommé pare-feu de type proxy ou passerelle applicative) fonctionne sur la couche 7 du modèle OSI. Cela suppose que le pare-feu connaisse l'ensemble des protocoles utilisés par chaque application. Chaque

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

(d) **Pare-feu authentifiant** Les pare-feux authentifiant permettent de mettre en place des règles de filtrage suivant les utilisateurs et non plus uniquement suivant des machines à 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. Il existe plusieurs méthode d'association. Par exemple authpf, qui utilise SSH, ou encore NuFW qui effectue l'authentification par connexion.

(e) **Pare-feu personnel** Les pare-feux personnels sont installés directement sur les postes de travail. Leur principal but est de contrer les virus informatiques et logiciels espions (spyware). Leur principal atout est qu'ils permettent de contrôler les accès aux réseaux des applications installés sur la machines. Ils sont capables en effet de repérer et d'empêcher l'ouverture de ports par des applications non autorisées à utiliser le réseau.[7]

1.7.2 Serveur proxy

SECURITE DU SYSTEME D'INFORMATION (SSI), 2010.2011, ISCAE Un serveur proxy (proxy server,appelé aussi serveur mandataire) Est à l'origine d'une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local et internet. La plupart du temps le serveur proxy est utilisé pour le web, il s'agit alors d'un proxy HTTP. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP, ...). La figure 1.12 illustre l'architecture du proxy.

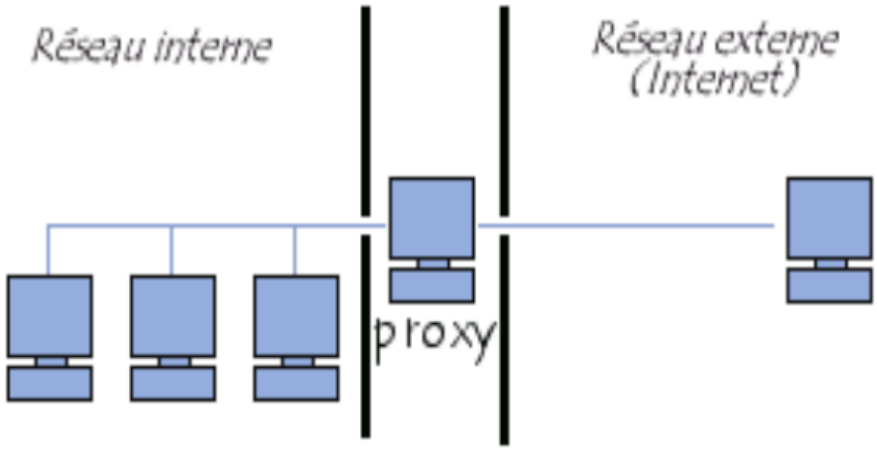

FIGURE 1.12 – Architecture du proxy

1.7.2.1 Principe d'un proxy

Le principe de fonctionnement basique d'un serveur proxy est assez simple : il s'agit d'un serveur "mandaté" par une application pour effectuer une requête sur Internet à sa place. Ainsi,

lorsqu'un utilisateur se connecte à internet à l'aide d'une application cliente configurée pour utiliser un serveur proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur proxy va alors se connecter au serveur que l'application cliente cherche à joindre et lui transmettre la requête. Le serveur va ensuite donner sa réponse au proxy, qui va à son tour la transmettre à l'application cliente.

1.7.3 Zone démilitarisée

Une DMZ est une zone tampon d'un réseau d'entreprise, située entre le réseau local et Internet, derrière le pare-feu. Il s'agit d'un réseau intermédiaire regroupant des serveurs publics (HTTP, DHCP, mails, DNS, etc.). Ces serveurs devront être accessibles depuis le réseau interne de l'entreprise et, pour certains, depuis les réseaux externes. Le but est ainsi d'éviter toute connexion directe au réseau interne. La figure 1.13 illustre l'architecture DMZ.

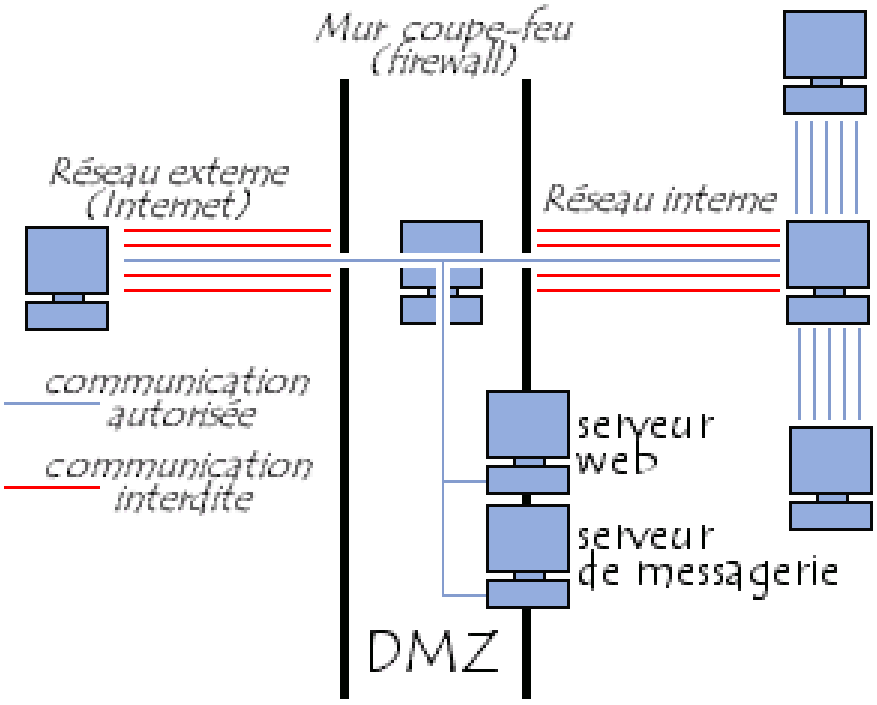

FIGURE 1.13 – Architecture DMZ

1.7.3.1 Principe de DMZ(Demilitarized Zone)

Comme principe on cite :

- **Moindre privilège :** Un sujet ne doit avoir que les privilèges minimales afin de compléter ses tâches.
- **Séparation des privilèges :** Un sujet ne doit pas être autorisé seulement en se basant sur une condition unique.
- **Protégé par défaut :** À moins d'être explicitement autorisé, un sujet ne doit pas avoir accès à un objet.
- Les mécanismes de sécurité doivent être le plus simple possible afin d'éviter des failles (logicielles ou matérielles) pouvant être exploitées.[8]

1.8 Sécurité informatique d'entreprise

La sécurité informatique de l'entreprise repose sur une bonne connaissance des règles par les employés, grâce à des actions de formation et de sensibilisation auprès des utilisateurs, et elle doit couvrir les champs suivants :

- Un dispositif de sécurité physique et logique, adapté aux besoins de l'entreprise et aux usages des utilisateurs.
- Une procédure de management des mises à jour.
- Une stratégie de sauvegarde correctement planifiée.
- Un plan de reprise après incident.
- Un système documenté à jour.

1.9 Virtualisation

La virtualisation est une couche d'abstraction qui découple le système d'exploitation du matériel afin de délivrer une meilleure utilisation et flexibilité des ressources de traitement (VirtuelBox)

1.9.1 Intérêts de la virtualisation :

La virtualisation permet :

- Un usage optimale des ressources.
- Une installation, déploiement et migration facile.
- Une économie sur le matériel par mutualisation(consommation électrique, entretien physique, monitoring, support, compatibilité matérielle, etc.).
- La sécurisation d'un réseau (arrêt des systèmes d'exploitation virtuels, mais pas des systèmes

d'exploitation hôtes qui sont invisible pour l'attaquant, tests d'architectures applicatives et réseau).

- L'isolation des différents utilisateurs simultanés d'une même machine (utilisateur de type site central).
- Une allocation dynamique de la puissance de calcul en fonction des besoins de chaque application à un instant donné.
- Une diminution des risques liés au dimensionnement des serveurs lors de la définition de l'architecture d'une application, l'ajout de puissance (nouveau serveur etc.) étant alors transparent.

1.9.2 Différentes techniques de virtualisation :

Il ya quatre types de virtualisation :

(a) **Virtuel machine (Hyperviseur de type 2 (ou Architecture hébergée))**
Un logiciel qui tourne sur l'OS hôte, permettant de lancer un ou plusieurs OS invités, c'est l'archétype de la solution de virtualisation par empilement de systèmes. La machine virtualise le matériel (ce qui passe généralement par une émulation partielle) pour les systèmes d'exploitation invités, les systèmes d'exploitation invités croient dialoguer directement avec le matériel. En pratique on a recours à une émulation logicielle des périphériques, et parfois aussi de tout ou partie de la machine.

- Application installée sur l'OS.
- Virtualise et/ou émule le matériel.
- Comparable à un émulateur mais accès direct au CPU, RAM, FS.
- Performances réduites si le CPU doit être émulé.
- Bonne étanchéité entre les OS invités.

(b) **Virtualisation d'OS ou Isolateur**
Un logiciel permettant d'isoler l'exécution des applications dans des contextes ou zones d'exécution. C'est l'archétype de la solution de virtualisation par "juxtaposition". L'isolateur permet ainsi de faire tourner plusieurs fois la même application (à base d'un ou plusieurs logiciels) prévue pour ne tourner qu'à une seule instance par machine.

- Isole l'exécution des applications dans des contextes d'exécution.
- Généralisation de la notion de contexte Unix, plus isolation des périphériques, et des systèmes de fichiers.
- Solution très performante et économique en mémoire.
- Partage du code noyau (donc mauvaise isolation). Exemple : chroot (changement de racine), Linux Vserver, OpenVZ (Virtuozzo), Docker, LXC (Cgroups).

(c) **Hyperviseur complet (dit de type-1 ou bare-metal)**
Un outil qui s'interpose entre la couche matérielle et logicielle. Celui-ci a accès aux composants de la machine et possède son propre noyau. C'est donc par dessus de ce noyau que les OS seront installés.
- Noyau système léger et optimisé.
- Outils de supervision.
- Permet l'exécution d'OS natifs.
- Usage d'instructions dédiées à la virtualisation (sinon émulation).
- Ex : XEN, KVM, Vmware vSphere.

(d) **Paravirtualisation (Hyperviseur de type 1 également)**
Un paravirtualiseur est un noyau hôte allégé et optimisé pour ne faire tourner que des noyaux de systèmes d'exploitation invités, adaptés et optimisés
- Noyau système allégé et optimisé.
- Noyau invités adaptés et optimisés.
- Utilisable sans les instructions spécifiques (ex : VT-x ou AMD-v).
- Impraticables pour les systèmes non libres.
- Exemples : Vmware Vsphere, XEN, Microsoft Hyper-V server, KVM,.. [9]

La figure 1.14 montre les différentes techniques de virtualisation.

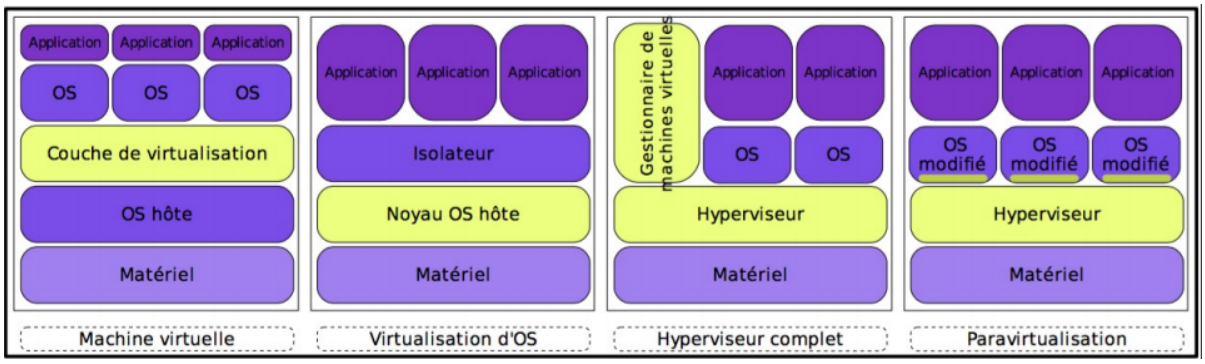

FIGURE 1.14 – Différents techniques de virtualisation

1.9.3 Sécurité par la virtualisation

La virtualisation consiste à recréer tout ou partie d'un ordinateur de manière logicielle. Ce procédé a une solution de sécurité, est une approche originale pour réduire les risques liés aux malwares, la virtualisation ne protège pas puisque l'ordinateur virtuel ou l'application virtualisée peuvent être infectés. En revanche, l'ordinateur physique et son système ne sont théoriquement pas menacés par le contenu de la machine virtuelle. On a deux types de sécurité par la virtualisation :

(a) **Virtualisation complète**
Les logiciels qui virtualisent entièrement une machine comme VMwar, Virtual PC ou virtualBox, permettent de revenir à l'état précédente de la machine, ce qui garantit l'absence de contamination persistante. Ces solutions de virtualisation sont très appréciables pour des postes ouverts à tous les publics. En revanche, elles nécessitent une isolation complète avec les réseaux sécurisés. Autre limitation, les machines virtuelles demandent des ordinateurs plus puissants pour assurer une bonne fluidité dans le système émulé. Enfin, de plus en plus de malwares peuvent détecter que leur environnement est virtuel. Il n'est donc pas impossible qu'ils puissent aussi tenter de s'évader de l'émulation en profitant de failles éventuelles.

(b) **Virtualisation applicative**
La virtualisation qui se limite à une application a le même intérêt : le système réel qui exécute l'application dans son environnement virtuel n'est pas accessible à l'éventuel malware. Cette astuce est très souvent appliquée aux navigateurs WEB qui sont les cibles privilégiées des cybercriminels.

Autre limitation évidente : ces machines virtuelles et applications virtualisées ne peuvent être utilisées pour manipuler des données sensibles puisqu'elles contiennent les mêmes failles qu'un système réel.

1.10 Conclusion

Dans ce chapitre, nous avons défini quelques notions fondamentales concernant les réseaux, la sécurité informatique et les dispositifs de protection à prendre pour remédier aux menaces et aux attaques. Le prochain chapitre sera consacré à la présentation de l'organisme d'accueil.

Chapitre 2

Présentation de l'organisme d'accueil

2.1 Introduction :

Dans une organisation Le savoir-faire en administration des systèmes incluent la connaissance des systèmes d'information et de la manière dont les gens les utilisent. Ceci comprend à la fois une certaine connaissance des systèmes d'exploitation et des logiciels applicatifs, ainsi que le dépannage matériel et logiciel.

Ce chapitre sera consacré pour présenter l'organisme d'accueil en premier lieu, posée la problématique et proposé une solution.

2.2 Historique :

La SARL RAMDY Ex (SARL Laiterie DJURDJURA) a été créée le 01/01/1983. Elle s'est spécialisée dans la production des yaourts, crèmes desserts, et les fromages frais et fondus.

Le 15 Octobre 2001, le groupe français DANONE s'est associé avec la laiterie DJURDJURA pour les activités yaourts, pâtes fraiches et desserts. Depuis, l'activité de la laiterie DJURDJURA s'est consacrée à la production des fromages fondus, aux pâtes molles (Camembert) et au lait pasteurisé.

Deux années plus tard, elle s'est implantée dans une nouvelle unité située en plein coeur de la zone d'activité TAHARACHT(AKBOU) triplant, ainsi, sa capacité de production en fromage fondus.

Dans le souci de répondre à une demande croissante du consommateur, la laiterie s'est équipée d'un matériel hautement performant dont une nouvelle conditionneuse de 220 portions/Minute, et une ligne complète du fromage barre.

En juin 2004, la SARL laiterie DJURDJURA a changé de raison sociale pour devenir SARL RAMDY. Et aujourd'hui, les produits laitiers DJURDJURA s'affichent sous la nouvelle dénomination ""RAMDY"".

En Octobre 2009, la SARL RAMDY a repris la production de yaourts et crèmes desserts. la figure 2.1 montre le logo de l'entreprise RAMDY.

FIGURE 2.1 – Logo de l'entreprise RAMDY

2.3 Moyens de l'entreprise

L'entreprise RAMDY à différents moyens qui sont :

2.3.1 Infrastructures

L'entreprise dispose d'un complexe intégré composé de deux(02) principaux départements de production "Atelier yaourt et crème dessert, Atelier fromage", et pour une surveillance de la qualité du produits et une protection optimale du consommateur, la SARL RAMDY s'est équipée d'un laboratoire d'auto-contrôle afin d'effectuer toutes les analyses physico-chimiques et microbiologiques exigées.

