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

AKKOUCHE Hassiba et MAHSAS Nesrine

Filière : Télécommunications

Spécialité : Réseaux et Télécommunications

Conception d'une passerelle internet sécurisée

Soutenu le 13/07/2021 devant le jury composé de:

Mr. AKLIOUAT	Hacene	MAA	UMBB	Président
Mme. MAHDI	Ismahane	MCB	UMBB	Examinatrice
Mme. MECHIDE	Samira	MAA	UMBB	Rapportrice

Année Universitaire : 2020/2021

Remerciement

Tout d'abord nous adressons nos plus sincères sentiments de reconnaissance et de remerciement envers ***ALLAH,*** *pour toute l'énergie qu'il nous a donnée durant ces cinq années, nous croyons au destin, nous pouvons traverser les moments difficiles en regardant toujours le bon côté de la chose, hamdoulillah.*

Nos pensées vont vers nos parents, qui ont toujours cru en nos. C'est Grâce à leur soutien et prières que nous avons accomplie ce travail.

Notre gratitude s'adresse à notre promotrice Mme ***MECHID Samira*** *pour son orientation, ses précieux conseils et Remarques.*

Comme nos remerciements notre encadreur Mr ***DELLAL Mohamed Amine*** *pour son orientation et la disponibilité qu'il nous a témoignée pour nous permettre de mener à bien ce travail. Ainsi que notre Co-encadreur, Mr* ***SOUISSI HICHEM****. Un grand merci pour ses précieux conseils.*

Nos vifs remerciements aux membres du jury d'avoir accepté d'examiner et d'évaluer notre travail. Un grand merci à tous les professeurs de Télécommunications qui ont participé à notre progrès pendant ces 5 ans.

Enfin, nos remerciements à tous nos amis, nos collègues qui nous ont soutenu et encouragé pour la réalisation de ce mémoire. Merci

Dédicace

Grace Allah

Je dédie ce modeste travail

À mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études,

A mes chères sœurs Ratiba et Wissem pour leurs encouragements permanents, et leur soutien moral,

A mes chers frères, Mohamed et Abdeslam pour leur appui et leur encouragement,

A toute ma famille pour leur soutien tout au long de mon parcours universitaire,

Que ce travail soit l'accomplissement de vos vœux tant allégués, et le fuit de votre soutien infaillible,

Merci d'être toujours là pour moi,

A tous mes enseignantes qui m'ont soutenu depuis 5 ans.

A Toute la promotion de l'année 2020-2021.

Hassiba

Dédicace

Grace Allah

Je dédie ce modeste travail

A Mes chers parents, qui m'ont soutenu depuis que j'ai vu le jour. Pour leur patience illimitée, leur amour et leurs grands sacrifices.

A mes frère adorées : Mohammed et Ayoub.

A ma très cher sœur « Lina» et son fils « Abderraouf »

Amon marie « Bilal »

A tous mes oncle : Mohammed et Abdelhamid et Hocine

A toutes mes tantes : Zahra et Nawel et zhour et khalida.

A meilleurs des enseignant Mme Mechide et Mr Messoudi et Mr Hammadouch.

A tous mes enseignantes qui m'ont soutenu depuis 5 ans.

A Toute la promotion de l'année 2020-2021.

Nesrine

Résumé

Le renforcement de la sécurité informatique est devenu une nécessité primordiale vu l'apparition des diverses formes d'attaques informatiques de nos jours. Et ce sont les réseaux d'entreprises, d'institutions, de gouvernements qui ont le plus besoin de cette sécurisation car elles sont fréquemment les cibles des attaques d'intrusion.Les pare-feu sont très populaires en tant qu'outils permettant d'élaborer efficacement des stratégies pour sécuriser un réseau informatique. Un firewall offre au système une protection d'un réseau interne, contre un certain nombre d'intrusions venant de l'extérieur, grâce à des techniques de filtrage rapides et intelligentes.

Ce projet à pour l'objectif d'étudier d'abord les concepts de la sécurité informatique en générale et en particulier la conception d'une passerelle internet sécurisée.Nous avons déployé les pare-feux « fortigate » qui contient une vaste fonctionnalités aprés nous avous configuré le filtrage du trafic du réseau LAN, ainsi que la création d'un tunnel VPN IPSec pour crypter les échanges et nous avons déployé aussi un serveur proxy pour bloquer les pages web.

Mots clés: sécurité informatique, attaque informatique, pare-feu, réseau informatique, filtrage, VPN IPSec, proxy.

Abstract

The reinforcement of computer security has become a primarynecessitygiven the appearance of variousforms of computer attacksthesedays. Moreover, itis the networks of companies, institutions and governmentsthatmostneedthissecuritybecausethey are frequentlytargets of intrusion attacks. Firewalls are verypopular as tools for effectivelydevelopingstrategies for securing a computer network. A firewall offers the system protection of an internal network, against a number of intrusions fromoutside, thanks to fast and intelligent filtering techniques.

The objective of this project is to first study the concepts of computer security in general and in particular the design of a secure internet gateway. We have deployed the "fortigate" firewalls which contain a wide range of functionalities after us. You have also configured the

filtering of LAN network traffic, as well as the creation of an IPSec VPN tunnel to encrypt the exchange and we have also deployed a proxy server to block web pages.

Keyword: Computer security, computer attack, firewall, computer network, filtering, VPN IPSec, proxy .

ملخص

أصبح تعزيز أمان الكمبيوتر ضرور ة أساسية نظرًا لظهور أشكال مختلفة من هجمات الكمبيوتر في الوقت الحاضر.حيث تحتاج شبكات الشركات والمؤسسات والحكومات إلى هذا الأمان أكثر من غيرها لأنها كثيرًا ما تكون أهدافًا لهجمات التسلل، من خلال تطوير استراتيجيات فعالة لتأمين شبكة الكمبيوتر.

يوفر جدار الحماية حماية النظام لشبكة داخلية، ضد عدد معين من التدخلات القادمة من الخارج، وذلك بفضل تقنيات التصفية السريعة والذكية.

الهدف من هذا المشروع هو دراسة مفاهيم أمان الكمبيوتر بشكل عام وبشكل خاص تصميم بوابة إنترنت آمنة. لقد نشرنا جدران الحماية "الحصينة" التي تحتوي على مجموعة واسعة من الوظائف. لقد قمنا أيضًا بتكوين تصفية حركة مرور شبكة LAN، وكذلك إنشاء نفق IPSec VPN لتشفير التبادلات و قمنا أيضًا بنشر خادم وكيل لحضر صفحات الويب.

الكلمات المفتاحية:

أمان الكمبيوتر، هجمات الكمبيوتر، جدار الحماية ، شبكة الكمبيوتر، التصفية، نفق، خادم وكيل.

Sommaire

Liste des figures

Liste des tableaux

Liste des abréviations

- **ACK** (Acknowledge)
- **ACL** (Access Control List)
- **DMZ** (Demilitarised Zone)
- **DNS** (Domain Name System)
- **DDOS** (Distributed Denial Of Service)
- **DOS** (Denial Of Service)
- **EVE-ng** (Emulated Virtual Environment – Next Generation)
- **FTP** (File Transfer Protocol)
- **HTTP** (Hypertexte Transfer Protocol)
- **HTTPS** (Hypertext Transfer Protocol Secure)
- **IP** (Internet Protocol)
- **IPSEC** (IP Security)
- **IETF** (Internet Engineering Task Force)
- **L2TP** (Layer 2ForwardingProtocol)
- **NAT** (Network Address Translation)
- **OSI** (Open Systems Interconnections)
- **PAT** (Port Address Translation)
- **PPTP** (Point-to-Point Tunneling Protocol)
- **SI** (System Informatique)
- **SSH** (Secure Socket Shell)
- **SSL** (Secure Socket Layer)
- **SQL** (Structured QueryLanguage)
- **TCP** (Transfer Control Protocol)
- **TLS** (Transport Layer Security)
- **UDP** (User Datagram Protocol)
- **URL** (Uniform Resource Locator)
- **VM** (Virtual Machines)
- **VPN** (Virtual Private Network)
- **VRRP** (Virtual Router Redondancy Protocol)

INTRODUCTION GÉNÉRALE

Introduction

Aujourd'hui, toutes les entreprises possédant un réseau local et nécessitant une interconnexion avec Internet, afin d'accéder à l'information disponible sur le réseau, et de pouvoir communiquer avec l'extérieur. Cette ouverture vers l'extérieur est indispensable et dangereuse en même temps car il rend l'entreprise vulnérable aux risques.

Ouvrir l'entreprise vers le monde signifie aussi laisser place ouverte aux étrangers pour essayer de pénétrer le réseau local de l'entreprise, et y accomplir des actions douteuses, parfois gratuites, de destruction, vol d'information confidentielles…

C'est pour cela que la sécurité Internet est devenue un sujet de recherche très intense.

Ces recherches ont permis le développement d'une passerelle Internet sécurisée mettant en œuvre au minimum des fonctions de filtrage périmétriques ainsi que des services applicatifs relais. Cette passerelle doit être incontournable.

La sécurité du réseau signifie assurer la sécurité du trafic Internet entre eux, les ressources de l'entreprise telles que le siège social ou le centre de données et les employés distants.

La sécurité informatique s'intéresse aussi à la protection contre les risques liés à l'informatique ; elle doit prendre en compte :

- les éléments à protéger : matériels, données, utilisateurs.
- leur vulnérabilité.
- leur sensibilité : quantité de travail impliqué, confidentialité…
- les menaces qui pèsent sur eux. [3]

C'est dans ce cadre que s'inscrit notre projet « Conception d'une passerelle internet sécurisé », réalisé au sein du Mobilis ATM (ATM acronyme d'Algérie Télécom Mobile), est un opérateur de téléphonie mobile algérienne, filiale d'Algérie Télécom.

Problématique

Internet est devenu un canal de communication indispensable pour les entreprises pour informer leurs clients des promotions et nouveauté de l'entreprise, Ces communications imposent une ouverture des systèmes d'information vers l'extérieur, notamment vers Internet.

Ainsi conjuguées, cette ouverture et cette dépendance rendent l'entreprise vulnérable aux risques ou affronter des conséquences qu'elle n'avait même pas imaginées parmi ces mesures

est mettre en place une passerelle internet qui dispose d'un outillage tout matériel et logiciel afin d'assurer une sécurité optimale.

Objectif

Dans notre démarche, D'abord, nous avons présenté une étude théorique de conception d'une architecture passerelle internet sécurisé, enfin nous présentons un cas pratique de l'implémentation d'une passerelle internet sécurisé.

- Concevoir une architecture passerelle internet sécurisé.
- Déployer un FIREWALL pour protéger le réseau interne.
- Déployer un PROXY
- Déployer un tunnel VPN IPSec.

De manière spécifique, Dans ce mémoire, nous adopterons une organisation comportant quatre principaux Chapitres.

Dans le premier chapitre, nous présentons une étude complète sur la sécurité informatique en se focalisant sur les risques et les défauts de sécurité existants ainsi que l'établissement d'une bonne stratégie de la politique de sécurité.

Dans le deuxième chapitre, nous allons définir plusieurs menaces de sécurité, pouvant résulter des systèmes de communications informatiques, au moyen de la piraterie, des attaques ainsi que des virus informatique.

Dans le troisième chapitre, nous présentons les mécanismes de la sécurité informatique telle que les outils nécessaires pour l'assurer.

Le dernier chapitre présente la phase de conception, Mettre en place une architecture de passerelle internet sécurisé qui dispose d'un outillage tout matériel et logiciel afin d'assurer une sécurité optimale.

Ce projet se termine par une conclusion générale résumant l'essentiel des travaux menés.

CHAPITRE I :

GÉNÉRALITÉ

I.1 Introduction

Aujourd'hui Internet est devenu important pour les entreprises, c'est devenu un média à part entière dans la mesure où il entre dans la stratégie de communication de celle-ci. C'est devenu aussi une vitrine pour ces dernières afin de faire connaître leurs produits, leurs services et acquérir ou fidéliser des clients.

Ainsi conjuguées, l'ouverture de l'entreprise vers Internet rend l'entreprise vulnérable aux risques. C'est pour cela que la sécurité Internet est devenue un sujet de recherche très intense.

Notons cependant que notre premier chapitre s'intéressera particulièrement à « **les notions du sécurité informatique ».**

Dans ce chapitre, nous faisons un survol des notions de sécurité informatique, telle que les objectifs de la sécurité informatique, et mise en place d'une politique de sécurité, mais avant définir ces notions il est nécessaire de définir l'utilité de l'internet dans l'entreprise et les risques qui menacent l'entreprise.

I.2 L'internet dans l'entreprise

I.2.1 Présentation

L'Internet est un vaste outil d'information et de communication en pleine évolution offrant des perspectives de croissance exceptionnelles. C'est devenu un formidable moyen de communiquer, d'échanger, de travailler, de rencontrer, d'apprendre et même de commercer.
Internet est devenu un canal de communication indispensable aujourd'hui. Il est devenu important non seulement pour les grandes entreprises, mais également les petites et moyennes entreprises.

I.2.2 Les services à travers l'internet dans l'entreprise

Afin de déployer une infrastructure d'interconnexion répondant au juste besoin fonctionnel de l'entité, il est nécessaire d'établir de manière exhaustive une liste des services du système informatique (SI) de l'entité (applications métier, services d'infrastructure) nécessitant une interconnexion à Internet, en distinguant les flux entrants et les flux sortants. Cette liste doit être mise à jour dès que nécessaire et revue régulièrement.

À titre d'exemple, voici une liste exhaustive de services nécessitant une interconnexion à Internet :

- la publication des sites Web.
- la récupération de sources ou de mises à jour logicielles depuis des sites de confiance.
- la résolution de noms DNS publics.
- les services publics de l'entité exposés sur Internet (ex : hébergements Web, DNS publics).
- les services d'infrastructures de l'entité exposés sur Internet (ex : passerelle VPN IPsec ou TLS pour les accès nomades, passerelle VPN IPsec pour des tunnels site à site).
- les services collaboratifs de l'entité exposés sur Internet (ex : messagerie, téléphonie, visioconférence, portail Extranet).
- les services métier de l'entité exposés sur Internet (ex : EDI 2).
- l'accès à Internet pour les employeurs**. [1]**

I.3 Les risques liés à la sécurité informatique

I.3.1 Présentation

La sécurité des systèmes d'information est de plus en plus abordée à l'aide d'approches basées sur les risques. L'expérience montre que de telles études prospectives réduisent de manière considérable les pertes liées aux faiblesses de sécurité des systèmes d'information.
La gestion des risques est définie par l'ISO comme l'ensemble des activités coordonnées visant à diriger et piloter un organisme vis-à-vis du risque. On dégage en général trois finalités à la gestion des risques pour les systèmes informatiques (SI) :

1. Améliorer la sécurisation des systèmes d'information.
2. Justifier le budget alloué à la sécurisation du système d'information.
3. Prouver la crédibilité du système d'information à l'aide des analyses effectuées.

I.3.2 Etudes des risques liés 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 avec les solutions et les coûts associés.

L'ensemble des solutions retenues sont organisés 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 ? **[3]**

En fait, avec le développement de l'utilisation d'internet, nombre d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs. 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 entre coûts, risques et contraintes. On comprendra mieux le poids d'un risque en se fiant à la formule suivante :

$$\mathbf{Risque} = \frac{\mathbf{Menace} * \mathbf{Vulnerabilite}}{\mathbf{Contremesure}} \qquad [3]$$

- **Risque** : C'est la probabilité qu'une menace exploite une vulnérabilité. Autrement dit, c'est une possibilité qu'un fait dommageable se produise.
- **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.
- **Menace** : C'est le danger (interne ou externe) tel qu'un hacker, un virus, etc.

- **Contre-mesure** : C'est un moyen permettant de réduire le risque dans une organisation. **[3]**

A partir 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.

Figure 1:Les deux cas du risques [3]

Avec :

R : Risque.

M : Menace.

V : Vulnérabilité.

CM : Contre-mesure.

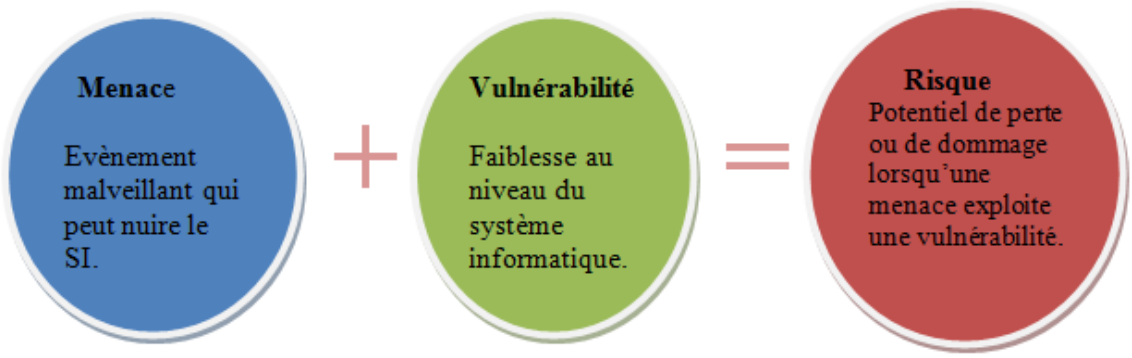

Figure 2: La différence entre menace et vulnérabilité, risque.

I.3.3 Les types des risques

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

I.3.3.1 Risques humains

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

On peut citer :

- **La maladresse :** commettre des erreurs ou exécuter de traitement non souhaité, ou effacer involontairement des données ou des programmes ; exemple: Mauvaises configurations (les erreurs de configuration, mots de passe par défaut).
- **L'inconscience et l'ignorance** : introduire des programmes malveillants sans le savoir (par exemple lors de la réception du courrier). Des nombreux utilisateurs d'outils informatiques sont encore inconscients ou ignorants des risques qu'ils font courir aux systèmes qu'ils utilisent. Réaliser des manipulations inconsidérées (autant avec des logiciels qu'avec du matériel) ;
- **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'ingénierie sociale :** une méthode pour obtenir d'une personne des informations confidentielles, que l'on n'est pas normalement autorisé à obtenir, en vue de les exploiter à d'autres fins. **[3]**

I.3.3.2 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. **[3]**

I.4 Le système d'information et la sécurité

I.4.1 Présentation

Le système d'information représente l'ensemble des données de l'entreprise ainsi que ses infrastructures matérielles et logicielles. Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger. **[2]**

La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. L'objectif de la sécurité informatique est d'assurer que les ressources matérielles et/ou logicielles d'un parc informatique sont uniquement utilisées dans le cadre prévu et par des personnes autorisées.

La sécurité informatique est de nos jours devenue un problème majeur dans la gestion des réseaux d'entreprise ainsi que pour les particuliers. Toujours plus nombreux à se connecter à Internet. La transmission d'information sensible et le désire d'assurer la confidentialité de celles-ci est devenue un point primordial dans la mise en place des réseaux informatiques.

La sécurité informatique vise généralement cinq principaux objectifs :

- **La confidentialité:** Seule les personnes habilitées doivent avoir accès aux données. Tout interception ne doit pas être en mesure d'aboutir, les données doivent être cryptées, seuls les acteurs de la transaction possèdent la clé de compréhension.
- **L'intégrité :** Il faut garantir à chaque instant que les données qui circulent sont bien celles que l'on croit, qu'il n'y a pas eu d'altération (volontaire ou non) au cours de la communication. L'intégrité des données doit valider l'intégralité des données, leur précision, l'authenticité et la validité.
- **La disponibilité :** Il faut s'assurer du bon fonctionnement du système, de l'accès à un service et aux ressources à n'importe quel moment. La disponibilité d'un équipement

se mesure en divisant la durée durant laquelle cet équipement est opérationnel par la durée durant laquelle il aurait dû être opérationnel.

- **La non-répudiation :** de l'information qui est la garantie qu'aucun des correspondants ne pourra nier la transaction. **[2]**
- **L'authentification :** Elle limite l'accès aux personnes autorisées. Il faut s'assurer de l'identité d'un utilisateur avant l'échange de données.

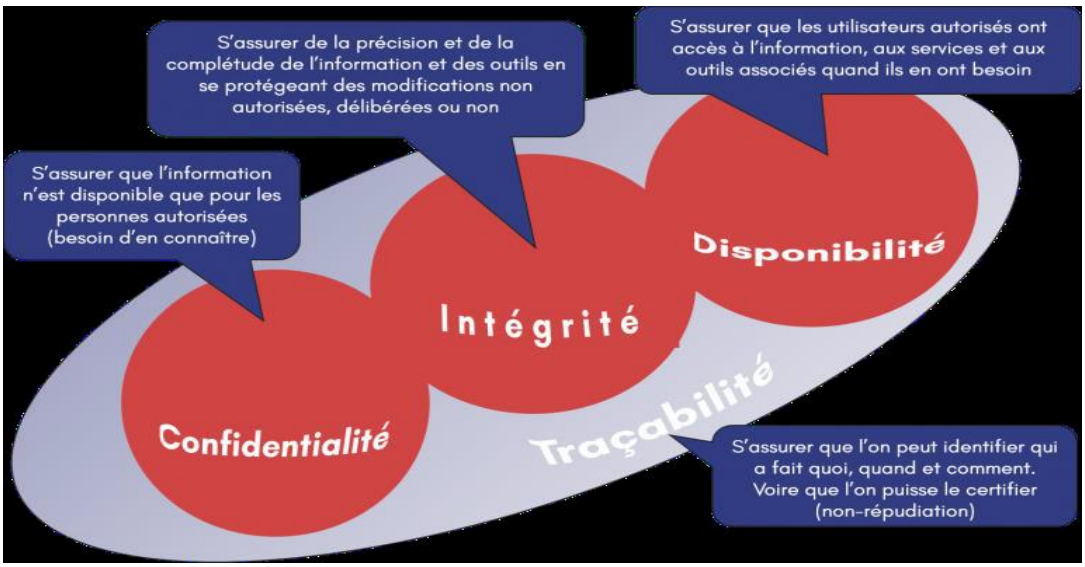

Figure 3: CIA (confidentiality, integrity, availability).

I.4.2 Nécessité 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.

Cela signifie que la sécurité doit être abordée dans un contexte global et notamment prendre en compte les aspects suivant :

- **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**. [2]**

I.4.3 Principaux défauts de sécurité informatique

Les défauts de sécurité peuvent être considérés comme des modifications accidentelles ou inconscientes du fonctionnement normal des équipements informatiques.

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.
- Faiblesses des protocoles.
- 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. **[3]**

I.4.4 Mise en place d'une 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 mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des ressources possèdent uniquement les droits qui leur ont été octroyés.

La sécurité informatique doit toutefois être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance. C'est la raison pour laquelle il est nécessaire de définir dans un premier temps une politique de sécurité, dont la mise en œuvre se fait selon les quatre étapes suivantes :

- Identifier les besoins en termes de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences.
- Elaborer des règles et des procédures à mettre en ouvre dans les différents services de l'organisation pour les risques identifiés.

- Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés. **[2]**

La politique de sécurité est donc l'ensemble des orientations suivies par organisation en termes de sécurité.

I.5 Conclusion

L'Internet est devenu important pour les entreprises en même temps rend l'entreprise vulnérable aux risques. C'est pour cela que la sécurité Internet est devenue un sujet de recherche très d'actualité.

Pour définir les menaces informatique et des mécanismes de sécurisation, il est nécessaire de définir avant tout, l'utilité de l'internet dans l'entreprise, les risques qui menacent l'entreprise et les objectifs de sécurité, pour obtenir tant que possible une sécurisation assez fiable de réseaux.

CHAPITRE II : LES MENACES INFORMATIQUES

II.1 introduction

En entreprise, c'est le réseau local qui est connecté à Internet, Et chaque ordinateur connecté à Internet et d'une manière plus générale à n'importe quel réseau informatique, est susceptible d'être victime d'une attaque d'un pirate informatique.

Dans ce chapitre, nous allons montrer les menaces informatiques telles que les attaques informatiques, les pirates et les virus informatiques.

II.2 Les attaques informatiques

II.2.1 Présentation

Une **attaque** est l'exploitation d'une faille (vulnérabilité ou brèche) d'un système informatique (système d'exploitation, logiciel ou bien même de l'utilisateur) à des fins non connues par l'exploitant du système et généralement préjudiciables **[8].**

II.2.2 Les motivations des attaques

Les motivations des attaques peuvent être assez simples. Les motivations principales qui animent la grande majorité des attaquants sont l'argent, la concourante et l'information.

Les motivations financières et d'espionnage représentent 93 % des motivations des attaques. D'autres motivations moins fréquemment rencontrées touchent à la recherche de plaisir, l'idéologie, la volonté de nuire**. [14]**

Parmi les motivations les plus courantes, on trouve les suivantes :

- **Motivation d'Argent :**

Un nombre très important de cyber attaques est motivé par le gain financier. On y retrouve les logiciels de rançon (ransomware), les campagnes de phishing et le vol de données.

Lorsque les données sont volées, ces données sont revendues sur le Dark Web, certaines données ayant une valeur marchande supérieure (données de santé notamment). **[14]**

- **Attaques provenant de concurrents :**

Entrer dans le système d'information d'un concurrent peut être extrêmement utile, que ce soit pour des raisons de vol de propriété intellectuelle, de chantage, de veille concurrentielle; C'est le moyen de nuire à l'image de son concurrent, de mobiliser les

ressources sur des sujets de violation de données personnelles au lieu de mobiliser les ressources sur la dynamique commerciale ou l'innovation. **[14]**

Dans le domaine industriel, qu'il s'agisse de secteurs technologiques, de l'industrie pharmaceutique, de fabrication de haute technologie, d'extraction de ressources, de services publics généraux, de systèmes industriels ou de secteurs similaires, au regard du manque de sophistication technique des systèmes dans les industries dont le cœur est la propriété intellectuelle complexe, les attaques informatiques motivées par des concurrents constituent un risque fort à prendre en compte. **[14]**

- **Motivations politiques :**

Comme nous le constatons avec de nombreux acteurs étatiques, la cybercriminalité est un outil de plus en plus utilisé pour atteindre des objectifs politiques. Qu'il s'agisse de piratage informatique pour couper l'électricité d'un pays, manipuler les élections ou semer le trouble avec la diffusion de Ransomware, l'action de l'État est une menace croissante pour toutes les organisations - même si elles ne sont pas forcément une cible directe. **[14]**

- **Autres motivations :**

Certains attaquants prennent plaisir à pouvoir exploiter les faiblesses des systèmes informatiques. D'autres le font pour des raisons idéologiques ou par simple plaisir de divulguer des informations jugées d'intérêt public. Enfin il existe une population de cybercriminels qui par simple rancune, parce qu'ils sont mécontents d'un service, d'un produit défectueux ou pour régler leur compte avec quelqu'un. **[14]**

II.2.3 Les objectifs des attaques

Les objectifs des attaques peuvent être :

- Obtenir un accès au système.
- Voler des informations, tels que des secrets industriels ou des propriétés intellectuelles.
- Glaner des informations personnelles sur un utilisateur.
- Récupérer des données bancaires.

- S'informer sur l'organisation (entreprise de l'utilisateur, etc.).
- Troubler le bon fonctionnement d'un service.
- Utiliser les ressources du système de l'utilisateur, notamment lorsque le réseau sur lequel il est situé possède une bande passante élevée, etc.
- Utiliser le système de l'utilisateur comme « rebond » pour une attaque.

II.2.4 Les types d'attaques

Les attaques peuvent être regroupées en deux familles différentes :

II.2.4.1 Attaque directe :

C'est la plus simple des attaques. L'hacker attaque directement sa victime à partir de son ordinateur par des scripts d'attaques faiblement paramétrable.

Les programmes de hack qu'ils utilisent envoient directement les paquets à la victime. Dans ce cas, il est possible en général de remonter à l'origine de l'attaque, identifiant par la même occasion l'identité de l'attaquant.

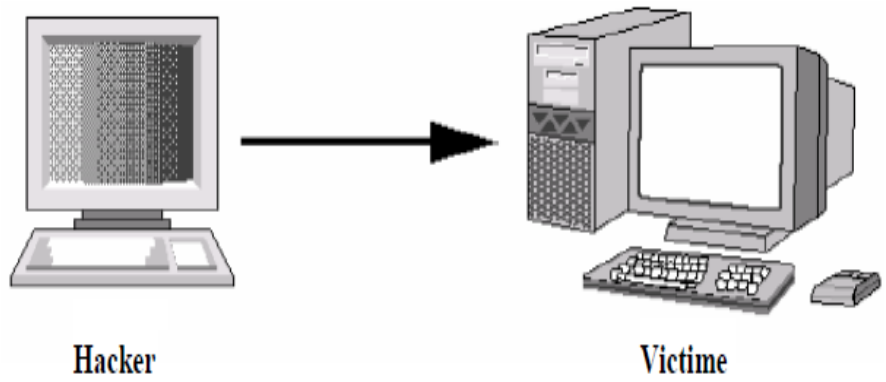

Figure 4: Attaque directe. [4]

II.2.4. Attaque indirecte :

- **Par rebond :** Les attaques par rebond consistant à attaquer une machine par l'intermédiaire d'une autre machine, afin de masquer les traces permettant de remonter

à lui (telle que son adresse IP) de dans le but d'utiliser les ressources de la machine servant de rebond.

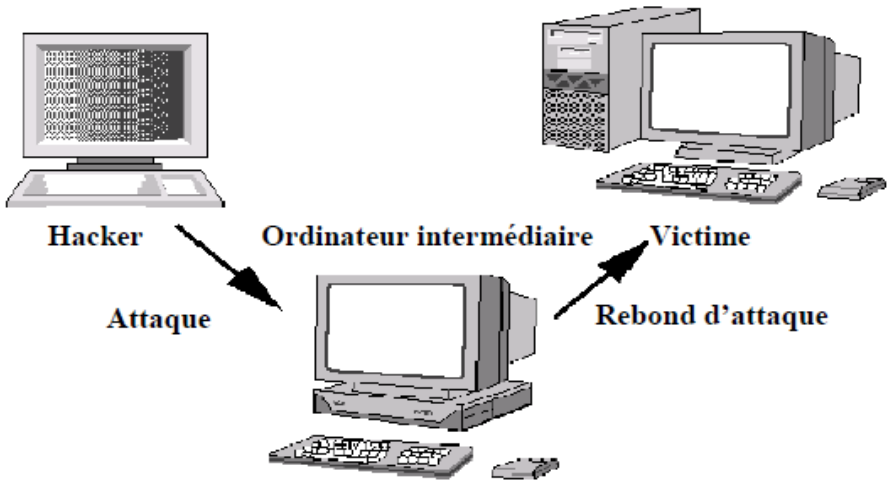

Figure 5:Attaque indirecte par rebond. [4]

- **Par réponse :** Cette attaque est un dérivé de l'attaque par rebond. Elle offre les mêmes avantages, du point de vue du hacker. Mais au lieu d'envoyer une attaque à l'ordinateur intermédiaire pour qu'il la répercute, l'attaquant va lui envoyer une requête. Et c'est cette réponse à la requête qui va être envoyée à l'ordinateur victime.

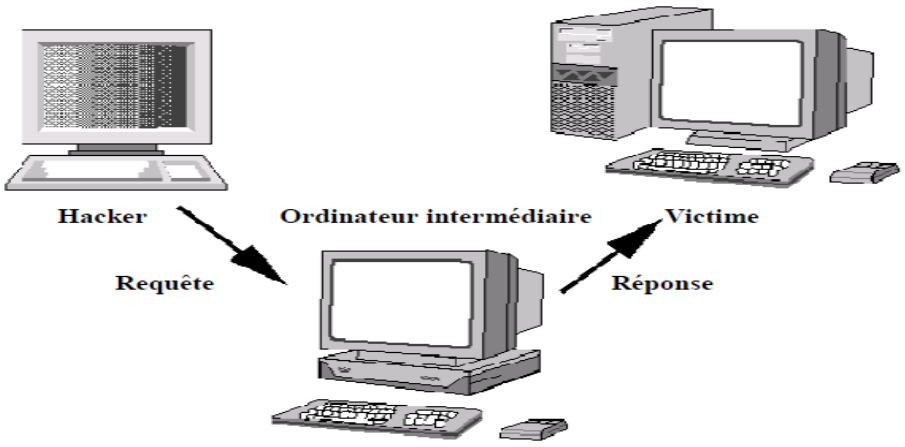

Figure 6: Attaque indirecte par réponse. [4]

II.2.5 Classification d'attaques

Les attaques touchent généralement les trois niveaux suivants : réseau, système, application.

