

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE MINISTÈRE DE  
L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE  
UNIVERSITÉ ABDERRAHMANE MIRA - BEJAIA  
FACULTÉ DE TECHNOLOGIE  
DÉPARTEMENT D'AUTOMATIQUE, TÉLÉCOMMUNICATIONS ET  
D'ÉLECTRONIQUE



MÉMOIRE DE FIN D'ÉTUDES  
EN VUE D'OBTENTION DU DIPLÔME DE MASTER  
OPTION RÉSEAUX ET TÉLÉCOMMUNICATIONS

---

# Etude et mise en place d'un serveur web sécurisé sous-linux -Général Emballage-

---

*Réalisé par :*  
M. LATBI Mazigh  
Mlle. BOUNEHAR Nadjet

*Encadré par :*  
M. DIBOUNE Abdelhani  
M. DJEBBARI Yacine

Membre de jury :

M. Azni

Mme. Mammeri

Promotion 2022 - 2023

# REMERCIEMENTS

---

En tout premier lieu, nous remercions le bon Dieu tout-puissant de nous avoir donné le courage, la volonté et la patience pour terminer ce travail.

Nous tenons à exprimer notre gratitude envers notre encadreur, M. DIBOUNE Abdel Hani, pour le temps qu'il nous a accordé et pour nous avoir accompagnés tout au long de nos démarches. Nous lui sommes reconnaissants pour les précieux renseignements qu'il nous a transmis, qui nous ont été essentiels pour la réalisation de ce travail.

Nos remerciements vont tout particulièrement à M. DJEBBARI.Y pour son aide précieuse et ses conseils avisés. Sa contribution a grandement enrichi notre projet.

Nous souhaitons également exprimer notre reconnaissance envers le personnel de « Generale emballage » pour avoir accepté de nous accueillir au sein de leur organisme et de nous permettre d'effectuer notre stage. Leur aimable accueil et leur disponibilité ont été très appréciés.

Nous tenons à remercier chaleureusement les membres du jury qui ont accepté de juger notre travail. Leur évaluation et leurs commentaires constructifs ont été d'une grande valeur pour nous.

Enfin, notre gratitude s'adresse également à tous ceux qui, de près ou de loin, nous ont soutenus pour achever ce modeste travail. Votre soutien a été précieux et nous en sommes profondément reconnaissants.

Merci à tous.

# DÉDICACE

---

À ma chère famille, à mes merveilleux amis et à ma binôme,

Aujourd'hui, je souhaite vous dédier ce travail avec une profonde gratitude et une immense joie. Votre soutien inconditionnel, votre présence précieuse et votre collaboration ont été les piliers qui ont soutenu ma réussite tout au long de ce parcours.

À ma famille aimante, vous avez été ma source de force et de motivation. Votre amour, votre confiance et votre soutien indéfectible ont nourri mes aspirations et m'ont permis de croire en moi-même. Votre présence à mes côtés, dans les moments de doute comme dans les moments de victoire, a été un cadeau inestimable.

À mes chers amis, vous êtes ma seconde famille. Vos encouragements constants, vos sourires réconfortants et votre amitié sincère ont illuminé mon chemin. Nos moments de partage, nos rires et nos soutiens mutuels ont rendu cette aventure plus belle et m'ont rappelé à quel point je suis chanceux de vous avoir dans ma vie.

À ma binôme, nous avons formé une équipe imbattable. Ta collaboration, ton dévouement et ton esprit de travail ont été essentiels pour la réussite de ce projet. Notre complicité et notre capacité à surmonter les défis ensemble ont été la clé de notre succès. Je suis reconnaissant d'avoir eu la chance de partager cette expérience avec toi.

À vous tous, ma famille, mes amis et ma binôme, je dédie ce travail. Votre amour, votre soutien et votre présence ont fait de cette aventure une expérience inoubliable. Je suis profondément reconnaissant de vous avoir dans ma vie, car vous êtes mes plus grands trésors.

Avec tout mon amour et ma gratitude,

**LATBI Mazigh**

# DÉDICACE

---

Je dédie ce présent mémoire à des personnes exceptionnelles qui ont joué un rôle essentiel dans mon parcours et ma réussite.

Tout d'abord, à ma mère, qui s'est toujours dévouée et sacrifiée pour moi. Tu as été mon pilier, ma source d'inspiration et ma plus grande supportrice. Tu as fait tout ce qui était en ton pouvoir pour m'aider à réussir, et je suis profondément reconnaissante pour tout l'amour, l'encouragement et le soutien inconditionnel que tu m'as apporté. Ce mémoire est le fruit de notre collaboration et de ton dévouement constant.

Je souhaite également adresser mes remerciements à toute ma famille. À mon père, pour sa présence et son soutien constant tout au long de mon parcours. À ma chère Kenza, mon frère Salah, ma grand-mère et mes tantes, qui m'ont prodigué des conseils avisés et ont toujours été là pour m'encourager. Votre confiance en moi a été une source de motivation sans faille, et je suis reconnaissante de vous avoir à mes côtés.

Je tiens également à exprimer ma gratitude à mon ami et binôme Mazigh. Tu as été mon compagnon de route tout au long de cette aventure, et ta présence a été d'une importance capitale. Tu m'as soutenue dans les moments de doute et de faiblesse, et ensemble, nous avons surmonté les obstacles. Notre collaboration a été une source d'inspiration et de croissance personnelle, et je suis convaincue que le meilleur reste à venir pour nous.

Enfin, je souhaite remercier tous ceux qui ont contribué de manière indirecte à ma réussite, que ce soit par leurs écrits, leurs recherches ou leurs travaux antérieurs. Vos contributions ont été une source d'inspiration et ont élargi mes horizons intellectuels.

À vous tous, je dédie ce mémoire, en espérant que cela soit un témoignage de ma reconnaissance éternelle et de mon affection sincère.

**BOUNEHAR Nadjat**

# Table des matières

Introduction générale . . . . .	12
<b>1 Notions de base sur la sécurité des systèmes d'information</b>	<b>14</b>
1.1 Introduction . . . . .	14
1.2 Généralité sur les réseaux TCP/IP . . . . .	15
1.2.1 Définition d'un réseau . . . . .	15
1.2.2 Classification des réseaux selon les critères d'ouverture . . . . .	15
1.2.3 La pile protocolaire TCP/IP . . . . .	17
1.3 Généralité sur la sécurité des systèmes d'information . . . . .	18
1.3.1 Définition de la sécurité informatique . . . . .	18
1.3.2 Les Critères de la sécurité informatique . . . . .	18
1.3.3 Les attaques et vulnérabilités . . . . .	20
1.3.4 Les protocoles de sécurité . . . . .	22
1.3.5 Les mécanismes de défense . . . . .	24
1.4 Conclusion . . . . .	25
<b>2 Généralités sur la sécurité d'un serveur web</b>	<b>26</b>
2.1 Introduction . . . . .	26
2.2 Le fonctionnement client/serveur du Web . . . . .	26
2.2.1 Client web . . . . .	26
2.2.2 Serveur web . . . . .	27
2.3 Présentation de l'architecture client /serveur . . . . .	27
2.4 Notion sur HTTP Secure(HTTPS) . . . . .	28
2.4.1 Définition de HTTPS . . . . .	28
2.4.2 Le principe de HTTPS . . . . .	28
2.5 Le protocole SSL/TLS . . . . .	30
2.5.1 Définition . . . . .	30
2.5.2 Historique . . . . .	30
2.5.3 Fonctionnement . . . . .	30

2.5.4	Services offerts par SSL/TLS . . . . .	31
2.6	Système de sécurisation utilisé par SSL/TLS . . . . .	32
2.6.1	Système de chiffrement symétrique . . . . .	32
2.6.2	Système de chiffrement asymétrique . . . . .	33
2.6.3	Système de signature cryptographique . . . . .	33
2.7	Les certificats SSL . . . . .	33
2.7.1	Fonctionnement d'un certificat SSL . . . . .	34
2.7.2	Fonctionnement d'un protocole sécurisé . . . . .	34
2.7.3	Authentification du serveur . . . . .	35
2.7.4	Authentification du client . . . . .	35
2.7.5	Chiffrement des données . . . . .	35
2.7.6	Les sous-protocoles SSL/TLS . . . . .	35
2.8	Conclusion . . . . .	40

### **3 Présentation de l'organisme d'accueil, problématiques et solutions** **41**

3.1	Introduction . . . . .	41
3.2	Présentation générale de General Emballage . . . . .	41
3.3	Organigramme de l'entreprise . . . . .	42
3.4	Systèmes informatique dans Général Emballage . . . . .	42
3.5	L'étude de l'existant . . . . .	42
3.6	Présentation de l'infrastructure réseau de département informatique .	43
3.7	L'architecture du réseau . . . . .	43
3.8	Matériels utilisés dans l'architecture . . . . .	44
3.8.1	PC ou ordinateur . . . . .	44
3.8.2	Commutateur (switch) . . . . .	44
3.8.3	Un routeur . . . . .	45
3.8.4	Un serveur informatique . . . . .	46
3.8.5	Un pare-feu (firewall) . . . . .	46
3.9	Problématique . . . . .	46
3.10	Solution . . . . .	47
3.10.1	DMZ (Zone démilitarisée) . . . . .	47
3.10.2	Pare-feu . . . . .	47
3.10.3	Certificat SSL . . . . .	48
3.10.4	Création des VLANs . . . . .	49
3.11	Conclusion . . . . .	50

<b>4</b>	<b>Réalisation</b>	<b>51</b>
4.1	Introduction . . . . .	51
4.2	Environnement de travail (présentation des outils de travail) . . . . .	51
4.2.1	GNS3 . . . . .	51
4.2.2	VMware Workstation . . . . .	52
4.2.3	Les machines virtuelles . . . . .	52
4.3	Méthodologie . . . . .	53
4.3.1	Gestions des Vlans . . . . .	53
4.3.2	Configuration de Switch DMZ . . . . .	58
4.3.3	La Configuration de PfSense . . . . .	59
4.3.4	La configuration du Serveur WEB . . . . .	64
4.3.5	Etape 7 : Test DHCP et Vérification de la connectivité . . . . .	73
4.4	Conclusion . . . . .	75
	Conclusion générale . . . . .	76
<b>A</b>	<b>Installation de VMware</b>	<b>77</b>
A.1	Les étapes d'installations VMware Workstation . . . . .	77
A.1.1	Téléchargement du logiciel . . . . .	77
A.1.2	Configuration des options d'installation . . . . .	77
<b>B</b>	<b>Installation de GNS3</b>	<b>82</b>
B.1	Les étapes d'Installation de GNS3 sous Windows . . . . .	82
<b>C</b>	<b>Configuration de la partie client extérieur</b>	<b>84</b>
C.1	configuration des routeurs . . . . .	84
<b>D</b>	<b>Installation de linux debian</b>	<b>86</b>
D.1	Les étapes d'Installation de Debian 11 sur VMware . . . . .	86
<b>E</b>	<b>Installation de PfSense</b>	<b>91</b>
E.1	Les étapes Installations firewall . . . . .	91

# Table des figures

1.1	Représentation d'une partie d'un réseau internet en 2005 [3]. . . . .	15
1.2	Les critères de la sécurité . . . . .	19
1.3	Représentation schématique d'une zone démilitarisée avec deux pare-feu [20]. . . . .	24
2.1	Communication client-serveur web en HTTP(S) [31]. . . . .	27
2.2	Différence entre HTTP et HTTPS. . . . .	29
2.3	Organisation du protocole ssl. [25]. . . . .	31
2.4	Schéma d'établissement de connexion sécurisée . [27]. . . . .	33
2.5	1. Fonctionnement d'un certificat SSL/TLS. [36]. . . . .	34
2.6	fonctionnement de handshake. [30]. . . . .	36
2.7	structure d'un certificat X.509. [37]. . . . .	37
2.8	SSL record. [35]. . . . .	39
3.1	logo de General Emballage . . . . .	41
3.2	Organigramme de l'unité d'Akbou . . . . .	42
3.3	Architecture réseau proposé de Général Emballage . . . . .	44
3.4	Commutateur (switch) . . . . .	45
3.5	Routeur . . . . .	46
4.1	GNS3 . . . . .	51
4.2	L'interface graphique de VMware Workstation pro 17 . . . . .	52
4.3	Debian . . . . .	53
4.4	Affichage des interfaces qui sont reliées . . . . .	54
4.5	Verification des interfaces . . . . .	54
4.6	Affichage des vlans . . . . .	56
4.7	Affichage des VLANs autorisés à traverser . . . . .	57
4.8	Affectation des ports pour les Vlans en mode accès . . . . .	58
4.9	Accées en mode interface grafique . . . . .	59
4.10	Page d'accueil de PfSense . . . . .	60



4.11	interface Assignments . . . . .	60
4.12	les vlans dans PfSense . . . . .	61
4.13	Le DHCP dans les vlans . . . . .	62
4.14	La redirection . . . . .	63
4.15	Affichage des interfaces . . . . .	63
4.16	Configuration de serveur . . . . .	64
4.17	vérification de l'activation de apache2 . . . . .	66
4.18	Création d'un nom de Domain . . . . .	66
4.19	Acceder à la page de apache avec generalemballage.org . . . . .	67
4.20	Test de l'ouverture de site . . . . .	68
4.21	vérification de l'installation de ssl . . . . .	69
4.22	Affichage du certificat . . . . .	70
4.23	test de l'ouverture avec https . . . . .	71
4.24	Test de l'ouverture avec https en acceptons les risques . . . . .	72
4.25	Assignment des adresses IPs . . . . .	73
4.26	test de connectivité entre le LAN et internet . . . . .	74
4.27	Tester la connectivité inter-VLAN . . . . .	74
4.28	Test de connectivité entre le LAN et le serveur . . . . .	75
E.1	Ecran de démarrage de l'installation de firewall. . . . .	91
E.2	Début de l'installation de firewall . . . . .	91
E.3	Fin de l'installation de firewall. . . . .	92
E.4	Menu de configuration de firewall. . . . .	92

# Liste des tableaux

1.1	Comparaison des caractéristiques d'Internet, de l'Intranet et de l'Extranet [7]. . . . .	17
2.1	Différence entre HTTP et HTTPS . . . . .	28
4.1	Les interfaces en mode trunk . . . . .	53
4.2	Tableau des Vlans . . . . .	55
4.3	Les interfaces en mode accès . . . . .	57
4.4	Mode des interfaces de Sw-DMZ . . . . .	58
C.1	Adressage des routeurs . . . . .	84

## Liste des abréviations

**AES** : Advanced Encryption Standard  
**CA** : Certification Authority  
**CERN** : Conseil européen pour la recherche nucléaire  
**DDoS** : Distributed Denial of Service  
**DES** : Data Encryption Standard  
**DHCP** : Dynamic Host Configuration Protocol  
**DNS** : Domain Name System  
**DMZ** : demilitarized zone  
**DSI** : Direction des Systèmes d'Information  
**FTP** : File Transfer Protocol  
**GNS3** : Graphical Network Simulator  
**HTML** : HyperText Markup Language  
**HTTP** : HyperText Transfert Protocol  
**HTTPS** : Hyper Text Transfer Protocol Secure  
**IETF** : Internet Engineering Task Force  
**IP** : Internet Protocol  
**IPsec** : Internet Protocol Security  
**LAN** : Local Area Network  
**MAC** : Media Access Control  
**PvLANs** : Private VLANs  
**POP** : Post Office Protocol  
**PGP** : Pretty Good Privacy  
**RAM** : Random Access Memory  
**RC4** : Rivest Cipher  
**SET** : Secure Electronic Transaction  
**S/MIME** : Secure/Multipurpose Internal Mail Extensions  
**SMTP** : Simple Mail Transfer Protocol  
**SSH** : Secure Shell  
**SSL** : Secure Sockets Layer  
**TELNET** : Teletype Network Protocol  
**TCP** : Transmission Control Protocol  
**TLS** : Transport Layer Security  
**UDP** : User Datagramme Protocol  
**URL** : Uniform Resource Locator

**VLAN** : Virtual Local Area Network

**VTP** : VLAN Trunking Protocol

**VPN** : Virtual Private Network

**WAN** : Wide Area Network

# Introduction générale

La sécurité des systèmes d'information est un enjeu majeur pour les entreprises et les organisations dans un monde de plus en plus connecté. La protection des données et la prévention des attaques informatiques sont devenues des priorités absolues. Dans ce contexte, la sécurisation des serveurs web joue un rôle crucial, car ces serveurs constituent souvent la porte d'entrée vers les systèmes d'information et contiennent des informations sensibles.

Ce mémoire porte sur le sujet de la sécurité des systèmes d'information, en mettant spécifiquement l'accent sur la sécurisation des serveurs web sous Linux. Nous nous intéresserons à l'étude et à la mise en place d'un serveur web sécurisé, en examinant les éléments clés de son architecture ainsi que les mesures de sécurité à prendre pour prévenir les attaques et garantir la confidentialité, l'intégrité et la disponibilité des données.

Dans la première chapitre, nous abordons les notions fondamentales de la sécurité des systèmes d'information. Nous commençons par une introduction générale sur les réseaux TCP/IP, en définissant ce qu'est un réseau et en présentant les critères d'ouverture des réseaux. Ensuite, nous examinons la pile protocolaire TCP/IP et les principaux aspects de la sécurité informatique tels que la confidentialité, l'intégrité, l'authentification, la non-répudiation, la disponibilité et la traçabilité. Nous abordons également les attaques et vulnérabilités courantes ainsi que les protocoles et mécanismes de sécurité utilisés pour se défendre contre ces menaces.

Dans la deuxième chapitre, nous nous concentrons sur la sécurité d'un serveur web. Nous commençons par une introduction sur le fonctionnement client/serveur du web, en présentant les rôles du client web et du serveur web. Ensuite, nous examinons l'architecture client/serveur du web et nous nous concentrons sur le protocole HTTP Secure (HTTPS) qui permet de sécuriser les échanges entre le client et le serveur. Nous explorons en détail le protocole SSL/TLS qui sous-tend HTTPS, en expliquant son fonctionnement, les services qu'il offre et les systèmes de sécurisation qu'il utilise, tels que le chiffrement symétrique, le chiffrement asymétrique et la

signature cryptographique. Nous abordons également les certificats SSL qui jouent un rôle crucial dans l'authentification du serveur et du client, ainsi que dans le chiffrement des données.

Dans la troisième chapitre, nous présentons l'organisme d'accueil de notre étude, General Emballage, en mettant en évidence les problématiques liées à la sécurité de son système informatique. Nous décrivons l'architecture réseau de son département informatique, en détaillant les matériels utilisés tels que les PC, les commutateurs, les routeurs, les serveurs informatiques et les pare-feu. Nous exposons ensuite la problématique spécifique rencontrée par General Emballage et nous proposons des solutions telles que l'utilisation de la DMZ (Zone démilitarisée), des pare-feu, des certificats SSL et des VLANs.

Dans la quatrième chapitre, nous décrivons la réalisation pratique de notre étude. Nous présentons l'environnement de travail que nous avons utilisé, notamment les outils tels que GNS3 et VMware Workstation, ainsi que les machines virtuelles que nous avons configurées. Nous détaillons la méthodologie suivie pour mettre en place la solution proposée, en expliquant les étapes de configuration des interfaces, du protocole Trunking VLAN (VTP), des VLANs, des routeurs, de la DMZ, du pare-feu, du serveur web, du DHCP et de la vérification de la connectivité.

Enfin, nous terminerons notre travail par une conclusion générale.

# Chapitre 1

## Notions de base sur la sécurité des systèmes d'information

### 1.1 Introduction

De nos jours, les systèmes informatiques et les réseaux sont largement utilisés dans de nombreux domaines de notre vie quotidienne, que ce soit pour la communication, le travail, les loisirs ou les transactions financières. Cette utilisation croissante des technologies de l'information a rendu la sécurité des systèmes d'information d'une importance vitale. En effet, la protection des données et des informations sensibles est essentielle pour prévenir les attaques malveillantes, les pertes financières et les violations de la vie privée.

Ainsi, ce premier chapitre sera divisé en deux grandes parties. Dans la première, nous aborderons une généralité sur les réseaux TCP/IP, qui sont le fondement des communications sur Internet. La deuxième partie de ce chapitre aura pour objectif de présenter les notions fondamentales de la sécurité informatique, notamment en abordant sa définition, ses objectifs, ainsi que les problématiques liées aux attaques informatiques et les types d'attaques courantes, ainsi que les protocoles de sécurité et les mécanismes permettant d'améliorer la sécurité. Enfin, nous conclurons en soulignant l'importance de la sécurité des systèmes d'information dans notre vie quotidienne.