2.3.2 Équipements de production

L'entreprise RAMDY a deux ateliers de production :

1. **Atelier yaourt et crème dessert :** IL contient :
   - **Poudrage :** une salle de poudrage bien équipée.
   - **Traitement :** un processus pour la production de yaourts, crèmes desserts, et brassés.
   - **Conditionnement :** deux (02) conditionneuses de 12 000 Pots/h. une de 9 000 Pots/h et une 21 600 Pots/h, 5 000 Pots/h et deux de 7 500 Pots/h.
2. **Atelier Fromage :** Il contient :
   - **U**ne salle de préparation du produits, et une pour préparation des moules bien équipée.
   - **D**eux cuissons (un pour fromage portion, et l'autre pour le fromage barre)
   - **T**rois machines de conditionnement du fromage portion. Et deux machine pour le fromage barre, une machine Banderoleuse Grandi, et deux salles bien équipée pour la mise en cartons.

2.4 Services de l'entreprise

Les services de SARL RAMDY sont :

- **Direction générale :** elle assure la bonne gestion de l'entreprise et supervise tout son effectif.
- **Département des ressources humaines et moyens :** elle regroupe le service personnel, le service hygiène, gestion et paie.
- **Département approvisionnements :**il s'occupe de l'approvisionnement en matières première, et tous les autres produits nécessaires à l ?activité de l'entreprise, ce service est devisé en deux sections : achat et gestion des stocks.
- **Département finance et comptabilité :** il rassemble trois fonctions complémentaires qui sont : fonction financière, fonction comptabilité générale, et la fonction analytique.
- **Département maintenance :** il veille à ce que les équipements de production soient en bon état de marche afin de garantir une durée de vie maximale.
- **Département commercial et Marketing :** ce service est chargé de commercialiser les produits, planifier les ventes, prospecter le marché national. Il se compose de trois sections : section vente ; section recouvrement ; section réception.
- **Département production :** il est considéré le plus important dans l'entreprise, il s'occupe de la production de fromage et du yaourt.
- **Département assurance et qualité :** elle assure le suivi permanent et continuel de processus de production sous la supervision du laboratoire central qui suit la qualité microbiologique des produits.
- **Département technique :** est chargé de manager l'ensemble de l'activité technique de l'entreprise. Sa mission et de partager entre avant-vente, développement et après vente. Il peut aussi animer, gérer une équipe de consultants techniques et entretenir les relations avec les partenaires.
- **Service informatique :** c'est un service qui appartient au service responsable d'organisation et TIC. Ses principales fonctions sont :
    - Le suivi des applications de gestion.
    - La maintenance du parc informatique de l'entreprise.
    - Audit et amélioration du système d'information.
    - Sauvegarde et contrôle des données de l'entreprise.
    - Le développement de nouvelles applications aux différentes structures.

2.4.1 Architecture de l'organisme SARL RAMDY

L'organigramme générale de SARL RAMDY est donné par la figure 2.2. [10]

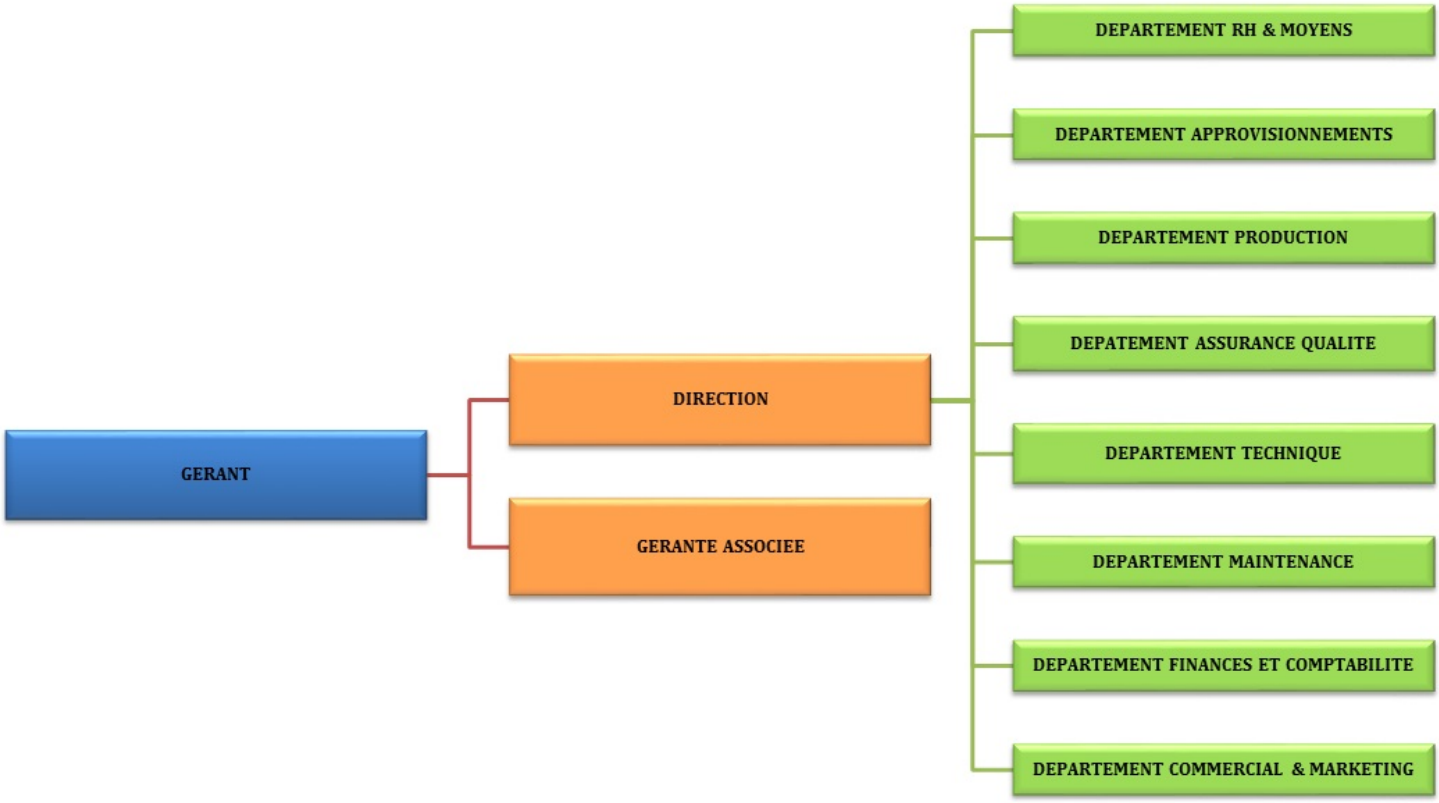

FIGURE 2.2 – Organigramme générale de SARL RAMDY

2.5 Problématique

Aujourd'hui l'Internet apporte une réelle valeur ajoutée aux entreprises, en permettant la communication avec de nombreux partenaires, fournisseurs et clients. Ce qui 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. Durant la période de stage, on a constaté des anomalies au niveau de la sécurisation du réseau de l'entreprise RAMDY. Les questions importantes qui méritent une attention particulière sont les suivantes :

- Qui doit être connecté au réseau (filaire ou sans fil) ?
- Que fait-il sur le réseau ?
- Qui attaque le réseau et quand est-ce que l'attaque a-t-elle eut lieu ?

Pour trouver une solution à notre problématique, il nous a été demandé de faire une étude en vue d'une mise en place d'un pare-feu open source qui sera associé au pare-feu existant suivant le principe de la défense en profondeur. Pour ce faire, nous avons crée un système de sécurité et monitoring du réseau. Nous allons donc installé un outil de sécurité et configuré un autre de monitoring réseau.

2.6 Conclusion

Dans ce chapitre on a donné un aperçu général sur l'organisme d'accueil SARL RAMDY, par la suite on a présenté quelques problèmes constaté durant la période du stage et à la fin on a proposé quelques solutions.

Chapitre 3

Monitoring

3.1 Introduction

Le monitoring réseau est un procédé de surveillance qui permet de contrôler et vérifier le bon fonctionnement d'une structure ou d'un parc informatique. Dans ce chapitre on va expliquer le monitoring réseau, son objectif. Ensuite on parlera sur le trafic réseau, gestion et le contrôle de trafic.

3.2 Présentation du monitoring

Le monitoring réseau ou network monitoring est une tâche de surveillance structurelle et de supervision applicative qui incombe à l'administrateur d'un réseau informatique. Sur base de points de contrôle préalablement établis, elle consiste essentiellement à s'assurer que le flux de données dans le réseau reste suffisamment important, et à remédier de manière proactive aux problèmes affectant les performances et la sécurité de l'ensemble du serveur. La figure 3.1 montre un exemple de monitoring.

FIGURE 3.1 – Monitoring système

3.2.1 Monitoring, un outil indispensable en entreprise

La sécurité est le premier objectif à l'installation d'un network monitor en entreprise. Au-délà des simples pare-feux ou antivirus, une solution de surveillance réseau met bien en évidence les pics d'activité inhabituels générés ou tout processus invalide, potentiellement révélateurs d'attaques malveillantes.
Grâce au reporting automatique des défaillances, les agents réseau peuvent donc répondre plus rapidement aux risques de sécurité clés, notamment ceux liés au transfert de fichiers, aux échanges de données sur le serveur ou aux mises à jour.

En temps réel et en temps différé via des protocoles et les formats de données SNMP, Syslog ou COPS, les outils de monitoring réseau et solutions de supervision permettent alors d'éviter ce genre de déconvenues en détectant rapidement les pertes de capacité du système d'information de l'entreprise. Le manager ou l'opérateur réseau reçoit alors des alertes (souvent par e-mail ou sms) en cas de surcharges ou de lenteurs et peut ainsi intervenir avec agilité directement via l'interface du network monitor.

En tant qu'outil de visualisation complet et holistique, le monitoring réseau permet la détection des anomalies sur l'ensemble du système informatique, internet et téléphonique de l'entreprise, les serveurs, les disponibilités réseaux (adsl, fibres, wi-fi), le courant électrique, les imprimantes, les applications, ainsi que tous les autres éléments actifs en contact avec le réseau (routeurs, switches, hubs, etc.). Une telle solution de supervision et de monitoring permet ainsi à l'administrateur de bien monitorer chaque point du réseau.

Enfin, un network monitor est également un puissant outil applicatif de bonne gouvernance et d'infogérance qui permet d'agir de manière proactive et de prévenir les problèmes de performance en amont pour maintenir le niveau de productivité global de l'entreprise.

3.2.2 Objectifs de monitoring d'un réseau :

Le monitoring vise à :

- Capter l'ensemble des actions importantes et des indicateurs de performance aux différents niveaux des systèmes (matériel et applicatif).
- Détecter les anomalies et/ou problèmes en temps réel et pouvoir agir.
- Être en mesure d'analyser la charge du système pour en déduire des tendances, repérer les corrélations et prévoir les besoins futurs (processeur, RAM, disques, réseau etc).
- Récupérer et analyser l'ensemble des logs système et applicatifs pertinents pour détecter et corriger les erreurs.

3.2.3 Utilité des outils de monitoring

Les logiciels de monitoring réseau permettent de garantir la disponibilité et la sécurité d'un réseau informatique. Ils fournissent aux administrateurs et managers des réseaux les outils de visualisation, d'analyse, de reporting, de supervision, de surveillance et d'alerte dont ils ont besoin pour assurer la bonne gestion de leurs infrastructures réseau et la productivité de leurs utilisateurs.

3.3 Open source

Open Source définit une licence qui permet d'accéder aux sources d'un programme informatique. La désignation open Source s'applique aux logiciels dont la licence respecte des critères précisément établis par l'Open Source Initiative, c'est-à-dire la possibilité de libère la distribution, d'accès au code source et aux travaux dérivés. Souvent un logiciel libre est qualifié d'open source, car les licences compatibles open source englobent les licences libres selon la définition de la Free Software.

3.3.1 Outils de de monitoring open source existants

Les outils de monitoring s'intègrent généralement à toute technologie et sont disponibles sous plusieurs formats, ce qui les rend très faciles à déployer en production. Leur gratuité permet aux entreprises de réorienter les budgets vers d'autres projets nécessitant un financement, ou alors de dépenser moins tout en offrant le même niveau de service et de support qu'avec des outils payants. Les outils existants sont montrés dans la figure 3.2.

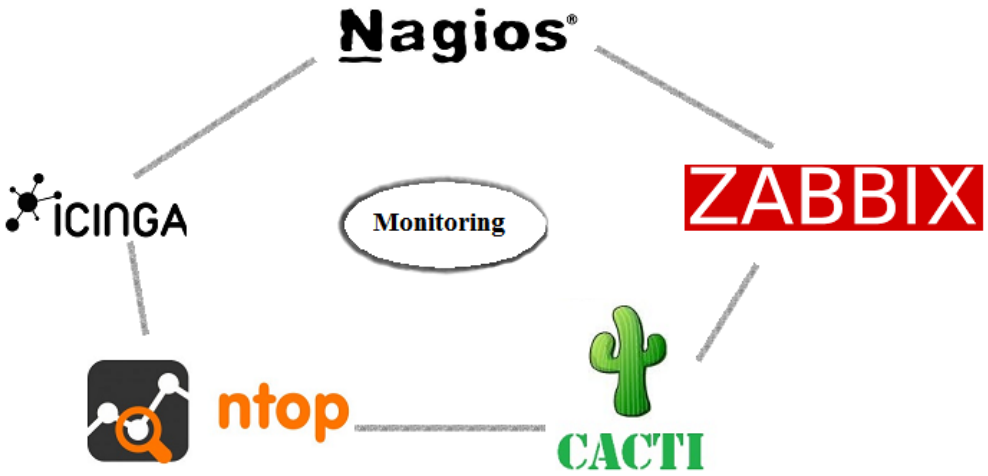

FIGURE 3.2 – Outils de monitoring

(a) **Nagios** Nagios est un puissant outil de surveillance du réseau, activement développé depuis de nombreuses années. Écrit en langage C, il permet d'effectuer presque toutes les tâches qu'un administrateur système et réseau peut attendre d'un package d'applications de surveillance. L'interface Web est rapide et intuitive, et la partie serveur est extrêmement fiable. La configuration assez complexe de Nagio peut poser un problème aux débutants, mais elle constitue également un avantage, l'outil pouvant être adapté à toutes les tâches de surveillance. L'interface Nagios est montrée par la figure 3.3

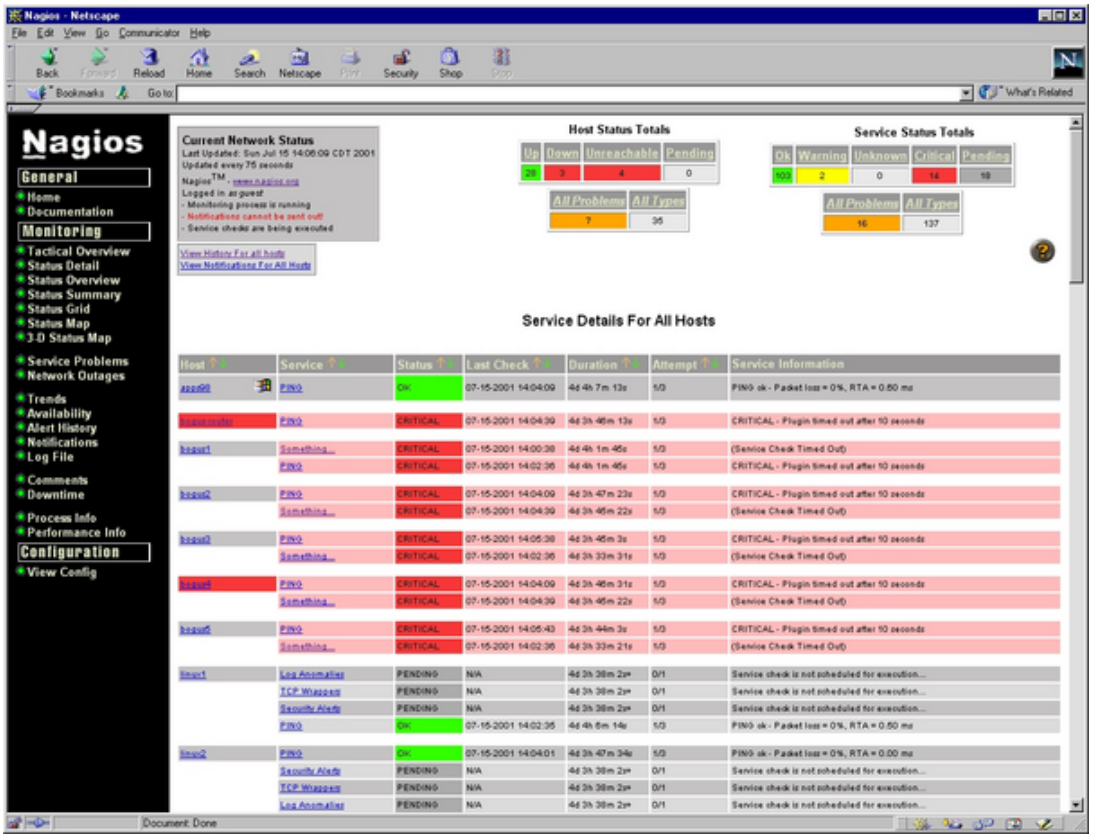

FIGURE 3.3 – Interface Nagios

(b) **Zabbix :** Zabbix est un outil complet de surveillance du réseau et du système, qui combine plusieurs fonctions dans une console Web. Il peut être configuré pour surveiller une grande variété de serveurs et d'équipements réseau et collecter des données. Il assure la surveillance des services et des performances de chaque objet. Zabbix permet de surveiller les serveurs et les réseaux à l'aide d'une vaste gamme d'outils, y compris des hyperviseurs de virtualisation dédiés à la surveillance et des piles d'applications WEB. L'interface Zabbix est montrée par la figure 3.4

