REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE M'HAMED BOUGARA-BOUMERDES

Faculté de Technologie

Département Ingénierie des Systèmes Electriques

Mémoire de Master

Présenté par

GOURI Hadjer et SOUMER Marwa

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

Contribution à l'amélioration de la sécurité informatique au sein de l'entreprise CETIM

Soutenu le 14 /07 /2022 devant le jury composé de:

HAROUN	Radia	MAA	UMBB	Président
DICHOU	Karima	MCA	UMBB	Examination
RAHMOUNE	Faycal	Prof	UMBB	Encadreur
CHERIFI	Hamza	Ingénieur	UMBB	Co-Encadreur

Année Universitaire : 2021/2022

Remerciement

Nos premiers remerciement s'adressent à Dieu le tout-puissant qui par sa bonté sa miséricorde nous a permis d'avoir le courage ,la foi et la volonté de mener à bien ce travail.

Nous tenons d'abord à remercier notre promoteur Mr.RAHMOUNE Fayçal pour avoir bien voulu encadrer ce travail ainsi que pour sa riche contribution et ses précieux conseils.

Nos vifs remerciements et nos profondes reconnaissances s'adressent particulièrement à nos encadreurs Mr.CHERIFI Hamza et Mlle .TALLACHE Meriem pour leurs présentes à tout moment de la réalisation de ce projet, leurs efforts et leurs professionnalismes.

Nos remerciements vont également à l'ensemble du personnel de l'entreprise CETIM et à toutes les personnes ayant contribuée au déroulement de notre formation et mon stage dans les meilleures conditions.

Nos sincères remerciements s'adressent à notre sœur SOUMER Fadwa pour son aide très précieuse et le temps qu'elle nous a accordé dans les moments les plus difficiles.

Nous tenons à remercier individuellement les membres du jury pour le temps consacré et l'analyse minutieuse qu'ils ont mené sur ce travail.

Nos remerciements s'adressent aussi à l'équipe pédagogique de l'université, et spécialement de département de génie électrique, qui ont fourni de grands efforts pour nous transmettre connaissances et savoir tout au long de notre cursus universitaire.

Enfin, nous tenons à remercier toute personne qui a contribué de près ou de loin à la réalisation de ce modeste travail.

Dédicaces

J'ai le grand plaisir de dédier ce travail en témoignage d'affectation et de reconnaissance :

A mes parents qui m'ont énormément soutenu dans les moments les plus difficiles, partagé mes joies et mes peines, qui se sont toujours sacrifiés pour moi, et à qui je souhaite une bonne santé et une longue vie pleine de bonheur,

A mes adorables sœurs Safia et Sarah pour leur grand amour,

A mes frères Soheib et Heithem pour leur soutien et leur encouragement,

A Mes chères frères Wael, Zakaria et Tarek source de joie et de bonheur

A la mémoire de mon grand-père Ibrahim et mon cher oncle Khaled

Que dieu vous accueille dans son vaste paradis,

A tous les membres de ma famille GOURI et Haddad sans exception,

À ma chère binôme Marwa et sa famille,

A Tous mes amies qui m'ontencouragé dans les moments difficiles

A tous ce qui me sont chers

A tous ceux qui de près ou de loi m'ont soutenus et encouragés durant ces années d'étude.

HADJER

Dédicaces

Je remercie le bon Dieu qui m'a aidée à surmonter toutes les difficultés rencontrées au long de cette période pour mener à terme ce travail.

Tous d'abord je dédie mon grand-père LAFATI AMER récemment perdu, et dont je souhaite la paix a son âme, c'était le premier dont il a pensé à nous faire grandir en aimant la connaissance et qui a fait de nous des ingénieurs et des professeurs dans tous les domaines, il était notre exemplaire et il le restera toujours, on ne t'oubliera jamais PAPI.

Je dédie ce modeste travail àmes très chers parents, pour leur patience, leurs sacrifices, et soutien durant mes études. Que dieu leur procure bonne santé et longue vie.

Mes sœurs et frère Fadwa Riham et Malek, pour leur grand amour et leur soutien,

Toute la famille de mon père et celle de ma mère sans exception,

Ma chère amie et binôme Hadjer,

Je souhaite d'adresser mes remerciements les plus sincères aux personnes qui m'ontapporté leur aide et qui ont contribué à l'élaboration de ce mémoire.

MARWA

INTRODUCTION GENERALE :

Avec le développement d'internet et du nomadisme, il est essentiel pour les entreprises d'assurer une protection efficace de leur système d'information, les attaques informatiques constituent l'une des préoccupations majeures des dirigeants. Et pour cause, les cyber-menaces se sont multipliées au fil des années. Or, les entreprises doivent souvent manipuler des données sensibles qui ne doivent, en aucun cas, tomber entre de mauvaises mains. D'où l'intérêt de renforcer la sécurité informatique, qu'il s'agisse d'une PME, une TPE ou d'une grande entreprise. Terme générique s'appliquant notamment aux réseaux, à Internet, au Cloud et à aux applications, la sécurité informatique permet de répondre à ce besoin.

La sécurité informatique ou plus précisément la sécurité réseau est devenue un sujet de recherche très intense. Ces recherches ont permis le développement de certains dispositifs de protection des systèmes informatiques et des réseaux tel que les pare-feu, les VPN, l'antivirus, les systèmes de cryptographie, …etc.

Un « pare-feu » ou « Firewall » Cet outil a pour but de sécuriser au maximum le réseau local de l'entreprise, de détecter les tentatives d'intrusion et d'y parer au mieux possible et avoir un contrôle sur les activités se déroulant dans son enceinte. Cela permet de rendre le réseau ouvert sur Internet beaucoup plus sûr.

Notre projet de fin d'étude a pour objectif d'étudier les failles de sécurité informatique au niveau de l'entreprise « CETIM » et d'implémenter une architecture sécurisée.

Dans le présent mémoire, nous présenterons en détail les étapes que nous avons suivies pour réaliser notre projet, illustré en quatre chapitres organisés comme suit :

Nous allons préluder par **« Généralités »** où nous présenterons les concepts de base liés aux réseaux et sécurité informatiques.

Le second chapitre intitulé « **faille de sécurité et mode de piratage »** nous allonsexposer un aperçu des menaces, des motivations éventuelles des pirates, de leur façon de procéder, afin de mieux comprendre comment il est possible de limiter les risques.

Le troisième chapitre nommé **« les mécanismes de sécurité »** ou nous aborderons lesdéférents dispositifs, protocoles et tout moyen qui permet d'améliorer la sécurité informatique de l'entreprise.

Pour le dernier chapitre **« conception et mise en œuvre**»nous présenterons l'organisme d'accueil, et étudier leur système d'information existant ainsi que la mise en place de la solution proposée pour résoudre les anomalies trouvées.

Et en fin, nous terminons notre mémoire par une conclusion générale en proposant des perspectives.

CHAPITRE I : GENERALITES

1 Introduction :

Grâce aux nouvelles technologies, les systèmes d'information représentent des outils extrêmement puissants en matière de gestion d'entreprise dans tous les métiers, en permettant de gérer les différents flux d'information présents dans toute entité.

Un système d'information qui néglige la protection de ses données et de ses communications peut avoir des grands risques, ainsi que la société qui l'utilise. C'est la raison pour laquelle la sécurité informatique s'occupe de toute protection.

L'objectif de ce chapitre est de présenter les concepts de base liés aux réseaux informatiques et la sécurité informatique. Ces notions formeront la base nécessaire à notre contribution.

2 Les réseaux informatiques

Un réseau informatique est un ensemble d'équipement informatiques reliés entre eux grâce à des supports de communication (câble : réseau câblé, ou onde : réseau sans fil..), donc en peut le définir par la mise en relation d'au moins deux systèmes informatiquesqui permettent de garantir la communication (transfert des informations électroniques) et le partage de ressources (matérielles et logicielles).

La transmission d'information entre deux programmes informatiques se passe par deux modèles:

- Le modèle OSI.
- Le modèle TCP/IP.

Ces deux normes permettent à chaque partie de la communication de dialoguer suivant différentes couches. Chaque couche doit envoyer un message compréhensible par le reçoit le message.

2.1 Classification des réseaux informatiques

On peut classifier les réseaux selon deux aspects :

- **Selon leurs tailles**

On compte généralement 4 catégories de réseaux informatiques différenciées par la distance maximale séparant les points les plus éloignés du réseau :

- ✓ **Réseau PAN (Personal Area Network):** ces réseaux personnels interconnectent sur quelquemètres les équipements personnels tel que : le GSM, Pc portable... etc. ces équipements appartiennent à un même utilisateur.
- ✓ **LAN (Local Area Network):** correspond par leur tailles aux réseaux d'entreprise, ils servent au transport de toutes les informations numériques de l'entreprise .la distance de câblage est de quelque centaines de mètres.

- ✓ **Le man (Metropolitan Area Network):** ils permettent l'interconnexion desentreprises ou des départements sur un réseau spécialisé à haut débit. Ce type correspond à une interconnexion de quelque bâtiment se trouvant dans une ville (campus).
- ✓ **WAN (Wide Area Network) :** il s'agit d'un réseau étendu à l'échelle d'un pays ou d'un continent puisqu'il peut couvrir des centaines ou des milliers de kilomètres

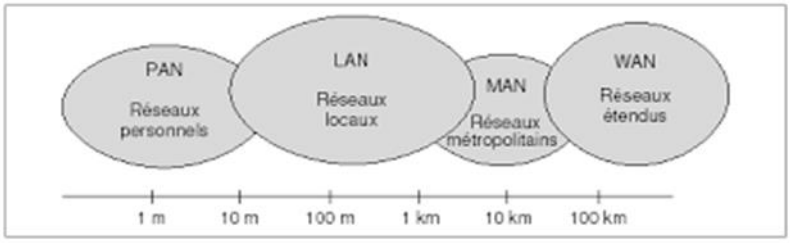

Figure 1 : Classification selon la taille.

- ❖ **Selon leurs topologies**

On peut également différencier le réseau selon leur structure et plus précisément leur organisation physique et logique.

- ✓ L'organisation physique est la façon dont les machines sont connectées « bus, anneau, étoile ».
- ✓ L'organisation logique montre comment les informations circulent sur le réseau « diffusion, point à point ».

3 Les systèmes d'information (SI)

C'est un élément clé de l'entreprise ou de l'organisation. Grace à lui que les informations peuvent circuler dans l'entreprise entre les différents acteurs. Il permet à ces derniers de communiquer, en comptant sur des outils et équipements en tout genre tel que :

- ❖ Les ordinateurs
- ❖ Les logiciels informatiques
- ❖ Les réseaux wifi, etc.

Ce système d'information poursuit un objectif bien définie qui consiste à fournir l'informationà ceux qui ont besoin, au format idéal et au moment adéquat. Il remplit aussi plusieurs fonctions essentielles parmi lesquelles en peut citer :

- ❖ **La collecte de l'information :** ce système recueille les données issues de l'environnement interne ou externe de l'entreprise.
- ❖ **Le stockage de l'information :** toutes les données collectées sont conservé dans le système d'information pour une durée indéterminée, pour permettre à toutes les personnes d'y accéder.

- **La transformation ou le traitement :** l'information stockée peut subir des modifications dans la forme ou même dans le fond. Pour s'adapté aux besoins de l'activité.
- **La diffusion :** enfin les données sont transmises par le système d'information, dans l'environnement interne ou externe de l'entreprise. [1]

4 Le Système informatique

C'est un systèmes automatisé de stockage, de traitement et de récupération de données qui tire parti des outils informatiques et électroniques pour effectuer une série complexe de processus et d'opérations.

Les systèmes informatiques sont des types de système d'information, c'est-à-dire, des systèmes organisés autour du traitement de données de différentes sortes. Cependant, tous les systèmes d'informations ne sont pas des systèmes informatiques .autrement dit, tous ne sont pas numériques automatisés ou électroniques. [2]

5 La sécurité informatique

Globalement la sécurité des systèmes d'information représente l'ensemble des moyens et de technique mise en œuvre pour assurer l'intégrité de la technologie de l'information utilisé au sein de l'entreprise .elle s'applique aux systèmes, aux réseaux et également aux données informatiques.

Elle permet d'éviter différent problèmes tel que les dommages, les attaques, les bugs ou encore les accès non autorisés [3]

La sécurité informatique et de nos jour devenue un problème majeur dans la gestion des réseaux d'entreprise ainsi pour les particuliers. Toujours plus nombreux à se connecter à internet .la transmission d'information sensible est le désire d'assurer la confidentialité de celles-ci est devenu un point primordiale dans la mise en place des réseaux informatique, la sécurité informatique vise généralement cinq principaux objectifs :

- **La Disponibilité :** ensemble des mécanismes garantissant que les ressources de l'entreprise est accessibles, que ces derniers concernent l'architecture réseau, la bande passante, le plan de sauvegarde, etc.
- **L'intégrité :** est la certitude de la présence non modifier ou non altérée d'une information et de la complétude des processus de traitement. Pour les messages échangés, il concerne la protection contre l'altération accidentelle ou volontaire d'un message transmis.

- **La confidentialité :** ensemble des mécanismes permettant d'une communication de données reste privé entre un émetteur et un destinataire. La cryptographe ou le chiffrement des données est la seule solution fiable pour assurer la confidentialité des données.
- **L'authentification :** est le moyen qui permet d'établir la validité de la requête émise pour accéder à un système.
- **La non-répudiation :** une transaction ne peut pas être niée par aucun des correspondants.la non-répudiation de l'origine et de la réception des données prouvent que les données ont bien été reçues. cela se fait par le biais de certificat numérique grâce à une clé privée. [4]

5.1 Nécessite d'une approche globale

La sécurité d'un système informatique fait souvent l'objet de métaphores. En effet, on la compare régulièrement à une chaîne en expliquant que le niveau de sécurité d'un système est caractérisé par le niveau de sécurité du maillon le plus faible. Ainsi, une porte blindée est inutile dans un bâtiment si les fenêtres sont ouvertes sur la rue. Cela signifie que la sécurité doit être abordée dans un contexte global et notamment prendre en compte les aspects suivants :

- La sensibilisation des utilisateurs aux problèmes de sécurité.
- La sécurité logique : c'est-à-dire la sécurité au niveau des données, notamment les données de l'entreprise, les applications ou encore les systèmes d'exploitation.
- La sécurité des télécommunications : technologies réseau, serveurs de l'entreprise, réseaux d'accès, etc.
- La sécurité physique : soit la sécurité au niveau des infrastructures matérielles (salles sécurisées, lieux ouverts au public, espaces communs de l'entreprise, postes de travail des personnels, etc.)[5]

5.2 Le processus de sécurité

Le processus de sécurité doit être intégré de façon dynamique :

a) Le contrôle de risque permet d'énumérer les vulnérabilités présentes, associées à des degrés de gravité.
b) Puis l'analyse des risques consiste à évaluer la criticité d'une menace en fonction de sa probabilité et son impact.
c) Afin d'élaborer une politique de sécurité cohérente, il faut émettre toutes les préconisations nécessaires à la sécurisation de l'infrastructure.
d) Une implémentation d'architecture sécurisée pourra alors être organisée. [6]

5.3 Etude des risques liée à la sécurité informatique

Les coûts d'un problème informatique peuvent être élevés et ceux de la sécurité le sont aussi. Il est nécessaire de réaliser une analyse de risque en prenant soin d'identifier les problèmes potentiels avec les solutions avec les coûts associés.

L'ensemble des solutions retenues doit être organisé sous forme d'une politique de sécurité cohérente, fonction du niveau de tolérance au risque. On obtient ainsi la liste de ce qui doit être protégé. Il faut cependant prendre conscience que les principaux risques restent câble arraché, coupure secteur, crash disque, mauvais profil utilisateur … Voici quelques éléments pouvant servir de base à une étude de risque :

- Quelle est la valeur des équipements, des logiciels et surtout des informations ?
- Quel est le coût et le délai de remplacement ?
- Faire une analyse de vulnérabilité des informations contenues sur les ordinateurs en réseau (programmes d'analyse des paquets, logs…).
- Quel serait l'impact sur la clientèle d'une information publique concernant des intrusions sur les ordinateurs de la société ? [8]

En fait, avec le développement de l'utilisation d'internet, nombre d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs, elles sont plus au niveau de l'architecture trois tiers ou n-tiers. Il devient donc nécessaire de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système.

En revanche, la sécurité est un compromis entrecoûts, risques et contraintes. On comprendra mieux le poids d'un risque en se fiant à la formule suivante :

$$\boldsymbol{Risque} = \frac{Menace \times Vulneribilité}{contre\ mesure}$$

- ✓ **Risque :** C'est la probabilité qu'une menace exploite une vulnérabilité. Autrement dit, c'est une possibilité qu'un fait dommageable se produise.
- ✓ **Menace :** c'est le danger (interne ou externe) tel qu'un hacker, un virus, etc.
- ✓ **Vulnérabilité :** C'est une faiblesse inhérente à un système (software ou hardware). Appelée parfois faille ou brèche, elle représente le niveau d'exposition face à la menace dans un contexte particulier.
- ✓ **Contre-mesure :** c'est un moyen permettant de réduire le risque dans une organisation.

Conséquences de la formule précédente on distingue deux cas :

- Le risque est d'autant plus réduit que les contre-mesures sont nombreuses ;
- Le risque est plus important si les vulnérabilités sont nombreuses [8]

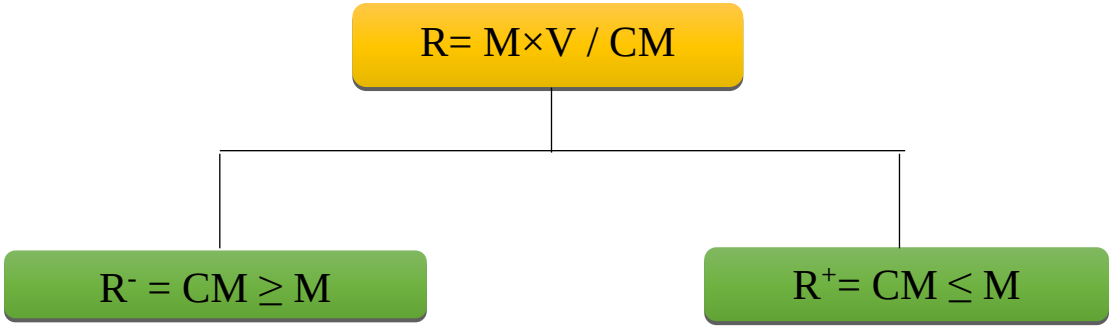

Figure 2 : les cas du risque.

Avec :

(R): Risque, **(V):**Vulnérabilité, **(M)** : Menace, **(CM)** : Contre-Mesure

5.3.1 **Typologie des risques informatique**

En sécurité informatique, il existe trois grands types des risques à savoir : les risques humains, matériels et juridiques.

5.3.1.1 ***Les Risques humains***

Les risques humains sont les plus importants, même s'ils sont le plus souvent ignorés ou minimisés. Ils concernent les utilisateurs mais également les informaticiens eux-mêmes.

- **La maladresse :** comme en toute activité, les humains commettent des erreurs ; il leur arrive donc plus ou moins fréquemment d'exécuter un traitement non souhaité, d'effacer involontairement des données ou des programmes, etc.
- **L'inconscience et l'ignorance :** de nombreux utilisateurs d'outils informatiques sont encore inconscients ou ignorants des risques qu'ils encourent aux systèmes qu'ilsutilisent, et introduisent souvent des programmes malveillants sans le savoir. Des manipulations inconsidérées (autant avec des logiciels que physiques) sont aussi courantes.
- **La malveillance :** ces dernières années, il est impossible d'ignorer les différents problèmes de virus et des vers. Certains utilisateurs peuvent volontairement mettre en péril le système d'informations, en y introduisant en connaissance de cause de virus ou en introduisant volontairement des mauvaises informations dans une base des données. On parle même de la « cybercriminalité ».

- **l'espionnage:**notamment industriel, emploie les même moyens, ainsi que bien d'autres (influence), pour obtenir des informations sur des activités concurrentes, procédés de fabrication, projets en cours, futurs produits, politique de prix, clients et prospects, etc.[6]

5.3.1.2 *Les risques matériels*

Ils sont liés aux défauts et pannes inévitables que connaissent tous les systèmes matériels et logiciels. Ces incidents sont plus ou moins fréquents selon les soins apportés lors de la fabrication et de l'application des procédures de tests effectués avant que les ordinateurs et les programmes ne soient mis en service. Certaines de ces pannes ont des causes indirectes, voire très indirectes, donc difficiles à prévoir. On peut citer :

- **Les incidents liés au matériel :** La plupart des composants électroniques modernes produits en grandes séries, peuvent comporter des défauts de fabrication. Ils finissent un jour ou l'autre par tomber en panne. Certains de ces pannes sont assez difficiles à déceler car intermittentes ou rares. Parfois, elles relèvent d'une erreur de conception.
- **Les incidents liés au logiciel :** Ce sont les plus fréquents. Les systèmes d'exploitation et les programmes sont de plus en plus complexes car ils font de plus en plus de choses. Ils nécessitent l'effort conjoint de dizaines, de centaines, voire de milliers de développeurs. Ces derniers peuvent faire des erreurs de manière individuelle ou collective que les meilleures méthodes de travail et les meilleurs outils de contrôle ou de test ne peuvent pas éliminer en totalité.
- **Les incidents liés à l'environnement** : les machines électroniques les réseaux de communication sont sensibles aux variations de températures ou de l'humidité ainsi qu'aux champs électromagnétiques.Dès lors, il est possible qu'un ordinateur tombe en panne de manière définitive ou intermittente à cause des conditions climatiques inhabituelles ou par l'influence d'installations électriques notamment industrielles. [6]

5.3.1.3 *Risques juridiques :*

L'ouverture des applications informatiques par le web et la multiplication des messages électroniques augmentent les risques juridiques liés à l'usage des technologies de l'information. On peut citer notamment :

- Le non-respect de la législation relative à la signature numérique.
- Les risques concernant la protection du patrimoine informationnel.
- Le non-respect de la législation relative à la vie privée. [6]

5.3.2 **Gestion des risques informatiques**

La gestion des risques informatiques est un ensemble d'opérations de gérer et de diriger les différentes incidences liées à la manipulation de l'outil informatique. La gestion des risques consiste en trois actions majeures :

- Etudier les risques potentiels : Cette phase consiste à faire un examen intégral de la méthodologie de l'étude des risques informatique en vigueur (identifier/mettre au jour ces risques).
- Imposer des règles de sécurité adéquates pour réduire ces risquesCeci consiste en la définition de procédures internes à l'entreprise basées sur
    - ✓ Des règles administratives.
    - ✓ Des règles physiques.
    - ✓ Des règles techniques.
- Formation des utilisateurs. [8]

5.4 **La politique de sécurité**

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

La politique de sécurité d'une entreprise se fond avant tout sur une gestion des risques décrivant les ressources critiques de l'entreprise, ces objectif de sécurité ces vulnérabilité, la probabilité d'occurrence de menace sur c'est ressources vitale, ainsi que leur conséquence sur l'entreprise.

A partir de cette politique de sécurité, une architecture, des outils et des procédures sont définir, déployés et vérifié afin de protéger les ressource critique et de rependre aux objectifs de sécurité de l'entreprise.

La sécurité informatique doit toutefois être étudiée de telles manières à ne pas empêcher les utilisateurs de développé les usages qui leur sont nécessaire, et 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, dans la mise en œuvre se fait selon les quatre étapes suivante :

- **Identifier les besoins** en termes de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquente.

- **Elaborer des règles et des procédures** à mettre en œuvre dans les défirent services de l'organisation pour les risque identifier.
- **Surveiller et détecter les vulnérabilités**de système d'information et se tenir informer des failles sur les applications et matériels utilisés.
- **Définir les actions** à entreprendre et les personnes en contacter en cas de détection d'une menace. [5]

5.5 Principaux défauts de sécurité :

Les défauts de sécurité d'un système d'information les plus souvent constatés sont :

- Installation des logiciels et matériels par défaut.
- Mises à jour non effectuées.
- Mots de passe inexistants ou par défaut.
- Services inutiles conservés (NetBIOS…).
- Traces inexploitées.
- Pas de séparation des flux opérationnels des flux d'administration des systèmes.
- Procédures de sécurité obsolètes.
- Eléments et outils de test laissés en place dans les configurations en production.
- Authentification faible.
- Télémaintenance sans contrôle fort. [12]

6 Conclusion

Les coûts d'un problème en Télécommunication et plus spécialement ce qui réside dans la sécurité nécessite à réaliser une analyse de risque en prenant soin d'identifier les problèmes potentiels avec les solutions avec les coûts associés. L'ensemble des solutions retenues doit être organisé sous forme d'une politique de sécurité cohérente qui doit être au préalable bien réfléchit et étudiée selon l'entreprise car une politique de sécurité ne se met pas en place en fonction du nombre de postes, mais du métier de l'entreprise, de la valeur des données qui circulent et de ce que représente l'outil informatique pour sa pérennité.

CHAPITRE II : LES FAILLES DE SECURITE ET MODE DE PIRATAGE

1 Introduction

Un défaut de sécurité au sein du système informatique peut avoir plusieurs répercussions sur la santé de l'entreprise. Les virus et autres codes malveillants recouvrent une réalité complexe. Il existe de nombreuses sous-catégories avec des techniques virales et des risques différents .Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les risques et les menaces potentielles, et donc de connaître et de prévoir la façon de procéder de l'ennemi.

Le but de ce chapitre est ainsi de donner un aperçu des menaces, des motivations éventuelles des pirates, de leur façon de procéder, afin de mieux comprendre comment il est possible de limiter les risques.

2 Les pirates informatiques

En informatique, le terme "Hacker " est utilisé définir les programmeurs débrouillards, avec des connaissances techniques élevées. Ces programmeurs sont avant tout passionnés par ce qu'ils font, ils nese posent pas de limites pour la connaissance ou pour assouvir leur curiosité. Les hackers sont également capables de détourner un objet ou un logiciel de son fonctionnement originel. Ils utilisent leur savoir pour découvrir les choses auxquelles ils ne sont pas censés avoir accès. Mais la communauté des hackers va également au-delà de la connaissance technique, Être un hacker correspondd'avantage à un état d'esprit plus qu'au fait de programmer. [3]

2.1 Les types de pirate

2.1.1 White Hats (chapeaux blancs)

Un white hat ou Ethical hacking se sont des experts en sécurité informatique qui se spécialisent dans les tests d'intrusion et d'autres méthodes pour s'assurer que les systèmes d'information d'une entreprise sont sécurisés. Ces professionnels de la sécurité informatique comptent sur un arsenal technologique en constante évolution pour combattre les « mauvais » pirates informatiques. [13]

2.1.2 Black Hats (les chapeaux noirs)

Un black hat est un hacker malveillant qui exerce les activités illégales pour des raisons malveillantes ou des gains personnels, causant d'énormes pertes pour les entreprises ainsi que des particuliers. Contrairement au « white hat » les « black hat »compromettent la sécurité informatique sons permission, afin de détruire des données et rendre le réseau inutilisable. [13]

2.1.3 Gray Hats (les chapeaux gris)

Un gray hat est un hacker compétant travaillant offensivement ou défensivement, selon la situation. C'est un hacker hybride entre le « white hat » et le « black hat », intéressé par les outils et les technologies de piratage, ils mettent en évidence les problèmes de sécurité dans un système pour éduquer les victimes afin d'améliorer leur sécurité mais peut occasionnellement connaitre des délits. [13]

2.1.4 Suicide Hackers (Un Script kiddie)

Sont des pirates informatiques débutants n'ayant pas les capacités nécessaires à lagestion de la sécurité informatique.

Un script est un programme, un ensemble de commandespermettant d'effectuer des opérations plus ou moins complexes. Kiddie vient du mot anglais"kid", qui signifie enfant. Ce mot fait référence au manque de capacité de ces piratesdébutants. Ils sont relativement dangereux, car ils peuvent modifier et/ou altérer lesfonctionnalités d'un système, grâce à des scripts qu'ils n'ont pas mis au point eux-mêmes etqu'ils ne maîtrisent donc pas forcément. [14]

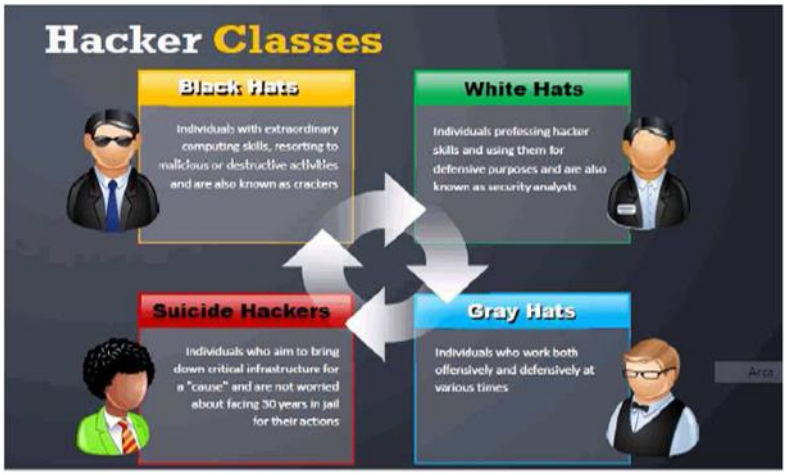

Figure 3 : les classes de hacker.

3 Les menaces

Les menaces sont considérées comme une violation potentielle du système de sécurité, elles viennent d'individus compétents à cause de vulnérabilités de système de sécurité.

3.1 Les types des menaces

Dans un système informatiques les menaces toucher les composants matérielles, logicielles ou informationnelles il existe principalement deux type de menaces. [15]

3.1.1 Les menaces accidentelles (risques)

Ce type de menaces peut se manifester ou résulter de l'exposition ou de la modification d'un objet, elle peut être des erreur des utilisateurs ou d'administrateur, matérielles ou accidents de nature industrielle (un incendie).

3.1.2 Les menaces intentionnelles (attaques)

L'ensemble des actions malveillantes (qui constituent la plus grosse partie de risque) qui devraient être l'objet principale des mesures de protection. C'est une action exécuté par une entité pour voiler la sécurité de l'information et l'utilisation non autorisée des ressources, parmi celles-ci on compte les menaces passives et les menaces actives.

- ✓ **Menaces actives**

Le pirate peut modifier le contenu des messages échangés ce qui menace l'intégrité de l'information ce type de menace et facile à détecter

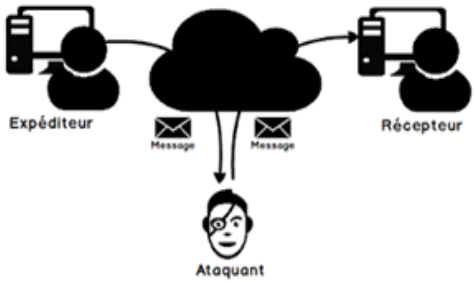

Figure 4 : Menaces active

- ✓ **Menaces passives**

Consiste essentiellement à copier ou à écouter l'information sur le réseau, elles nuisent à la confidentialité des données. En générale il est très difficile de détecter une attaque passive car elle n'interagit pas dans le fonctionnement de système.