## 1.2 Généralité sur les réseaux TCP/IP

### 1.2.1 Définition d'un réseau

Un réseau est une infrastructure de communication qui connecte plusieurs appareils ou objets entre eux. Il permet l'échange et la transmission de données selon des protocoles et des règles préétablies pour assurer un transfert efficace et sécurisé des informations[1].

### 1.2.2 Classification des réseaux selon les critères d'ouverture

Pour permettre aux ordinateurs de communiquer entre eux, un réseau informatique est indispensable. En effet, il permet d'échanger des informations entre deux ou plusieurs machines. Il existe différents types de réseaux informatiques tels que l'internet, l'intranet et l'extranet dont chacun a ses applications et ses rôles.

#### 1.2.2.1 Les réseaux internet

**1.2.2.1.1 Qu'est-ce qu'Internet** À l'origine, Internet était un système qui permettait aux chercheurs de communiquer entre eux et d'accéder à distance aux ordinateurs mis à leur disposition. C'est devenu peu à peu un gigantesque regroupement mondial de réseaux d'ordinateurs reliés entre eux : réseaux d'universités, d'entreprises, d'organisations gouvernementales, de particuliers, de sociétés qui proposent des accès à Internet, de sociétés qui hébergent des sites Web, etc[2].

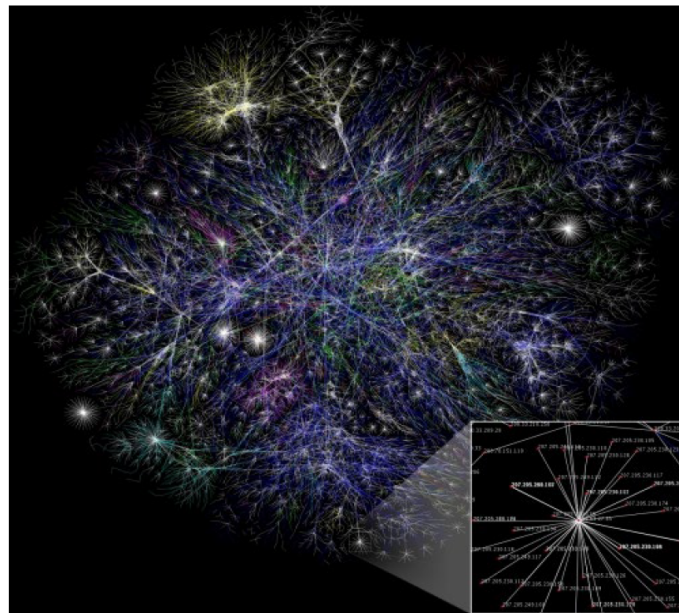


FIGURE 1.1 – Représentation d'une partie d'un réseau internet en 2005 [3].



### 1.2.2.1.2 Application d'internet

- Télécharger des programmes et des fichiers.
- E-Mail.
- Conférences audios et vidéos.
- Commerce électronique .
- Partage de fichiers.
- Navigation d'informations.
- Rechercher les adresses Web pour y accéder via un moteur de recherche.
- Discussion en ligne et bien plus encore, etc.[4].

### 1.2.2.2 Les réseaux intranet

**1.2.2.2.1 Définition** L'intranet est un réseau local réservé à une entreprise et utilisé en interne. Il fournit un espace aux employés pour partager des informations et des documents confidentiels tels que des documents internes sur leur rémunération, des informations sur leur situation salariale (par exemple les demandes de congé), des notes de frais et des informations relatives au comité d'entreprise. L'intranet permet également l'échange de documents en interne et l'accès à des applications métiers pour soutenir la vie de l'entreprise.

**1.2.2.2.2 Authentification et sécurisation de l'intranet** Il est primordial que l'accès à l'intranet soit sécurisé. Bien que les documents et informations échangés soient destinés exclusivement à une utilisation interne, la DSI (direction des systèmes d'information) doit veiller à donner des accès uniquement aux personnes autorisées.

L'intranet est considéré comme un site internet normal, il nécessite donc un serveur web, les mêmes langages et protocoles (dont HTML et Javascript). Une vigilance accrue est nécessaire pour éviter toutes tentatives d'intrusion sur cet espace interne. La connexion de l'utilisateur en interne de l'entreprise doit être sécurisée par une authentification avec un identifiant et un mot de passe[5].

### 1.2.2.3 Les réseaux extranet

**1.2.2.3.1 Définition** L'extranet est une extension du système d'information de l'entreprise permettant aux partenaires tels que les clients, les fournisseurs et les employés situés en dehors du réseau de bénéficier d'un accès privilégié à certaines ressources informatiques de l'entreprise. Il peut s'agir soit d'une authentification simple (authentification par nom d'utilisateur et mot de passe) ou d'une authentification forte (authentification à l'aide d'un certificat). Il est important de noter que contrairement à l'intranet ou au site internet, l'extranet est un système distinct et autonome qui offre des fonctionnalités supplémentaires pour les partenaires de l'entreprise[6].

### 1.2.2.3.2 Avantage d'extranet

- Amélioration de la qualité des services offerts par l'entreprise.
- Réduction des coûts de déplacement.
- Réduction des coûts administratifs et autres coûts indirects

- Réduction de la paperasse.
- Livraison d'informations précises en temps voulu.
- Amélioration du service client.
- Meilleure communication.
- Amélioration globale de l'efficacité de l'entreprise[4].

#### 1.2.2.4 Différence entre internet intranet et extranet

Tableau 1.1 résume la différence entre les trois réseaux :

CRITÈRE	INTERNET	INTRANET	EXTRANET
TYPE DE RE-SEAU	Ouvert	Interne	Privé
ACCES	Public	Privé	Contrôlé
UTILISATEURS	Tout le monde	Membre d'entreprise	Partenaires et clients
INFORMATION	Partagée	Propriétaire	Sélective
COÛT	Gratuit ou peu Coûteux	Coûteux	Coûteux

TABLE 1.1 – Comparaison des caractéristiques d'Internet, de l'Intranet et de l'Extranet [7].

Internet est un réseau ouvert accessible au public, où les utilisateurs peuvent partager une grande variété d'informations. L'intranet est un réseau interne qui n'est accessible qu'aux membres d'une entreprise et ce qui garantit que les informations sensibles restent confidentielles. L'extranet, quant à lui, est un réseau qui permet aux partenaires et aux clients d'une entreprise d'accéder à certaines informations spécifiques et sélectionnées. Enfin, les coûts associés à l'installation et à la maintenance d'un intranet ou d'un extranet sont généralement plus élevés que ceux d'internet.

### 1.2.3 La pile protocolaire TCP/IP

La pile protocolaire TCP/IP est un élément clé de l'architecture réseau, car elle permet la communication entre les différents équipements du réseau et assure la fiabilité de cette communication. Elle est composée d'un ensemble de protocoles de communication largement utilisés et pris en charge par de nombreux équipements réseau, systèmes d'exploitation et applications. La pile TCP/IP offre les avantages suivants :

1. **Universalité** : La pile TCP/IP est largement adoptée, ce qui garantit une interopérabilité élevée et facilite la communication entre différents dispositifs et plates-formes.
2. **Fiabilité** : Les protocoles TCP/IP, tels que TCP (Transmission Control Protocol), offrent des mécanismes de contrôle d'erreur, de retransmission et de gestion de la congestion, assurant ainsi une transmission fiable des données sur le réseau.

3. **Flexibilité** :La pile TCP/IP est conçue de manière modulaire, permettant l'ajout, la modification ou la suppression des protocoles selon les besoins spécifiques. Cela offre une grande flexibilité dans la conception et la configuration des réseaux.
4. **Évolutivité** :La pile TCP/IP est capable de prendre en charge des réseaux de toutes tailles, du plus petit réseau local (LAN) au plus grand réseau étendu (WAN). Elle offre une structure évolutive qui peut s'adapter aux besoins de croissance et d'expansion d'une organisation.
5. **Support de l'Internet** :La pile TCP/IP est utilisée comme base pour l'Internet et est essentielle pour la communication et l'échange de données à l'échelle mondiale. Elle permet aux utilisateurs d'accéder à des services en ligne, de naviguer sur le Web et de communiquer à travers les frontières géographiques.
6. **Sécurité** :La pile TCP/IP peut inclure des fonctionnalités de sécurité telles que l'IPsec (Internet Protocol Security) pour assurer la confidentialité, l'intégrité et l'authenticité des données en transit. Cela permet de mettre en place des connexions sécurisées et de protéger les informations sensibles.

## 1.3 Généralité sur la sécurité des systèmes d'information

### 1.3.1 Définition de la sécurité informatique

La sécurité des systèmes d'information (SSI) ou plus simplement sécurité informatique, est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher l'utilisation non autorisée, le mauvais usage, la modification ou le détournement du système d'information. Assurer la sécurité du système d'information est une activité du management du système d'information[13].

### 1.3.2 Les Critères de la sécurité informatique

Les critères de sécurité sont des indicateurs permettant d'évaluer la qualité de la sécurité informatique. Les principaux critères sont la confidentialité, l'intégrité, l'authentification, la non-répudiation, la disponibilité et la traçabilité. Ils sont essentiels pour protéger les données et les ressources contre les attaques malveillantes lors de la conception et de l'évaluation des systèmes informatiques[14].

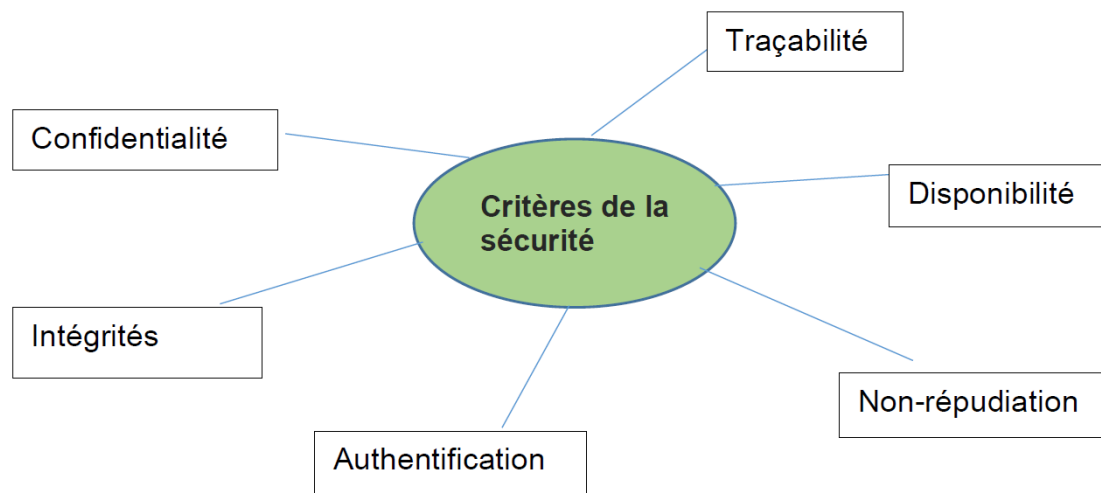


FIGURE 1.2 – Les critères de la sécurité

### 1.3.2.1 Confidentialité

La confidentialité consiste à protéger les données transmises contre les attaques passives. Il est possible d'envisager plusieurs niveaux de protection pour la confidentialité. Le service le plus général permet de protéger toutes les données échangées entre deux utilisateurs pendant une période donnée. Des formes plus spécifiques peuvent également être définies, comme la protection d'un message particulier ou de champs spécifiques à l'intérieur d'un message. La protection du flot de trafic contre l'analyse est un autre aspect important de la confidentialité. Cela nécessite qu'un attaquant ne puisse pas observer les sources et les destinations, les fréquences, les longueurs ou d'autres caractéristiques du trafic circulant sur un équipement de communication.

### 1.3.2.2 Intégrité

L'intégrité garantit que les données échangées ne sont pas modifiées ou supprimées de manière non autorisée. Des techniques telles que le hachage, la somme de contrôle ou le code d'authentification de message avec une clé secrète sont utilisées pour valider l'authenticité des données échangées et garantir leur précision. Différents services d'intégrité sont disponibles en fonction des besoins de protection globale ou spécifique des messages échangés.

### 1.3.2.3 Authentification

L'authentification permet de vérifier l'identité des utilisateurs, des applications et des systèmes informatiques. Elle contrôle l'accès aux ressources et aux informations sensibles. Les critères courants d'authentification incluent :

- **Les mots de passe** : Les utilisateurs doivent créer des mots de passe forts, qui sont difficiles à deviner ou à craquer, et doivent les changer régulièrement.

- **Les cartes à puce** : c'est une puce qui stocke des informations d'identification, telles que des clés ou des certificats numériques.
- **Les certificats numériques** : utilisés pour vérifier l'identité des entités, telles que les sites web, les applications et les serveurs. Ils sont émis par des autorités de certification (CA) et contiennent des informations sur l'entité à authentifier.
- **Les tokens d'authentification** : ils sont souvent utilisés pour les connexions à distance ou les connexions VPN. Ils génèrent un code d'authentification à usage unique qui doit être entré avec le mot de passe pour accéder aux ressources.
- **La biométrie** : utilise des caractéristiques physiques uniques, telles que les empreintes digitales ou la reconnaissance faciale, pour authentifier les utilisateurs.

L'utilisation de ces critères renforce la sécurité informatique en limitant l'accès aux utilisateurs autorisés.

#### 1.3.2.4 Non-répudiation

La non-répudiation empêche tant l'expéditeur que le receveur de nier avoir transmis ou reçu un message. Ainsi, lorsqu'un message est envoyé, le receveur peut prouver que le message a bien été envoyé par l'expéditeur prétendu. De même, lorsqu'un message est reçu, l'expéditeur peut prouver que le message a bien été reçu par le receveur prétendu.

#### 1.3.2.5 Disponibilité

Il existe de nombreuses attaques qui peuvent causer une perte ou une diminution de la disponibilité d'un service ou d'un système. Certaines de ces attaques peuvent être contrées par des contre-mesures automatisées telles que l'authentification et le chiffrement, tandis que d'autres nécessitent une intervention humaine pour prévenir ou rétablir la disponibilité des éléments du système.

#### 1.3.2.6 Traçabilité

La traçabilité est la caractéristique qui conserve les traces de l'état et des mouvements de l'information. Elle permet de déterminer qui a accédé à quelles données et à quel moment, et de détecter toute tentative d'accès non autorisé ou toute modification non autorisée des données. Sans la traçabilité, il serait impossible de garantir l'intégrité, la confidentialité et la disponibilité des données.

### 1.3.3 Les attaques et vulnérabilités

#### 1.3.3.1 Vulnérabilité

**1.3.3.1.1 Définition** La vulnérabilité, également connue sous le terme anglais "vulnerability", est une faille ou une faiblesse dans un composant matériel ou logiciel

qui expose un système à des menaces spécifiques. En informatique, une vulnérabilité fait référence à une faille ou une faiblesse qui compromet l'intégrité et la confidentialité des données. Elle permet à un attaquant d'accéder de manière non autorisée, de voler ou de contourner les informations. Généralement, les attaquants cherchent à exploiter les failles logicielles.

#### 1.3.3.1.2 Exemples de vulnérabilité

- **Couche application** : utilisation de mots de passe non robustes dans une application qui stocke des informations sensibles, comme des informations de carte de crédit. Cela pourrait permettre à un attaquant de deviner facilement le mot de passe et d'accéder aux informations confidentielles.
- **Couche transport** : utilisation d'un protocole de communication non sécurisé pour envoyer des informations sensibles, comme un mot de passe ou des informations de carte de crédit. Cela pourrait permettre à un attaquant de lire les informations en transit et de les utiliser à des fins malveillantes.
- **Couche internet** : utilisation d'un serveur DNS non sécurisé pour résoudre les noms de domaine. Cela pourrait permettre à un attaquant d'intercepter et de modifier les requêtes DNS pour rediriger les utilisateurs vers des sites web malveillants.
- **Couche accès** : utilisation de comptes d'utilisateur sans mot de passe ou avec des mots de passe facilement devinables, comme "password" ou "123456". Cela pourrait permettre à un attaquant de se connecter au système en tant qu'utilisateur légitime et d'accéder aux informations sensibles.
- **Couche applicatif** : manque de formation en sécurité informatique pour les employés d'une organisation. Cela pourrait permettre à un attaquant de tromper un employé et de l'inciter à divulguer des informations confidentielles ou à télécharger un logiciel malveillant sur le réseau de l'organisation[15].

#### 1.3.3.2 Les attaques

**1.3.3.2.1 Définition** Une attaque informatique est toute tentative d'accès non autorisé à un ordinateur, un système informatique ou un réseau informatique dans le but de causer des dommages. Les attaques informatiques visent à désactiver, perturber, détruire ou contrôler des systèmes informatiques ou à modifier, bloquer, supprimer, manipuler ou voler les données contenues dans ces systèmes[16].

**1.3.3.2.2 Types d'attaques informatiques** Nous allons décrire les types d'attaque les plus courants [17] :

##### 1. Les attaques par déni de service DoS et DDoS

Les attaques DoS, également appelées « Déni de Service », ont pour objectif de perturber un système en le submergeant d'un grand nombre de requêtes, le rendant ainsi indisponible aux utilisateurs légitimes. Les attaques DDoS, quant à elles, fonctionnent de la même manière, mais sont lancées à partir de plusieurs machines simultanément, ce qui les rend encore plus difficiles à contrer. Il est important de noter que ces types d'attaques ne permettent pas

aux attaquants de voler des données ou de prendre le contrôle d'un système ; leur seul but est de paralyser un site Web ou un système en réduisant sa disponibilité.

## 2. Les attaques par rebond

également connues sous le nom d'attaques de relais, sont une méthode utilisée par les pirates informatiques pour brouiller leur propre identité et leur adresse IP. Les attaquants ciblent une machine en passant par une autre machine, souvent compromise, appelée « rebond ». Cela leur permet d'utiliser les ressources de la machine intermédiaire pour mener leur attaque, tout en masquant leur propre adresse IP et leur identité. Les attaques de relais peuvent prendre différentes formes, telles que les attaques de type « smurf » ou les attaques de type « FTP bounce », et leur utilisation a augmenté avec la popularité des réseaux sans fil, qui peuvent être plus vulnérables aux attaques.

## 3. Les logiciels malveillants

Un logiciel malveillant, c'est un logiciel qui est installé sur un ordinateur sans le consentement de son propriétaire. La famille des logiciels malveillants est très vaste : elle comprend notamment les virus furtifs, qui s'attaquent aux logiciels antivirus pour les rendre incapables de détecter d'autres virus, et les logiciels espions, qui récoltent des informations sur les utilisateurs. Les chevaux de Troie se cachent dans d'autres logiciels et servent à attaquer un système ou à aménager une « back door » qui permettent aux hackers d'accéder à l'ordinateur. Les virus macro infectent les fichiers Microsoft et Excel et compromettent les données, tandis que les vers se propagent dans les boîtes emails.

## 4. Ingénierie sociale

Contrairement aux attaques précédentes, l'ingénierie sociale n'utilise pas de technologie compliquée. Elle exploite les failles humaines, et non les vulnérabilités matérielles. Le phishing consiste ainsi à demander à un utilisateur de changer un mot de passe ou à fournir des informations confidentielles, par le biais d'un simple email dans lequel le hacker se fait passer pour une banque, un service de messagerie, ou toute institution respectable.

### 1.3.4 Les protocoles de sécurité

Les protocoles de sécurité sont conçus pour protéger les systèmes informatiques contre les menaces potentielles. Ils sont utilisés pour assurer l'authentification des utilisateurs et des dispositifs, pour chiffrer les données de manière à ce qu'elles ne puissent pas être lues par des tiers non autorisés, pour surveiller l'utilisation des systèmes et pour gérer les accès aux ressources.

Les protocoles de sécurité peuvent être implémentés à différents niveaux du système informatique [18] :

#### **1.3.4.1 SSH : Secure Shell**

Le Protocol SSH (Secure Shell) est utilisé pour un établir un accès sécurisé afin d'effectuer des opérations sensibles sur des machines distantes et des transferts de fichiers à travers un réseau ouvert tout en garantissant l'authentification, la confidentialité et l'intégrité des données. L'établissement d'une connexion SSH se fait en plusieurs étapes :

- Le serveur et le client s'identifient mutuellement .
- Le client s'authentifie auprès du serveur pour obtenir une session.
- La méthode la plus connue est le traditionnel mot de passe .
- Une méthode moins connue mais plus souple est l'utilisation de clefs publiques.