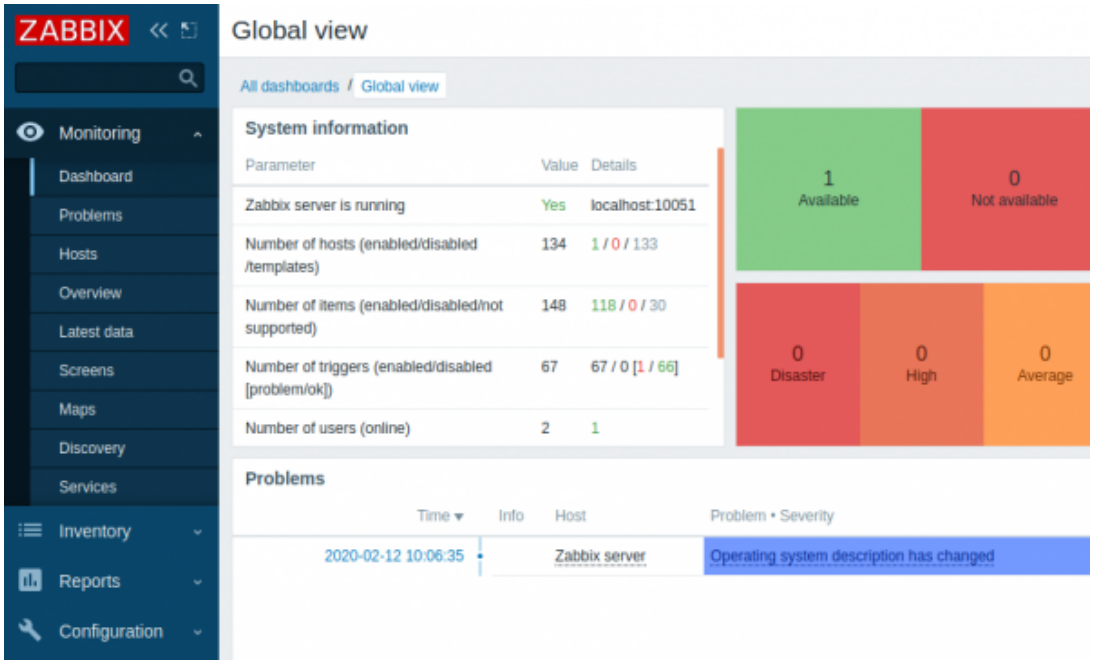

FIGURE 3.4 – Interface Zabbix

(c) **Cacti :** Cacti est un logiciel open source de surveillance du réseau particulièrement apprécié. Il se concentre sur la représentation graphique du réseau. Cacti est disponible en téléchargement gratuit, et il est inclus dans la suite LAMP (Linux, Apache, MySQL, PHP), qui offre une plateforme logicielle standardisée pour la création de graphiques pour tout type de données statistiques. Si un périphérique ou un service renvoie des données numériques, il est fort probable qu'il peut être intégré à Cacti. Il comporte des modèles pour les plateformes de surveillance des applications de serveur, depuis les serveurs Linux et Windows jusqu'aux routeurs et commutateurs Cisco, de manière générale tout ce qui communique avec le protocole SNMP. Bien que la méthode standard de collecte des données Cacti soit le protocole SNMP, les scripts Perl et PHP peuvent également être utilisés. Linterface de cacti est présentée par la figure 3.5

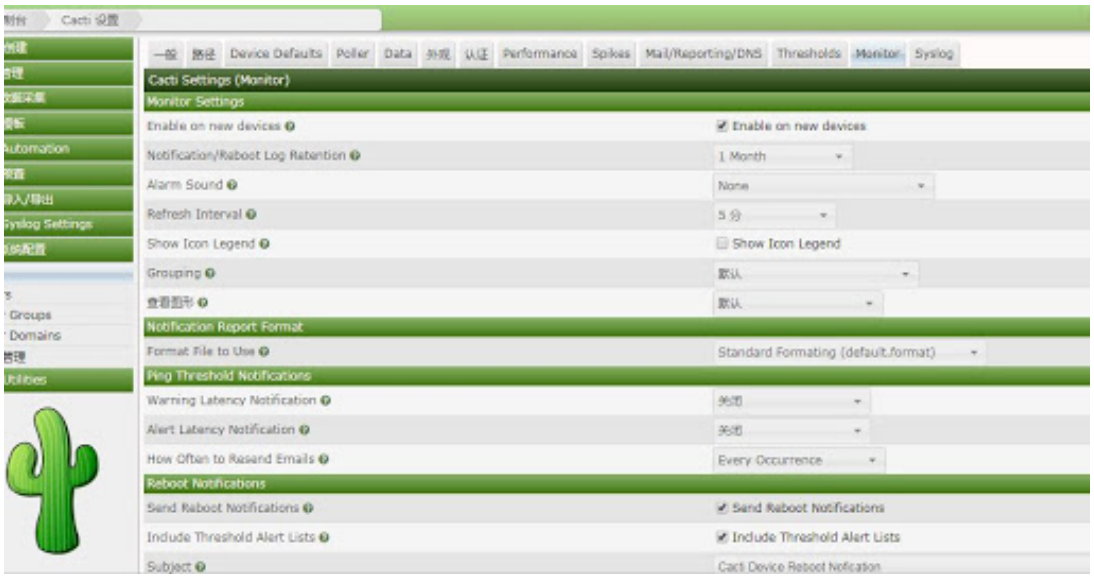

FIGURE 3.5 – Interface Cacti

(d) **Icinga :** Icinga est un autre excellent outil open source de surveillance du réseau. Icinga était à l'origine une branche du système de surveillance Nagios, avant d'être réécrit en 2009 pour devenir une solution autonome appelée Icinga 2. À l'heure actuelle, les deux versions du programme sont activement développées et disponibles. Alors qu'Icinga 1.x est compatible avec un grand nombre de plug-ins et de configurations Nagios, Icinga 2 a été conçu pour être moins fastidieux, plus performant et plus convivial. Il est doté d'une architecture modulaire et d'une conception multi-thread, ce qui n'est pas le cas de Nagios ni d'Icinga 1. Plusieurs variantes de l'interface Web pour Icinga sont proposées. La figure 3.6 montre l'interface de Icinga.[11]

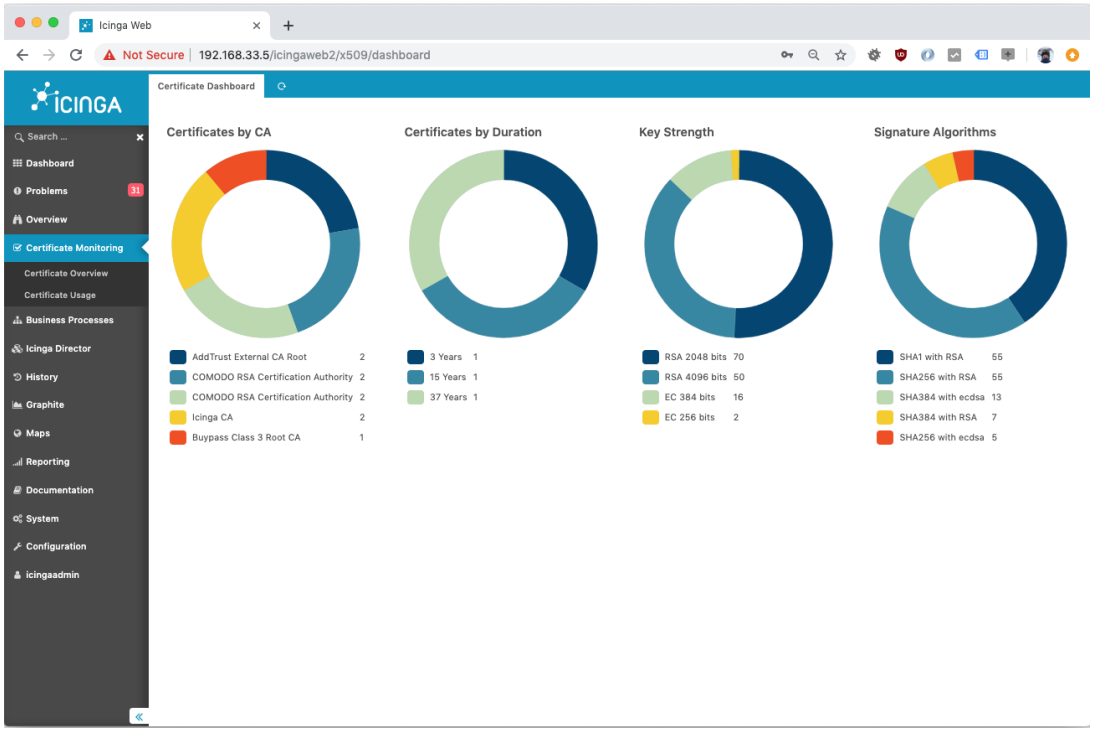

FIGURE 3.6 – Interface Icinga

(e) **Network top (Ntop)** Ntop est un outil de supervision réseau conçu pour l'observation et la résolution de problème d'un réseau. C'est une application open source développée par Luca Deri durant ses études portant sur le réseau à l'université de Pisa (Italie).
La première version de ce logiciel a vu le jour en 1998, la dernière version est la vers. 3.2 datant d'octobre 2005. Ce programme a pour objectif de produire des informations et des graphiques sur le trafic d'un réseau (comme pourrait le faire la commande unix " top" avec les processus).
Ntop n'est pas seulement un analyseur TCP/IP, il s'appuie sur une librairie nommée "libpcap" lui permettant d'être un analyseur hybride couche 2/couche 3.
Il capture et analyse les trames* d'une interface donnée et permet d'observer une majeure partie des caractéristiques du trafic (entrant et sortant) grâce à deux modes de fonctionnement : une interface web et un mode texte. La figure 3.7 montre une interface Ntop. [12]

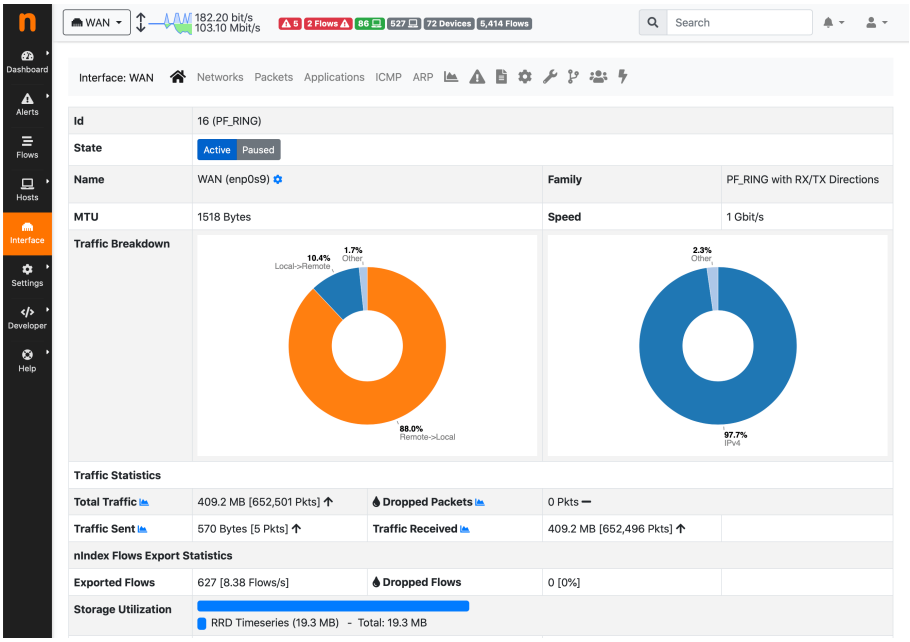

FIGURE 3.7 – Interface Ntop

3.3.2 Choix de l'outil Ntop

Ntop est un outil :

— De pointe de surveillance du réseau doté d'une interface Web rapide et facile à utiliser.

— D'analyse des paquets, il affiche les données en temps réel du trafic réseau, et des informations sur les flux de données hôte et les connexions hôte en temps réel

— Un outils qui propose de bons graphiques et tableaux représentant le trafic réseau actuel et passé,l'historique de transactions spécifiques et de cartes illustrant l'utilisation du réseau en temps réel.

— Modulaire il permet d'accueillir un grand nombre de modules. Ntop comporte une API pour le langage de script Lua, qui peut servir à prendre en charge des extensions.
— stockage de données des hôtes dans des fichiers RRD, pour une collecte permanente des données.

3.4 Trafic réseau

Le trafic réseau ou le trafic de donnée désigne les données qui transitent sur un réseau à un moment donné. Les données réseau sont constituées de paquets, les unités de données essentielles les plus petites qui transitent sur un réseau.
Les données de trafic réseau sont divisées en paquets avant d'être transmises, puis réassemblées une fois arrivées à destination. Les paquets comportent des charges utiles (les données brutes) et des en-têtes (les métadonnées) contenant des informations comme les adresses IP d'origine et de destination. Cette circulation de données se déroule a l'aide de plusieurs protocle de communication (IPV4, ICMP, ARP, DHCP...) qui gère l'acheminement et le contrôle de ces données.

Il existe quatre catégories générales de trafic réseau :

— Trafic dense qui utilise beaucoup de bande passante.
— Trafic en temps différé qui correspond à la bande passante utilisée pendant les heures de travail.
— Trafic interactif qui se dispute la bande passante et ralentit les temps de réponse si aucune priorité n'est établie pour le trafic et les applications.
— Trafic sensible à la latence également susceptible de ralentir les temps de réponse alors qu'il tente de s'accaparer la bande passante.

3.4.1 Types de commutation

La commutation dans un réseau informatique permet de communiquer tous les équipements et matériels informatiques connectés directement avec autres hôtes et transmettre des informations. Il existe quatre grands types de réseaux commutés : les réseaux à commutation de circuits, à commutation de message, les réseaux à commutations de paquets et les réseau à commutation de cellules.

3.4.1.1 Commutation de circuits

La première commutation utilisée dans l'histoire, par exemple dans le réseau téléphonique à l'aide des auto-commutateurs. Elle consiste à créer dans le réseau un circuit particulier entre l'émetteur et le récepteur avant que ceux-ci ne commencent à échanger des informations. Ce circuit sera propre aux deux entités communiquant et il sera libéré lorsque l'un des deux coupera sa communication. Par contre, si pendant un certain temps les deux entités ne s'échangent rien le circuit leur reste quand même attribué. C'est pourquoi, un même circuit (ou portion de circuit)

pourra être attribué à plusieurs communications en même temps. Cela améliore le fonctionnement global du réseau mais pose des problèmes de gestion (files d'attente, mémorisation,...)

3.4.1.2 Commutation de messages

Elle consiste à envoyer un message de l'émetteur jusqu'au récepteur en passant de noeud de commutation en neuud de commutation. Chaque noeud attend d'avoir reçu complètement le message avant de le réexpédier au noeud suivant. Cette technique nécessite de prévoir de grandes zones tampon dans chaque noeud du réseau, mais comme ces zones ne sont pas illimitées il faut aussi prévoir un contrôle de flux des messages pour éviter la saturation du réseau.