II.2.5.1 Attaques réseaux

II.2.5.1.1 Les sniffers :

Un sniffer (analyseur réseau) est un dispositif permettant d'écouter le trafic d'un réseau, c'est-à-dire de capter les données qui transitent dans un réseau afin de collecter des informations telles que des mots de passes transmis en clair [4].

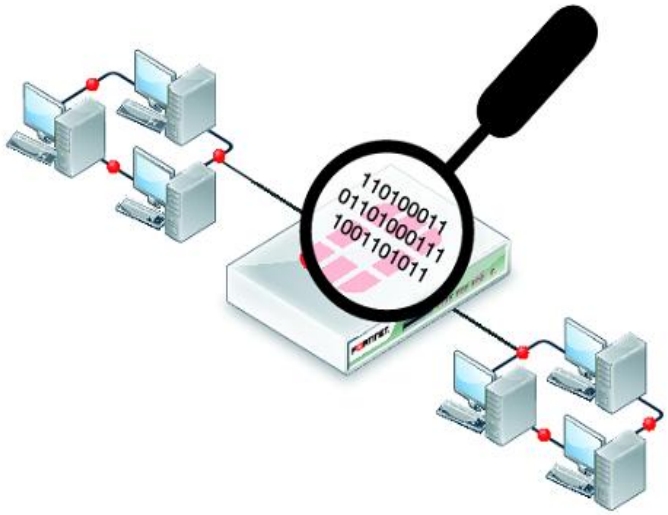

Figure 7:Attaque sniffer. [15]

II.2.5.1.2 L'IP Spoofing:

Le Spoofing est une technique permettant de s'infiltrer dans un ordinateur en se faisant passer pour un hôte de confiance (Trusted Host). Avant de rentrer dans des détails plus techniques, voici un bref résumé du fonctionnement de cette technique: une station se fait passer pour une autre en envoyant un paquet dont l'adresse IP est autorisée par le serveur visé. La source IP envoyée trompe donc la cible qui accorde l'accès en pensant avoir affaire à une machine de confiance.

Le spoofing peut être utilisé pour :

- 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.

Il existe différents types de Spoofing, nous n'aborderons ici que les notions d'IP Spoofing, celles ayant traits aux DNS Spoofing, Web Spoofing . . ..

❖ **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'ARP (Address Résolution Protocol) est un protocole qui convertit les adresses IP en adresses MAC (Media Access Control) pour la transmission des données. 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.

❖ **Spoofing du serveur DNS :**

Les serveurs DNS (Domain Name System) 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.

II.2.5.1.3 Attaque Man In The Middle

L'attaque man-in-the-middle (MITM) ou « attaque de l'homme du milieu » est une technique de piratage informatique consistant à intercepter des échanges cryptés entre deux personnes ou deux ordinateurs pour décoder les messages. L'attaquant doit donc être capable de recevoir les messages des deux parties et d'envoyer des réponses à une partie en se faisant passer pour l'autre. Le biais le plus couramment employé pour ce type d'attaque est une connexion Internet entre des ordinateurs et/ou des terminaux mobiles.

Voici quelques types courants d'attaques de l'homme du milieu :

❖ **ARP Poisoning :**

C'est l'attaque la plus célèbre des attaques « **man in the middle** », elle consiste à s'interposer entre deux machines du réseau et de transmettre à chacune un paquet ARP falsifié indiquant que l'adresse MAC de l'autre machine a changé, et l'adresse MAC fournie étant celle de l'attaquant. Les deux machine cibles vont ainsi mettre à jour leurs tables dynamique appelées Cache ARP. De cette manière, à chaque fois qu'une des deux machines souhaitera communiquer avec la machine distante, les paquets seront envoyés à l'attaquant, qui les transmettra de manière transparente à la machine destinatrice.

❖ **Vol de session TCP (TCP session hijacking) :**

L'ARP poisoning permet de rediriger tout le trafic IP mais, si l'attaquant n'a besoin que du trafic TCP, il peut interférer entre une connexion client-serveur pour rediriger le flux du client vers lui. La synchronisation TCP est assurée par les numéros de séquences TCP. Si, pendant un échange, l'attaquant envoie des paquets malformés au client avec une adresse IP correspondant à celle du serveur en y plaçant des mauvais numéros de séquences, le client va croire qu'il a perdu la connexion et stoppera ses échanges avec le serveur. Mais si l'attaquant envoie les bons numéros de séquences au serveur, il récupèrera la connexion pour lui.

Par exemple, l'attaque pourrait se dérouler ainsi :

- ✓ Un client se connecte à un serveur.
- ✓ L'ordinateur de l'attaquant prend le contrôle du client.
- ✓ L'ordinateur de l'attaquant déconnecte le client du serveur.
- ✓ L'ordinateur de l'attaquant remplace l'adresse IP du client par sa propre adresse IP et son propre nom de domaine et usurpe les numéros de séquence du client.
- ✓ L'ordinateur de l'attaquant poursuit le dialogue avec le serveur, le serveur croit qu'il communique toujours avec le client. **[9]**

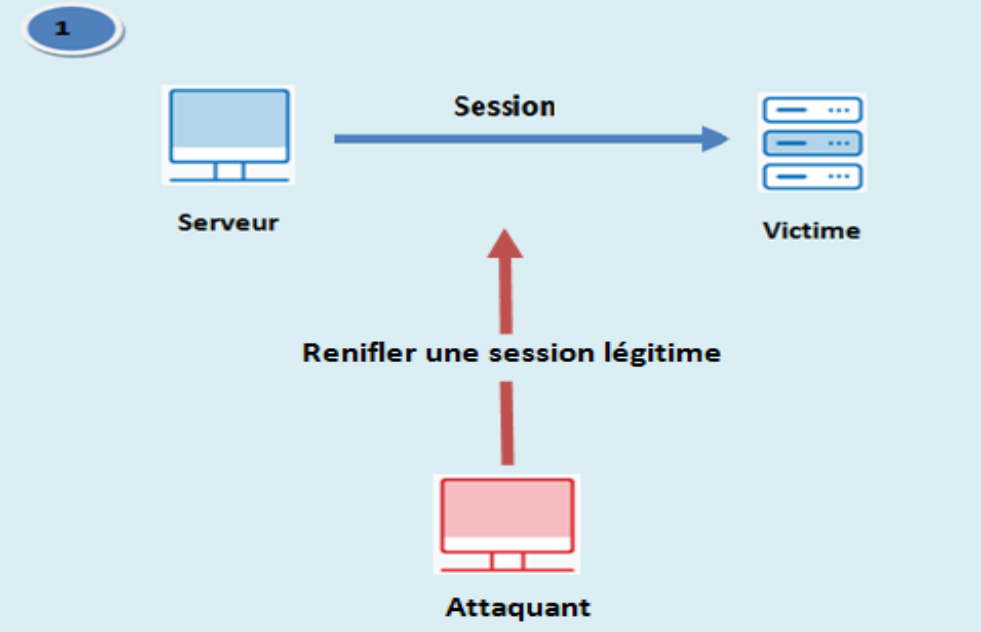

Figure 8: Exemple d'une attaque Vol de session TCP (étape 1). [9]

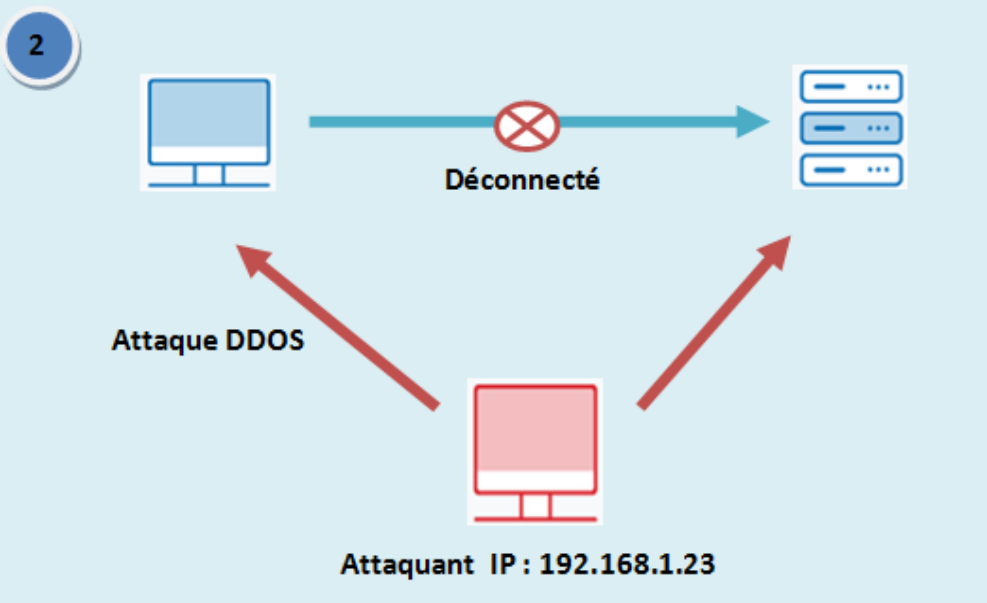

Figure 9: Exemple d'une attaque Vol de session TCP (étape 2). [9]

II.2.5.1.4 Déni de service (DoS)

Les attaques de type Denial-of-Service (DoS) ont pour but de saturer un routeur ou un serveur afin de le crasher ou en préambule d'une attaque massive. Ces types d'attaque sont

très faciles à mettre en place et très difficile à empêcher. Mais quelles sont les raisons qui peuvent pousser un attaquant à utiliser les DoS en sachant que cela peut mener à la des tractions du routeur ou du serveur visé :

❖ **Récupérer un accès**

Une attaque de type Denial-of-Service fait, la plupart du temps, partie d'une attaque visant à obtenir le contrôle d'une machine ou d'un réseau. Par exemple l'attaque de type **SYN Flood**, très répandue, est souvent utilisée de paire avec une tentative de **Spoofing**.

❖ **Masquer les traces**

Ce type d'attaque permet également de **crasher** une station qui par exemple aurait contenir des traces du passage d'un **Hacker**. En détruisant cette station, il s'assure ainsi une certaine pérennité.

❖ **Se venger**

Très fréquemment, ces attaques sont utilisées afin d'assouvir une vengeance personnelle contre une personne, un administrateur ou bien encore une entreprise. . . . . .

Voici quelques exemples de programmes disponibles sur Internet permettant de réaliser ce genre d'attaque:

- Ping'O Death.
- Land – Blat.
- Jolt.
- Tear Drop – SynDrop**. [4]**

II.2.5.2 Attaques systèmes

II.2.5.2.1 Les malwares

Un malware est un logiciel développé dans le but de nuire à un système informatique.

Il existe plusieurs familles de malwares, On va définir les plus intéressantes :

❖ **Les virus :**

Un virus est un petit programme informatique situé dans le corps d'un autre, qui, lorsqu'on l'exécute, se charge en mémoire et exécute les instructions que son auteur a programmé.

❖ **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. [6]

Les chevaux de Troie peuvent être classés selon leur façon d'infecter des systèmes et le type de dommages dont ils sont la cause. Sept types principaux de chevaux de Troie ont été identifiés :

- Chevaux de Troie pour accès à distance.
- Chevaux de Troie pour envoi de données.
- Chevaux de Troie destructeurs.
- Chevaux de Troie pour proxy.
- Chevaux de Troie pour FTP.
- Chevaux de Troie pour désactivation de logiciel de sécurité.
- Chevaux de Troie pour attaque par déni de service.

❖ **Les Vers :**

Un ver informatique est un programme qui peut s'auto reproduire et se déplacer à travers un réseau en utilisant ses mécanismes, sans avoir réellement besoin d'un support physique au logique (disque dur, programme hôte, fichier, etc.) pour propager.

❖ **Les Rootkits :**

Les rootkits sont des logiciels qui permettent au cybercriminel de contrôler à distance l'ordinateur d'une victime avec des privilèges administratifs complets. **[6]**

❖ **Les bombes logiques :**

Les bombes logiques sont les virus dont le déclanchement s'effectuer à un moment déterminé en exploitant la date du système, le lancement d'une commande, ou n'importe quel appel au système.

❖ **Spywares :**

Un spyware est un type de programme qui s'installe sur un ordinateur personnel, avec ou sans permission, afin de collecter des informations sur l'utilisateur, son ordinateur ou ses habitudes de navigation, de suivre tout ce qu'il fait sans qu'il le sache, et d'envoyer ces données à un utilisateur distant. Le spyware peut aussi télécharger d'autres programmes

malveillants depuis Internet et les installer sur votre ordinateur. Un spyware fonctionne comme un logiciel publicitaire mais, généralement, c'est un programme séparé qui s'installe incognito lorsque vous installez un autre programme ou application de type freeware. **[7]**

II.2.5.2.2 Attaque de mot de passe

Voici quelque type d'attaques de mots de passe courantes et les étapes que vous pouvez suivre pour les empêcher ou au moins réduire leurs chances de réussite.

- **Attaque par dictionnaire :**

Une attaque qui profite du fait que les utilisateurs ont tendance à employer des mots communs et des mots de passe courts. Le pirate utilise une liste de mots communs, le dictionnaire, et les essaye, bien souvent avec des chiffres avant et/ou après les mots, à l'encontre des comptes d'une entreprise pour chaque nom d'utilisateur. (Les noms d'utilisateur sont généralement très simples à identifier car ils sont presque toujours basés sur le nom des employés). **[8]**

- **Attaque par force brute :**

Utilisation d'un programme pour générer des mots de passe potentiels ou même des ensembles de caractères aléatoires. Ces attaques commencent par les mots de passe faibles et couramment utilisés, comme Motdepasse123 puis évoluent. Les programmes qui exécutent ces attaques essayent habituellement des variantes avec des majuscules et minuscules. **[8]**

- **Attaque hybride :**

L'attaque hybride vise particulièrement les mots de passe constitués d'un mot traditionnel et suivi d'une lettre ou d'un chiffre. Elle s'agit d'une combinaison des attaques précédentes.

II.2.5.2.3 Porte dérobée « backdoor »

Depuis que les intrusions informatiques existent, leurs adeptes ont mis au point un certain nombre de techniques leur facilitant l'accès aux systèmes pénétrés. La technique la plus connue, et sans doute la plus utilisée, est celle des Backdoors (portes dérobées ou portes de service).

La backdoor est un point d'entrée dans un programme ou un système plus au moins secret. **[17]** Elle permette, à celui qui en connait l'existence et le fonctionnement, de revenir sur un système de façon détournée, c'est-à-dire sans passer par les méthodes d'authentification habituelles.

II.2.5.3 Attaques applicative

II.2.5.3.1 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**.[9]**

II.2.5.3.2 Injection SQL

Grâce à l'injection SQL, les pirates peuvent exécuter des commandes non autorisées sur la base de données SQL d'une victime.

Les attaques par injection de commandes SQL sont des attaques visant les sites web s'appuyant sur des bases de données relationnelles. Dans ce type de sites, des paramètres sont passés à la base de données sous forme d'une requête SQL. Ainsi, si le concepteur n'effectue aucun contrôle sur les paramètres passés dans la requête SQL, il est possible à un pirate de modifier la requête afin d'accéder à l'ensemble de la base de données, voire à en modifier le contenu.

Un certain nombre de règles permettent de se prémunir des attaques par injection de commandes SQL :

- Vérifier le format des données saisies et notamment la présence de caractères spéciaux.

- Ne pas afficher de messages d'erreur explicites affichant la requête ou une partie de la requête SQL.
- Supprimer les comptes utilisateurs non utilisées, notamment les comptes par défaut.
- Eviter les comptes sans mot de passe.
- Restreindre au minimum les privilèges des comptes utilisés.
- Supprimer les procédures stockées.

En effet, certains caractères permettent d'enchaîner plusieurs requêtes SQL ou bien ignorer la suite de la requête. Ainsi, en insérant ce type de caractères dans la requête, un pirate peut potentiellement exécuter la requête de son choix. **[10]**

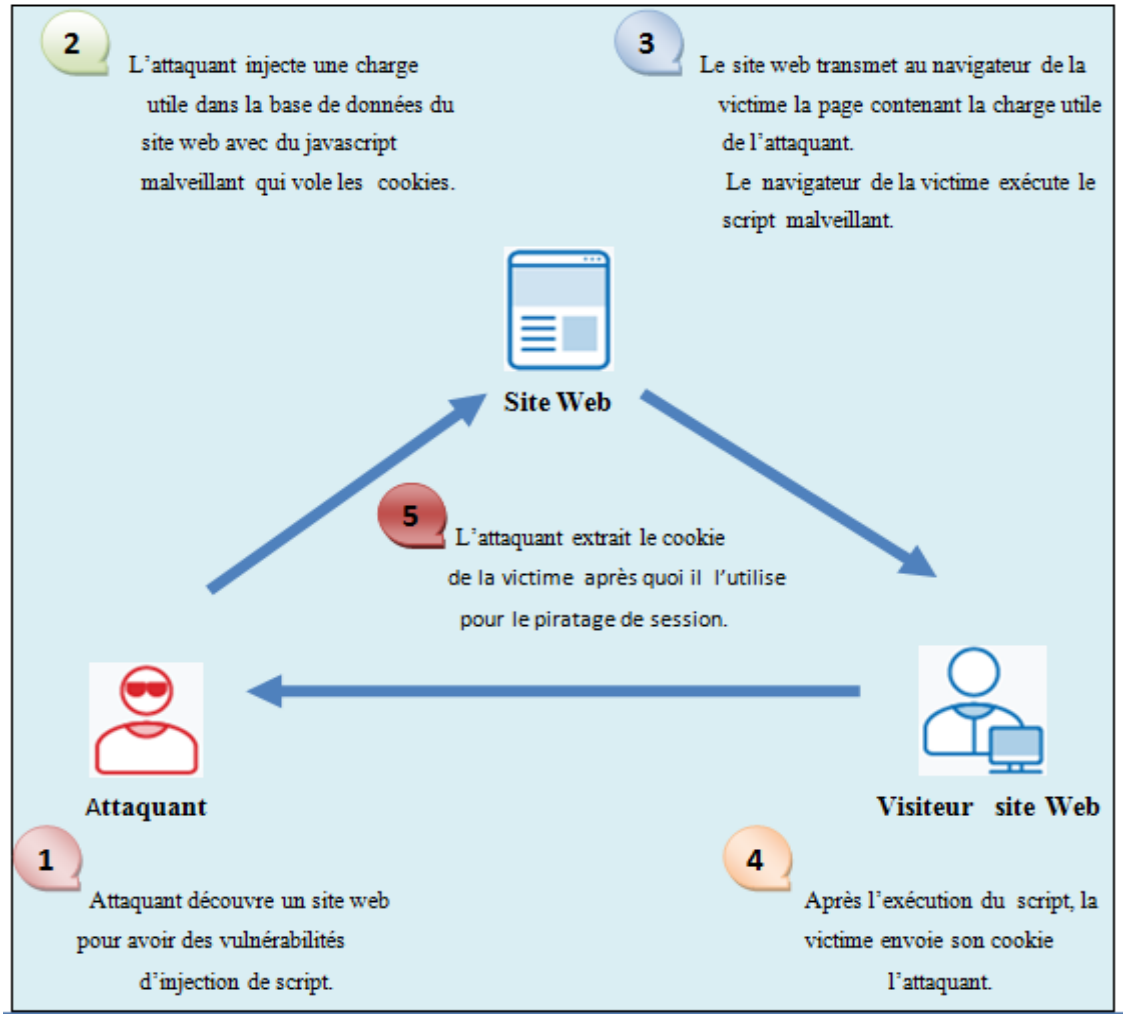

Figure 10:Attaque Injection SQL.

II.2.5.3.3 Attaques phishing et spear phishing

L'attaque phishing (hameçonnage) consiste à envoyer des e-mails qui semblent provenir de sources fiables dans le but d'obtenir des informations personnelles ou d'inciter les utilisateurs à faire quelque chose. Cette technique combine ingénierie sociale et stratagème technique. Elle peut impliquer une pièce jointe à un e-mail, qui charge un logiciel malveillant sur votre ordinateur. Elle peut également utiliser un lien pointant vers un site Web illégitime qui vous incite à télécharger des logiciels malveillants ou à transmettre vos renseignements personnels.

Le harponnage (spear phishing) est un hameçonnage très ciblé. Les attaquants prennent le temps de mener des recherches sur leurs cibles et de créer des messages personnels et pertinents. Pour cette raison, le harponnage peut être très difficile à identifier et encore plus difficile à combattre. L'un des moyens les plus simples pour un pirate de mener une attaque de harponnage est d'usurper une adresse électronique, c'est-à-dire de falsifier la section « De » d'un e-mail, pour vous donner l'impression que le message a été envoyé par une personne que vous connaissez. **[9]**

II.2.5.3.4 Vol de cookie

La majorité des sites web utilisent aujourd'hui des cookies pour offrir une expérience plus personnalisée. Similairement, les navigateurs utilisent des cookies pour sauvegarder vos mots de passe, les favoris de votre navigateur et historique pour une navigation plus rapide. Pour assurer votre sécurité en ligne, saisissez vos identifiants uniquement sur des sites cryptés qui utilisent le système HTTPS, la version sécurités de http, au risque de permettent aux pirates d'utiliser cette opportunité pour intercepter vos données et pirater votre cession de navigation. Ceci leur donnerait accès à vos cookies ainsi qu'à vos identifiants. **[11]**

II.3 Les pirates informatiques

II.3.1 Présentation

Sur Internet des attaques ont lieu en permanence, à raison de plusieurs attaques par minute sur chaque machine connectée. Ces attaques sont pour la plus part lancées automatiquement à partir de machines infectées (par des virus, chevaux de Troie, etc.), à l'insu de leur propriétaire. Plus rarement il s'agit de l'action de **pirates informatiques**.

Un pirate informatique(ou Hacker) est la personne qui fait l'attaque.

II.3.2 Les Hackers

La définition de terme **hacker** est modifier et/ou améliorer tout et n'importe quoi (logiciel et matériel, informatique ou non)…pas par nécessité, mais par curiosité.

Le terme de hacker est souvent utilisé pour désigner un pirate informatique. Les victimes de piratage sur des réseaux informatique aiment à penser qu'ils ont attaqués par des pirates chevronnés ayant soigneusement étudié leur système et ayant développé des outils spécifiquement pour crée une faille dans leur système. [4]

II.3.3 Bref historique de mot hacker

Le terme hacker a eu plus d'une signification depuis son apparition à la fin des années 50. Ce nom désignait convenablement les programmeurs avertis, qui pour la plupart sont devenus les fondateurs des plus grandes entreprise informatiques.

C'est au cours des années 80 que ce mot a été utilisé pour catégoriser les personnes impliquées dans le piratage de jeux vidéo, en désamorçant les protections de ces derniers, puis en revendant des copies. Aujourd'hui ce mot est souvent utilisé pour désigner les personnes s'introduisant dans les systèmes informatiques**. [4]**

II.3.4 Les différents types de pirates :

En réalité il existe de nombreux types de pirates catégorisés selon leur expérience et selon leurs motivations :

- **Les white hat hackers :** hacker au sens noble du terme, dont le but est d'aider à l'amélioration des systèmes et technologies informatiques, sont généralement à l'origine des principaux protocoles et outils informatiques que nous utilisons aujourd'hui. Le courrier électronique en est un exemple.
- **Les black hat hackers :** plus couramment appelés pirates, hacker au sens nuisible, c'est-à-dire des personnes s'introduisant dans les systèmes informatiques dans le but nuisible.
- **Les scripts kiddies :** sont de jeunes qui utilisent les scripts sur internet pour pirater leurs amis.
- **Les phreakers :** sont des pirates s'intéressant au réseau téléphonique commuté (RTC) afin de téléphoner gratuitement grâce à des circuits électroniques (qualifiées de

box, comme la blue box, le violet box, …) connectés à la ligne téléphonique dans le but d'en falsifier le fonctionnement.

- **Les carders :** s'attaquent principalement aux systèmes de cartes à puces pour en comprendre le fonctionnement et en exploiter les failles (en particulier les cartes bancaires).
- **Les crackers :** sont des personnes dont le but est de créer des outils logiciels permettant d'attaquer des systèmes informatiques ou de casser les protections contre la copie des logiciels ayants.
- **Les hacktivistes :**(contraction de hackers et activistes que l'on peut traduire en cybermilitant ou cyber-résistant), sont des hackers dont la motivation est principalement idéologique. Ce terme a été largement porté par la presse, aimant à véhiculer l'idée d'une communauté parallèle (qualifiée généralement d'underground), par analogie aux populations souterraines des films de science-fiction.
- **Grey hat:** Les Grey hats peuvent commettre des délits mais ils le font avec la volonté d'agir pour la bonne cause. Ils sont à mi-chemin entre les black hats et les white hats.

En général, ils sont donc plus motivés par la curiosité, le **goût du risque** et le **défi** de mettre le doigt sur quelque chose d'inédit que par un intérêt purement financier**. [12]**

II.3.5 Méthodologie d'une intrusion sur un réseau

Comme toute entreprise ambitieuse, une cyberattaque réussie exige une planification soignée et une exécution précise. Ce que les piratages efficaces ont en commun est le fait de pouvoir attendre à couvert le bon moment pour frapper. Et si les attaques ont recours à diverses méthodes, elles ont généralement plusieurs étapes similaires en commun. Afin de pouvoir parer les cyberattaques, il est important de comprendre quelles sont ces étapes.

Voici les quatre étapes d'un cyber attaque réussie :

- **Reconnaissance :**

Avant de perpétrer une attaque, les hackers commencent par identifier une cible vulnérable et ils explorent le meilleur moyen de l'exploiter. La cible initiale peut être n'importe qui au sein d'une entreprise, que ce soit un dirigeant ou un administrateur. Les

agresseurs ont juste besoin d'un point d'entrée pour démarrer. Les e-mails de phishing ciblés sont courants à cette étape pour introduire efficacement un malware.

❖ **Scan :**

Une fois la cible identifiée, l'étape suivante consiste à identifier un maillon faible permettant aux agresseurs de s'infiltrer. Ils procèdent généralement par l'exploration du réseau d'une entreprise, au moyen d'outils faciles à trouver sur Internet, jusqu'à repérer des points d'entrée. Cette étape du processus peut prendre du temps, parfois des mois, le temps que les criminels repèrent des vulnérabilités.

❖ **Maintenir l'Accès:**

Une fois les faiblesses du réseau ciblé identifiées, l'étape suivante de la cyberattaque consiste à se frayer un accès et remonter. Dans quasiment tous les cas, un accès privilégié est nécessaire car il permet aux agresseurs d'évoluer librement au sein de l'environnement. Des tableaux Rainbow et d'autres outils comparables aident les infiltrés à voler des identifiants, à faire remonter les privilèges jusqu'au niveau admis, puis à s'introduire dans tout système du réseau accessible via le compte administrateur. Une fois que les agresseurs disposent de privilèges élevés, ils prennent le réseau d'assaut, lequel leur « appartient » désormais.

❖ **Effacer les traces :**

Le plus souvent, les agresseurs souhaitent effacer leurs traces, mais ce n'est pas une vérité universelle, encore moins s'ils souhaitent laisser une « carte de visite » pour se vanter de leurs exploits. L'objectif de l'offuscation est de perturber l'enquête légale, de rendre l'investigation confuse et de désorienter les enquêteurs. Plusieurs techniques et outils le permettent, y compris ceux de nettoyage de fichiers journaux, de spoofing, de désinformation, de comptes zombis, de commandes de chevaux de Troie, etc. **[13]**

II.4 Les virus informatiques

II.4.1 Présentation

Un **virus informatique** est un automate auto réplicatif à la base non malveillant, mais aujourd'hui souvent additionné de code malveillant (donc classifié comme logiciel malveillant), conçu pour se propager à d'autres ordinateurs en s'insérant dans des logiciels légitimes, appelés « hôtes ». Il peut perturber plus ou moins gravement le fonctionnement de

l'ordinateur infecté. Il peut se répandre par tout moyen d'échange de données numériques comme les réseaux informatiques et le CD-ROM, les clefs USB, les disques durs, etc.

Sur Internet, les virus peuvent contaminer une machine de plusieurs manières :

- Téléchargement de logiciel puis exécution de celui-ci sans précautions.
- Ouverture sans précautions de documents contenant des macros.
- Pièce jointe de courrier électronique (exécutable, script type vbs…).
- Ouverture d'un courrier au format HTML contenant du javascript exploitant une faille de sécurité du logiciel de courrier.
- Exploitation d'un bug du logiciel de courrier (effectuer souvent les mises à jour). **[3]**

II.4.2 Objectifs de l'attaque par virus

Tout comme le virus biologique, le virus informatique poursuit 3 objectifs :

- se dissimuler le plus longtemps possible aux yeux de l'utilisateur infecté.
- Il contamine tout ce qui est à sa portée.
- Il tente de se répandre, sans se cantonner au support sur lequel il se trouve. **[3]**

II.4.3 Quelques virus connus :

Voici les quelques virus les plus célèbres du monde informatique :

- **Cabir :** est considéré comme le tout premier virus informatique se propageant par la téléphonie mobile grâce à la technologie Bluetooth et du système d'exploitation Symbian OS.
- **MyDoom.A :** est un virus informatique qui se propage par les courriels et le service P2P de Kazaa. Les premières infections ont eu lieu le 26 janvier 2004.
- **Psyb0t :** est un virus informatique découvert en janvier 2009. Il est considéré comme étant le seul virus informatique ayant la capacité d'infecter les routeurs et modem haut-débit.
- **Le virus Tchernobyl ou CIH :** est connu pour avoir été un des plus des tracteurs. Il détruisait l'ensemble des informations du système attaqué et parfois il rendait la machine quasiment inutilisable. Il a sévi de 1998 à 2002.
- **Le ver Conficker :** exploite une faille du Windows Server Service utilisé par Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003 et Windows Server 2008.

- **Cryptolocker :** est un logiciel malveillant dont la présence sur le web a augmenté de 700 % entre 2012 et 2014. Selon les calculs du FBI en juin 2014, il a causé pour 27 millions de dollars de pertes aux utilisateurs. Sous couvert d'une mise à jour Adobe Flash, le logiciel malveillant chiffre les fichiers des victimes et exige un paiement (pouvant aller de 100 dollars à 400 dollars) pour les décrypter.
- **Zeus Bot :** est responsable d'environ 4 millions d'infections rien qu'aux États-Unis. Il a provoqué pour 70 millions de dollars de pertes pour les entreprises et consommateurs américains avant d'être démantelé par le FBI début 2014. Il exploite les vulnérabilités présentes dans Adobe Reader et Adobe Flash pour infecter les machines. **[3]**

II.4.4 Caractéristiques des virus

- **Le chiffrement :** à chaque réplication, le virus est chiffré (afin de dissimuler les instructions qui, si elles s'y trouvaient en clair, révéleraient la présence de ce virus ou pourraient indiquer la présence de code suspect).
- **Le polymorphisme :** le virus est chiffré et la routine de déchiffrement est capable de changer certaines de ses instructions au fil des réplications afin de rendre plus difficile la détection par l'antivirus.
- **Le métamorphisme :** contrairement au chiffrement simple et au polymorphisme, où le corps du virus ne change pas et est simplement chiffré, le métamorphisme permet au virus de modifier sa structure même et les instructions qui le composent.
- **La furtivité :** le virus « trompe » le système d'exploitation (et par conséquent les logiciels antivirus sur l'état des fichiers infectés. Des rootkits permettent de créer de tels virus. Par exemple, l'exploitation d'une faille de sécurité au niveau des répertoires permet de masquer l'existence de certains fichiers exécutables ainsi que les processus qui leur sont associés. **[3]**

II.4.5 Classification des virus

Il n'existe pas de classification stricte des virus. Cependant on peut en retenir 4grandes classifications :

- **Classification selon le format visé :**(exécutable ou documents).
- **Classification selon leur comportement :**(rapide, lent, résident, polymorphe…).