#### **1.3.4.2 SSL/TLS : Secure Socket Layer/Transport Layer Security**

Le protocole SSL (Secure Socket Layer) était un protocole de sécurité largement utilisé pour sécuriser les connexions sur internet. Cependant, en raison de vulnérabilités et de failles de sécurité, SSL a été remplacé par TLS (Transport Layer Security) qui est une version plus récente et plus sécurisée du protocole. Aujourd'hui, TLS est largement utilisé pour assurer la sécurité des échanges entre les clients et les serveurs sur internet.

#### **1.3.4.3 SET : Secure Electronic Transaction**

La sécurité des transactions de paiement, utilisant la carte bancaire, repose sur le protocole Secure Electronic Transaction (SET) élaboré conjointement par Visa, MasterCard et les acteurs majeurs de la communauté informatique.

#### **1.3.4.4 S/MIME : Secure/Multipurpose Internal Mail Extensions**

S/MIME (Secure/Multipurpose Internal Mail Extensions) est un protocole utilisé pour l'envoi de messages chiffrés et signés numériquement. S/MIME permet de chiffrer les e-mails et les signer numériquement, Il utilise un système de cryptage asynchrone et de signature digitale pour assurer l'authentification de l'émetteur et garantir que le message reçu est exactement celui qui a été envoyé, sans modification préalable par un tiers malveillant.

#### **1.3.4.5 PGP : Pretty Good Privacy**

PGP (Pretty Good Privacy) est un protocole de sécurité qui permet de crypter et décrypter des messages électroniques sans utiliser de certificats numériques. Il utilise des clés de cryptage privées et publiques pour protéger les communications électroniques et garantir la confidentialité des données échangées. PGP ne fournit pas de signature numérique, mais il peut être utilisé en conjonction avec d'autres protocoles pour assurer l'authenticité de l'émetteur.



## 1.3.5 Les mécanismes de défense

Les différents mécanismes de défense sont :

### 1.3.5.1 Chiffrement

Il existe deux types de chiffrement :

**Chiffrement symétrique** : utilise une seule clé pour chiffrer et déchiffrer les données.

**Chiffrement asymétrique** : utilise une paire de clés (clé publique et clé privée) pour chiffrer et déchiffrer les données.

### 1.3.5.2 Pare-feu

Un pare-feu est un dispositif (logiciel ou matériel) qui contrôle le trafic réseau en appliquant des règles de sécurité spécifiques. Il permet de filtrer les communications autorisées ou interdites selon la politique de sécurité définie.

**1.3.5.2.1 Certificats** Les certificats sont utilisés pour l'authentification et l'identification des entités dans un réseau sécurisé. Ils permettent de vérifier l'identité d'une partie, comme un serveur ou un utilisateur, en utilisant des clés publiques et des autorités de certification.

### 1.3.5.3 DMZ(zone démilitarisée)

Une DMZ est une zone intermédiaire entre le réseau interne sécurisé et le réseau externe non sécurisé, tels qu'Internet. Elle héberge des serveurs accessibles depuis l'extérieur, tout en limitant l'accès direct au réseau interne sécurisé.

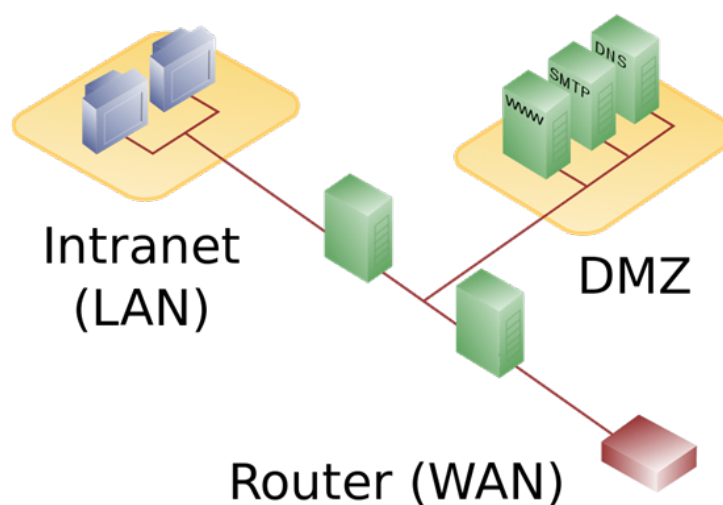


FIGURE 1.3 – Représentation schématique d'une zone démilitarisée avec deux pare-feu [20].

#### **1.3.5.4 Antivirus**

Un antivirus est un programme qui a pour finalité de protéger la machine ou l'appareil sur lequel il est installé. Le protéger les logiciels malveillants. Comme le firewall ou pare-feu, l'antivirus est l'un des principaux dispositifs de sécurité pour garantir la protection des données de l'utilisateur et une navigation optimale sur le web. Ce logiciel élimine ou réduit le risque de cyberattaques sur l'ordinateur, le téléphone ou la tablette qui disposent d'un accès à Internet.

## **1.4 Conclusion**

La sécurité informatique est devenue une priorité absolue pour les entreprises, les gouvernements et les particuliers, car les pertes et les dommages causés par des violations de sécurité peuvent être très importants. Il est donc important de sensibiliser les utilisateurs aux risques de sécurité informatique et de mettre en place des mesures de sécurité adéquates pour garantir la protection des données et des systèmes informatiques.

# Chapitre 2

## Généralités sur la sécurité d'un serveur web

### 2.1 Introduction

La sécurité des serveurs web est une préoccupation importante dans le monde numérique. Pour garantir la sécurité des données stockées et échangées, il est essentiel de comprendre les bases du système client/serveur, les différences entre les protocoles HTTP et HTTPS, ainsi que les mécanismes de chiffrement tels que SSL (Secure Socket Layer) /TLS (Transport Layer Security). Dans ce chapitre, nous allons explorer ces concepts de sécurité pour vous aider à protéger votre serveur web et à maintenir la confidentialité et l'intégrité de vos données.

### 2.2 Le fonctionnement client/serveur du Web

Le système client/serveur est au cœur du fonctionnement du Web, qui est un vaste système d'information distribué permettant aux clients d'accéder aux objets de données partagés sur différents serveurs. Dans ce modèle, la communication entre le client et le serveur se fait par le biais de requêtes et de réponses, avec le client initiant toujours la demande. Pour accéder aux documents web, le client utilise un navigateur, qui crée une requête correspondante et l'envoie au serveur web approprié lorsque le client sélectionne le document souhaité.

#### 2.2.1 Client web

Est un logiciel qui se connecte à un serveur pour envoyer des demandes de service (requêtes). Le demandeur (client) commence par envoyer une demande de connexion au serveur d'origine, puis envoie des requêtes pour obtenir des informations ou des services. Pour se connecter au serveur d'origine, le client peut utiliser le DNS pour obtenir l'adresse IP correspondante dans chaque URL[21].

## 2.2.2 Serveur web

Le serveur web est une partie essentielle de l'architecture client/serveur. Il s'agit d'un programme qui permet à des clients web de se connecter à des services en ligne en envoyant des requêtes et en recevant des réponses. Le serveur web traite ces requêtes en fournissant des informations ou des services en ligne aux clients web.

Le serveur web peut être de deux types : le serveur original (ou final) qui stocke les ressources originales comme les fichiers HTTP, FTP, etc. ; et le serveur intermédiaire (ou proxy) qui agit comme un serveur pour les clients et comme un client pour un autre serveur. Le serveur web est un élément vital de l'infrastructure de communication en ligne qui permet aux utilisateurs de profiter de services numériques divers. Sans serveur web, les clients web ne pourraient pas accéder à ces services[21].

## 2.3 Présentation de l'architecture client /serveur

Le fonctionnement des services web repose sur le modèle client-serveur pur, comme illustré dans la figure 2.1. Le processus commence par la connexion d'un client à un serveur. Le client formule ensuite une requête http(s) au serveur pour demander des informations ou des services. Le serveur répond à la requête, soit en fournissant des documents tels que des pages web ou des images, soit en signalant une erreur si la requête est incorrecte ou si les données demandées ne sont pas disponibles.

L'échange entre le client et le serveur peut reprendre à l'étape 2 de la figure 2.1, si le client souhaite effectuer une autre requête, ou se terminer, s'il a obtenu les informations ou les services souhaités. Il est important de noter que le serveur ne propose ni ne demande jamais rien directement au client, mais seulement en réponse à une requête formulée par le client. Le modèle client-serveur pur est donc fondamental pour le fonctionnement des services web.

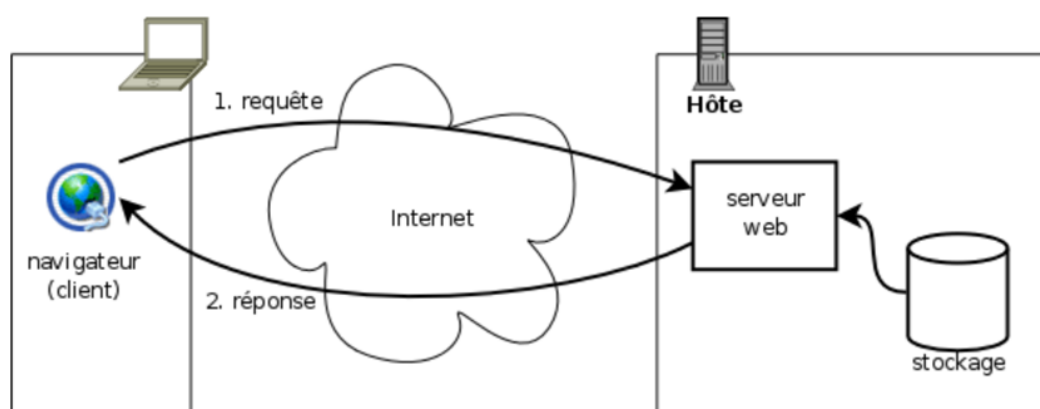


FIGURE 2.1 – Communication client-serveur web en HTTP(S) [31].

## 2.4 Notion sur HTTP Secure(HTTPS)

Dans cette section, nous présentons le protocole HTTP, qui est le protocole par défaut des navigateurs web afin de récupérer des données sur un serveur au moyen d'une URL. Le standard HTTP n'est pour l'instant pas nécessairement sécurisé. Ainsi, dans le cas de l'usage de HTTP non sécurisé, les URL commencent par `http://` puis sont suivies du nom de domaine ou adresse IP du serveur et du chemin de la page recherchée. HTTP est un protocole applicatif et a besoin du protocole TCP pour être transporté. Ce protocole HTTP est attribué par défaut au port 80 pour la version non sécurisée. Lorsque HTTP est sécurisé avec SSL/TLS, les URL débutent alors par `https://` et le port par défaut est le port 443. Conçu par Tim Berners-Le et al. Entre 1989 et 1991 au CERN (Conseil européen pour la recherche nucléaire) [22] .

HTTP	HTTPS
C'est le protocole de transfert hypertexte (HTTP).	C'est le protocole de transfert hypertexte sécurisé (HTTPS).
Ce n'est pas sécurisé et fiable.	Il est sécurisé et fiable.
Les URL HTTP commencent par <code>http://</code> .	Les URL Htts commencent par <code>https://</code> .
Il utilise le port 80 par défaut.	Il utilise le port 443 par défaut.
Il est susceptible d'attaques de type "homme du milieu" (man in the middle) et d'écoutes clandestines (eavesdropping).	Il est conçu pour résister à de telles attaques et est considéré comme sécurisé contre ces attaques.

TABLE 2.1 – Différence entre HTTP et HTTPS

### 2.4.1 Définition de HTTPS

L'HTTPS, ou Hypertext Transfer Protocol Secure, est en effet la version sécurisée du protocole HTTP utilisé pour la communication entre un client (généralement un navigateur web) et un serveur sur le World Wide Web. Il utilise un protocole de sécurité tel que SSL (Secure Sockets Layer) ou TLS (Transport Layer Security) pour chiffrer les données échangées entre le client et le serveur, assurant ainsi la confidentialité et l'intégrité des informations[23].

### 2.4.2 Le principe de HTTPS

L'un des principaux objectifs de l'HTTPS est de garantir l'authentification du serveur, ce qui permet aux utilisateurs de vérifier que le site web auquel ils accèdent est légitime et qu'il n'a pas été compromis. Cela est généralement indiqué par la

présence d'un cadenas dans la barre d'adresse du navigateur, ainsi que par un préfixe "https://" au lieu de "http://" dans l'URL du site.

En plus de l'authentification du serveur, l'HTTPS peut également permettre l'authentification du client dans certaines situations, par exemple lors de la connexion à un site web avec des identifiants de compte.

L'adoption de l'HTTPS est devenue de plus en plus courante sur le web, en particulier pour les sites web nécessitant la transmission de données sensibles telles que les informations de paiement lors des achats en ligne. Cela contribue à renforcer la sécurité et la confiance des utilisateurs lors de la navigation sur le web. Il est recommandé aux propriétaires de sites web de mettre en place l'HTTPS pour protéger les données de leurs utilisateurs et assurer la confidentialité des informations échangées sur leur site. Les certificats HTTPS sont généralement délivrés par des autorités de certification (CA) reconnues, telles que GlobalSign, Thawte ou Trustico, pour garantir l'authenticité du certificat et du site web sécurisé. Les utilisateurs doivent toujours faire preuve de prudence lors de la navigation en ligne et vérifier que les sites web qu'ils visitent utilisent l'HTTPS pour protéger leurs données. La présence d'un cadenas et du préfixe "https://" dans l'URL sont de bons indicateurs de la sécurité d'un site web, mais il est également important de vérifier la réputation et la légitimité du site avant de partager des informations sensibles en ligne[23].

En résumé, l'HTTPS est un protocole de sécurité essentiel pour protéger la confidentialité et l'intégrité des données échangées sur le web, et il est largement utilisé sur les sites web qui nécessitent un haut niveau de sécurité, tels que les sites de commerce électronique et les sites de services bancaires en ligne.

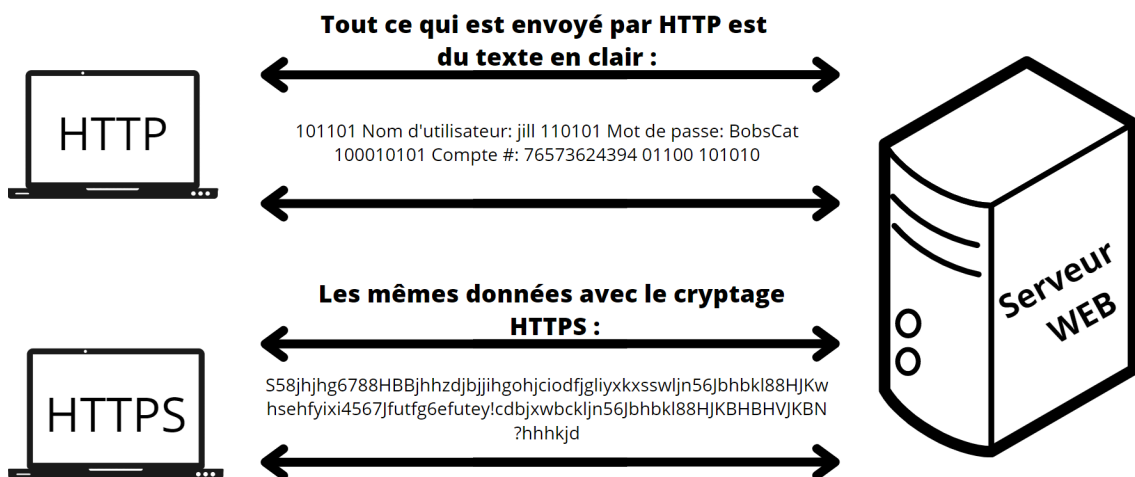


FIGURE 2.2 – Différence entre HTTP et HTTPS.

## 2.5 Le protocole SSL/TLS

### 2.5.1 Définition

SSL (Secure Sockets Layer) ou TLS (Transport Layer Security) est un protocole de sécurité utilisé pour sécuriser les communications sur Internet. Il fonctionne en fournissant une couche de sécurité entre les protocoles de la couche application, tels que HTTP, FTP, et d'autres protocoles de la couche application, et la couche de transport, telle que TCP (Transmission Control Protocol) [24].

### 2.5.2 Historique

Le protocole SSL a été développé à l'origine chez Netscape et la première version, SSL 2, a été publiée en novembre 1994, mais elle présentait des faiblesses sérieuses et a été remplacée par SSL 3 à la fin de l'année 1995. En mai 1996, le groupe de travail TLS a été formé pour migrer SSL de Netscape vers l'IETF, et TLS 1.0 a finalement été publié en janvier 1999. TLS 1.1 a été publié en avril 2006, et TLS 1.2 a été publié en août 2008. La prochaine version, actuellement en développement, vise à simplifier la conception, à supprimer de nombreuses fonctionnalités faibles et moins désirables, et à améliorer les performances[32].

### 2.5.3 Fonctionnement

Les protocoles SSL et TLS se décomposent en deux couches principales, qui comprennent en réalité quatre protocoles distincts.

Le protocole de poignée de main SSL et TLS permet de sélectionner la version de SSL/TLS à utiliser, d'authentifier les parties en échangeant des certificats, et de négocier le niveau de sécurité en choisissant les algorithmes de chiffrement appropriés. Ce protocole configure la transaction.

Le protocole d'enregistrement SSL et TLS encapsule et divise les données. Il s'agit du protocole de transmission des données.

La première étape consiste en une phase de négociation entre le client et le serveur, pour configurer la transaction et échanger les clés de chiffrement. Ensuite, les données sont échangées entre les deux parties[33].

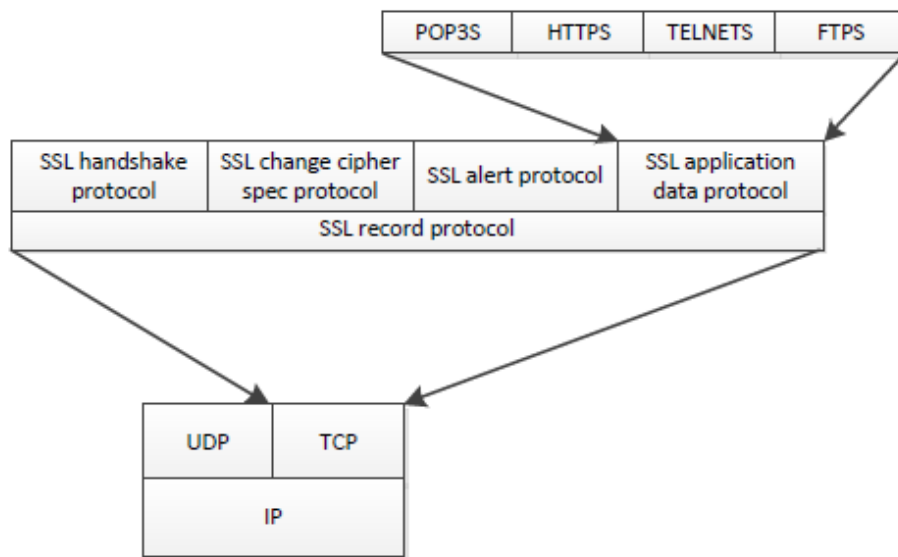


FIGURE 2.3 – Organisation du protocole ssl. [25].

Les protocoles SSL et TLS sont composés de quatre protocoles principales :

- Le protocole SSL handshake : initialise l'échange SSL avec l'authentification par certificat, l'échange des paramètres de sécurité...
- Le protocole SSL change cipher spec : pour établir de nouveaux paramètres de sécurité dans un échange
- Le protocole SSL alert : signale les erreurs et les alertes liées à la sécurité.
- Le protocole SSL application data : la couche applicative transmet directement ses données au protocole SSL record pour les transmettre de façon sécurisée. Utilisé quand l'initialisation a été effectuée avec succès par le SSL handshake[25].

## 2.5.4 Services offerts par SSL/TLS

### 2.5.4.1 Intégrité

SSL/TLS garantit l'intégrité des données en utilisant des codes de hachage pour vérifier que les données n'ont pas été modifiées ou altérées en transit. Les codes de hachage sont des algorithmes de calcul qui produisent une empreinte numérique unique pour chaque message, qui est ensuite utilisée pour vérifier l'intégrité du message à la réception. Si les données ont été modifiées en transit, le code de hachage ne correspondra pas, ce qui indiquera à l'utilisateur que les données ont été altérées[26].