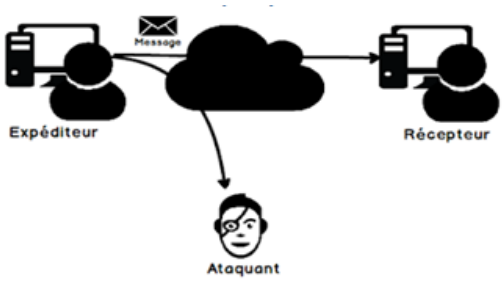

Figure 5: Menaces passive

✓ **Comparaison entre les menaces active et passive :**

Base de comparaison	Attaque active	Attaque passive
De base	Une attaque active tente de modifier les ressources du système ou d'affecter leur fonctionnement.	L'attaque passive tente de lire ou d'utiliser les informations du système mais n'influence pas les ressources du système.
Modification dans l'information	Se produit	n'a pas lieu
Dommage au système	Cause toujours des dommages au système.	Ne cause aucun dommage
Menace pour	Intégrité et disponibilité	Confidentialité
Conscience d'attaque	L'entité (victime) est informée de l'attaque.	L'entité n'est pas au courant de l'attaque.
Tâche effectuée par l'attaquant	La transmission est capturée en contrôlant physiquement la partie d'un lien.	Juste besoin d'observer la transmission.
L'accent est mis sur	Détection	La prévention

Tableau 1 : comparaison entre les menaces active et passive [16]

4 Les attaques

Une cyberattaque ou attaque informatique est tout type d'action offensive qui vise des systèmes, des infrastructures ou des réseaux informatiques, ou encore des ordinateurs personnels, en s'appuyant sur diverses méthodes pour voler, modifier ou détruire des données ou des systèmes informatiques.[17]

4.1 Objectifs des attaques

- Voler des données (données personnelles bancaires…etc.).
- Endommager ou altérer le fonctionnement normal de systèmes d'information.
- Utiliser le système compromis pour rebondir.
- Empêcher l'accès et prendre le contrôle des ressources. [18]

4.2 Les types d'attaques

Les personnes malveillantes utilisent plusieurs techniques d'attaques qui peuvent être regroupé en trois familles différentes. [28]

✓ **Les attaques directes**

Le pirate attaque directement sa victime à partir de son ordinateur. En effet, les programmes de hacking qu'ils utilisent ne sont que faiblement paramétrable, et un grand nombre de ces logiciels envoient directement les paquets à la victime.

Figure 6 : Attaque directes.

✓ **Les attaques indirectes par rebond**

Les attaques peuvent aussi être lancées indirectement par l'intermédiaire d'un système rebond afin de masquer l'identité (adresse IP) du pirate et d'utiliser les ressources du système intermédiaire. Les paquets d'attaque sont dans ce cas envoyés au système intermédiaire, lequel répercute l'attaque vers le système cible, comme l'illustre la figure 7.

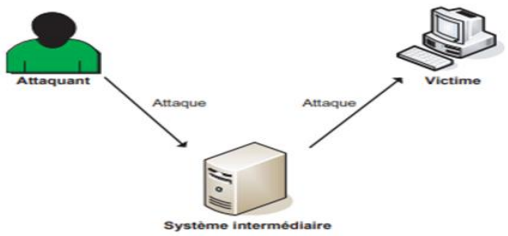

Figure 7 : Attaques indirectes par rebond.

✓ **Les attaques indirectes par réponse**

Les attaques indirectes par réponse, offrent au pirate les mêmes avantages que les attaques par rebond. Au lieu d'envoyer l'attaque au système intermédiaire pour qu'il la répercute, l'attaquant lui envoie une requête, et c'est la réponse à cette requête qui est envoyée au système cible, comme l'illustre la figure 8.

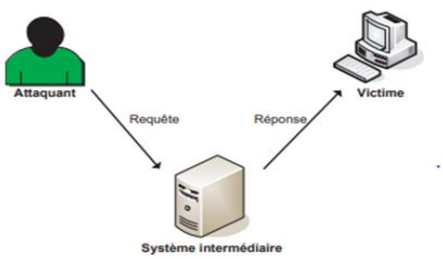

Figure 8 : Les attaques indirectes par réponse.

4.3 Les différentes étapes d'une attaque

La plupart des attaques, de la plus simple à la plus complexe fonctionnent suivant le même schéma : [19]

a) Identification de la cible

Cette étape est indispensable à toute attaque organisée ; elle permet de récolter un maximum de renseignements sur la cible en utilisant des informations publiques et sans engager d'actions hostiles. On peut citer par exemple l'interrogation des serveurs DNS….

b) Le scanning

L'objectif est de compléter les informations réunies sur une cible visée.il est ainsi possible d'obtenir les adresses IP utilisées, les services accessibles de même qu'un grand nombre d'informations de topologie détaillée (version des services, règle de firewall…). Il faut noter que certaines techniques de scans particulièrement agressives sont susceptibles de mettre à mal un réseau et entraîner la défaillance de certains systèmes.

c) L'exploitation

Cette étape permet à partir des informations recueillies d'exploiter les failles identifiées sur les éléments de la cible, que ce soit au niveau protocolaire, des services et applications ou des systèmes d'exploitation présents sur le réseau.

d) La progression

Il est temps pour l'attaquant de réaliser son objectif. Le but ultime étant d'obtenir les droits de l'utilisateur rootsur un système afin de pouvoir y faire tout ce qu'il souhaite (inspection de la machine, récupération d'informations, nettoyage des traces...).

4.4 Les techniques d'attaque:

Tout ordinateur connecté à un réseau informatique est potentiellement vulnérable à une attaque. Cette dernière est l'exploitation d'une faille d'un système informatique à des fins non connues. Il existe plusieurs telle que :

4.4.1 Les attaques réseaux:

4.4.1.1 *Le Spoofing:*

Le spoofing regroupe l'ensemble des cybersattaques qui consiste dans le vol de l'identité électronique telle que l'adresse mail, le nom de domaine ou l'adresse IP et a pour but : [22]

- Accéder aux informations personnelles d'une cible,
- Diffuser des logiciels malveillants par le biais de liens ou de pièces jointes infectées,

- Contourner les contrôles d'accès réseau,
- Redistribuer le trafic pour mener une attaque par déni de service.

✓ **IP spoofing:**

L'usurpation d'adresse IP ou IP spoofing, fait référence à la création de paquets IP avec une fausse adresse IP source pour se faire passer pour un autre système informatique. L'usurpation d'adresse IP permet aux cybercriminels d'effectuer des actions malveillantes, souvent sans détection. Cela peut inclure le vol des données, l'infection des appareils par des logiciels malveillants ou la panne de serveur. [20]

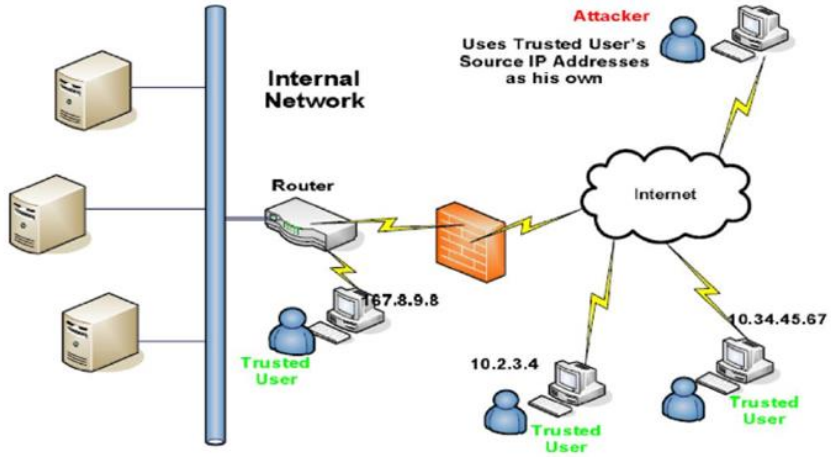

Figure 9 : IPspoofing. [21]

✓ **Sniffing :**

Les sniffers ou renifleurs de paquets sont des outils qui servent à récupérer l'ensemble des données transmises par le biais d'un réseau de la couche 2 à la couche 7 du modèle OSI.

Afin d'écouter le trafic, il faudra configurer la carte réseau en « promiscuous mode», ce mode permet d'intercepter tout le trafic réseau, même les paquets qui ne lui sont pas destinés. De nombreux protocoles réseau ne chiffrent pas les données, il est donc possible de voir en clair les mots de passe Telnet, POP, FTP... mais il est tout aussi possible de voir les sites visitées sur le réseau et de lire les données non cryptées (utilisateur et mot de passe compris). [3]

✓ **Web Spoofing :**

Le spoofing de site web fait référence au cas où un site web est conçu pour imiter un site existant connu et/ou auquel l'utilisateur fait confiance. Les pirates utilisent ces sites pour obtenir des informations de connexion et d'autres informations personnelles des utilisateurs.

- ✓ **ARP Spoofing** :

L'usurpation d'identité ARP est utilisée pour lier le MAC d'un pirate à une adresse IP d'un réseau légitime. L'attaquant peut ainsi recevoir des données destinées au propriétaire associé avec cette adresse IP. L'usurpation d'identité ARP est couramment utilisée pour voler ou modifier des données, mais elle peut également être utilisée dans les attaques par déni de service, les attaques man in the middle ou dans le détournement de session.

- ✓ **DNS Spoofing :**

Les serveurs DNS convertissent les URL et les adresses e-mail en adresses IP correspondantes. L'usurpation d'identité DNS permet aux attaquants de détourner le trafic vers une adresse IP différente, conduisant les victimes vers des sites qui propagent des logiciels malveillants.

4.4.1.2 *Man-In-The-Middle :*

Une attaque de l'homme du milieu ou MITM est un type d'attaque d'écoute clandestine, où les attaquants interrompent une conversation ou un transfert de données en cours. Après s'être insérés au "milieu" du transfert, les attaquants se font passer pour des participants légitimes. Cela permet à un attaquant d'intercepter des informations et des données de l'une ou l'autre des parties tout en envoyant des liens malveillants ou d'autres informations aux deux participants légitimes d'une manière qui pourrait ne pas être détectée avant qu'il ne soit trop tard. [24]

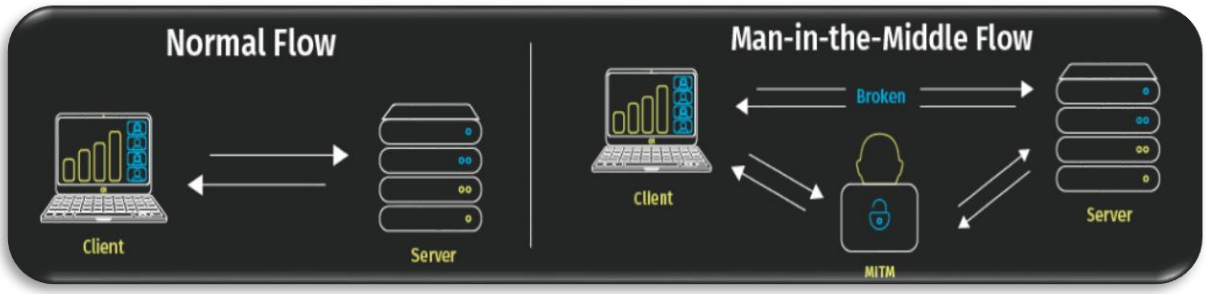

Figure 10 : Example d'uneattaque Man In The Middle.

4.4.1.2.1 Progression de l'attaque MITM:

L'exécution réussie de MITM comporte deux phases distinctes : l'interception et le déchiffrement. [26]

a) Interception :

La première étape intercepte le trafic utilisateur via le réseau de l'attaquant avant qu'il n'atteigne sa destination prévue.

La façon la plus courante (et la plus simple) de le faire est une attaque passive dans laquelle un attaquant met à la disposition du public des points d'accès Wi-Fi gratuits et malveillants. Généralement nommés d'une manière qui correspond à leur emplacement, ils ne sont pas protégés par un mot de passe. Une fois qu'une victime se connecte à un tel point d'accès, l'attaquant obtient une visibilité complète sur tout échange de données en ligne.

Les attaquants souhaitant adopter une approche plus active de l'interception peuvent lancer l'une des attaques suivantes :

- L'usurpation d'adresse IP ;
- L'usurpation ARP ;
- L'usurpation DNS.

b) Décryptage :

Après interception, tout trafic SSL bidirectionnel doit être déchiffré sans alerter l'utilisateur ou l'application. Plusieurs méthodes existent pour y parvenir :

- ✓ **L'usurpation d'identité HTTPS :**

  Lorsqu'une victime tente de se connecter à un site sécurisé, un faux certificat est envoyé à son navigateur, ce qui la conduit plutôt sur le site web malveillant de l'attaquant. Cela permet à l'attaquant d'accéder à toutes les données partagées par la victime sur ce site.

- ✓ **Le détournement SSL :**

  Chaque fois que vous vous connectez à un site web non sécurisé, indiqué par « HTTP » dans l'URL, votre serveur vous redirige automatiquement vers la version HTTPS sécurisée de ce site. Avec le piratage SSL, l'attaquant utilise son propre ordinateur et serveur pour intercepter le réacheminement, ce qui lui permet d'interrompre toute information transmise entre l'ordinateur et le serveur de l'utilisateur. Cela leur donne accès à toutes les informations sensibles que l'utilisateur utilise au cours de sa session.

- ✓ **Le stripping SSL :**

  Le stripping SSL implique que l'attaquant interrompe la connexion entre un utilisateur et un site Web. Cela se fait en rétrogradant la connexion HTTPS sécurisée d'un utilisateur vers une version HTTP non sécurisée du site web. Cela connecte l'utilisateur au site non sécurisé tandis que l'attaquant maintient une connexion au site

sécurisé, rendant l'activité de l'utilisateur visible à l'attaquant sous une forme non cryptée.

4.4.1.3 *Denial-of-service (DoS) :*

Une attaque par déni de service ou DoS est une attaque ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser. Il peut s'agir de : [27]

- ✓ l'inondation d'un réseau afin d'empêcher son fonctionnement ;
- ✓ la perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ;
- ✓ l'obstruction d'accès à un service à une personne en particulier.

L'attaque par déni de service peut ainsi bloquer un serveur de fichiers, rendre impossiblel'accès à un serveur web, empêcher la distribution de courriel dans une entreprise ou rendre indisponible un site internet, Voici quelques attaques réseaux permettant de rendre indisponible un service :

- ✓ **SYN Flooding :**

Le principe est de laisser un grand nombre de connexions TCP en attente. Le pirate envoie de nombreuses demandes de connexion (SYN), reçoit les SYN-ACK mais ne répond jamais avec ACK. Les connexions en cours occupent des ressources mémoire ce qui va entraîner une saturation et l'effondrement du système.

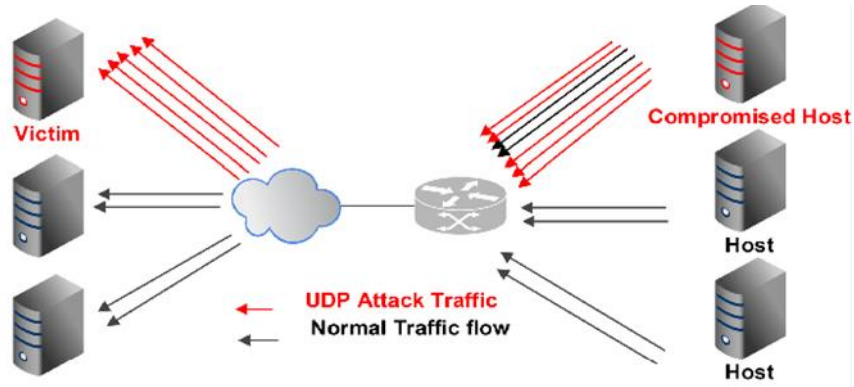

Figure 11 : SYN Flooding

- ✓ **UDP Flooding :**

Le trafic UDP est prioritaire sur TCP. Le but est donc d'envoyer un grand nombre de paquets UDP, ce qui va occuper toute la bande passante et ainsi rendre indisponible toutes les connexions TCP.

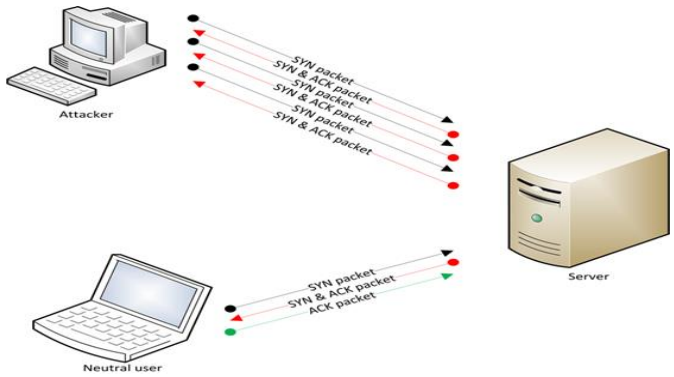

Figure 12 : UDP Flooding.

✓ **Packet Fragment :**

Cette attaque utilise une mauvaise gestion de la défragmentation au niveau ICMP. Exemple: ping of death. La quantité des données est supérieure à la taille maximum d'un paquet IP.

✓ **Smurfling :**

Le pirate fait des requêtes ICMP ECHO à des adresses de broadcast en spoofant l'adresse source (en indiquant l'adresse de la machine cible). Cette machine cible va recevoir un nombre énorme de réponses, car toutes les machines vont lui répondre, et ainsi utiliser toute sa bande passante.

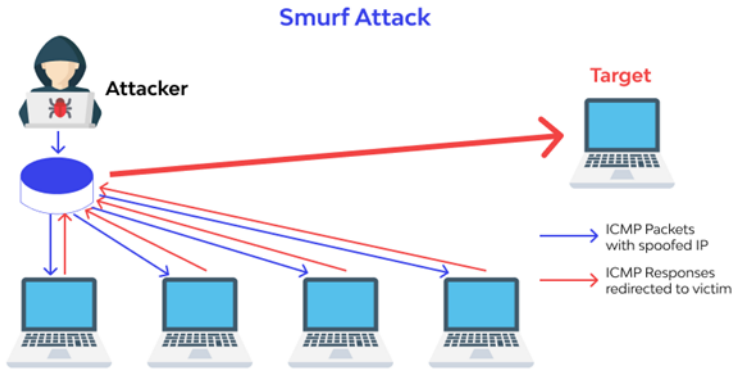

Figure 13 :smurfling.

4.4.2 Attaques systèmes

4.4.2.1 *Les malwers*

Un programme ou une partie de programme destiné à perturber, altérer ou détruire tout ou partie des éléments logiciels indispensables au bon fonctionnement d'un système informatique. Il existe plusieurs familles de malwares. On va définir les plus intéressants : [5]

❖ **Virus**

Un virus informatique est un programme doté des propriétés, infection, multiplication et possession d'une fonction nocive. La fonction d'infection permet au virus de s'introduire dans des programmes et données utilisant un langage de script. Lors de l'accès à ces derniers, le code du virus s'exécutera de façon d'abord silencieuse (phase de multiplication pendant laquelle il infectera d'autres fichiers) puis visible (activation de la fonction nocive). Cette dernière pourra être déclenchée par des facteurs très variables selon le virus (au bout de n réplications, à une date fixe, lors de l'exécution de certaines tâches précises…). Elle peut se limiter à l'affichage d'un message agaçant ou conduire à des perturbations graves de l'ordinateur (ralentissement du fonctionnement, effacement ou corruption de fichiers, formatage du disque dur...). [28]

❖ **Vers réseau**

Un ver est un programme qui peut se reproduire et se déplacer à travers un réseau en utilisant ses mécanismes, sans avoir réellementbesoin d'un support physique ou logique (disque dur, programme hôte, fichier...) pour se propager, donc un ver est un virus réseau. Voici la façon dont le ver se propagerait sur le réseau :

- ✓ Il s'introduisait sur une machine ;
- ✓ Il dressait une liste des machines qui lui étaient connectées ;
- ✓ Il forçait les mots de passe à partir d'une liste de mots ;
- ✓ Il se faisait passer pour un utilisateur auprès des autres machines ;
- ✓ Il créait un petit programme sur la machine pour pouvoir se reproduire. [6]

❖ **Cheval de Troie :**

Un cheval de Troie est un logiciel malveillant, souvent téléchargé par mégarde par l'utilisateur qui clique sur la pièce jointe d'un email piégé, qui a pour but de faire profiter à un tiers les ressources de votre ordinateur.Un cheval de Troie peut par exemple : [19]

- ✓ voler des mots de passe ;
- ✓ copier des données sensibles ;
- ✓ exécuter toute autre action nuisible, etc.

❖ **Bombes logiques**

Elles sont de véritables bombes à retardement. Ce sont de petits programmes restant inactifs tant qu'une condition n'est pas remplie, une fois la condition remplie (une date par exemple), une suite de commandes est exécutée (dont le but, le plus souvent, hélas, est de faire le plus de dégâts possible). Les bombes logiques sont généralement utilisées dans le but

de créer un déni de service en saturant les connexions réseau d'un site, d'un service en ligne ou d'une entreprise.

- **Spywares**

Un spyware ou espiogiciels est un programme chargé de recueillir des informations sur l'utilisateur de l'ordinateur dans lequel il est installé afin de les envoyer à la société qui le diffuse pour lui permettre de dresser le profil des internautes, Les récoltes d'informations peuvent ainsi être :

- ✓ les adresses web (URL) des sites visités ;
- ✓ les mots-clés saisis dans les moteurs de recherche ;
- ✓ l'analyse des achats réalisés via Internet, voire les informationsde paiement bancaire (numéro de carte bleue/VISA) ;
- ✓ des informations personnelles (numéro de sécurité sociale, etc.).

- **Keyloggers :**

Les keyloggers sont des enregistreurs de touches et par extension des enregistreurs d'activités informatiques permettant d'enregistrer les touches utilisées par un utilisateur sur son clavier et tous les évènements déclenchés. Ils sont très utiles par exemple en cas d'espionnage industriel.

- **Les Rootkits :**

Les rootkits sont des logicielsmalveillants qui permettent au cybercriminel de contrôler à distance a un ordinateur ou un réseau d'une victime avec des privilèges administratifs complets.Les rootkits ont deux caractéristiques principales :

- ✓ Ils modifient profondément le fonctionnement du système d'exploitation
- ✓ Ils se rendent invisibles (difficile à les détecter)

4.4.2.2 *Attaque de mot de passe*

Les mots de passe étant le mécanisme le plus couramment utilisé pour authentifier les utilisateurs d'un système informatique, l'obtention de mots de passe est une approche d'attaque courante et efficace. Le mot de passe d'une personne peut être obtenu en fouillant le bureau physique de la personne, en surveillant la connexion au réseau pour acquérir des mots de passe non chiffrés, en ayant recours à l'ingénierie sociale, en accédant à une base de données de mots de passe ou simplement en devinant.[17]

❖ **Les attaques par force brute**

Consistent à adopter une approche aléatoire : essayer différents mots de passe en espérant que l'un d'entre eux fonctionnera. Une certaine logique peut être appliquée : essayer des mots de passe liés au nom de la personne, à son poste, à ses passe-temps ou à des éléments similaires.

❖ **attaque par dictionnaire**

Un dictionnaire des mots de passe courants est utilisé pour tenter d'accéder à l'ordinateur et au réseau d'un utilisateur. Une approche consiste à copier un fichier chiffré contenant les mots de passe, à appliquer le même chiffrement à un dictionnaire des mots de passe couramment utilisés et à comparer les résultats.

4.4.2.3 *Porte dérobée*

Une porte dérobée crée un point d'entrée alternatif dans un appareil, un réseau ou un logiciel qui accorde un accès à distance à des ressources telles que des bases de données et des serveurs de fichiers.

Les pirates analysent le Web à la recherche d'applications vulnérables qu'ils utilisent pour installer des virus de porte dérobée. Une fois installé sur votre appareil, un virus de porte dérobée peut être difficile à détecter car les fichiers ont tendance à être très obscurcis.

L'existence d'une porte dérobée dans votre appareil donne aux auteurs la possibilité d'effectuer à distance diverses fins de piratage telles que : [23]

- ✓ Surveillance ;
- ✓ Piratage d'appareil ;
- ✓ Installation de logiciels malveillants ;
- ✓ Vol d'informations financières et ;
- ✓ Vol d'identité.

4.4.3 **Les attaques applicatives**

4.4.3.1 *Attaque XSS*

Les attaques XSS utilisent des ressources Web tierces pour exécuter des scripts dans le navigateur Web de la victime ou dans une application pouvant être scriptée. Plus précisément, l'attaquant injecte un JavaScript malveillant dans la base de données d'un site Web. Lorsque la victime demande une page du site Web, le site Web transmet la page à son navigateur avec le script malveillant intégré au corps HTML. Le navigateur de la victime exécute ce script, qui envoie par exemple le cookie de la victime au serveur de l'attaquant, qui l'extrait et l'utilise pour détourner la session.

Les conséquences les plus graves se produisent lorsque XSS sert à exploiter des vulnérabilités supplémentaires. Ces vulnérabilités peuvent non seulement permettre à un attaquant de voler des cookies, mais aussi d'enregistrer les frappes de touches et des captures d'écran, de découvrir et de collecter des informations réseau et d'accéder et de contrôler à distance l'ordinateur de la victime.[25]

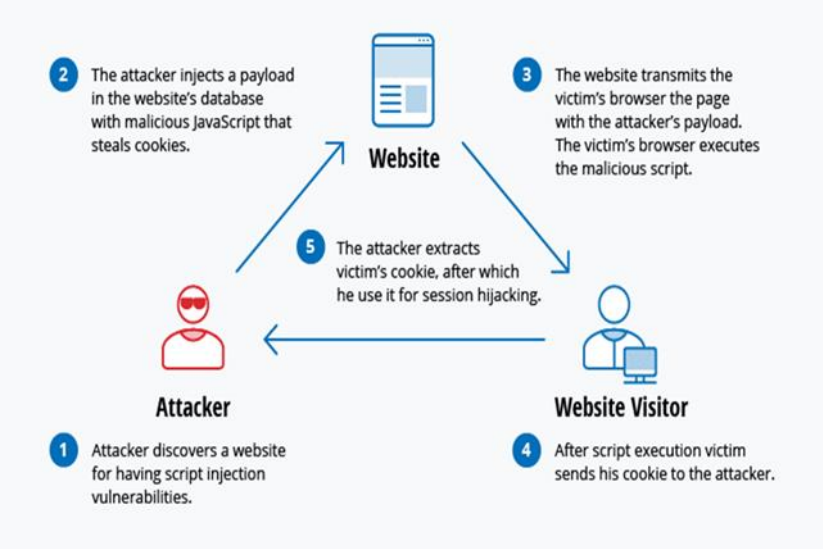

Figure 14 : Attaque XSS.

4.4.3.2 ***Attaque par injection SQL***

L'injection SQL est devenue un problème courant qui affecte les sites Web exploitant des bases de données. Elle se produit lorsqu'un malfaiteur exécute une requête SQL sur la base de données via les données entrantes du client au serveur. Des commandes SQL sont insérées dans la saisie du plan de données (par exemple, à la place du nom d'utilisateur ou du mot de passe) afin d'exécuter des commandes SQL prédéfinies. Un exploit d'injection SQL réussi peut lire les données sensibles de la base de données, modifier (insérer, mettre à jour ou supprimer) les données de la base de données, exécuter des opérations d'administration de la base de données (par exemple la fermer), récupérer le contenu d'un fichier spécifique, et dans certains cas envoyer des commandes au système d'exploitation. [25]

4.4.3.3 ***Attaques Phishing et SpearPhishing***

L'hameçonnage ou Phishing est un cybercrime qui consiste à utiliser de faux courriels, sites Web et messages textes incitant la victime à révéler des informations personnelles et corporatives confidentielles (données de carte de crédit, numéro de téléphone,informations sur une entreprise…etc).

Ces informations sont ensuite utilisées par les criminels pour effectuer un vol d'identité et commettre une fraude. Si les cybercriminels parviennent à piéger leur victime en utilisant des tactiques d'hameçonnage, c'est qu'ils prennent soin de se dissimuler derrière des courriels et des sites Web qui leur sont familiers. Par exemple, un message pressant le destinataire de mettre à jour les informations de son compte pour se protéger d'une fraude pourrait être envoyé via l'adresse courriel « administrator@paypal.org.com », au lieu de « administrator@paypal.com ».

Le harponnage ou Spear Phishing est un type de cyberattaque utilisant les courriels pour cibler des individus et des entreprises. Les criminels appliquent des tactiques habiles pour recueillir des données personnelles sur leurs cibles et leur envoyer des courriels qui semblent familiers et dignes de confiance.

En général, ces courriels contiennent une pièce jointe qui comporte un lien malveillant vers un maliciel, un rançongiciel ou un logiciel espion et le message mentionne une action urgente à réaliser par le destinataire telle que le transfert d'une somme d'argent ou l'envoi de données personnelles comme un mot de passe bancaire. [29]

4.4.3.1 *Vol de cookies*

Dans cette attaque, l'attaquant prend le contrôle de la session de l'utilisateur. Une session commence lorsqu'un utilisateur se connecte à un service particulier, par exemple Internet Banking, et se termine lorsqu'il se déconnecte. L'attaque est basée sur la connaissance que le pirate a des cookies de session des utilisateurs.

Dans de nombreuses situations, lorsqu'un utilisateur se connecte à une application Web, le serveur définit un cookie de session temporaire dans le navigateur Web. Grâce à ce cookie de session temporaire, nous savons que cet utilisateur spécifique est connecté à une session particulière. Il convient de noter qu'un piratage de session réussi ne se produira que lorsque le cybercriminel connaîtra la clé de session ou l'identifiant de session de la victime. Ainsi, dans le cas où il peut voler des cookies de session, il peut reprendre la session de l'utilisateur. Une autre façon de voler les cookies de l'utilisateur consiste également à le forcer à cliquer sur un lien malveillant. [30]

5 Conclusion

L'architecture réseau d'aujourd'hui est complexe et est confrontée à un environnement de menaces en constante évolution et à des attaquants qui essaient toujours de trouver et d'exploiter des vulnérabilités. Comme nous l'avons vu dans ce chapitre les vulnérabilités peuvent

exister dans un grand nombre de domaines, y compris les appareils, les données, les applications, les utilisateurs et les emplacements.

Dans ce qui suit, on va s'intéresser à l'étude des mécanismes de sécurité qui permet d'éviter les intrusions, ça sera le sujet du troisième chapitre.

CHAPITRE III : LES MECANISMES DE SECURITE

1 Introduction

A partir du moment où un réseau d'une entreprise se connecte à Internet, celui-ci devient vulnérable à un certain nombre d'attaques venant de l'extérieur. Donc il est primordial d'implémenter des mécanismes de sécurité qui garantir la fiabilité et la confidentialité des communications entre les utilisateurs.

Dans ce chapitre nous aborderons les défirent dispositifs, protocoles et toute moyenne qui permet de amélioré la sécurité informatique d'entreprise.

2 Les systèmes de détection d'intrusion IDS

Un IDS est un équipement permettant de surveiller l'activité d'un réseau ou d'un hôte donné. Composé généralement de logiciel et éventuellement de matériel, ce système informatique a le rôle de détecter toute tentative d'intrusion.

Un IDS réagit en cas d'anomalie, à condition que le système puisse bien identifier les intrus externes ou internes qui ont un comportement anormal, en déclenchant un avertissement, une alerte, en analysant éventuellement cette intrusion pour empêcher qu'elle ne se reproduise, ou en paralysant même l'intrusion.