- **Classification selon l'organe visé :**(boot sector, driver…).
- **Classification selon le langage utilisé :**(virus assembleur, macrovirus, virus interprété…). **[3]**

II.5 Conclusion

Pour organiser une bonne défense, il faut connaître les attaques. Ce chapitre a passé en revue les déffirent types d'attaque ainsi que les attaques les plus courantes, les pirates utilisent pour perturber et compromettre les systèmes informatiques et leur méthodulogie et enfin les virus informatique.

Ainsi, il est nécessaire de se protéger de ces attaques réseaux en installant un dispositif de protection. C'est le sujet du chapitre suivant qui parle sur les mécanismes de sécurité informatique.

CHAPITRE III : LES MÉCANISMES DE SÉCURITÉ

III.1 Introduction

Pour pallier à ce problème de sécurité et d'interconnexion, il est primordial d'implémenter des mécanismes et des solutions sures assurant la confidentialité et la sécurité du transfert entre deux ou plusieurs entités d'un réseau public, donc chaque ordinateur connecté à Internet nécessite une protection de ces attaques réseaux en installant un dispositif de protection.

Dans ce chapitre, nous allons montrer les moyens et les dispositifs de sécurité utilisés pour l'assurer. Nous étudierons en particulier, les Pare-feux, les Proxys et les VPNs (réseaux privés virtuels).

III.2 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 attaques réseaux en installant un dispositif de protection (Pare-feux, réseaux privés virtuel, Proxys, etc.) permettant d'ajouter un niveau de sécurisation supplémentaire.

III.2.1 Pare-feu

III.2.1.1 Présentation

Le pare-feu est une passerelle filtrante qui protège un ordinateur ou un réseau des intrusions venues d'Internet. Il filtre en effet les paquets de données qui sont échangés. Il est parfois traduit comme coupe-feu, barrière de sécurité ou garde-barrière. Il est doté au moins de deux interfaces, l'un destiné au réseau interne et l'autre au réseau externe. Pour que le pare-feu s'intègre à un appareil, il importe que:

- le système informatique soit protégé.
- le système de filtrage des paquets soit unique.
- la machine soit puissante.

Il permet d'assurer la sécurité des informations d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur.

Le firewall propose donc un véritable contrôle sur le trafic réseau de l'entreprise. Il permet d'analyser, de sécuriser et de gérer le trafic réseau, et ainsi d'utiliser le réseau de la façon pour

laquelle il a été prévu. Tout ceci sans l'encombrer avec des activités inutiles, et d'empêcher une personne sans autorisation d'accéder à ce réseau de données.

III.2.1.2 Intérêts et limites du pare-feu

III.2.1.2.1 Avantage

- Avec une architecture réseau cohérente, on bénéficie d'une centralisation dans la gestion des flux réseaux.
- De plus, avec un plan d'adressage correct, la configuration du pare-feu est peu ou pas sensible au facteur d'échelle (règles identiques pour 10 comme 10000 équipements protégés).
- L'utilisation de la journalisation offre une capacité d'audit du trafic réseau et peut donc fournir des traces robustes en cas d'incident, si le pare-feu n'est pas lui-même une des cibles.
- Enfin le pare-feu permet de relâcher les contraintes de mise à jour rapide de l'ensemble d'un parc en cas de vulnérabilité sur un service réseau : il est possible de maintenir une certaine protection des équipements non vitaux au prix de la dégradation du service avec la mise en place d'un filtrage.

III.2.1.2.2 Inconvénients

- La capacité de filtrage d'un équipement dépend de son intégration dans le réseau mais le transforme en goulet d'étranglement (capacité réseau et ressources du pare-feu).
  - De par sa fonction, le pare-feu est un point névralgique de l'architecture de sécurité avec de fortes contraintes de disponibilité. Il existe des solutions permettant la synchronisation de l'état des pare-feu, comme l'élection du routeur avec VRRP (Virtual Router Redondancy Protocol)
  - Enfin une bonne gestion d'un pare-feu nécessite la compréhension des protocoles filtrés surtout lorsque les interactions deviennent complexes comme dans les cas FTP, H323,...avec le transport de paramètres de connexion dans le segment de données.

III.2.1.3 Principe de fonctionnement

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

- soit d'autoriser uniquement les communications ayant été explicitement autorisées.

- soit d'empêcher les échanges qui ont été explicitement interdits.

Il permet de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante comportant au minimum les interfaces réseau suivante :

- une interface pour le réseau à protéger (réseau interne).
- une interface pour le réseau externe. [5]

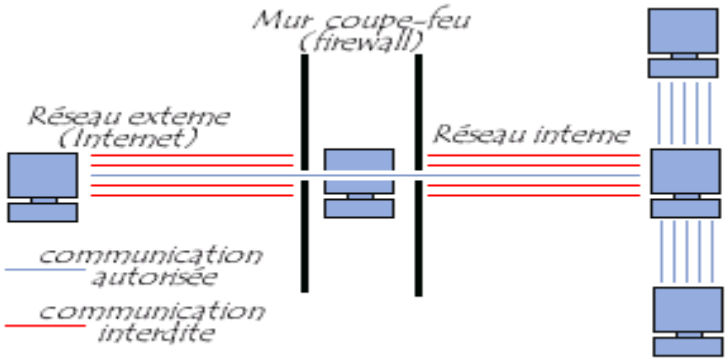

Figure 11:principe de fonctionnement de pare-feu. [25]

Le choix de l'une ou l'autre de ces méthodes dépend de la politique de sécurité adoptée par l'entreprise désirant mettre en œuvre un filtrage des communications. La première méthode de pare-feu est sans nul doute la plus sûre, mais elle impose toutefois une définition précise et contraignante des besoins en communication.

III.2.1.4 Principes du filtrage

III.2.1.4.1 Le filtrage simple de paquets

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

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

- adresse IP de la machine émettrice.
- adresse IP de la machine réceptrice.
- type de paquet (TCP, UDP, etc.).

Le numéro de port (rappel: un port est un numéro associé à un service ou une application réseau).

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

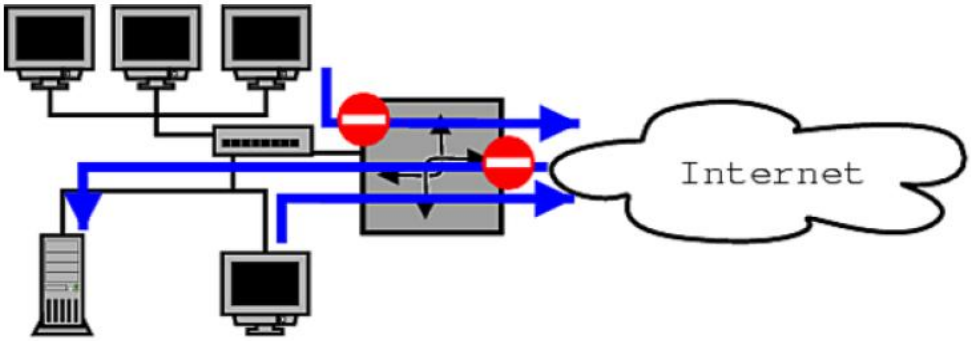

Figure 12: Le filtrage de paquet des donnes. [5]

III.2.1.4.2 Le filtrage dynamique et adaptatif

Ce mécanisme se veut le meilleur que le monde précédent en apportant une capacité de filtrage applicative tout en restant au niveau de la couche transport/session.

Le filtrage dynamique ajoute la prise en compte de l'historique au simple filtrage de paquet : l'idée de base étant qu'avec un échange client/serveur si un paquet est passé dans un sens il en passera un dans l'autre (commutation de la source et destination du couple IP/port pour les paquets TCP/UDP). Diverses temporisations sont introduites : poignés de main TCP, fermeture de connexion ou de session,.... Ce mode permet de générer à la volée des règles temporaires de filtrage des paquets. Ces dernières disparaissent lorsqu'aucun paquet ne passe pendant un délai configuré ou avec la fermeture de la session en TCP (RST, FIN).

Le filtrage adaptatif recherche, en outre, des signatures dans le segment de données des paquets afin de déterminer le type et l'état du protocole applicatif transporté et de procéder ainsi à des vérifications de cohérences. C'est dans cette catégorie que l'on peut ranger le terme

de « stateful inspection » utilisée par divers éditeurs**. [5]**

III.2.1.5 Les types des firewalls

III.2.1.5.1 Les firewalls bridge

Ces derniers sont relativement répandus. Ils agissent comme de vrais câbles réseau avec la fonction de filtrage en plus, d'où leur appellation de firewall. Leurs interfaces ne possèdent pas d'adresse Ip, et ne font que transférer les paquets d'une interface à une autre en leur appliquant les règles prédéfinies. Cette absence est particulièrement utile, car cela signifie que le firewall est indétectable pour un hacker lambda. 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, étant donné qu'aucun paquet ne sera traité par ce dernier comme étant sa propre destination. Donc, la seule façon de le contourner est de passer outre ses règles de drop. Toute attaque devra donc « Faire » avec ses règles, et essayer de les contourner. Dans la plupart des cas, ces derniers ont une interface de configuration séparée. Un câble vient se brancher sur une troisième interface, série ou même Ethernet, et qui ne doit être utilisée que ponctuellement et dans un environnement sécurisé de préférence. Ces firewalls se trouvent typiquement sur les Switchs.

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

III.2.1.5.2 Les firewalls matériels

Ils se trouvent souvent sur des routeurs achetés dans le commerce par de grands constructeurs comme Cisco ou Nortel. Intégrés directement dans la machine, ils font office de « boite noire », et ont une intégration parfaite avec le matériel. Ces firewalls se Trouvent généralement dans les routeurs à large bande.

- **Avantage :**
  - Intégré au matériel réseau.
  - Administration relativement simple.
  - Bon niveau de sécurité.
- **Inconvénients :**
  - Dépendant du constructeur pour les mises à jour.
  - Souvent peu flexibles.

III.2.1.5.2 Les firewalls logiciels

Ceci est conçu afin de protéger les périphériques informatiques en bloquant l'envoi et la réception d'informations à partir d'un réseau local ou d'Internet par certains programmes.
Présents à la fois dans les serveurs et les routeurs « faits maison », on peut les classer en plusieurs catégories par exemple :

III.2.1.5.3 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.
Il est installé dans des appareils informatiques comme n'importe quel autre logiciel qui peut être personnalisé.

- **Avantage :**
  - Sécurité en bout de chaîne (le poste client).
  - Personnalisable assez facilement.
- **Inconvénients :**
  - Facilement contournable.
  - Difficiles à départager de par leur nombre énorme.

III.2.1.6 Les réactions des firewalls aux attaques classiques

- **IP spoofing :**

L'IP spoofing consiste à modifier les paquets IP afin de faire croire au firewall qu'ils proviennent d'une adresse IP considérée comme « de confiance ». Par exemple, une IP présente dans le réseau local de l'entreprise. Cela laissera donc toute latitude au hacker de passer outre les règles du firewall afin d'envoyer ses propres paquets dans le réseau de

l'entreprise. Les derniers firewalls peuvent offrir une protection contre ce type d'attaque, notamment en utilisant un protocole VPN, par exemple IPsec. Cela va crypter les entêtes des paquets, et ainsi rendre impossible leur modification par un intrus, et surtout, l'intrus ne pourra générer de paquets comme provenant de ce réseau local, ce dernier n'ayant pas la clé nécessaire au cryptage. Les algorithmes utilisés dans de tels protocoles sont de type RSA. [5]

- **DOS et DDOS :**

Le DOS, ou Denial Of Service attack, consiste à envoyer le plus de paquets possibles vers un serveur, générant beaucoup de trafic inutile, et bloquant ainsi l'accès aux utilisateurs normaux. Le DDOS, pour Distributed DOS, implique venir de différentes machines simultanées, cette action étant le plus souvent déclenchée par un virus : ce dernier va d'abord infecter nombre de machines, puis à une date donnée, va envoyer depuis chaque ordinateur infecté des paquets inutiles vers une cible donnée. On appelle aussi ce type d'attaque « flood ». Les firewalls ici n'ont que peu d'utilité. En effet, une attaque DOS ou DDOS utilise le plus souvent des adresses sources différentes (le but n'est pas de récupérer une réponse ici) et souvent, impossible de distinguer ces paquets des autres... Certains firewalls offrent une protection basique contre ce genre d'attaque, par exemple en droppant les paquets si une source devient trop gourmande, mais généralement, ces protections sont inutiles. Cette attaque brute reste un des gros problèmes actuels, car elle est très difficilement évitable. [5]

- **Port scanning :**

Ceci constitue en fait une « pré-attaque » (Etape de découverte). Elle consiste à déterminer quels ports sont ouverts afin de déterminer quelles sont les vulnérabilités du système. Le firewall va, dans quasiment tous les cas, pouvoir bloquer ces scans en annoncent le port comme « fermé ». Elles sont aussi aisément détectables car elles proviennent de la même source faisant les requêtes sur tous les ports de la machine. Il suffit donc au firewall de bloquer temporairement cette adresse afin de ne renvoyer aucun résultat au scanner. [5]

- **Exploit :**

Les exploits se font en exploitant les vulnérabilités des logiciels installés, par exemple un serveur Http, Ftp, etc. Le problème est que ce type d'attaque est très souvent considéré comme des requêtes tout a fait « valides » et que chaque attaque est différente d'une autre, vu que le bug passe souvent par reproduction de requêtes valides non prévues par le

programmeur du logiciel. Autrement dit, il est quasiment impossible au firewall d'intercepter ces attaques, qui sont considérées comme des requêtes normales au système, mais exploitant un bug du serveur le plus souvent. La seule solution est la mise à jour périodique des logiciels utilisés afin de barrer cette voie d'accès au fur et à mesure qu'elles sont découvertes. **[5]**

III.2.2 Réseaux privés virtuels(VPN)

III.2.2.1 Présentation

Un réseau privé virtuel (Virtual Private Network) est un tunnel sécurisé à l'intérieur d'un réseau (Internet notamment). Il permet d'échanger des informations de manière sécurisée et anonyme en utilisant une adresse IP différente de celle de votre ordinateur.

Le VPN est un service qui vous permet d'accéder au web de manière sécurisé et privé en acheminant votre connexion via un serveur et cache l'action en ligne

Le VPN est parfaitement légal : de nombreuses entreprises y ont recours pour protéger les échanges d'informations entre deux filiales à l'étranger par exemple. **[22]**

Un VPN crée un tunnel privé sur l'internet ouvert .L'idée est que tout ce que vous envoyez soit encapsulé dans ce canal de communication privé et crypté de manière à ne pas pouvoir être déchiffré, même si les paquets sont interceptés.

III.2.2.2 Objectifs et caractéristiques des VPN

- Étanchéité du trafic entre les différents réseaux privés virtuels
- Sécurité des communications :
  - ✓ Confidentialité (chiffrement des données).
  - ✓ Authentification (utilisateurs ou DATA).
  - ✓ Filtrage de paquet.
- Notion de qualité de service.
  - ✓ Type best effort dans le cas de simples tunnels créés par l'utilisateur.
  - ✓ QOS bien meilleure dans le cadre d'une offre VPN d'opérateur.
- Coût :
  - ✓ Permet de réduire les coûts liés à l'infrastructure réseau des entreprises par la mise en place d'une liaison VPN.

III.2.2.3 Principe de fonctionnement

Le VPN repose sur un protocole de tunneling qui est un protocole permettant de chiffrer les données par un algorithme cryptographique entre les deux réseaux.

Le principe de tunneling consiste à construire un chemin virtuel après avoir identité l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Les VPN simulent un réseau privé alors qu'ils utilisent une infrastructure partagées et ceux afin d'assurer un accès aisée et peu couteux au intranet ou aux extranets.[20]

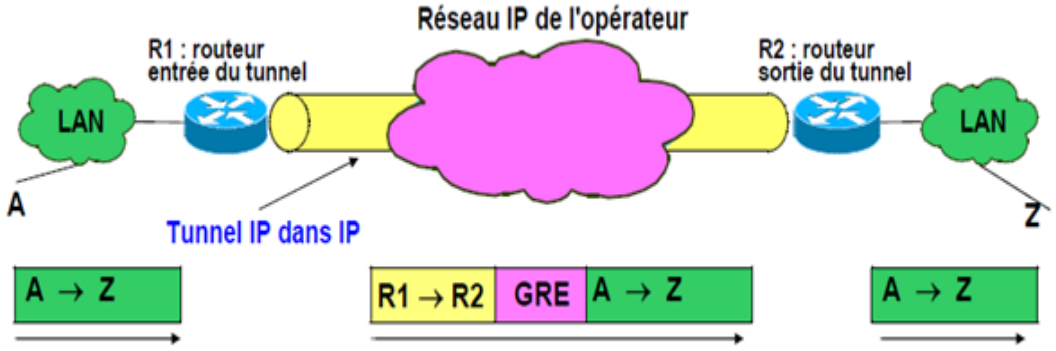

Figure 13: Principe de fonctionnement de VPN. [22]

- Un tunnel est créé entre R1 et R2 :
  - ✓ Configuré dans les routeurs d'entrée et de sortie.
  - ✓ Le paquet IP privé (avec adresses IP privées) est encapsulé dans un paquet IP public.
  - ✓ Les adresses de R1 et R2 sont des adresses publiques
- Tunnel IP dans IP :
  - ✓ Le protocole GRE permet d'encapsuler les paquets IP dans IP.
  - ✓ L'entête GRE permet d'annoncer le type de paquet encapsulé (IPv4).**[22]**

III.2.2.4 Types de VPN

On peut dénombrer deux grands types de VPN, chacun d'eux caractérise une utilisation bien particulière de cette technologie.

III.2.2.4.1 Le VPN d'accès (poste - a - site)

Ce type nomade, également appelé « Road Warrior » permet à un utilisateur distant de son entreprise de se connecter à celle-ci pour pouvoir porter de ses services.

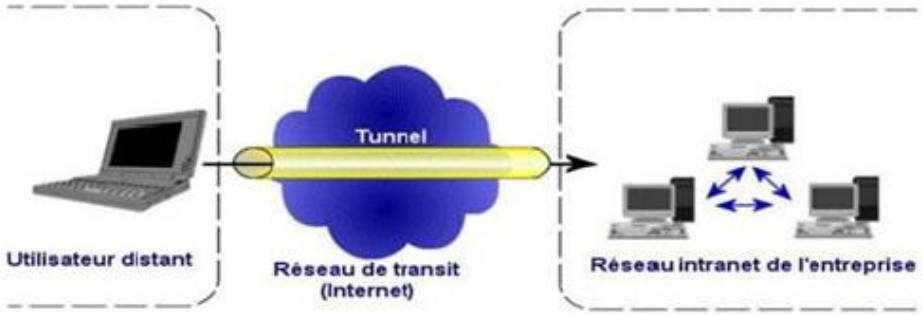

Figure 14: Architecture VPN poste - a - site. [22]

III.2.2.4.2 Site a site (LAN to LAN)

Qui permet de relier deux réseaux d'entreprises entre eux de façon transparente.

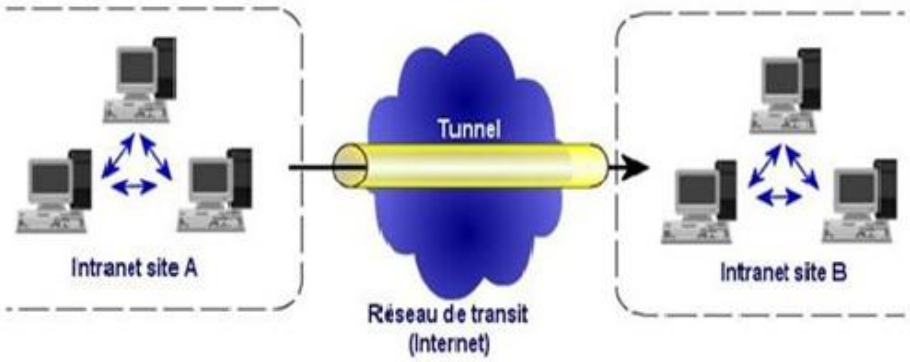

Figure 15: Architecture VPN LAN to LAN. [22]

III.2.2.5 Les fonctionnalités du VPN

Le VPN n'est qu'un concept, ce n'est pas une implémentation. Il se caractérise par les obligations suivantes :

- ✓ Authentification des entités communicantes : le serveur VPN doit pouvoir être sûr de parlera vrai client VPN et vice-versa.

- ✓ authentification des utilisateurs : seuls les bonnes personnes doivent pouvoir se connectera réseau virtuel. On doit aussi pouvoir conserver les logs de connexions.
- ✓ Gestion des adresses : tous les utilisateurs doivent avoir une adresse privée et le nouveau client en obtenir une facilement.
- ✓ Cryptage du tunnel : les données échangées sur Internet doivent être dûment cryptées entre le client VPN et le serveur VPN et vice-versa.
- ✓ Les clés de cryptage doivent être régénérées souvent (automatiquement).
- ✓ le VPN dit supporter tous les protocoles afin de réaliser un vrai tunnel comme s'il y avait réellement un câble entre les deux réseaux**. [23]**

III.2.2.6 Principaux protocoles

- ➢ **Passenger Protocol :**

Les données originales (IP…) à transmettre.

- ➢ **Encapsulating Protocol :**

Le protocole (IP sec, PPTP, L2TP) utilisé pour encapsuler les données originales.

- ➢ **Carrier Protocol**

Le protocole employé par le réseau pour transporter les données. **[23]**

III.2.2.7 Les algorithmes utilisés dans le VPN

III.2.2.7.1 L'algorithme SHA

Signifie Secure Hashing Algorithm (algorithme de hachage sécurisé) le hachage est un processus clé dans toutes les formes de cryptage. Fondamentalement, lorsque vous commencez avec un message qui doit être crypté, il doit passer par une fonction de hachage avant d'être entièrement crypté.

Les hachages sont des processus irréversibles, et ils sont généralement utilisés comme outils d'authentification. Parce que lorsque vous appliquez un hachage comme SHA, vous pouvez le comparer aux fichiers source, en veillant à ce que les deux correspondent. Lorsque cela se produit, vous pouvez être certain que les données n'ont pas été altérées pendant le transit.

III.2.2.7.2 L'algorithme Diffie-Hellman

Les groupes Diffie-Hellman déterminent la force de la clé utilisée dans le processus d'échange de clés. Les groupes portant un numéro supérieur sont plus sûrs, mais il faut plus de temps pour créer la clé.

Fireware prend en charge ces groupes Diffie-Hellman :

- Groupe Diffie-Hellman 1 : groupe 768 bits
- Groupe Diffie-Hellman 2 : groupe 1 024 bits
- Groupe Diffie-Hellman 5 : groupe 1 536 bits
- Groupe Diffie-Hellman 14 : groupe 2 048 bits
- Groupe Diffie-Hellman 15 : groupe 3 072 bits
- Groupe Diffie-Hellman 19 : groupe de courbe elliptique 256 bits
- Groupe Diffie-Hellman 20 : groupe de courbe elliptique 384 bits

Les deux pairs d'un échange VPN doivent utiliser le même groupe, qui est négocié pendant la phase 1 du processus de négociation IPsec. Lorsque vous définissez un tunnel VPN manuel, vous spécifiez le groupe Diffie-Hellman pendant la phase de création d'une connexion IPsec.

III.2.2.7.3 l'algorithme d'AES

Le chiffrement AES (Advanced Encryptions Standard) est l'algorithme de chiffrement le plus utilisé et le plus sûr disponible aujourd'hui. Ouvert au public. L'AES est beaucoup plus sûr et flexible que son prédécesseur.

Il s'agit d'un procédé dont l'objectif est de sécuriser vos informations en les «brouillant» afin de les rendre incompréhensibles aux yeux des individus non concernés. Pour y parvenir, un algorithme de chiffrement est utilisé. Seuls ceux qui possèdent la clé déchiffrement associée pourront alors déverrouiller le système pour lire les données.

III.2.3 Serveurs mandataires (Proxy)

III.2.3.1 Présentation

Un serveur **proxy** (appelé aussi «serveur mandataire») est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local et internet.

Un système mandataire (Proxy) repose sur un accès à l'Internet pour 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, …) et permet de centraliser, donc de sécuriser, les accès extérieurs (filtrage applicatif, enregistrement des connexions, masquage des adresses des clients, …).

Un serveur proxy permet de sécuriser et d'améliorer l'accès à certaines pages web en stockant des copies (ou caches), en filtrant certains contenus web et logiciels malveillants, et en renforçant l'anonymat de ses utilisateurs.

Le proxy vous permet de naviguer en toute discrétion car l'adresse IP qui est utilisée est celle du proxy, et non pas la vôtre. Il protège ainsi votre anonymat et votre vie privée.

III.2.3.3 Le principe de fonctionnement d'un proxy

Le principe de fonctionnement basique d'un serveur proxy est assez simple : il s'agit d'un serveur "mandaté" par une application pour effectuer une requête sur Internet à sa place. Ainsi, lorsqu'un utilisateur se connecte à Internet à l'aide d'une application cliente configurée pour utiliser un serveur proxy, celle-ci va se connecter en premier lieu au serveur proxy et lui donner sa requête. Le serveur proxy va alors se connecter au serveur que l'application cliente cherche à joindre et lui transmettre la requête.

Le serveur va ensuite donner sa réponse au proxy, qui va à son tour la transmettre à l'application cliente.

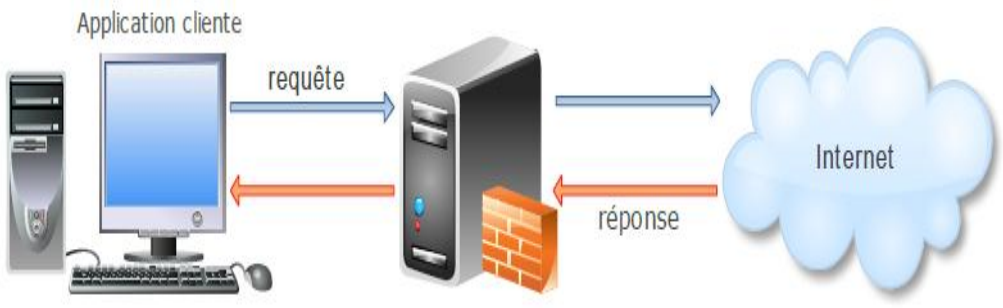

Figure 16: Principe de fonctionnement d'un proxy. [18]

Le client devient donc invisible pour l'Internet, si un client est derrière un proxy, les autres machines sur Internet penseront qu'il s'agit du serveur.

III.2.3.4 Les fonctionnalités d'un proxy

Désormais, avec l'utilisation de TCP/IP au sein des réseaux locaux, le rôle de relais du serveur proxy est directement assuré par les passerelles et les routeurs. Pour autant, les serveurs proxy sont toujours d'actualité grâce à un certain nombre d'autres fonctionnalités.

III.2.3.4.1 La fonction de cache :

La plupart des proxys assurent ainsi une fonction de cache, c'est-à-dire la capacité à garder en mémoire en « cache » les pages les plus souvent visitées par les utilisateurs du réseau local afin de pouvoir les leur fournir le plus rapidement possible.

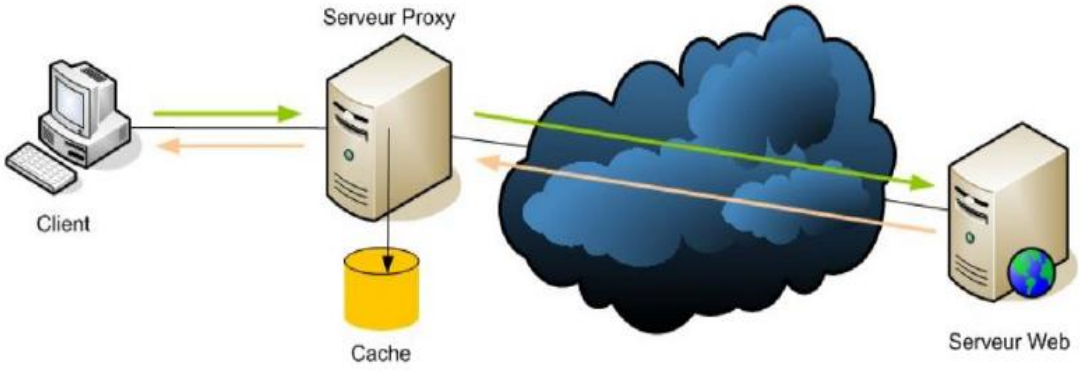

Figure 17:Cache proxy.[18]

Cette fonctionnalité implémentée dans certains serveurs proxy permet d'une part de réduire l'utilisation de la bande passante vers internet ainsi que de réduire le temps d'accès aux documents pour les utilisateurs. Toutefois, pour mener à bien cette mission, il est nécessaire que le proxy compare régulièrement les données qu'il stocke en mémoire cache avec les données distantes afin de s'assurer que les données en cache sont toujours valides.

III.2.3.4.2 Le filtrage

D'autre part, grâce à l'utilisation d'un proxy, il est possible d'assurer un suivi des connexions via la constitution de journaux d'activité (logs) en enregistrant systématiquement les requêtes des utilisateurs lors de leurs demandes de connexion à Internet.

Il est ainsi possible de filtrer les connexions à internet en analysant d'une part les requêtes des clients, d'autre part les réponses des serveurs. Lorsque le filtrage est réalisé en comparant la requête du client à une liste de requêtes autorisées, on parle de liste blanche, lorsqu'il s'agit d'une liste de sites interdits on parle de liste noire.

Au niveau des serveurs, l'analyse des réponses en fonction de certains critères s'appelle le filtrage de contenu (mots clés, adresses IP, noms de domaines, ...). [18]

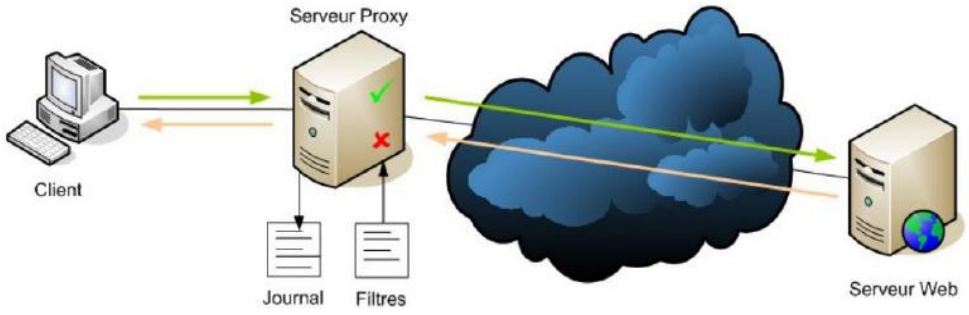

Figure 18:Filtrage. [18]

III.2.3.4.3 L'authentification

Dans la mesure où le proxy est l'intermédiaire indispensable des utilisateurs du réseau interne pour accéder à des ressources externes, il est parfois possible de l'utiliser pour authentifier les utilisateurs, c'est-à-dire de leur demander de s'identifier à l'aide d'un nom d'utilisateur et d'un mot de passe par exemple. Il est ainsi aisé de donner l'accès aux ressources externes aux seules personnes autorisées à le faire et de pouvoir enregistrer dans les fichiers journaux des accès identifiés. [18]

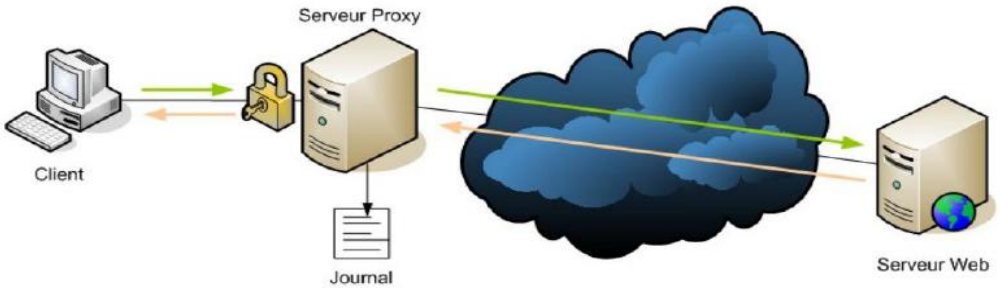

Figure 19: Authentification. [18]

III.2.3.4.4 Le reverse-proxy

On appelle reverse-proxy un serveur proxy-cache « monté à l'envers », c'est-à-dire un serveur proxy permettant non pas aux utilisateurs d'accéder au réseau internet, mais aux utilisateurs d'internet d'accéder indirectement à certains serveurs internes.