3.4.1.3 Commutation de paquets

Elle est apparue au début des années 70 pour résoudre les problèmes d'erreur de la commutation de messages. Un message émis est découpé en paquets et par la suite chaque paquet est commuté à travers le réseau comme dans le cas des messages. Les paquets sont envoyés indépendamment les uns des autres et sur une même liaison on pourra trouver les uns derrière les autres des paquets appartenant à différents messages. Chaque noeud redirige chaque paquet vers la bonne liaison grâce à une table de routage.

3.4.1.4 Commutation de cellules

Une cellule est un paquet particulier dont la taille est toujours fixée à 53 octets (5 octets d'en-tête et 48 octets de données). C'est la technique de base des réseaux hauts débits ATM (Asynchronous Transfert Mode) qui opèrent en mode connecté où avant toute émission de cellules, un chemin virtuel est établi par lequel passeront toutes les cellules. Cette technique mixe donc la commutation de circuits et la commutation de paquets de taille fixe permettant ainsi de simplifier le travail des commutateurs pour atteindre des débits plus élevés. [13]

3.4.2 Débit binaire

Le débit binaire est une mesure utilisée pour déterminer la quantité de données transmises dans un intervalle de temps fixé, mesurée en bits par seconde (bit/s,b/s ou bps). Ses principaux multiples sont :

— Le kilobit par seconde (symbole kbit/s) équivalent à 1000 bit/s.
— Le megabit par seconde (symbole Mbit/s) équivalent à 1000 kbit/s.
— Le gigabit par seconde (symbole Gbit/s) équivalent à 1000 Mbit/s.

Le débit binaire est quelque fois indiqué en bande par abus de langage, lorsque le système de transmission code un bit par symbole transmit.

3.4.3 Bande passante

La bande passante est la limite de la vitesse à laquelle les données peuvent être transférées entre vos serveurs et le web public. La bande passante est mesurée en mégabits par seconde (Mb/s) et parfois en gigabits par seconde (Gb/s). La bande passante typique en hébergement se situe entre 10Mbps et 1 Gb/s, avec 100 Mb/s de bande passante généralement en place pour des serveurs dédiés à haute performance.

3.4.4 Gestion et contrôle de trafic réseau

La gestion et le contrôle sont des techniques qui améliore la circulation d'information sur le réseau et la bande passante.

3.4.4.1 Gestion du trafic réseau

La gestion du trafic consiste à contrôler le partage de la bande passante des liens afin d'assurer la qualité de service des diverses applications. Elle permet de définir la bande passante maximale disponible pour les différents types de trafic et de garantir un minimum de bande passante pour certains flux de trafic.

3.4.4.2 Contrôle de trafic réseau

Le contrôle du trafic réseau est le processus de gestion, de contrôle ou de réduction du trafic réseau, en particulier la bande passante Internet. Il est utilisé par les administrateurs réseau pour réduire la congestion, la latence et la perte de paquets. Cela fait partie de la gestion de la bande passante. Pour utiliser efficacement ces outils, il est nécessaire de mesurer le trafic réseau afin de déterminer les causes de l'encombrement du réseau et résoudre ces problèmes.

3.4.4.3 Contrôle de flux :

Le contrôle de flux implique la mesure des flux de trafic pour une classe, est un ensemble de méthodes utilisées sur un réseau pour éviter les congestions pour observer ce qui se passe pour réguler le trafic puis de libérer les paquets sur le réseau à un débit défini.

3.4.5 Surveillance et analyse de trafic réseau

Les entreprises utilisent une grande variété de systèmes et d'applications sur ces réseaux. L'équipe d'administrateurs réseau doit être capable de fournir un environnement opérationnel, sécurisé, fiable et efficace pour supporter les activités quotidiennes de l'entreprise. Surveiller le

trafic à un ou plusieurs endroits dans le réseau d'un opérateur permet de comptabiliser le trafic, d'identifier des applications qui posent problème, d'identifier la source des problèmes, les corriger et de répartir le trafic sur le réseau.

3.5 Conclusion

Dans ce chapitre on a introduit le monitoring, le trafic réseau, et on a expliqué le choix de l'outil utilisé afin de faire notre réalisation dans le quatrième chapitre.

Chapitre 4

Réalisation

4.1 Introduction

La phase de réalisation consiste à déployer des moyens et des dispositifs visant à sécuriser le système d'information ainsi que de faire appliquer les règles définies dans la politique de sécurité. Dans cette partie nous allons installer Pfsense le configurer, et ensuite installer l'outil de monitoring NTOPNG.

4.2 Pfsense

Le projet pfSense est une distribution de pare-feu réseau gratuite, basée sur le système d'exploitation FreeBSD avec un noyau personnalisé et comprenant des packages de logiciels gratuits tiers pour des fonctionnalités supplémentaires. Le logiciel pfSense, avec l'aide du système de package, est capable de fournir la même fonctionnalité ou plus que les pare-feu commerciaux courants, sans aucune des limitations artificielles. Il a remplacé avec succès tous les grands pare-feu commerciaux dans de nombreuses installations à travers le monde.

Le logiciel pfSense comprend une interface Web pour la configuration de tous les composants inclus. Il n'a besoin d'utiliser la ligne de commande pour quoi que ce soit, et pas besoin de modifier manuellement les ensembles de règles. Les utilisateurs familiarisés avec les pare-feux commerciaux s'approprient rapidement l'interface Web, bien qu'il puisse y avoir une courbe d'apprentissage pour les utilisateurs non familiarisés avec les pare-feux de qualité commerciale. La figure 4.1 montre l'interface Pfsense. [14]

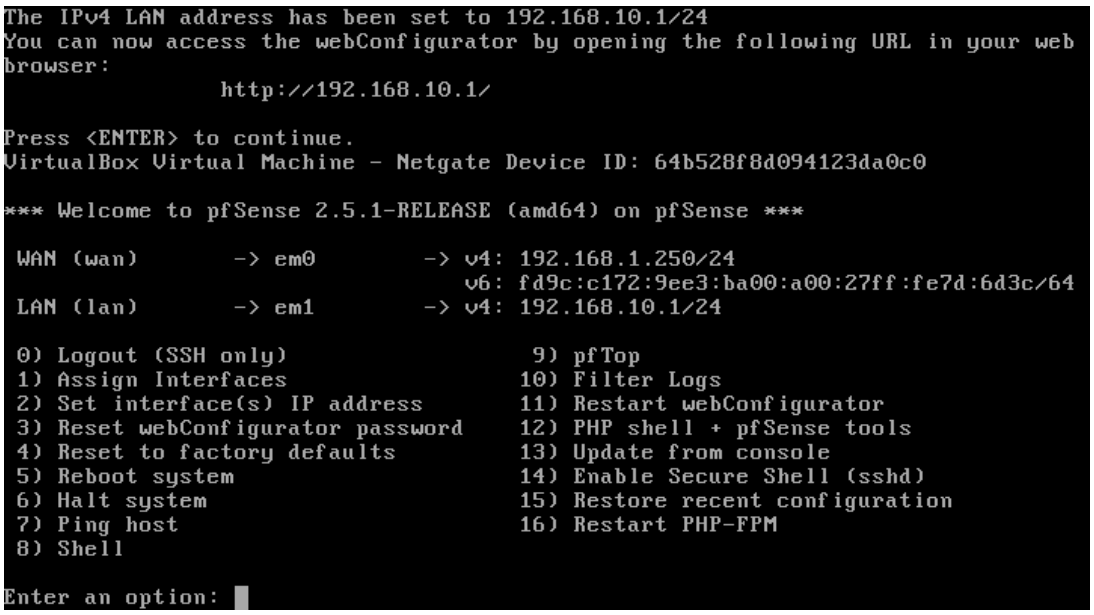

FIGURE 4.1 – Interface Pfsense

4.2.0.1 Fonctionnalité

Pfsense offre plusieurs fonctionnalité tels que :

- Filtrage par IP source et destination, port du protocole, IP source et destination pour le trafic TCP et UDP
- Capable de limiter les connexions simultanées sur une base de règle 36
- Pfsense un utilitaire permettant de filtrer le trafic en fonction du système d'exploitation qui initie la connexion.
- Possibilité d'enregistrer ou de ne pas enregistrer le trafic correspondant à chaque règle.
- Politique très souple de routage possible en sélectionnant une passerelle sur une base par règle (pour l'équilibrage de charge, basculement, Connexions WAN multiple, etc)
- Utilisation d'alias permettant le regroupement et la désignation des adresses IP, des réseaux et des ports, rendant ainsi votre jeu de règles de pare-feu propre et facile à comprendre, surtout dans des environnements avec plusieurs adresses IP publiques et de nombreux serveurs.
- Filtrage transparent au niveau de la Couche 2, le pare-feu est capable d'agir en pont filtrant.
- La normalisation des packets est utilisée, il n'y a donc aucune ambiguïté dans l'interprétation de la destination finale du paquet. Le directif scrub ré-assemble aussi des paquets fragmentés, protège les systèmes d'exploitation de certaines formes d'attaque, et laisse les paquets TCP contenants des combinaisons de Flags invalides.[15]

4.2.0.2 Système des extensions Pfsense (modules ou plugins)

Le système de packages du logiciel pfSense® offre la possibilité d'étendre les fonctionnalités du logiciel sans ajouter de surcharge et de vulnérabilités de sécurité potentielles à la distribution de base.

Certains packages ont été écrits par la communauté pfSense, et d'autres directement développés par Netgate. Les packages disponibles varient considérablement et certains sont plus matures et bien entretenus que d'autres. Il existe des packages qui installent et fournissent une interface graphique pour les logiciels tiers, tels que Squid, et d'autres qui étendent les fonctionnalités du logiciel pfSense, comme le package OpenVPN Client Export Utility qui crée automatiquement des fichiers de configuration OpenVPN.[16]

Exemples de packages disponibles :

- Fonctionnalité de filtrage supplémentaire (pfBlockerNG)
- Logiciel IDS/IPS (Snort et Suricata)
- Des moniteurs de bande passante qui affichent le trafic par adresse IP, comme ntopng et Darkstat.
- Services supplémentaires tels que FreeRADIUS et BIND.
- Proxy client Web (Squid) et filtrage proxy (SquidGuard).
- Proxy inverse pour HTTP et HTTPS tels que HAProxy.
- Proxy pour d'autres services tels que SIP et FTP.
- Utilitaires système tels que NUT pour la surveillance d'un onduleur.
- Utilitaires tiers populaires tels que nmap, iperf et arping.
- Routage BGP, routage OSPF, édition Cron, agent Zabbix et bien d'autres.
- Fonctionnalités qui étaient auparavant dans le système de base mais ont été déplacées vers des packages, tels que RIP (routé).

4.2.1 Free Brekeley Software Distribution ou FreeBSD

FreeBSD est un système d'exploitation de type Unix librement disponible, largement utilisé par des fournisseurs d'accès à Internet, dans des solutions tout en un et des systèmes embarqués et partout où la fiabilité par rapport à un matériel informatique est primordiale. FreeBSD est plus célèbre pour sa force en tant que serveur internet et il est un excellent choix comme plate forme sous jacente pour n'importe quel service réseau. La figure 4.2 montre le système FreeBSD.[17]

FIGURE 4.2 – FreeBSD

4.3 Ntopng

Ntopng est la version de nouvelle génération du ntop original , une sonde de trafic réseau qui surveille l'utilisation du réseau. NTOPNG est basé sur libpcap ,PF-RING et il a été écrit de manière portable afin de fonctionner virtuellement sur toutes les plates-formes Unix, MacOS et Windows également.

Ntopng fournit une interface utilisateur Web intuitive et cryptée pour l'exploration des informations de trafic en temps réel et historiques.[18]
La figure 4.3 illustre l'interface Ntopng.

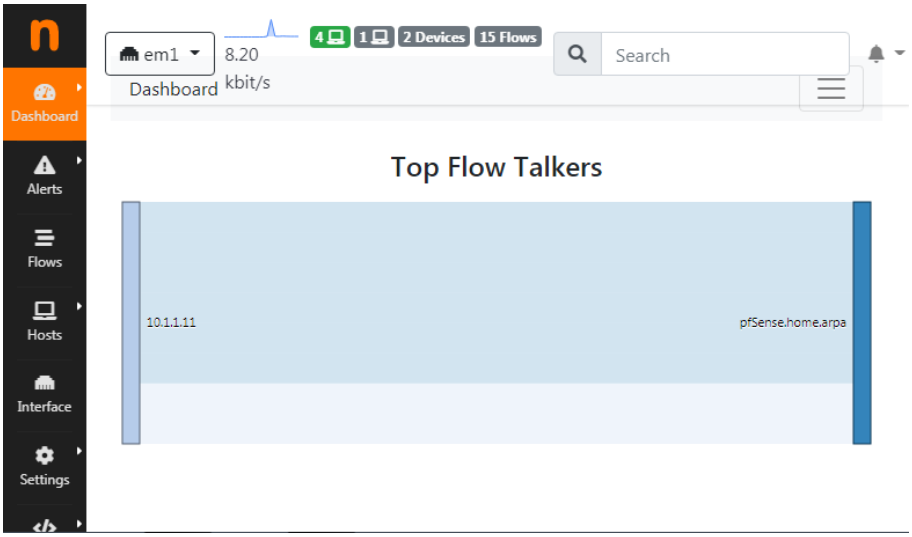

FIGURE 4.3 – Interface Ntopng

4.3.0.1 Caractéristiques principales

NTOPNG est caractérisé par :

- Trier le trafic réseau en fonction de nombreux critères, notamment l'adresse IP, le port, les protocoles d'application de couche 7 (L7), le débit, les systèmes autonomes (AS).
- Afficher le trafic réseau en temps réel et les hôtes actifs.
- Produire des rapports à long terme pour plusieurs métriques de réseau, y compris le débit et les protocoles d'application L7
- Top locuteurs (expéditeurs/récepteurs), meilleurs AS, meilleurs protocoles d'application L7
- Surveiller et rapporter le débit en direct, les latences du réseau et des applications, le temps d'aller-retour (RTT), les statistiques TCP (retransmissions, paquets en panne, paquets perdus) et les octets et paquets transmis
- Stocker sur le disque des statistiques de trafic persistantes pour permettre de futures explorations et analyses post-mortem
- Géolocaliser et superposer les hôtes dans une carte géographique
- Découvrir les protocoles d'application de couche 7 (Facebook, YouTube, BitTorrent, etc.) en tirant parti de la technologie nDPI , ntop Deep Packet Inspection (DPI)
- Analyser le trafic IP et le trier selon la source/destination

4.4 Présentation du projet

Afin de sécuriser un réseau d'entreprise, on a choisi parmi plusieurs logiciels pfsense par rapport à sa performance, sa fiabilité et sa simplicité. On a pu constater cette différenciation durant le stage au sein de RAMDY qui ma permet d'accueillir des connaissances pour configurer ce logiciel et de réaliser ce projet. Premièrement nous avons installé virtualbox afin de créer quatre machines

virtuelle qui ont des systèmes différents, puis deuxièmement on va installé Pfsense et Ntopng, les outils choisi pour réaliser le travaille.

4.4.1 VirtualBOX

VirtualBox est un virtualiseur complet à usage général pour le matériel x86, destiné aux serveurs, aux postes de travail et à l'utilisation intégrée.Un puissant produit pour les entreprises et les particuliers. VirtualBox est non seulement un produit hautement performant et extrêmement riche en fonctionnalités pour les entreprises clientes, mais c'est aussi la seule solution professionnelle disponible gratuitement en tant que logiciel Open Source sous les termes de la GNU General Public License (GPL) version 2.[19] La figure 4.4 montre la page d'accueil de virtualBox.