### 2.5.4.2 Authentification

SSL/TLS garantit l'authentification en utilisant des certificats numériques pour vérifier l'identité des parties impliquées dans la communication. Les certificats numériques sont délivrés par des autorités de certification (CA) de confiance, qui vérifient l'identité de l'entité demandant le certificat avant de le délivrer. Le certificat numérique contient les informations d'identification de l'entité et est utilisé pour établir la confiance entre les parties. Ainsi, SSL/TLS permet aux clients de vérifier que le serveur avec lequel ils communiquent est bien celui qu'ils pensent être. Depuis SSL 3.0, le serveur peut également demander au client de s'authentifier en utilisant des certificats numériques ou des noms d'utilisateur et des mots de passe[26].

## 2.6 Système de sécurisation utilisé par SSL/TLS

La sécurité SSL/TLS (Couche de Sockets Sécurisée / Sécurité de la Couche de Transport) implique le cryptage des données avant leur transfert sur le réseau local ou Internet, dans le but de garantir la confidentialité et l'intégrité des informations transmises.

### 2.6.1 Système de chiffrement symétrique

SSL/TLS utilise des algorithmes de chiffrement symétrique pour protéger les données en transit entre le client et le serveur. Ces algorithmes sont appelés symétriques car ils utilisent la même clé pour le chiffrement et le déchiffrement des données. Cela signifie que la clé de chiffrement doit être partagée entre le client et le serveur avant que les données puissent être échangées de manière sécurisée.

SSL/TLS prend en charge plusieurs algorithmes de chiffrement symétrique, y compris :

RC4 : c'était un algorithme de chiffrement largement utilisé dans les versions antérieures de SSL/TLS, mais il est maintenant considéré comme peu sûr et obsolète.

AES (Advanced Encryption Standard) : il s'agit d'un algorithme de chiffrement symétrique standardisé qui est largement utilisé dans SSL/TLS pour assurer la sécurité des données. Il est considéré comme l'un des algorithmes les plus sûrs et les plus fiables disponibles.

3DES (Triple Data Encryption Standard) : c'est un algorithme de chiffrement symétrique qui utilise trois clés différentes pour chiffrer les données. Il est également largement utilisé dans SSL/TLS, mais est maintenant considéré comme moins sûr qu'AES.

Le choix de l'algorithme de chiffrement symétrique dépend de la version de SSL/TLS utilisée et de la configuration du serveur et du client. Les versions plus récentes de SSL/TLS recommandent l'utilisation d'AES, tandis que les versions plus anciennes peuvent toujours utiliser RC4 ou 3DES[34].

## 2.6.2 Système de chiffrement asymétrique

Les techniques de chiffrement asymétrique se fondent sur la distribution d'une clé publique entre les différents utilisateurs et l'utilisation d'un certificat signé, qui est couramment utilisé. Un schéma graphique présenté ci-dessous explique comment le chiffrement des données échangées entre un serveur et un client HTTPs peut être réalisé à l'aide d'un certificat.

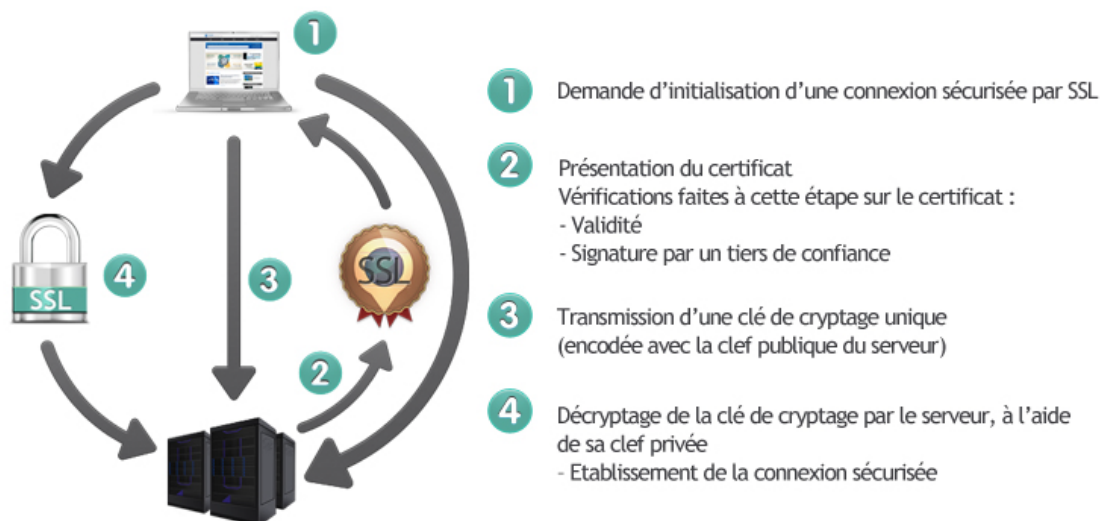


FIGURE 2.4 – Schéma d'établissement de connexion sécurisée . [27].

## 2.6.3 Système de signature cryptographique

Est une méthode permettant de garantir l'authenticité et l'intégrité d'un document ou d'un message électronique. Il repose sur l'utilisation d'un algorithme de chiffrement asymétrique, où l'émetteur signe le document avec sa clé privée et le destinataire vérifie la signature à l'aide de la clé publique correspondante. Si la signature est valide, cela prouve que le document n'a pas été altéré et que l'émetteur est bien celui qu'il prétend être. Ce système est largement utilisé dans les transactions électroniques et les échanges de données sensibles[28].

## 2.7 Les certificats SSL

Un certificat SSL/TLS est un fichier électronique qui est utilisé pour lier une clé cryptographique à des informations d'identification de l'entité qui utilise le certificat. Les certificats SSL/TLS sont principalement utilisés pour sécuriser les communications sur Internet en permettant aux utilisateurs de vérifier l'identité des parties auxquelles ils se connectent et en garantissant la confidentialité et l'intégrité des données échangées.

## 2.7.1 Fonctionnement d'un certificat SSL

Le fonctionnement d'un certificat SSL/TLS repose sur la cryptographie à clé publique (ou cryptographie asymétrique) et implique plusieurs acteurs et étapes. Voici un résumé du processus :

L'entreprise ou l'organisation qui souhaite obtenir un certificat SSL/TLS en fait la demande auprès d'une autorité de certification (AC).

L'AC vérifie les informations d'identification de l'entreprise et lui délivre un certificat SSL/TLS qui inclut une clé publique et une signature numérique.

Lorsqu'un navigateur accède à un site web sécurisé qui utilise un certificat SSL/TLS, il reçoit ce certificat et utilise la clé publique pour vérifier la signature numérique et s'assurer de l'authenticité du certificat.

Le navigateur et le serveur web échangent des clés de session secrètes qui seront utilisées pour chiffrer les communications entre eux.

Les données échangées entre le navigateur et le serveur sont chiffrées avec la clé de session secrète, ce qui garantit leur confidentialité et leur intégrité.

À la fin de la session, la clé de session secrète est détruite et la prochaine session utilisera une nouvelle clé de session[29].

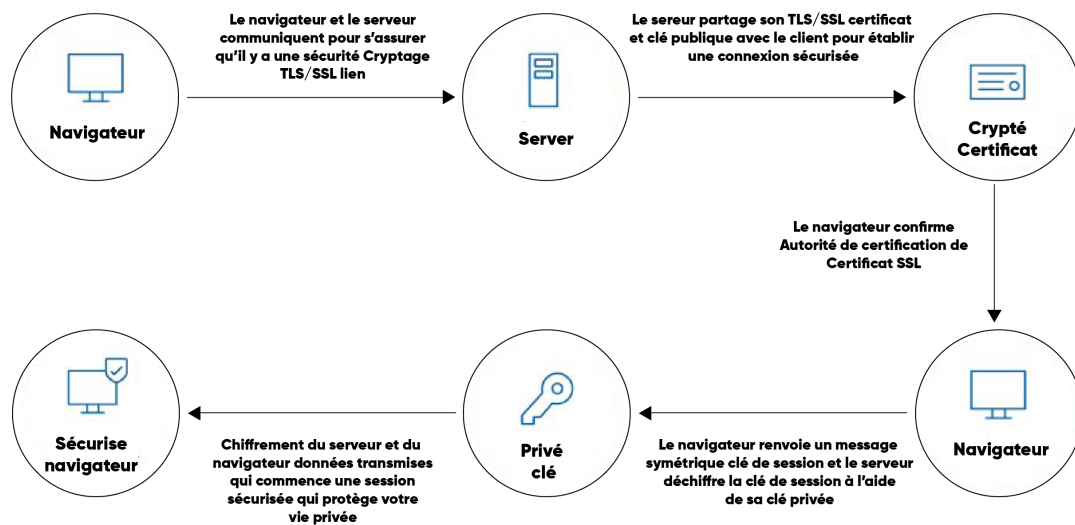


FIGURE 2.5 – 1. Fonctionnement d'un certificat SSL/TLS. [36].

## 2.7.2 Fonctionnement d'un protocole sécurisé

Le fonctionnement d'un protocole sécurisé, comme SSL/TLS (Transport Layer Security), implique plusieurs étapes pour sécuriser les communications sur Internet.

Tout d'abord, une poignée de main SSL/TLS est réalisée entre le client (par exemple, un navigateur web) et le serveur (par exemple, un site web). Cette poignée de main permet d'établir une connexion sécurisée en négociant les paramètres de chiffrement et d'authentification à utiliser. Ensuite, l'authentification du serveur et éventuellement du client peut avoir lieu. Enfin, une fois que l'authentification est réussie, le protocole SSL/TLS chiffre les données échangées entre le client et le serveur à l'aide d'un algorithme de chiffrement et d'une clé de session générée lors de la poignée de main SSL/TLS.

### **2.7.3 Authentification du serveur**

L'authentification du serveur est réalisée grâce au certificat SSL émis par une autorité de certification (CA) de confiance. Le certificat SSL contient des informations sur le site web, telles que son nom de domaine et sa clé publique, et est signé numériquement par la CA pour garantir son authenticité. Lorsque le navigateur de l'utilisateur reçoit le certificat SSL du serveur, il vérifie la validité du certificat en s'assurant qu'il a été émis par une CA de confiance et qu'il n'a pas été altéré.

### **2.7.4 Authentification du client**

L'authentification du client, également appelée authentification mutuelle, est une fonctionnalité optionnelle du protocole SSL/TLS qui permet au serveur de vérifier l'identité du client. Dans ce cas, le client doit également posséder un certificat SSL avec une clé privée correspondante. Lors de la poignée de main SSL/TLS, le client envoie son certificat au serveur, qui peut alors vérifier son authenticité en utilisant la clé publique associée dans le certificat. Cela permet au serveur de s'assurer que le client est bien celui qu'il prétend être.

### **2.7.5 Chiffrement des données**

Le chiffrement des données est une étape essentielle du protocole sécurisé. Une fois que l'authentification du serveur et du client est réussie, le protocole SSL/TLS utilise des techniques de chiffrement pour protéger les données échangées entre le navigateur et le serveur. Les données sont chiffrées à l'aide d'un algorithme de chiffrement et d'une clé de session générée lors de la poignée de main SSL/TLS. Le chiffrement rend les données illisibles pour toute personne ou tout dispositif qui tenterait de les intercepter sans la clé de session appropriée, garantissant ainsi leur confidentialité pendant leur transit sur le réseau.

### **2.7.6 Les sous-protocoles SSL/TLS**

SSL (Secure Sockets Layer) est composé de plusieurs modules ou sous-protocoles qui travaillent ensemble pour assurer la sécurité des communications sur Internet. Les quatre principaux sous-protocoles de SSL sont :

### 2.7.6.1 Le protocole Handshake

Protocole de poignée de main (Handshake Protocol) : Ce sous-protocole permet au client et au serveur de s'authentifier mutuellement, d'échanger les paramètres de sécurité et de négocier le niveau de chiffrement et d'authentification à utiliser pour la session SSL.

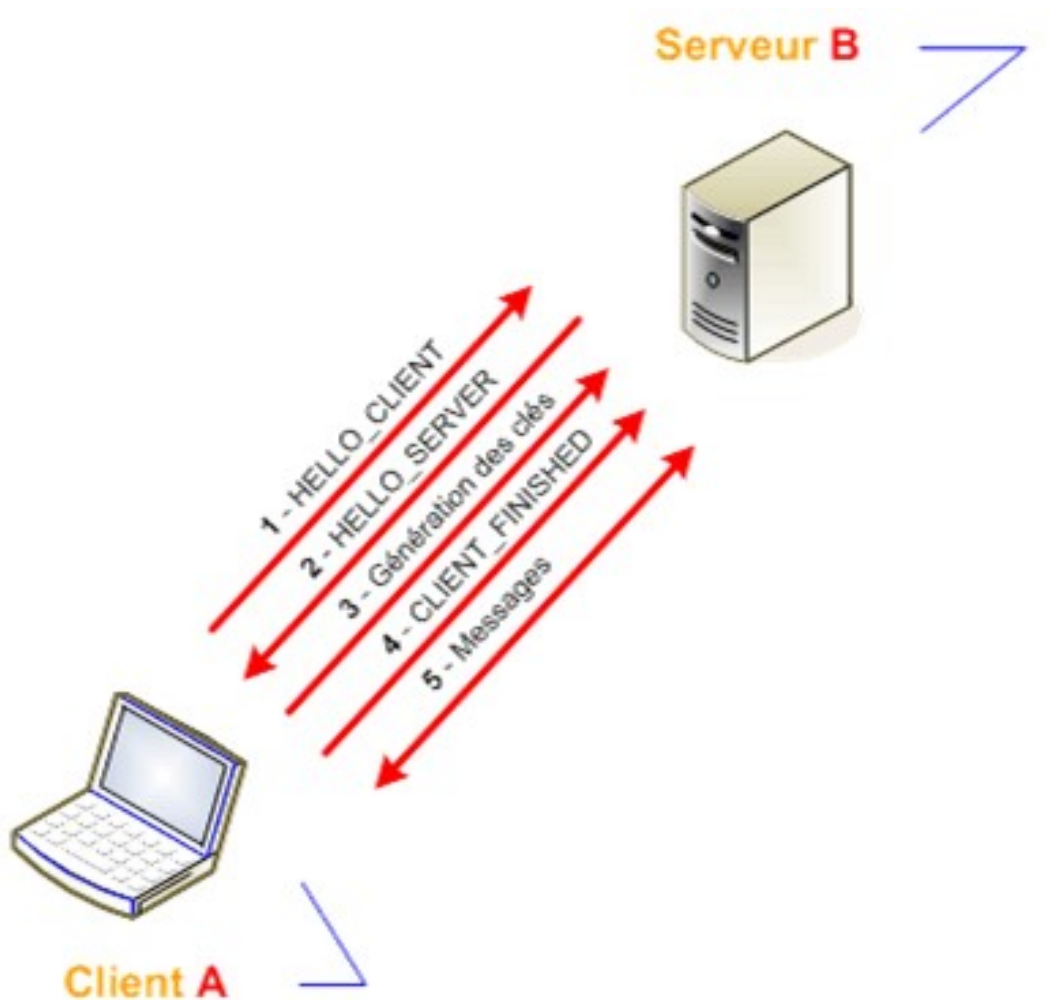


FIGURE 2.6 – fonctionnement de handshake. [30].

a. Le client envoie un message HELLO-CLIENT en clair au serveur, contenant les informations suivantes :

- La version la plus haute de SSL/TLS que le client peut utiliser.
- Un horodatage de 32 bits et une valeur aléatoire de 28 octets générée par le client, qui seront utilisés pour signer les messages.
- Un identifiant de session, qui peut être un zéro indiquant la volonté du client d'établir une nouvelle connexion, ou un autre nombre indiquant la volonté de changer les paramètres ou de créer une nouvelle connexion sur une session existante.
- Une liste d'algorithmes de chiffrement, par ordre de préférence, que le client supporte pour l'échange de clé et le chiffrement.

- Une liste d'algorithmes de compression, par ordre de préférence, que le client supporte. Ensuite, le client attend une réponse du serveur
- b. Le serveur répond au client en clair avec un message HELLO-SERVER, contenant les informations suivantes :
  - La version la plus haute de SSL/TLS que le serveur peut utiliser.
  - Un horodatage de 32 bits et une valeur aléatoire de 28 octets générée par le serveur.
  - L'identifiant de session de la session qui débute.
  - La première suite d'algorithmes de chiffrement choisie par le serveur parmi ceux proposés par le client.
  - La méthode de compression qui sera utilisée. Une fois les algorithmes choisis, le serveur s'authentifie auprès du client en envoyant ses certificats (X.509) au client. À cette étape, le serveur peut également demander un certificat au client. Le client vérifie alors l'authenticité du serveur, et si cette authenticité est mise en doute, la transaction est interrompue.

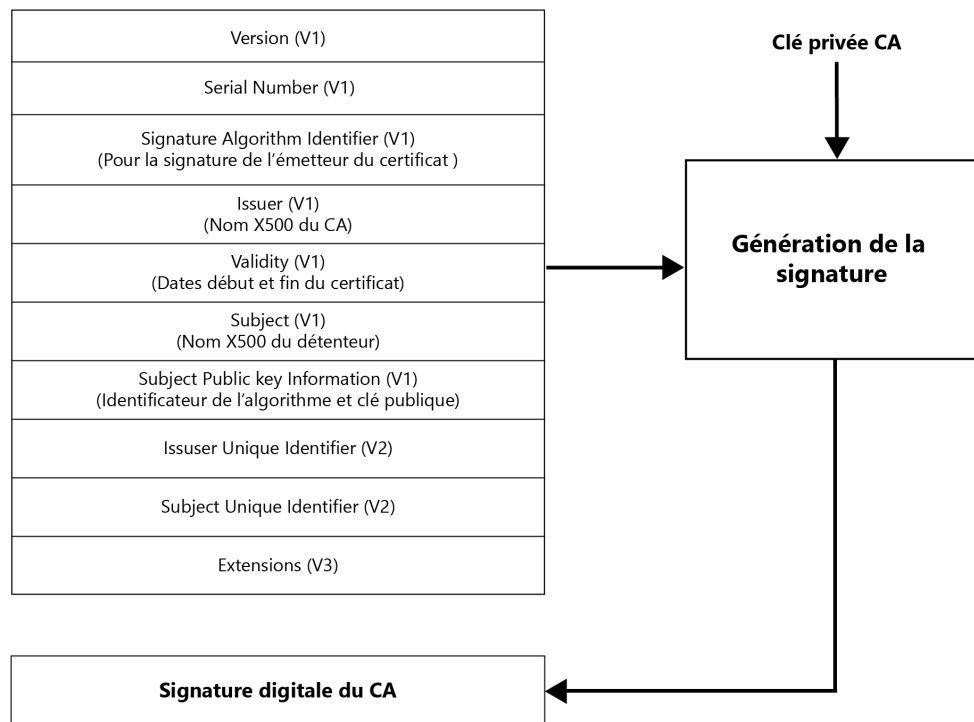


FIGURE 2.7 – structure d'un certificat X.509. [37].

- c. Génération des clés de chiffrement symétrique : Le client génère une pré clé de chiffrement de session, qui est envoyée au serveur chiffré avec la clé publique du serveur. À partir de cette pré clé, le serveur et le client génèrent quatre clés pour la session : La clé secrète de hachage des messages émis par le serveur. La clé secrète de hachage des messages émis par le client. La clé de chiffrement des données émises

par le serveur. La clé de chiffrement des données émises par le client. Ces clés ne sont pas échangées entre le serveur et le client. Si nécessaire, le serveur peut vérifier l'authenticité du client.

d. Le client envoie un message CLIENT-FINISHED au serveur, chiffré et signé avec les clés générées précédemment. Cela signifie que, à partir de maintenant, le client communiquera de cette manière.

e. Le serveur procède de même en envoyant un message similaire, qui est confirmé par le sous-protocole Change Cipher Spec (qui définit uniquement ces messages) [30].

### 2.7.6.2 Le protocole Change Cipher Spec

Protocole de changement de spécification de chiffrement (Change Cipher Spec Protocol) : Ce sous-protocole est utilisé pour annoncer la fin de la négociation des paramètres de chiffrement et indiquer que de nouvelles clés de chiffrement sont prêtes à être utilisées. Il contient un seul message appelé "change-cipher-spec" qui est envoyé par les deux parties à la fin de la négociation. Ce message est chiffré en utilisant l'algorithme de chiffrement symétrique qui a été négocié précédemment entre le client et le serveur. Une fois que les parties reçoivent ce message, elles mettent en place les nouvelles clés de chiffrement pour protéger les données échangées par la suite. Cela garantit la confidentialité et l'intégrité des données lors de la communication sécurisée entre le client et le serveur [30].