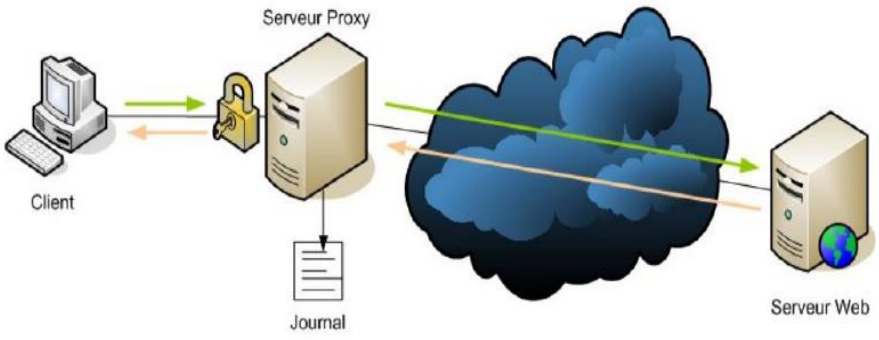

Figure 20: Principe de fonctionnement d'un reverse-proxy. [18]

Le reverse-proxy sert ainsi de relais pour les utilisateurs d'Internet souhaitant accéder à un site web interne en lui transmettant indirectement les requêtes. Grâce au reverse-proxy, le serveur web est protégé des attaques directes de l'extérieur, ce qui renforce la sécurité du réseau interne. D'autre part, la fonction de cache du reverse-proxy peut permettre de soulager la charge du serveur pour lequel il est prévu, c'est la raison pour laquelle un tel serveur est parfois appelé « accélérateur ».

III.2.4 DMZ (zone démilitarisée)

III.2.4.1 Présentation

Est un sous-réseau physique ou logique qui sépare un réseau local interne (LAN) d'autres réseaux non sécurisés tels qu'Internet. Tout service fourni aux utilisateurs sur Internet doit être placé dans la zone démilitarisée. Cela concerne notamment les services suivants : Web, messagerie, DNS, FTP et VoIP. **[20]**

Il existe une approche plus sécurisée qui consiste à utiliser deux pare-feux pour créer une zone démilitarisée. Le premier, également appelé pare-feu de périmètre, laisse passer uniquement le trafic à destination de la zone démilitarisée. Le second pare-feu, ou pare-feu interne, n'autorise que le trafic entre la zone démilitarisée et le réseau interne. Cette configuration est

considérée comme mieux sécurisée, puisqu'un pirate devra compromettre deux machines pour accéder au LAN interne. **[5]**

III.2.4.2 Architecture DMZ

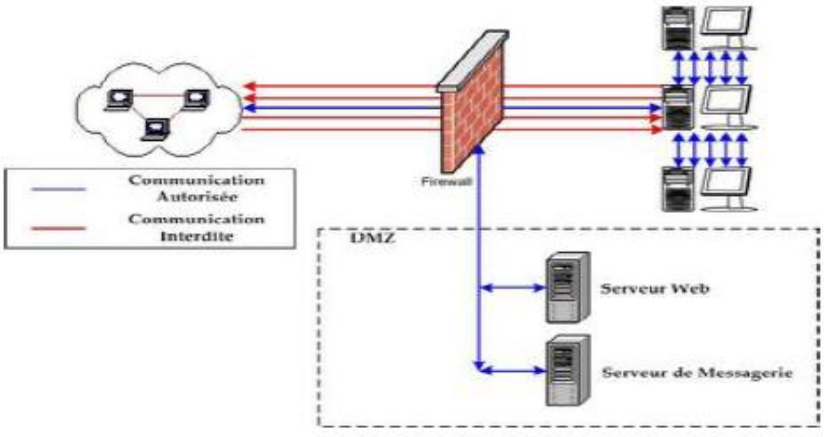

Figure 21: Architecture DMZ. [5]

Lorsque certaines machines du réseau interne ont besoin d'être accessibles de l'extérieur (serveur web, un serveur de messagerie, un serveur FTP public, etc.), il est souvent nécessaire de créer une nouvelle interface vers un réseau à part, accessible aussi bien du réseau interne que de l'extérieur, sans pour autant risquer de compromettre la sécurité de l'entreprise. On parle ainsi de « zone démilitarisé ». 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. **[5]**

III.2.5 La cryptographie

III.2.5.1 Présentation

La cryptographie est la science qui utilise les mathématiques pour chiffrer et déchiffrer des données. La cryptographie vous permet de stocker des informations sensibles ou de les

transmettre à travers des réseaux non sûrs (comme Internet) de telle sorte qu'elles ne puissent être lues par personne à l'exception du destinataire convenu. **[24]**

Alors que la cryptographie est la science de la sécurisation des données, la cryptanalyse est la science de l'analyse et du cassage des communications sécurisées. La cryptanalyse classique mêle une intéressante combinaison de raisonnement analytique, d'application d'outils mathématiques, de découverte de redondances, de patience, de détermination, et de chance. Les cryptanalyses sont aussi appelés attaquants. **[21]**

III.2.5.2 La fonctionnalité de la cryptographie

Un algorithme cryptographique, ou chiffre, est une fonction mathématique utilisée dans le processus de chiffrement et de déchiffrement. Un algorithme cryptographique fonctionne en combinaison avec une clé – un mot, un nombre, ou une phrase – pour chiffrer le texte clair. Le même texte clair se chiffre en un texte chiffré différent si l'on utilise des clés différentes. La sécurité des données chiffrées est entièrement dépendante de deux choses: la force de l'algorithme cryptographique et le secret de la clé.

Un algorithme cryptographique, plus toutes les clés possibles et tous les protocoles qui le font fonctionner constitue un crypto système. PGP est un crypto système. **[21]**

III.2.6 Translation d'adresses (NAT)

III.2.6.1 Présentation

Son principe consiste à modifier l'adresse IP source ou destination, dans l'en-tête d'un Datagramme IP lorsque le paquet transite dans le Pare-feu (Proxy) en fonction de l'adresse source ou destination et du port source ou destination.

Lors de cette opération, le Pare-feu garde en mémoire l'information lui permettant d'appliquer la transformation inverse sur le paquet de retour. La traduction d'adresse permet de masquer le plan d'adressage interne (non routable) à l'entreprise par une ou plusieurs adresses routables sur le réseau externe ou sur Internet. Cette technologie permet donc de cacher le schéma d'adressage réseau présent dans une entreprise derrière un environnement protégé. **[2]**

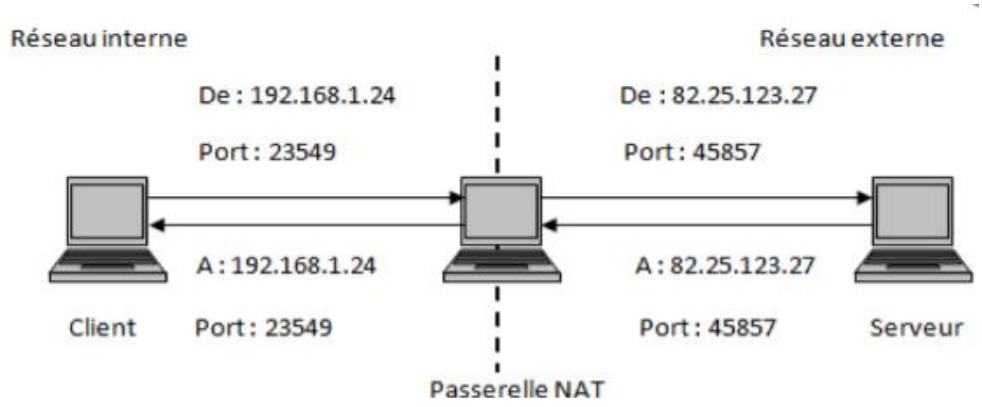

Figure 22: Translation d'adresses (NAT). [2]

III.2.6.2 PAT (Port Address Translation) ou Overloading

PAT est une extension de Traduction d'adresses de réseau (NAT). En effet, que nous ne disposons pas d'adresse IP publique suffisantes pour toutes nos machines locales, il va donc falloir partager réutiliser nos adresses.

PAT permet à plusieurs hôtes internes de partage adresse unique sur une interface externe en ajoutant des numéros de port différent à chaque connexion c'est pour distingue les requêtes des différentes machines, on va utiliser le numéro du port. **[24]**

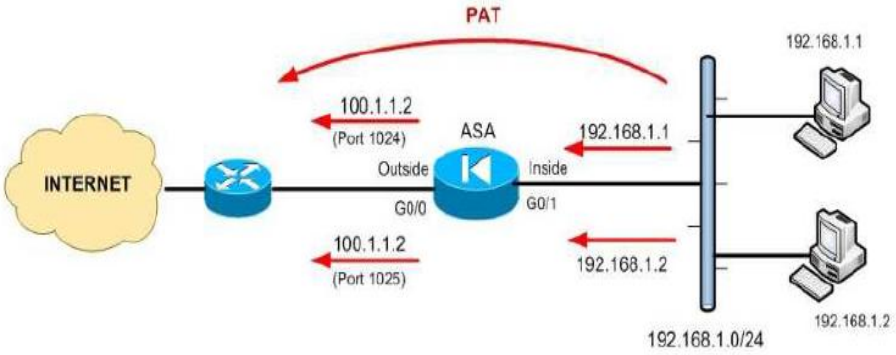

Figure 23:PAT. [24]

III.2.7 Antivirus

La politique de sécurité du réseau doit mentionner que tous les ordinateurs du réseau doivent être tenus à jour et théoriquement qu'ils doivent tous être protégés par le même système d'antivirus (entre autres, afin de réduire au maximum les frais de maintenance et de mise_à_jour).

Avec des milliers de nouveaux virus générés chaque mois, il est crucial que la base de données des virus soit tenue à jour. La base de données des virus est l'enregistrement du logiciel d'antivirus qui permet d'identifier les virus connus lorsqu'ils surviennent.

III.2.8 Secure Email Gateway

Une passerelle de courrier électronique sécurisée (Secure Email Gateway) est un dispositif ou un logiciel utilisé pour surveiller les courriers électroniques envoyés et reçus. Un SEG est conçu pour se protéger contre les courriers électroniques indésirables et délivrer les bons courriers électroniques. Les messages non désirés comprennent le spam, les attaques de phishing, les logiciels malveillants ou les contenus frauduleux. Les messages sortants peuvent être analysés pour empêcher des données sensibles de quitter l'entreprise ou pour chiffrer automatiquement les emails qui contiennent des informations sensibles.

III.3 Les protocoles de sécurité

III.3.1 Présentation

Ensemble de règles régissant le comportement d'individus pour répondre aux besoins d'une application (paiement en ligne, vote électronique, authentification d'individus, etc).

L'utilisation des protocoles est transparente pour l'utilisateur.

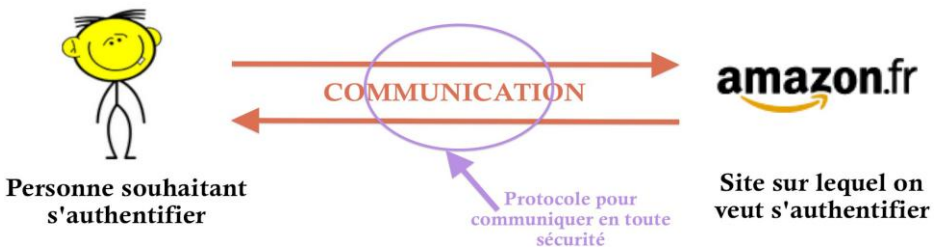

Figure 24: Les protocoles de sécurité. [17]

III.3.2 L'objectif des protocoles de sécurité

- Établir une communication sécurisée entre 2 individus ➔ Sécurité
- Être sûr de communiquer avec la bonne personne, et pas un intrus voulant voler des informations (comme le mot de passe) ➔ Authentification
- Être sûr que les données ne sont pas modifiées en cours de route ➔ Intégrité

III.3.3 Les déférents protocoles de sécurité

Dans le domaine de la sécurité dans les réseaux, il existe plusieurs solutions de sécurité telles que le protocole :

III.3.3.1 IPsec (IP Security)

IPsec permet, par encapsulation, de protéger en confidentialité, intégrité et anti-rejeu un flux au niveau de la couche réseau (couche de la pile TCP/IP ou couche 3 du modèle OSI). IPsec est normalisé par l'IETF.

Un très grand nombre d'équipements réseaux, en particulier les routeurs et les pare-feux, permettent l'utilisation d'IPsec. De même, les principaux systèmes d'exploitation pour micro-ordinateurs ou ordiphones prennent en charge IPsec nativement**.**

Le dialogue IPsec est généralement possible entre ces différents systèmes et équipements. Dans de nombreux cas, l'utilisation d'IPsec présente un rapport "bénéfice en sécurité" sur "coût" appréciable dans la mesure où cette technologie est prise en charge nativement par la plupart des systèmes clients et des équipements réseau et ne nécessite pas donc généralement d'investissements lourds. **[19]**

III.3.3.2 Le protocole SSL/TLS (Socket Secure Layer/Transport Layer Security)

Le protocole SSL (Secure Sockets Layer) était le protocole cryptographique le plus largement utilisé pour assurer la sécurité des communications sur Internet avant d'être précédé par le TLS (Transport Layer Security) en 1999. Malgré la dépréciation du protocole SSL et l'adoption du TLS pour le remplacer, le terme 'SSL' est encore largement utilisé pour faire référence à ce type de technologie.

Le SSL créé un canal sécurisé entre deux machines ou appareils communiquant sur Internet ou un réseau interne. Son usage le plus courant est la sécurisation de la communication entre un navigateur web et un serveur web. L'adresse URL passe alors de HTTP à HTTPS.

III.3.3.3 Le protocole SSH (Secure Shell)

SSH, ou Secure Socket Shell, est un protocole réseau qui permet aux administrateurs d'accéder à distance à un ordinateur, en toute sécurité. SSH désigne également l'ensemble des utilitaires qui mettent en œuvre(BH) le protocole.

Le protocole Secure Shell assure une authentification forte et des communications de données chiffrées sécurisées entre deux ordinateurs connectés sur un réseau peu sûr, tel qu'Internet. SSH est largement utilisé par les administrateurs réseau pour gérer à distance les systèmes et les applications, car il leur permet de se connecter à un autre ordinateur sur un réseau, d'exécuter des commandes et de déplacer des fichiers d'un ordinateur à un autre.

SSH désigne à la fois le protocole de réseau cryptographique et les utilitaires qui mettent en œuvre ce protocole. SSH fonctionne selon le modèle client-serveur, en connectant une application client Secure Shell - là où s'affiche la session - à un serveur SSH - là où s'exécute la session. **[24]**

III.3.3.4 Le protocole https

S-HTTP (Secure HTTP) est un procédé de sécurisation des transactions HTTP reposant sur une amélioration du protocole HTTP. Il permet de fournir une sécurisation des échanges lors de transactions de commerce électronique en cryptant les messages afin de garantir aux clients la confidentialité de leur numéro de carte bancaire ou de toute autre information personnelle**. [24]**

III.4 Conclusion

Nous avons vu dans ce chapitre les mécanismes à utiliser afin de mettre en place une politique de sécurité.

Malgré tous cela les hackers manquent pas d'ingéniosité pour inventer d'autre outils et méthode d'attaque ,ce qui pousse à être a jour en s'informant sur les nouvelles techniques d'attaques et les nouveaux outils et mécanismes concernant la technologie de sécurité.

CHAPITRE IV :

CONCEPTION ET

RÉALISATION

IV.1 Introduction

Ce présent chapitre, sera consacré à la Réalisation de notre projet, la conception d'une passerelle internet sécurisée. Débutant par la description de l'environnement de travail tel que l'installation et la configuration de l'émulateur EVE-ng ainsi les différents logiciels adaptent à cette dernière. Et enfin la conception de l'architecture et la réalisation des tests en parallèle.

IV.2 Environnement du travail

Le travail a été effectué sur notre propre matériel ainsi

IV.2.1 Environnement Matériel

- Modèle : DELL
- Processeur : Intel(R) Core(TM) i5-4310U CPU @ 2.00GHz 2.60GHz
- RAM : 8.00 GB
- Disque dur : 1 TB

IV.2.1 Environnement Logiciel

❖ **Présentation de VMware Workstation :**

VMware Workstation(Virtual machine) est un programme qui permet la création d'une ou plusieurs Machines virtuelles au sein d'un même système d'exploitation, ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique (hôte).Il est possible de faire fonctionner plusieurs machines virtuelles en même temps, la limite correspond aux performances de l'ordinateur hôte.

VMware Workstation supporte fortement la compatibilité matérielle et fonctionne comme un pont entre l'hôte et la machine virtuelle pour toutes sortes de ressources matérielles, y compris les disques durs, les périphériques USB et les CD-ROM. Tous les pilotes de périphériques sont installés via la machine hôte. **[26]**

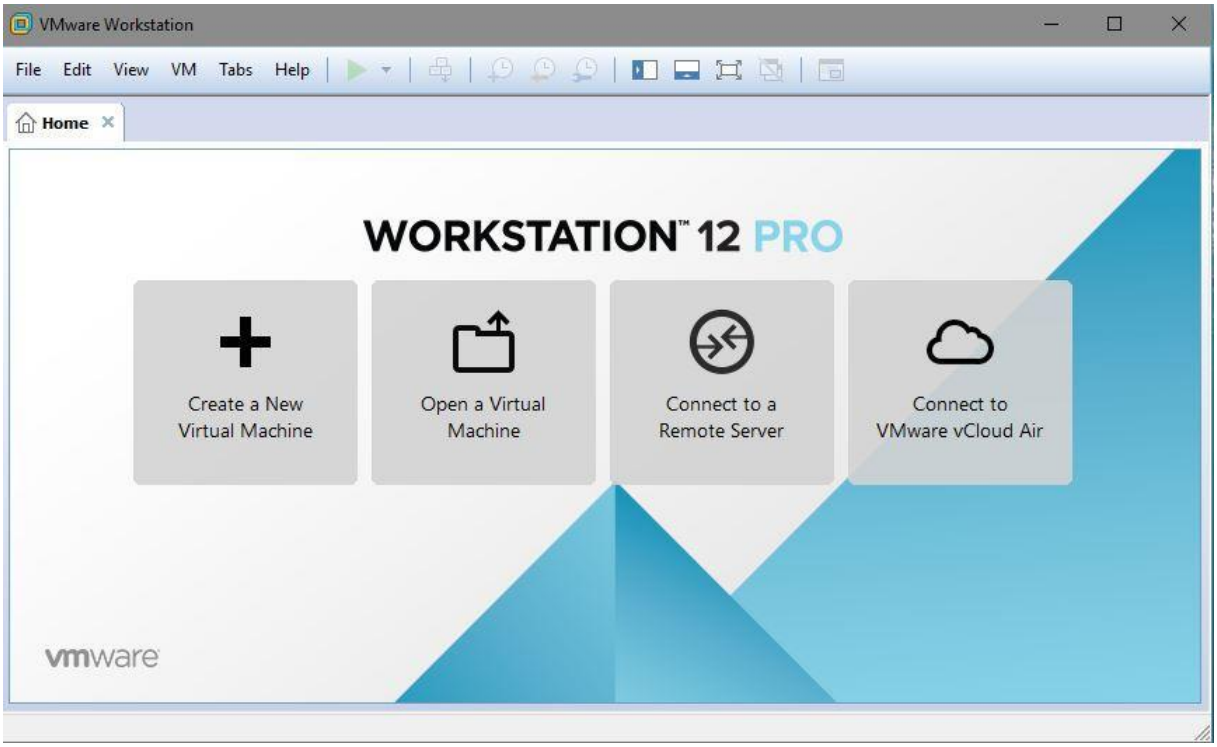

Figure 25:la page d'accueil de VMware Workstation 12 PRO.

❖ **Présentation de Emulated Virtual Environment – Next Generation (EVE-ng) :**

EVE-NG est un simulateur de réseau virtuel multifournisseur, il a été développé pour les particuliers et les petites entreprises. Il propose une édition communautaire gratuite ainsi qu'une édition professionnelle.

EVE-NG a été évalué en utilisant la version 2.0.3-95 dans une machine virtuelle avec 16 Go de mémoire et 4 CPU. Les nœuds de périphériques réseau utilisés pour l'évaluation comprenaient les images logicielles Cisco IOU, IOL, Dynamips, QEMU. **[27]**

➢ **Bref description sur l'Installation et configuration d'EVE-ng :**

- Téléchargez le fichier EVE-NG OVA à partir de l'URL suivant : https://www.eve-ng.net/index.php/download/
- Ensuite, créez une nouvelle machine virtuelle dans VMware Workstation. Cliquez sur Ouvrir une machine virtuelle dans l'accueil.
- Importé le fichier **EVE-Community.**
- EVE-NG apparaîtra dans la page d'accueil.

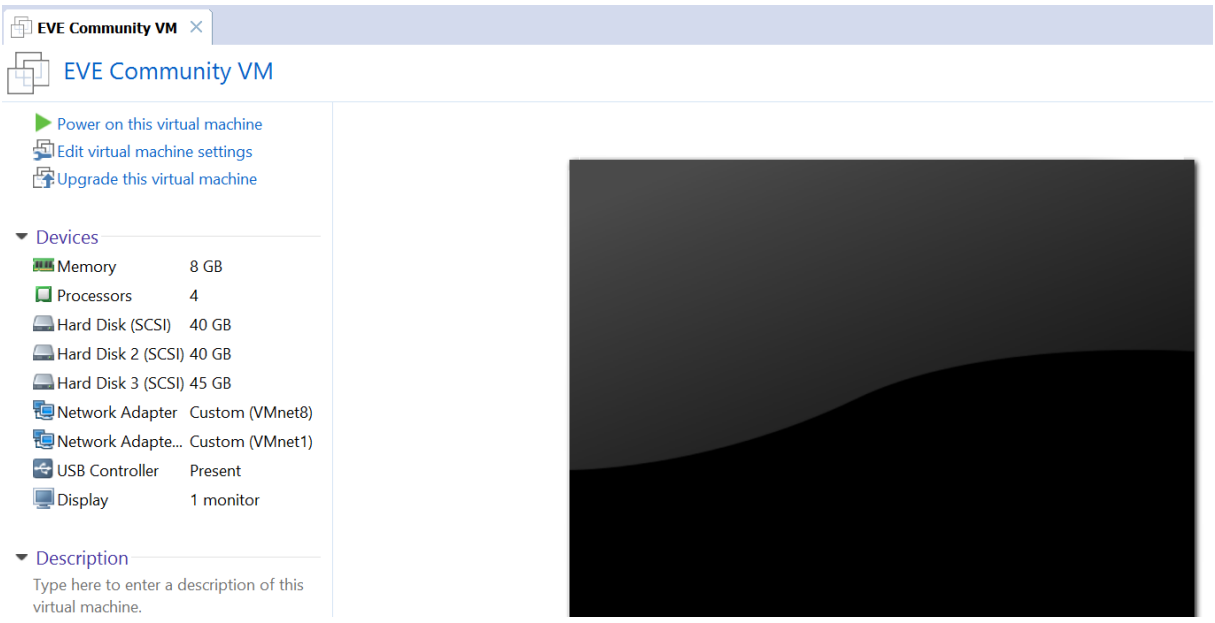

Figure 26: La page d'accueil d'EVE-ng.

- Tout d'abord, vous verrez l'écran de démarrage EVE-NG.

Figure 27: l'écran de démarrage EVE-NG.

- Dans, l'invite de connexion à la console d'EVE-NG. Vérifiez l'adresse IP affichée au-dessous de l'invite de connexion. Il devrait afficher **192.168.227.128** car nous l'avons défini comme adresse IP statique.

- Connectez-vous ensuite.

  Login: root

  Password: eve

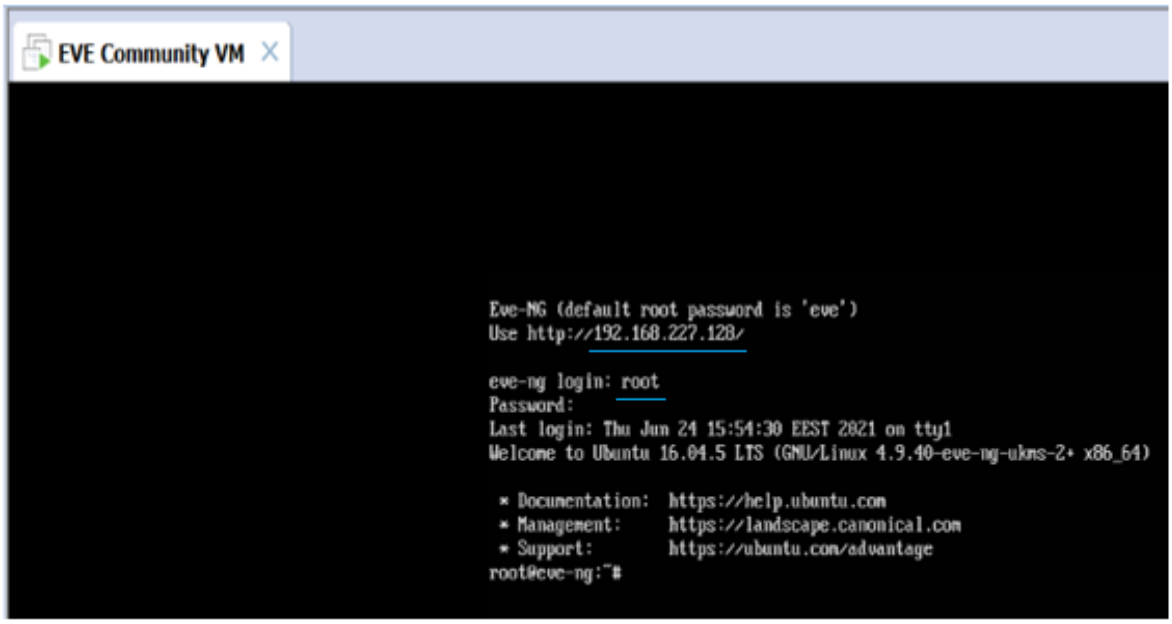

Figure 28: VM d'EVE-ng.

- Après la mise à niveau, connectez-vous à l'interface web d'EVE-NG à l'aide du navigateur chrome. Sur la barre de recherche tapez : http://192.168.227.128

Figure 29: Ecran de connexion EVE-ng.

- l'interface utilisateur de l'émulateur EVE-ng :

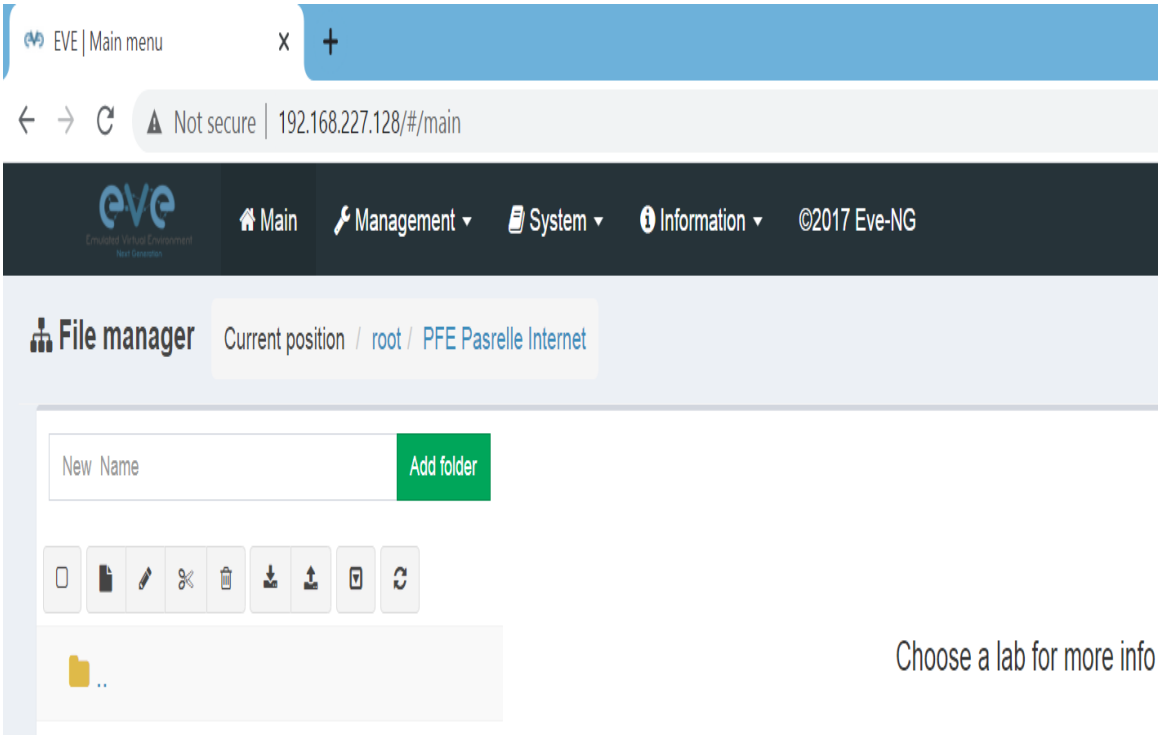

Figure 30: Interface utilisateur EVE-ng.

❖ **Le pack côté client Windows :**

Lorsque vous construisez des laboratoires sur EVE-NG. Vous avez besoin du pack client, qui installera tout le nécessaire pour exécuter des applications Telnet, VNC, Wireshark. Il contient :

- PUTTY 0.73

- Wireshark 3.4.0.0

- Ultra VNC 1.2.3.1 [28]

➢ **PUTTY 0.73**

C'est un programme de terminal pour Windows, linux ou MacOs. Il prend en charge les connexions **SSH, Telnet**. **[29]**

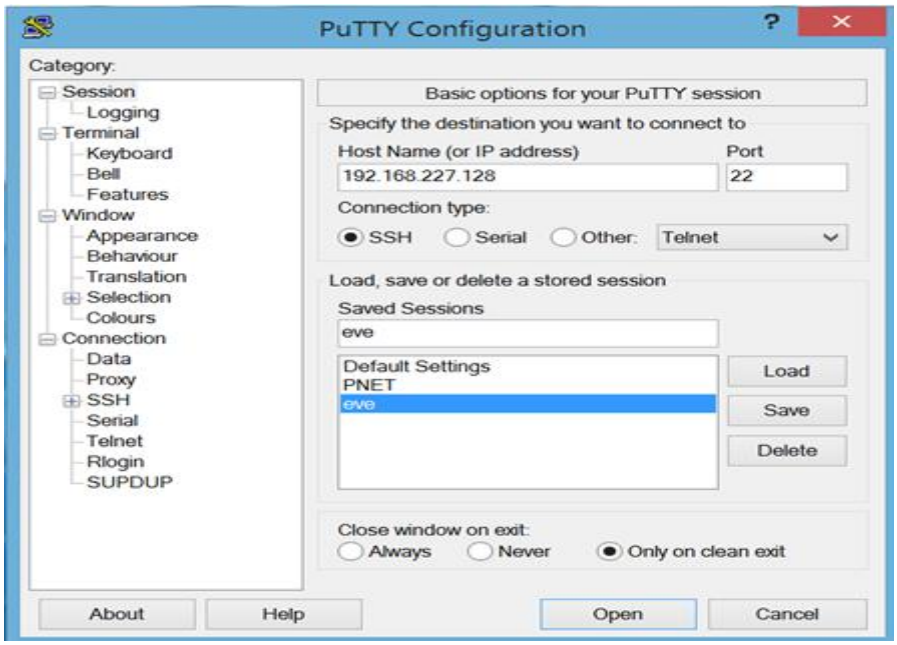

Figure 31: Configuration de putty.