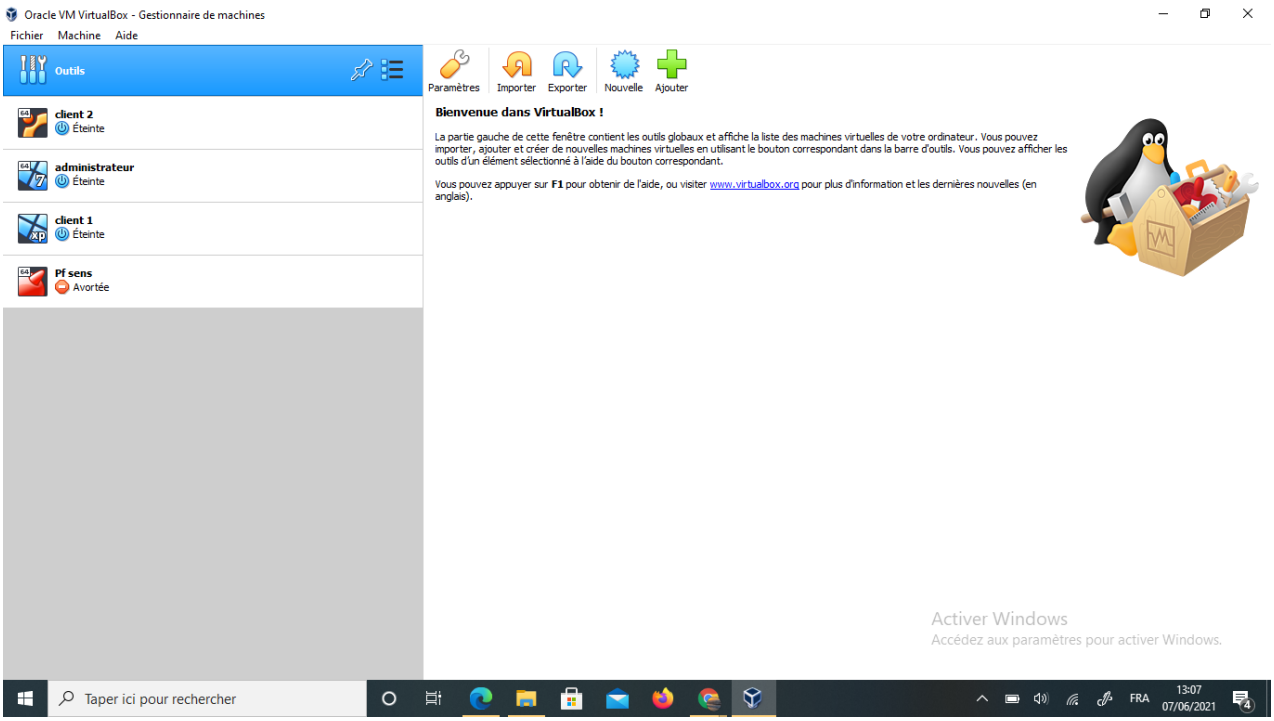

FIGURE 4.4 – page d'accueil de Virtualbox

4.5 Préparation de l'environnement de travail

Vu l'importance des informations et des services fournis par les serveurs de RAMDY, nous allons travailler dans un environnement virtuel avec VirtualBox. Nous allons créer quatre (04) machines virtuelles qui sont :

1. **Pfsense :** C'est sur cette machine que nous allons installer Pfsense. Ses caractéristiques sont les suivantes :

   · Mémoire RAM : 1024 MB ;

· Nombre de processeurs : 2 ;

· Nombre de cartes réseaux : 2 (1 pour servir de passerelle par défaut d'un réseau et l'autre pour fournir l'Internet) ;

· Système d'exploitation : FreeBSD. La figure 4.3 montre la page d'accueil Pfsense sur le système FreeBSD

2. **Administrateur :** Cette machine sera utilisé pour installé et configurer PFsense et NTOPNG. Ses caractéristiques sont les suivantes :

   · Mémoire RAM : 1024 MO ;

   · Nombre de processeurs : 2 ;

   · Nombre de cartes réseaux : 2 (utilisées pour se connecter au réseau) ;

   · Système d'exploitation : Windows 7

3. **Client 1 :** Cette machine sera utilisée pour simuler un utilisateur normal dans le réseau interne disposant des paramètres de connexions. Ses caractéristiques sont les suivantes :

   · Mémoire RAM : 1024 MO ;

   · Nombre de processeurs : 2 ;

   · Nombre de cartes réseaux : 2 (utilisées pour se connecter au réseau) ;

   · Système d'exploitation : Windows XP

4. **Client 2 :** Cette machine sera également configurée comme un second utilisateur normal dans le réseau interne .Ses caractéristiques sont les suivantes :

   · Mémoire RAM : 1Go ;

   · Nombre de processeurs : 1 ;

   · Nombre de cartes réseaux : 2 (utilisées pour se connecter au réseau) ;

   · Système d'exploitation : Ubuntu

4.5.1 Installation du Pfsense

Il est possible de mettre en place d'autres solutions pour réaliser un proxy, comme :Windows. Le choix de Pfsense est simple, c'est un OS ayant une interface graphique, simple d'utilisation et permettant l'installation rapide et efficace de service.

Dans cette partie,après avoir fais les configurations sur VirtuelBox, nous allons lancer l'image IOS de Pfsense téléchargé et l'installé.

Configuration de Pfsense sur VirtualBox

1. On attribue un nom a notre machine, le type et une version, ce que la figure 4.5 montre.
   (a) **Nom :** Pfsense.
   (b) **Dossier de la machine :**D.
   (c) **Type :**BSD.

(d) **Version :**FreeBSD(64bit).

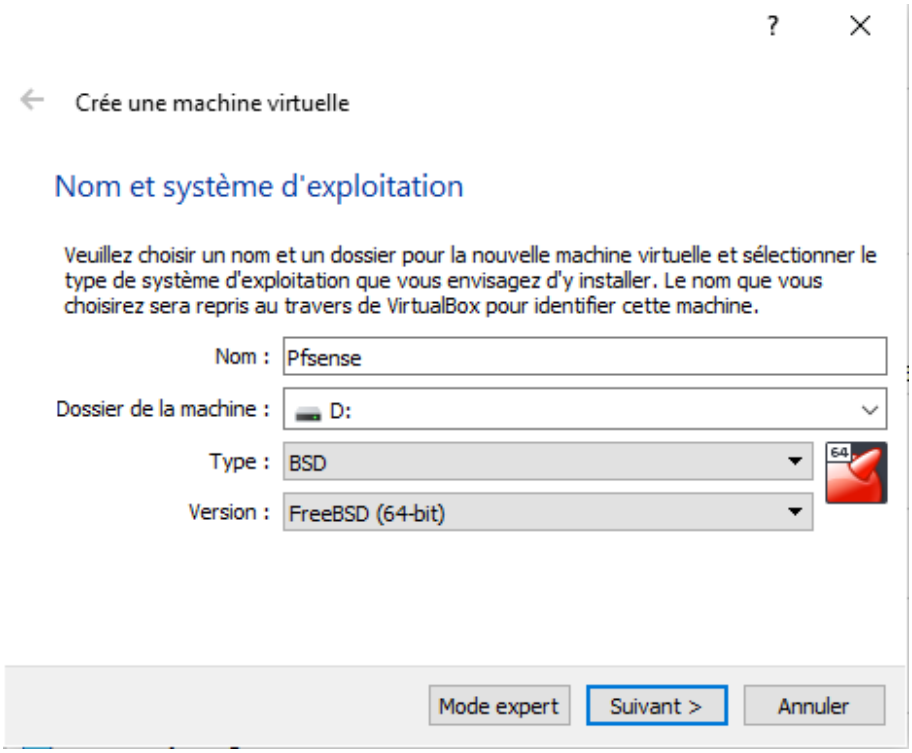

FIGURE 4.5 – Nom de la machine Pfsense

2. On réserve une taille mémoire (1024 MB) ce que montre la figure 4.6

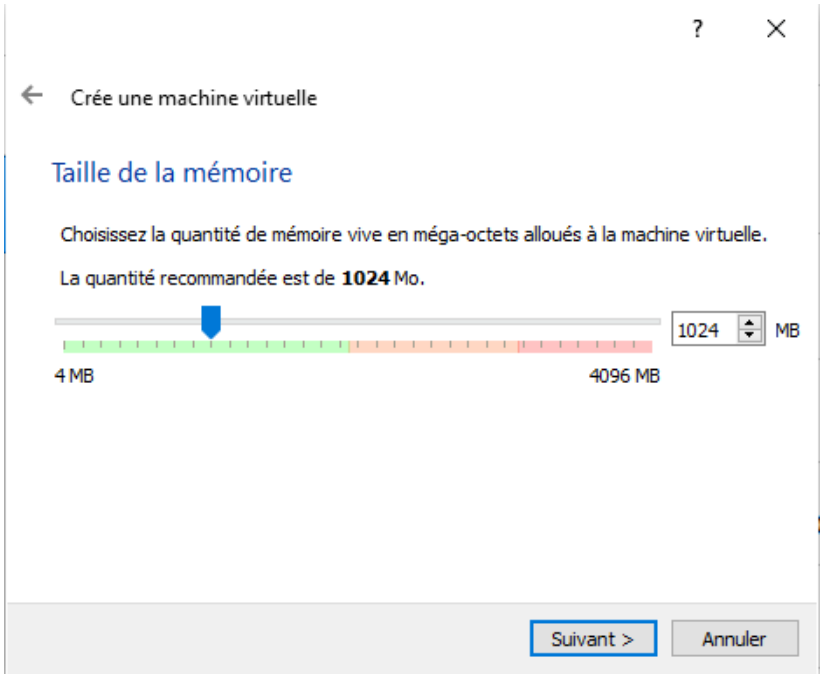

FIGURE 4.6 – Réservation de la taille mémoire

3. Configurer la première carte réseau pour avoir accès au WLAN comme suit :
   (a) **Mode d'accèe réseau :** Accès par port.
   (b) **Nom :**Intel(R)Dual Wireless

   La figure 4.7 montre la configuration de la première carte réseau.

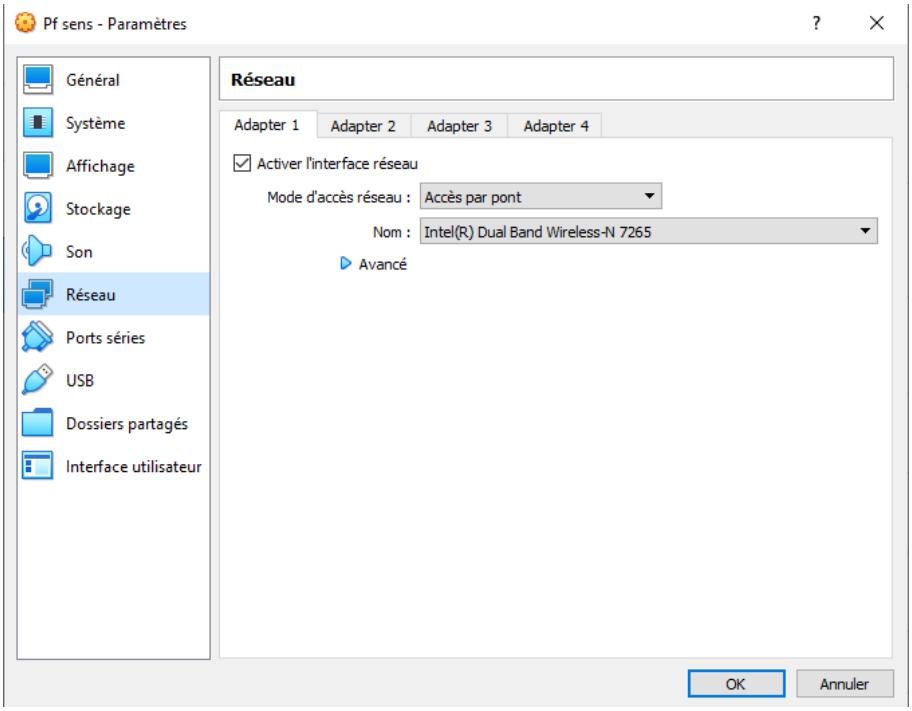

FIGURE 4.7 – Configuration de la carte réseau 1

4. Configurer la deuxième carte réseau pour avoir accès au LAN comme suit :
   (a) **Mode d'accèe réseau :** Réseau interne.
   (b) **Nom :**intnet

   La figure 4.8 montre la configuration de la deuxième carte réseau.

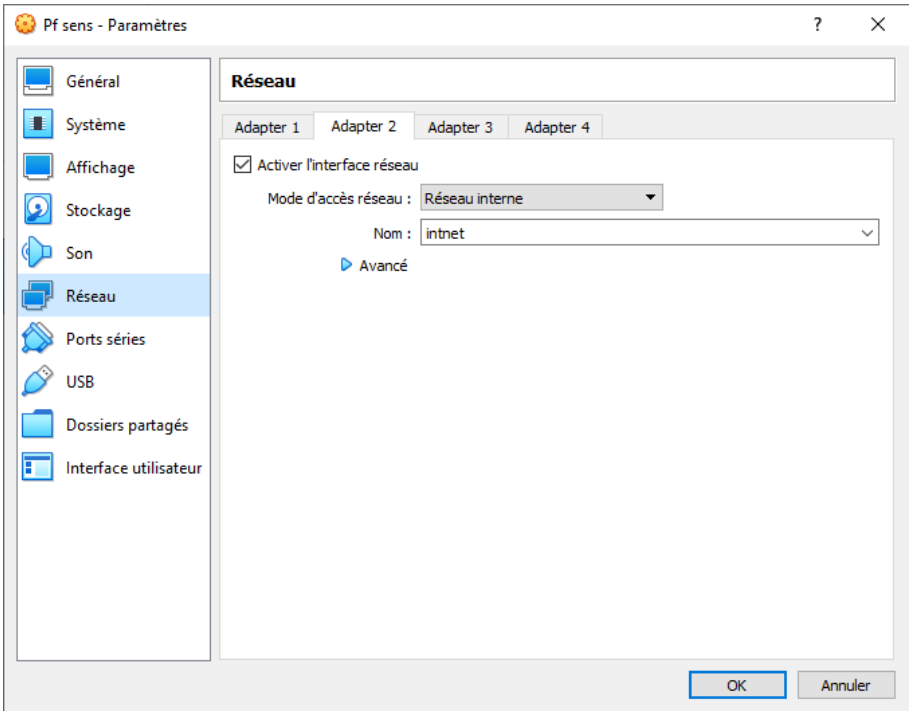

FIGURE 4.8 – Configuration de la carte réseau 2

Lancement de l'image de Pfsense :

Après la configuration de Pfsense sur VirtualBox, on va lancer l'image de Pfsense télécharger. Comme le montre la figure 4.9

FIGURE 4.9 – L'écran de bienvenu Pfsense

Puis une boite de dialogue sera afficher pour choisir l'installation du Pfsense, comme le montre la figure 4.10.

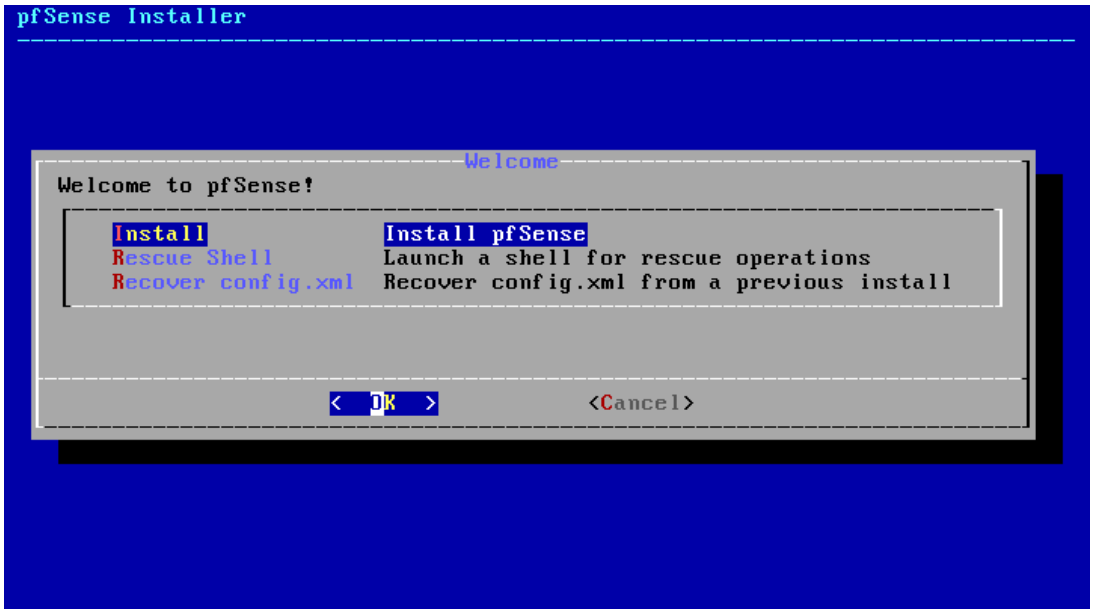

FIGURE 4.10 – Installation

En suite, une autre boite dialogue s'affiche pour choisir la partition de disque. Voir la figure 4.11.