### 2.7.6.3 Le protocole Alert

Protocole d'alerte (Alert Protocol) : Est un sous-protocole qui spécifie les messages d'erreur que les clients et les serveurs peuvent s'envoyer entre eux. Ces messages d'erreur sont composés de deux octets. Le premier octet indique s'il s'agit d'un avertissement ("warning") ou d'une erreur fatale ("fatal"). Si le niveau est "fatal", la connexion est abandonnée et les autres connexions sur la même session ne sont pas coupées, mais il n'est pas possible d'établir de nouvelles connexions. Le deuxième octet donne le code d'erreur spécifique.

a. Les erreurs fatales peuvent inclure les suivantes :

- Unexpected-message : indique que le message n'a pas été reconnu.
- Bad-record-mac : signale une signature MAC incorrecte.
- Decompression-failure : indique que la fonction de décompression a reçu une mauvaise entrée.
- Handshake-failure : impossible de négocier les bons paramètres lors de la phase de poignée de main.
- Illegal-parameter : indique un champ mal formaté ou ne correspondant à rien.

b. Les avertissements peuvent inclure les suivants :

- Close-notify : annonce la fin d'une connexion.
- No-certificate : répond à une demande de certificat s'il n'y en a pas.
- Bad-certificate : le certificat reçu n'est pas valide, par exemple, sa signature est

incorrecte.

- Unsupported-certificate : le certificat reçu n'est pas reconnu.
- Certificate-revoked : le certificat a été révoqué par l'émetteur.
- Certificate-expired : le certificat a expiré.
- Certificate-unknown : pour tout autre problème concernant les certificats et qui n'est pas listé ci-dessus.

Le protocole Alert permet ainsi de gérer les erreurs et les avertissements qui peuvent survenir lors d'une communication sécurisée avec SSL/TLS, en permettant aux parties de se signaler mutuellement les problèmes rencontrés [30].

#### 2.7.6.4 Le protocole SSL Record

Protocole d'enregistrement (Record Protocol) : Ce sous-protocole est responsable de la fragmentation, du chiffrement et de l'intégrité des données échangées entre le client et le serveur. Il assure la protection des données elles-mêmes en les fragmentant en blocs plus petits, en les chiffrant pour garantir leur confidentialité et en ajoutant des informations d'intégrité pour vérifier leur intégrité lors de la transmission.

En combinant ces sous-protocoles avec le protocole d'enregistrement, SSL assure la sécurité des données échangées entre le client et le serveur en protégeant à la fois les données elles-mêmes (par le biais du protocole d'enregistrement) et les processus d'authentification, de négociation et de signalisation (par le biais des autres sous-protocoles).

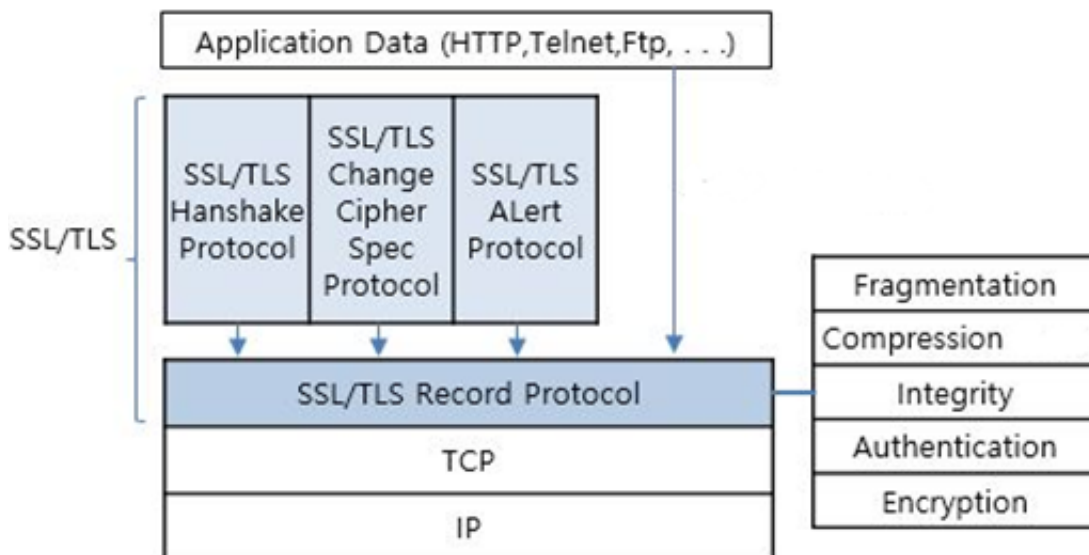


FIGURE 2.8 – SSL record. [35].



## 2.8 Conclusion

SSL/TLS est essentiel à la sécurité du Web. Il offre une forte confidentialité, intégrité des messages et authentification du serveur aux utilisateurs. Le secteur du commerce électronique est étroitement lié à la confiance des consommateurs dans le fonctionnement de SSL à travers Internet. À l'avenir, les dispositifs de terminaison SSL seront en mesure de gérer plus de transactions à une vitesse plus rapide. Le chiffrement des longueurs de clé et les suites de chiffrement utilisées continueront également à évoluer afin de garantir la sécurité des informations sensibles sur le Web. Ainsi, le commerce électronique pourra continuer à gagner en popularité à mesure que les utilisateurs auront de plus en plus confiance dans les achats en ligne, les opérations bancaires en ligne et l'adoption de nouvelles applications en ligne.

# Chapitre 3

## Présentation de l'organisme d'accueil, problématiques et solutions

### 3.1 Introduction

Dans ce chapitre, nous commencerons par présenter Général Emballage, en mettant en évidence son engagement envers les systèmes informatiques et la sécurité des données. Nous explorerons également les spécificités de l'infrastructure réseau du département informatique. Ensuite, nous aborderons la problématique liée à la sécurisation du serveur web de Général Emballage. Nous mettrons en lumière les menaces courantes auxquelles les sites web sont exposés, telles que les attaques par défiguration et les dénis de service, qui peuvent avoir des conséquences néfastes sur l'image de l'organisme et engendrer des pertes financières. Nous soulignerons également l'importance de ne pas sous-estimer les attaques les plus insidieuses.

### 3.2 Présentation générale de General Emballage

Général Emballage Akbou est une entreprise spécialisée dans la production d'emballages en carton ondulé. Fondée en 2002, elle est située à Akbou, en Algérie. L'entreprise se consacre à la fabrication d'une large gamme d'emballages en carton ondulé pour différents secteurs d'activité tels que l'alimentaire, le textile, l'électronique, le cosmétique, et bien d'autres. Leurs produits incluent des boîtes, des plateaux, des caisses, des présentoirs, et des solutions d'emballage sur mesure.



FIGURE 3.1 – logo de General Emballage

### 3.3 Organigramme de l'entreprise

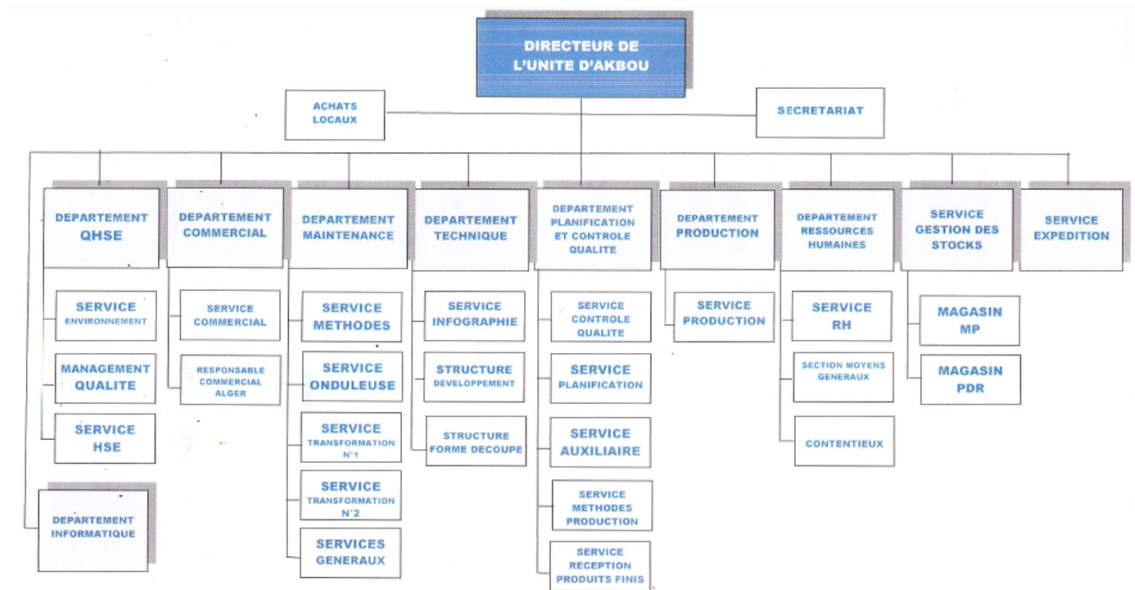


FIGURE 3.2 – Organigramme de l'unité d'Akbou

### 3.4 Systèmes informatique dans Général Emballage

Les systèmes informatiques jouent un rôle essentiel dans les opérations de Général Emballage, facilitant la gestion des données, des communications et des processus internes. L'entreprise accorde une grande importance à la sécurité des données et met en œuvre diverses mesures pour protéger ses systèmes. En ce qui concerne la sécurité, Général Emballage déploie des mesures appropriées pour protéger ses systèmes et ses données sensibles. Cela peut inclure l'utilisation d'antivirus pour détecter et éliminer les menaces potentielles, l'implémentation de pare-feu pour contrôler et filtrer le trafic réseau, ainsi que le chiffrement des données pour garantir leur confidentialité lors de leur transmission et de leur stockage.

### 3.5 L'étude de l'existant

L'étude d'existant au sein d'une entreprise revêt une importance capitale lorsqu'il s'agit d'évaluer l'état actuel de son infrastructure informatique. Dans le contexte spécifique de l'analyse de l'architecture réseau de l'entreprise, l'objectif est d'analyser les différents composants du réseau tels que les serveurs, les postes de travail, les commutateurs, les pare-feu, les équipements de téléphonie, etc. Cette analyse permet de déterminer la configuration du réseau, d'identifier les éventuelles vulnérabilités en matière de sécurité, de mesurer les performances, de repérer les zones à risque et d'évaluer les besoins futurs en investissements et en améliorations. L'étude d'existant constitue ainsi une étape essentielle pour toute entreprise souhaitant améliorer son infrastructure réseau et garantir un niveau de sécurité optimal.

## 3.6 Présentation de l'infrastructure réseau de département informatique

L'infrastructure réseau de Général Emballage est composée d'une combinaison de serveurs, de commutateurs, de routeurs et de pare-feu, qui travaillent en collaboration pour assurer le bon fonctionnement du réseau de l'entreprise. Les serveurs utilisés peuvent être de différents types, tels que des serveurs Windows et des serveurs Linux, qui hébergent les applications et les services essentiels pour les opérations de l'entreprise.

Pour la connectivité au sein du réseau, Général Emballage utilise des commutateurs, tels que les commutateurs Cisco Catalyst, qui fournissent des connexions rapides et fiables entre les différents appareils du réseau, tels que les ordinateurs, les serveurs et les imprimantes.

Pour acheminer le trafic entre les différents bureaux ou sites de l'entreprise, des routeurs sont utilisés. Ces routeurs assurent la transmission des données entre les différents réseaux locaux, en utilisant des protocoles de routage pour choisir les chemins les plus efficaces.

Enfin, pour garantir la sécurité du réseau, Général Emballage utilise des pare-feu qui contrôlent le trafic entrant et sortant, en appliquant des règles de sécurité pour protéger le réseau contre les menaces potentielles.

## 3.7 L'architecture du réseau

Nous proposons une architecture sous GNS3 conçue pour sécuriser un serveur web. Cette architecture repose sur plusieurs composants interconnectés qui travaillent ensemble afin d'assurer la sécurité et la disponibilité du serveur.

Au cœur de cette architecture se trouve le serveur web lui-même, hébergé sur une machine virtuelle (VM) configurée spécifiquement pour cette tâche. La VM est connectée à un commutateur (switch) qui gère la connectivité réseau entre les différents composants.

Pour renforcer la sécurité, nous avons ajouté un pare-feu (firewall) qui agit comme une barrière de protection entre le serveur web et le reste du réseau. Ce pare-feu filtre et contrôle le trafic réseau entrant et sortant, en appliquant des règles de sécurité définies pour prévenir les attaques et les intrusions.

Afin de simuler un réseau réel, nous avons également inclus des machines clientes qui représentent les utilisateurs accédant au serveur web.

Toute cette architecture est configurée et interconnectée dans l'environnement de virtualisation GNS3, qui permet de simuler un réseau complet et de tester la configuration et le fonctionnement des différents composants.

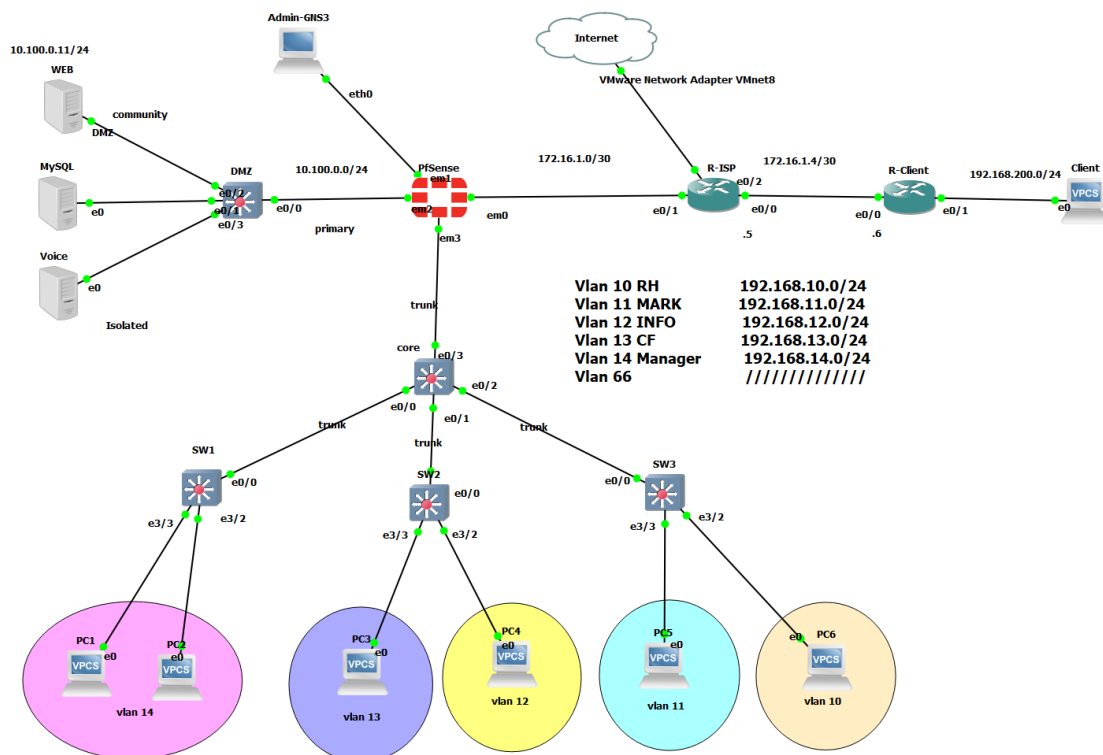


FIGURE 3.3 – Architecture réseau proposé de Général Emballage

## 3.8 Matériels utilisés dans l'architecture

### 3.8.1 PC ou ordinateur

Le terme "PC" est l'abréviation de "personal computer" (ordinateur personnel). Il fait généralement référence à un ordinateur de bureau ou à un ordinateur portable utilisé par une seule personne. Il s'agit d'un équipement informatique qui permet d'exécuter diverses tâches telles que la navigation sur Internet, le traitement de texte, la gestion des fichiers, etc.

Des ordinateurs équipés de processeurs puissants, de mémoire RAM suffisante et de capacités de stockage adaptées pour répondre aux besoins des utilisateurs.

### 3.8.2 Commutateur (switch)

Un commutateur, également appelé "switch", est un dispositif réseau utilisé pour connecter plusieurs appareils au sein d'un réseau local (LAN). Contrairement à un concentrateur (hub) qui diffuse les données à tous les appareils connectés, un commutateur établit des connexions directes entre les appareils intéressés par l'information, ce qui améliore l'efficacité du réseau en réduisant le trafic inutile. Les commutateurs sont couramment utilisés dans les réseaux informatiques pour acheminer efficacement les données entre les différents périphériques connectés.

Des équipements de réseau avec un nombre varié de ports pour connecter les dispositifs du réseau local. Ils offrent une capacité de commutation élevée pour assurer

un transfert de données rapide et fiable.



FIGURE 3.4 – Commutateur (switch)

### 3.8.3 Un routeur

Est un équipement essentiel dans les réseaux informatiques. Il permet l'interconnexion de différents réseaux en acheminant les informations entre eux. Le routeur dispose de ports (connecteurs RJ45) pour se connecter aux différents réseaux et utilise un système d'exploitation et un logiciel pour router les paquets de données. Son rôle principal est d'acheminer les paquets de données vers leur destination en déterminant le chemin le plus approprié. Cela permet d'assurer un transfert efficace des données et une communication fluide entre les réseaux.

Des appareils permettant de diriger le trafic entre différents réseaux. Ils offrent une capacité de routage élevée et disposent de différentes interfaces pour se connecter à différents types de réseaux.



FIGURE 3.5 – Routeur

### 3.8.4 Un serveur informatique

Informatique est un équipement qui fournit des services accessibles via un réseau, répondant aux requêtes émises par des clients. Dans le contexte du web, un serveur web est spécifiquement conçu pour permettre l’affichage de sites internet via un navigateur web.

Des machines puissantes utilisées pour stocker et gérer les données, les applications et les ressources du réseau. Ils sont dotés de processeurs performants, de mémoire étendue et d’une grande capacité de stockage.

### 3.8.5 Un pare-feu (firewall)

est un outil informatique, matériel et/ou logiciel, qui a pour but de protéger les données d’un réseau en contrôlant les flux de données entrants et sortants, selon des règles de sécurité préalablement définies par l’administrateur.

Des dispositifs de sécurité qui contrôlent et filtrent le trafic réseau entrant et sortant. Ils offrent des fonctionnalités de sécurité avancées telles que la détection d’intrusion et la prévention des attaques, ainsi qu’un débit maximal élevé pour supporter un trafic réseau important.

## 3.9 Problématique

Les sites web sont particulièrement exposés aux attaques et nécessitent une sécurisation rigoureuse. Les menaces courantes incluent les défigurations, où un individu malveillant modifie le contenu légitime du site, et les dénis de service, qui rendent le site inaccessible aux utilisateurs légitimes. Ces attaques peuvent nuire à l’image du propriétaire du site et entraîner des pertes financières.

Il est important de ne pas sous-estimer les attaques plus insidieuses. Un site web compromis peut servir de point d’entrée vers le système d’information de l’hébergeur

ou être utilisé comme relais pour attaquer d'autres systèmes. De plus, il peut être utilisé pour stocker du contenu illégal ou piéger les clients habituels du site.

Ces attaques cherchent à rester discrètes et peuvent passer inaperçues pendant longtemps. La protection contre ces menaces nécessite des mesures préventives et des mécanismes de détection d'attaques.

Comment protéger son site internet ? Comment se prémunir des cyber risques pour sécuriser son site web ? Comment se protéger des cyber-attaques ?

## 3.10 Solution

### 3.10.1 DMZ (Zone démilitarisée)

Nous allons mettre en place une DMZ (zone démilitarisée) sur notre réseau afin de renforcer la sécurité de nos sites web. La DMZ sera un réseau neutre situé entre Internet et notre réseau privé. Au lieu d'exposer directement nos serveurs internes au trafic extérieur, nous avons décidé de déployer des serveurs relais dans la DMZ.

Cette approche nous permettra de masquer la topologie interne de notre réseau et d'avoir un meilleur contrôle sur les flux de données, renforçant ainsi la sécurité de nos sites web. Dans notre architecture, nous autoriserons les flux de données du WAN (wide area network) vers la DMZ et du réseau local vers la DMZ, tout en bloquant les flux du WAN vers le réseau local.

En segmentant notre réseau de cette manière, nous isolerons nos serveurs web et autres services publics dans la DMZ, protégeant ainsi nos machines internes qui contiennent des données sensibles. Nous créerons des VLANs (Virtual Local Area Networks) pour organiser notre réseau en différents groupes de périphériques capables de communiquer entre eux.

Dans notre configuration de la DMZ, nous utiliserons des Private VLANs (Pv-LANs) pour une segmentation encore plus fine du réseau. Par exemple, nous configurerons le VLAN 100 en tant que VLAN principal (private-vlan primary) pour la DMZ. Les VLANs 101 et 102 seront créés en tant que VLANs communautaires (private-vlan community) et isolés (private-vlan isolated), respectivement.