- **Wireshark 3.4.0.0**

C'est un analyseur de paquets gratuit et open source. Il est utilisé pour le dépannage du réseau, l'analyse, le développement de logiciels et de protocoles de communication. **[30]**

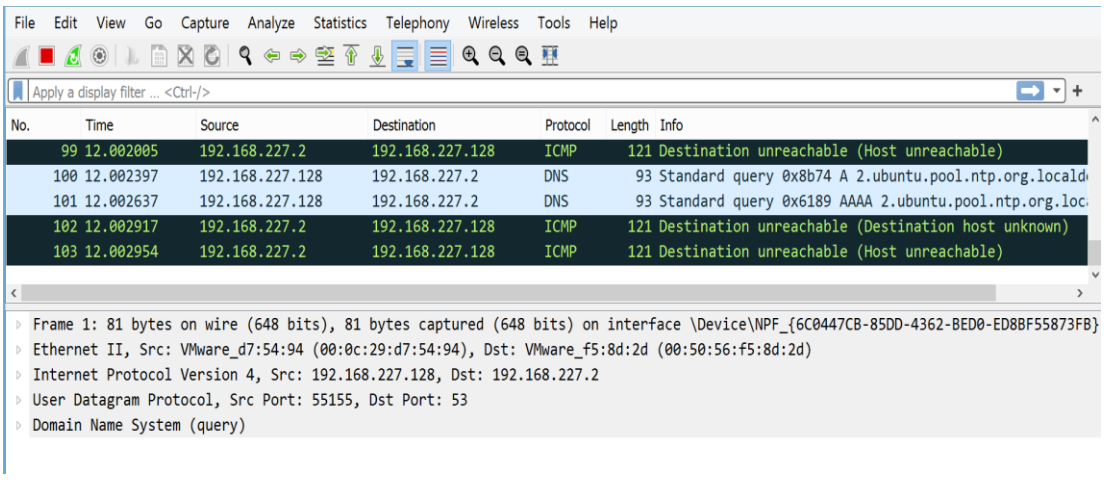

Figure 32: interface Wireshark.

- **Ultra VNC 1.2.3.1**

Ultra VNC est un logiciel d'accès PC à distance puissant, facile à utiliser et gratuit qui peut afficher l'écran d'un autre ordinateur (via Internet ou réseau) sur votre propre écran. Le

programme vous permet d'utiliser votre souris et votre clavier pour contrôler l'autre PC à distance. **[31]**

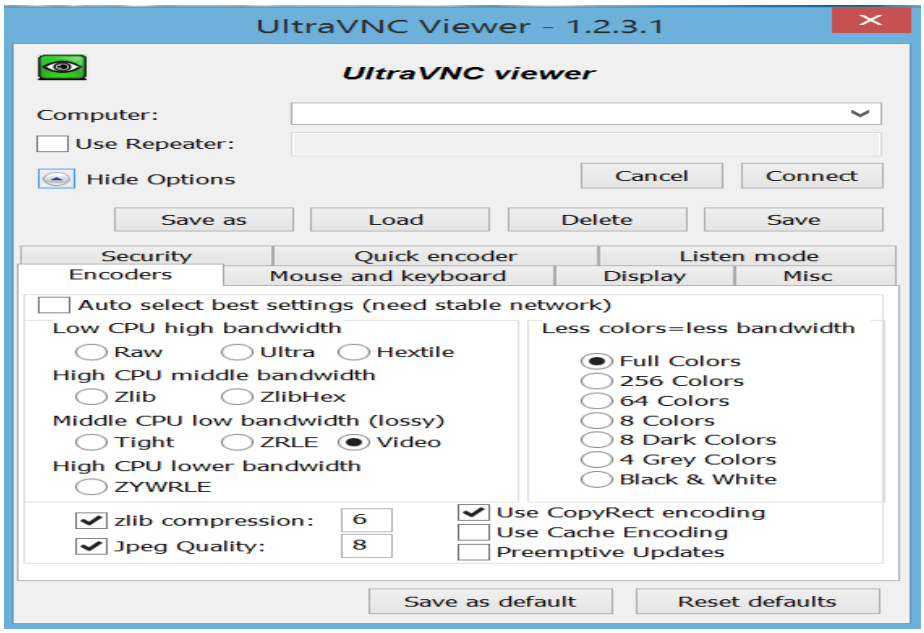

Figure 33: interface Ultra VNC.

➢ **WinSCP :**

WinSCP est une libre open source client SFTP, client FTP. Sa fonction principale est le transfert de fichiers entre un ordinateur local et un ordinateur distant. **[32]**

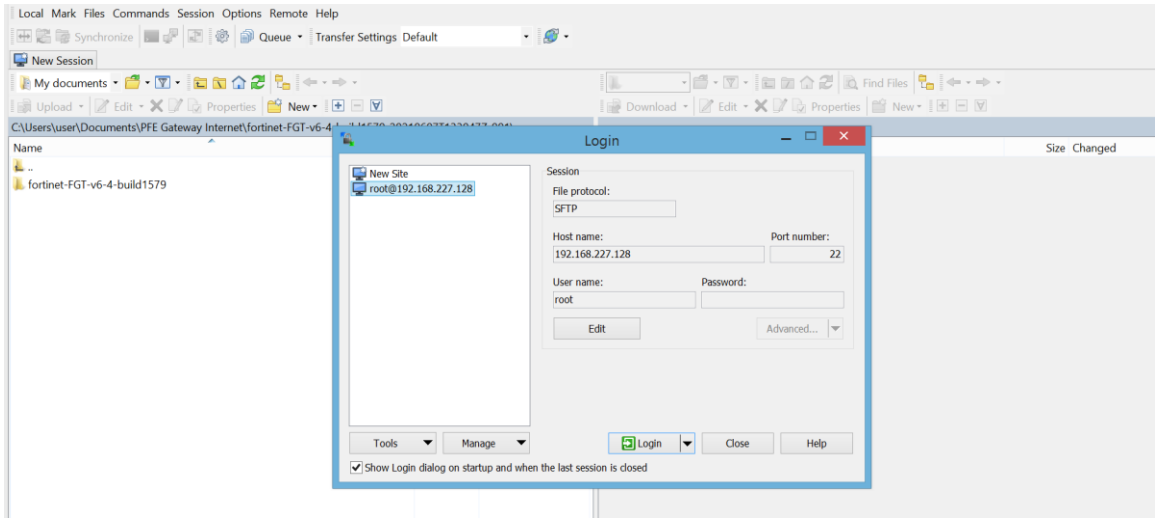

Figure 34: Interface de WinSCP.

❖ **Ajouter des images à EVE-NG :**

EVE-NG n'est pas fourni avec les images logicielles, donc on doit les télécharger puis les transférer vers les répertoires de la VM.

IV.3 Fortinet

Fortinet est un fournisseur de solutions de sécurité protégeant l'entreprise et ses utilisateurs des risques liés à l'exploitation de failles informatiques sur leur réseau, quelle que soit leur origine.

Fortinet est une société hautement technologique qui conçoit ses propres solutions de sécurité, principalement sous la forme de support matériel mais également de logiciels. La gamme de produits proposée par Fortinet permet de mettre en œuvre une sécurité de bout en bout (poste de travail, serveurs, cœur de réseau, périmètre, nomades, sites distants). Il est associé à des fonctionnalités clés de sécurité telle que VPN, antivirus, système de prévention des intrusions (IPS), filtrage Web, anti-spam et allocation de bande passante, lutte contre la perte d'information pour fournir une sécurité multi-niveaux**. [26]**

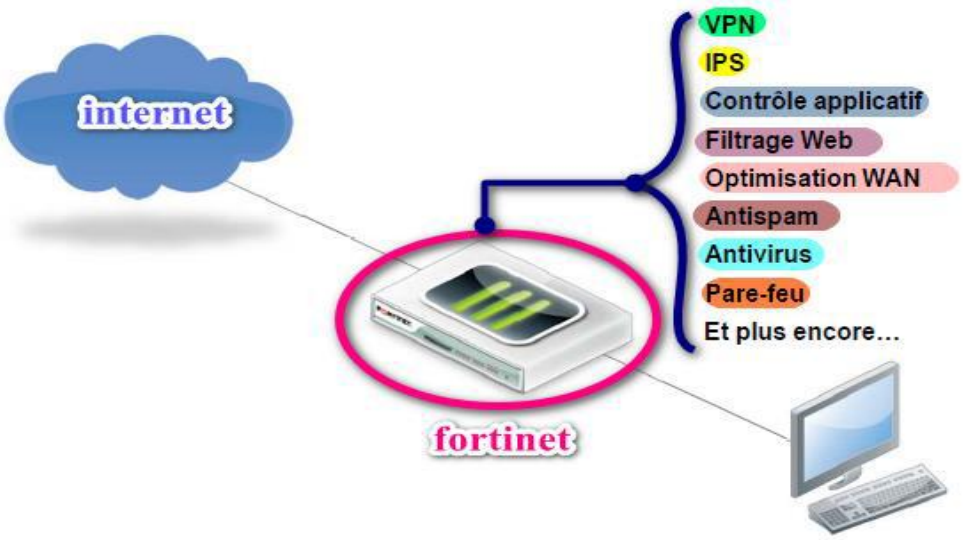

Figure 35:Profils de sécurités.

Le contrôle de données transitant sur le réseau est réalisé par la gamme d'applications FortiGate.

- **FortiGate**

FortiGate est une application matérielle offrant une combinaison intelligente de multiples fonctions de sécurité, dite application UTM (UnifiedThreat Management) ou Application multi-services, mais également ces derniers temps Firewall Next Generation .

Figure : Interface web de fortigate. **[26]**

- **VPN IPsec site a site :**

La création d'un tunnel VPN IPsec site à site permettre la communication entre deux réseaux situés derrière différents appareils FortiGate.

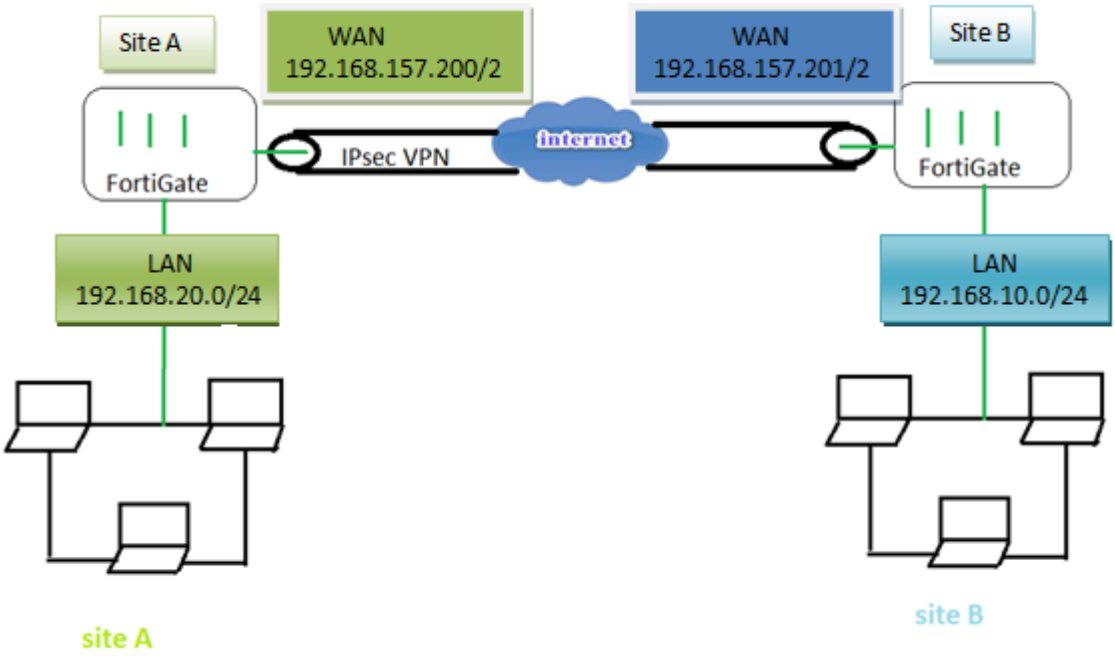

Figure 36:VPN IPSec site a site.

IV.4 Squid

Squid est un proxy de mise en cache pour le Web prenant en charge HTTP, HTTPS, FTP, etc. Il réduit la bande passante et améliore les temps de réponse en mettant en cache et en réutilisant les pages Web fréquemment demandées. Il dispose de contrôles d'accès étendus et constitue un excellent accélérateur de serveur. Il fonctionne sur la plupart des systèmes d'exploitation disponibles. **[33]**

- **Le fichier de configuration /etc/squid/squid.conf**

Tous les paramètres du serveur proxy Squid sont définis dans le fichier :

/etc/squid/squid.conf

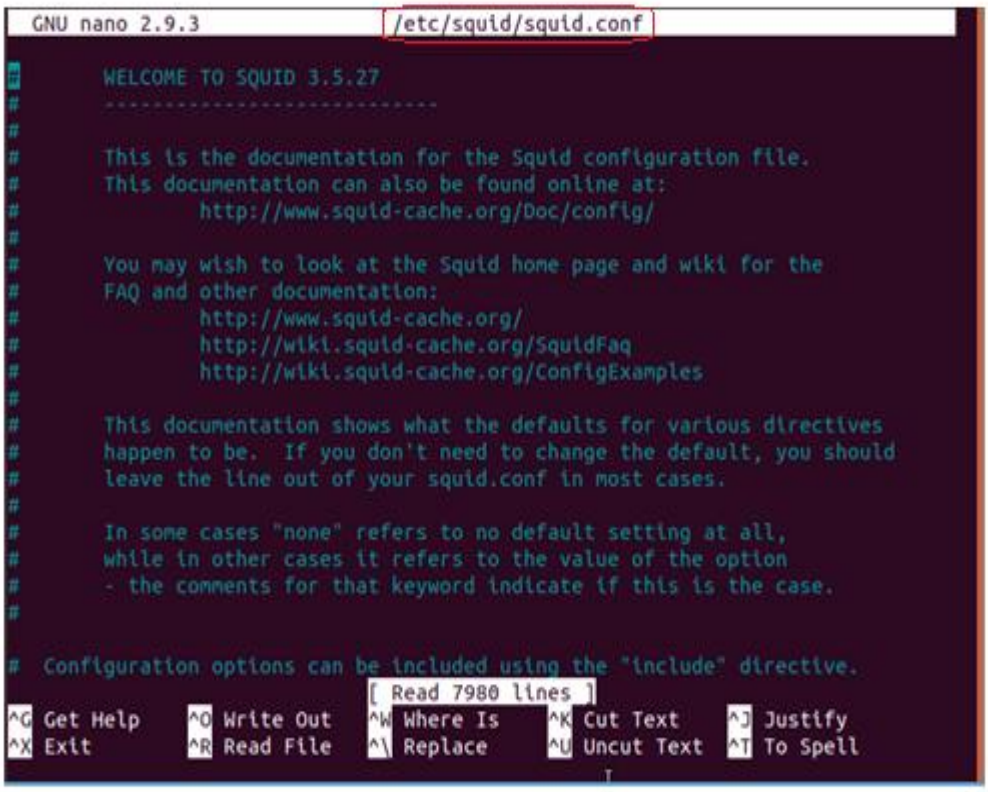

Figure 37:Fichier de configuration de squid.

- **Options de configuration générale :**
  - **Visible_hostname :** le nom du proxy utilisé si aucun identifiant spécifique n'est défini.
  - **http_port :** C'est le port sur lequel Squid écoute les demandes des clients. Le port par défaut est 3128.
- **Options pour les contrôles d'accès :**

Squid fournit un système intelligent qui contrôle l'accès au proxy. En implémentant des ACL.

- **Les ACL (Access Control List) :**

Une liste de contrôle d'accès permet d'autoriser ou de refuser des paquets en fonction d'un certain nombre de critères.

- ✓ **acl<acl_name><type><data>:**
  - **<acl_name> :** le nom de l'ACL.
  - **<type> :** sélectionnez parmi une variété d'options différentes, dans la section contrôles d'accès du fichier de configuration.
  - **<data> :** dépend du type d'ACL (ex : noms d'hôte, des adresses IP ou des URL).
- ✓ **http_access autoriser <acl_name>:** définit qui est autorisé à utiliser le proxy et qui peut accéder à Internet. **[34]**

IV.5 Procédure de configuration

Pour la réalisation, on a utilisé l'émulateur EVE-ng sur VMware Workstation version 12 pro. A travers lequel on va entamer nos étapes d'œuvres.

IV.5.1 Mise en œuvre de la simulation

Apres l'étude de tous les concepts théoriques nécessaires à la réalisation de la partie pratique qui consiste à concevoir une passerelle internet sécurisée, la démarche à suivre sera :

- Liste des équipements utilisés.
- Concevoir l'architecture sur l'émulateur EVE-ng.
- Configuration de routeur.
- Configuration des PC avec des adresses IP.
- Configuration du FG-A.
- Installation du serveur proxy.
- Configuration du FG-B.
- Configuration VPN site a site IPSec entre les deux Fortinet.
- Installation du serveur proxy.

IV.5.1.1 Liste des équipements utilisés

L'architecture est constituée de :

- Un Routeur.
- 2 Switch.
- 2 Cloud (cloud 0 et cloud 1) : cloud 0 pour accéder à l'internet et cloud 1 pour accéder à l'interface graphiques des Fortinets.

- 6 PC (Linux- Ubuntu 18.04, Windows 7, 4 VPC pour les tests de ping).
- 2Pare-feu Fortinet.

❖ **Tables d'adressage :**

Les interfaces des différents équipements sont indiquées dans le tableau suivant :

Tableau 1: Tableau d'adressage**.**

Equipements	Interface	Adresse IP	Masque de sous réseau	Passerelle
Routeur	Fa1/0	192.168.227.10	255.255.255.0	192.168.227.2
	Fa0/0	192.168.227.2	255.255.255.252	
	Fa0/1	192.168.227.6	255.255.255.252	
FG-A	Port1	192.168.157.100	255.255.255.0	192.168.157.2
	Port2	192.168.10.1	255.255.255.0	
	Port3	192.168.1.1	255.255.255.252	192.168.1.2
	Port4	172.16.0.1	255.255.255.192	
	Port5	192.168.30.1	255.255.255.0	
FG-B	Port1	192.168.157.110	255.255.255.0	192.168.157.2
	Port2	192.168.20.1	255.255.255.0	
	Port3	192.168.1.5	255.255.255.252	192.168.1.6
VPC1-B	Eth0	192.168.20.20	255.255.255.0	192.168.20.1
VPC2-B	Eth0	192.168.20.10	255.255.255.0	192.168.20.1
VPC1-A	Eth0	192.168.10.20	255.255.255.0	192.168.10.1
VPC2-A	Eth0	192.168.30.12	255.255.255.0	192.168.30.1
Cloud 1	/	192.168.157.0	255.255.255.0	192.168.157.2
Cloud 0	/	192.168.227.0	255.255.255.0	192.168.227.2
Window7	E0	192.168.10.10	255.255.255.0	192.168.10.1
Server (Linux)	E0	172.16.0.20	255.255.255.192	172.16.0.1

IV.5.1.2Présentation de l'architecture :

➢ **Schéma globale :**

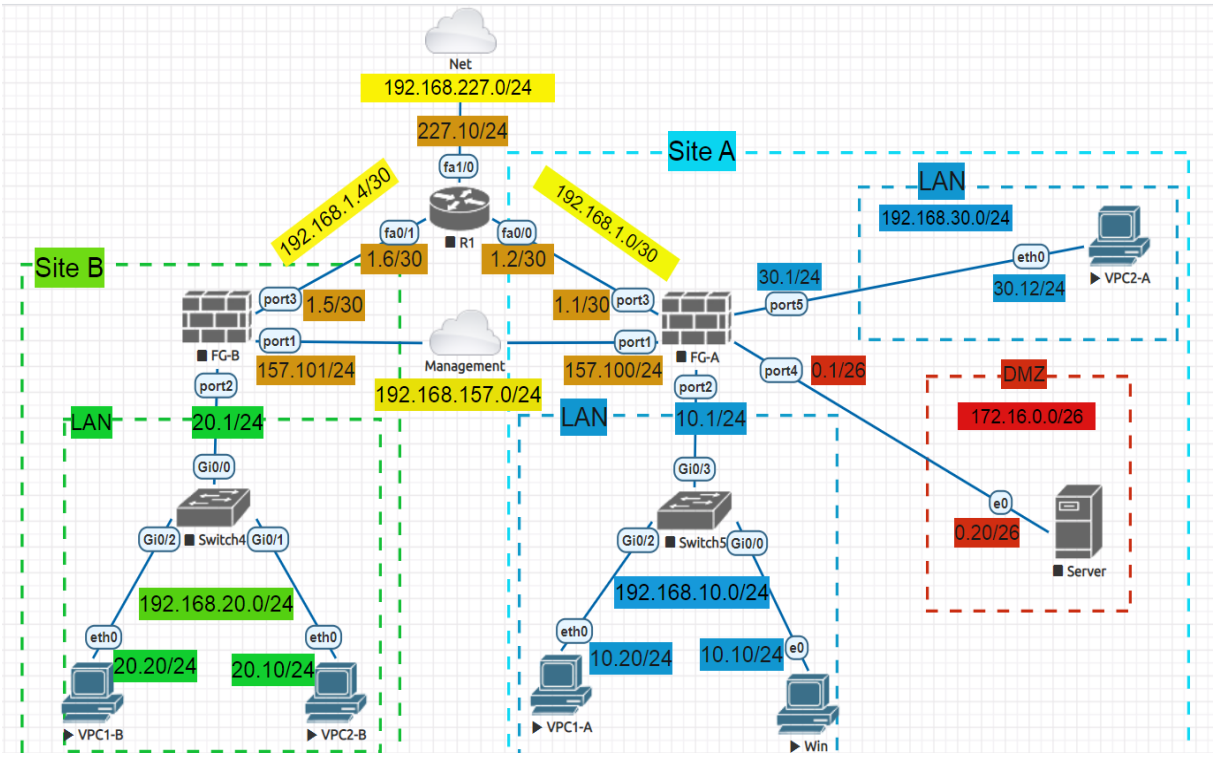

Figure 38:Topologie du projet.

IV.5.1.3Configuration du site A :

- **Schéma SITE A:**

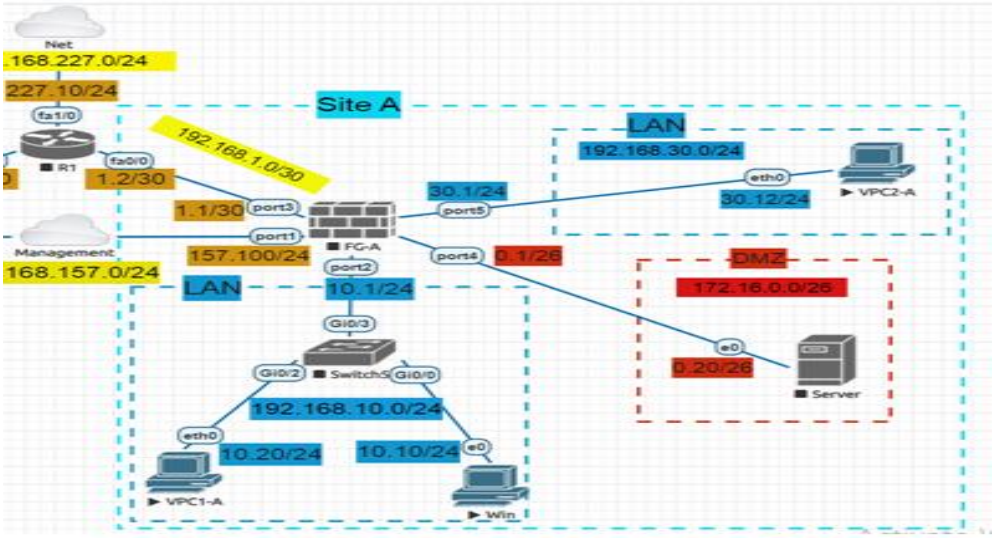

Figure 39:Architecture de site A.

➢ **Configuration du ROUTEUR :**

- **Attribuez les adresses aux interfaces :**

```
R1(config)#interface fastEthernet 0/0
R1(config-if)#ip address 192.168.1.2 255.255.255.252
R1(config-if)#no sh
R1(config-if)#no shutdown
```

Figure 40: Configuration de l'interface fa 0/0.

```
R1(config)#interface fastEthernet 0/1
R1(config-if)#ip address 192.168.1.6 255.255.255.252
R1(config-if)#no shutdown
```

Figure 41: Configuration de l'interface fa 0/1.

```
R1(config)#interface fastEthernet 1/0
R1(config-if)#ip address 192.168.227.10 255.255.255.0
R1(config-if)#no shutdown
```

Figure 42: Configuration de l'interface fa 1/0.

- **Configurez les IP route.**

```
R1(config)#ip route 0.0.0.0 0.0.0.0 192.168.227.2
R1(config)#ip route 192.168.10.0 255.255.255.0 192.168.1.1
R1(config)#ip route 192.168.30.0 255.255.255.0 192.168.1.1
R1(config)#ip route 172.16.0.0 255.255.255.192 192.168.1.1
R1(config)#ip route 192.168.20.0 255.255.255.0 192.168.1.5
```

Figure 43: Configuration des routes.

- **Pour sauvegarder les modifications exécutez la commande.**

```
R1#copy running-config startup-config
```

Figure 44:Enregistré la configuration de routeur.

- **Teste de connectivité :**

```
R1#ping 192.168.227.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.227.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/8/12 ms
```

Figure 45:Test de connectivité entre le routeur et l'internet.

D'après ce résultat on a conclu que le trafic est bien passé vers l'internet.

➢ **Configuration des machines :**

- **Configurez les adresses ip pour les PC :**

❖ **VPC1-A**

```
VPCS> ip 192.168.10.20 255.255.255.0 192.168.10.1
```

Figure 46:Configurer l'adresse IP pour VPC 1-A.

❖ **VPC2-A**

```
VPCS> ip 192.168.30.12 255.255.255.0 192.168.30.1
```

Figure 47:Configurer l'adresse IP pour VPC 2-A.

❖ **PC-Win**

Figure 48:Configurer l'adresse IP pour PC-Win.

➢ **Configuration du FG-A :**

- Attribuez un nom au fortigate (FG-A) et Configurez port1 par les lignes de commandes suivantes :

```
FG-A login: admin
Password:
Welcome !

FG-A # config system interface

FG-A (interface) # edit port1

FG-A (port1) # set mode static

FG-A (port1) # set ip 192.168.157.100 255.255.255.0

FG-A (port1) # set allowaccess https http ping ssh

FG-A (port1) # end
```

Figure 49:Configuration du port 1 de FG-A.

- Accédez depuis le navigateur à l'interface web du fortigate avec @ IP 192.168.157.100 puis introduisez le nom admin et le mot de passe et cliquez sur login.

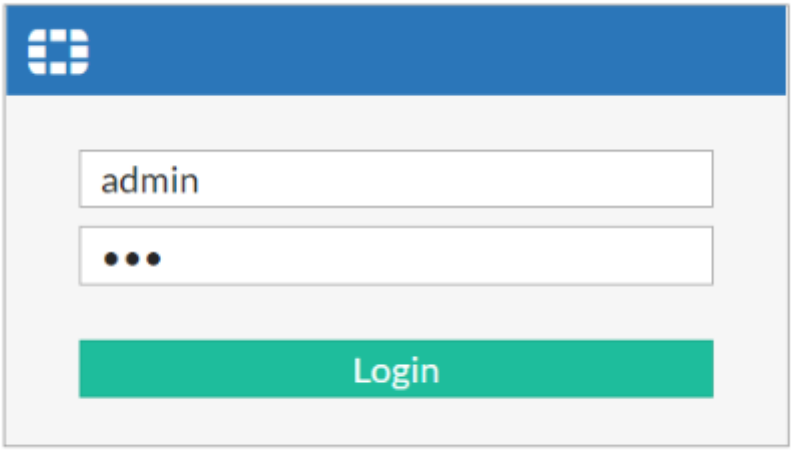

Figure 50: Ecran de connexion FG-A.

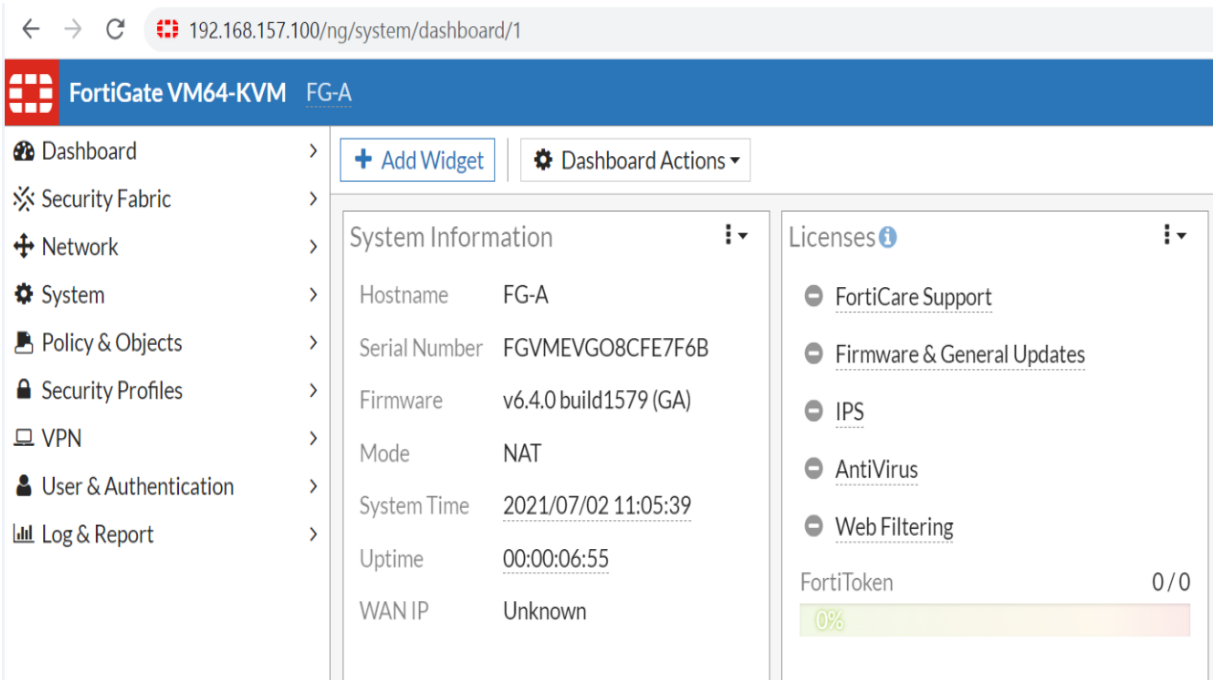

Figure 51: Interface web de FG-A.