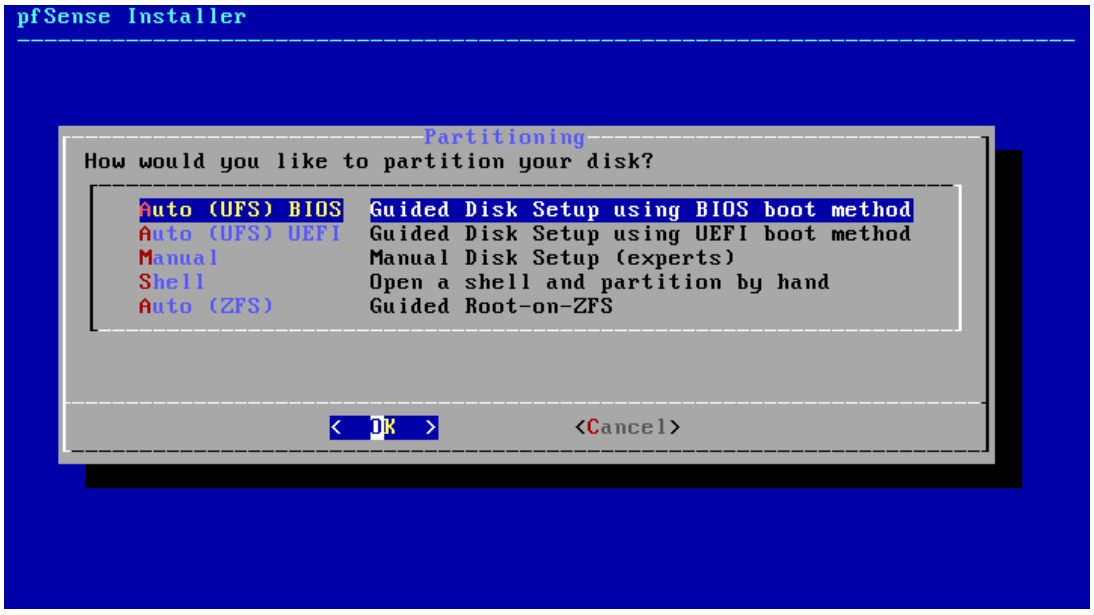

FIGURE 4.11 – Choix de la partition

Après le redémarrage, la console Pfsense :

1. Demandera si on doit configurer des VLAN.
2. Le système essaiera de détecter la liste des interfaces réseau disponibles.
3. Le système demandera de choisir une interface comme interface externe [WAN]. Dans notre exemple, nous avons configuré l'interface em0 en externe.
4. Le système demandera de choisir une interface comme interface interne [LAN]. Dans notre exemple, nous avons configuré l'interface em1 en interne.

la figure 4.12 montre que l'installation a été bien réalisée.

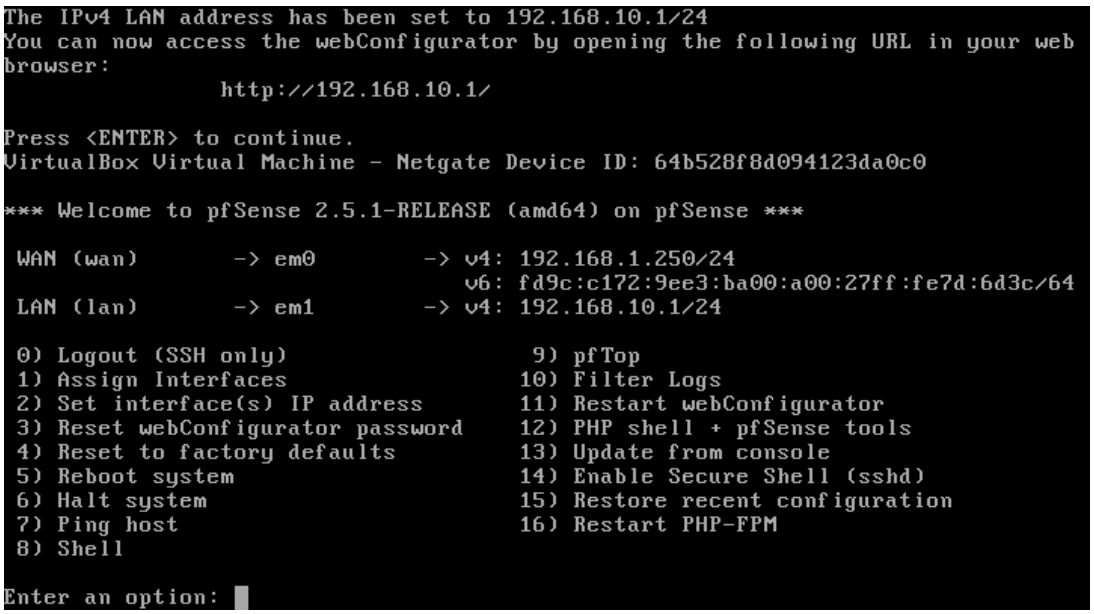

FIGURE 4.12 – Interface par défaut

La figure 4.13 montre la configuration de LAN.

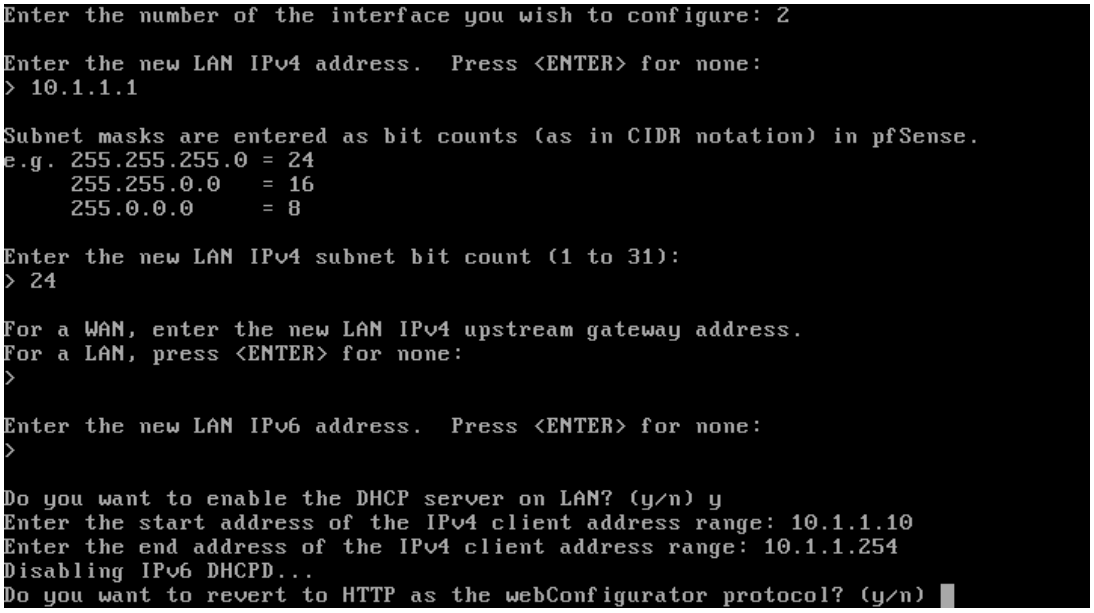

FIGURE 4.13 – Configurer réseau LAN

La figure 4.14 nous montre l'interface de connexion.

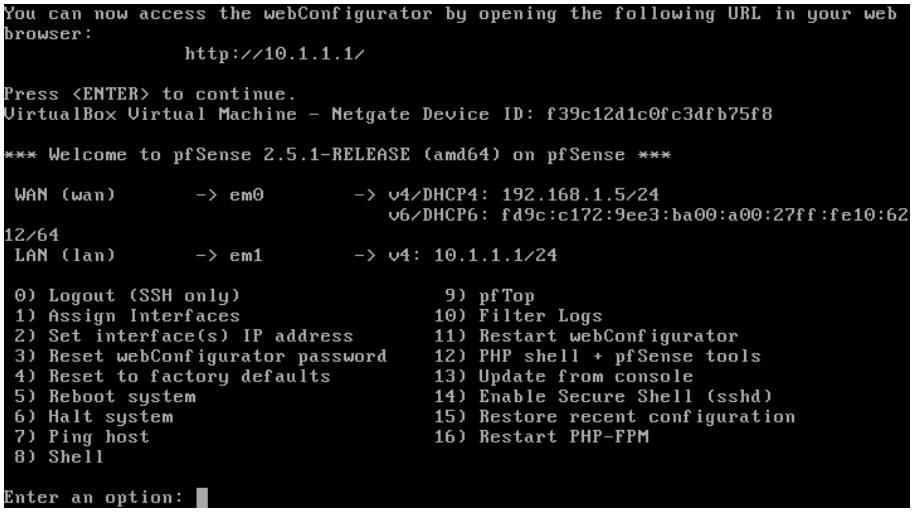

FIGURE 4.14 – Interface de connexion

4.5.1.1 Connexion au tableau de bord Pfsense :

Une fois la configuration du réseau local (LAN) est terminée, on garde Pfsense allumé et on accède à l'interface Web. La figure 4.15 montre que notre connexion LAN est bien configurée. Pfsense connecté sur l'adresse 10.1.1.11.

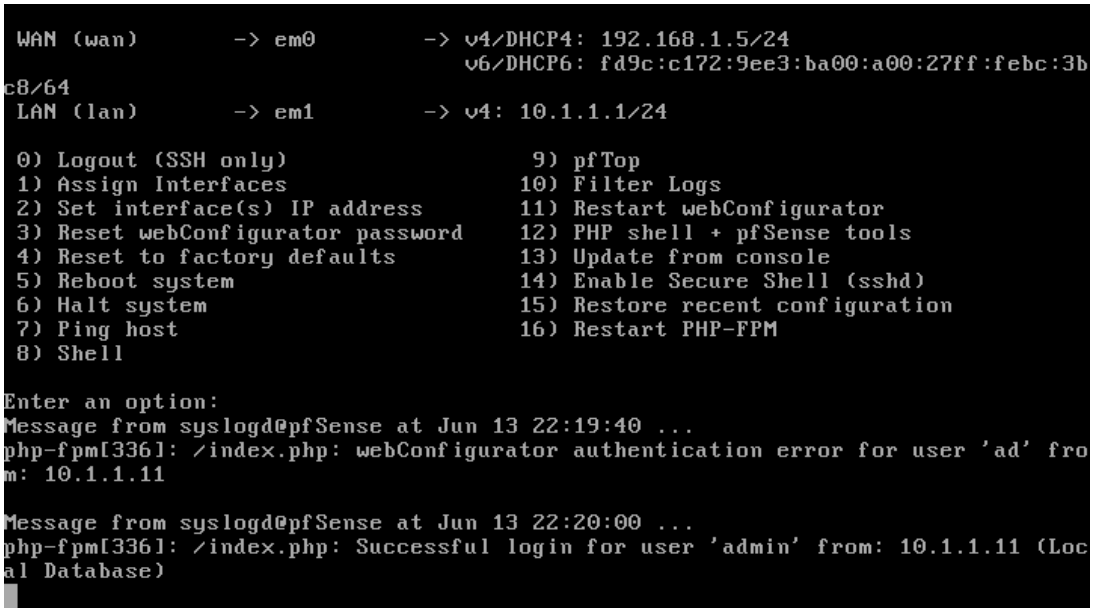

FIGURE 4.15 – PFsense connecté

Ouvrir un logiciel de navigation, écrire l'adresse IP de notre pare-feu Pfsense et accéder à l'interface Web. L'URL suivante a été entrée dans le navigateur :
https ://10.1.1.1.
La figure 4.16 illustre la page d'accueil de Pfsense sur le navigateur.

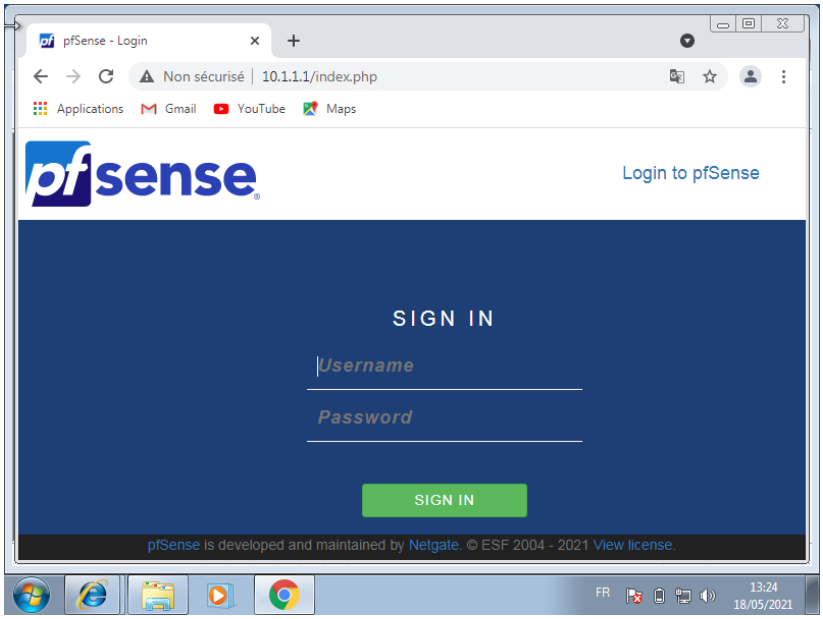

FIGURE 4.16 – Portail de connexion PFsense

Sur l'écran d'invité, on entre les informations de connexion du mot de passe par défaut Pfsense.

- Nom d'utilisateur : admin
- Mot de passe : pfsense

Après une connexion réussie, on sera envoyé au tableau de bord Pfsense. Comme le montre la figure 4.17.

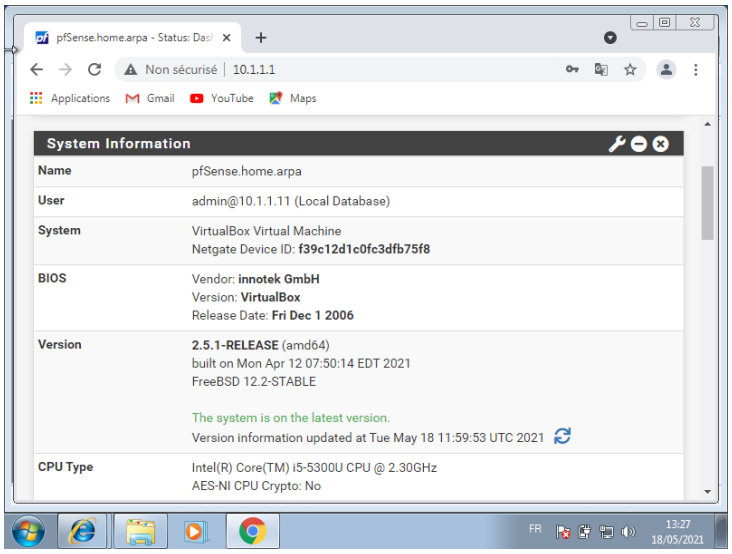

FIGURE 4.17 – Système d'information Pfsense

4.5.2 Installation de NTOPNG :

Pour installer Ntopng, on accède a la page d'accueil Pfsense, puis dans l'onglet **System >Package Manager>Available Package Ntopng** on installe ntopng. comme le montre La figure 4.18 et la figure 4.19.

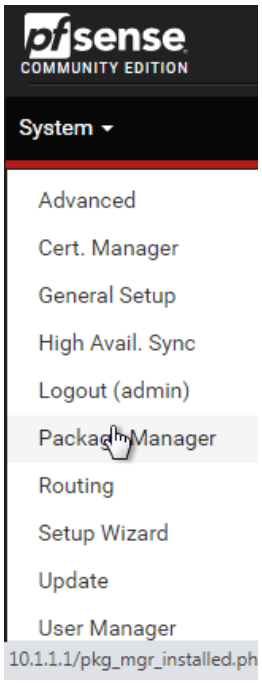

FIGURE 4.18 – Package manager

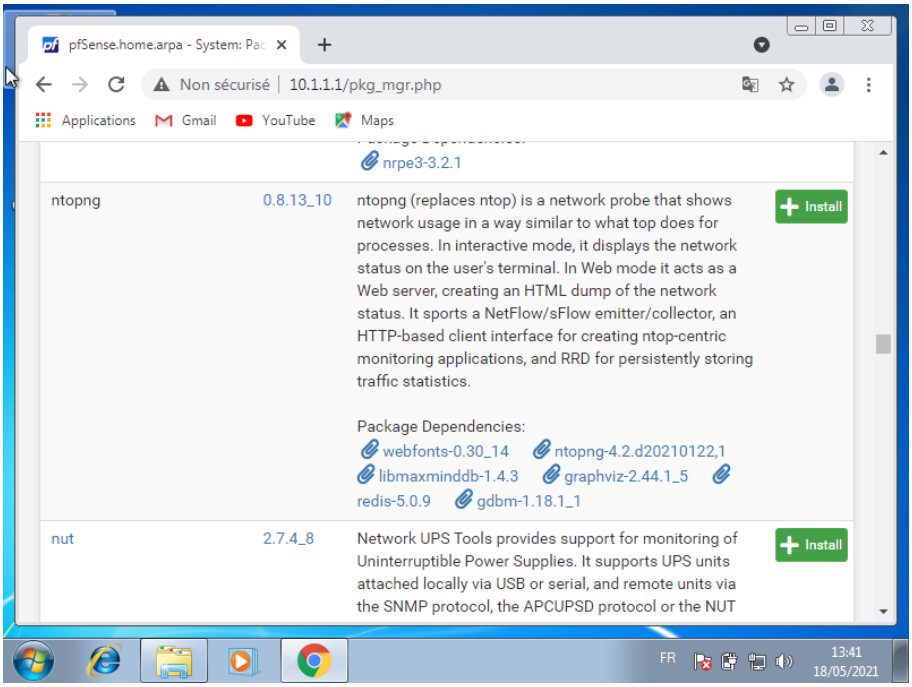

FIGURE 4.19 – Extension NTOPNG

4.5.3 Configuration de NTOPNG :

Une fois l'installation est terminée, on se rend dans l'onglet **Diagnostics>Ntopng Settings** pour initialiser Ntopng et lancer le service correspondant, comme l'indique la figure 4.20.