En mettant en place cette DMZ avec une segmentation appropriée et des mécanismes de contrôle des flux de données, nous renforcerons la sécurité de nos sites web. Cela nous permettra de protéger nos serveurs internes, de prévenir les attaques de défiguration ou de déni de service, et de réduire les risques liés à l'utilisation d'un site web compromis.

La sécurité de nos sites web est une priorité absolue, et la mise en place de cette DMZ sera une mesure essentielle pour protéger nos données, préserver notre image de marque et maintenir la confiance de nos utilisateurs.

### 3.10.2 Pare-feu

Nous allons intégrer pfSense dans notre infrastructure pour bénéficier de ses fonctionnalités avancées, notamment pour la gestion du DHCP (Dynamic Host Confi-



guration Protocol) et la redirection du protocole HTTP vers HTTPS.

Tout d'abord, nous allons configurer le serveur DHCP de pfSense afin d'attribuer dynamiquement des adresses IP aux périphériques de notre réseau. Cette approche simplifie considérablement la gestion des adresses IP en automatisant le processus d'assignation, ce qui évite les conflits d'adresses et les erreurs humaines. De plus, le serveur DHCP de pfSense permet la configuration de réservations d'adresses IP pour des périphériques spécifiques, assurant ainsi que ces périphériques obtiennent toujours la même adresse IP.

En ce qui concerne la redirection du protocole HTTP vers HTTPS, nous allons configurer les règles de pare-feu de pfSense pour rediriger automatiquement les requêtes HTTP entrantes vers le protocole HTTPS. Cette mesure garantit que toutes les connexions vers notre site web seront sécurisées en utilisant le chiffrement SSL/TLS. La redirection du trafic HTTP vers HTTPS protège les données des utilisateurs et renforce la confidentialité et l'intégrité des informations échangées.

Grâce à pfSense, nous pourrions facilement configurer ces fonctionnalités en utilisant son interface conviviale. L'interface graphique de pfSense nous permettra de gérer et de surveiller le serveur DHCP, d'ajouter des réservations d'adresses IP, de configurer les règles de pare-feu et de mettre en place la redirection HTTP vers HTTPS en quelques clics.

En utilisant pfSense pour le DHCP et la redirection HTTP vers HTTPS, nous améliorerons la gestion de notre réseau en automatisant la configuration des adresses IP et en garantissant la sécurité des communications web. Ces fonctionnalités contribueront à renforcer la protection de nos données et à offrir une expérience utilisateur plus sécurisée lors de l'accès à nos services en ligne.

### 3.10.3 Certificat SSL

Nous allons sécuriser les communications sur notre serveur Debian en générant un certificat SSL auto-signé. Bien que ce type de certificat ne soit pas reconnu par les autorités de certification, il nous permettra d'établir une connexion sécurisée et chiffrée.

Pour commencer, nous allons nous assurer d'avoir OpenSSL installé sur notre serveur Debian.

Une fois OpenSSL installé, nous suivrons les étapes suivantes pour générer notre certificat auto-signé :

Nous allons générer une clé privée de 2048 bits qui sera utilisée pour signer notre certificat.

Ensuite, nous allons générer le certificat auto-signé. On nous demandera de fournir des informations sur notre entité, telles que le nom du site et l'adresse e-mail. Notre certificat sera valable pendant 365 jours.

Une fois que notre certificat auto-signé est généré, nous l'appliquerons à notre serveur en suivant ces étapes supplémentaires :

Nous allons configurer notre serveur web (dans notre cas, Apache) en modifiant la configuration pour activer le support SSL/TLS et spécifier le chemin vers notre

certificat et notre clé privée. Nous ouvrirons le fichier de configuration SSL d'Apache et modifierons les sections appropriées en indiquant les chemins absolus vers notre certificat et notre clé privée.

Après avoir enregistré les modifications et fermé le fichier, nous activerons le module SSL et le site SSL par défaut.

Enfin, nous redémarrerons Apache pour prendre en compte les modifications.

Une fois terminé, notre site sera accessible via une connexion sécurisée HTTPS en utilisant notre certificat auto-signé.

Il est important de noter que les certificats auto-signés ne sont pas reconnus par les navigateurs web et peuvent générer des avertissements de sécurité pour les utilisateurs. Pour les sites web publics ou ceux impliquant des transactions sensibles, il est recommandé d'obtenir un certificat émis par une autorité de certification reconnue. Les certificats auto-signés sont plus adaptés aux environnements de développement ou aux réseaux internes où la confiance des navigateurs n'est pas un facteur critique.

### 3.10.4 Création des VLANs

Nous allons implémenter plusieurs VLANs (Virtual Local Area Networks) dans notre infrastructure dans le but de segmenter notre réseau et d'améliorer la sécurité, la gestion des ressources et les performances. Chaque VLAN représentera un groupe spécifique de périphériques qui pourront communiquer entre eux. Voici un aperçu des VLANs que nous allons créer, y compris les VLANs privés :

- Le VLAN 10 sera dédié aux Ressources Humaines.
- Le VLAN 11 sera réservé au département Marketing.
- Le VLAN 12 sera destiné à l'équipe Informatique.
- Le VLAN 13 sera spécifiquement conçu pour la Comptabilité et la Finance.
- Le VLAN 14 sera réservé à la Direction et au Management.

Dans notre configuration de la DMZ, nous allons également utiliser des Private VLANs (PvLANs) pour une segmentation plus fine du réseau. Par exemple, nous attribuerons le VLAN 100 en tant que VLAN principal (private-vlan primary) pour la DMZ. Les VLANs 101 et 102 seront créés respectivement en tant que VLANs communautaires (private-vlan community) et VLANs isolés (private-vlan isolated).

Grâce à cette configuration des VLANs, nous pourrions séparer les différents départements, équipes et dispositifs au sein de notre réseau, créant ainsi des zones distinctes qui réduiront les risques de compromission de sécurité et minimiseront les impacts des problèmes potentiels.

Dans l'ensemble, l'implémentation de ces VLANs nous permettra d'améliorer la sécurité, la gestion et les performances de notre réseau. La segmentation logique offerte par les VLANs facilitera la gestion des autorisations d'accès et renforcera la confidentialité des données sensibles.

## 3.11 Conclusion

Ce chapitre dédié à la présentation de l'organisme d'accueil et à la détermination de la problématique liée à la sécurisation d'un serveur web, nous avons pu acquérir une compréhension approfondie de l'environnement dans lequel notre projet se déroule. En soulignant ainsi l'importance de prendre des mesures adéquates pour protéger les données et les ressources de l'organisme.

# Chapitre 4

## Réalisation

### 4.1 Introduction

Ce chapitre sera consacré à la sécurisation d'un serveur web sous Linux, au sein de l'entreprise Générale Emballage. Notre objectif est de décrire les étapes suivies pour garantir la sécurité du site web de Générale Emballage en utilisant des mesures de sécurité appropriées.

### 4.2 Environnement de travail (présentation des outils de travail)

#### 4.2.1 GNS3

GNS3 (Graphical Network Simulator 3) est un logiciel open-source utilisé pour simuler et modéliser des réseaux informatiques. Il permet aux utilisateurs de créer des topologies réseau virtuelles en utilisant des images de routeurs, de commutateurs et d'autres périphériques réseau réels ou virtuels.

GNS3 offre une interface graphique conviviale qui permet de configurer, de connecter et de tester des équipements réseau virtuels, offrant ainsi une plateforme de simulation réaliste pour les professionnels des réseaux et les étudiants en informatique.



FIGURE 4.1 – GNS3

## 4.2.2 VMware Workstation

VMware Workstation est un logiciel de virtualisation qui permet de créer et d'exécuter plusieurs machines virtuelles sur un même ordinateur physique. Il offre aux utilisateurs la possibilité de virtualiser différents systèmes d'exploitation, tels que Windows, Linux, MAC OS, et de les exécuter simultanément sur une seule machine. Il propose des fonctionnalités avancées, telles que la prise en charge de la virtualisation matérielle, la mise en réseau virtuel, la gestion des snapshots, le partage de fichiers entre les machines virtuelles et l'hébergement de serveurs virtuels.

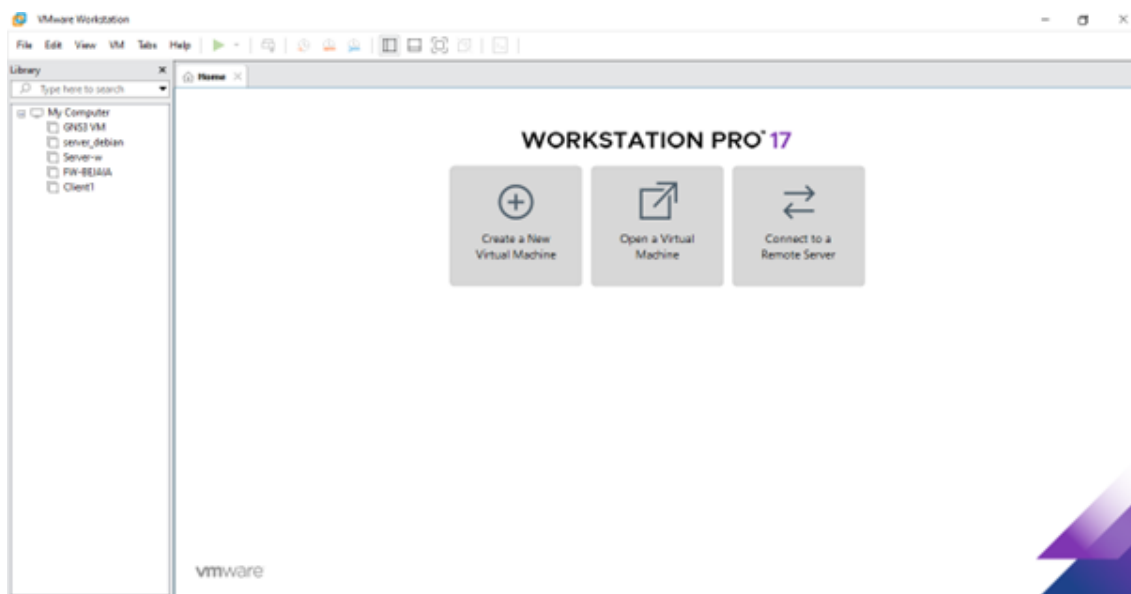


FIGURE 4.2 – L'interface graphique de VMware Workstation pro 17

## 4.2.3 Les machines virtuelles

### 4.2.3.1 Le pfSense

pfSense est un système d'exploitation open source ayant pour but la mise en place de routeur/pare-feu basé sur le système d'exploitation FreeBSD. Il utilise le pare-feu à états Packet Filter ainsi que des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques.

Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. pfSense convient pour la sécurisation d'un réseau domestique ou d'entreprise.

### 4.2.3.2 Dobain 11

Debian 11, également connu sous le nom de code "Bullseye", est la dernière version majeure du système d'exploitation Debian. Debian est une distribution Linux populaire et largement utilisée, connue pour sa stabilité, sa sécurité et sa vaste collection de logiciels. Debian 11 apporte des mises à jour significatives, des améliorations de performances et de nombreuses nouvelles fonctionnalités pour répondre aux besoins des utilisateurs.



FIGURE 4.3 – Debian

## 4.3 Méthodologie

Dans notre architecture, grâce au mode trunk (norme 802.1Q) les trames des différents VLANs sont encapsulées dans une seule trame, ce qui permet de les transmettre efficacement sur le même lien. Cela optimise l'utilisation des ressources réseau en évitant la nécessité d'allouer un lien dédié à chaque VLAN.

### 4.3.1 Gestions des Vlans

#### 4.3.1.1 La configuration des interfaces en mode trunk

Device	interface	Adresse ip	description	passerelle
Switch	E0/0	En mode trunk	Connecter au SW1	//
	E0/1	En mode trunk	Connecter au SW2	//
(Core)	E0/2	En mode trunk	Connecter au SW3	//
	E0/3	En mode trunk	Connecter au Pfsense	//

TABLE 4.1 – Les interfaces en mode trunk

- **la configuration dans les switches :**

Tout abord on utilise la commande `show cdp neighbors` pour afficher des informations sur les périphériques connectés.

```

core
SW4#
SW4#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone,
                  D - Remote, C - CVTA, M - Two-port Mac Relay

Device ID      Local Intrfce   Holdtme    Capability   Platform   Port ID
SW1            Eth 0/0         130        R S I       Linux Uni  Eth 0/0
SW2            Eth 0/1         134        R S I       Linux Uni  Eth 0/0
SW3            Eth 0/2         124        R S I       Linux Uni  Eth 0/0

Total cdp entries displayed : 3
SW4#

```

FIGURE 4.4 – Affichage des interfaces qui sont reliées

- La mise en place de la configuration des interfaces en vue d'utiliser le mode trunk

```

core(config)#interface ethernet 0/0
core(config-if-range)#switchport trunk encapsulation dot1q
core(config-if-range)#switchport mode trunk

```

Répéter ces étapes pour chaque port qu'on souhaite configurer en mode trunk.

```

SW4#show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Et0/0    on        802.1q         trunking    1
Et0/1    on        802.1q         trunking    1
Et0/2    on        802.1q         trunking    1
Et0/3    on        802.1q         trunking    1

SW1#show interface trunk
Port      Mode      Encapsulation  Status      Native vlan
Et0/0    on        802.1q         trunking    1

```

FIGURE 4.5 – Verification des interfaces

#### 4.3.1.2 Configuration de vlan Trunking Protocol (VTP)

Le VTP (VLAN Trunking Protocol) facilite la gestion des VLAN en offrant trois modes de configuration :

1. **Mode serveur** : Dans ce mode, les commandes de configuration des VLAN sont centralisées dans le switch de distribution. Les modifications effectuées sur le switch de distribution sont propagées aux autres switches du réseau VTP, y compris les switches d'accès.
2. **Mode client** : Les switches d'accès sont configurés en mode client pour recevoir et appliquer la configuration des VLAN provenant du switch de distribution en mode serveur. Les switches d'accès ne peuvent pas effectuer de modifications sur la configuration des VLAN.

3. **Mode transparence** : Les switches en mode transparence ne participent pas activement à la propagation des informations de configuration des VLAN. Ils retransmettent simplement les messages VTP reçus aux autres switches, mais n'appliquent pas ces informations sur leurs propres VLAN. Les modifications de configuration des VLAN doivent être effectuées manuellement sur chaque switch en mode transparence.

- **Configuration de VTP serveur**

```
core#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
core(config)#vtp mode server
Device mode already VTP Server for VLANS.
core(config)#vtp password cisco1234
Setting device VTP password to cisco1234
core(config)#vtp domain ge.vtp
Changing VTP domain name from NULL to ge.vtp
core(config)#vtp version 2
core(config)#vtp pruning
Pruning switched on
core(config)#exit
```

- **Configuration de VTP client**

```
SW1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
SW1(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
SW1(config)#vtp password cisco1234
Setting device VTP password to cisco1234
SW1(config)#vtp domain ge.vtp
Changing VTP domain name from NULL to ge.vtp
SW1(config)#vtp version 2
SW1(config)#exit
```

#### 4.3.1.3 Création configuration des vlans

Nom vlans	IP vlans	Réseau/préfixe
RH	10	192.168.10.0/24
MRK	11	192.168.11.0/24
INFO	12	192.168.12.0/24
CF	13	192.168.13.0/24
Manager	14	192.168.14.0/24
Native	66	////////////////////

TABLE 4.2 – Tableau des Vlans



Une fois que le serveur VTP est configuré avec les VLAN souhaités, il va diffuser cette configuration aux switches clients VTP. Les switches clients VTP recevront alors les informations de configuration des VLAN provenant du serveur et les appliqueront localement sur leurs propres switches.

Cela signifie que les clients VTP n'ont pas besoin de créer manuellement les VLAN, car ils recevront automatiquement la configuration depuis le serveur VTP. Cela simplifie la création et la gestion des VLAN dans le réseau, car les modifications effectuées sur le serveur VTP sont propagées aux clients VTP de manière automatique.

- **création des vlans sur le switch core**

```
core(config)#vlan 10
core(config-vlan)#name RH
core(config-vlan)#vlan 11
core(config-vlan)#name MARK
core(config-vlan)#vlan 12
core(config-vlan)#name INFO
core(config-vlan)#vlan 13
core(config-vlan)#name CF
core(config-vlan)#vlan 14
core(config-vlan)#name Manager
core(config-vlan)#vlan 66
core(config-vlan)#name native
```

- **La vérification des vlans créés sur les switches**

Vérification de la création des vlans avec la commande **Show vlan brief**

```
SW4#show vlan brief
VLAN Name                Status    Ports
-----
1    default                active    Et1/0, Et1/1, Et1/2, Et1/3
                    Et2/0, Et2/1, Et2/2, Et2/3
                    Et3/0, Et3/1, Et3/2, Et3/3
10   RH                    active
11   MARK                 active
12   INFO                 active
13   CF                   active
14   Manager              active
66   native               active
1002 fddi-default         act/unsup
1003 trcrf-default      act/unsup
1004 fddinet-default    act/unsup
1005 trbrf-default      act/unsup
```

FIGURE 4.6 – Affichage des vlans

Tous les VLANs définis sur le serveur VTP seront également présents sur les clients VTP. Cela permet d'assurer une cohérence et une gestion centralisée des VLANs dans le réseau.

- Mise en place de la configuration pour le VLAN native et les VLAN autorisées sur une connexion de tronc (trunk).

```
core(config)#interface range eth0/0-2
core(config-if-range)#switchport trunk native vlan 66
core(config-if-range)#switchport trunk allowed vlan 10-14,66
```

Répéter ces étapes pour chaque port sur une connexion trunk.

```
SW4#show interface trunk

Port      Mode           Encapsulation  Status        Native vlan
Et0/0     on             802.1q         trunking      66
Et0/1     on             802.1q         trunking      66
Et0/2     on             802.1q         trunking      66
Et0/3     on             802.1q         trunking      1

Port      Vlans allowed on trunk
Et0/0     10-14,66
Et0/1     10-14,66
Et0/2     10-14,66
Et0/3     1-4094

Port      Vlans allowed and active in management domain
Et0/0     10-14,66
Et0/1     10-14,66
Et0/2     10-14,66
Et0/3     1,10-14,66

Port      Vlans in spanning tree forwarding state and not pruned
Et0/0     none
Et0/1     10-14,66
Et0/2     10-14,66
Et0/3     1,10-14,66
SW4#
```

FIGURE 4.7 – Affichage des VLANs autorisés à traverser

- Affectation des ports pour les Vlan en mode accès

Device	interface	Adresse ip	description	passerelle
Switch (SW1)	E3/3	En mode accès	connecter au PC1	//
	E3/2	En mode accès	connecter au PC2	//
Switch (SW2)	E3/3	En mode accès	connecter au PC3	//
	E3/2	En mode accès	connecter au PC4	//
Switch (SW3)	E3/3	En mode accès	connecter au PC5	//
	E3/2	En mode accès	connecter au PC6	//

TABLE 4.3 – Les interfaces en mode accès

```
SW1(config)#interface eth3/2
SW1(config-if-range)#switchport mode access
SW1(config-if-range)#switchport access vlan 14
```

Répéter ces étapes pour chaque port qu'on souhaite configurer en mode accès et pour chaque VLAN auquel on souhaite les associer.