- Pour compléter la configuration des autres ports, accédez à Network puis Interfaces, double cliquez sur le port et appuyez sur Edit.

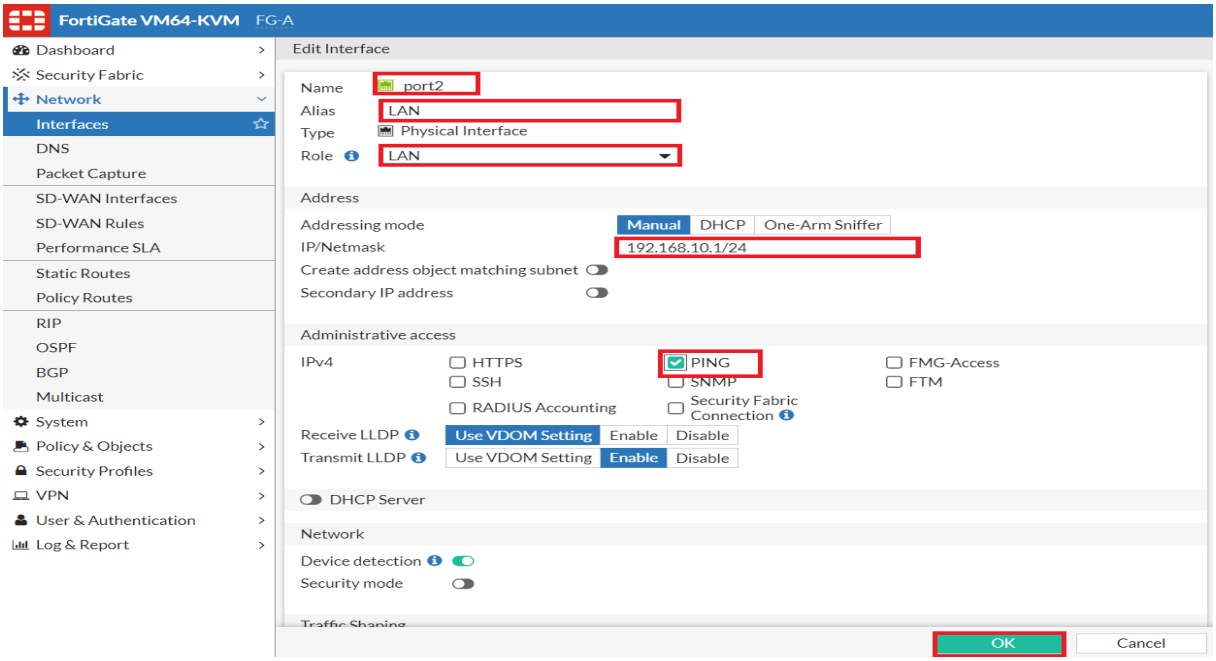

Figure 52:Configuration du port 2 de FG-A.

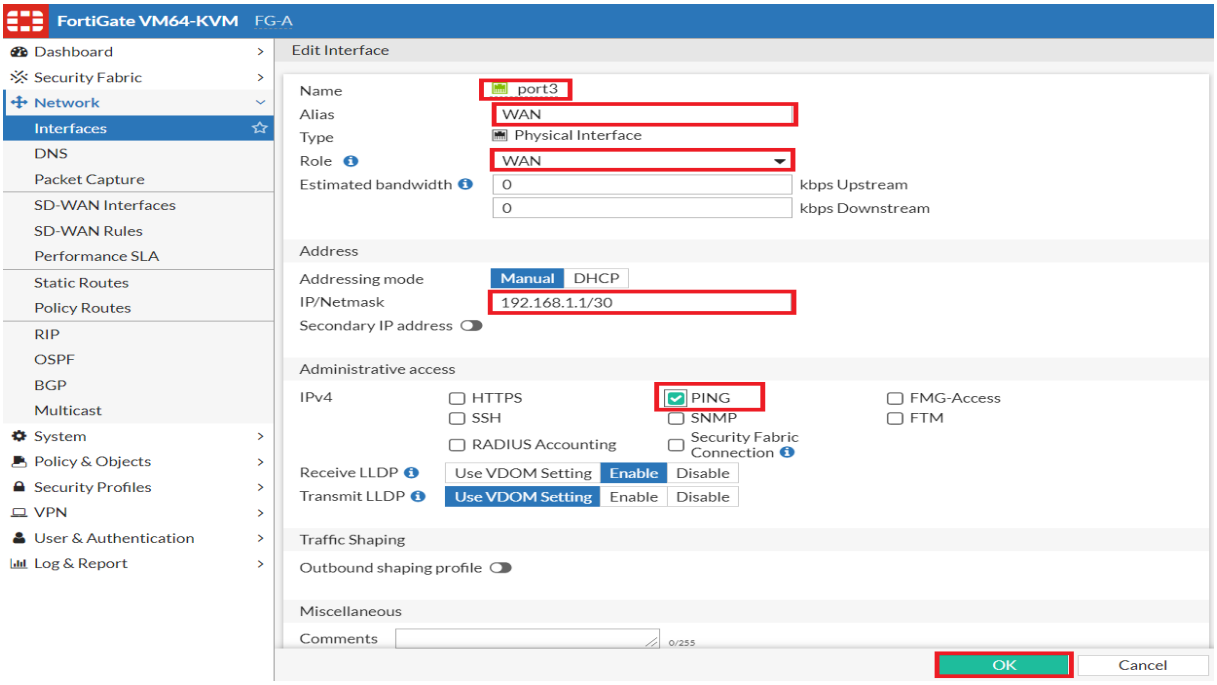

Figure 53:Configuration du port 3 de FG-A.

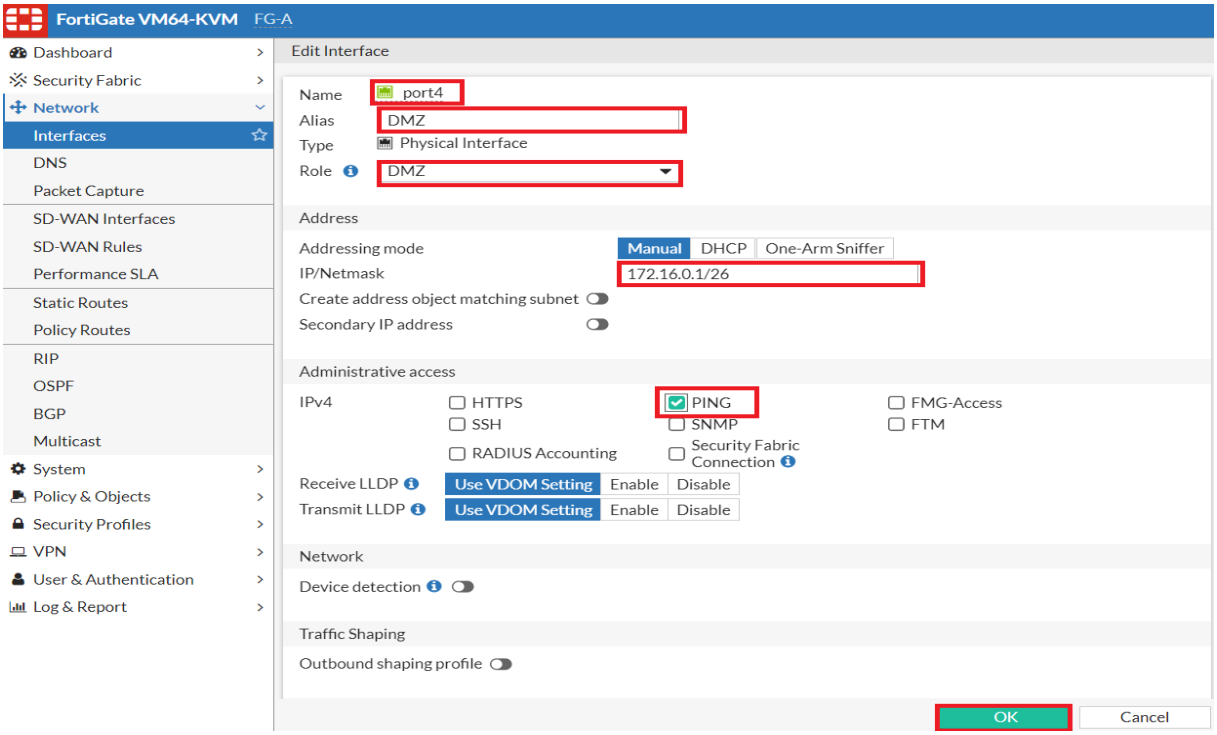

Figure 54:Configuration du port 4 de FG-A.

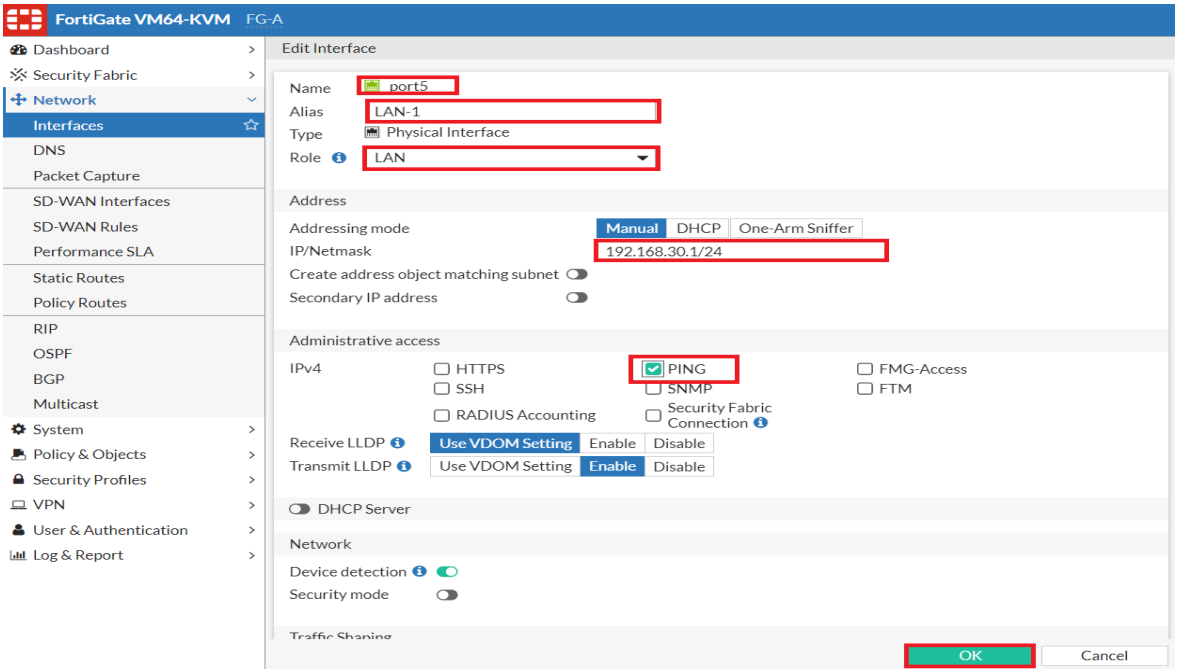

Figure 55:Configuration du port 5 de FG-A.

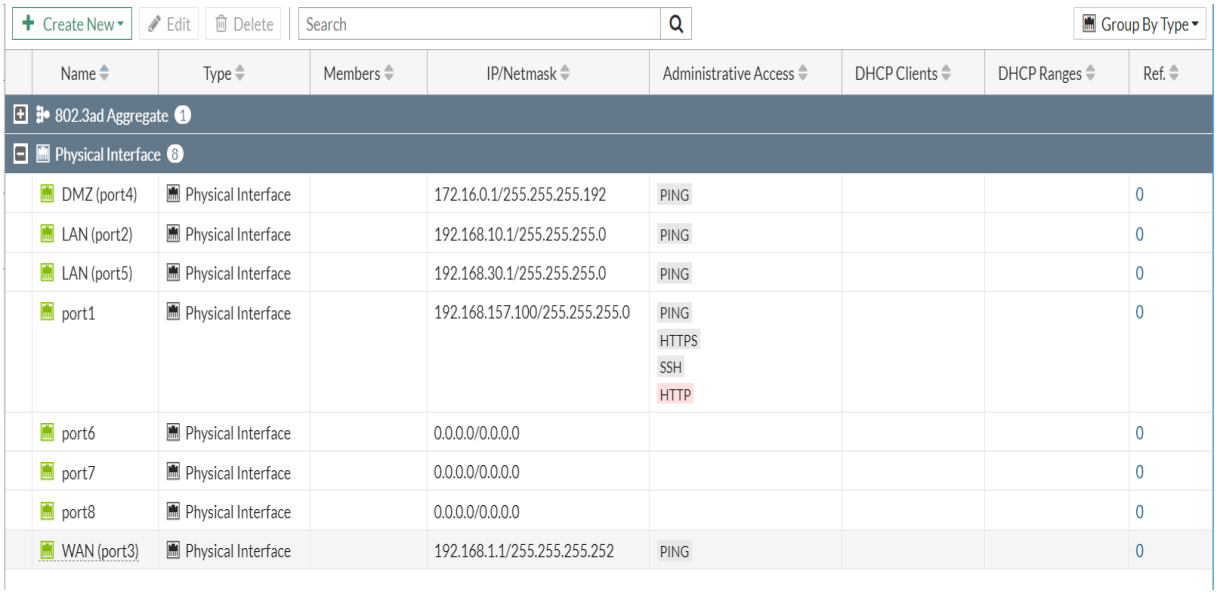

Figure 56: Liste des ports configurés et leurs adresses.

- Ajoutez une route statique, en cliquant sur Network puis sur Static Routes. Insérez la passerelle (192.168.1.2) et cliquez sur ok.

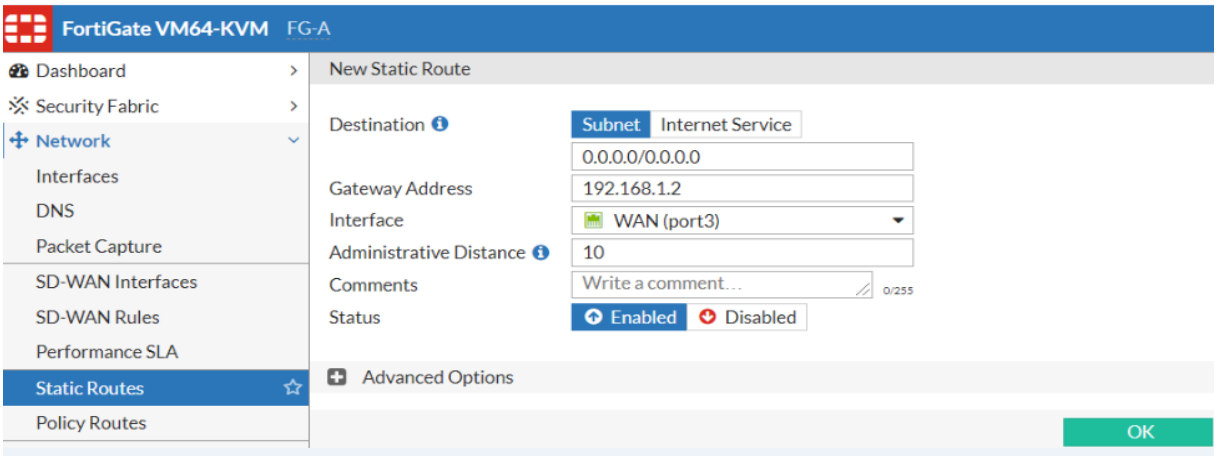

Figure 57:Configuration du la route statique.

- Résultat de la route statique :

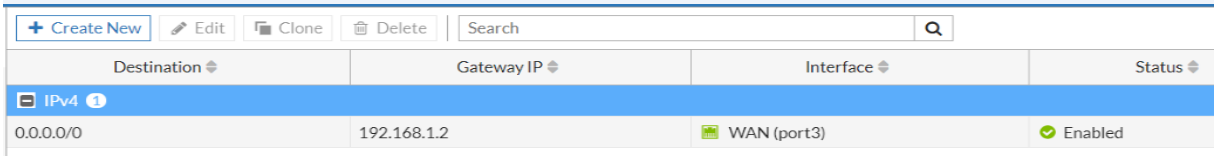

Figure 58:Les résultats du la route statique.

- Création des adresses pour les règles de sécurité du FG-A. pour cela accédez à Policy &Objects puis à Addresses, cliquez sur Create New.

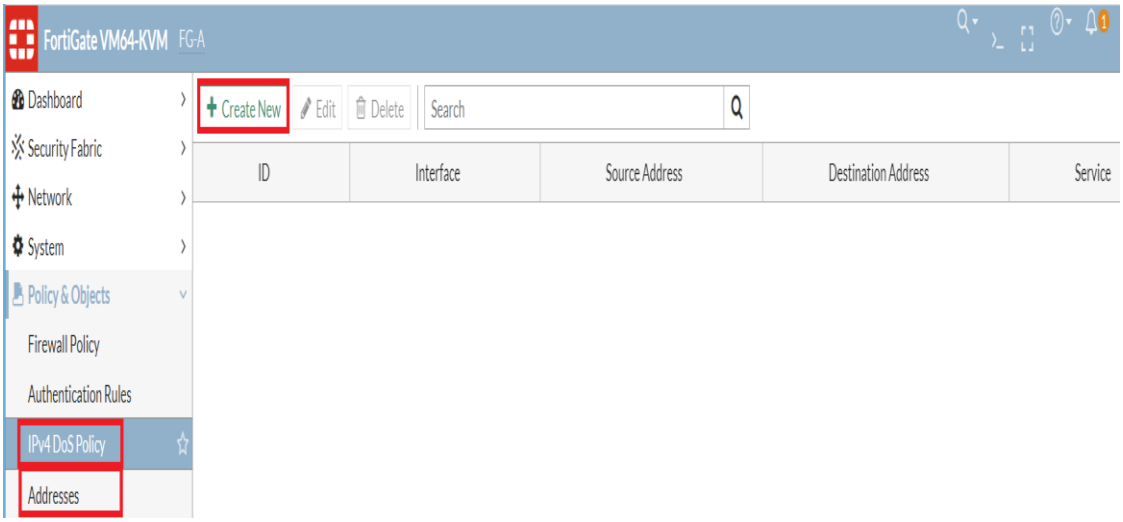

Figure 59:Création des adresses pour les ACL du FG-A.

- Création des règles de sécurités du FG-A. accédez à Policy &Objects puis à IPv4 DoS Policy et cliquez sur Create New.

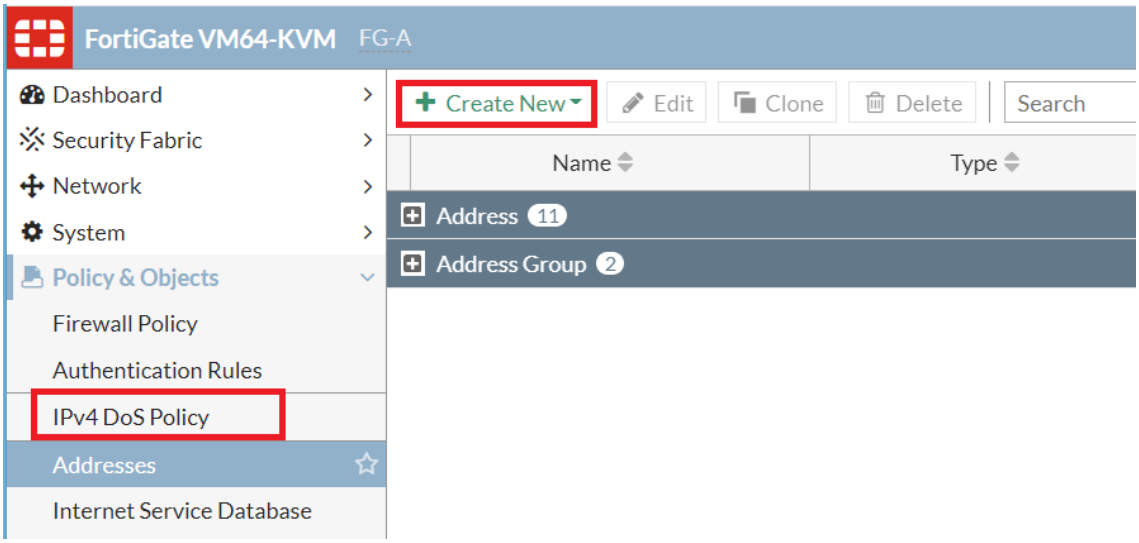

Figure 60:Création des ACL du FG-A.

- Cette règle, spécifiée une autre méthode de sécurité qui utilise les profils de sécurités du fortigate, pour accéder directement à internet.

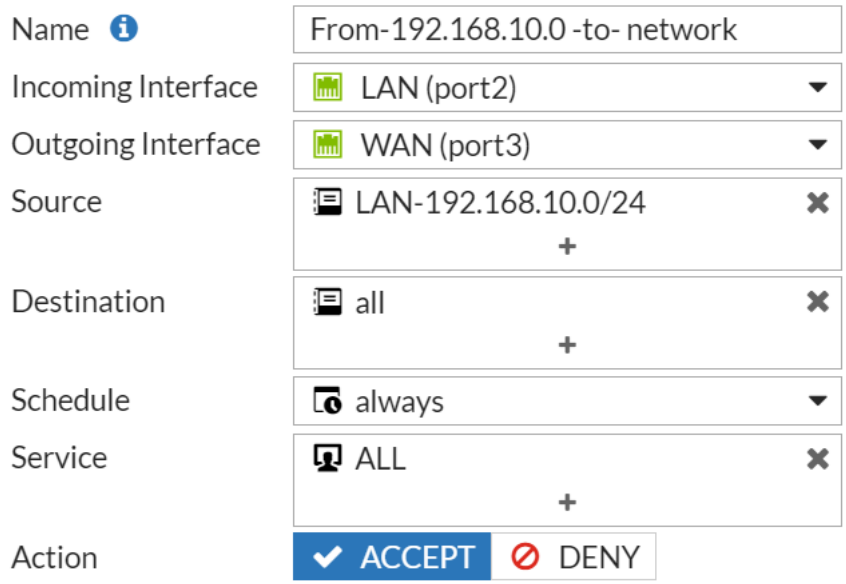

Figure 61:Ajoute d'une ACL pour accéder à internet.

- La règle suivante, autorise le trafic de la zone DMZ vers internet.

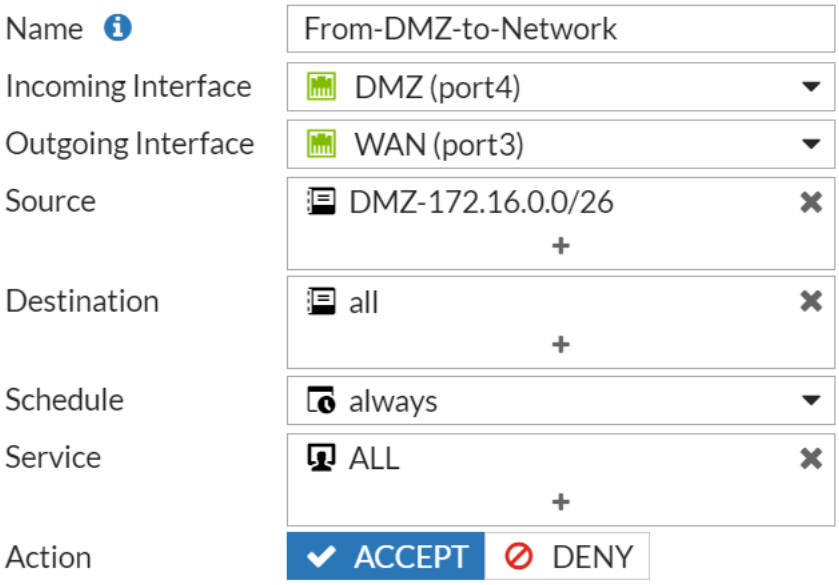

Figure 62:Ajoute d'une ACL pour accéder de la zone DMZ à internet.

- La règle suivante, afin d'effectuer une requête internet depuis le réseau local vers internet ce dernier doit passer par le proxy.

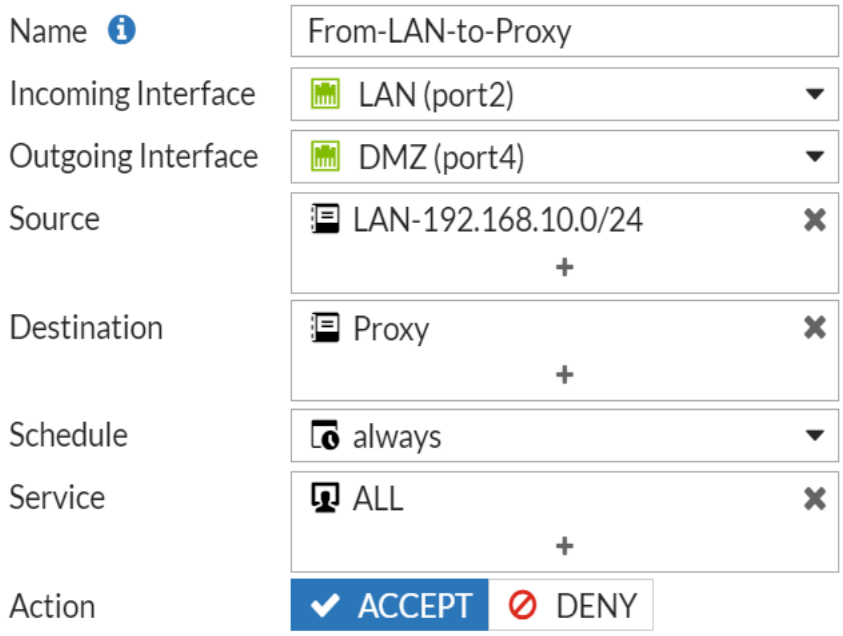

Figure 63:Ajoute d'une ACL pour accéder au proxy.

- Les règles de sécurités configurées.

Name	Source	Destination	Schedule	Service	Action	NAT
DMZ (port4) → WAN (port3) 1						
From-DMZ-to-Network	DMZ-172.16.0.0/26	all	always	ALL	ACCEPT	Disabled
LAN (port2) → DMZ (port4) 1						
From-LAN-to-Proxy	LAN-192.168.10.0/24	Proxy	always	ALL	ACCEPT	Disabled
LAN (port2) → WAN (port3) 1						
From-192.168.10.0 -to- network	LAN-192.168.10.0/24	all	always	ALL	ACCEPT	Disabled

Figure 64:Liste des ACL ajoutées.

➢ Installation du serveur Squid :

- Pour installer squid tapez la commande apt-get install squid et y pour continuer

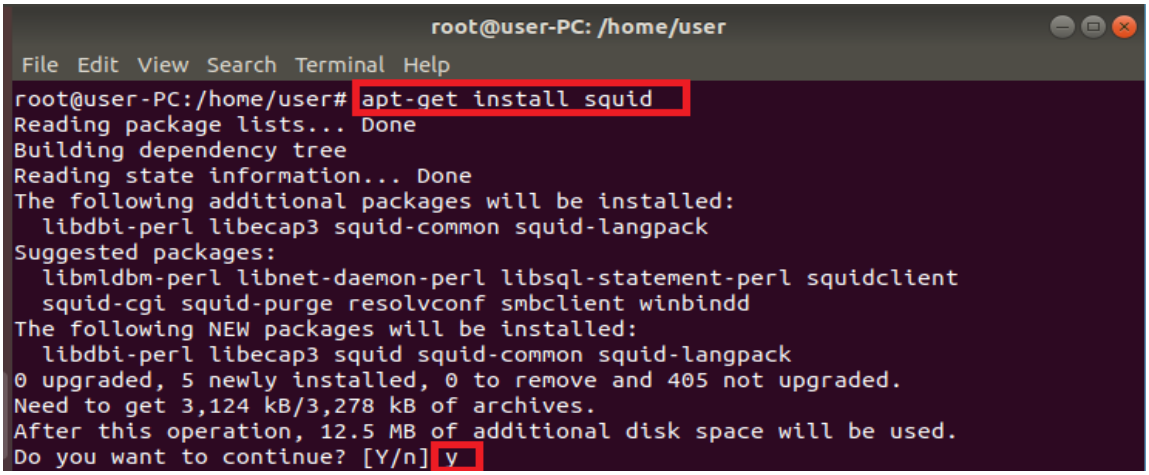

Figure 65:Installation de squid.

- Copiez le fichier de configuration du Squid /squid.conf dans squid.conf. Original, et pour commencer la configuration, ouvrez le fichier squid.conf

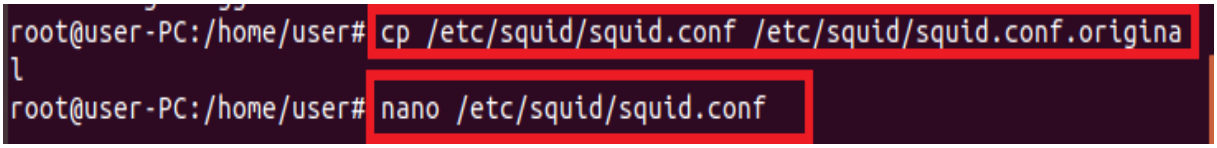

Figure 66: Ouvrir le fichier de configuration du squid.

- Le fichier de configuration :

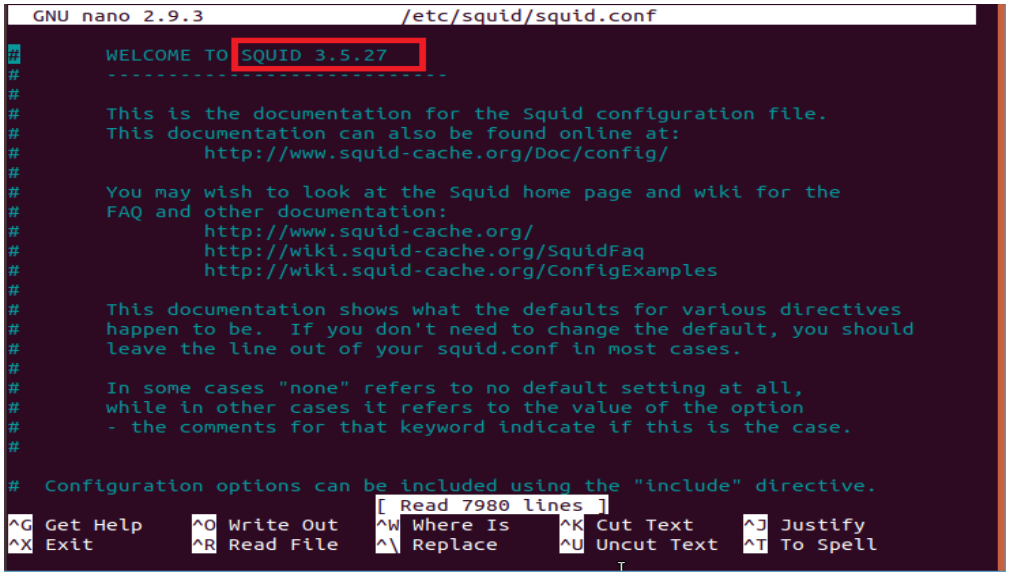

Figure 67:Fichier < squid.conf >.

- Définissiez un nom au proxy, sur le fichier de configuration cliquez sur ctrl+w pour effectuer une recherche sur celui-ci puis tapez visible_hostname, sous la ligne #TAG : visible_hostname réécrivez visible_hostname puis insérez un nom à votre choix.