Un IDS est un capteur informatique qui écoute de manière furtive le trafic sur un système, vérifie, filtre et repère les activités anormales ou suspectes, ce qui permet ultérieurement de décider d'action de prévention. Sur un réseau, l'IDS est souvent réparti dans tous les emplacements stratégiques du réseau. [31]

2.1 Les types d'IDS

- **IDS réseaux**

Le rôle essentiel d'un IDS réseau est l'analyse et l'interprétation des paquets circulant sur ce réseau. L'implantation d'un NIDS sur un réseau se fait de la façon suivante : des capteurs sont placés aux endroits stratégiques du réseau et génèrent des alertes s'ils détectent une attaque. Ces alertes sont envoyées à une console sécurisée, qui les analyse et les traiteséventuellement. Cette console est généralement située sur un réseau isolé, qui relie uniquement les capteurs et la console. [32]

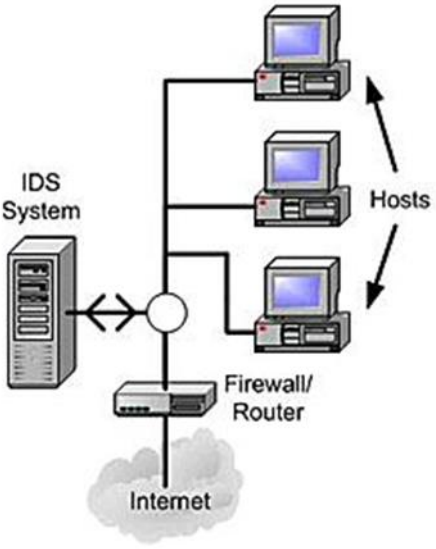

Figure 15 : Architecture d'un NIDS [33]

❖ **IDS Host**

Les HIDS (Host IDS) analysent le fonctionnement et l'état des machines sur lesquels ils sont installés afin de détecter les attaques en se basant sur des démons (tels que syslogd par exemple). L'intégrité des systèmes est alors vérifiée périodiquement et des alertes peuvent être levées. Par nature, ces IDS sont limités et ne peuvent détecter les attaques provenant des couches réseaux (tels que les attaques de type DOS).[33]

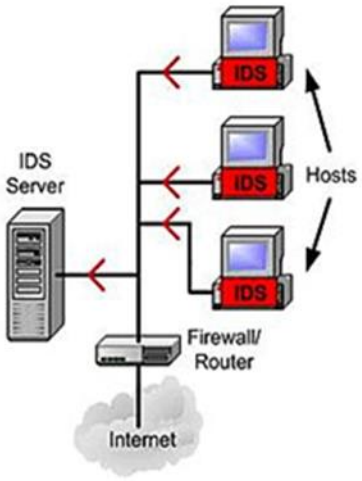

Figure 16 : Architecture d'un HIDS [33]

❖ **IDS Hybrides**

Les IDS hybrides rassemblent les caractéristiques des NIDS et HIDS. Ils permettent, en un seul outil, de surveiller le réseau et les terminaux. Les sondes sont placées en des points stratégiques, et agissent comme NIDS et/ou HIDS suivant leurs emplacements. Toutes ces

sondes remontent alors les alertes à une machine qui va centraliser le tout, et agréger/lier les informations d'origines multiples. Ainsi, on comprend que les IDS hybrides sont basés sur une architecture distribuée, où chaque composant unifie son format d'envoi (par exemple IDMEF). Cela permet de communiquer et d'extraire des alertes plus pertinentes. Les avantages des IDS hybrides sont multiples : [34]

- ✓ Moins de faux positifs
- ✓ Meilleure corrélation (la corrélation permet de générer de nouvelles alertes à partir de celles existantes)
- ✓ Possibilité de réaction sur les analyseurs

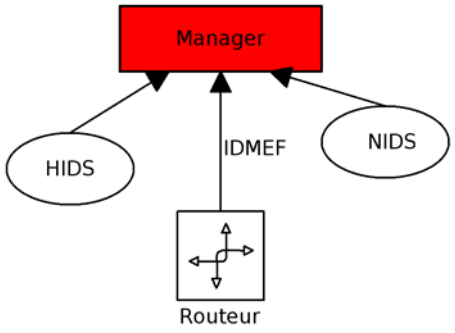

Figure 17 : Principe de l'IDS hybride.

3 Systèmes de prévention d'intrusion (IPS)

Un système de prévention d'intrusion est un outil des spécialistes en sécurité des systèmes d'information, similaire aux IDS, sauf que ce système peut prendre des mesures afin de diminuer les risques d'impact d'une attaque. C'est un IDS actif, il détecte un balayage automatisé, l'IPS peut bloquer les ports automatiquement. [38]

3.1 Systèmes de prévention d'intrusion réseau (NIPS)

Un NIPS est un logiciel ou matériel connecté directement à un segment du réseau.il a comme rôle d'analyser les tous les paquets circulant dans ce réseau. La principale différence entre un NIDS et un NIPS tient principalement en deux caractéristiques: le positionnement en coupure sur le réseau du NIPS et non plus seulement en écoute comme pour le NIDS et la possibilité de bloquer immédiatement les intrusions et ce quel que soit le type de protocole de transport utilisé et sans reconfiguration d'un équipement tierce. Ce qui induit que le NIPS est constitué d'une technique de filtrage de paquets et de moyens de blocage. [39]

3.1.1 Fonctionnement d'un NIPS

Le NIPS combine les caractéristiques d'un IDS standard avec celles d'un firewall. On le qualifie parfois de firewall à inspection en profondeur (deep inspection). Comme avec un firewall, le NIPS a au minimum deux interfaces réseau, une interne et une externe. Les paquets arrivent par une des interfaces et sont passés au moteur de détection. L'IPS fonctionne pour le moment comme un IDS en déterminant si oui ou non le paquet est malveillant. Cependant, en plus de déclencher une alerte dans le cas où il détecte un paquet suspect, il rejettera le paquet et marquera cette session suspecte. Quand les paquets suivants de cette session arriveront à l'IPS ils seront rejetés. Les NIPS sont déployés en ligne avec le segment du réseau à protéger, du cout toutes les données qui circulent entre le segment surveillé et le reste du réseau sont forcés de passer par le NIPS.

Un NIPS déclenche des alarmes du type ‘‘tel ou tel trafic a été détecter en train d'essayer d'attaquer ce système et a été bloqué’’.

3.2 Systèmes de prévention d'intrusion Kernel (KIPS) :

Grâce à un KIPS, tout accès suspect peut être bloqué directement par le noyau, empêchant ainsi toute modification dangereuse pour le système. Le KIPS peut reconnaître des motifs caractéristiques du débordement de mémoire, et peut ainsi interdire l'exécution du code.

Le KIPS peut également interdire l'OS d'exécuter un appel système qui ouvrirait un shell de commandes .Puisqu'un KIPS analyse les appels systèmes, il ralentit l'exécution. C'est pourquoi ce sont des solutions rarement utilisées sur des serveurs souvent sollicités.

4 La cryptographie :

La cryptographie est une méthode de protection des informations et des communications par l'utilisation de codes, de sorte que seuls les destinataires des informations puissent les lire et les traiter.

En informatique la cryptographie désigne des techniques d'information et de communication sécurisées dérivées de concepts mathématiques et d'un ensemble de calculs basés sur des règles, appelés algorithmes, pour transformer les messages de manière difficile à déchiffrer. Ces algorithmes déterministes sont utilisés pour la génération de clés cryptographiques, la signature numérique, la vérification pour protéger la confidentialité des données, la navigation sur Internet et les communications confidentielles telles que les transactions par carte de crédit et le courrier électronique. [41]

Le chiffrement se fait généralement à l'aide d'une clé de chiffrement, le déchiffrement nécessite quant à lui une clé de déchiffrement. On distingue généralement deux types de clés :

- **Les clés symétriques :** il s'agit de clés utilisées pour le chiffrement ainsi que pour le déchiffrement. On parle alors de chiffrement symétrique ou de chiffrement à clé secrète.
- **Les clés asymétriques :** il s'agit de clés utilisées dans le cas du chiffrement asymétrique (aussi appelé chiffrement à clé publique). Dans ce cas, une clé différente est utilisée pour le chiffrement et pour le déchiffrement.

4.1 Objectifs de la cryptographie

La cryptographie est traditionnellement utilisée pour dissimuler des messages aux yeux de certains utilisateurs. Cette utilisation a aujourd'hui un intérêt d'autant plus grand que les communications via internet circulent dans des infrastructures dont on ne peut garantir la fiabilité et la confidentialité. Désormais, la cryptographie sert non seulement à préserver la confidentialité des données mais aussi à garantir leur intégrité et leur authenticité.

4.1 Les types de cryptage

4.1.1 Cryptage symétrique

Le cryptage symétrique appelé également cryptage à clé secrète ou chiffrement conventionnel utilise une même clé pour crypter et décrypter le message, très efficace et assez économe en ressource CUP. Les algorithmes de chiffrement les plus connus sont : DES (Data Encryptions Standard) et 3DES et AES

Le principe problème de cette technique la distribution des clés dans un réseau étendu, nécessite de partager une seul clé avec chacun de nos correspondants. [18]

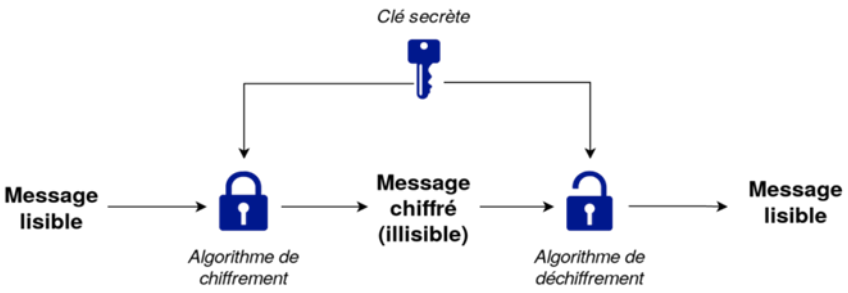

Figure 18 : cryptage symétrique.

4.1.2 Cryptage asymétrique

Ce système de cryptage utilise deux clés différentes pour chaque utilisateur : une est privée et n'est connue que par son propriétaire ; l'autre est publique et donc accessible par tout le monde.

Les clés publique et privée sont mathématiquement liées par l'algorithme de cryptage de telle manière qu'un message crypté avec une clé publique ne puisse être décrypté qu'avec la clé privée correspondante car ces deux clés générer au même temps. Une clé est donc utilisée pour le cryptage et l'autre pour le décryptage.

Le principal avantage du cryptage à clé publique est de résoudre le problème de l'envoi de clé privée sur un réseau non sécurisé. Bien que plus lent que la plupart des cryptages à clé privée il reste préférable pour 3 raisons :

- ✓ Plus évolutif pour les systèmes possédant des millions d'utilisateurs.
- ✓ permet de signer le message donc garantir l'Authentification et la non- répudiation.
- ✓ Supporte les signatures numériques.

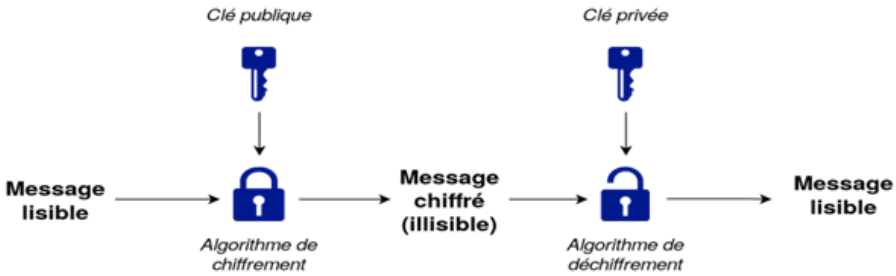

Figure 19 : cryptage asymétrique.

5 Les protocoles

5.1 Les protocoles sécurisés

Les protocoles réseau sont un ensemble de règles, de conventions et de structures de données qui dictent la manière dont les appareils échangent des données sur les réseaux. En d'autres termes, les protocoles réseau peuvent être assimilés à des langages que deux appareils doivent comprendre pour une communication transparente des informations, indépendamment de leur infrastructure et des disparités de conception.

Il existe de nombreux protocoles réseaux, mais ils n'ont pas tous, ni le même rôle, ni la même façon de procéder. Sur Internet, les protocoles utilisés font partie d'un ensemble de protocoles, appelés protocoles TCP/IP. Cette suite de protocoles contient entre autres les protocoles TCP pour le transport des données, HTTP pour le web, FTP pour le transfert de fichiers, ICMP pour le contrôle des erreurs, etc.

La plupart des protocoles de la suite TCP/IP ne sont pas sécurisés, c'est-à-dire que les données transitent en clair sur le réseau. Ainsi, des protocoles de plus haut niveau, dits « pro-

tocoles sécurisés» ont été mis au point afin d'encapsuler les messages dans des paquets de données chiffrés. [5]

5.1.1 **Protocole IPSec**

IPSec (Internet Protocol Security) est un ensemble de protocoles (couche 3 modèle OSI) utilisant des algorithmes permettant le transport de données sécurisées sur un réseau IP, réalisé dans le but de fonctionner avec le protocole IPv6, il fut adapté pour l'actuel protocole IPv4.IPSec va fournir et assurer à ses utilisateurs :

- **Authentification des données :**IPSec permet de s'assurer que chaque paquet échangé, il a bien été émis par la bonne machine et qu'il est bien à destination de la seconde machine.
- **Confidentialité des données échangées :** on peut décider de chiffrer le contenu des paquets IP pour empêcher qu'une personne extérieure ne le lise.
- **Intégrité des données échangées :** IPSec permet de s'assurer qu'aucun paquet n'a subi une quelconque modification durant son trajet.
- **Protection contre l'analyse du trafic :**IPSec permet de chiffrer les adresses réelles de l'expéditeur et du destinataire, ainsi que tout l'entête IP correspondant (c'est le principe du tunneling).

5.1.1.1 ***Architecture***

IPSec est constitué de deux protocoles : [36]

- **AH (Authentication Header)** : est responsable de l'authentification des parties ; mais ne garantit aucune confidentialité.
- **ESP (Encapsulating Security Payload)** : est responsable du chiffrement des données. Il peut garantir l'authentification des parties, mais apporte une certaine redondance avec AH. Ces deux protocoles peuvent être alors utilisés séparément ou combinés.

IPSec négocie les paramètres de sécurité entre les deux parties et notamment les algorithmes qui seront utilisés. IPSec propose également un cadre permettant de renégocier régulièrement les clés utilisées sur la base de leur temps de vie.

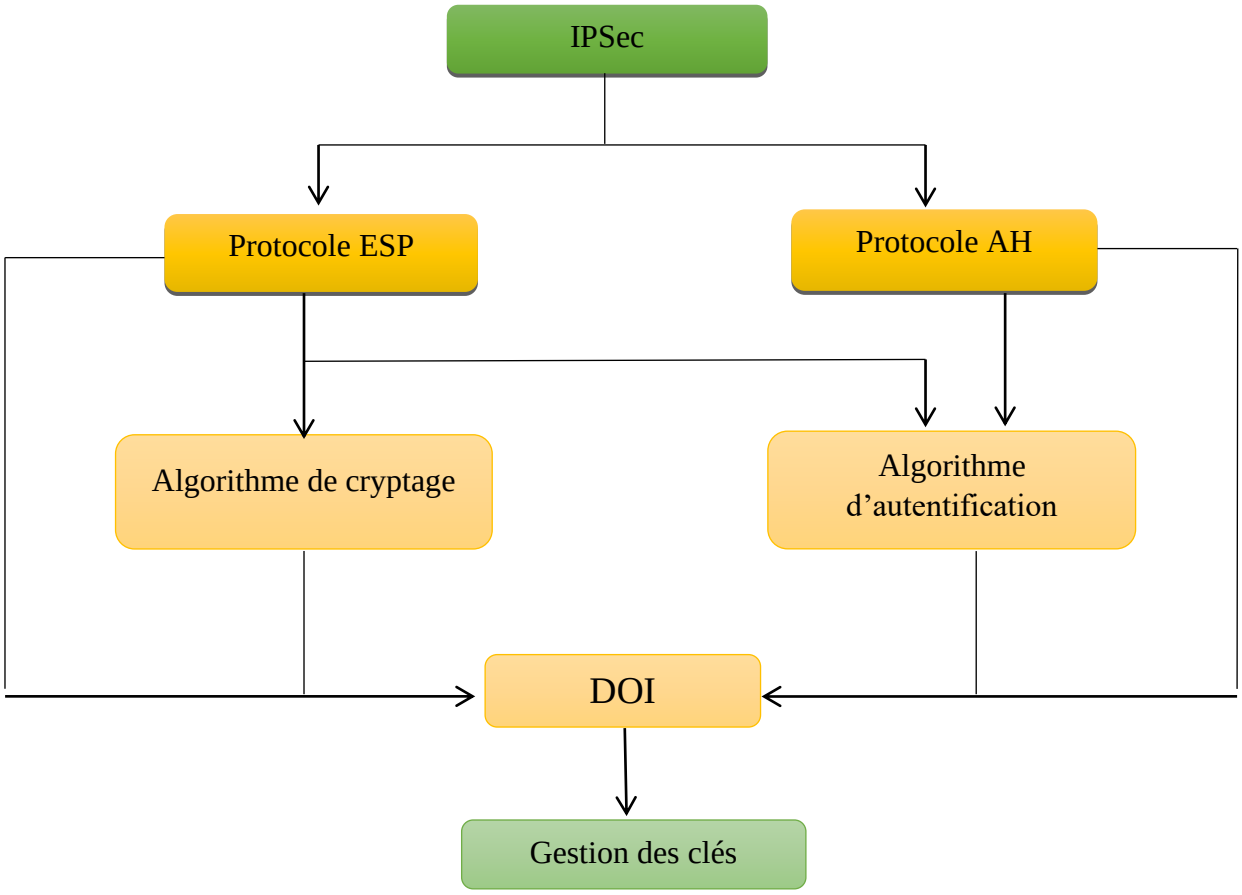

Figure 20: Architecture IPSec.

- **DOI (Domain d'interprétation)** : est l'identifiant qui prend en charge les protocoles AH et ESP. Il contient les valeurs nécessaires pour la documentation liée les unes aux autres.
- **Gestion des clés** : contient le document qui décrit les clés sont échangées entre l'expéditeur et le destinataire.

5.1.2 Protocole SSL

SSL (Secure Sockets Layer) est un procédé de sécurisation des transactions effectuées via Internet, repose sur un procédé de cryptographie par clé publique afin de garantir la sécurité de la transmission de données sur Internet.

Son principe consiste à établir un canal de communication sécurisé (chiffré) entre deux machines (un client et un serveur) après une étape d'authentification.

Le système SSL est indépendant du protocole utilisé, ce qui signifie qu'il peut aussi bien sécuriser des transactions faites sur le Web par le protocole HTTP que des connexions via les protocoles FTP, POP ou IMAP. En effet, SSL agit telle une couche supplémentaire permet-

tant d'assurer la sécurité des données, située entre la couche application et la couche transport (protocole TCP par exemple).

La totalité des navigateurs supportent aujourd'hui le protocole SSL. Sur les sites qui l'utilisent, un cadenas apparaît sur la même ligne que son adresse web.

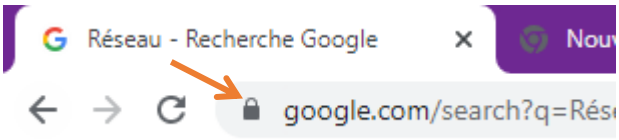

Figure 21 : exemple de protocole SSL sous Chrome.

5.1.3 **Protocole SSH**

Le protocole SSH (Secure Shell) est un protocole permettant à un client d'ouvrir une session interactive sur une machine distante (serveur) afin d'envoyer des commandes ou des fichiers de manière sécurisée : Les données circulant entre le client et le serveur sont chiffrées, ce qui garantit leur confidentialité Il n'est donc pas possible d'écouter le réseau à l'aide d'un analyseur de trames.

Le client et le serveur s'authentifient mutuellement afin d'assurer que les deux machines qui communiquent sont bien celles que chacune des parties croit être. Il n'est donc plus possible pour un pirate d'usurper l'identité du client ou du serveur (Spoofing). [18]

5.1.4 **Protocole HTTPs**

HTTPS (protocole de transfert hypertexte sécurisé) est un protocole de communication internet qui protège l'intégrité ainsi que la confidentialité des données lors du transfert d'informations entre l'ordinateur de l'internaute et le site, Les données envoyées à l'aide du protocole HTTPS sont sécurisées via le protocole TLS, qui offre trois niveaux clés de protection :[37]

- **Le chiffrement :** il fait usage de méthode cryptographie symétrique pour le chiffrement des données échangées pour les protéger des interceptions illicites. En d'autres termes, lorsqu'un internaute navigue sur un site Web, personne ne peut "écouter" ses conversations, suivre ses activités sur diverses pages ni voler ses informations.
- **L'intégrité des données :** les informations ne peuvent être ni modifiées, ni corrompues durant leur transfert, que ce soit délibérément ou autrement, sans être détectées.
- **L'authentification :** il fait par l'usage de méthodes de cryptographie asymétrique pour que les internautes communiquent avec le bon site web ce qui permet de lui protéger contre les attaques MTIM et instaure un climat de confiance pour l'internaute.

5.1.5 **Protocole S/MIME**

S/MIME (Secure MIME ou extensions du courrier électronique à buts multiples et sécurisées) est un procédé de sécurisation des échanges par courrier électronique permettant de garantir la confidentialité et la non-répudiation des messages électroniques. Est basé sur le standard MIME, dont le but est de permettre d'inclure dans les messages électroniques des fichiers attachés autres que des fichiers texte (ASCII).

5.1.5.1 ***Fonctionnement***

S/MIME fonctionne sur la base d'un cryptage asymétrique. Cela signifie qu'il existe un ensemble de clés impliquées pour chiffrer et déchiffrer un e-mail.

Un certificat S/MIME est installé sur les clients de messagerie du destinataire et de l'expéditeur. Lorsqu'un e-mail est envoyé, l'expéditeur crypte l'e-mail à l'aide de la clé publique du destinataire et le destinataire décrypte l'e-mail à l'aide de la clé privée.

S/MIME attache également une signature numérique à un e-mail. Cela garantit que l'expéditeur est autorisé à envoyer des e-mails à partir d'un certain domaine.

5.1.6 **Protocole DNSSec**

DNSsec (Domain Name System Security Extensions)leur rôle principale de de sécuriser la transmission des serveurs DNS,il constitue d'une des extensions du protocole DNS et est censé assurer l'authentification et l'intégrité des enregistrements du DNS.

Son fonctionnement est basé sur des vérifications de signatures numériques et d'échange de données cryptées, il permet ainsi de constituer une chaîne d'identification sécurisée. L'utilisateur pourrait donc mieux identifier si tel ou tel sous-domaine d'un site web est bien celui auquel il veut s'adresser.il pourrait être mis en place de façon systématique pour contrer les failles du protocole DNS et le phénomène de phishing.

5.2 **Les protocoles d'authentifications**

L'authentification est une procédure permettant pour un système informatique de vérifier l'identité d'une personne ou d'un ordinateur et d'autoriser l'accès de cette entité à des ressources (systèmes, réseaux, applications).Le terme AAA est souvent utilisé pour désigner les facettes suivantes de la sécurité : [5]

- **Authentification (Authentication) :** il s'agit de la vérification de l'identité d'un utilisateur.
- **Autorisation (Authorization) :** il s'agit des droits accordés à un utilisateur, tels que l'accès à une partie d'un réseau, à des fichiers, le droit d'écriture, etc.

- **Comptabilité (Accounting) :** il s'agit des informations récoltées pendant toute la durée de la session, après identification de l'utilisateur.

5.2.1 Protocole Kerberos

Kerberos est un service d'authentification qui est utilisé sur les réseaux informatiques ouverts ou non sécurisés. Le protocole de sécurité authentifie les demandes de service entre deux hôtes de confiance ou plus, via un réseau non approuvé comme Internet. Pour l'authentification d'applications client-serveur et la vérification de l'identité de l'utilisateur, il utilise le chiffrement cryptographique et un tiers de confiance.

Les utilisateurs, ordinateurs et services qui utilisent Kerberos s'appuient sur le KDC, qui assure deux fonctions en un seul processus : l'authentification et l'attribution de tickets. Les « tickets KDC » authentifient toutes les parties impliquées, en vérifiant l'identité de tous les nœuds, les points de départ et d'arrivée des connexions logiques. Pour cela, le processus d'authentification Kerberos utilise un mécanisme de clés secrètes qui évite que les paquets de données transmis ne soient lus ou modifiés. Ils sont ainsi protégés contre les écoutes et attaques répétées. [40]

5.2.2 Protocole PAP

Le protocole PAP (PasswordAuthentication Protocol) est un protocole d'authentification par mot de passe. Le protocole PAP a été originalement utilisé dans le cadre du protocole PPP.

Le principe du protocole PAP consiste à envoyer l'identifiant et le mot de passe en clair à travers le réseau. Si le mot de passe correspond, alors l'accès est autorisé. Ainsi, le protocole PAP n'est utilisé en pratique qu'à travers un réseau sécurisé.

5.2.3 Protocole CHAP

Le protocole CHAP (Challenge Handshake Authentication Protocol), est un protocole d'authentificationaméliore le protocole PAP dans la mesure où le mot de passe n'est plus transmis en clair sur le réseau basé sur la résolution d'un défi (challenge), c'est-à-dire une séquence à chiffrer avec une clé et la comparaison de la séquence chiffrée ainsi envoyée. Les étapes du défi sont les suivantes :

a) un nombre aléatoire de 16 bits est envoyé au client par le serveur d'authentification, ainsi qu'un compteur incrémenté à chaque envoi ;
b) la machine distante « hache » ce nombre, le compteur ainsi que sa clé secrète (le mot de passe) avec l'algorithme de hachage MD5 et le renvoie sur le réseau ;

c) le serveur d'authentification compare le résultat transmis par la machine distante avec le calcul effectué localement avec la clé secrète associée à l'utilisateur ;
d) si les deux résultats sont égaux, alors l'identification réussit, sinon elle échoue.

5.2.4 Protocole MS-CHAP

Le protocole CHAP implique que l'ensemble des mots de passe des utilisateurs soient stockés en clair sur le serveur, ce qui constitue une vulnérabilité potentielle. Ainsi MS-CHAPpropose une fonction de hachage propriétaire permettant de stocker un hash intermédiaire du mot de passe sur le serveur. Lorsque la machine distante répond au défi, elle doit ainsi préalablement hacher le mot de passe à l'aide de l'algorithme propriétaire.

6 La signature

Dans toute transaction professionnelle, les deux parties doivent offrir une garantie de leurs identités. La signature numérique et le certificat sont des moyens d'identification de l'émetteur d'un message.

6.1.1 La signature électronique

Le paradigme de signature électronique est un procédé permettant de garantir l'authenticité de l'expéditeur (fonction d'authentification) et de vérifier l'intégrité du message reçu.
La signature électronique assure également une fonction de nonrépudiation, c'est-à-dire qu'elle permet d'assurer que l'expéditeur a bien envoyé le message.

Il existe deux classes de signatures, l'une symétrique (utilisation d'une clé partagée entre la source et la destination d'un message), l'autre asymétrique (utilisation d'une paire de clés par entité). [5]

6.1.2 Certificat numérique

Un certificat numérique (ou certifier l'identité)du propriétaire d'une clé publique, un peu à la manière d'une carte d'identité.
Un certificat est généré dans une infrastructure à clés publiques (PKI) par une autorité de certification (CA) qui a donc la capacité de générer des certificats numériques contenant la clé publique en question.
Le format reconnu actuellement est le format X509V3. C'est un petit fichier, qui contient au moins les informations suivantes : [18]

- le numéro de série.
- l'algorithme de signature.
- le nom de l'émetteur (autorité de certification).
- la date de début de fin de validité.

- l'adresse électronique du propriétaire.
- la clé publique à transmettre.
- le type de certificat.
- l'empreinte du certificat (signature électronique).

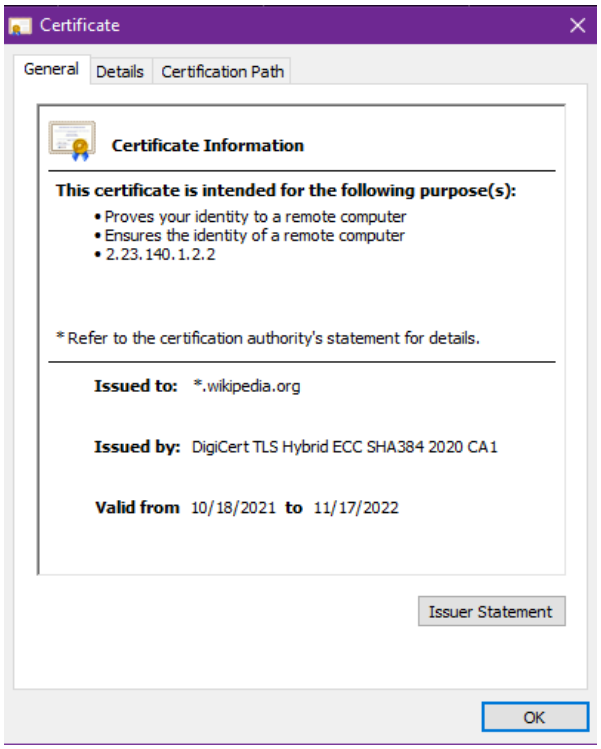

Figure 22 : Exemple d'un certificat numérique.

7 Les Anti-virus

Un antivirus est un logiciel informatique capable de détecter la présence de malware sur un ordinateur et, dans la mesure du possible, désinfecter ce dernier.

L'antivirus analyse les fichiers entrants (fichiers téléchargés ou courriers électroniques), la mémoire vive de l'ordinateur et les périphériques de stockage, les clés USB …etc. La détection d'un logiciel malveillant peut reposer sur trois méthodes : [42]

- Reconnaissance d'un code déjà connu (appelé signature) et mémorisé dans une base de données ;
- Analyse du comportement d'un logiciel ;
- Reconnaissance d'un code typique d'un virus.

8 LES VLANs (Virtual Local Area Network)

Dans un réseau local la communication entre les différentes machines est régie par l'architecture physique. Grâce aux réseaux virtuels (VLANs) il est possible de s'affranchir

des limitations de l'architecture physique (contraintes géographiques, contraintes d'adressage, ...) en définissant une segmentation logique (logicielle) basée sur un regroupement de machines grâce à des critères (adresses MAC, numéros de port, protocole, etc.) donc les VLAN offrent une solution pour regrouper les stations et les serveurs en ensembles indépendants, de sorte à assurer une bonne sécurité des communications.

Côté avantages, le VLAN améliore la gestion du réseau en apportant plus de souplesse dans son administration. Il apporte davantage de sécurité en imposant, par exemple, le passage par un routeur pour la communication entre deux machines de VLANs différend. Il optimise enfin la bande passante, sépare les flux et réduit la diffusion du trafic.Il existe trois différents types de réseau local virtuel : [43]

- ✓ VLAN de niveau 1 (aussi appelé VLAN par port) ;
- ✓ VLAN niveau 2 (VLAN par adresse MAC) ;
- ✓ VLAN de niveau 3 (VLAN par adresse IP).

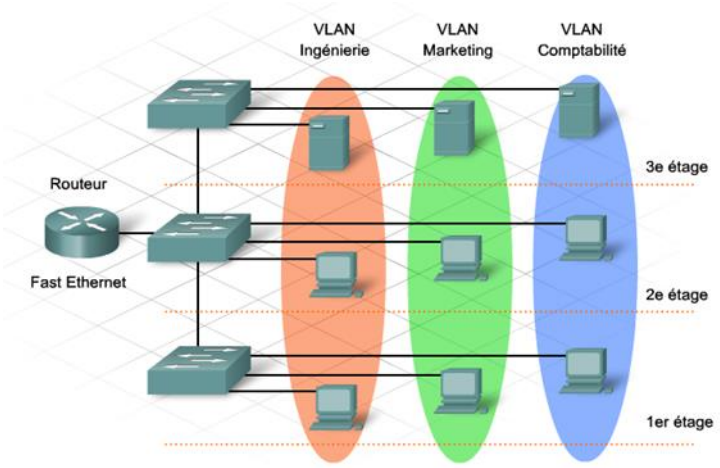

Figure 23 : exemple des Vlans.

9 VPN (virtual private network)

Un VPN est un tunnel sécurisé permettant la communication entre deux entités y compris au travers des réseaux peu sûrs comme peut l'être le réseau Internet.

Les VPNs ont pour objectif de contribuer à la sécurisation des échanges de données privées, sensible sur les réseaux publics.IL fonctionne selon un système de tunnelisation privé, c'est-à-dire qu'un tunnel est créé, à l'intérieur duquel transitent toute la communication et ou toutes les données transmises qui sont cryptées.

Un VPN est très fermé, un utilisateur non autorisé, ne peut en aucun cas avoir accès aux données transmises sur le réseau et en cas d'interceptions, les informations interceptées sont cryptées, illisibles, et donc inutilisables [43].