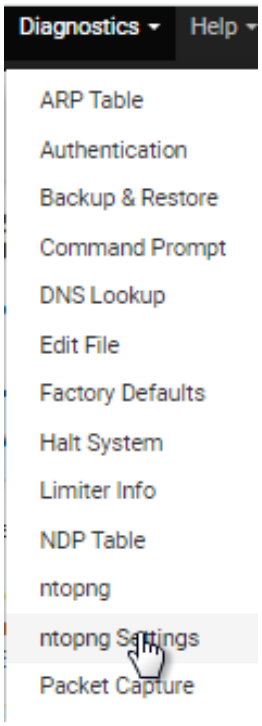

FIGURE 4.20 – Ntopng settings

Les paramètres disponibles ici sont moindres, et permettent seulement de configurer le mot de passe administrateur pour accéder à la configuration avancée de Ntopng, ainsi qu'à l'interface d'écoute. Voir les figures 4.21 et la figure 4.22 montre plus de détaille.

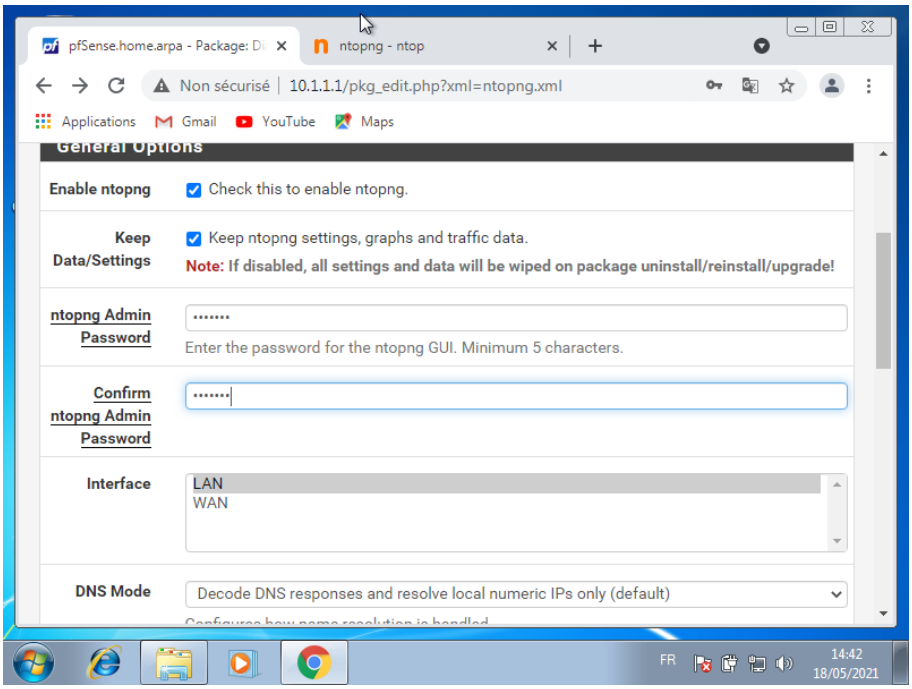

FIGURE 4.21 – Générale option(ntopng)

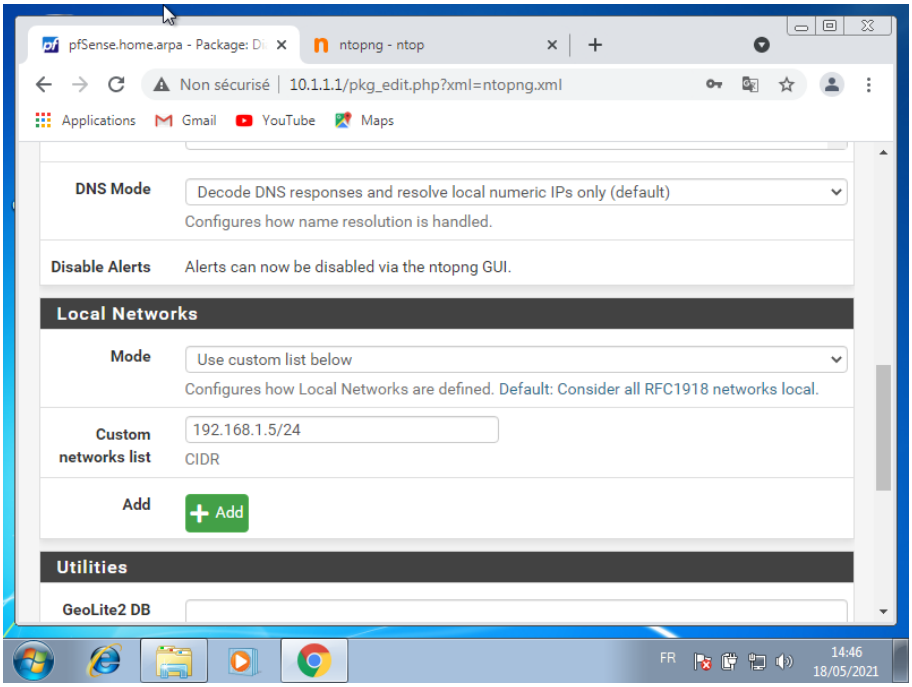

FIGURE 4.22 – Réseau local NTOPNG

4.5.3.1 Connexion au tableau de bord NTOPNG :

Une fois la configuration est terminée sur l'onglet **Diagnostics>Ntopng**, nous envoi sur une fenêtre dans l'URL suivante a été entrée dans le navigateur : https ://10.1.1.1 :3000 La figure 4.23 montre le portail d'accueil Ntopng.

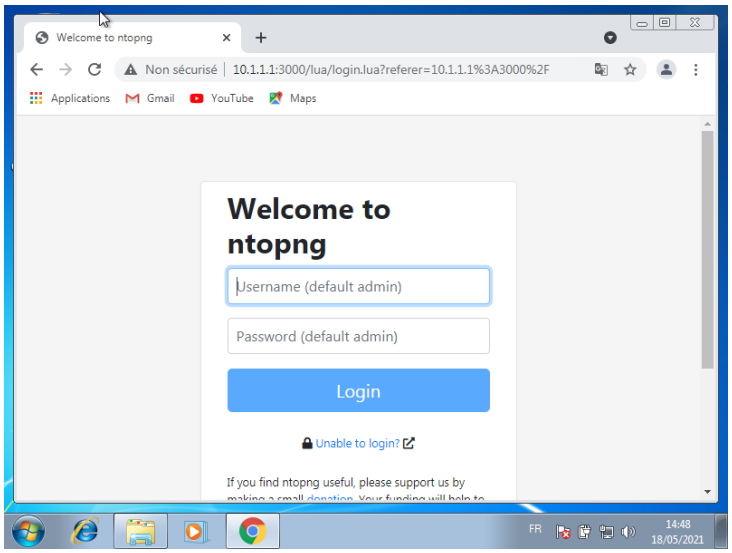

FIGURE 4.23 – Portail d'accueil NTOPNG

Sur l'écran d'invité, on fais entré les informations de connexion du mot de passe par défaut admin ou les donnés entré dans la configuration avancée.

- Nom d'utilisateur : admin
- Mot de passe : admin

Une fois authentifié et connecté à Ntopng, on sera envoyer au tableau de bord.

4.5.3.2 Fonctionnement de Ntopng :

Ntopng propose plusieurs fonctionnalité de monitoring :

(a) **Système de surveillance :** Ntopng permet au moniteur d'avoir des détails de chacun des hôtes connecté au réseau surveillé les figures suivantes donne exemple :
La figure 4.24 montre un exemple sur un simple réseau.

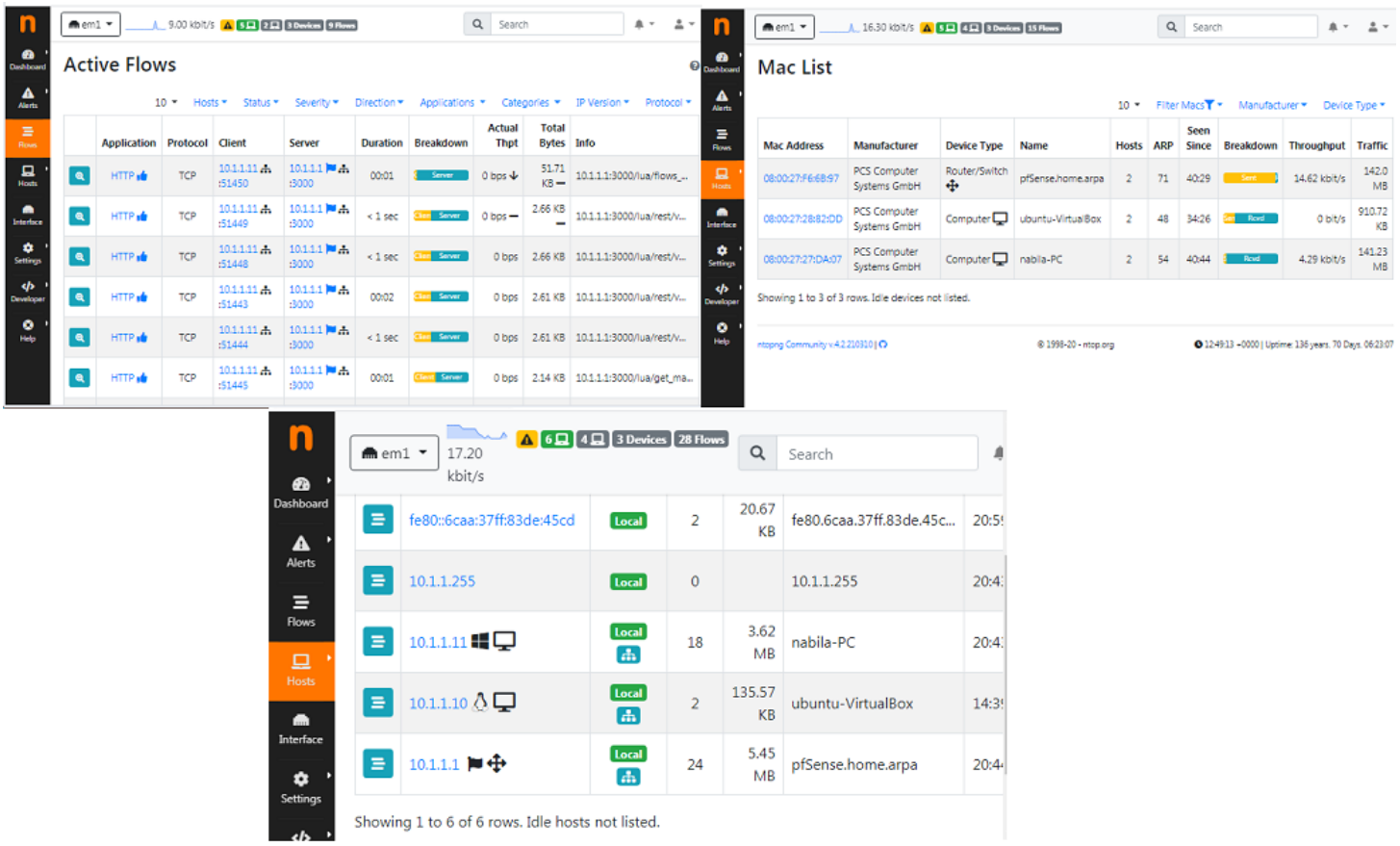

FIGURE 4.24 – Exemple sur le réseau installé

La figure4.25 montre un exemple sur le système de surveillance du réseau de SARL RAMDY.

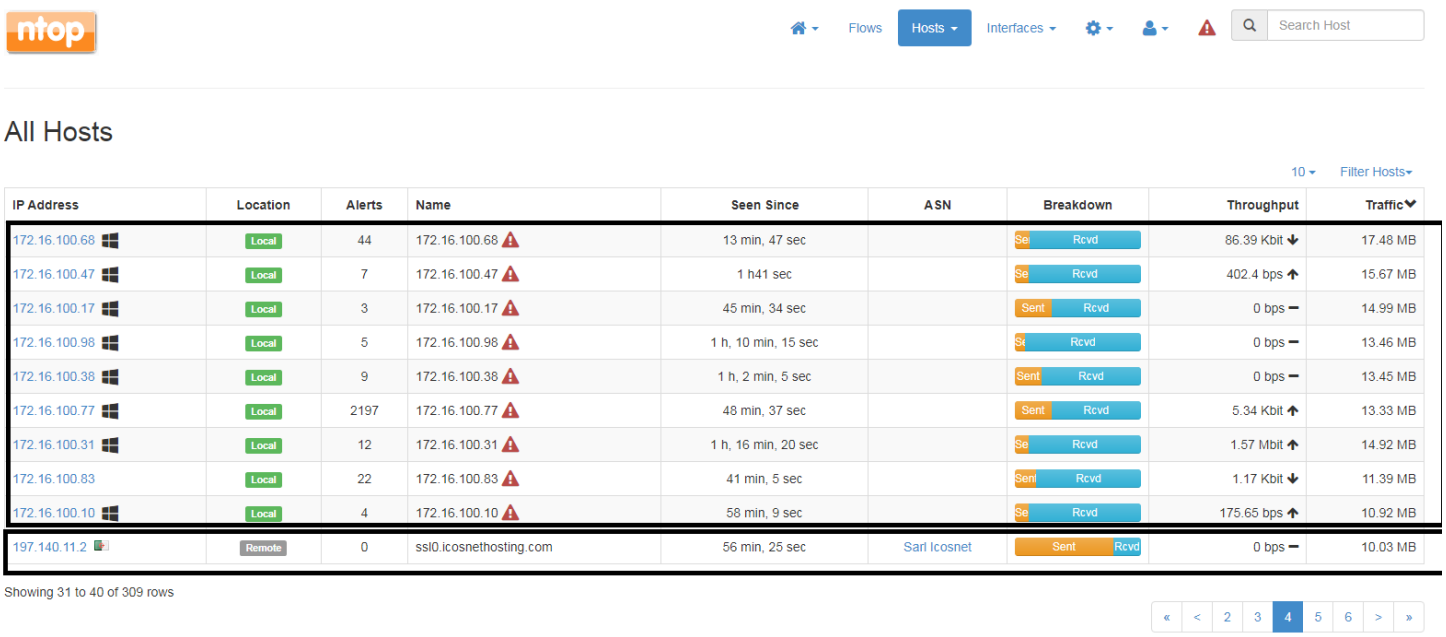

FIGURE 4.25 – Exemple sur le réseau RAMDY

(b) **Système d'analyse :** Ntopng permet d'analysé le trafic et de donner le débit consommé du réseau sous plusieurs formes de diagrammes.

i. **Analyse :**

La figure 4.26 illustre un diagramme circulaire par pont.