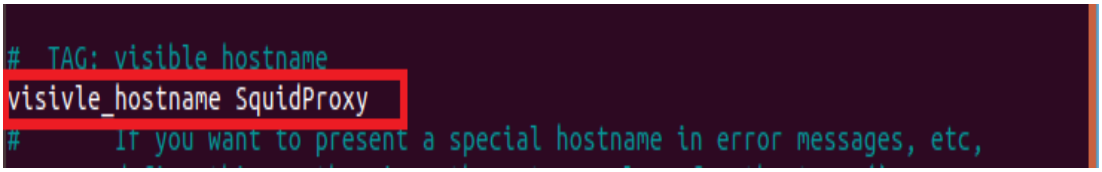

Figure 68:Définis un nom pour le serveur proxy.

- Recliquez sur ctrl+w et tapez http_port, puis faite défilé jusqu'à la ligne squid normally listens to port 3128, ensuite nous avons laissé la valeur de port par défaut 3128.

Figure 69:Changement du port d'écoute.

- A ce là, les acls sont configuré mais ne sont pas activé pour ce faire il faut ajouter la ligne « http_access allow all »dans la rubrique des autorisations de navigation.

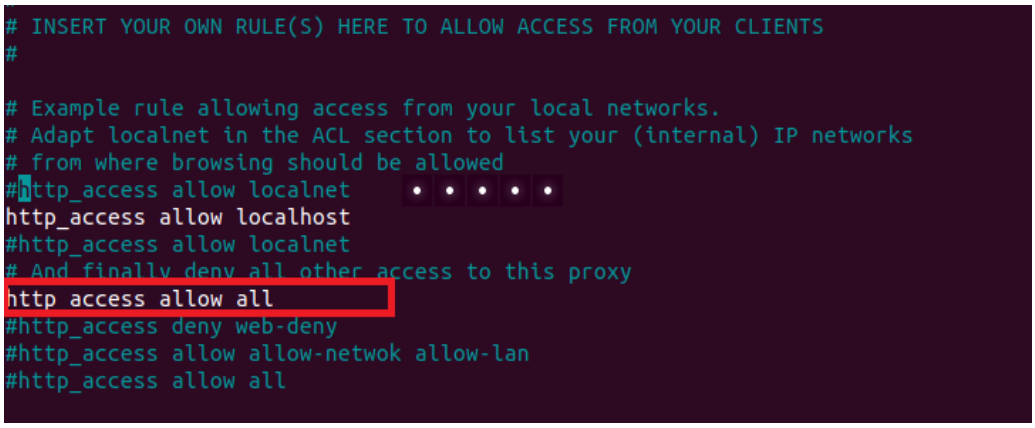

Figure 70:Activation des ACLs.

- Apres avoir effectué toutes les étapes précédentes ajouter, le serveur squid est prêt à l'emploi, cependant il reste une fonctionnalité intéressante à tester qui se trouve être le filtrage par demain, donc nous avons comme exemple le site de facebook.

- La ligne concernant la commande de blacklistage sera ajoutée juste en dessous des acls pour bloqué l'accès à facebook.

Figure 71:ACL bloquant l'accès à Facebook.

- Il faut bien sûr activer cet acl, cela se fait en ajoutant une ligne dans la rubrique qui concerne le blocage d'accès.

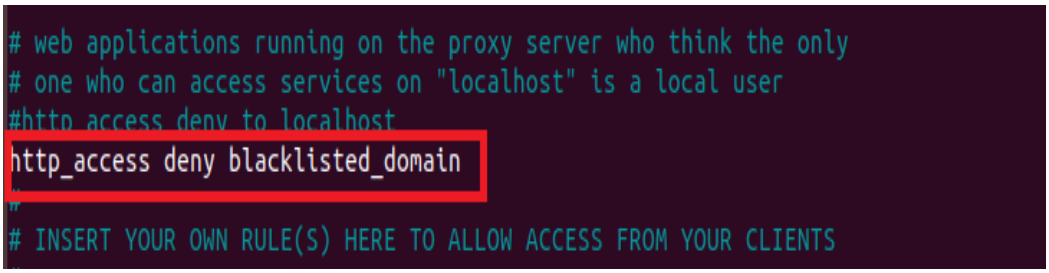

Figure 72:Activation de l'acl blacklist.

- Pressez sur ctrl+o, pour sauvegarder les modifications puis sur ctrl+x pour quitter le fichier de configuration.
- Redémarrez le service squid.

Figure 73: Redémarrage de squid.

- Vérification de l'état de serveur proxy par la commande « service squid status »

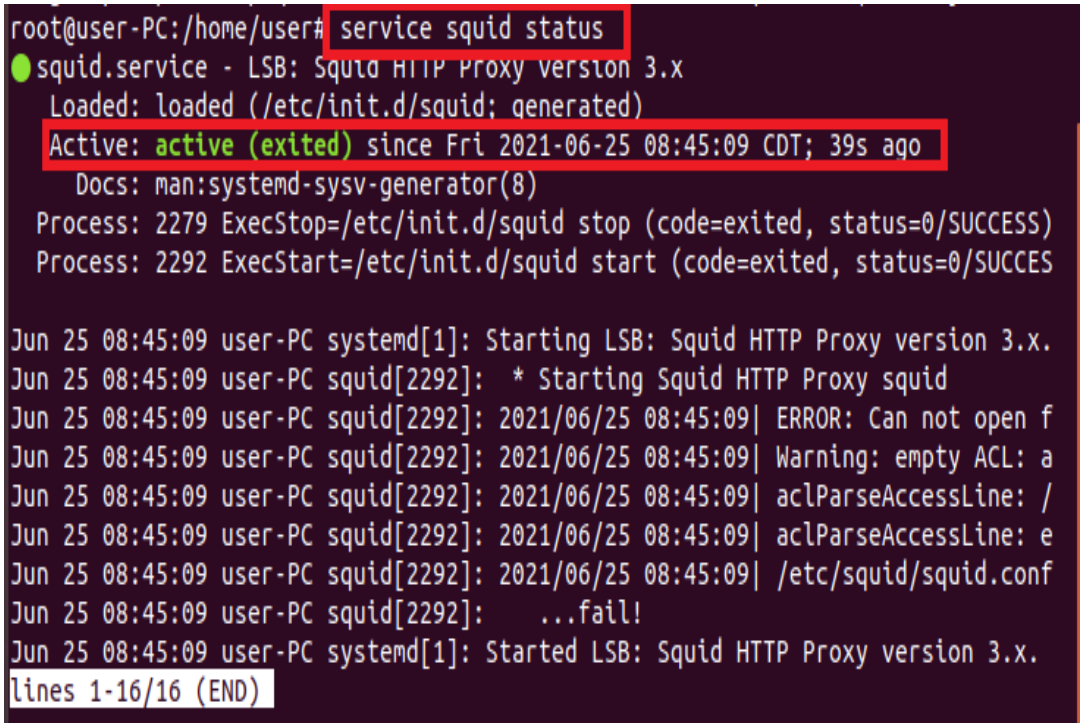

Figure 74: Vérification de l'état de squid.

- **Configuration du Proxy sur Windows :**
  - Maintenant que le serveur proxy est configuré dans notre machine linux sous Ubuntu 18, c'est au tour de la machine Windows du réseau « Lan »d'être configuré afin de fonctionner avec notre proxy.
  - Après avoir attribué une adresse statique à la machine nous devrons procéder à l'ajoute de l'adresse du proxy à la configuration réseau de la machine.
  - pour ce faire accédons aux propriétés internet. Puis aux paramètres du Lan afin d'ajouter l'adresse du serveur Proxy ainsi que le port sur lequel il écoute.

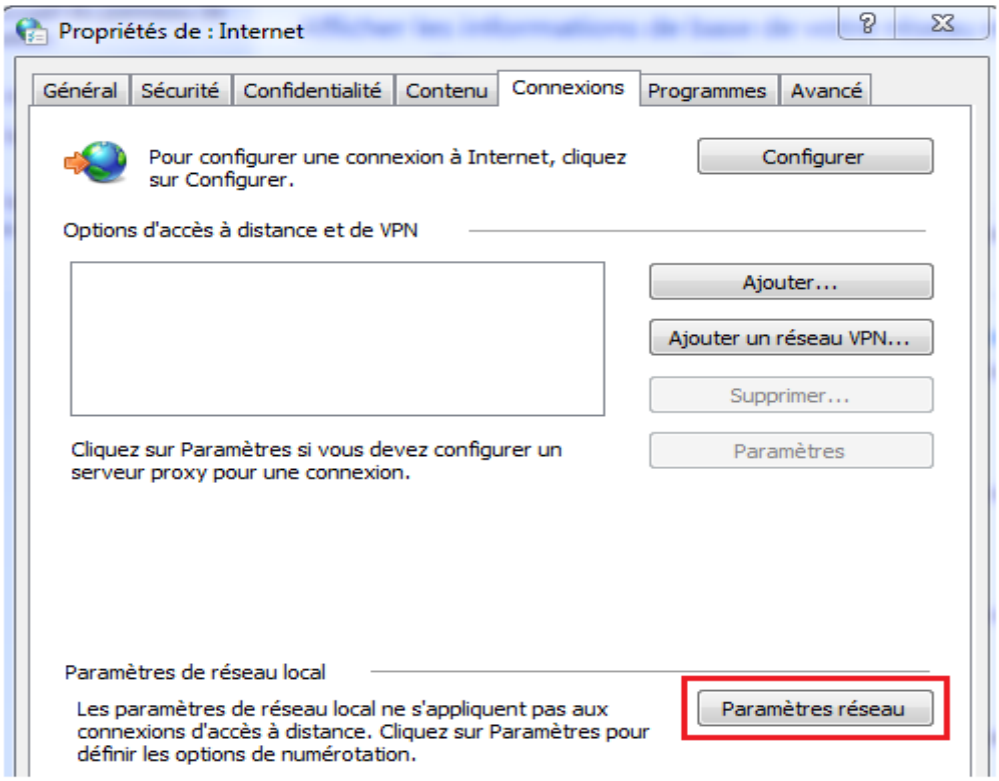

Figure 75:Propriété internet de Windows.

- Dans les paramètres réseau cochez la case utiliser un proxy pour le réseau local, puis insérez votre adresse IP (172.16.0.20) suive d'un numéro de port (3128). Ensuite, cliquez sur ok pour confirmer.

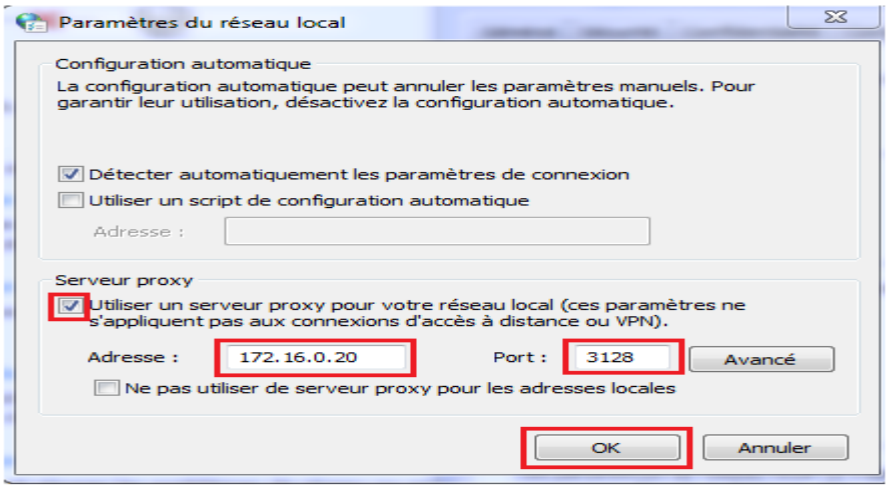

Figure 76:l'ajout du proxy à la config Windows.

- Accédez depuis votre navigateur au site www.facebook.com, ce dernier sera refusé par le squid.

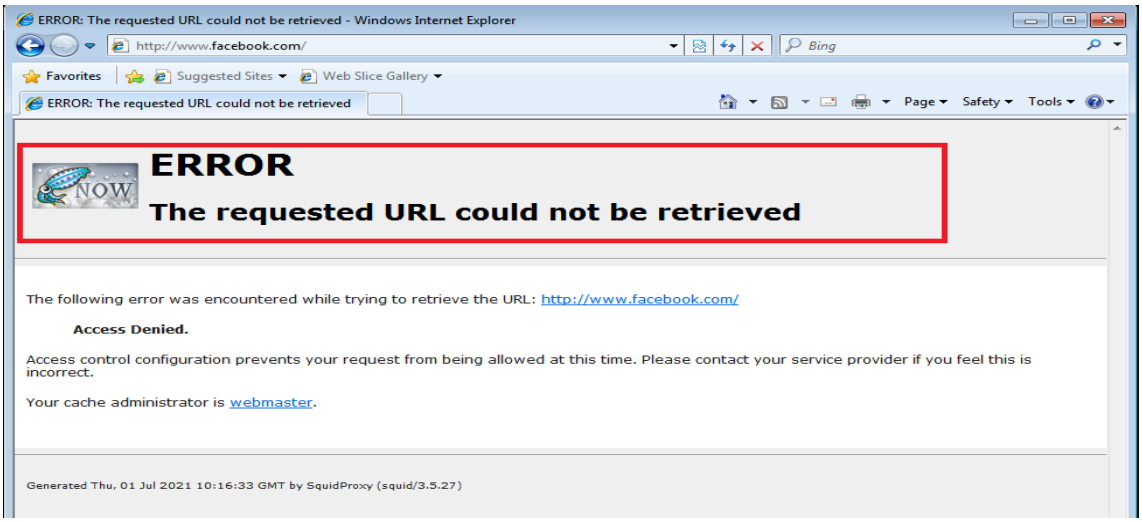

Figure 77:Blocage de facebook par le proxy.

- la figure précédente prouve bien que les requêtes transitent par le serveur proxy « SquidProxy ».

IV.5.1.4 Configuration du site B :

- **schéma SITE B :**

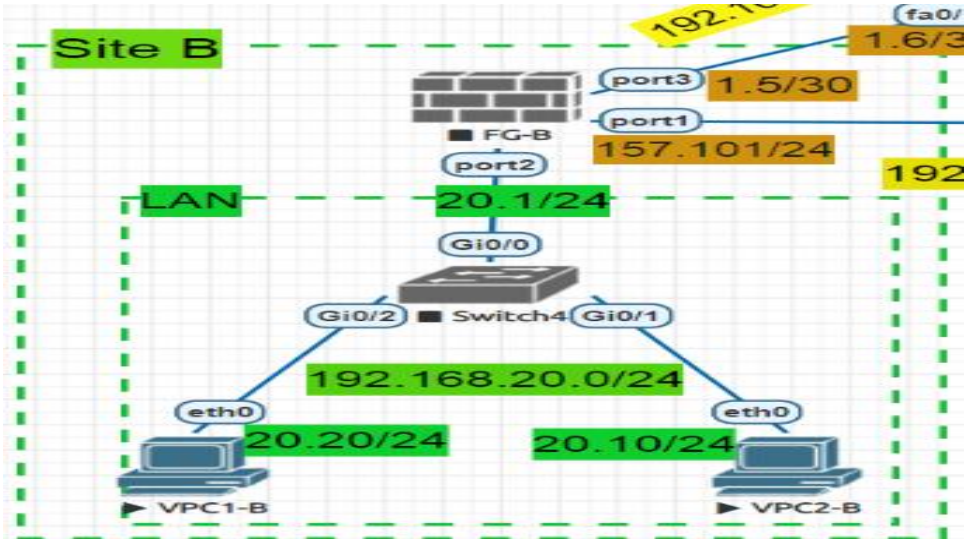

Figure 78:Architecture de site B.

➢ Configuration des machines :

- **Configurez les adresses ip pour les VPC :**

❖ **VPC1-B**

```
VPCS> ip 192.168.20.20 255.255.255.0 192.168.20.1
```

Figure 79:Configurer l'adresse IP pour VPC 1-B.

❖ **VPC2-B**

```
VPCS> ip 192.168.20.10 255.255.255.0 192.168.20.1
```

Figure 80:Configurer l'adresse IP pour VPC 2-B

➢ Configuration du FG-B :

- Attribuez un nom au fortigate (FG-B) et Configurez port1 par les lignes de commandes suivantes :

```
FG-B login: admin
Password:
Welcome !

FG-B # config system interface

FG-B (interface) # edit port1

FG-B (port1) # set mode static

FG-B (port1) # set ip 192.168.157.101 255.255.255.0

FG-B (port1) # set allowaccess https http ping ssh

FG-B (port1) # end
```

Figure 81: Configuration du port 1 de FG-B.

- Accédez depuis le navigateur à l'interface web du fortigate @IP 192.168.157.101 puis introduisez le nom admin et le mot de passe et cliquez sur login.

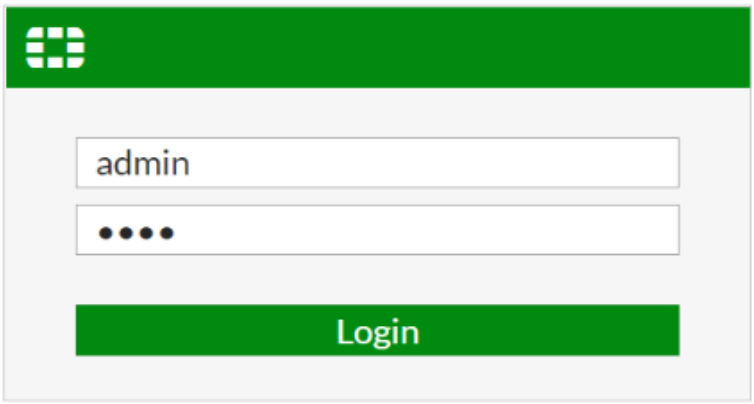

Figure 82: Ecran de connexion FG-B.

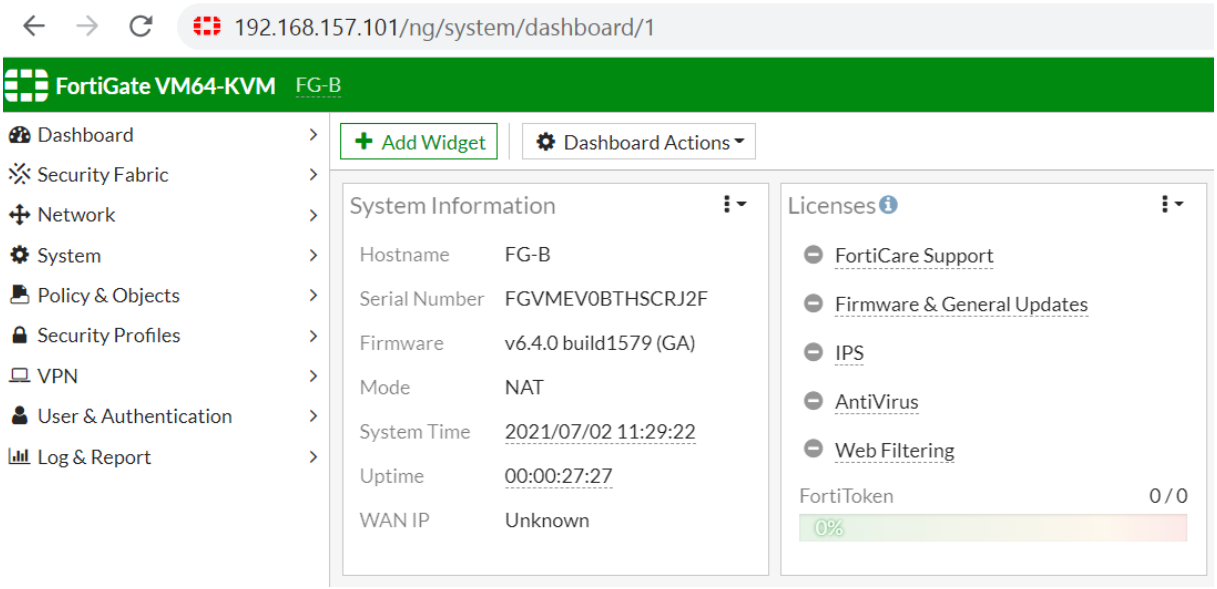

Figure 83: Interface web de FG-B.

- Compléter la configuration des ports :

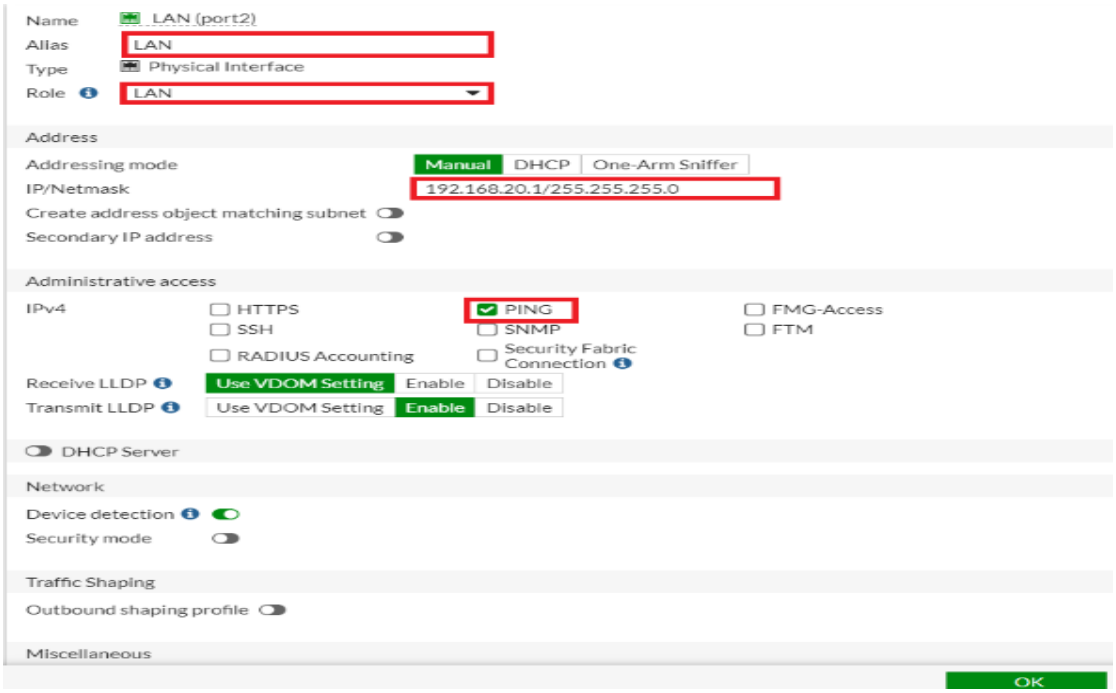

Figure 84:Configuration du port 2 de FG-B.

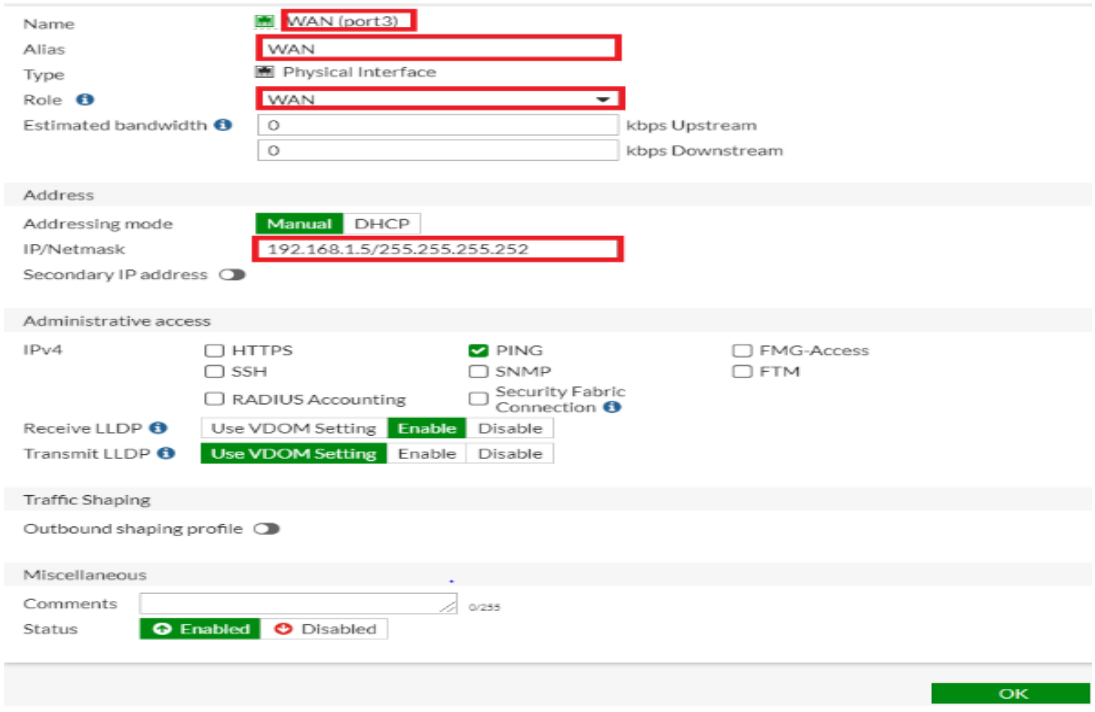

Figure 85:Configuration du port 3 de FG-B.

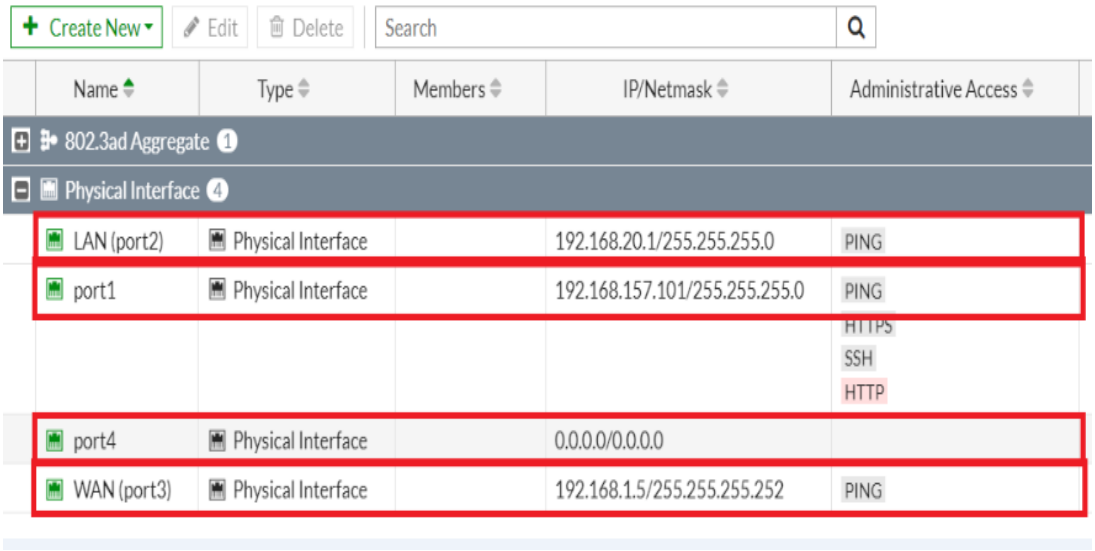

Figure 86:Liste des ports configurés et leurs adresses.

- Ajoutez une route statique, en cliquant sur Network puis sur Static Routes. Insérez la passerelle (192.168.1.6) et cliquez sur ok.

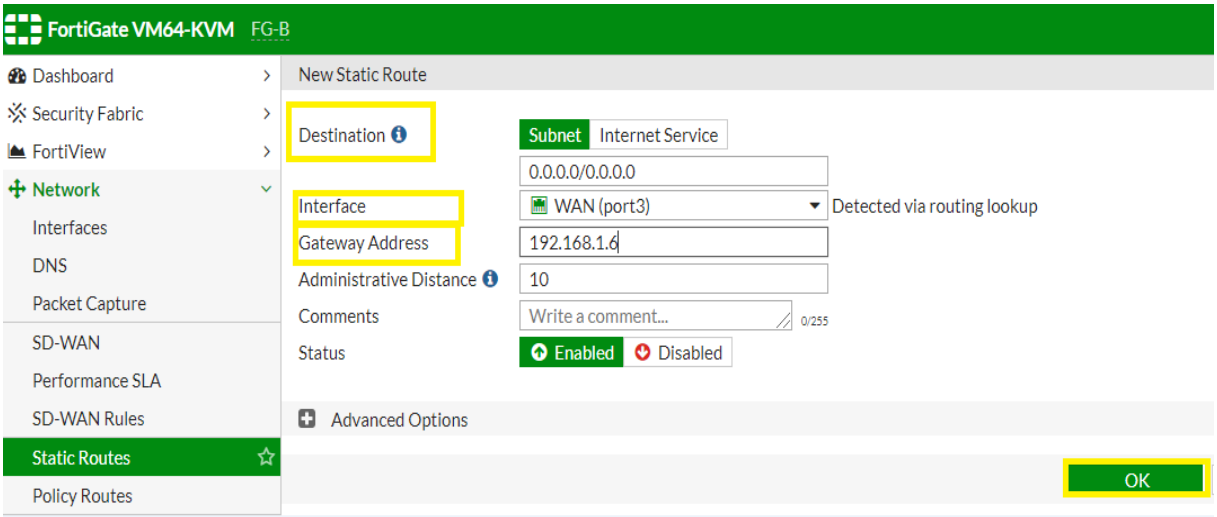

Figure 87:Configuration du la route statique.

IV.5.1.5 Configuration de VPN site a site entre SITEA et SITEB :

- Schéma VPN :

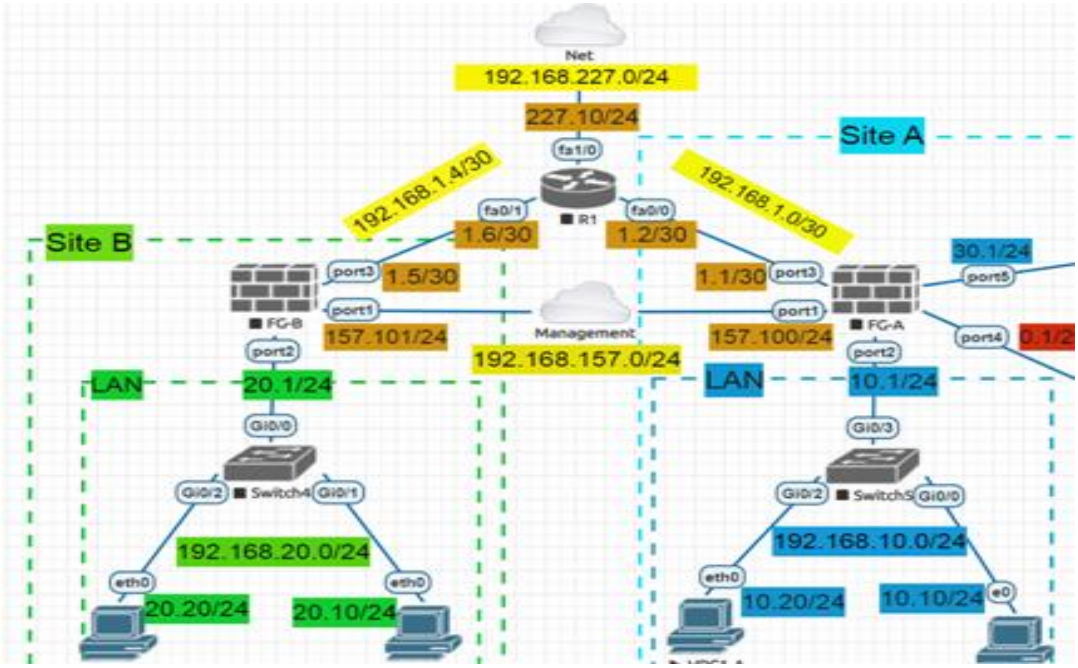

Figure 88:Schéma du VPN site A to site B.

- **Vpn site a site entre SITEA et SITEB :**

- Sur le fortigate dans la section VPN cliquez sur IPsec Wizard.