Le fonctionnement des VPN repose sur des technologies appelées protocoles de tunnelisation ou protocoles VPN et parmi eux nous retrouvons :

- ✓ Internet Protocol Security (IPSec).
- ✓ Layer 2 Tunneling Protocol (L2TP).
- ✓ Point-to-Point Tunneling Protocol (PPTP).
- ✓ HybridVPN.

9.1 Les principaux avantages d'un VPN

- ❖ Sécurité : assure des communications sécurisées et chiffrées
- ❖ Simplicité : utilise les circuits de télécommunication classiques.
- ❖ Economie : utilise Internet en tant que média principal de transport, ce qui évite les couts liés à une ligne dédiée.

9.2 Les contraintes d'un VPN

Le principe d'un VPN est d'être transparent pour les utilisateurs et pour les applications y ayant accès. Il doit être capable de mettre en œuvre les fonctionnalités suivantes :

- ✓ Authentification d'utilisateur : seule les utilisateurs autorisés doivent avoir accès au canal VPN.
- ✓ Cryptage des données : lors de leur transport sur le réseau public, les données doivent être protégées par un cryptage efficace.
- ✓ Gestion de clés : les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.
- ✓ Prise en charge multi protocole : la solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP.

9.3 Les différents types de VPN

9.3.1 VPN d'accès à distance

Est le plus couramment utilisé. Il connecteles utilisateurs à un serveur qui est situé dans un autre pays, ce qui leur permet de naviguer en utilisantleur propre réseau tout en partageant des données qui ont été chiffrées. Il est idéal pour un usagepersonnel et individuel. Il s'agit d'un outil particulièrement sécuritaire, car en plus de connecter lesutilisateurs à distance, il anonymise et protège les données. [44]

9.3.2 Le VPN de site à site

Est principalement dédié aux entreprises qui ont des bureaux à plusieurs endroits. Ilpermet de créer des connexions sécurisées entre différentes localisations.

Le VPN de site à site permettre d'échanger des ressources numériques de façon sécurisée. Les éléments connectés peuvent être des ordinateurs, mais également des imprimantes, des fax ou encore des webcams. Ce travail de mise en tunnel est réalisé firewalls, ce qui permet aux utilisateurs de ne pas avoir à changer de poste de travail pour entrer en communication avec un autre appareil situé à l'autre bout du monde. Il existe différents types de VPN de site à site :[44]

- **Le VPN intranet**

Ce type de VPN est principalement utilisé dans les petites entreprises. Il connecte les différents réseaux localisés (LAN) au réseau étendu (WAN), ce qui permet à l'entreprise de partager ses informations de façon privée et sécurisée entre toutes ses antennes, et ce quelle que soit leur localisation.

- **Le VPN extranet**

Le VPN extranet est principalement utilisé par les grandes entreprises qui possèdent des liens commerciaux avec des entités tierces n'ayant pas accès à l'intranet. Il permet la mise en place d'un réseau extranet protégé et sécurisé.

10 ACL (Access Control List)

Les ACL sont des règles appliquées aux trafics transitant via les interfaces du routeur que ce soit en entrée (in) ou en sortie (out). Les ACL filtrent le trafic en demandant aux interfaces d'acheminer ou non les paquets qui y transitent. Pour ce faire, le routeur lit l'en-tête de chaque paquet afin de déterminer s'il doit être acheminé ou non en fonction des conditions définies dans la liste de contrôle d'accès ACLs. Les paramètres contrôlés sont: [28]

- ✓ Adresse source;
- ✓ Adresse destination;
- ✓ Protocoleutilisé ;
- ✓ Numéro de port.

10.1 Les types d'ACL

- **Les ACL standard :** permettent d'autoriser ou de refuser le trafic en provenance d'adresse IP source et la destination du paquet, tandis que les ports n'ont aucune incidence.

- **Les ACL étendues :** filtrent les paquets IP en fonction de plusieurs attributs, dont le type de protocole, l'adresse IP source, l'adresse IP destination, les ports TCP ou UDP source et destination et les informations facultatives sur le type de protocole pour une meilleure précision du contrôle. Lors de la configuration des ACL, chaque liste est identifiée par un numéro unique attribué. Ce numéro permet d'identifie le type d'ACL créé et doit être compris dans les plages suivantes :
  - ✓ Les ACL standard : 1-99 ,1300-1999.
  - ✓ Les ACL étendues : 100-199, 2000-2699.

11 Le NAT (Network Address Translation)

Dans les entreprises de grandes tailles, différents réseaux interconnectés peuvent utiliser les mêmes adresses IP .Pour que la communication soit possible entre nœuds des deux coté, il est nécessaire de modifier les références de l'émetteur de paquets afin qu'il n'y ait pas de conflits et que la transmission soit fiable. Des équipements de translation d'adresse NAT sont chargés d'adopter cette fonctionnalité .Ils permettent le changement d'une adresse IP par une autre. Il existe trois types de traduction d'adresses:[28]

- **NAT statique** : traduit une adresse IP privée en une adresse publique. L'adresse IP publique est toujours la même.
- **NAT dynamique** : les adresses IP privées sont mappées au pool d'adresses IP publiques.
- **Traduction d'adresse de port (PAT)** : une adresse IP publique est utilisée pour tous les périphériques internes, mais un port différent est attribué à chaque adresse IP privée. Également connu sous le nom de surcharge NAT.

12 Les dispositifs de protection

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 des dispositifs de protection et cela permettre d'ajouter une autre couche de sécurité au réseau.

12.1 Système pare-feu (Firewall)

Un firewall ou pare-feu est un appareil de sécurité réseau qui surveille le trafic réseau entrant et sortant et autorise ou bloque les paquets de donnés en se basant sur un ensemble de règles de sécurité.

Il est chargé de dresser une barrière entre le réseau interne et le trafic entrant provenant de sources externes (comme Internet) afin de bloquer le trafic malveillant des virus et des pirates. [46]

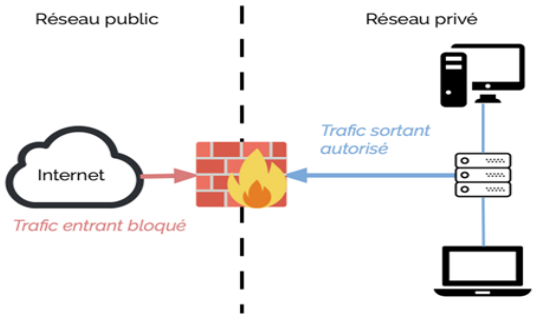

Figure 24 : Firewall.

12.1.1 **Principe de fonctionnement**

Un système pare-feu contient un ensemble de règles prédéfinies permettant : [47]

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

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

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

La première méthode est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

12.1.2 **Les déférents types de filtrage de paquets**

- **Le filtrage simple de paquet (Stateless)**

C'est la méthode de filtrage la plus simple, elle opère au niveau de la couche réseau et transport du modèle OSI. La plupart des routeurs d'aujourd'hui permettent d'effectuer du filtrage simple de paquet. Cela consiste à accorder ou refuser le passage de paquet d'un réseau à un autre en se basant sur : [48]

- L'adresse IP Source/Destination.
- Le numéro de port Source/Destination.
- Et bien sur le protocole de niveaux 3 ou 4.

Cela nécessite de configurer le Firewall ou le routeur par des règles de filtrages, généralement appelées des ACL (Access Control Lists).

❖ **Le filtrage dynamique (Stateful)**

Cette technique a été proposée pour pallier aux certaines limites de pare-feu utilisant le filtrage simple. L'idée est de conserver les traces de sessions et de connexions dans des tables d'états internes aux pare-feu. Ces traces seront également prises en considération par les pare-feu lors de prise de décisions. Ces informations augmentent considérablement les capacités des pare-feu à détecter des attaques sophistiquées. Il reste, cependant que les failles applicatives (les failles liées aux logiciels), qui sont à l'origine de la plus grande majorité de problèmes de sécurité, pour ce type de filtrage.[48]

❖ **Le filtrage applicatif (pare-feu de type proxy)**

Il a été proposé comme étant une amélioration supplémentaire du filtrage dynamique. Ce mécanisme est attaché au niveau de la couche application, où il peut extraire les données du protocole de niveau 7 pour les étudier. Le filtrage applicatif suppose une connaissance des protocoles utilisés par chaque application. Il permet la destruction des en-têtes précédant le message applicatif, ce qui permet de fournir un niveau de sécurité supplémentaire. [48]

12.1.3 **Les différents types de firewall**

12.1.3.1 ***Les Firewall Bridge***

Ces derniers sont relativement répandus. Ils agissent comme de vrais câbles réseau avec la fonction de filtrage en plus, d'où leur appellation de firewall. Leurs interfaces ne possèdent pas d'adresse IP, et ne font que transférer les paquets d'une interface a une autre en leur appliquant les règles prédéfinies. Cette absence est particulièrement utile, car cela signifie que le firewall est indétectable pour un hacker.

En effet, quand une requête ARP est émise sur le câble réseau, le firewall ne répondra jamais. Ses adresses Mac ne circuleront jamais sur le réseau, et comme il ne fait que « transmettre » les paquets, il sera totalement invisible sur le réseau. Cela rend impossible toute attaque dirigée directement contre le firewall, ces firewalls se trouvent typiquement sur les Switchs.

Avantages	Inconvénients
✓ Impossible de l'éviter (les paquets passeront par ses interfaces) ; ✓ Peu coûteux.	✓ possibilité de le contourner (il suffit de passer outre ses règles) ; ✓ Configuration souvent contraignante ; ✓ Les fonctionnalités présentes sont très basiques (filtrage sur adresse IP, port, le plus souvent en Stateless).

Tableau 2 : Avantages & inconvénients de Firewall bridge.

12.1.3.2 *Les Firewallsmatériels*

Est un périphérique physique installé à l'entrée et à la sortie du réseau local, il garantit davantage de protection en terme de sécurité. Cette solution est notamment privilégiée pour les réseaux comportant plusieurs ordinateurs, par exemple dans le cadre de sociétés privées (le pare-feu matériel se révèle alors moins onéreux qu'un pare-feu logiciel, et il assure une plus grande protection pour le réseau).

Avantages	Inconvénients
✓ Intégré au materiel réseau; ✓ Administration relativement simple; ✓ Bon niveau de sécurité.	✓ Dépendant du constructeur pour les mises à jour. ✓ Souventpeu flexibles.

Tableau 3:Avantages & inconvénients de Firewall matériels.

12.1.3.3 *Les Firewalls logiciels:*

Présents à la fois dans les serveurs et les routeurs « faits maison », on peut les classer en plusieurs catégories :

❖ **Les Firewalls personnels:**

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

Avantages	Inconvénients
✓ Sécurité en bout de chaîne (le poste client) ; ✓ Personnalisable assez facilement.	✓ Facilement contournable; ✓ Difficiles à départager de par leur nombre énorme.

Tableau 4 : Avantages & inconvénients de firewall matériels.

❖ **Les firewalls plus « sérieux »**

Tournant généralement sous linux, car cet OS offre une sécurité réseau plus élevée et un contrôle plus adéquat, ils ont généralement pour but d'avoir le même comportement que les firewalls matériels des routeurs, à ceci près qu'ils sont configurables à la main.

Avantages	Inconvénients
✓ Personnalisables; ✓ Niveau de sécurité très bon.	✓ Nécessite une administration système supplémentaire

Tableau 5 :Avantages&inconvénients d'un Firewall plus sérieux.

12.1.4 **Types d'architectures**

Pour assurer une meilleure sécurité du réseau, il est important de mettre en place plusieurs filtres de différents niveau0x, mais il s'accompagne d'un cout plus élevé. [31]

12.1.4.1 ***Firewall avec routeur de filtrage***

La solution Firewall la plus simple, mais aussi la moins sure, se borne au réseau. On l'obtient en configurant le routeur qui assure la connexion avec l'Internet. Cette solution permet de réaliser les différents serveurs d'un Intranet sur plusieurs systèmes.

Le routeur de filtrage contient les autorisations d'accès basées exclusivement sur les adresses IP et les numéros de port.

Figure 25 : Firewall avec routeur de filtrage.

Avantages	Inconvénients
✓ facilité de configuration ; ✓ peu coûteux.	✓ lorsque le routeur est contourné ou paralysé, le réseau entier est ouvert.

Tableau 6 : les avantage & inconvénients de firewall avec routeur de filtrage.

12.1.4.2 ***Passerelle double- le réseau bastion***

Il s'agit d'un ordinateur inclus à la fois dans les deux réseaux Internet et Intranet. Cette machine doit être équipée de deux cartes réseau. Comme elle est la seule soupape de sécurité entre les deux réseaux, elle doit être configurée avec le plus grand soin.

La passerelle double n'autorise aucun trafic IP entre les réseaux. On l'appelle également réseau bastion, car il contrôle tous les services accessibles de l'extérieur comme de l'intérieur du réseau interne tels que les serveurs Web, FTP et Mail.

Un " serveur Proxy " supplémentaire est également configuré pour permettre aux utilisateurs du réseau interne d'accéder à Internet. Le nom "réseau bastion" découle des mesures particulières de protection qui sont prises en prévision de possibles intrusions.

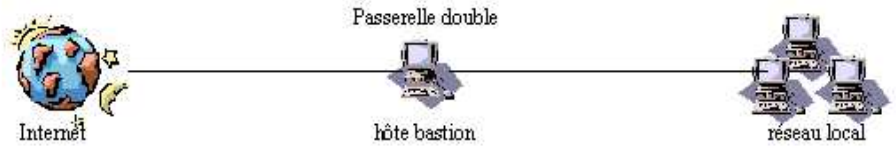

Figure 26 : La passerelle double.

Avantage	Inconvénients
✓ Bon marché.	✓ La configuration pourra rencontrer des problèmes de performances et cela est dû aux taches qu'elle doit faire (routage et application)

Tableau 7 : Avantages& inconvénients de passerelle double.

12.1.4.3 ***Firewalls avec réseau de filtrage***

La combinaison des deux méthodes est ici plus sûre et efficace. Au niveau du réseau, un routeur sous écran est configuré de façon à n'autoriser les accès de l'extérieur et de l'intérieur que par l'intermédiaire du réseau bastion sur lequel fonctionnent tous les serveurs assurant les serveurs Internet.

Pour la grande majorité des entreprises, cette solution est sûre et abordable, car les prestataires Internet assurent la seconde partie de la protection à l'autre bout de la ligne. En effet, l'entreprise y est également connectée à un routeur, et le trafic de données est réglé par un serveur Proxy au niveau de la couche application. Les pirates doivent par conséquent franchir deux obstacles.

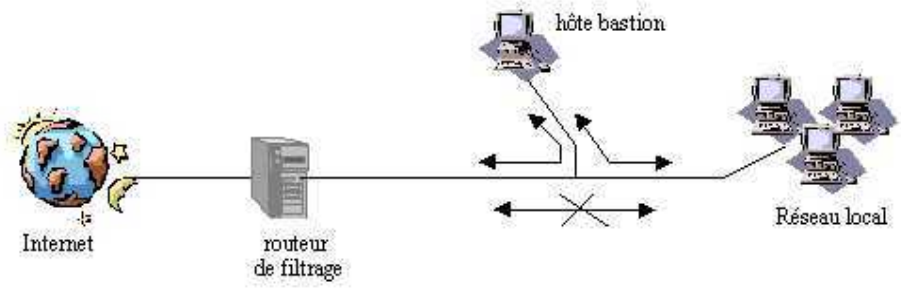

Figure 27 : Firewalls avec réseau de filtrage.

Avantage	Inconvénients
✓ bon marché et sûr lorsque le prestataire est équipé en conséquence.	✓ le système comporte deux sécurités distinctes, le routeur et le réseau bastion, Si l'une des deux est paralysée, le réseau est menacé dans son intégralité.

Tableau 8 : Avantages & inconvénients Firewalls avec réseau de filtrage.

12.1.4.4 ***Firewall avec sous-réseau de filtrage***

Cette solution est de loin la plus sûre, mais également la plus onéreuse. Un Firewall avec sous-réseau de filtrage se compose de deux routeurs sous écran. L'un est connecté à Internet, et l'autre à l'intrant. Plusieurs réseaux bastions peuvent s'intercaler pour former entre ces deux routeurs, en quelque sorte, leur propre réseau constituant une zone tampon entre un Intranet et l'Internet appelée zone démilitarisée.

De l'extérieur, seul l'accès aux réseaux bastions est autorisé. Le trafic IP n'est pas directement transmis au réseau interne.

De même, seuls les réseaux bastions, sur lesquels des serveurs Proxy doivent être en service pour permettre l'accès à différents services Internet, sont accessibles à partir du réseau interne.

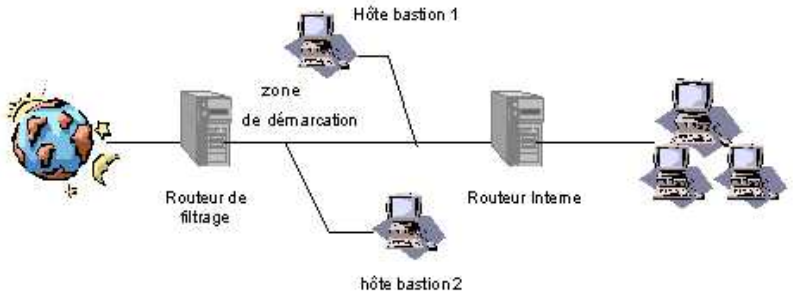

Figure 28 : Firewall avec sous-réseau de filtrage.

Avantage	Inconvénients
✓ système Firewall très sûr.	✓ coût d'investissement élevé, effort administratif important.

Tableau 9 : Avantages & inconvénients Firewalls avec réseau de filtrage

12.1.5 **La zone Démilitarisée (DMZ)**

En sécurité informatique, une zone démilitarisée (ou DMZ) fait référence à un sous-réseau qui héberge les services exposés et accessibles de l'extérieur d'une entreprise. Elle agit comme une zone tampon avec les réseaux non sécurisés tels qu'Internet.

Les DMZ ont pour objectif de renforcer le niveau de sécurité du réseau local de l'entreprise. Dans ce système, un nœud de réseau protégé et surveillé, tourné vers l'extérieur, a accès aux éléments exposés au sein de la zone dématérialisée tandis que le reste du réseau estprotégé par un pare-feu. Lorsqu'elles sont correctement mises en œuvre, les DMZ aident les entreprises à détecter et corriger les failles de sécurité avant qu'elles n'atteignent le réseau interne, où sont stockées les ressources les plus précieuses. [50]

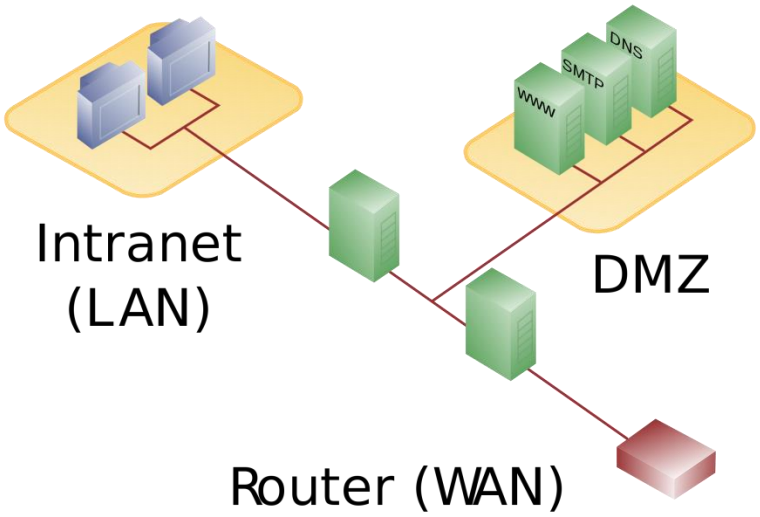

Figure 29 : DMZ.

La politique de sécurité mise en œuvre sur la DMZ est généralement la suivante :

- Trafic du réseau externe vers la DMZ autorisé ;
- Trafic du réseau externe vers le réseau interne interdit ;
- Trafic du réseau interne vers la DMZ autorisé ;
- Trafic du réseau interne vers le réseau externe autorisé ;
- Trafic de la DMZ vers le réseau interne interdit ;
- Trafic de la DMZ vers le réseau externe interdit.

12.2 **Serveurs mandataire (Proxy)**

Un système mandataire repose sur un accès à l'internet par une machine dédiée: le serveur mandataire ou Proxy server joue le rôle de mandataire pour les autres machines locales, et exécute les requêtes pour le compte de ces dernières.

Un serveur mandataire est configuré pour un ou plusieurs protocoles de niveau applicatif (http, FTP, SMTP, etc.) et permet de centraliser, donc de sécuriser, les accès extérieurs (filtrage applicatif, enregistrement des connexions, masquage des adresses des clients, etc.).

Les serveurs mandataires configurés pour http permettent également le stockage de pages web dans un cache pour accélérer le transfert des informations fréquemment consultées vers les clients connectés. [43]

Figure 30 : proxy.

12.3 **Principe de fonctionnement**

Le principe de fonctionnement 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 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. [5]

13 Conclusion

A la fin de chapitre nous tenons à conclure que malgré les différentes mécanismes de sécurité qui se traduise en : Les systèmes de détection d'intrusion (IDS), Systèmes de prévention d'intrusion (IPS), La cryptographie, Les protocoles, La signature, LES Vlans, VPN, ACL, Le NAT, Système pare-feu, Serveurs mandataire.

La politique de sécurité reste un enjeu qui est difficile à résoudre à cause des hackers qui ne cessent pas de développé des méthodes de pénétration au système ce qui nous met dans l'obligation à notre tour de développé de fur et à mesure de nouvelle technique de sécurité.

CHAPITRE IV : CONCEPTION ET MISE EN ŒUVRE

1 Introduction

Dans ce chapitre nous allons nous intéresser à la sécurité d'un réseau d'entreprise, en commençant par trouver les failles de celui-ci. A partir de là nous proposerons des solutions et l'implémenter pour améliorer la sécurité de ce réseau.

2 L'entreprise CETIM

Le CETIM est l'abréviation de « Le Centre d'Etudes et de services Technologiques de l'Industrie des Matériaux de construction ». C'est le centre technique algérien de l'industrie produisant les matériaux tels que le ciment, les bétons, les chaux et plâtre, les briques tuiles et céramiques.

3 L'organisation interne du CETIM

Le CETIM dispose essentiellement :

- D'une infrastructure (4 bâtiments).
- De 10 laboratoires de traitement, d'essais et analyses (8 opérationnels 1 en développement et 1 en projet).
- D'équipes multidisciplinaires (55 ingénieurs et 42 Techniciens) assurant les prestations d'études et d'expertises.

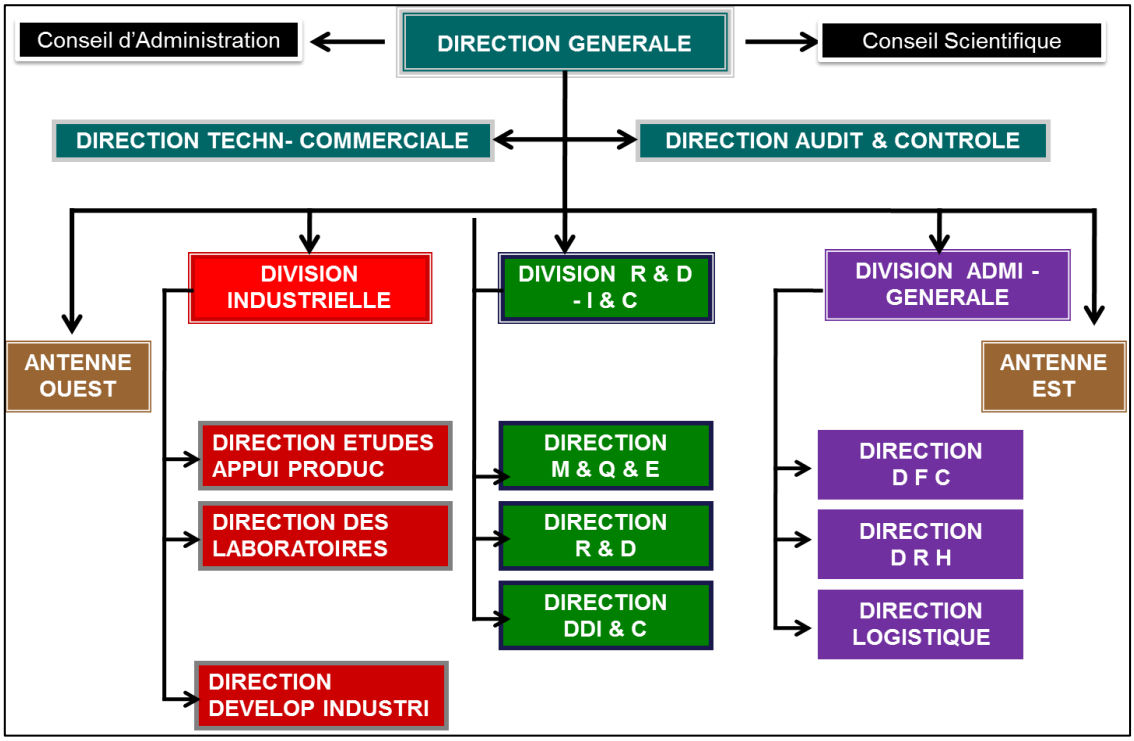

Figure 31 : Organisation interne de l'entreprise.

4 Partie I : Etude de réseau existant

4.1 Topologie existante

Le Réseau Local Du CETIM, Se Compose De :

- ✓ Deux (02) Serveurs HPE Dl380.
- ✓ Cinq Armoires De Brassage.
- ✓ Un Router Cisco 2951.
- ✓ Cinq (05) Switch Cisco 24 Ports.
- ✓ Deux Switch Cisco 48 Ports.
- ✓ 184 Postes De Travail Connecté Au Réseau.

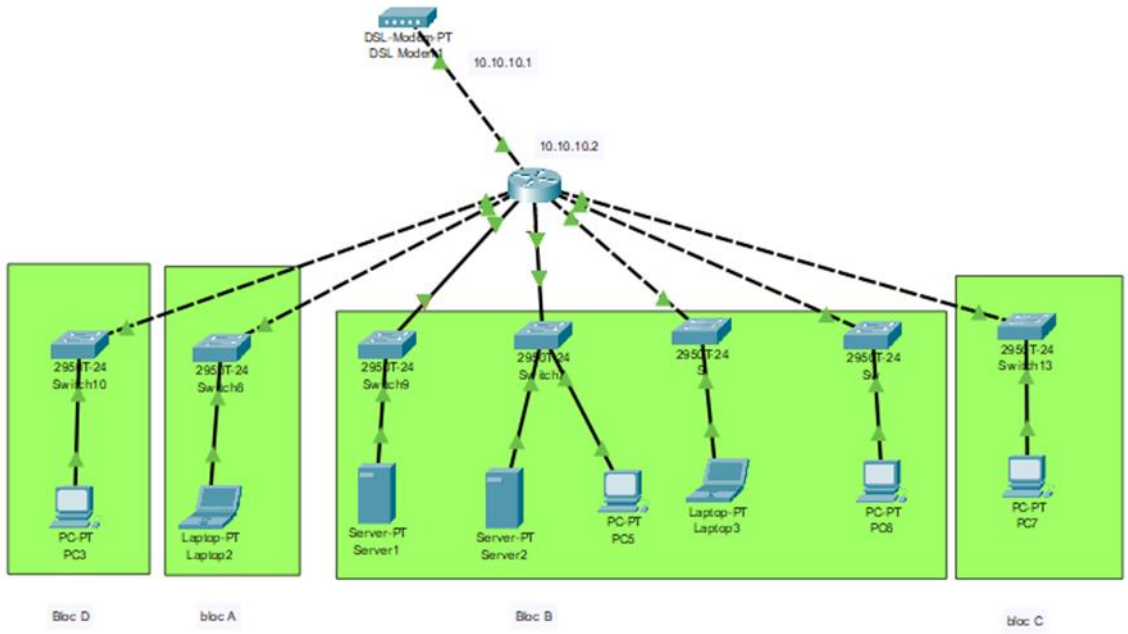

Figure 32 : Topologie existante du réseau actuelle.

4.2 Les critiques du réseau existant

Une analyse du réseau de l'entreprise, nous a permis de définir un nombre de contraintes pouvant réduire ces performance voir même sa dégradation, certaine de ces contraintes peuvent être un obstacle à la réalisation de la mission de cette entreprise.

- ✓ Les seuls systèmes de sécurité utilisée sont des antivirus installés sur les machines.
- ✓ Le réseau est non sécurisé contre les intrusions d'une façon fiable.
- ✓ Absence de système de défense L'inexistence d'un firewall, ou d'un proxy pour restreindre le trafic entrant et sortant du réseau peut causer l'infiltration d'un paquet malveillant.
- ✓ Aucun système de protection contre la divulgation de donné interne.

- ✓ Point unique de défaillanceL'architecture est composée d'un seul routeur dont dépend tout le réseau. Une simple panne de celui-ci engendrerait la coupure de communication entre les clients et les serveurs à l'échelle LAN,

4.3 Solution proposé

L'objectif de notre projet est de proposer des solutions afin de renforcer la politique de Sécurité du réseau local après l'issue d'une étude préalable de réseau existant nous proposons d'implémenter un firewall « pfsense » afin de filtrer le flux de données traversant le réseau.

4.4 Présentation de l'outil pfSense

pfSense est un système d'exploitation open source ayant pour but la mise en place de routeur/pare-feu basé sur le système d'exploitation FreeBSD. Très fréquemment rencontré dans les PME et les petites structures.

pfSense offre une solution complète de routage, filtrage, VPN et partage de connexion et intègre un grand nombre de composants tiers : serveur DHCP/DNS, serveur de temps, proxy web, monitoring... etc. La configuration se fait entièrement via une interface web et elle recommande au minimum:

- ✓ Cartes réseaux
- ✓ Disque dur de 60Go.
- ✓ Mémoire vive de 2 Go.

4.5 Pourquoi utiliser le pare-feu pfsense

- ❖ pfSense est une solution open source.
- ❖ Ils se révèlent être un élément clé qui contribue très largement à améliorer la sécurité des systèmes d'informations.
- ❖ Le pare-feu protège la totalité du trafic réseau et a la capacité d'identifier et de bloquer le trafic indésirable.
- ❖ Simplicité de l'activation /désactivation des modules de filtrage.
- ❖ Des fonctionnalitésde réseaux avancés.

4.6 Nouvelle topologie réseau en utilisant le pare-feu pfsense :

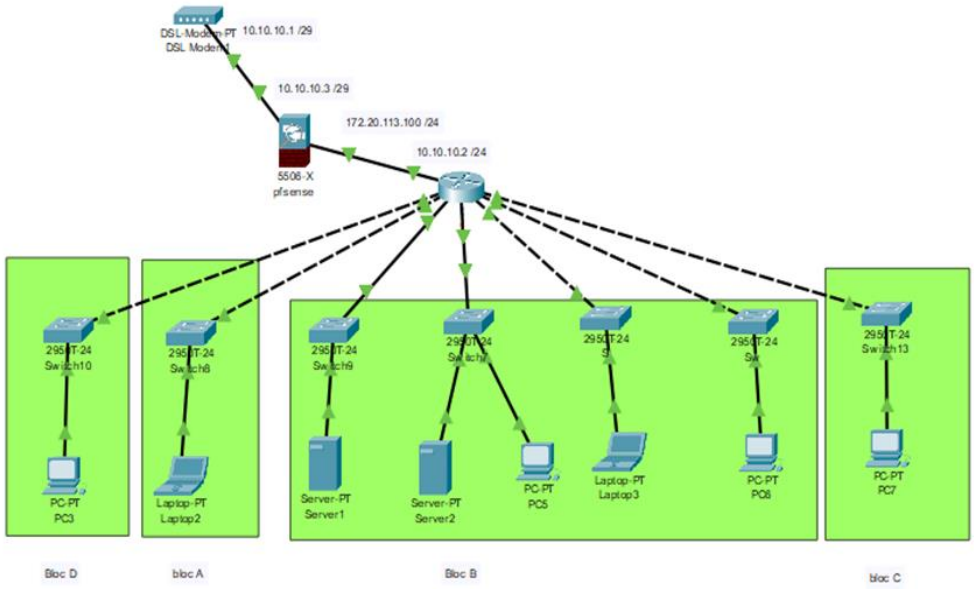

Figure 33 : Nouvelle architecture en utilisant le pare-feu pfsense.