VLAN Name	Status	Ports
1 default	active	Et0/1, Et0/2, Et0/3, Et1/0 Et1/1, Et1/2, Et1/3, Et2/0 Et2/1, Et2/2, Et2/3, Et3/0 Et3/1
10 RH	active	
11 MARK	active	
12 INFO	active	
13 CF	active	
14 Manager	active	Et3/2, Et3/3
66 native	active	

VLAN Name	Status	Ports
1 default	active	Et0/1, Et0/2, Et0/3, Et1/0 Et1/1, Et1/2, Et1/3, Et2/0 Et2/1, Et2/2, Et2/3, Et3/0 Et3/1
10 RH	active	
11 MARK	active	
12 INFO	active	Et3/2
13 CF	active	Et3/3
14 Manager	active	
66 native	active	

VLAN Name	Status	Ports
1 default	active	Et0/1, Et0/2, Et0/3, Et1/0 Et1/1, Et1/2, Et1/3, Et2/0 Et2/1, Et2/2, Et2/3, Et3/0 Et3/1
10 RH	active	Et3/2
11 MARK	active	Et3/3
12 INFO	active	
13 CF	active	
14 Manager	active	

FIGURE 4.8 – Affectation des ports pour les Vlan en mode accès

### 4.3.2 Configuration de Switch DMZ

Device	interface	Adresse ip	description	passerelle
Sw-DMZ	Eth0/0	primary	Pfsense	//
	Eth0/1	community	Web	//
	Eth0/2	community	MySQL	//
	Eth0/3	isolated	Voice	//

TABLE 4.4 – Mode des interfaces de Sw-DMZ

Les commandes ci-dessus configurent les VLANs privés et leurs associations sur le commutateur Sw-DMZ, avec une interface en mode promiscuous et d'autres interfaces en mode hôte associées aux VLANs spécifiés.

```
Sw-DMZ(config)#vtp mode transparent
Setting device to VTP Transparent mode for VLANS.
Sw-DMZ(config)#vlan 100
Sw-DMZ(config-vlan)#private-vlan primary
Sw-DMZ(config-vlan)#private-vlan association 101,102
Sw-DMZ(config-vlan)#exit

Sw-DMZ(config)#vlan 101
Sw-DMZ(config-vlan)#private-vlan community
Sw-DMZ(config-vlan)#exit
```

```
Sw-DMZ(config)#vlan 102
Sw-DMZ(config-vlan)#private-vlan isolated
Sw-DMZ(config-vlan)#exit
```

```
Sw-DMZ(config)#interface eth 0/0
Sw-DMZ(config-if)#switchport mode private-vlan promiscuous
Sw-DMZ(config-if)#switchport private-vlan mapping 100 101,102
Sw-DMZ(config-if)#exit
```

```
Sw-DMZ(config)#interface range eth 0/1-2
Sw-DMZ(config-if-range)#switchport mode private-vlan host
Sw-DMZ(config-if-range)#switchport private-vlan host-association 100 101
Sw-DMZ(config-if-range)#exit
```

```
Sw-DMZ(config)# Sw-DMZ(config)#interface eth 0/3
Sw-DMZ(config-if)#switchport mode private-vlan host
Sw-DMZ(config-if)#switchport private-vlan host-association 100 102
Sw-DMZ(config-if)#end
```

### 4.3.3 La Configuration de PfSense

#### 1. Methodes d'accès à PfSense

Accéder à l'interface web de pfSense en ouvrant un navigateur et en entrant l'adresse IP attribuée à l'interface LAN de pfSense dans la barre d'adresse.

On se connecte à l'interface web en utilisant les identifiants d'administrateur.

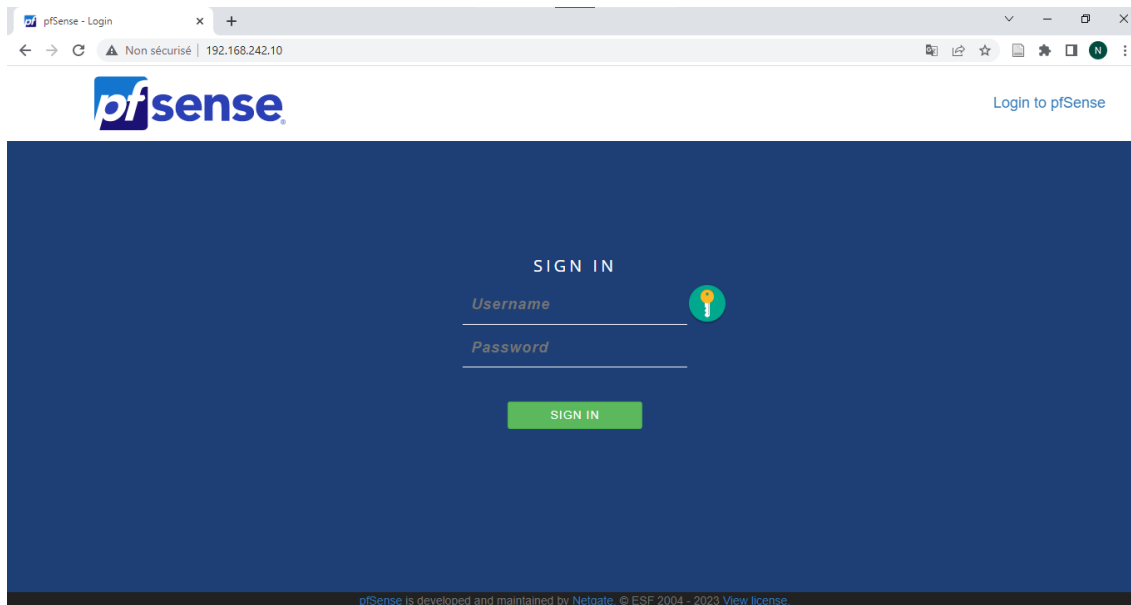


FIGURE 4.9 – Accés en mode interface graphique

Dès la saisi du nom d'utilisateur et du mot passe, la page d'accueil de PfSense s'affiche comme suite :

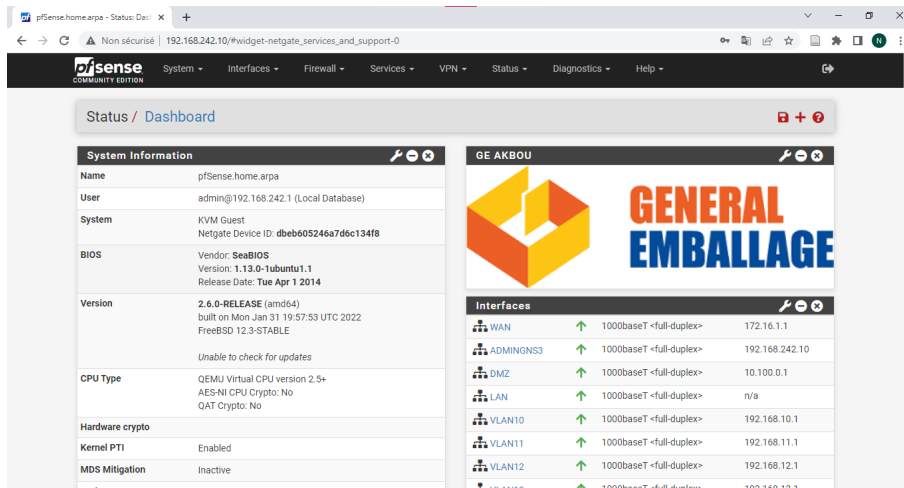


FIGURE 4.10 – Page d'accueil de PfSense

## 2. Création des interfaces

Dans le menu principal, on clique sur "Interfaces" pour accéder à la page de gestion des interfaces. Sur cette page, on clique sur le bouton "Ajouter" pour créer une nouvelle interface. On choisit le type d'interface en fonction de nos besoins, comme "LAN" pour le réseau local, "WAN" pour la connexion Internet étendue, ou "OPTx" pour les interfaces supplémentaires.

Dans les interfaces supplémentaires, on ajoute l'interface vers la DMZ en choisissant le type d'interface approprié, tel que "OPT" ou "DMZ". Ensuite, on configure les paramètres spécifiques de l'interface, tels que l'adresse IP, le masque de sous-réseau et les options de sécurité. Après avoir rempli les informations requises, on enregistre l'interface.

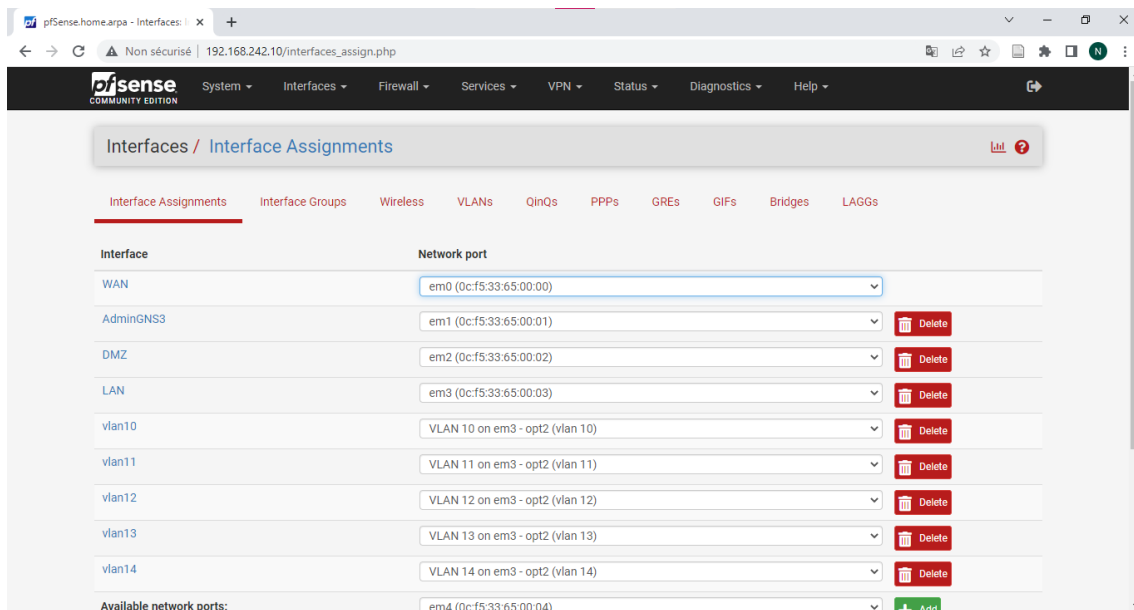


FIGURE 4.11 – interface Assignments

### 3. Création des vlans

Pour créer un VLAN dans pfSense, On choisit le type d'interface "VLAN" pour créer un VLAN spécifique. Les paramètres du VLAN, tels que le numéro du VLAN, le nom du VLAN et l'interface parente associée, sont configurés selon les besoins. Enfin, on enregistre les modifications pour créer le VLAN. Cette méthode permet à l'utilisateur de créer facilement des VLAN personnalisés dans pfSense afin de segmenter et gérer le trafic de manière efficace au sein du réseau.

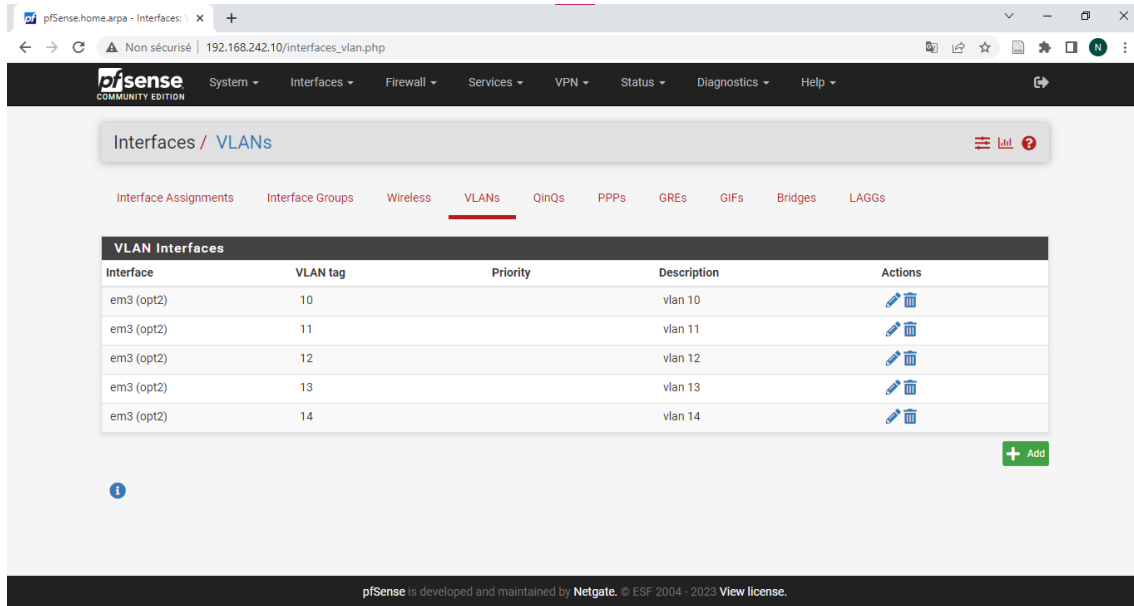


FIGURE 4.12 – les vlans dans PfSense

Une fois les VLAN créés dans pfSense, on a la possibilité de configurer les règles de pare-feu, les passerelles, les options DHCP, et bien d'autres fonctionnalités pour chaque VLAN individuellement. Cela permet de contrôler de manière précise le trafic et la connectivité entre les différents VLAN et les autres interfaces de pfSense.

### 4. Autoriser le DHCP pour chaque vlan

Pour autoriser le service DHCP dans pfSense, on se rend dans le menu principal et on sélectionne "Services", puis "DHCP Server" dans le sous-menu. Sur la page de configuration du serveur DHCP, on choisit l'interface désirée dans le menu déroulant. En cochant la case "Enable DHCP server on [interface]", on active le service DHCP pour cette interface spécifique. On peut ensuite configurer les paramètres du serveur DHCP, tels que le pool d'adresses IP, le masque de sous-réseau, la passerelle par défaut et les serveurs DNS. Une fois les modifications effectuées, on enregistre les changements pour activer le service DHCP. Cela permettra à pfSense de distribuer automatiquement les adresses IP aux périphériques connectés à cette interface, simplifiant ainsi la gestion du réseau.

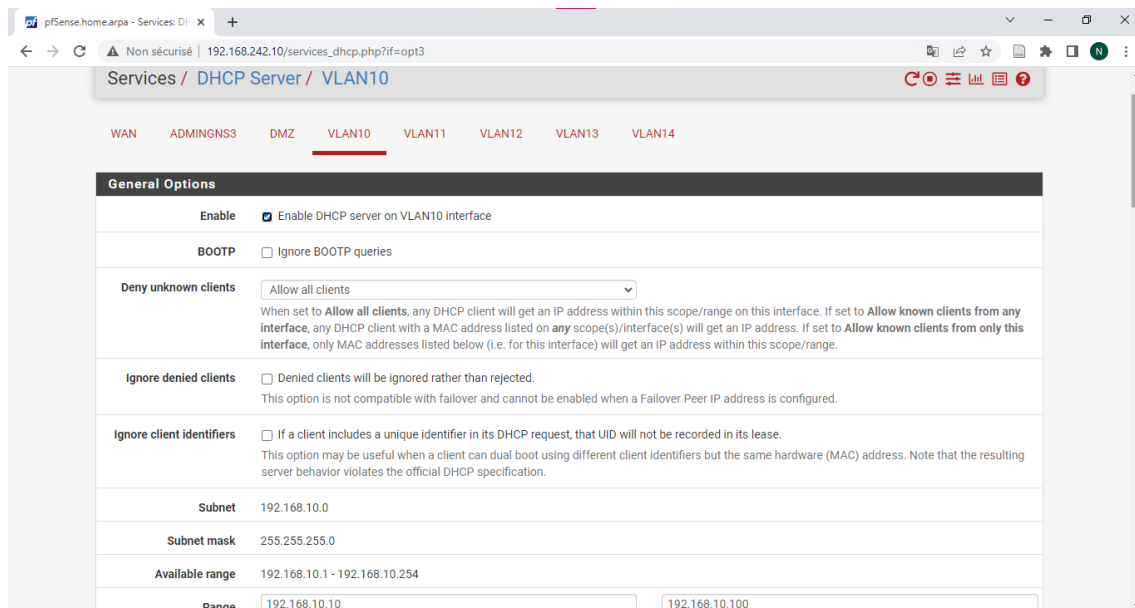


FIGURE 4.13 – Le DHCP dans les vlans

## 5. Crée une redirection de http vers Https

Pour rediriger le trafic de HTTP vers HTTPS dans pfSense, vous pouvez configurer une règle de redirection en suivant ces étapes :

Accédez au menu "Firewall" et sélectionnez "NAT". Choisissez ensuite l'option "Port Forward" pour accéder à la configuration des règles de redirection. Ajoutez une nouvelle règle de redirection en spécifiant les paramètres suivants : choisissez l'interface appropriée, le protocole TCP, le port source 80 pour HTTP, l'adresse de destination du pfSense lui-même, le port de destination 443 pour HTTPS.

Cochez les cases "Rediriger l'adresse IP" et "Rediriger le port" pour utiliser les valeurs par défaut du pfSense.

Enregistrez la règle de redirection pour activer la redirection de HTTP vers HTTPS.

Une fois la règle de redirection configurée, tout le trafic entrant sur le port 80 sera automatiquement redirigé vers le port 443, assurant ainsi une communication sécurisée via HTTPS.

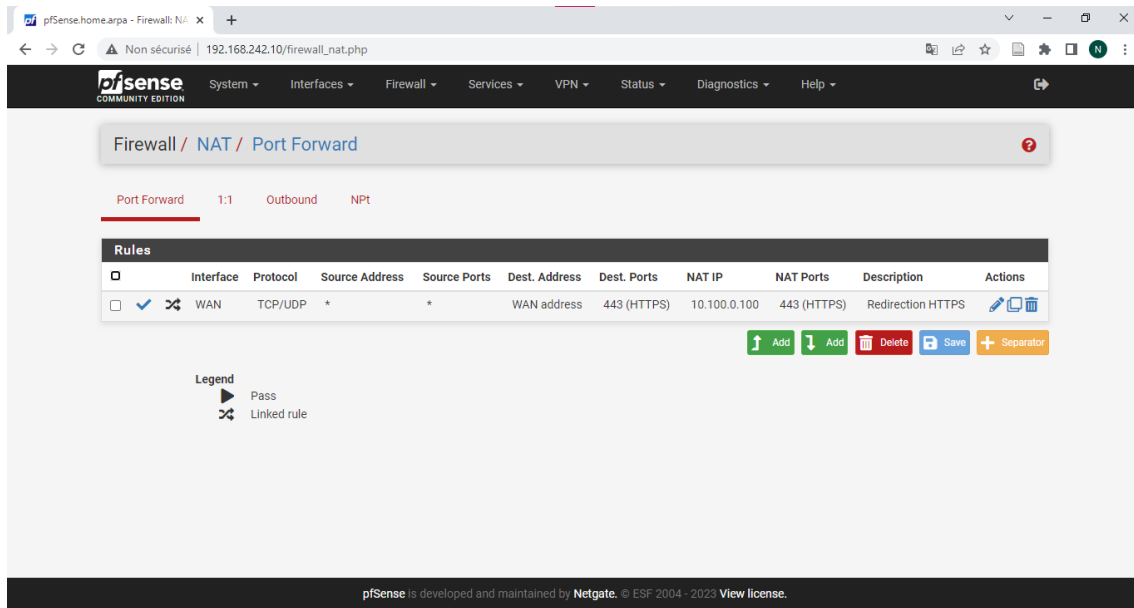


FIGURE 4.14 – La redirection

## 6. Vérification des interfaces ajoutées

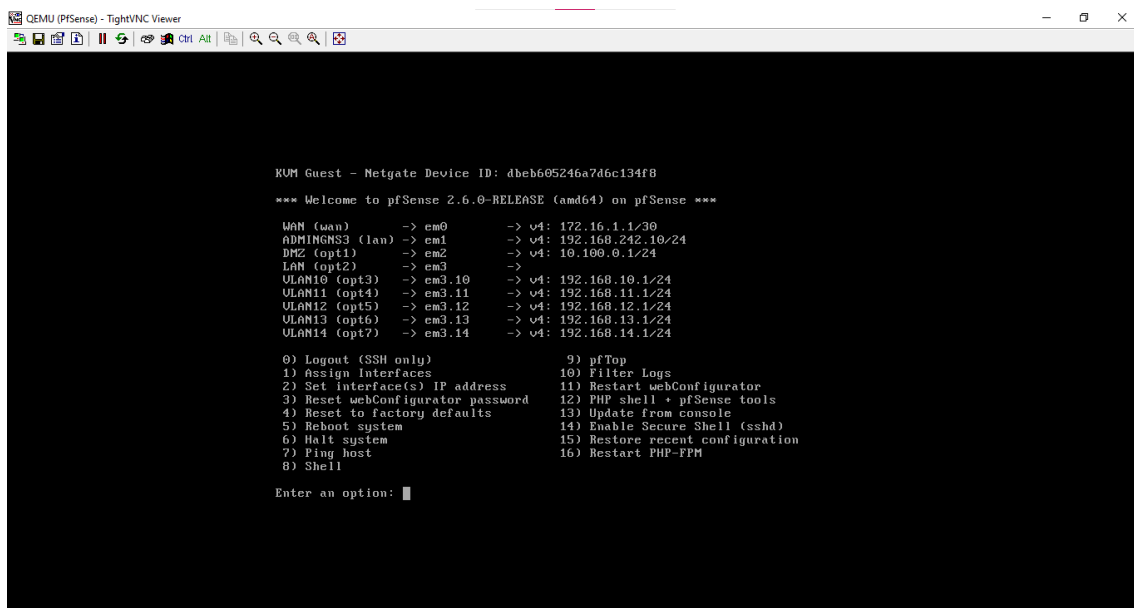


FIGURE 4.15 – Affichage des interfaces



## 4.3.4 La configuration du Serveur WEB

### 4.3.4.1 Attribuer une adresse IP statique

On attribue une adresse IP statique à un serveur Debian en utilisant l'interface graphique. Tout d'abord, on recherche l'option "Réseau" ou "Connexions réseau" dans le Centre de contrôle. Ensuite, on repère l'interface réseau spécifique à laquelle on souhaite assigner une adresse IP statique, puis on effectue un clic droit dessus et on sélectionne l'option "Propriétés" ou "Configurer". Dans la fenêtre de configuration, on recherche l'onglet ou l'option liée aux paramètres IP ou IPv4. On choisit ensuite l'option pour spécifier une adresse IP statique et on entre les informations requises, comme l'adresse IP souhaitée, le masque de sous-réseau et la passerelle par défaut. Après avoir enregistré les modifications et fermé la fenêtre de configuration, il est recommandé de redémarrer le service réseau pour que les changements prennent effet.