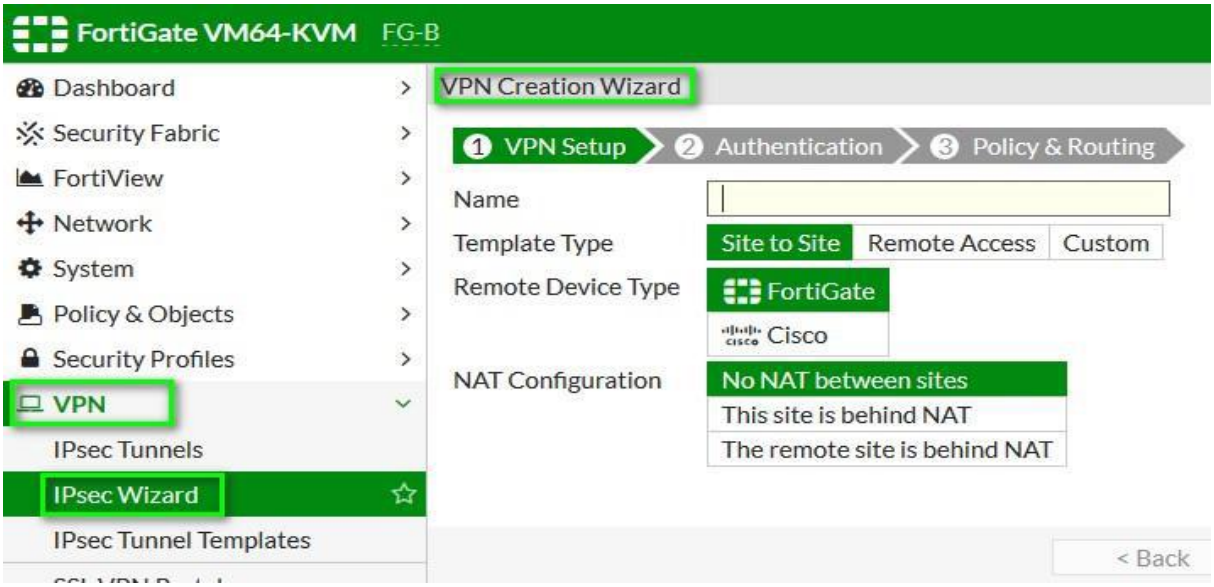

Figure 89:Création VPN site-To-site

VPN SITE A :

- 1er étape : attribuez un nom au VPN puis cliquez sur **Next**.

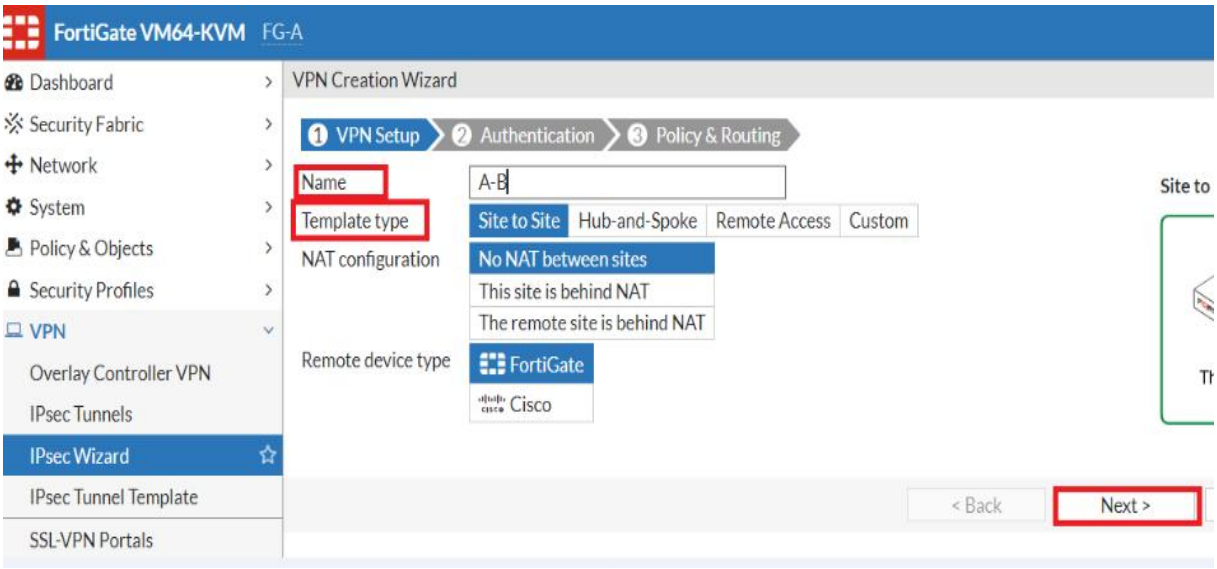

Figure 90:Première étape de la configuration VPN site A- To- site B.

- 2eme : insérez l'adresse du fortigate distant (FG-A) et attribuez une clé pré-partagé.

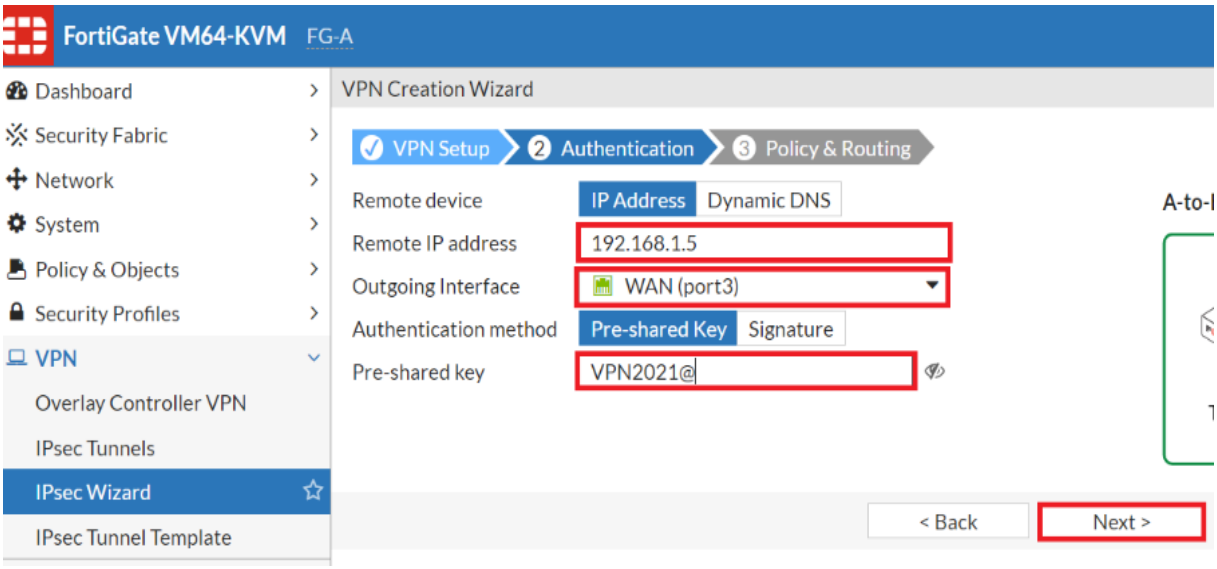

Figure 91: Deuxième étape de la configuration VPN site A- To- site B.

- 3eme étape : introduisez l'interface LAN du FG-A puis l'adresse locale du FG-B et cliquez sur **Create**.

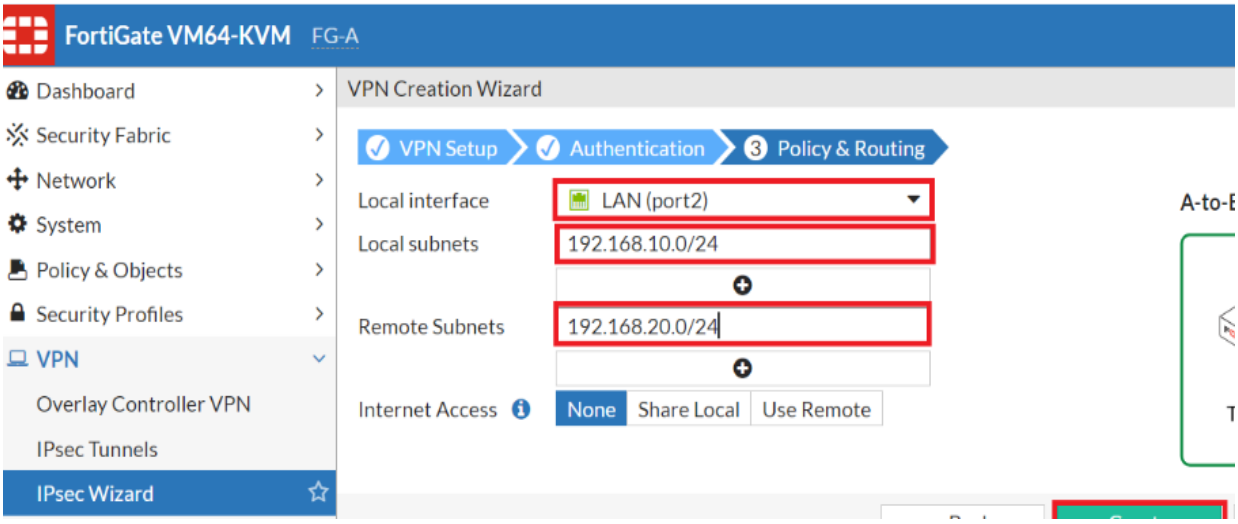

Figure 92:Dernière étape de la configuration VPN site A- To- site B.

- Le VPN est créé avec les règles de sécurités et les routes statiques.

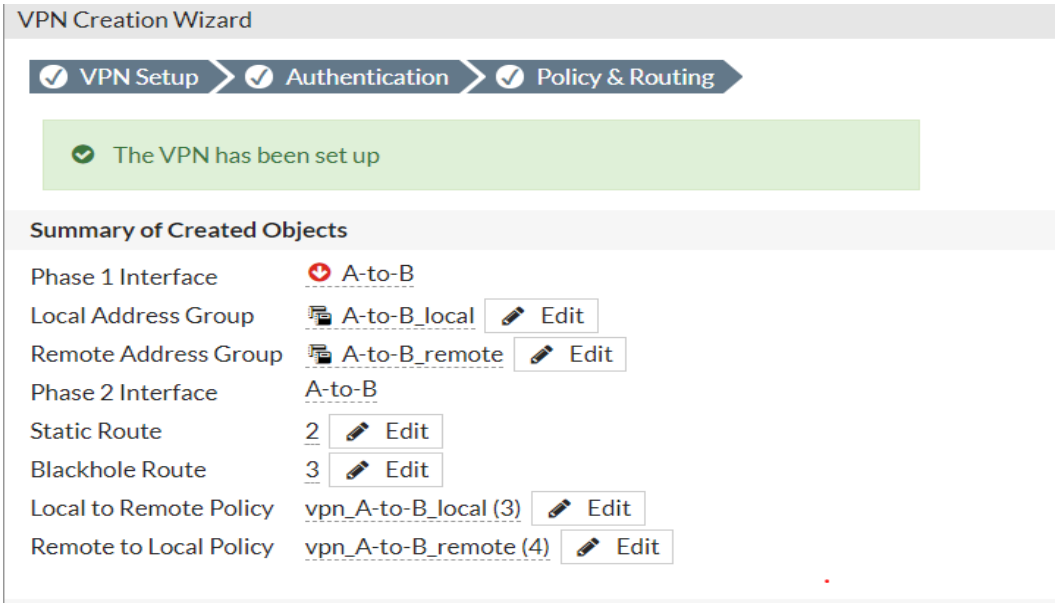

Figure 93: Les résultats de création VPN site A-To-site B.

VPN SITE B :

- 1er étape : attribuez un nom au VPN puis cliquez sur **Next**.

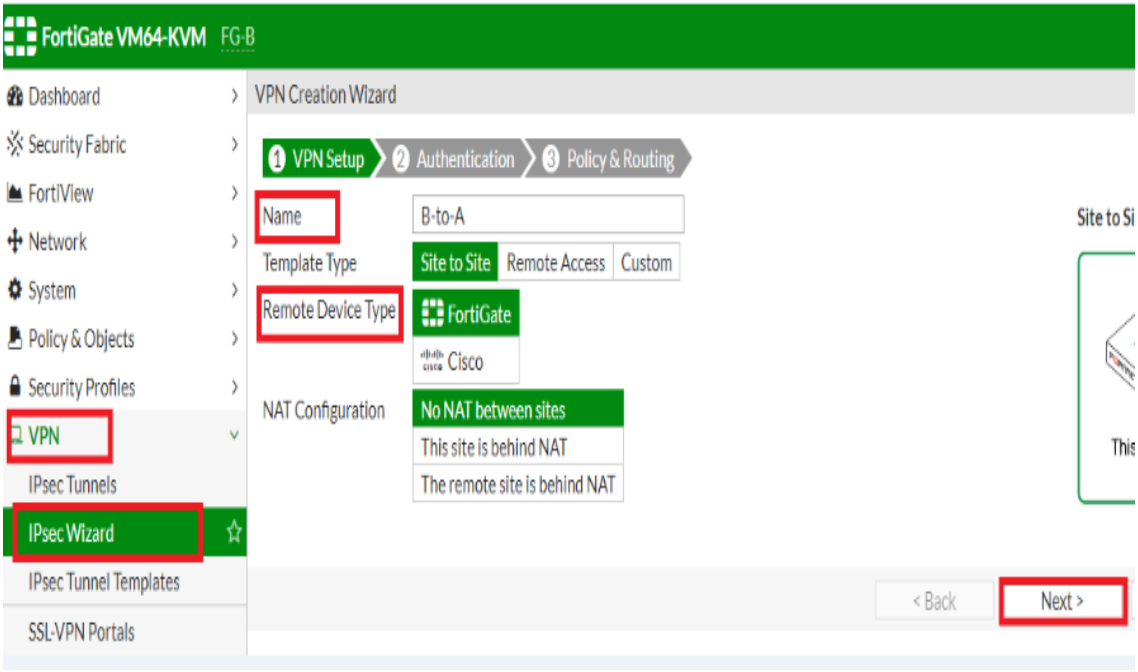

Figure 94:Première étape de la configuration VPN site B- To- site A.

- 2eme étape: insérez l'adresse du fortigate distant (FG-B) et attribuez une clé pré-partagé.

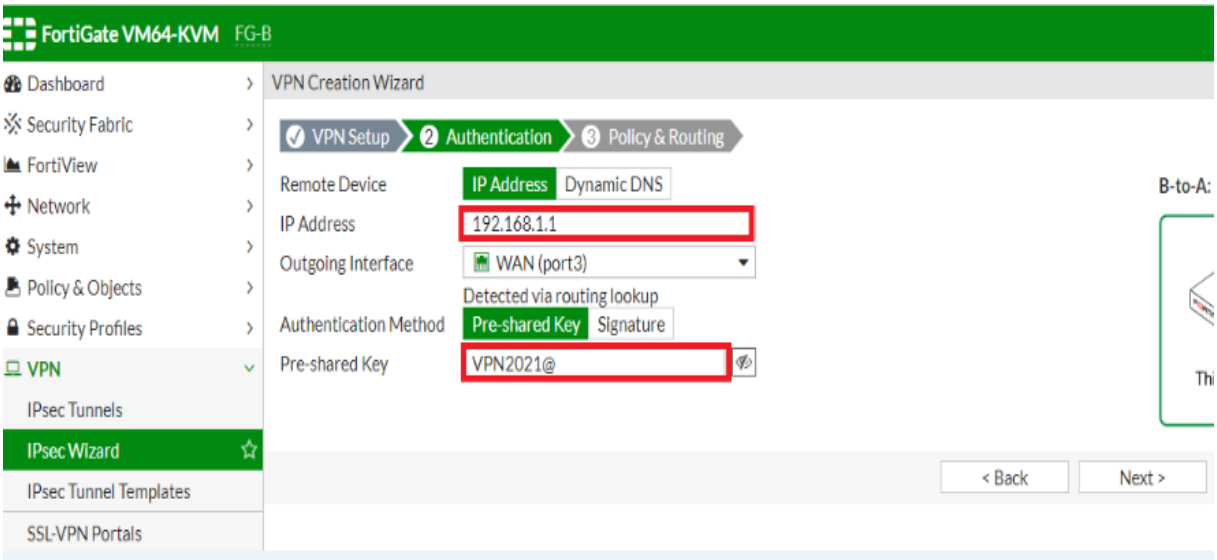

Figure 95: Deuxième étape de la configuration VPN site B- To- site A.

- 3eme étape : introduisez l'interface LAN du FG-A puis l'adresse locale du FG-B et cliquez sur **Create.**

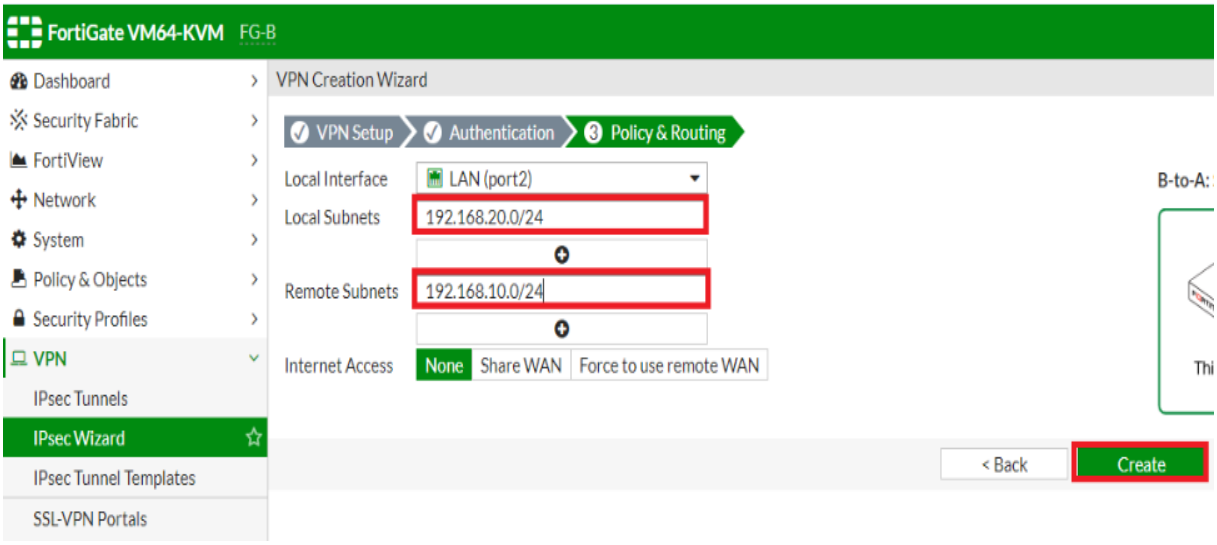

Figure 96:Dernière étape de la configuration VPN site B- To- site A.

- Le VPN est créé avec les règles de sécurités et les routes statiques.

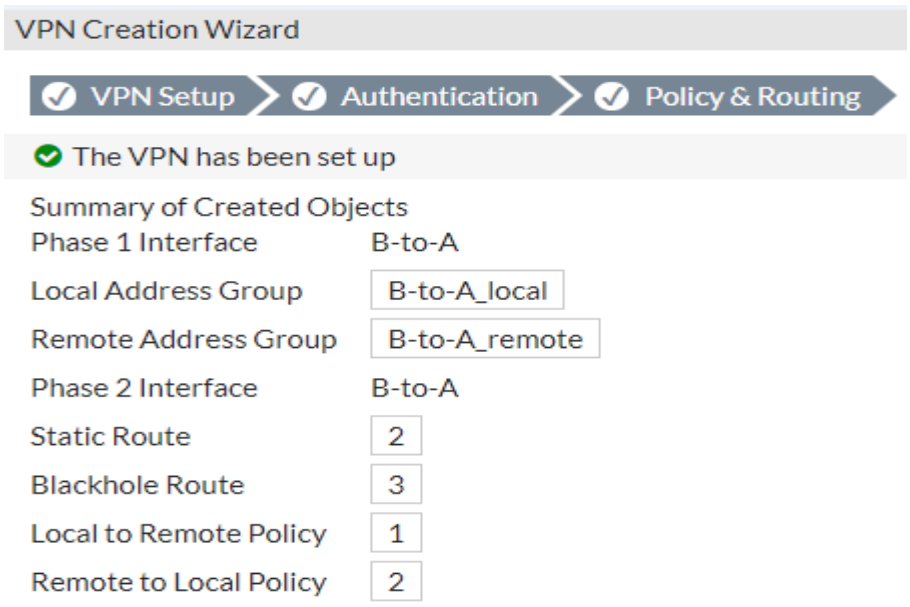

Figure 97: Les résultats de création VPN site B-To-site A.

➢ **Teste du VPN :**

- Ping du VPC2-B vers VPC1-A

```
VPCS> ping 192.168.10.20

84 bytes from 192.168.10.20 icmp_seq=1 ttl=62 time=20.568 ms
84 bytes from 192.168.10.20 icmp_seq=2 ttl=62 time=23.228 ms
84 bytes from 192.168.10.20 icmp_seq=3 ttl=62 time=24.082 ms
84 bytes from 192.168.10.20 icmp_seq=4 ttl=62 time=18.939 ms
84 bytes from 192.168.10.20 icmp_seq=5 ttl=62 time=21.172 ms
```

Figure 98: Teste du VPN site B-To-site A.

- Ping du VPC1-A vers VPC2-B

```
VPCS> ping 192.168.20.10

84 bytes from 192.168.20.10 icmp_seq=1 ttl=62 time=43.966 ms
84 bytes from 192.168.20.10 icmp_seq=2 ttl=62 time=22.117 ms
84 bytes from 192.168.20.10 icmp_seq=3 ttl=62 time=23.514 ms
84 bytes from 192.168.20.10 icmp_seq=4 ttl=62 time=21.130 ms
84 bytes from 192.168.20.10 icmp_seq=5 ttl=62 time=20.702 ms
```

Figure 99:Teste du VPN site A-To-site B.

- Capture du trafic VPN :

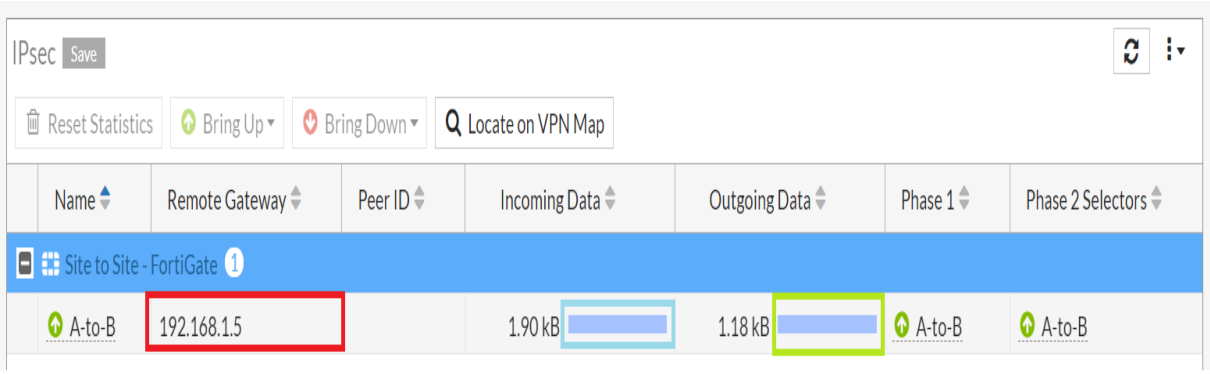

Figure 100:Trafic VPN.

- D'après les pings précédents on a trouvé que le trafic est bien passé à travers le tunnel VPN (site to site).

IV.6 Conclusion

Pour conclure ce chapitre, on peut dire que cette partie nous a permis d'exploiter au maximum de connaissances théoriques et pratiques pour mettre en place la passerelle internet sécurisée. Au début, nous avons cite les étapes nécessaires utilise lors de notre processus. Et tout au long de ce chapitre, nous avons donné une explication à chaque fonctionnalité. Pour finir, le travail qu'on a entrepris dans ce chapitre nous a acquiert la compréhension de l'environnement de la sécurité du système d'information.

Conclusion générale

Le travail que nous avons accompli a pour objectif la proposition d'une conception d'une passerelle internet sécurisée pour la filiale d'ATM Mobilis. Ce projet nous a permis de mettre en pratique les connaissances acquises durant le cycle de notre formation, de se familiariser avec un environnement dynamique et d'avoir une idée plus profonde sur la sécurité des réseaux. Dans ce mémoire, donc nous avons présenté quelques généralités sur la sécurité des systèmes d'information ainsi que les concepts principaux pour avoir une sécurité robuste dont on cite les menaces les plus courantes qui subissent le réseau informatique lors des échanges et de transfert des données confidentielles sur internet.

Dans cette nouvelle architecture, nous avons proposé de déployer le pare-feu « fortigate » qui contient de vastes fonctionnalités. Pour atteindre une sécurité vigoureuse, on a configuré le filtrage du trafic du réseau LAN, ainsi que la création d'un tunnel VPN IPSec pour crypter les échanges.

La réalisation de ce projet a été bénéfique car elle nous a permis d'acquérir de nouvelles connaissances qui seront utiles pour nous à l'avenir.

Le problème majeur que nous avons en contré étant la durée de vie du système des firewalls, en effet ce sont des versions d'essaies et elles se désactivent tous les 3 jours il faut donc être vigilant et effectuer des sauvegardes régulièrement afin de pouvoir les récupérer sur un nouveau firewall.

Enfin, nous pouvons dire que ce projet nous a permis de renforcer nos connaissances théoriques et pratiques déjà acquises et également d'en développer d'autres connaissances nouvelles dans un domaine très exploré ces dernières années .comme perspectives on propose :

- Déployer un serveur WEB pour une haute disponibilité en cas de rupture du lien avec le réseau public et un serveur MAIL pour la gestion de la messagerie local.
- la création d'un tunnel VPN IPSec site à poste pour crypter les échanges.

Bibliographies

[1] : GUIDE ANSSI, « *Recommandations relatives à l'interconnexion d'un système d'information à internet* », Paris, le 18/06/2019.

[2] : BOUCHERBA Khadidja, ZIANE Saloua, « *Mise en place d'un pare-feu d'entreprise open source PfSense* », thèse de master, UAMB, 2015.

[3] : RAPHAEL Yende, « *Support de cours de sécurité informatique et crypto* », HAL, 25/12/ 2018.

[4] : BELALIA Mohamed cherif, MAACHE Khaled, « *Etude et conception d'un firewall*», thèse de master, USDB, 2010/2011.

[5] : BENDAHMANE Ahmed, « *Installation et configuration d'un firewall* », Mémoire de fin d'études, UABBT, 2010/2011.

[17] : LOUIS Salvail, Cours 10, Mécanismes de sécurité des systèmes.pdf, 2014

[18] : SECURITE DU SYSTEME D'INFORMATION (SSI).pdf, 2010-2011.

[19]: NT_IPsec.pdf, Paris, No DAT-NT-003 /ANSSI/SDE/NP, du 03 aout 2015.

[20] : BELMAHBOUL Oussama, Mobilité et Sécurité sur le réseau [universitaire], «*mise en place de solutions VPN* », thème de mémoire master, CUABM ,2018/2019.

[21] : Bendahmane Ahmed, «*Installation et configuration d'un firewall*», thèse de master, UABBT ,2011.

[22] : Les Réseaux Privés Virtuels.pdf

[23] : SLIMANOU Dehia, «*Mise en place d'une solution VPN sur pare-feu Cas d'étude : Entreprise Tchin-Lait(Candia)*», thème de mémoire, UAMB, 2016/2017.

[24] : Belaid, Hamadouche Yacine, «*Etude et sécurisation d'une infrastructure DMZ avec ASA CISCO5510*», thème de Mémoire de master, UMMT, 2015.

[25] : NESNAS Ouerdia, ZIKIOU Nadia, «*Optimisation et réalisation d'un réseau local sécurisé au sein de l'IAP de BOUMERDES*», Mémoire de fin d'études, UMMT, 2008/2009.

[26] : SENA Samy, SKLAB Madjid, «*Installation et configuration d'un VPN pour l'entreprise (Adel Computers)*», Mémoire fin de cycle, UAMB, 2016/2017.

Webography

[6] :[En ligne].Quels sont les différents types de malware ?, https://www.pandasecurity.com/fr/mediacenter/mobile-news/differents-types-de-malware/,(18 décembre 2019), (Consulté le 30 mai 2021)

[7]: [En ligne]. What are malware virus's spyware and cookies and what differentiates them? https:/www.websecurity.digicert.com/fr/ca/security-topics/what-are-malware-viruses-spyware-and-cookies-and-what-differentiates-them,(Consulté le 30 mai2021)

[8] : [En ligne].Cours sur les types d'attaques informatique-Cours et formation gratuit, www.clicours.com,(Consulté le 22mai 2021)

[9] : [En ligne].Pierre-Louis Lussan, Les 10 types de cyberattaques les plus courants, https://blog.netwrix.fr/2018/07/04/les-10-types-de-cyberattaques-les-pluscourants/, netwrix Blog, (Mis à jour le 18septembre2019),(Consulté le 03juin 2021)

[10] : [En ligne].Attaques par injection de commandes SQL, https://www.commentcamarche.net/contents/56-attaques-par-injection-de-commandes-sql, (Consulté le 03 juin 2021)

[11] : [En ligne]. Définition du piratage (hacking) « Les 5 types les plus dangereux », https://softwarelab.org/fr/piratage/, (Consulté le 03 juin 2021)

[12]: [En ligne].Les différents types de hackers et autres pirates du web, https://www.appitel.fr/blog/securite/les-differents-types-de-hackers-et-autres-pirates-du-web,(Consulté le 03 juin 2021)

[13] : [En ligne].WILLIAM Culbert, Les sept étapes d'une cyberattaque réussie, https://www.globalsecuritymag.fr/Les-sept-etapes-d-une-cyberattaque,20180705,79676.html, (Crée le juillet 2018), (Consulté le 03 juin 2021)

[14] :[En ligne].CYBERCRIMINALITE: PROFILS ET MOTIVATION, https://www.cyber cover.fr/cyber-documentation/cyber-criminalite/cybercriminalite-profils-et-motivations, CYBER COVER, PARIS, (Consulté le 27 mai 2021)

[15]:[En ligne].Victor Garretas, Ruiz,http://tecfaetu.unige.ch/perso/maltt/garretv0/impress/technique_attaque_info.html, (Consulté le 27 mai 2021)

[16] :[En ligne].ZELLAGUI Amine, Les attaques réseaux, https://www.slideshare.net/docteuraminedz29/les-attaques-reseaux-par-zellagui-amine, (23 décembre, 2015),(Consulté le 27 mai 2021)

[27]: [En ligne].Available, https://www.brianlinkletter.com/how-to-set-up-the-eve-ng-network-emulator-on-a-linux-system/,(Consulté le 03 juillet 2021)

[28]: [En ligne]. Available, https://www.eve-ng.net/index.php/download/,(Consulté le 03 juillet 2021)

[29]: [En ligne]. Available, https://www.ssh.com/ssh/putty/,(Consulté le 03 juillet 2021)

[30]: [En ligne]. Available, https://findwords.info/term/wireshark,(Consulté le 03 juillet 2021)

[31]: [En ligne]. Available, https://www.uvnc.com/,(Consulté le 03 juillet 2021)

[32]: [En ligne]. Available, https://winscp.net/eng/index.php,(Consulté le 03 juillet 2021)

[33]: [En ligne]. Available, https://ubuntu.com/server/docs/proxy-servers-squid,(Consulté le 03 juillet 2021)

[34]: [En ligne]. Available, https://www.novell.com/documentation/suse91/suselinux-adminguide/html/ch18s03.html,(Consulté le 03 juillet 2021)