5 Partie II : implémentation de solution

5.1 Environnement de travail

Le travail a été effectué sur une machine physiques comporte Caractéristiques techniques :

- ✓ Modèle : HP 280 G2
- ✓ Processeur : Intel®Core™ i5-6400 2,4 GHz
- ✓ RAM : 4 Go DDR4
- ✓ Disque dur : 500 GO

5.2 Les étapes d'installation de Pfsense

1. Télécharger l'image ISO Pfsense

Pour faire fonctionner pfsense nous avons besoin d'une image iso de 64 bits que vous pouvez télécharger sur le lien suivant :

https://www.pfsense.org/download/mirror.php?section=downloads.

2. Installation de Pfsense

- Effectuez le démarrage de l'ordinateur
- à l'aide du support d'installation Pfsense. Sur l'écran de bienvenue, appuyez sur Entrée pour démarrer le processus d'installation de Pfsense

Figure 34 : L'écran de bienvenue pfsense

- Acceptez le contrat de licence utilisateur final pfsense.

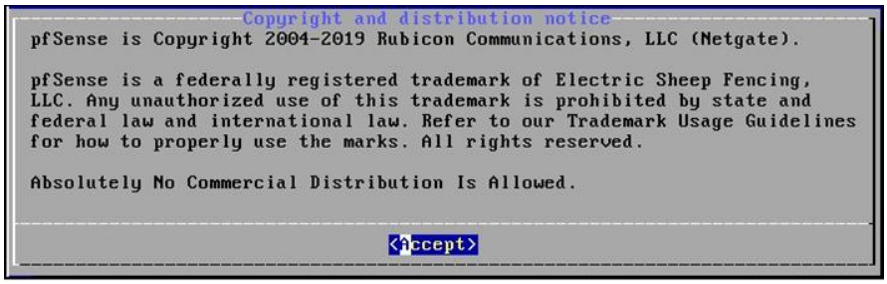

Figure 35 : Licence pfsense.

- Sélectionnez l'option Installer sur l'écran d'accueil

Figure 36 : Installation pfsense.

- Sélectionnez la disposition de clavier Pfsense souhaitée.

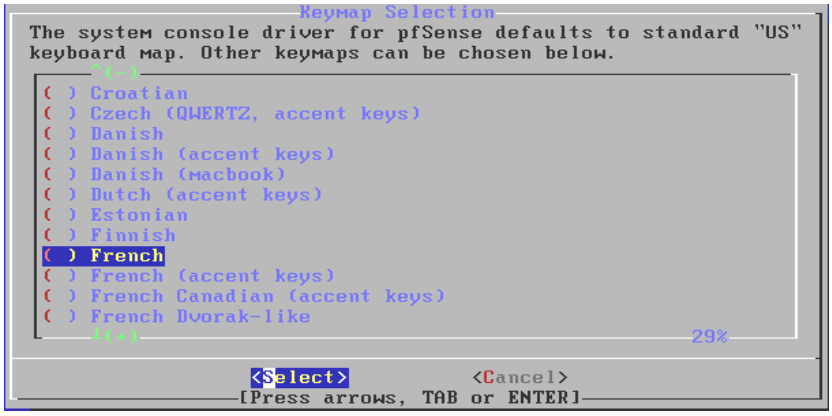

Figure 37 : Disposition de clavier Pfsense.

- Sélectionnez l'option Auto (UFS) pour effectuer automatiquement le partitionnement du disque.

Figure 38: Partitionnement du disque.

- Après que le système termine l'installation du serveur Pfsense en sélectionne l'option Non pour configuration manuel puis retirez le support d'installation et appuyez sur Entrée pour redémarrer l'ordinateur.

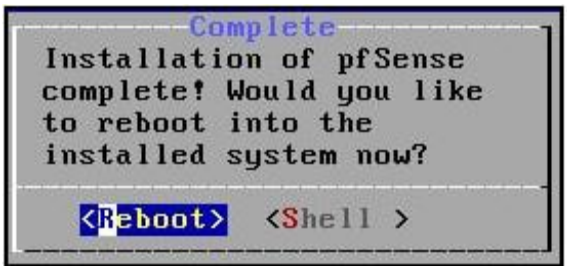

Figure 39 : Rebooter.

- Une fois que le démarrage est finalisé et après avoir sélectionné les interfaces réseau souhaitées, le menu d'installation de Pfsense sera présenté. On voit bien nos deux interfaces réseaux (WAN et LAN). On voit également que l'interface WAN a bien récupéré une adresse IP automatiquement depuis un DHCP [10.10.10.3/29]. Concernant le LAN, il attribue une adresse statique par défaut [192.168.1.1/24].

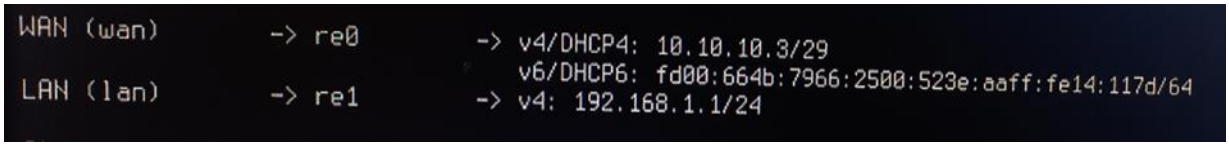

Figure 40 : Adressage d'interfaces par défaut.

3. Configuration des cartes réseau :

- Dans notre cas « **re0** » correspond à l'interface WAN par contre « **re1** » correspond à l'interface LANqu'il faudra configurer.

  En a configuré l'interfaces LAN selon les étapes suivant :

  - Modifier l'adresse IP et le masque sous réseau pour l'intégrer le Pfsense à notre réseau selon l'adresse [**172.20.113.100 /24**].
  - serveur DHCP qui porte une plage d'adressage [**172.20.113.101** jusqu'à **172.20.113.254**].
  - activez le retour à http en tant que protocole de configuration Web.

Figure 41 : Carte réseaux configuré.

4. Configuration de Pfsense

- Donc les deux cartes sont configurées. Nous pouvons accéder au Pfsense à partir d'une interface Web qui se trouve dans la machine client en utilisant l'adresse IP de LAN, Admin pour (username) et pfsense pour (password).

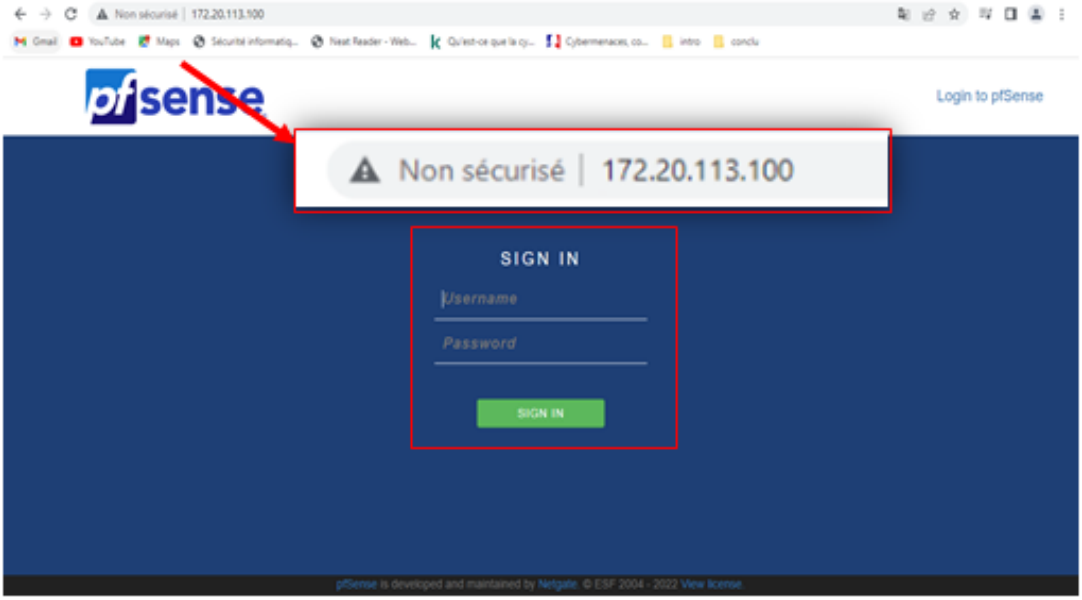

*Figure 42 :*l'interface web de PFSense.

5. Assistant d'installation de PFSense

- L'assistant de configuration de pfsense nous permettre de finaliser l'installation de notre firewall. Au niveau de la partie des **informations générales**, on a modifié le **nom du firewall** et déclarer **nom de domaine de CETIM** ainsi que **un serveur DNS local** qui porte l'adresse IP **[172.20.113.12]**.

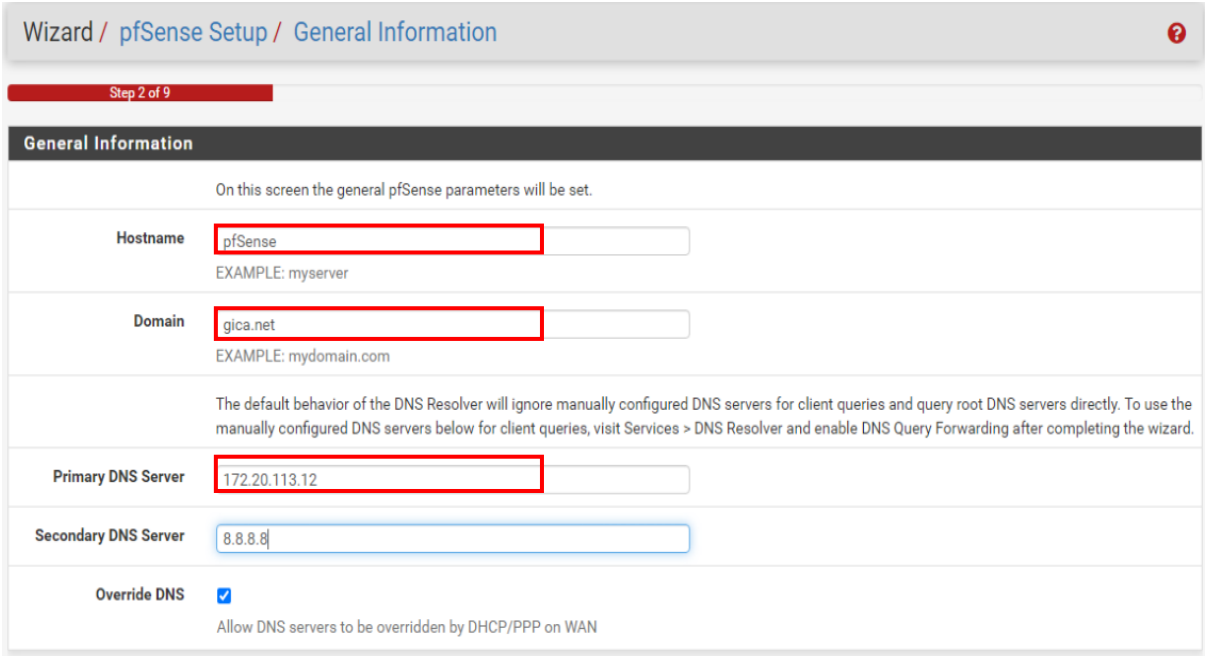

Figure 43 : Information générale.

- Ensuite nous arrivons à la configuration de l'interface WAN. pour cette partie en a juste décoché Les deux dernières options de cette page définissent que tout trafic entrant sur l'interface WAN et venant d'une classe d'adresse réseau privé est automatiquement bloqué.

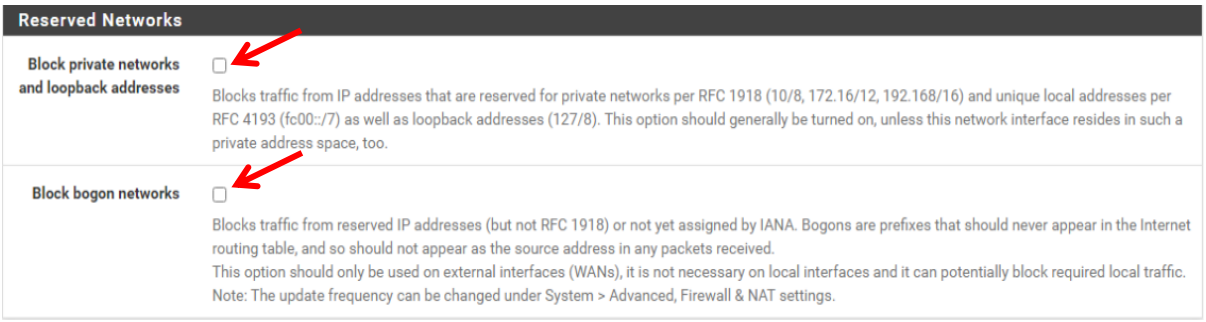

Figure 44 : Modification des règles de l'interface WAN.

- Pour finalisé cette installation il est également nécessaire de changer les identifiants par défaut du compte admin de pfsense.Après cette étape en sur le tableau de bord de

pfsense. Ou en retrouve les infos sur l'utilisation des ressources de la machine elle-même, ses différentes adresses IP, sa version et ses mises à jour si nécessaire …etc.

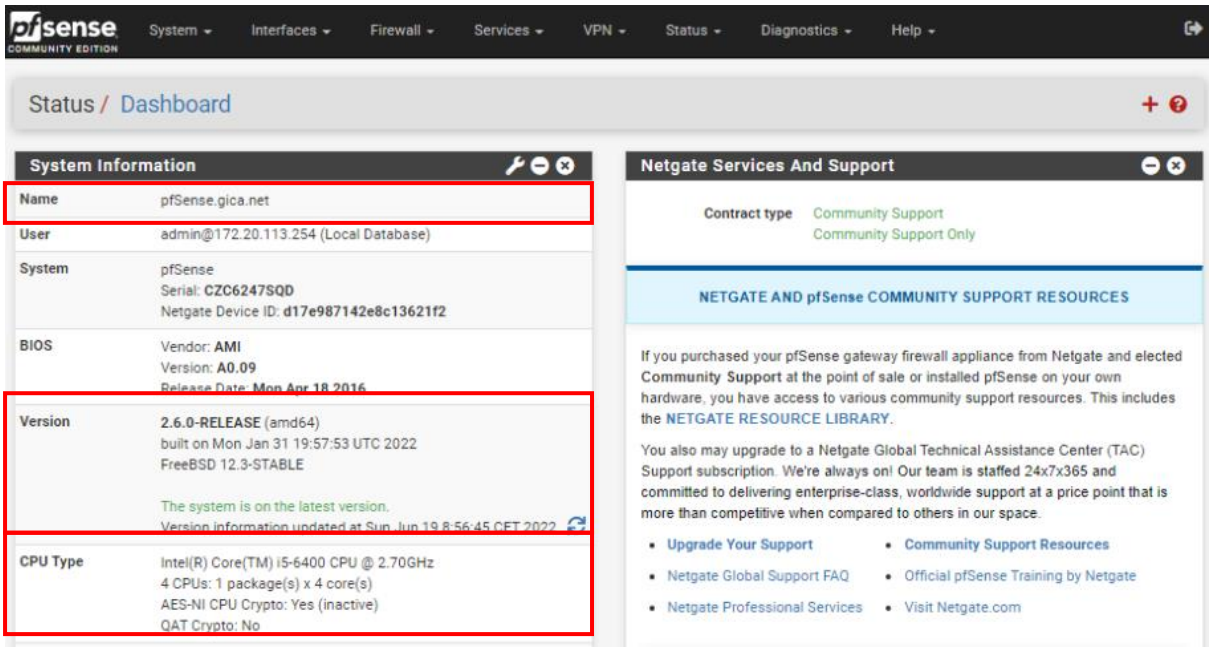

Figure 45 : Tableau de bord de pfsense.

- Pour assurer la bonne mise en place de firewall pfsense en a effectuer un test de **ping** vert les deux interfaces LAN et WAN de pfsense et un **trace route** vert www.google.com

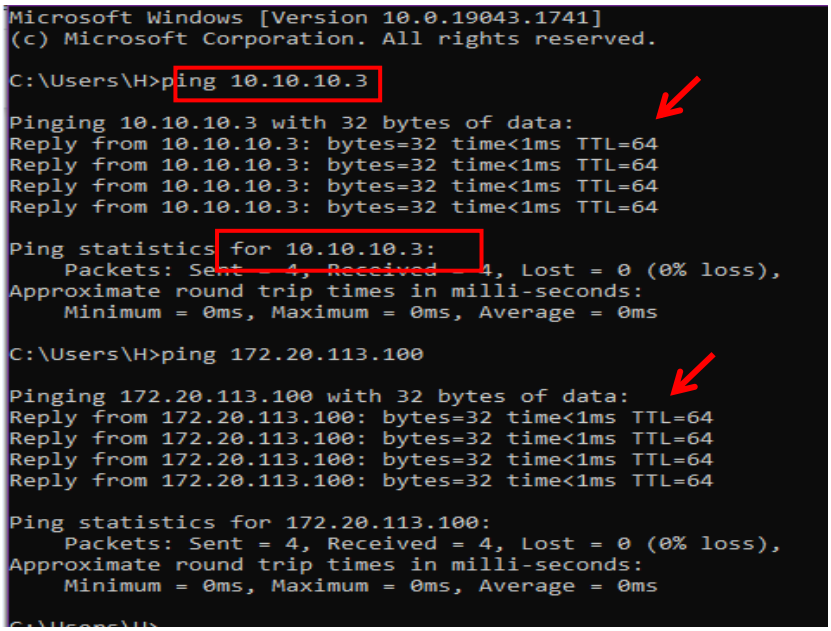

Figure 46 : Test de ping.

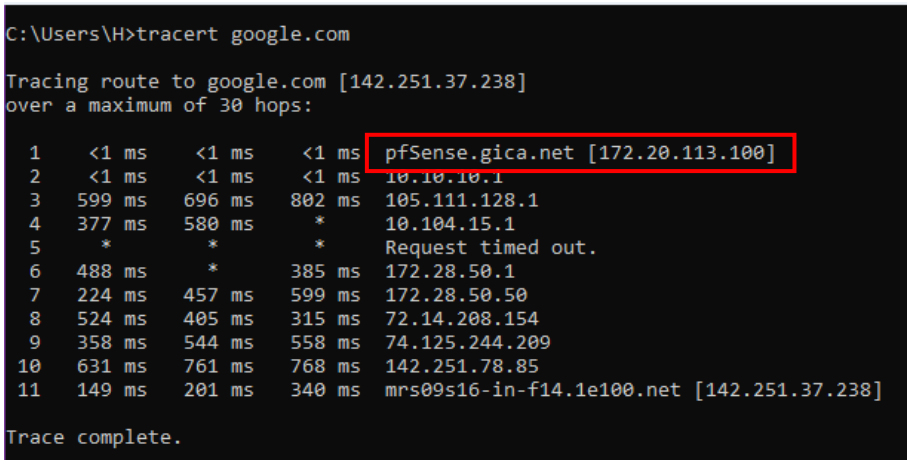

Figure 47 : Trace route Google.

6 Paramétrage avancé

6.1 Le filtrage par alias

1. Qu'est-ce qu'un alias ?

Un alias permet de définir un groupe de ports réseaux, d'hôtes ou de sous-réseaux. Ces alias peuvent ensuite être utilisés dans les règles de filtrage, les règles de redirection de ports, les règles de NAT, etc. Utiliser des alias est une bonne pratique pour disposer de règles claires, courtes, simples et lisibles sur notre firewall. Dans notre cas en veut autoriser tous le réseau a un accès illimité à l'internet sauf aux réseaux sociaux exemples Facebook pour réaliser ce filtrage en passe par deux étapes :

a) Création des alias

- Pfsense permet de créer des alias sur chaque interface (LAN etWAN), Paramétrer les alias dans l'onglet Firewall aliases et pour ajouter des alias, sur « **Add** » pour l'ajouter.
- Au niveau de la partie paramétrage de l'alias en a modifié le nom, le type de l'alias sur « **network** » qui nous a permettre d'ajouté une adresse IP qui correspond à l'adresse deping vert Facebook.

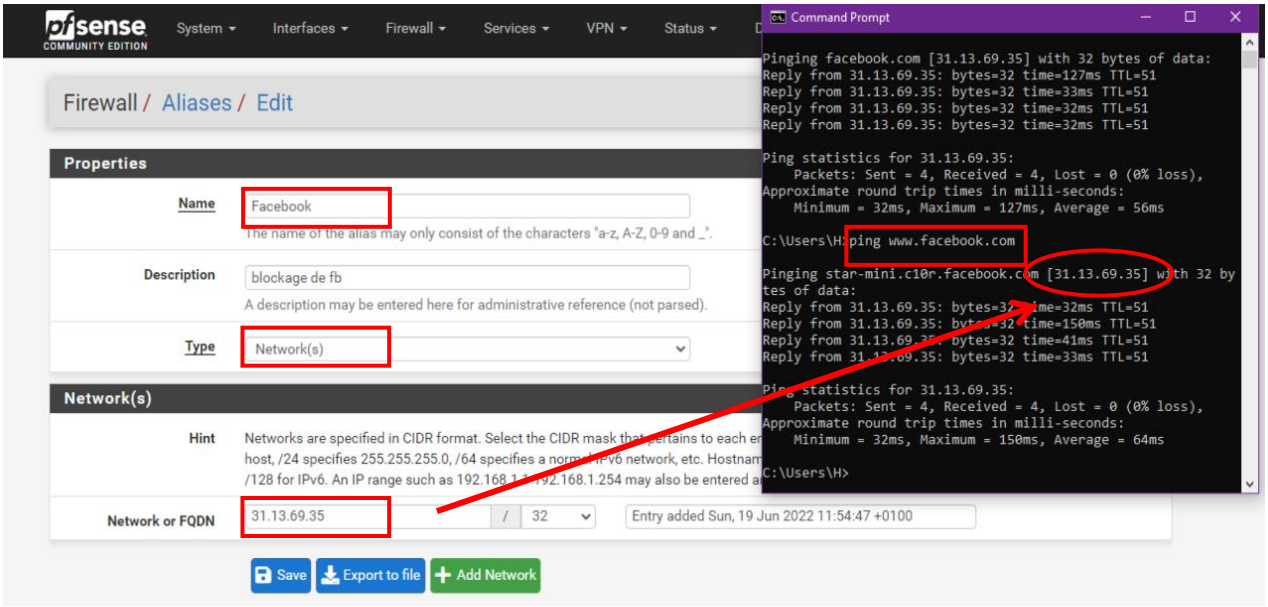

Figure 48 : Création des alias.

b) Les règles de filtrages

Elles permettent d'autoriser ou de bloquer des requêtes en provenance de LAN, Pour ajouter Une nouvelle règle, Tout d'abord rendez-vous dans **Firewall** => **Rules** => **l'interfaceLANv** puit **Add** .Il y'a plusieurs actions qui peuvent être appliquées sur la règle :

- ✓ Block : Détruit le paquet sans retour vers la source ;
- ✓ Reject : Un retour est effectué vers la source disant qu'il est refusé ;
- ✓ Pass : Accepte le paquet.

- Dans notre cas nous choisirons l'action **reject**et le protocole **Any**

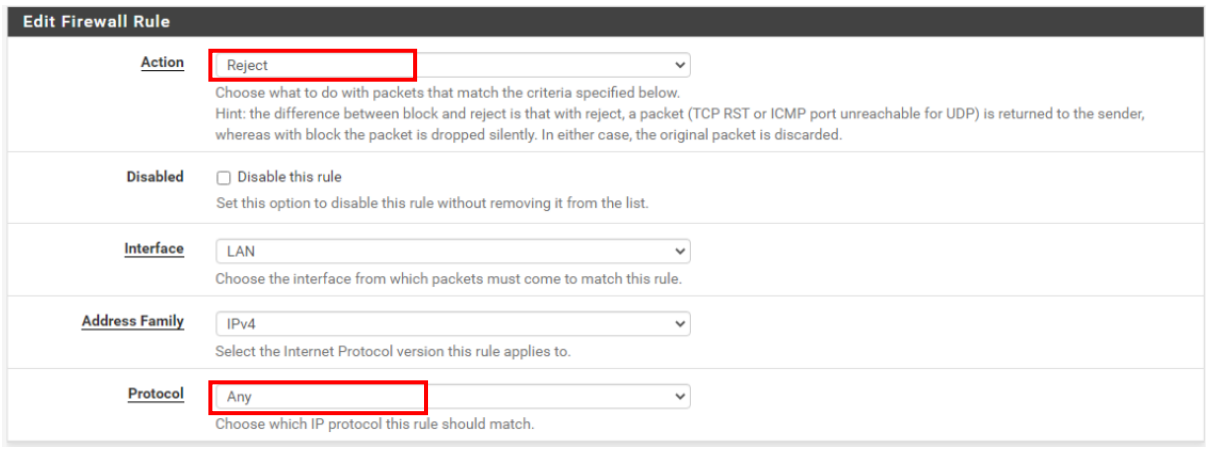

Figure 49 : paramétrage de Règle de filtrage.

- On modifie la destination a «**single host or alias** » et récrire le nom de alias crée au début « **Facebook** ».

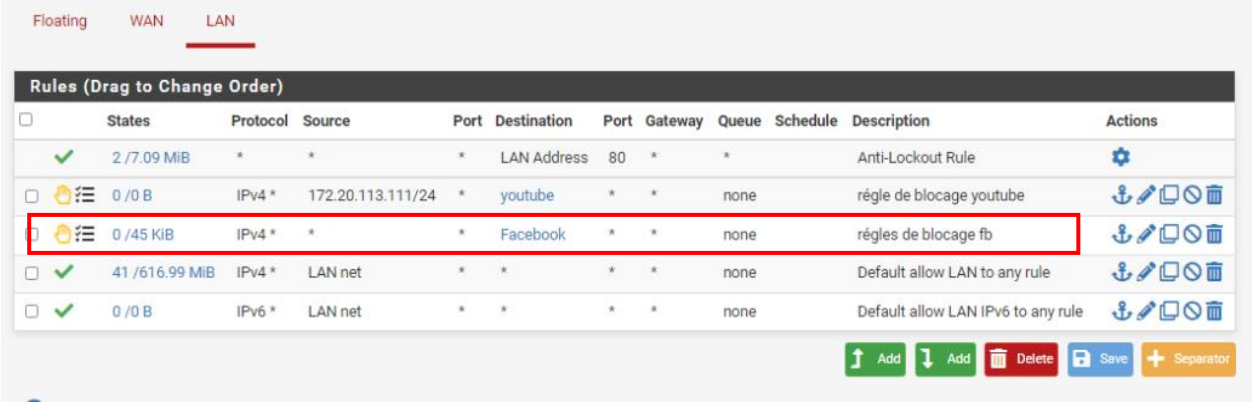

Figure 50 : Règle de filtrage.

2. Le test

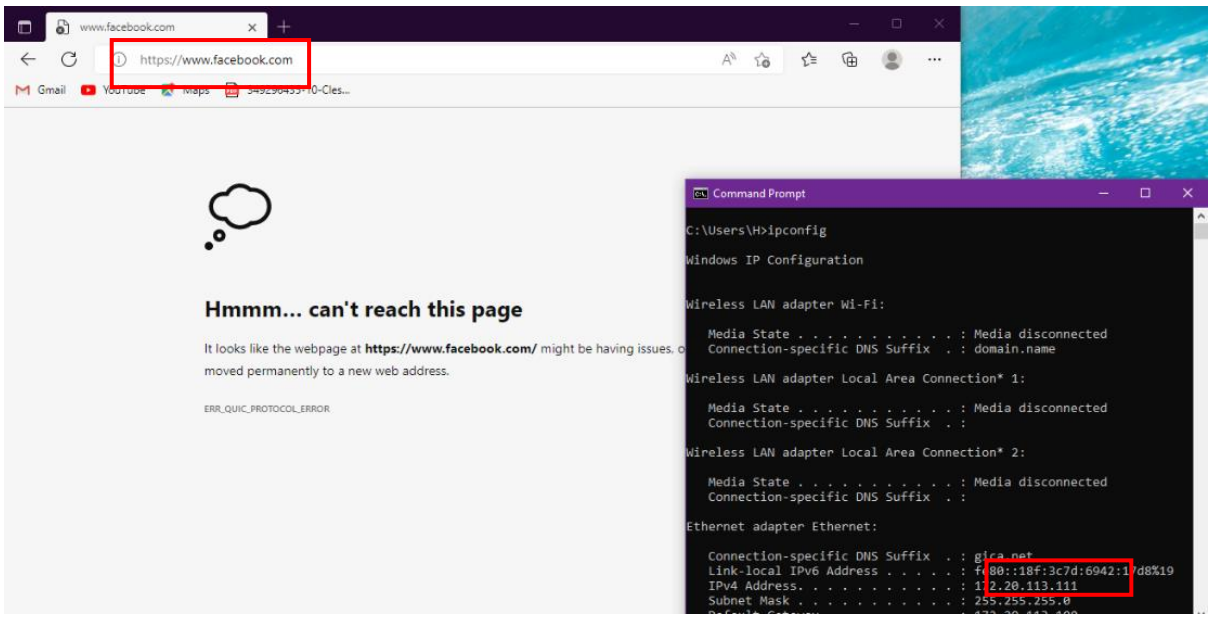

Figure 51 : Test Facebook.

6.2 Filtrage basé sur IP/DNS

Pour cette réalisation en a utilisé le package**pfBlockerNG** qu'il permet d'étendre la fonctionnalité principale du Firewall de pfSense en permettant aux utilisateurs de contrôler et de gérer l'accès entrant et sortant via le pare-feu à l'aide de listes de contrôle IP et DNS.

pfBlockerNG donne au logiciel pfSensela possibilité de offrir un filtrage avancé en prendre des décisions d'autorisation/de refus basées sur des éléments tels que la géolocalisation d'une adresse IP, le nom de domaine d'une ressource…etc.

Notre objectif de cette réalisation et de bloquer l'accès au réseau sociaux dans notre exemple Facebook à partir de leur **AS** (système autonome).

a) Installation et configuration de pfBlockerNG

- Tout d'abord en accèdeeaux packages disponibles sur l'interface graphique du pfSenspuis recherche le package « **pfBlockerNG »** puis l'installer.