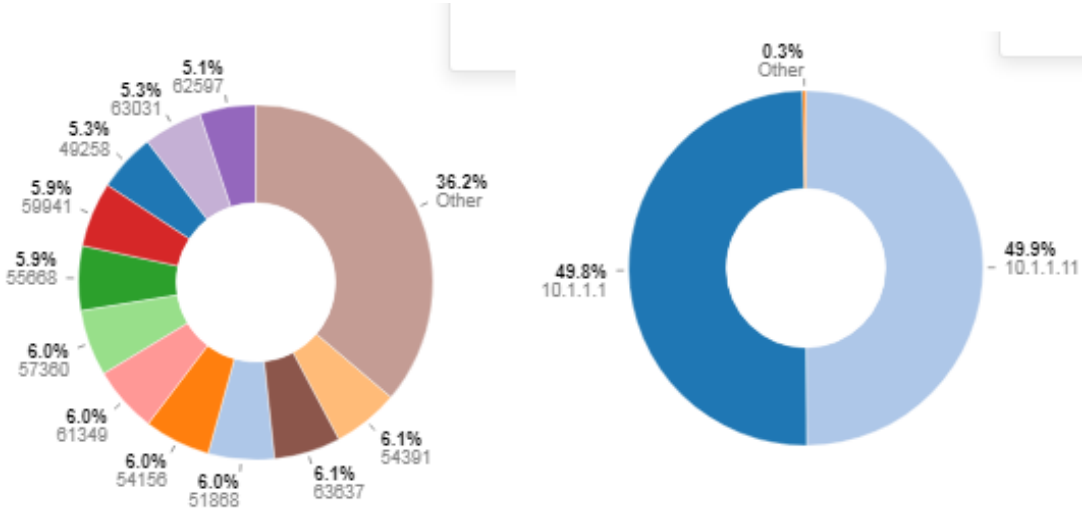

FIGURE 4.26 – Diagramme circulaire par port

Ntopng illustre les paquets envoyer et reçu sous forme de diagramme circulaire afin de montré en détaille la consommation de débit. la figure 4.27 illustre un diagramme circulaire de consommation de débit.

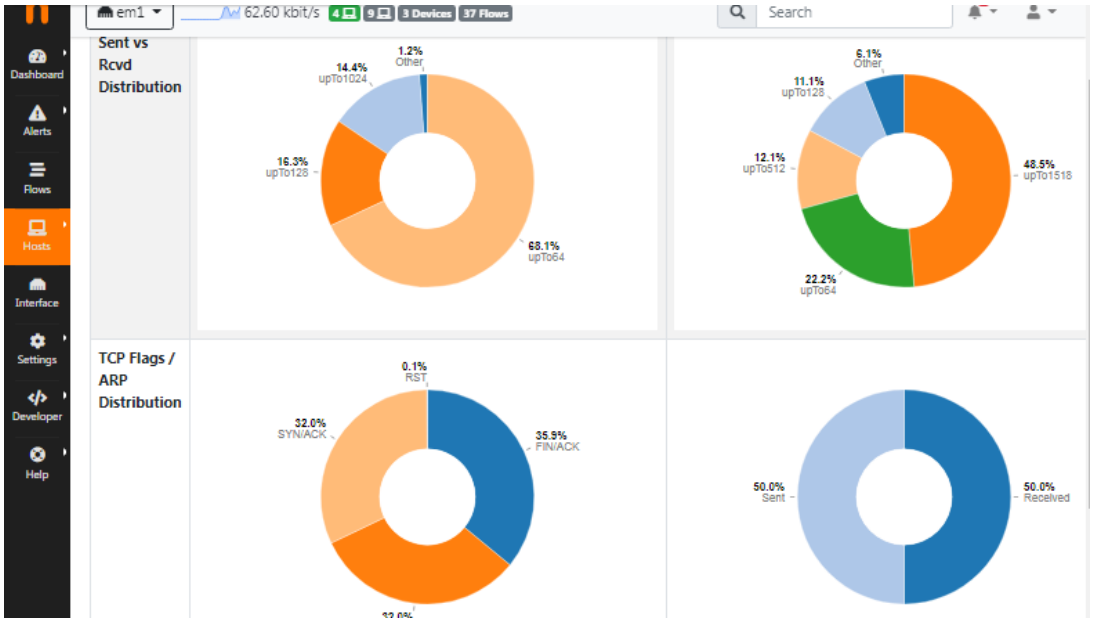

FIGURE 4.27 – Diagramme circulaire de paquet envoyer et reçu sur le réseau

ii. **Consommation de débit :** Ntopng nous permet de voir comment le débit est consommé en le schématisant sous forme d'un diagramme. La figure 4.28 illustre le diagramme.

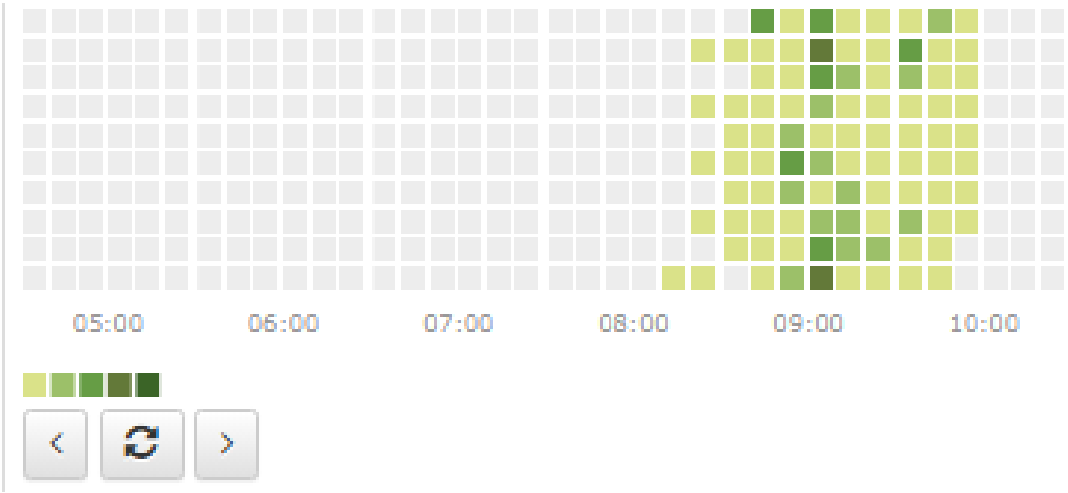

FIGURE 4.28 – Diagramme de consommation de débit par heur d'un utilisateur

(c) **Système d'alerte :** Les alertes ntopng sont :

— Évalué avec des vérifications pour les pools d'hôtes, d'interfaces, de périphériques SNMP et d'autres éléments de réseau.

— Livré aux destinataires à l'aide de critères basés sur le type ou la gravité.

La figure 4.29 illustre les alertes signalées sur l'interface Ntopng.

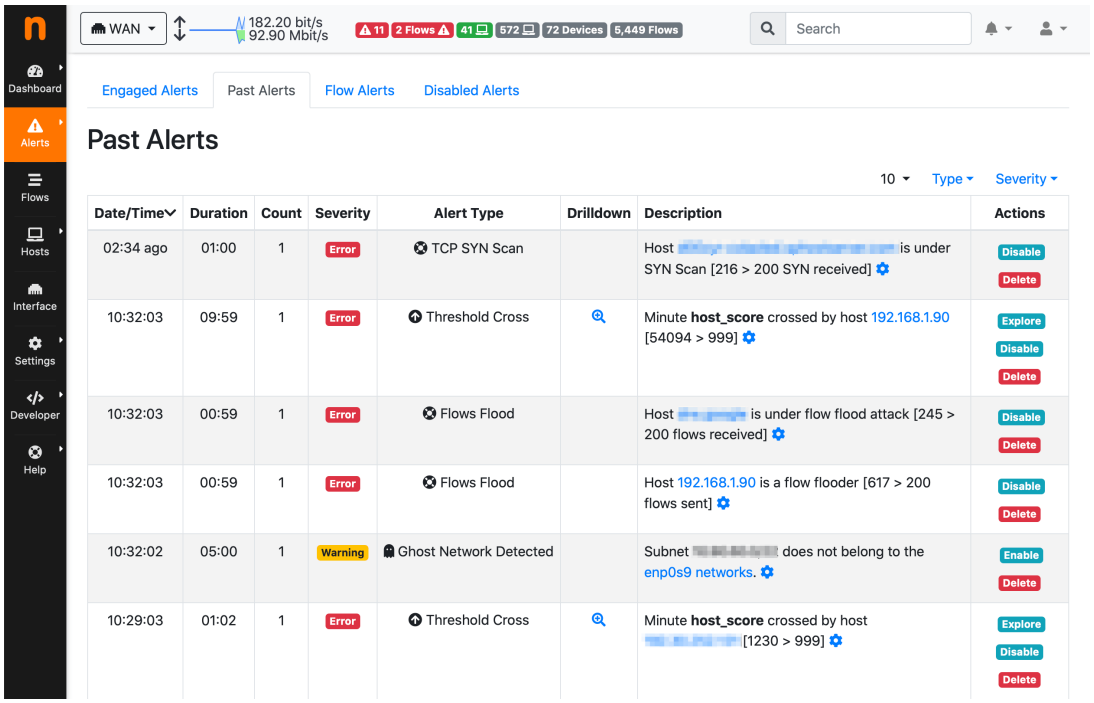

FIGURE 4.29 – Alerte

4.6 Conclusion :

A travers ce chapitre, nous avons pu expliquer notre environnement de travail et présenté les outils utilisés, afin de protéger et surveiller le réseau local de SARL RAMDY.

Conclusion générale

Pare-feu open source ou Pfsense est une technologie qui offre des services efficaces pour les réseaux locaux, et pour toutes les entreprises qui veulent être compétitive et moderne, cette technologie est plus souple et ne nécessite pas un investissement lourd et elle est beaucoup moins couteuse. Elle propose aussi de nouveaux services et beaucoup d'autres avantages. Elle vise principalement à faciliter les tâches de l'administrateur réseau pour la sécurisation, surveillance, l'analyse et d'autres tâches. Les services offerts par pfsense se développent à une vitesse fulgurante.Elle parait comme une bonne solution en matière de filtrage, de routage, de sécurité réseau, la raison pour laquelle plusieurs entreprises dans leurs stratégies de sécurisation des surveillances au niveau de son réseau local proposent de mettre en oeuvre le serveur pfsense.

L'objectif de mon projet est sécurisé et monitoring du réseau local de SARL RAMDY. Et pour cela on a défini quelques généralité sur les réseaux et la sécurité informatique, puis présenté l'organisme d'accueil SARL RAMDY, ensuite le monitoring et le trafic réseau et enfin la réalisation qui consiste a installer Pfsense, le configurer sur la machine virtuelle et installer l'outils de monitoring Ntopng sur Pfsense et le configurer.

Ce travail ma permis d'améliorer mes connaissances dans l'administration et la sécurité des réseaux dans le monde professionnel, notamment le pare-feu open source ou pfsense.

Liste des abréviations

PAN : Personnal Area Network.
LAN : Local Area Network.
MAN : Metropolitaine Area Network.
WAN : Wide Area Network.
WLAN : Wireless Local Area Network.
SAN : Storage Area Network.
WiFi : Wireless Fidelity.
ISO : International Organization for Standardization.
OSI : Open Systems Interconnection.
TCP/IP : Transmission Control Protocol/ Internet Protocol.
ARPA :Advanced Research Projects Agency.
UDP : User Datagram Protocol.
IPV4 : Internet Protocol Version 4.
FTP : File Transfert Protocol.
SMTP : Simple Mail Transfert Protocol.
ADSL :Asymmetric Digital Subscriber Line.
WWW : World Wide Web.
ACL : Acess Contolr Lists.
HTTP : Hypertext Transfer Protocol.
HTTPS : Hypertext Transfer Protocol Secure.
SSH : Secure Shell.
NuFW : Now User Filtering Works.
DMZ : Demilitarized Zone.
DHCP : Dynamic Host Configuration Protocol.
OS : Operating System.
CPU : Central Processing Unit.
RAM : Random Access Memory.
CHROOT : Changement de racine.
KVM : Kernel-based Virtual Machine.
VMware vSphere : Virtual Machine ware vSphere.
TIC : Technologie de l'information et de la communication.
API : Application Programming Interface.
SNMP :Simple Network Management Protocol.
Syslog : System Logging Protocol.
MySQL : My Structured Query Language.
PHP : Hypertext Preprocessor.

Liste des abréviations

LAMP : Linux, Apache, Mysql, PHP.
AS : Autonom System.
ATM : Asynchronous Transfert Mode.
DPI :Deep Packet Inspection.
ICMP : Internet Control Message Protocol.
ARP : Adress Resolution Protocol.
FreeBSD : Free Brekeley Software Distribution.
OpenVPN : Open Virtual Private Network
IDS : Intrusion Detection System.
IPS : Intrusion Prevention System.
SIP : Session Initiation Protocol.
RIP : Routag Information Protocol.
GPL : General Public License.
VLAN : Virtual Local Area Network.

Bibliographie

[1] Jean-François CARPENTIER. La sécurité informatique dans la petite entreprise, 2nd édition.

[2] https ://cisco.goffinet.org/ccna, (Consulter Mai 2021).

[3] https ://waytolearnx.com/2018/07/difference-entre-le-modele-tcp-ip-et-le-modele-osi.html, (Consulté le 10 Juin 2021).

[4] Réseau d'entreprise https ://cours-informatique-gratuit.fr (Consulté le Mai 2021).

[5] Jean-François Pillou et Jean-Philippe Bay. Sécurité informatique.3ième édition, Dunod, Paris 2013.

[6] Nicolas Baudoin et Marion Karle, NT Réseaux : IDS et IPS, Rapport Ingéniorat, Discrete Applied Mathematics, 2000.

[7] Masquelier, Mottier, Pronzato,Les Firewalls.Informatique et Réseaux 3ème année. 2000.

[8] Jean françois phillou , jean Phillippe Bay.Tout sur la sécurité informatique. Comment ca marche.net.

[9] Julien Garet, Introduction a la Virtualisation,Techniques de virtualisation, septembre 2011.

[10] Présentation de l'Entreprise RAMDY, Documents internes de RAMDY.

[11] Le Top 4 des logiciels de monitoring réseau, https ://www.appvizer.fr (Consulter en juin 2021).

[12] Gaultier Baptiste, Introduction à la supervision réseau sous GNU/Linux, 2005-2007.

[13] Type de commutation, https ://d1n7iqsz6ob2ad.cloudfront.net (Consulter en juin 2021).

[14] https ://www.pfsense.org/getting-started/. (Consulter en juin 2021).

[15] https ://forum.netgate.com/.(Consulter en juin 2021)

[16] Paquets, Informations sur le paquet https ://docs.netgate.com/pfsense. (Consulter en mai 2021).

[17] Michael W. Lucas, FreeBSD 7.0, Le guide complet du FreeBSD.

[18] Analyse du trafic Web à grande vitesse et collecte de flux, https ://www.ntop.org/products/traffic-analysis/ntop/ (Consulter en juin 2021).

[19] https ://www.virtualbox.org/. (Consulter en mai 2021).

RÉSUMÉ

La sécurité informatique est devenu l'objectif principale des entreprises vu quelles sont fréquemment les cible des diverses formes d'attaques informatiques qui menaces leur réseaux. Les pare-feu sont très populaires en tant qu'outils permettant d'élaborer efficacement des stratégies pour sécuriser un réseau informatique. Il offre au système une protection d'un réseau interne, contre un certain nombre d'intrusions venant de l'extérieur, grâce à des techniques de filtrage rapides et intelligentes. Le firewall propose un véritable contrôle sur le trafic réseau de l'entreprise. Il permet d'analyser et de gérer le trafic réseau. Dans ce mémoire, en premier lieu on a introduit le réseau et la sécurité informatique, ensuite on a présenté l'organisme d'accueil SARL RAMDY, puis on a donner des explications sur le monitoring et le trafic réseau. Finalement on a installer Pfsense en utilisant la machine virtuelle virtualBox, et ensuite on a installé Ntopng dans Pfsense comme outil de monitoring.
Mots clés : Sécurité ; Monitoring ; Trafic ; RAMDY ; Pare-feu ; Pfsense ; Ntopng ;

ABSTRACT

Computer security has become the main objective of companies as they are frequently the target of various forms of computer attacks that threaten their networks. Firewalls are very popular as a tool to effectively develop strategies to secure a computer network. It offers the system protection of an internal network against a number of intrusions from the outside, thanks to fast and intelligent filtering techniques. The firewall offers real control over the company's network traffic. It allows to analyze and manage the network traffic. In this thesis, first we introduced the network and computer security, then we presented the host organization SARL RAMDY, then we gave explanations on monitoring and network traffic. Finally we installed Pfsense using the virtualBox virtual machine, and then we installed Ntopng in Pfsense as a monitoring tool.
Key words : Security ; Monitiring ; Traffic ; RAMDY ; Firewall ; Pfsense ; Ntopng ;