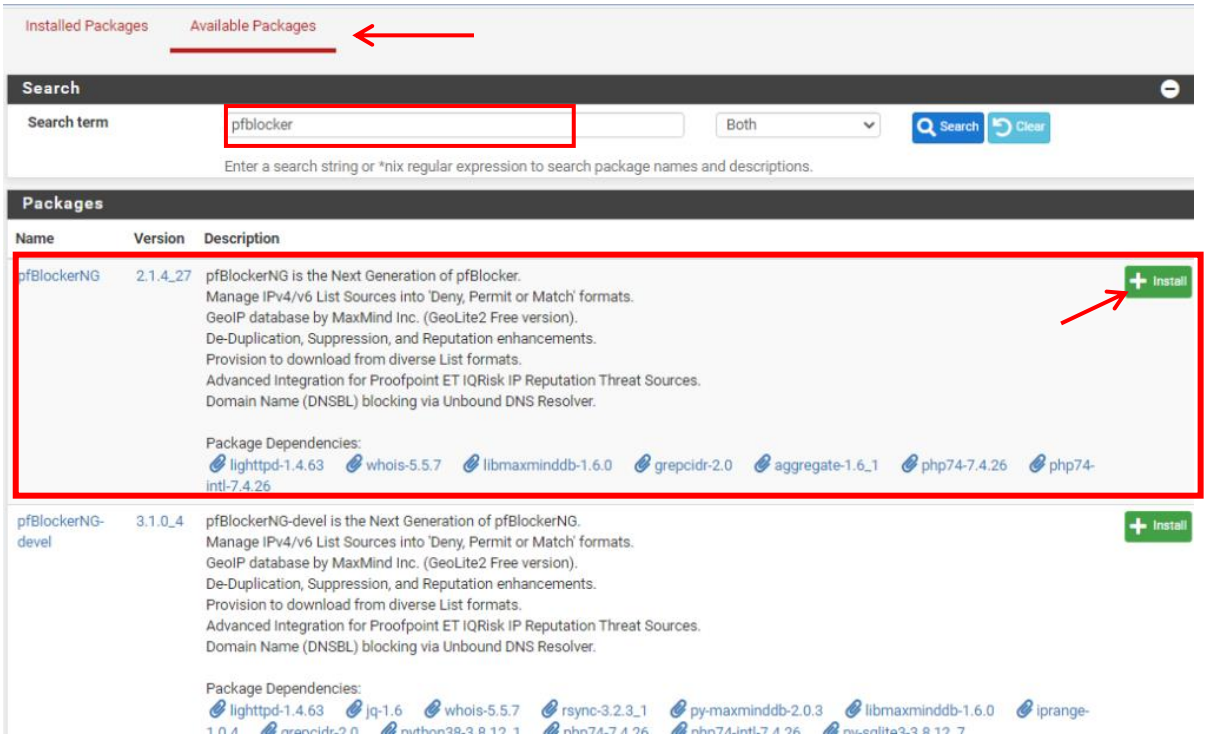

Figure 52 : Installation de package pfBlockerNG.

- Une fois le package installé, on clique sur l'onglet **Firewall** => **pfBlockerNG** puis dans la configuration générale en active le package et ajuste la configuration de l'interface/des règlesde façon que le trafic entrant et sortant doit être bloqué.

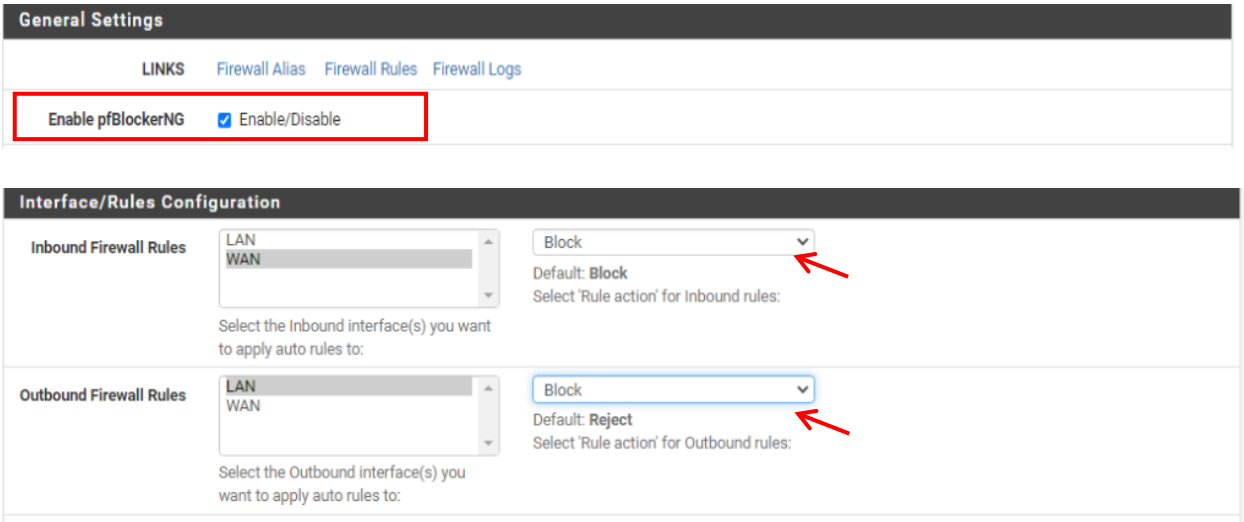

Figure 53 ; Configuration de pfBlockerNG.

b) Création des alias

- Pour configurer notre alias on clique sur l'onglet IPv4 et le paramétrer comme suit :
  - ✓ Modifier le nom d'alias.
  - ✓ Modifier la liste IPv4 a whois qui nous a permet de bloquer des AS, des Domain ou adresse IP.
  - ✓ Remplir la source avec un AS de Facebook pour trouver ce numéro de système autonome en accède au lien trouvé dans **liste settings**etlui donnée une adresse IP de Facebook pour nous offrir leur numéro **AS** associé.

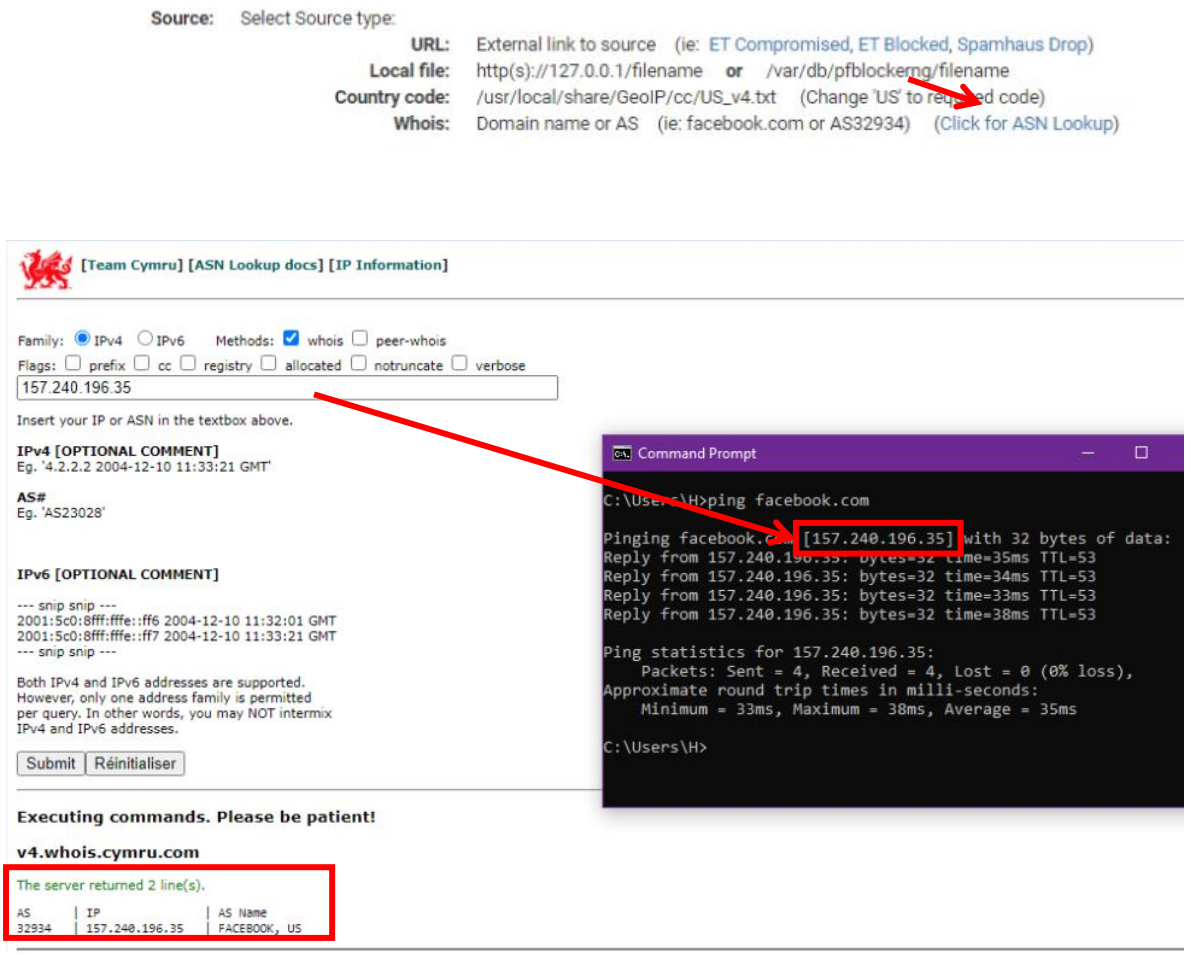

Figure 54 : Trouver le numéro de système autonome de Facebook.

- ✓ On Réécrire ce numéro dans le champ de source IPv4 List.
- ✓ Activer la mise ajour de système qui nous permet de rafraîchir les déférentes adresses IP de Facebook.

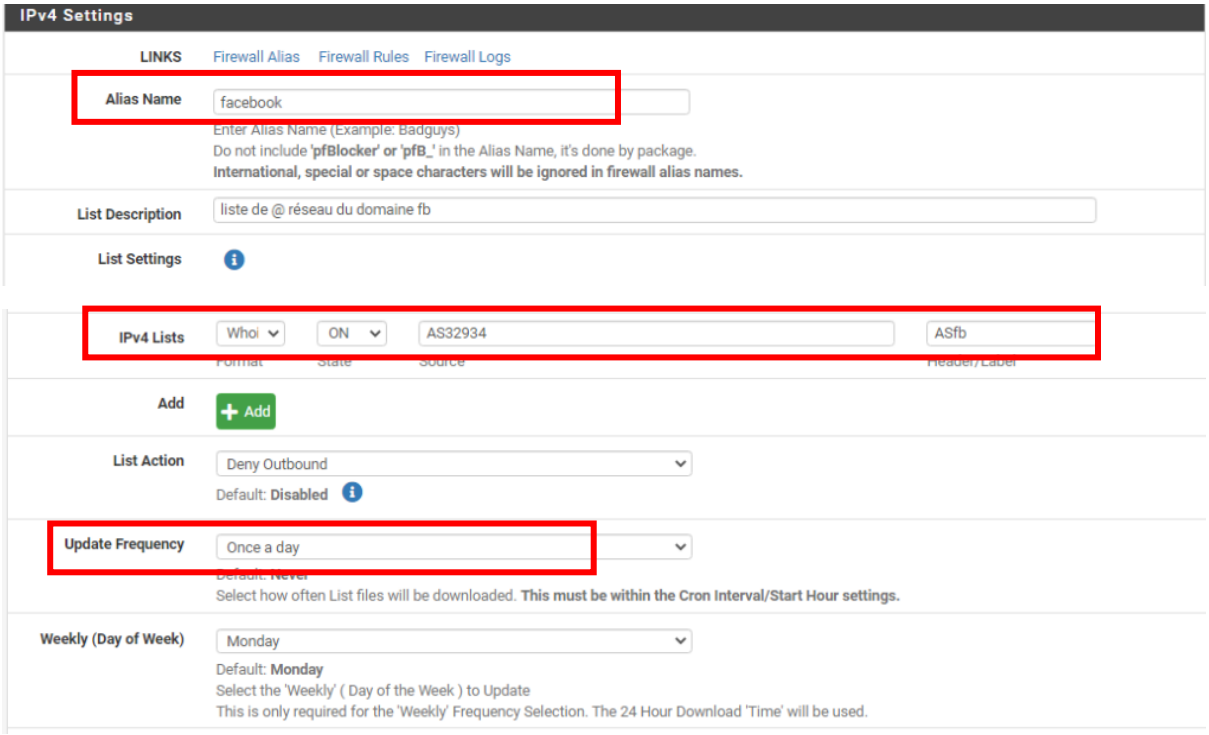

Figure 55 : Paramétrage d'alias.

c) Vérification des règles de filtrage :

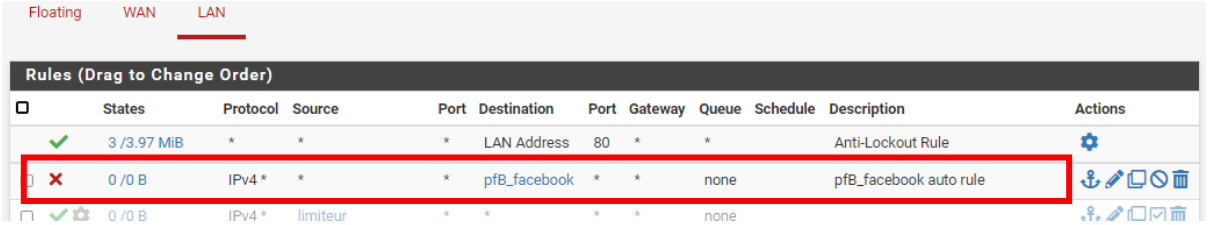

Figure 56 : Règle de filtrage du pfBlockerNG.

d) Le Test :

Figure 57 : le test de connexion a Facebook.

6.3 Gestion bande passante

Les limiters sont une évolution des technologies de priorisation de trafic existante sur pfSense D'une façon générale, les limiters permettent de définir une bande-passante maximale pour un usage. Ils peuvent être utilisés pour limiter le trafic d'une adresse IP spécifique, d'un sous-réseau, de service spécifique (ex : e-mail, web, ...) ou répartir de manière équitable le trafic entre plusieurs utilisateurs.

Dans notre réalisation en veut de limiter la bande passante pour un utilisateur.

1. Configuration de trafic shaper

1. Création des limites

- Pour Créer des limites, nous allons dans **Firewall** =>**Traffic Shaper** =>**Limiter**. Dans notre exemple nous mettons une limite de **3 Mbits/s** dans **Download** et ajuster le masque a«**Sourceaddresses**» figure 58, avec une limite de **150 kbit/s** dans **Upload**et ajusterle masque a « **Destination addresses** » figure 59**.**

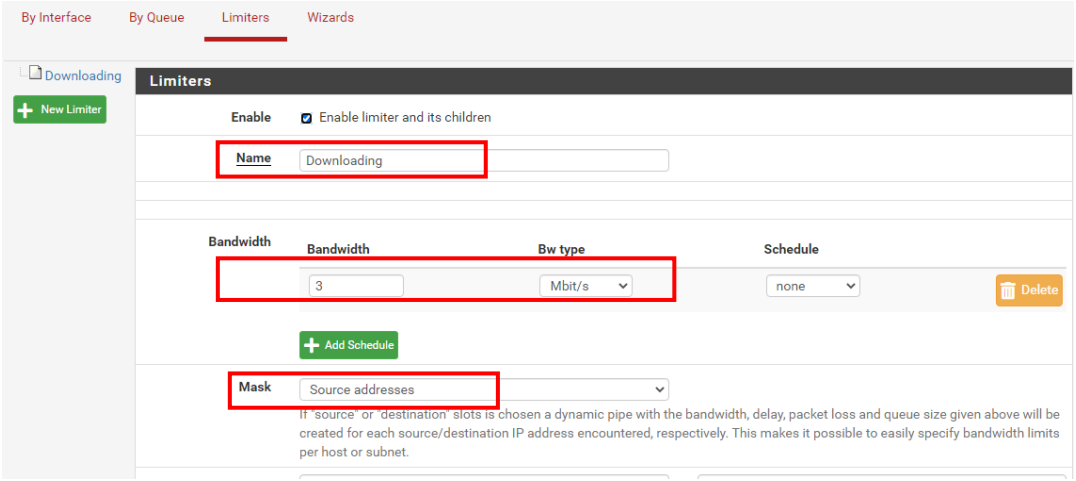

Figure 58 : limite Download.

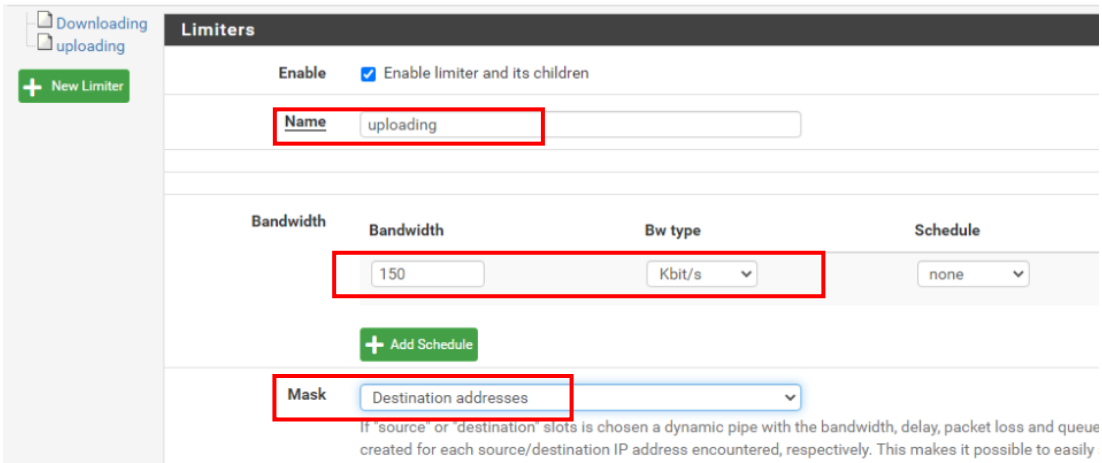

Figure 59 : limite Upload.

2. Application des limites

- Après on a créé une alias pour le limiteur comme illustré dans la figure 60Maintenant il reste d'éditer les règles que nous voulons appliquer les limiter sur ils dons rendez-vous dans**Firewall** =>**Rules**, puis allons dans la section **Advanced features**=>**In/Out**, et cliquons sur le bouton Advanced et en fin nous sélectionnons dans la liste la limite en entrée et en sortie sans oublié d'insérer l'alias de limiteur dans la source des règles figure 61.

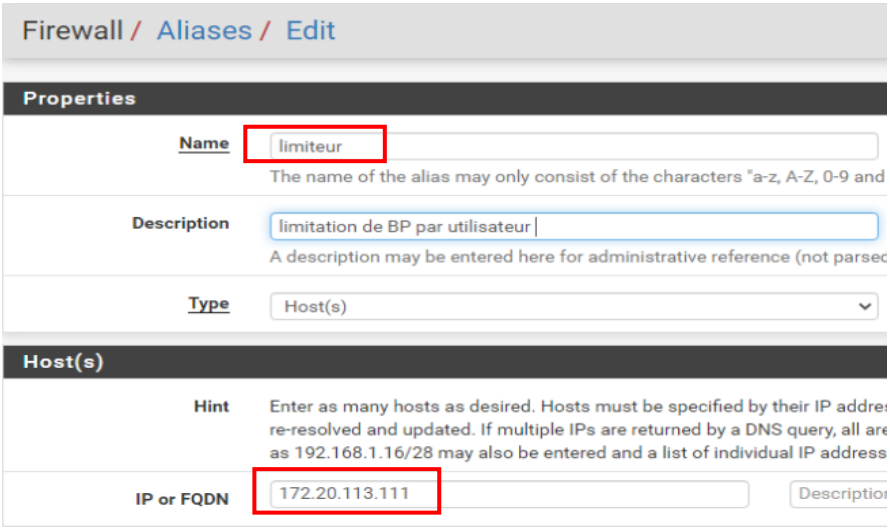

Figure 60 : Alias de limiteur.

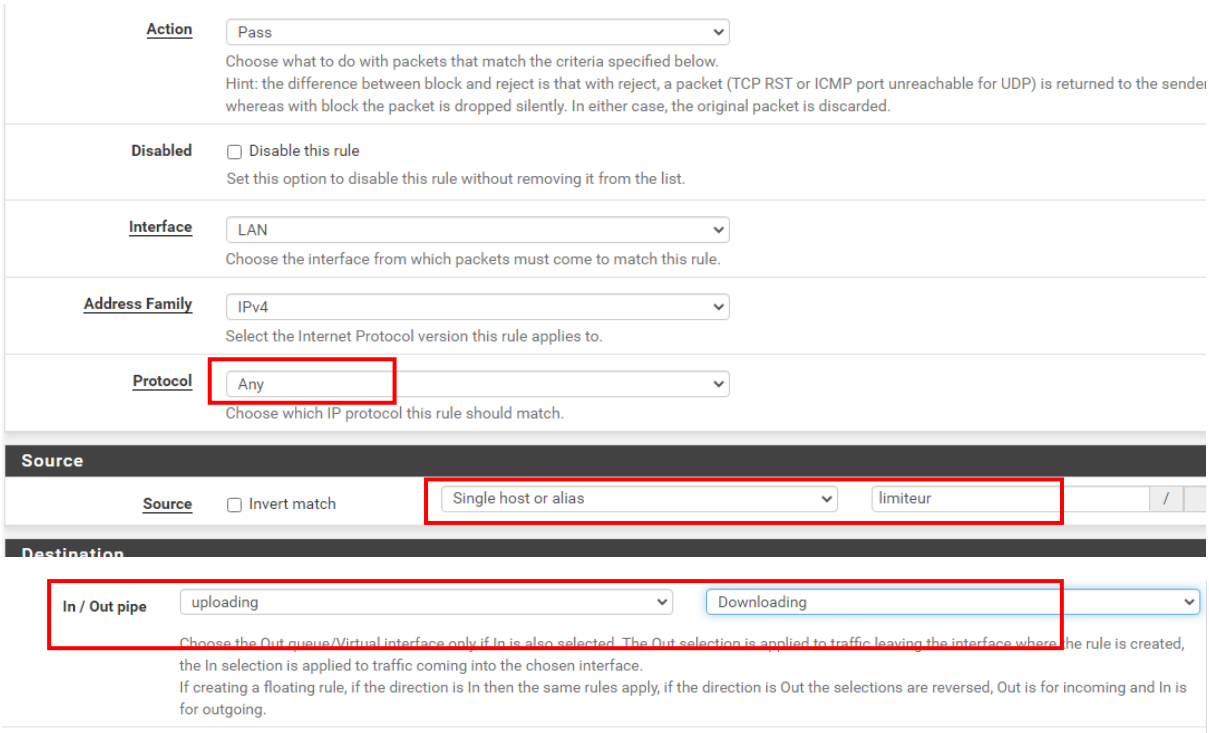

Figure 61 : Règle de limite.

3. Test

En testé de bande passante avec le site https://www.nperf.com/fr/ le test est effectuer depuis 2 utilisateur qui sont relié dans le même réseau (le premier utilisateur a un accès limiter à l'internet et l'autre non).

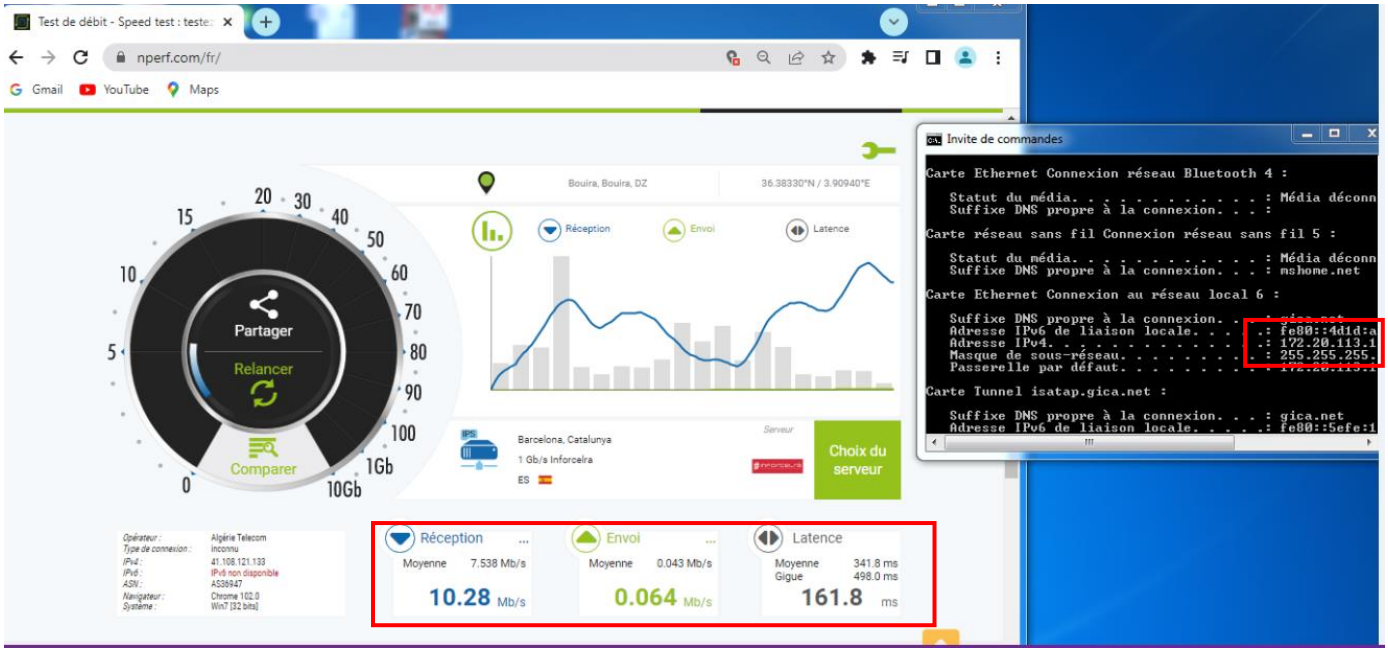

Figure 62 : Test avec un accès non limité.

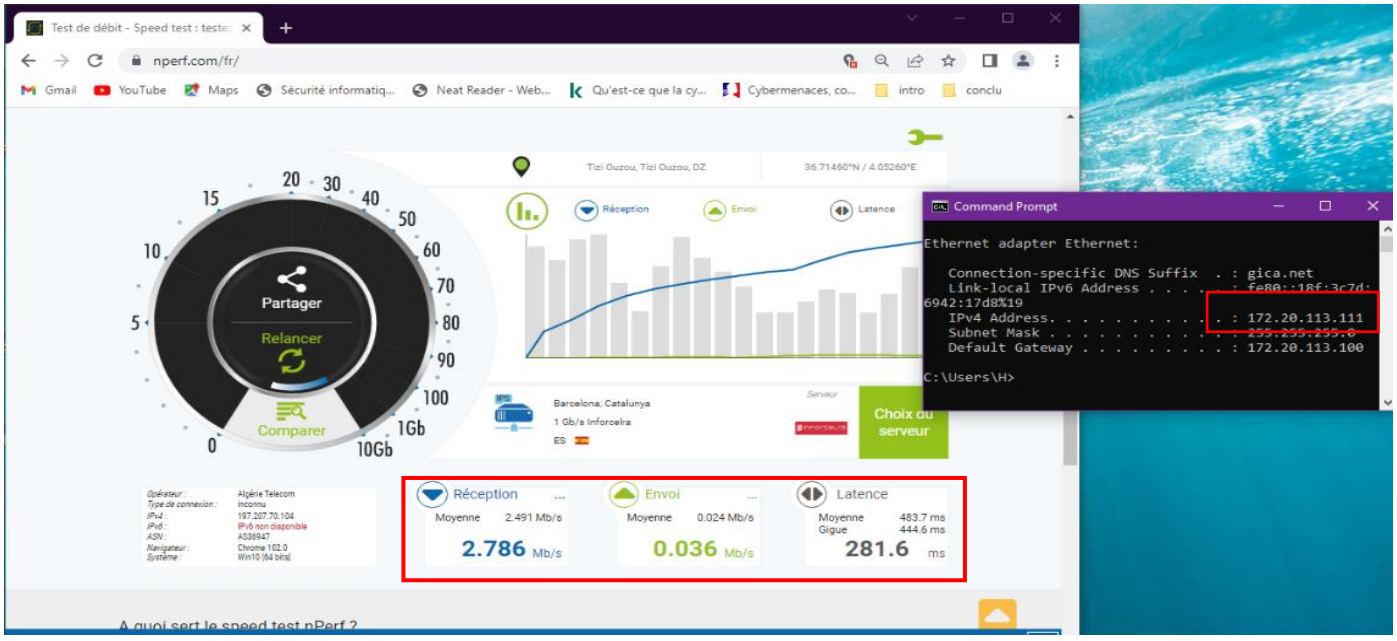

Figure 63 : Test avec accès limité.

6.4 Activation du serveur proxy

Nous allons mettre en place un serveur proxy, avec Squid, lui adjoindre des fonctions avancées de filtrage avec SquidGuard.

- **Squid et SquidGuard**

Squid est un serveur mandataire, entièrement libre et très performant. Squid est capable de gérer les protocoles FTP, HTTP, HTTPS. Il est généralement utilisé pour des fonctions de filtrage d'URL ou en tant que tampon. Les pages Internet sont stockées localement ce qui évite d'aller les recharger plusieurs fois et permet d'économiser la bande passante.

SquidGuard est un filtre, un redirecteur et un plugin de contrôle d'accès pour Squid. Il va notamment permettre d'appliquer sur un proxy une liste noire de sites ou mots-clés interdits. Pour installer les deux packages suivants, aller dans System **Package Manager** =>**Available Package.**

1. **Installation des packages Squid et SquidGuard**

- Pour réaliser l'installation de squid et squidguard, on clique sur le menu système de PFsense suivie par package manager puis avalable package, après la recherche de squid en installe les deux pakacheges « **squid** » et « **squidguard** ».

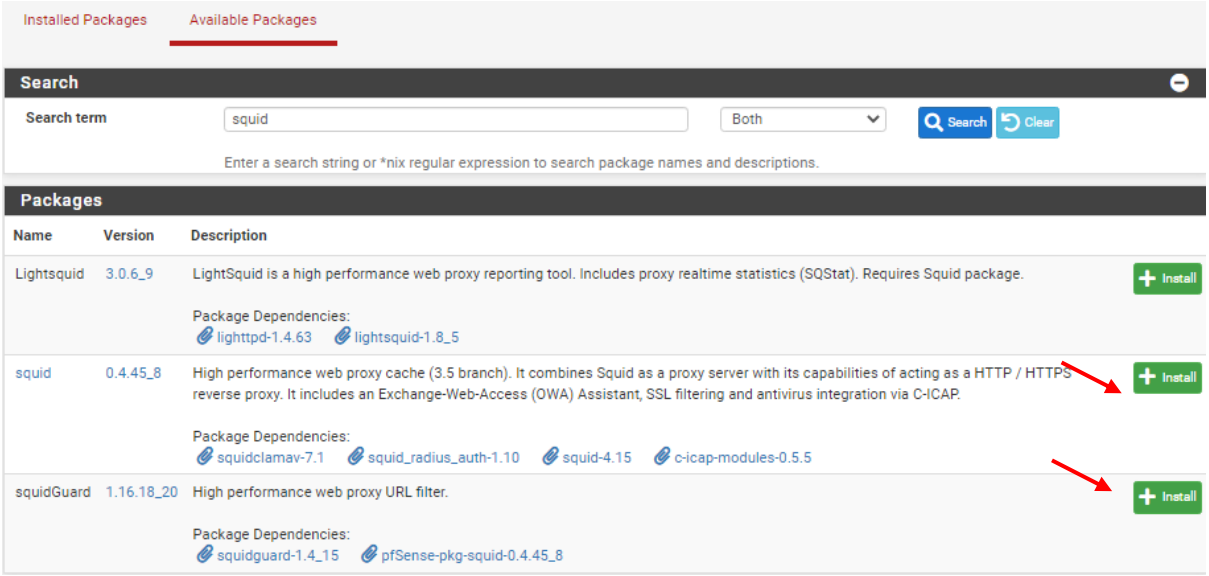

Figure 64: Installation des packages Squid et SquidGuard.

2. **Configuration squid et Squidguard**

- **Création d'une autorité de certification**

✓ Pour commencer, nous nous rendons dans le menu **System** => **Cert Manager** =>***Cas*** =>« **Add** ». Dans Les champs à renseigner nousAvons choisie Gica comme Descriptive

name alors que parmis les 3 méthodes nous avons choisie : « **Create an internal Cefícte Authority**» enfin Nous validons notre configuration, Notre autorité de certification est créée.

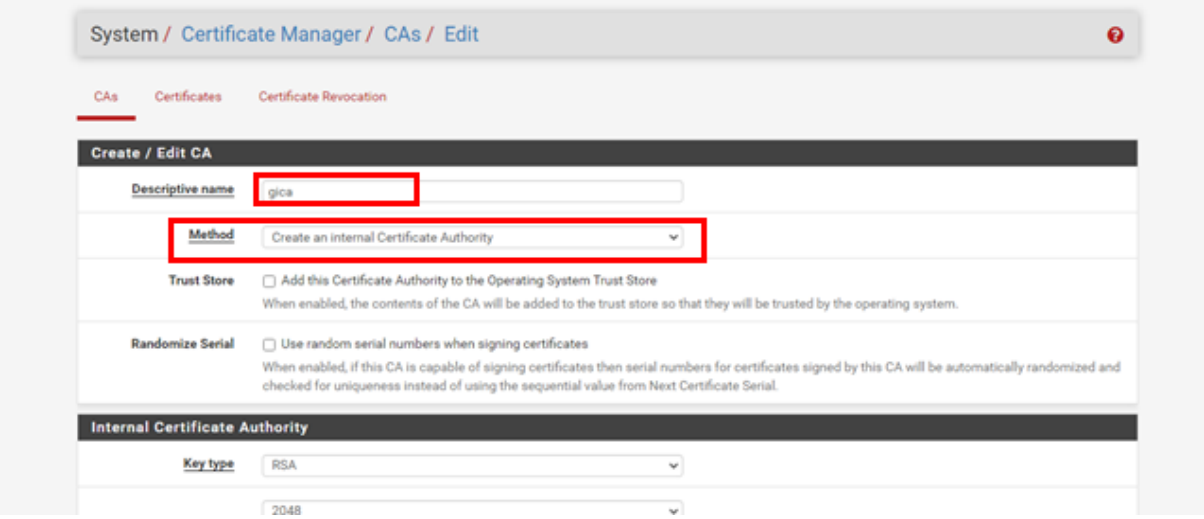

Figure 65: Création d'une autorité de certification

- **Configuration Squid (proxy server)**

Sur le menu Services, on choisit « SquidGuard Proxy filter ». Afin de pouvoir activer Squid, il faut configurer le cache local sinon le démarrage du processus Squid échouera. Ensuite, dans la partie « **General** », nous remplissons les champscomme dans la capture d'écran suivant :

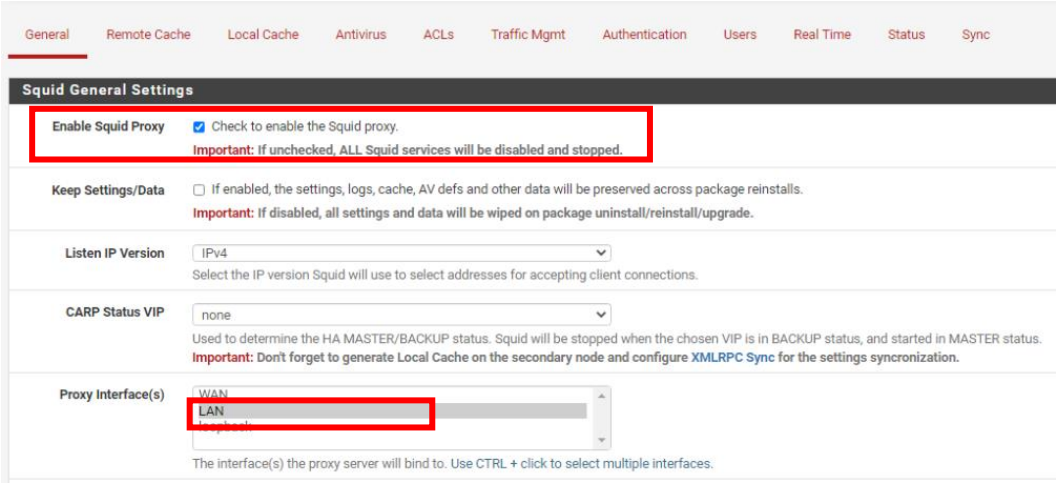

Figure 66 : Activation du serveur Proxy.

Le mode transparent http proxy redirige automatiquement tout le trafic web entrant vers leserveur proxy Squid. Dans la plupart des cas, l'utilisateur ne remarque même pas que sontrafic traverse un serveur mandataire.

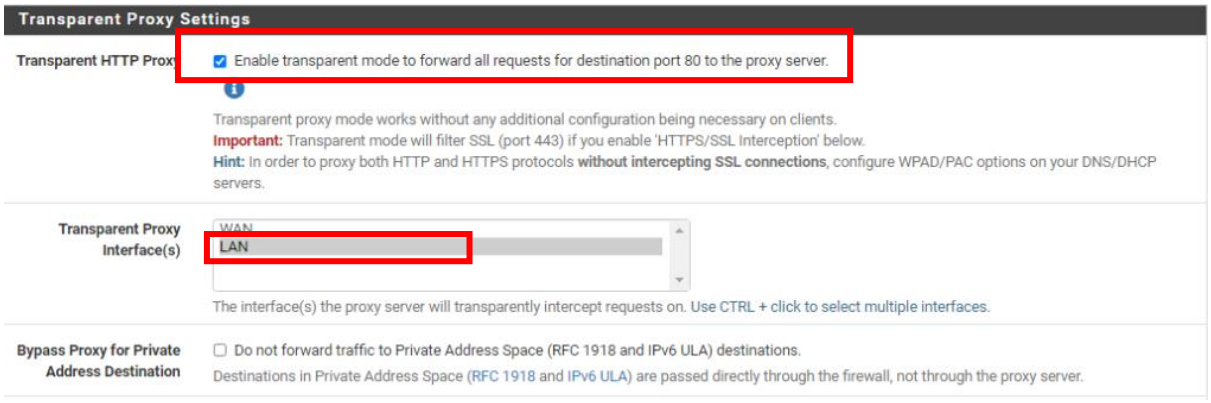

Figure 67 : Activation du proxy transparent.

- **Configuration SquidGuard (proxy filter http)**

SquidGuard permet de filtrer et de contrôler les accès.Nous allons utiliser la liste noire qu'on trouvesur le site suivant :

«http://dsi.utcapitole.fr/blacklists/download/blacklists_for_pfsense.tar.gz »

Nous allons dans le menu «**Services** » =>« **SquidGuard Proxy filter** ». Dans la partie **General setting**, nous remplissons les champs comme dans la capture d'écran suivant :

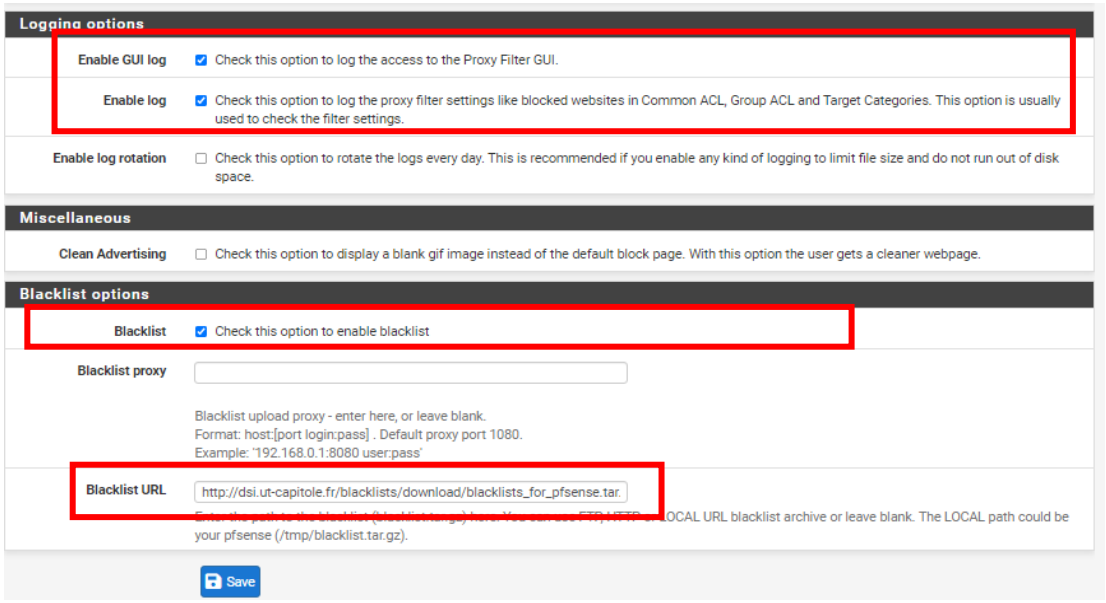

Figure 68 : Configuration du SquidGuard.

On clique sur le bouton « **Download** » pour télécharger la liste noire que nous avons renseignée dans les paramètres de SquidGuard.

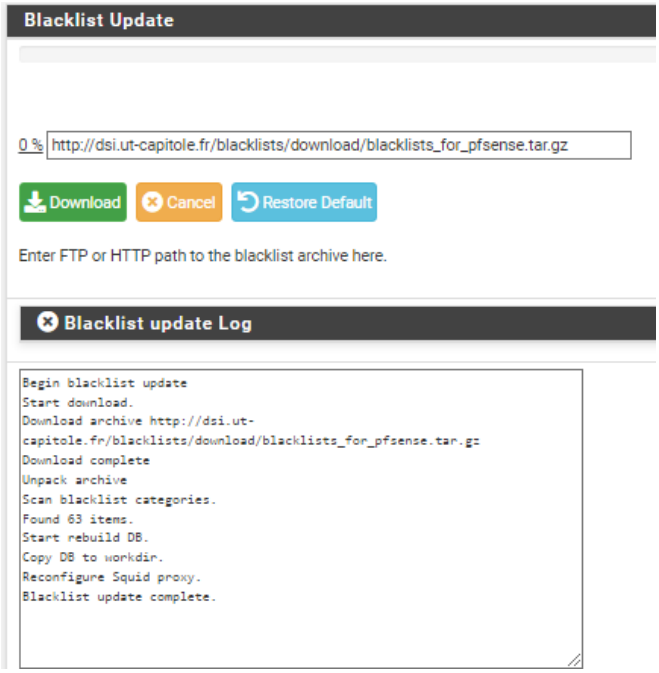

Figure 69 : Installation de blacklist.

Afin d'exploiter la liste noire, nous devons créer des règles sous la forme d'ACL, donc On a bloqué la catégorie « **VPN** » correspondante à « **[blk_blacklists_vpn]** »

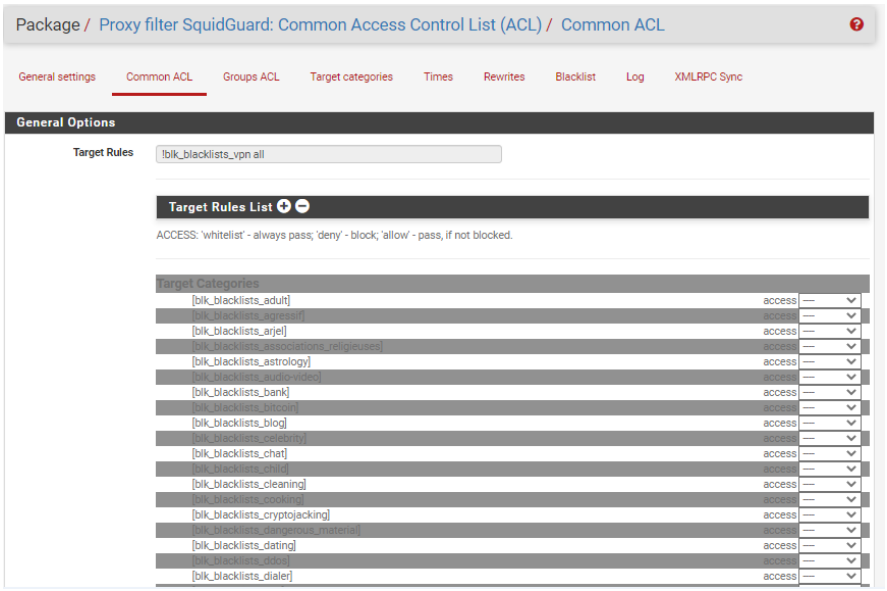

Figure 70: Catégories de blocage.

En fin, nous retournons dans l'onglet General Settings puis nous cochons la case **Enable** et nous faisons un **apply**pour appliquer la configuration.

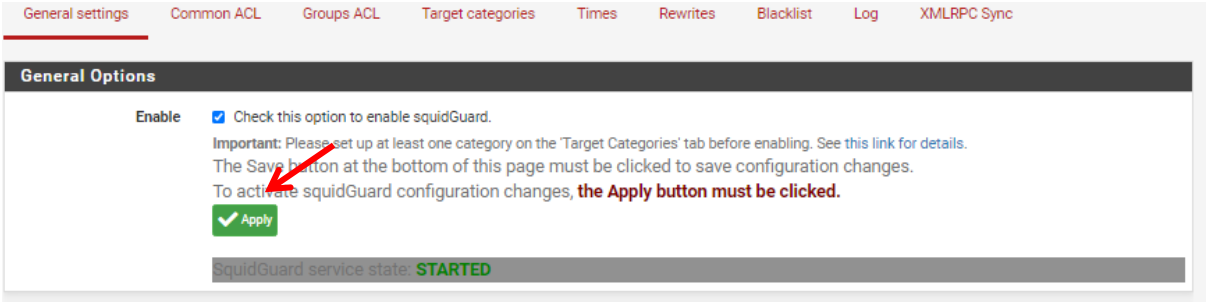

Figure 71 : Application des modifications.

3. Test

À partir d'un poste client, une recherche au site web « **nordvpn** » a été effectué, les résultats obtenues sont apparu sous forme d'erreur de connexion.

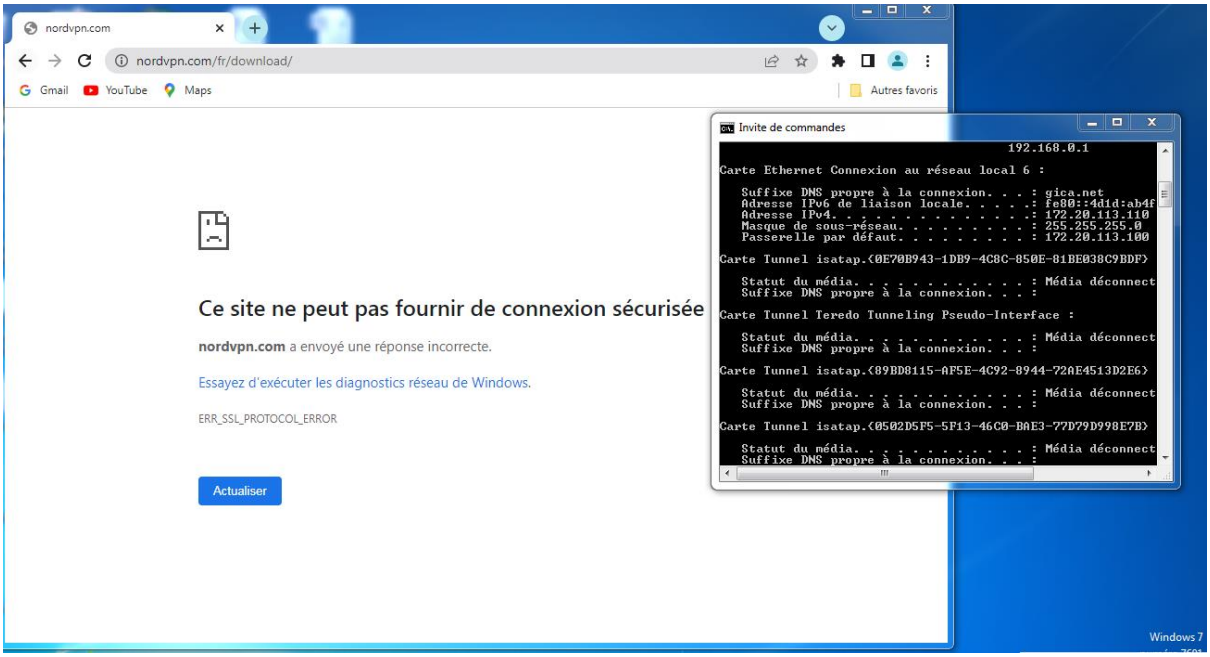

Figure 72: Test d'Interdiction du site nordvpn

6.5 AntivirusclamAV

ClamAV est un antivirus GPL pour UNIX. La principale qualité de cet antivirus est qu'il permet de balayer les courriels reçus et envoyés avec un logiciel de messagerie classique. Le paquet que nous allons installer inclut un démon multi-tâches flexible et configurable, un antivirus en ligne de commande et un utilitaire pour une mise à jour automatique des définitions de virus via Internet.

1. Configuration de clamAV

On a accédé à **Services** =>**Squid Proxy Server** =>**Antivirus**, Cocher**Enable AV** pour activer l'antivirus, Choisir la **période de mise à jour** de l'antivirus et la localisation, pour moi toutes les **8 heures** avec comme **localisation l'Europe**.

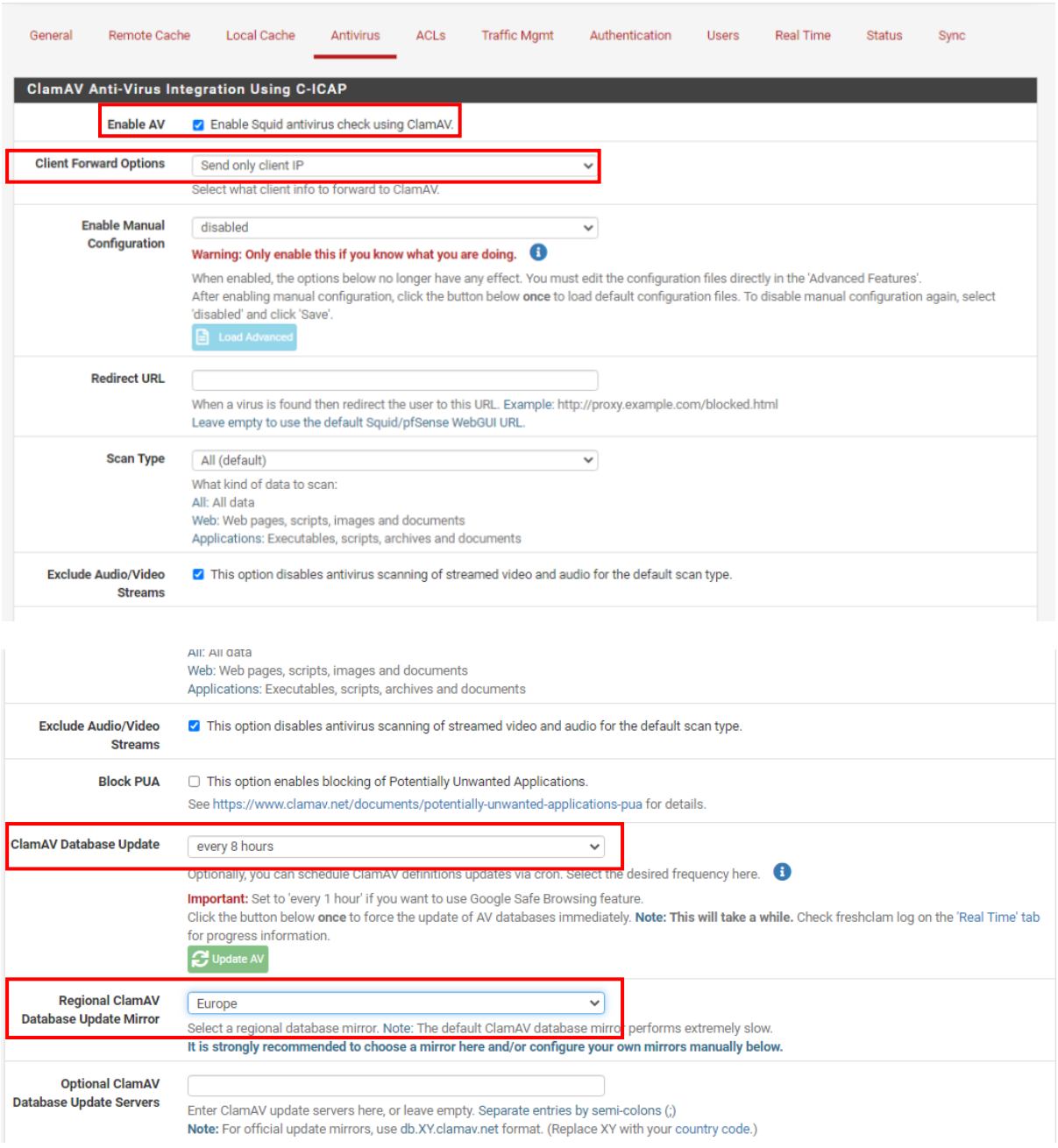

Figure 73 : Configuration de l'antivirus clamAV.

Ensuite aller dans **Diagnostics =>Command prompt** et faire la commande: **freshclam** pour actualiser l'anti-virus. Puis aller sur l'accueil (Dashboard) et ajouter **Squid Antivirus status** pour pouvoir visualiser le statut de l'antivirus.

Les voyants devraient être verts si l'antivirus est correctement démarré.

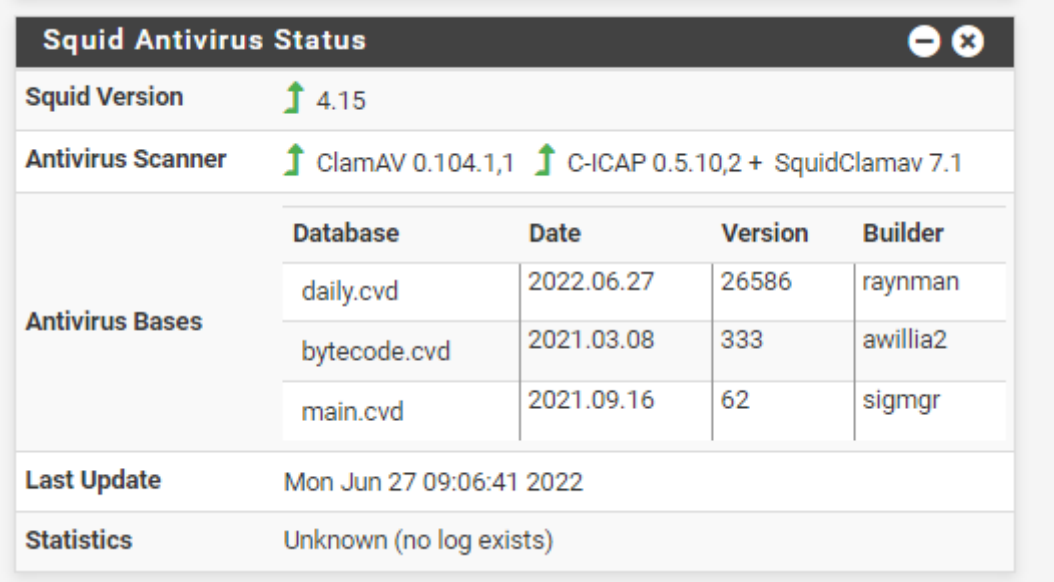

Figure 74 : statut ClamAV

2. Test

Il existe plusieurs sitesweb qui proposent des fichiers testés à télécharger pour détecter les virus. En téléchargeant un fichier sur http://www.eicar.org/85-0-Download.html l'antivirus bloque automatiquement le téléchargement!

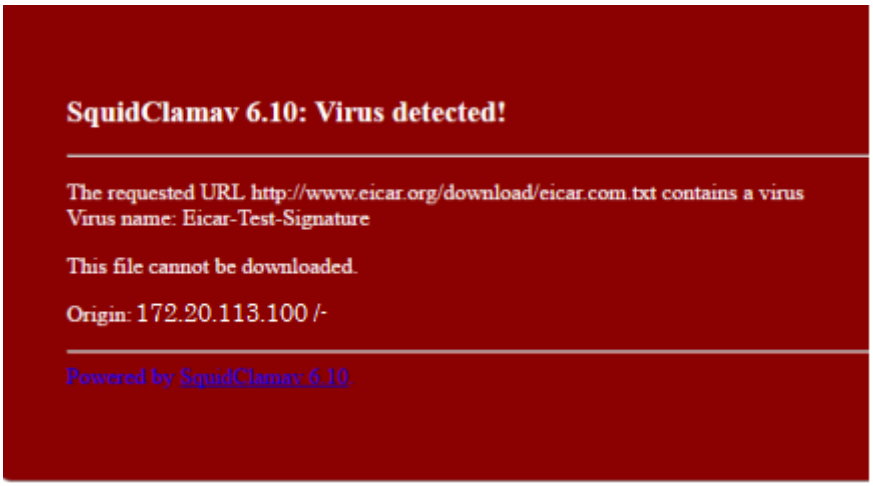

Figure 75 : Test d'antivirus.

6.6 Détection d'intrusion

La détection d'intrusion permet desécuriser et desurveiller lesdiverses menaces sur Internet. Pour cela nous allons installer Snort.

Snort est un IDS (Système de détection d'intrusion) open source qui peuventêtre installé sur un pare-feu pfSense pourprotéger un réseau.Il peut également être configuré pour fonctionner comme un système de prévention d'intrusion (IPS), ce quilerend très souple.

1. **Configuration de Snort :**
   - Aller dans System =>Package Manager et installer le paquet snort .
   - Accédez au site Web de Snort, créez un compte et obtenez un Oinkcode gratuit.
   - Aller ensuite dans **Services** =>**Snort** =>**Global Settingset** activer **Snort VRT** et coller le code Oinkcode.

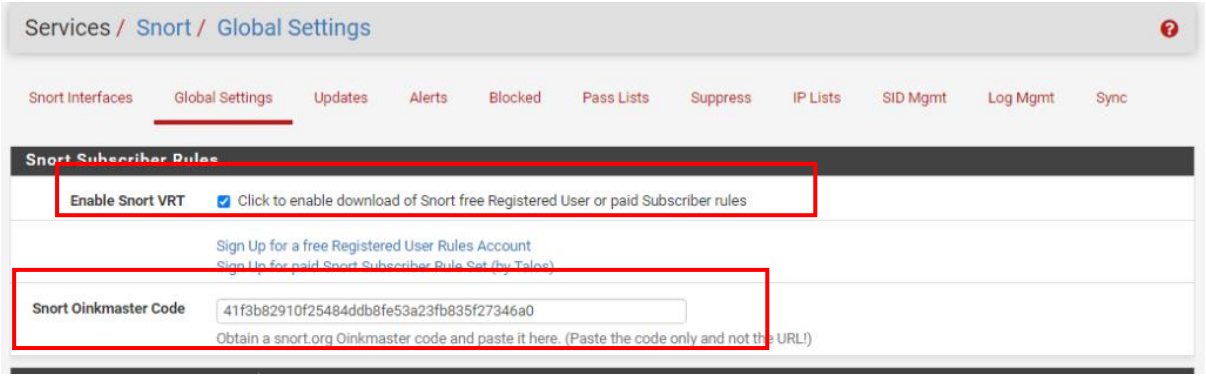

Figure 76 : configuration de snort.

- Dans l'onglet Updates, il faut cliquer sur Update **rules**pour mettre à jour les règles.
- Dans l'onglet Snort Interfaces, cliquez sur le bouton **Add**et effectuez la configuration suivante :
  - Activer => Oui
  - Interface =>wan :Dans le cadre d'une entreprise, il est préférable dedéployer cela sur le WAN car les attaques doivent être contrées au niveau du WAN

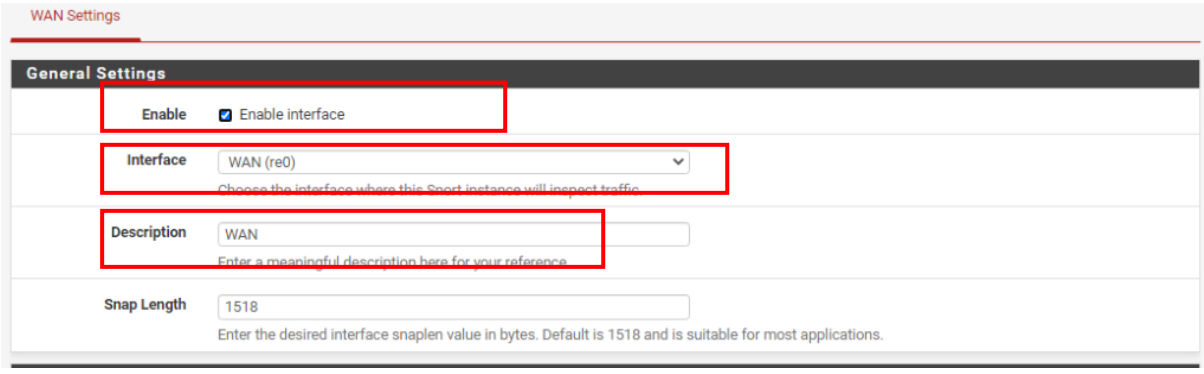

Figure 77 : configuration de l'interface WAN.

- Dans l'onglet «**wancategories »** En coche « **use IPS Policy** ».

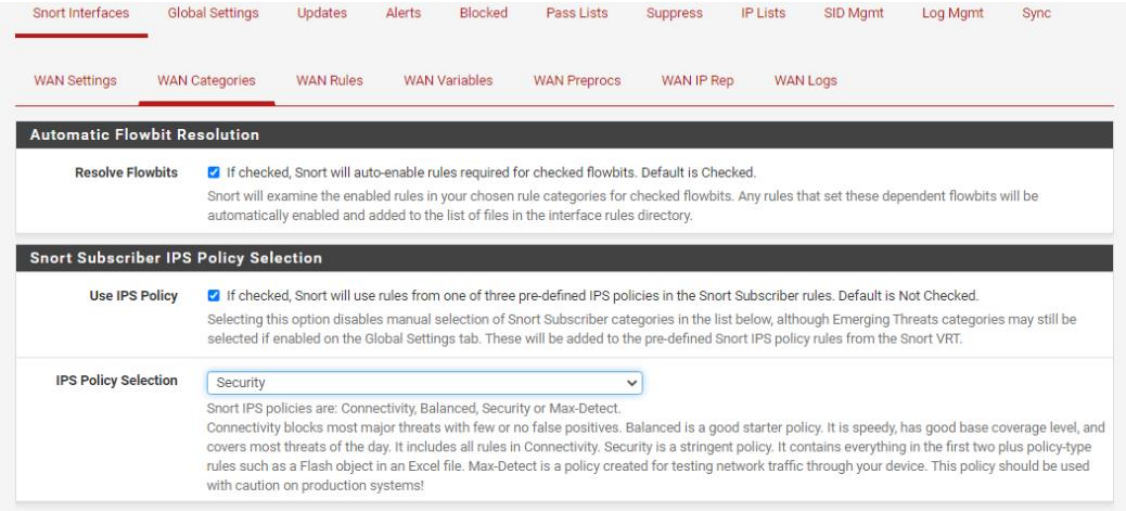

Figure 78 : configuration wan categories

- Sur la liste des interfaces, Cliquez sur la petite icône « **Play »**, Activer le Service de surveillance.

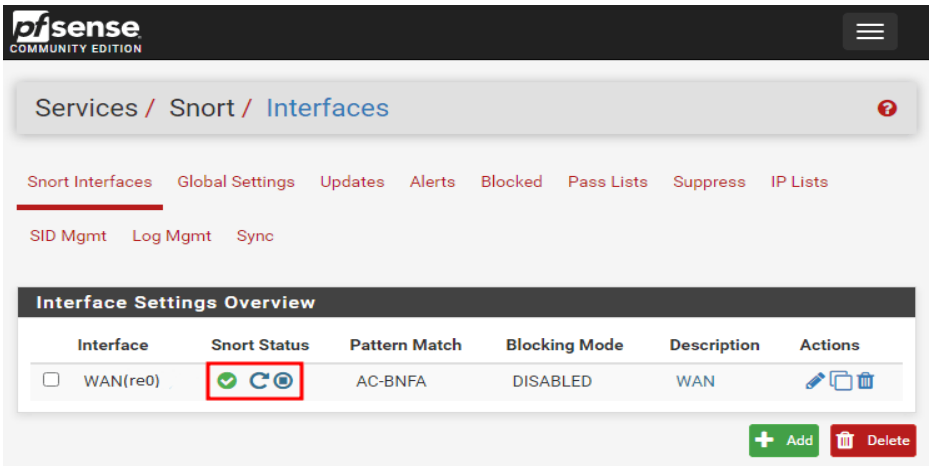

Figure 79 : Activationdu servicesnort

1. Analyse des paquets bloqués:

- Il est maintenant possible de regarder ce que l'IDS a détecté. Pour ce faire, aller dans l'onglet « **alerts »** qui présente une liste des alertes interceptées par Snort. Au meme temps en peut appuyez sur « **Download »** pour téléchargement les journaux ou sur « **Clear »** pour supprimer les alertes. La suppression des journaux après le télécharge-ment est une bonne décision pour empêcher les journaux d'occuper l'espace disque.

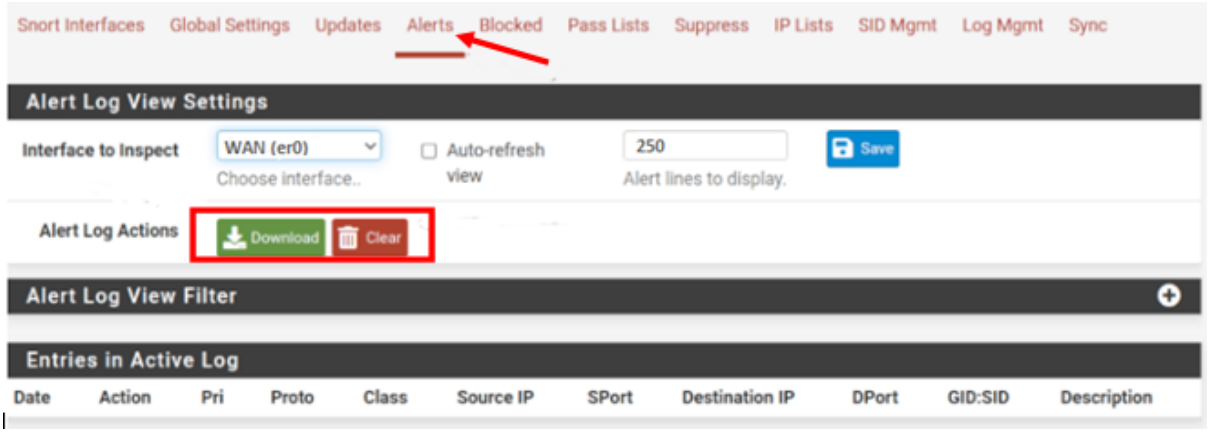

Figure 80 : liste des alertes.

- Dans l'onglet « **Blocked »** nous pouvons constater les adresses IP bloquées qui ont été détecté en intrusion.

6.7 Supervision des réseaux

Ntopngest un outil de supervision libre, permet d'avoir une surveillance sur les informations du trafic réseau en temps réel.et avoir une vue globale sur la consommation de la bande passante, il est capable de détecter jusqu'à ou les connexions ont été faites par les ordinateurs locaux et combien de bandes passantes ont été utilisées sur des connexions individuelles. Il fait partie des paquets disponibles sur Pfsense et nous l'avons à cet effet exploité.

1. Installation et configuration de Ntopng

- Tout d'abord en clique sur l'onglet **System**=>**Package Manager** =>**AvailablePackage**puisrecherche le package ntopNG puis l'installer.

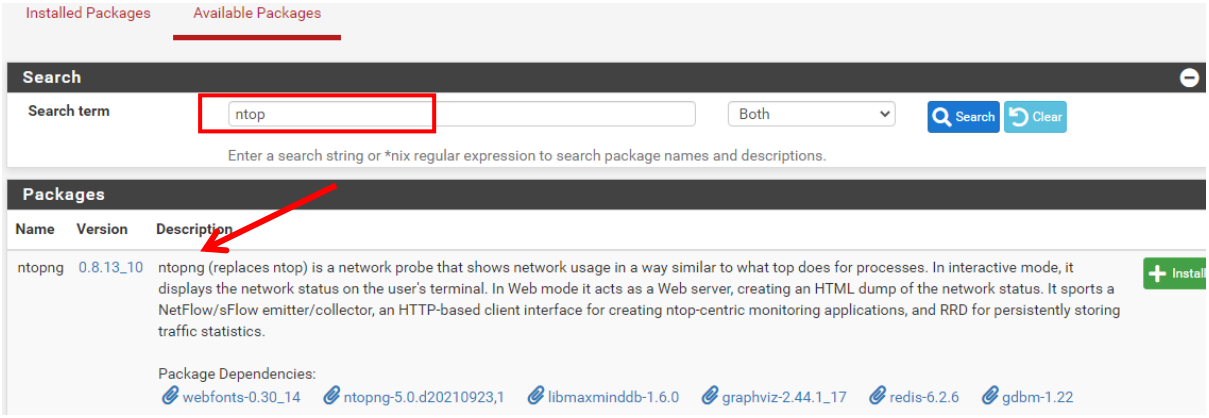

Figure 81 : Installation de package ntopng.

2. Configuration du service Ntopng

- Une fois l'installation terminée, il faut se rendre dans l'onglet **Diagnostics** =>**Ntopng Settings** en active les services et configurer le mot de passe et l'interfaces d'écoute.

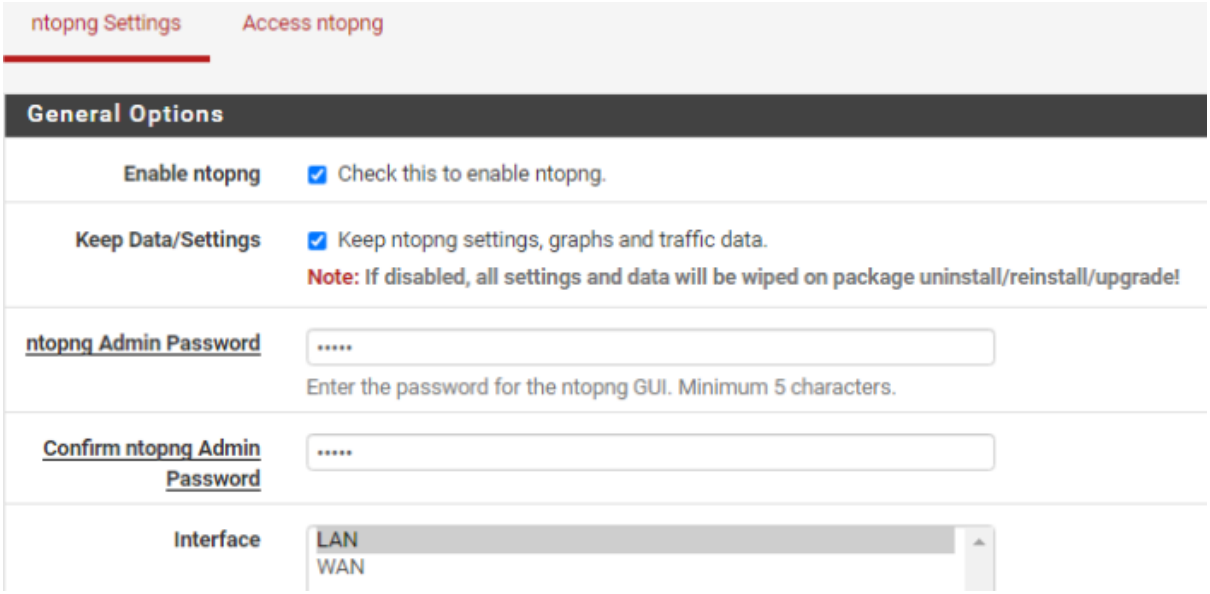

Figure 82 : configuration de ntopng.

3. L'accès au ntopng

- En peux accéder à ntopng à partir de l'authentification dans l'onglet « **Access ntopng** »

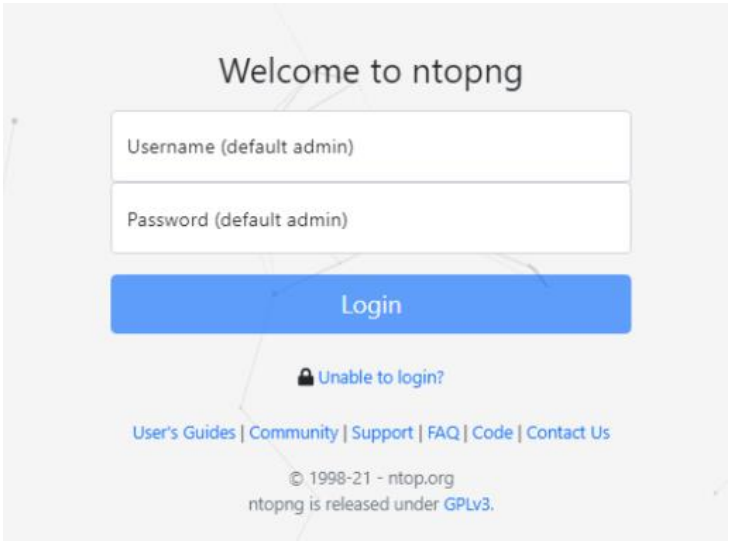

Figure 83 : Interface d'authentification

- dans le tableau de bord de ntopng en peu de collecter les données d'utilisation de la bande passante, Principaux clients, Protocoles utilisés, Applications utilisées, Ports utilisés… Etc.

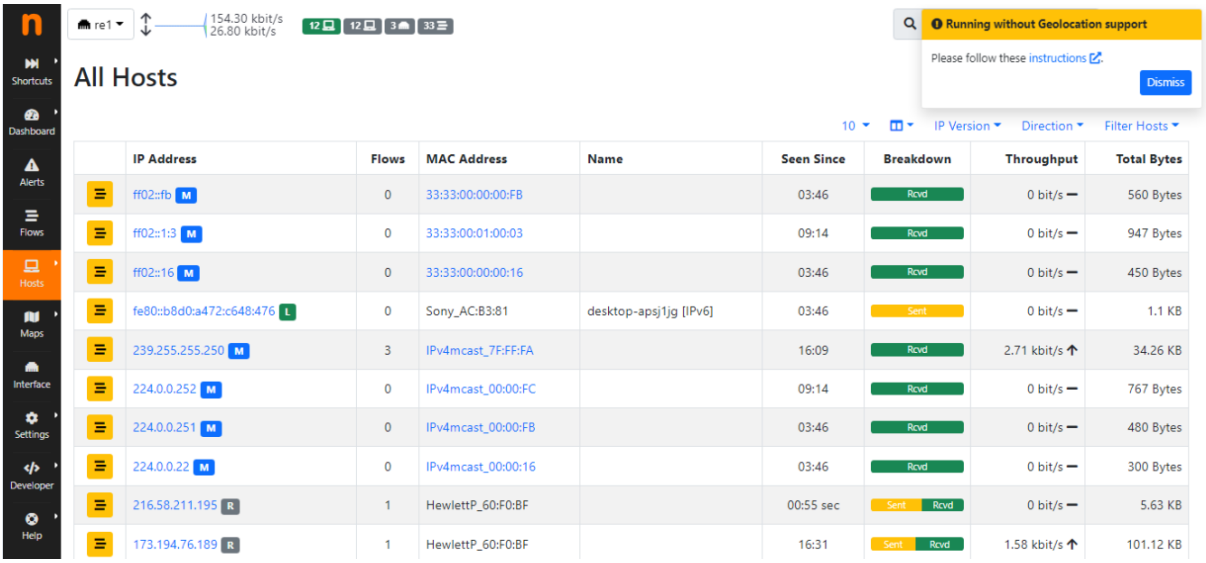

Figure 84 : Exemple de la liste des hôtesconnecter au réseau.

7 Conclusion

La sécurité d'un réseau est extrêmement importante au sien d'une entreprise. C'est pourquoi, la mise en place de solutions de protection, de surveillances telles qu'un firewall permet de répondre à ce besoin de sécurisation.

Durant ce chapitre, au premier lieu, on a étudié profondément l'architecture existante de l'entreprise, nous avons pu cerner les failles qui pèsent sur cette dernière. Pour palier à ses manques sécuritaires, nous avons proposé une solution qui renforce notre politique de sécurité consiste à implémenter et configurer le firewall « pfsense » et pour cela, on a modifié l'architecture du réseau en ajoutant ce fameux firewall.

À la seconde partie, nous avons présenté le prérequis utilisés afin de configurer Pfsense, puis nous avons expliqué à travers diverses captures, les étapes de son installation et de sa configuration, à travers lesquelles nous définissons quelques fonctionnalités que propose cet outil.

Conclusion générale

Pour un bon déroulement d'une entreprise, la présence d'un réseau et système informatique est indispensable.

Dans la première partie de notre travaille, nous avons représenté les différents problèmes qui peuvent être mené pour le système informatique d'une entreprise et qui représente par des failles du réseau informatique, ses failles peuvent attribuer des attaques, des hakers ce qui cause la destruction du système informatique de l'entreprise et c'est ce qu'on a vu dans le deuxième chapitre.

Comme nous l'avons représenté dans le troisième chapitre, plusieurs solutions sont utilisées pour régler le problème, parmi celle-ci le Firewall qui a répondu à notre problématique qui consiste de contribuer à l'amélioration de la sécurité informatique au sein de l'entreprise CE-TIM.

L'objectif principal assigné notre travail est la mise en place d'un firewall logiciel qui est le pfsense, qui permet de sécurisé le réseau d'entreprise contre les intrusions et les failles de systèmes et des attaques qui vienne par les hackeur, en filtrant tout information et fichier qui rentre et sort du réseau privé vers Internet

Ce travail nous a permis d'améliorer nos connaissances dans le domaine de la sécurité des réseaux notamment le pare feu « pfsense » ainsi son fonctionnement et son rôle dans la sécurité d'entreprise.

Le pfsense possède plusieurs fonctionnalité, de plus il nous a permis d'ajouter des package qui a leur tours lui permettent d'être totalement modulables.

Parmi ces fonctionnalités nous sommes intéressés à la mise en place des limites afin de répartir équitablement la bande-passante de notre connexion Internet entre tous les usagers de notre réseau local.

Et afin de réaliser un filtrage des sites web on a utilisé des déférentes méthodes qui sont représenté par l'installation et la configuration de déférents package.

Il serait intéressant de combiner plusieurs packages pour une meilleure sécurisation. En effet, le package SNORT permet la détection et la prévention d'intrusion aux réseaux et d'inclure des règles d'accès pour mieux gérer la bande passante, comme il nous offre aussi la fonctionnalité d'un antivirus qui permet de balayer les courriels reçus et envoyer avec un logiciel de messagerie classique.

Ainsi il est intéressent d'avoir une surveillance sur les informations du trafic réseau en temps réel comme nous avons vue avec l'installation de ntopNG.

Les résultats des tests obtenue confirment que la solution de sécurité proposé est redoutable, mais cela n'empêche pas la poursuite des recherche des solutions basé sur le pfsense et qui pourrait accomplir notre travaille, tel que la mise en place d'un « DMZ », et amélioré des mécanismes de sécurité en installant et configurant un « portail captif »ainsi que la configuration « Dual-Wan » qui permettent d'accroitre le débit disponible pour l'accès internet ou d'assurer une continuité de service en cas de panne du lien principale , par exemple.

ANNEXE

1. Modèles de réseaux :

✓ MODÉLE OSI (Open Systems Interconnection):

Le modèle OSI est un modèle conceptuel, il a pour but d'analyser la communication en découpant les différentes étapes en 7 couches, chacune de ces couches remplissant une tâche bien spécifique. Afin de connaitre les services de chaque couche on va les présenter ci-dessous l'une après l'autre :

1. **La couche physique :** cette couche assure la transmission d'une suite de bits sur le média de transmission (support physique), ces bits deviennent des signaux numériques ou analogiques.
2. **La couche Liaison:** dans cette couche on cherche à savoir comment deux stations sur le même support physique vont être identifiées. Pour ce faire, on peut par exemple assigner à chaque station une adresse (cas des réseaux Ethernet,....).
3. **La couche Réseau:** le rôle de cette couche est de trouver un chemin pour acheminer un paquet entre 2 machines qui ne sont pas sur le même support physique.
4. **La couche Transport:** elle permet à la machine source de communiquer directement avec la machine destinatrice. On parle de communication de bout en bout.
5. **La couche Session:** elle identifie le rôle de chaque station à un moment donné. Elle assure l'ouverture et la fermeture de session entre les applications. En fait, ellecontrôle le dialogue et définit les règles d'organisation, de synchronisation, le droit de parole.
6. **La couche Présentation:** A ce niveau on doit se préoccuper de la manière dont les données sont échangées entre les applications.
7. **La couche Application:** Dans cette couche on trouve normalement les applications qui communiquent ensemble. (Courrier électronique, transfert de fichiers,...)

✓ modèle TCP/IP

TCP/IP est un ensemble de protocole standard de l'industrie permettant la communication dans un environnement hétérogène. Le nom de ce modèle de référence provient de ses deux principaux protocoles (TCP et IP). Les objectifs principaux de cette modélisation sont :

- relier des réseaux hétérogènes de façon transparente ;
- garantir les connexions quel que soit l'état des lignes de transmission ;
- assurer le fonctionnement d'applications très différentes (transfert de fichier,..)

Le rôle de chaque couche :

1. **La couche Accès réseau :** Elle a pour rôle de transmettre les données sur le média physique utilisé.

2. **La couche Internet :** Elle a pour rôle de transmettre les données à travers une série de réseaux physiques différents qui interconnectent un hôte source avec un hôte destination. Les protocoles de routage sont étroitement associés à ce niveau.
3. **La couche Transport :** Elle prend en charge la gestion de connexion, le contrôle de flux, la retransmission des données perdues et d'autres modes de gestion des flux.
4. **La couche Application :** Elle sert à l'exécution des protocoles de niveau utilisateur tels que les échanges de courrier électronique, le transfert de fichiers, ou les connexions distantes.

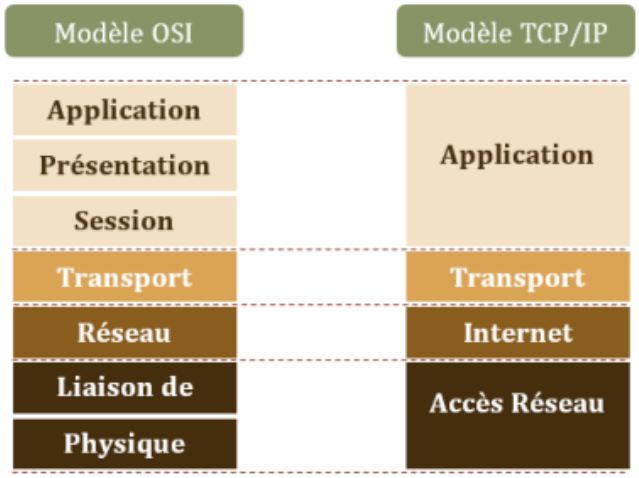

Figure 85 : Comparaison entre les couches de modèle OSI et TCP/IP

2. Maliciel :

Logiciel malveillant qui infecte votre ordinateur et permet aux cybercriminels d'infiltrer votre ordinateur ou d'endommager votre système ou votre appareil.

3. Rançongiciel:

Technique d'attaque courante de la cybercriminalité, le rançongiciel ou ransomware consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement.

4. Cookiede session :

Un cookie est un petit fichier stocké par un serveur dans le terminal (ordinateur, téléphone, etc.) d'un utilisateur et associé à un domaine webCe fichier est automatiquement renvoyé lors de contacts ultérieurs avec le même domaine.

Un cookie de session est un cookie dont la durée de vie est limitée à une session de navigation.

5. Protocole IP :

Le protocole IP fait partie de la couche Internet de la suite de protocoles TCP/IP.il permet l'élaboration et le transport des datagrammes IP (les paquets de données), sans toutefois en assurer la « livraison ». En réalité, le protocole IP traite les datagrammes IP indépendamment les uns des autres en définissant leur représentation, leur routage et leur expédition.

6. Protocole TCP :

Est Protocole de Contrôle de Transmission) est un des principaux protocoles de la couche transport du modèle TCP/IP. Il permet, au niveau des applications, de gérer les données en provenance (ou à destination) de la couche inférieure du modèle (c'est-à-dire le protocole IP)

7. Protocole FTP :

Est un protocole de communication destiné au partage de fichiers sur un réseau TCP/IP. Il permet, depuis un ordinateur, de copier des fichiers vers un autre ordinateur du réseau, ou encore de supprimer ou de modifier des fichiers sur cet ordinateur. Ce mécanisme de copie est souvent utilisé pour alimenter un site web hébergé chez un tiers.

8. Protocole ICMP :

Est un protocole de la couche réseau utilisé par les périphériques réseau pour diagnostiquer les problèmes de communication du réseau. L'ICMP est principalement utilisé pour déterminer si les données atteignent ou non leur destination en temps voulu.

9. Protocole IMAP :

Ce protocole permet à un client de messagerie (comme Outlook, Mail..) d'accéder aux messages stockés sur un serveur de messagerie (Orange, Gmail, La poste...). L'IMAP permet de consulter ses courriels depuis n'importe quel ordinateur connecté à Internet.

10. Protocole POP :

Permet la récupération des mails situés sur un serveur distant (serveur POP). L'objectif de ce protocole est de relever le courrier électronique depuis un hôte qui ne contient pas sa boite aux lettres. Il vient tout simplement télécharger les messages à partir du serveur et les stocke sur le poste de travail.

11. Protocole DHCP :

Est un protocole de communication. Les administrateurs réseau l'utilisent pour gérer et automatiser de manière centralisée la configuration réseau des appareils rattachés à un réseau IP Cette approche évite, par exemple, l'affectation préalable et la configuration manuelle de cette adresse pour chaque appareil.

12. UFS :

Abréviation d’Unix File System, est un système de fichier utilisé par de nombreux systèmes d’exploitation de type Unix.

13. Système autonome:

Un AS peut être considéré comme un groupe connecté de réseaux IP gérés par une seule entité administrative, telle qu'une université, un gouvernement, une organisation commerciale ou un autre type de fournisseur de services Internet.

14. Promiscuous mode :

Se réfère à une configuration de la carte réseau, qui permet à celle-ci d'accepter tous les paquets qu'elle reçoit, même si ceux-ci ne lui sont pas adressés.

A:

ARP: Address Resolution Protocol.

AH: Authentication Header.

ACL: Access Control List.

AS: Autonomous system.

C:

CHAP: Challenge Handshake Authentication Protocol.

CA: Certification Authority.

D:

DNS: Domain Name System.

DOS: Denial Of Service

DOI: Domaine D'interprétation.

DNSSec: Domain Name System Security Extensions.

DES: Data Encryptions Standard.

E:

ESP: Encapsulating Security Payload.

F:

FTP: File Transfer Protocol.

G:

GPL: General public license.

H:

HTTP: HyperText Transfer Protocol.

HTTPS: HyperText Transfer Protocol Secure

HTML: Hyper Text Markup Language.

I:

ISO: International organization for standardization.

ICMP: Internet Control Message Protocol.

IPSec: Internet Protocol Security.

IMAP: Internet Message Access Protocol.

K:

KDC: Key Distribution Center

L:

L2TP: Layer 2 Tunneling Protocol

LAN: Local Area Network.

M:

MITM: Man In The Middle.

N:

NAT: Network Address Translation.

O:

OSI: Open Systems Interconnection.

P:

POP: Post Office Protocol

PPP: Point-to-Point Protocol

PAP: Password Authentication Protocol

PPTP: Point-to-Point Tunneling Protocol

PKI: Public Key Infrastructure.

PAT: Port Address Translation

R:

RADIUS: Remote Authentication

S:

SQL: Structured Query Language

SSL: Secure Sockets Layer.

SSH: Secure Shell.

SSL: Secure Socket Layer.

S/MIME: Secure/Multipurpose Internet Mail Extensions

T:

TCP: Transmission Control Protocol.

TLS: Transport Layer Security.

U:

URL: Uniform Resource Locator.

UDP: User Datagram Protocol.

V:

VISA: Virtual Instrument Software Architecture

VLANs: Virtual Local Area Network.

VPN: Virtual Private Network

W:

WAN: Wide Area Network.

X:

XSS: Cross-Site Scripting.

Webographie

[1] https://www.wavesoft.it/fr/en-quoi-consiste-la-securite-informatique/

[2]https://www.cyberuniversity.com/post/systeme-informatique-definition-structure-et classification.

[11]https://www.itgovernance.eu/fr-fr/normes-informatiques-fr

[12] https://www.institut-numerique.org/iii2-principaux-defauts-de-securite-

[14]https://www.appitel.fr/blog/securite/les-differents-types-de-hackers-et-autres-pirates-du-web/

[16] https://waytolearnx.com/2018/07/difference-entre-attaque-active-et-attaque-passive.html

[17]https://blog.netwrix.fr/2018/07/04/les-10-types-de-cyberattaques-les-plus-courants/

[19]https://www.pandasecurity.com/fr/mediacenter/mobile-news/differents-types-de-malware/

[20]https://www.kaspersky.com/resource-center/threats/ip-spoofing

[21]https://slideplayer.com/slide/16485873/

[22]https://actualiteinformatique.fr/cybersecurite/definition-spoofing

[23] https://geekflare.com/fr/prevent-backdoor-virus-attacks/

[24]https://www.veracode.com/security/man-middle-attack

[25] https://blog.netwrix.fr/2018/07/04/les-10-types-de-cyberattaques-les-plus-courants/

[26]https://www.pandasecurity.com/fr/mediacenter/securite/attaque-man-in-the-middle/

[27]https://www.techno-science.net/glossaire-definition/Attaque-par-deni-de-service.html

[29] https://terranovasecurity.com/

[30] https://itigic.com/fr/cookie-theft-prevent-cybercriminals-from-stealing-them/

[33] http://www-igm.univ-mlv.fr/~dr/XPOSE2004/IDS/IDSPres.html

[35]https://www.techno-science.net/definition/1378.html

[36]https://fr.acervolima.com/architecture-ipsec/

[37]https://developers.google.com/search/docs/advanced/security/https?hl=fr

[38]https://fr-academic.com/dic.nsf/frwiki/1591636

[40]https://www.ionos.fr/digitalguide/serveur/securite/kerberos/

[41] https://actualiteinformatique.fr/cryptomonnaie/definition-cryptographie

[42]https://www.futura-sciences.com/tech/definitions/informatique-antivirus-10999/

[44] https://www.extenzilla.org/quels-sont-les-differents-types-de-vpn/

[46] https://www.forcepoint.com/fr/cyber-edu/firewall

[47]https://www.clicours.com/cours-informatique-le-fonctionnement-dun-systeme-pare-feu/

[49]https://wikimemoires.net/2012/08/quest-ce-quun-firewall-fonctionnement-et-types-de-firewall/

[50] https://fr.barracuda.com/glossary/dmz-network

Bibliographie

[3] ACISSI, Sécurité informatique Ethical Hacking Apprendre l'attaque pour mieux se défendre, ENI-Février 2015.

[4] Jean François Carpentier, sécurité informatique dans la petite entreprise Etat de l'art et bonnes pratiques, ENI-Décembre 2012.

[5] jean Françoise Pillou,tout sur la sécurité informatique,Dunod2016.

[6] Andra CODREANU, « sécurité des systèmes informatiques », projetFiabilité et contrôle de la qualité , UPB,2011.

[7] Solange Ghernaouti,Cybersécurité Analyser les risques mettre en œuvre les solutions,Dunodseptembre 2019.

[8] Raphael Yende, « Support de cours de sécurité informatique et crypto», HAL 25 décembre 2018.

[9] Cédric Liorens, Laurent Levier, Denis Valois, Tableaux de bordde la sécuritéréseau,Eyrolles, 2006.

[10] Laurent Bloch,ChristopheWolfhugel,Principes et méthodes à l'usage des DSI, RSSI et administrateurs, EYROLLES 2013.

[13] DjemahMassicilia, « Test d'intrusion interne avec une mise en place d'une solution de sécurité »,30/9/2015.

[15] MessahelNouara ,Saadikhadra , « l'installation et configuration d'un fierwall logiciel Pfsense ENIEM »,UMMTO 2016/2017

[18] YESGUER Fatima, « Implémentation d'une politique de sécurité pour une infrastructure réseau d'entreprise », UMMTO 2012/2013.

[19] JabouChaouki , Schillings Michaël, Hantach Anis , « TER Detection d'anomalies sur le réseau »,Université Paris-Descartes 2008/2009.

[28]DibounTerkouia,DahmaniHakima, « mise en place une solution de sécurité d'un réseau informatique cas d'un banque »,UMMTO 2013/2014.

[31] ATBANE Ramdane, «Proposition et implémentation d'une solution sécurité pour un réseau LAN», UMMTO 2017/2018.

[32] Nicolas Baudoin, Marion Karle, «NT Réseaux IDS et IPS» ,2003/2004

[34] MichaëlAMAND,Mohamed NSIRI, «Etude d'un système de détection d'instrusion comportemental pour l'analyse du trafic aèroportuaire», IENAC 2011.

[39] Saci Souhila, Batouche Sonia, «Etude et mise en place d'un système deDétection d'intrusion sous Linux» Université Abderrahmane Mira de Béjaïa2014/2015

[43] Mr KHERROUBI, Younes Mr IDIR Krim«Mise en œuvre d'une sécurité réseau basée sur l'utilisation du pare-feu PfSence Cas : Algérie Télécom de Tizi-Ouzou», UMMTO 22/09/2018.

[45] TALMAT AISSI Ghenima, AKNOUCHECelia , «Etude et configuration d'un système de sécurité ASA 5510» UMMTO 2017.

[48] BELALIA Mohamed cherif, MAACHE Khaled, «Etude et conception d'un Firewall», USDB 2010/2011.

Résumé

Avec l'essor d'Internet, et la majorité des entreprises et organisations utilisant des processus informatisés, les menaces contre les systèmes d'information n'ont cessé d'augmenter et de se complexifier, faisant de la sécurité informatique d'aujourd'hui une nécessité pour tous les types de structures.

Le but de ce travail est de créer une stratégie de sécurité pour pouvoir protéger au maximum le réseau informatique du CETIM, notre solution est basée sur un firewall open source "pfsense" qui nous offrir d'avoir un réel contrôle sur le trafic de l'entreprise réseau. Il aide à analyser, sécuriser et gérer le trafic réseau, et ainsi d'utiliser le réseau de la façon pour laquelle il a été prévu.

Mots-clés : Sécurité informatique, attaque, firewall, vulnérabilité, sécurité des réseaux informatique, risque.

Abstract

With the rise of the Internet, and the majority of companies and organizations using computerized processes, threats against information systems have continued to increase and become more complex, making today's computer security a necessity for all types of structures.

The purpose of this work is to create a security strategy to be able to protect the CETIM's computer network as much as possible; our solution is based on an open source firewall "pfsense" which offers us to have real control over the traffic of the network business. It helps analyze, secure, and manage network traffic, so you can use the network the way it was intended.

Keywords: Computer security, attack, firewall, vulnerability, computer network security, risk.

الملخص

مع صعود الإنترنت ، واستخدام غالبية الشركات والمؤسسات للعمليات المحوسبة ، استمرت التهديدات ضد أنظمة المعلومات في الزيادة وأصبحت أكثر تعقيدًا ، مما يجعل أمان الكمبيوتر اليوم ضرورة لجميع أنواع الهياكل .
الغرض من هذا العمل هو إنشاء إستراتيجية أمنية لتكون قادرًا على حماية شبكة كمبيوتر CETIM قدر الإمكان ، ويستند حلنا إلى جدار حماية مفتوح المصدر "pfsense" والذي يتيح لنا التحكم الحقيقي في حركة مرور الشبكة اعمال.
يساعد في تحليل حركة مرور الشبكة وتأمينها وإدارتها،حتى تتمكن من استخدام الشبكة بالطريقة التي تريدها.

الكلمات الرئيسية: أمن الكمبيوتر،الهجوم، جدار الحماية،الضعف، أمن شبكة الكمبيوتر، المخاطر.