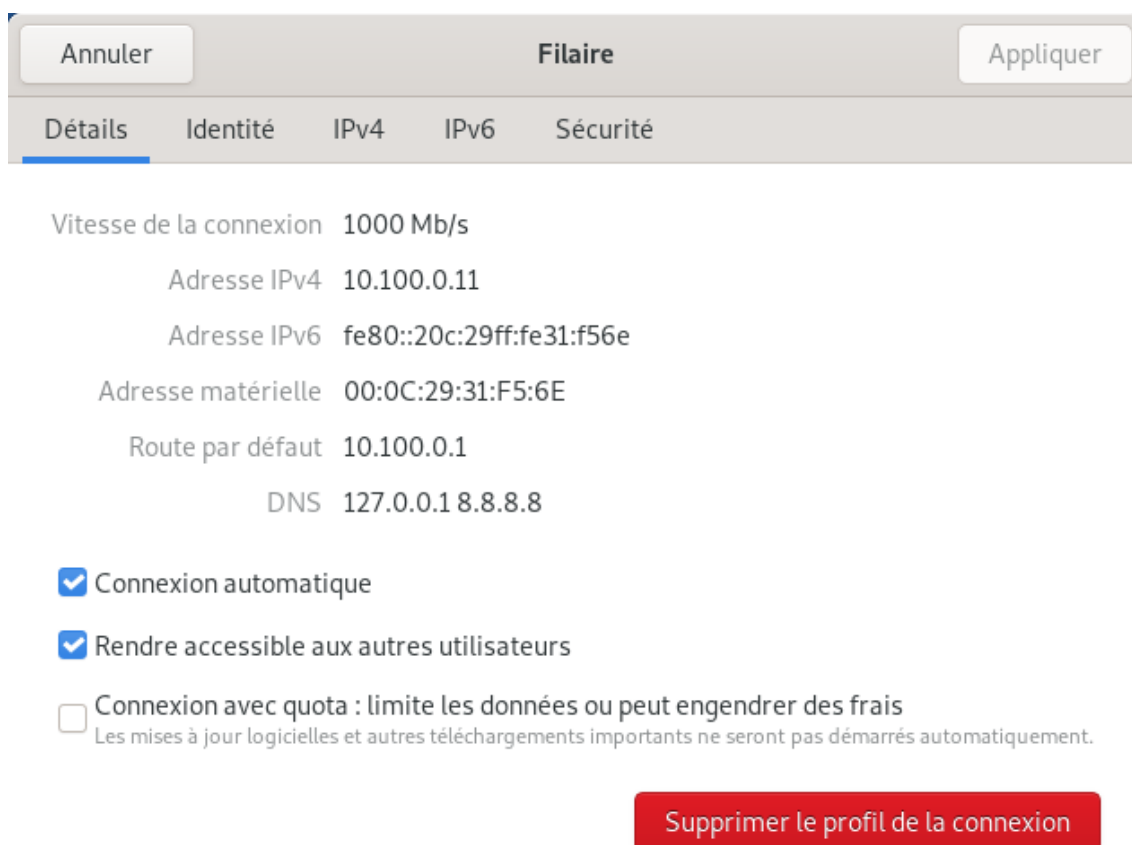


FIGURE 4.16 – Configuration de serveur

#### 4.3.4.2 Ajouter l'utilisateur "web" en tant qu'administrateur

Pour ajouter l'utilisateur "web" en tant qu'administrateur dans le fichier sudoers sur un serveur Debian, on se connecte au serveur en tant qu'utilisateur disposant des droits d'administration. Ensuite, dans le terminal, on exécute la commande "sudo visudo" pour ouvrir le fichier sudoers en mode sécurisé. À l'intérieur du fichier, on recherche la section qui concerne les autorisations des utilisateurs et des groupes. On ajoute alors la ligne "**web ALL=(ALL :ALL) ALL**" juste en dessous de la ligne "**root ALL=(ALL :ALL) ALL**". Après avoir vérifié la syntaxe du fichier, on le sauvegarde. Désormais, l'utilisateur "web" aura les privilèges nécessaires pour utiliser la commande sudo avec des privilèges d'administrateur.

#### 4.3.4.3 Installation de SSH (Secure Shell)

Pour installer le service SSH (Secure Shell). On exécute les commandes "**sudo apt update**" pour mettre à jour les paquets du système, puis "**sudo apt install openssh-server**" pour installer le paquet OpenSSH Server. Pendant l'installation, on peut être invité à fournir un mot de passe. Une fois l'installation terminée, le service SSH sera opérationnel et on pourra se connecter au serveur en utilisant un client SSH et les informations d'identification appropriées. Il est recommandé de prendre des mesures de sécurité supplémentaires, telles que la désactivation de l'accès root distant et l'utilisation de l'authentification par clé publique, pour renforcer la sécurité de la connexion SSH.

#### 4.3.4.4 Installation de apache

Pour installer Apache sur Debian, on peut utiliser la commande suivante dans le terminal :**sudo apt-get install apache2**

Cela va télécharger et installer Apache sur le système. Une fois l'installation terminée, Apache sera automatiquement démarré et prêt à l'emploi. On peut vérifier si Apache fonctionne en ouvrant un navigateur et en accédant à l'adresse IP du serveur Debian. Si tout est configuré correctement, la page par défaut d'Apache s'affichera.

```
server-w@WEB:~$ sudo su
[sudo] Mot de passe de server-w :
root@WEB:/home/server-w# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor prese
   Active: active (running) since Fri 2023-06-09 17:53:40 CEST; 4min 14s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 547 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUC
 Main PID: 595 (apache2)
    Tasks: 55 (limit: 2264)
   Memory: 20.8M
      CPU: 270ms
   CGroup: /system.slice/apache2.service
           └─595 /usr/sbin/apache2 -k start
             └─599 /usr/sbin/apache2 -k start
               └─600 /usr/sbin/apache2 -k start

juin 09 17:53:39 WEB systemd[1]: Starting The Apache HTTP Server...
juin 09 17:53:40 WEB apachectl[571]: AH00558: apache2: Could not reliably deter
juin 09 17:53:40 WEB systemd[1]: Started The Apache HTTP Server.
lines 1-17/17 (END)
```

FIGURE 4.17 – vérification de l'activation de apache2

#### 4.3.4.5 Créer un nom de domaine

Pour créer une entrée dans le fichier hosts sur un serveur Debian, on accède au fichier hosts en utilisant un éditeur de texte tel que Nano. On ouvre un terminal en tant qu'utilisateur disposant des droits d'administration et on exécute la commande "**sudo nano /etc/hosts**" pour ouvrir le fichier. On ajoute une nouvelle ligne en spécifiant l'adresse IP et le nom d'hôte que l'on souhaite associer dans notre cas "**generalemballage.org**".

```
server-w@WEB:~$ sudo nano /etc/hosts
GNU nano 5.4 /etc/hosts
127.0.0.1    localhost
127.0.1.1    WEB
10.100.0.11 WEB, generalemballage.org, www.generalemballage.org
# The following lines are desirable for IPv6 capable hosts
::1         localhost ip6-localhost ip6-loopback
ff02::1     ip6-allnodes
ff02::2     ip6-allrouters

[ Lecture de 8 lignes ]
^G Aide      ^O Écrire    ^W Chercher  ^K Couper    ^T Exécuter  ^C Emplacement
^X Quitter   ^R Lire fich.^N Remplacer  ^U Coller    ^J Justifier ^_ Aller ligne
```

FIGURE 4.18 – Création d'un nom de Domain

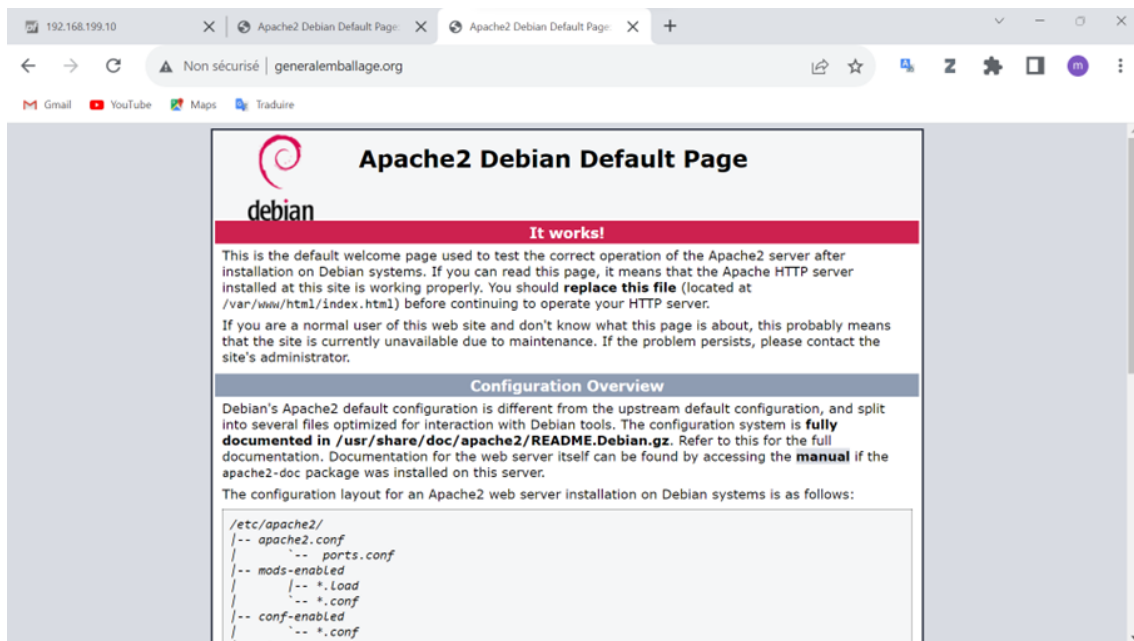


FIGURE 4.19 – Accéder à la page de apache avec generalemballage.org

#### 4.3.4.6 Héberger un site web

Pour ajouter le contenu du site "**generalembalage.org**", on doit placer les fichiers du site web dans le répertoire racine spécifié dans la configuration du serveur web. Par défaut, dans le cas d'Apache, le répertoire racine est `/var/www`. Il faut donc s'assurer que les fichiers du site web sont correctement organisés dans ce répertoire. On utilise le terminal pour copier les fichiers vers le répertoire racine avec la commande :

```
sudo cp -r /chemin/vers/fichiers /var/www
```

dans notre cas :

```
sudo cp -r generalemballage.org/ /var/www
```

#### 4.3.4.7 Créer un fichier d'hôte virtuel (Virtual Host)

Pour créer un fichier d'hôte virtuel (Virtual Host) dans Apache sur un serveur Debian, voici les étapes à suivre :

1. On accède au répertoire des fichiers de configuration Apache en utilisant la commande suivante :  
`cd /etc/apache2/sites-available`
2. On crée un nouveau fichier de configuration pour l'hôte virtuel en utilisant un éditeur de texte, par exemple :  
`sudo nano generalemballage.org.conf`
3. Dans le fichier de configuration, on spécifie les directives appropriées pour l'hôte virtuel, comme le nom de domaine, le répertoire racine du site web, les options de configuration, etc. Voici la configuration pour notre hôte virtuel :

```

<VirtualHost *:80>
  ServerName generalemballage.org
  ServerAlias www.eneralemballage.org
  DocumentRoot /var/www/generalemballage.org
  <Directory /var/www/generalemballage.org>
    Require all granted
  </Directory>
</VirtualHost>

```

On enregistre le fichier de configuration et on quitte l'éditeur de texte.

4. On active le fichier d'hôte virtuel en créant un lien symbolique vers le répertoire des sites activés puis On redémarre le service Apache pour appliquer les modifications

```

sudo a2ensite generalemballage.org.conf
sudo service apache2 restart

```

Une fois ces étapes terminées, l'hôte virtuel est configuré et prêt à servir le site web.

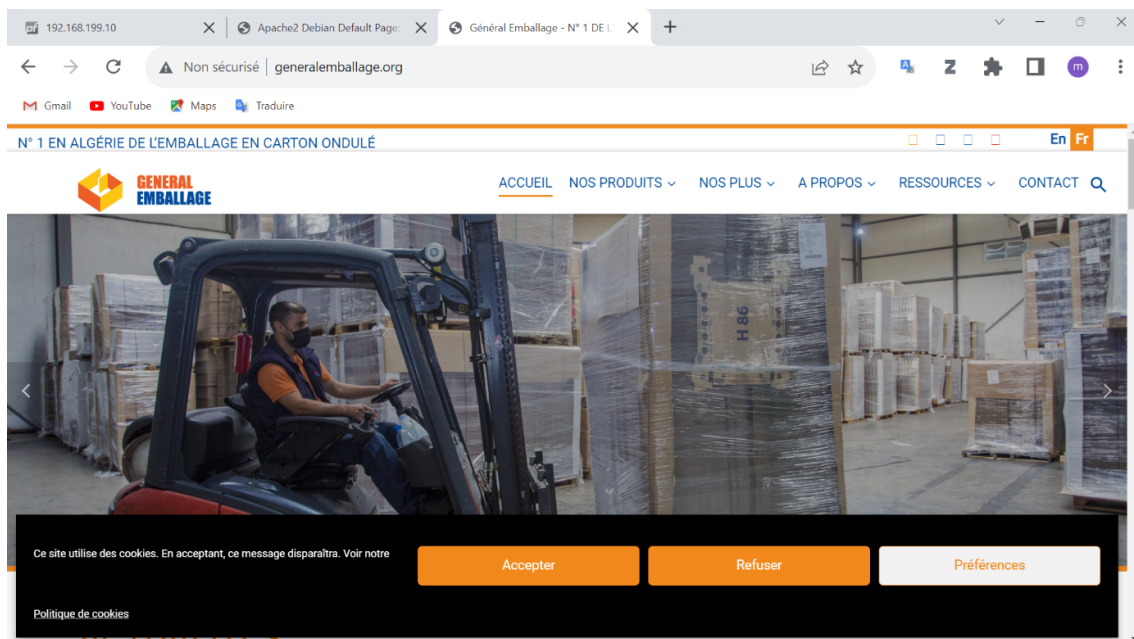


FIGURE 4.20 – Test de l'ouverture de site

#### 4.3.4.8 Sécurisation serveur apache

##### 1. Installation de ssl

Pour installer SSL sur le serveur Debian, voici les étapes à suivre :

On installe le package OpenSSL nécessaire à la gestion des certificats SSL en utilisant la commande suivante :

```
sudo apt-get install openssl
```



```
server-w@WEB: ~  
server-w@WEB:~$ openssl version  
OpenSSL 1.1.1n 15 Mar 2022  
server-w@WEB:~$ █
```

FIGURE 4.21 – vérification de l'installation de ssl

##### 2. générer un certificat SSL auto-signé

- (a) on commence par créer un sous dossier SSL "generalemballage.org" à l'aide de la commande :

```
root@web-server:/etc/ssl# sudo mkdir generalemballage.org
```

- (b) On doit aussi créer un sous dossier generalemballage.org "private" pour stocker la clé privée à l'aide de la commande :

```
root@web-server:/etc/ssl/generalemballage.org#  
sudo mkdir private
```

- (c) Pour générer un certificat SSL auto-signé, peut utiliser la commande suivante :

```
root@web-server:/etc/ssl/generalemballage.org#  
openssl req -x509 -nodes -days 365 -newkey  
rsa:2048 -keyout private/generalemballage.org.key  
-out generalemballage.org.crt
```

- **Openssl** : générer le certificat CRC auto signé.
- **req-x509** : permet de faire un certificat.
- **nodes** : notre certificat n'est pas coder par un mot de passe.
- **newkey rsa 2048** : nouvelle clé privé qui va utiliser l'algorithme rsa : 2048.
- **keyout** : permet de préciser ou nous voulons stoker la nouvelle clé privé.
- **out** : permet de préciser le nom de fichier ou on trouve le certificat CRS.

On active le module SSL dans Apache et on le redémarre pour appliquer les modifications en utilisant les commandes suivante :

```
sudo a2enmod ssl  
sudo service apache2 restart
```

```
server-w@WEB: ~
root@WEB:/etc/ssl/generalemballage.org# cat generalemballage.org.crt
-----BEGIN CERTIFICATE-----
MIIEBTCCAu2gAwIBAgIUUbXIAafoUo4z5S2sfGWJIIx9imEwDQYJKoZIhvcNAQEL
BQAwgZExCzAJBgNVBAYTAkRaMQ8wDQYDVQQIDAZCRUpBSUExDjAMBGNVBAcMBUFL
Qk9VMRkwFwYDVQQKDBBHRU5FUkFMRU1CQUxMQUdFMR0wGwYDVQQDDBRnZW5lcmFs
ZW1iYWxsYWdlLm9yZzEnMCUGCSqGSIB3DQEJARYYbGF0YmlyXppZ2g2QGhvdG1h
aWwuyY29tMB4XDTEzMDUwNTE4NTczMVoXDTI0MDUwNDE4NTczMVoVowgZExCzAJBgNV
BAYTAkRaMQ8wDQYDVQQIDAZCRUpBSUExDjAMBGNVBAcMBUFLQk9VMRkwFwYDVQQK
DBBHRU5FUkFMRU1CQUxMQUdFMR0wGwYDVQQDDBRnZW5lcmFsZW1iYWxsYWdlLm9y
ZzEnMCUGCSqGSIB3DQEJARYYbGF0YmlyXppZ2g2QGhvdG1haWwuyY29tMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxzGSCjkZRHyXwSwgtMrfzbIG0cTE
FPH7VRT/at7KGuJgrD/+JhkTKIcZ+ctawLAjsz8UqPvyjkIMjReiejMdo3I0jZCI
qliIoJlXpRiB8xk/Qyb25DYSQNofdnBBNGSB7fpeT0w0ozilqRqg8m/qkSLLKS
GL5s2Q3NpQmbHtBxjstXpNhhn+2mpdJCJ4P1tbVbYnrlBF6wepSFZRZ3AGLD3oh
8zysbwRGRy31RWyCr+mjP9btY15xPmLX229jH6pyBSXbP8lFVlsrMmMfQHph6t5K
DFTPa0De3qyW+++EabniQ8Be8go8uqKBjgHrsRdqpeK7iUASmbkKrCeYnwIDAQAB
o1MwUTADBgNVHQ4EFgQUtPrKvGl8jRapHfyJTeBIevyweIwHwYDVR0jBBgwFoAU
tPrKvGl8jRapHfyJTeBIevyweIwDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0B
AQsFAAOCAQEAvxVa81wdDa4GikT5yVYmS/mFsdvYB+z4yn4r0xtyUC5sDpTxcdNr
JJZwYQwx2P0widS3PG5NNSQJm8A0y7LRDiDMhaWxAK2+MZcMYX95wTkxKFne/y8GS
/ToROVfd7zLZVwhDhUe1SLDU5IWZVTBntuF4FBj7tyyyI9wBw689GHLA6Rpx8P+
Fxtct2LYsfZ1b1C10VmBNVfVbuSraaapzPAATBUNH9V8NM/GmQQRDGYVP9VHAQqo
HnD08wDuEMekhiVYUcgCJ3V5uu56wZsYdUki7AsfihaUIVYIrYN6qT8Fscf61l5e
XF1Juf2TT2wmkt+iZqX6NASGU3+qhmUA8w==
-----END CERTIFICATE-----
root@WEB:/etc/ssl/generalemballage.org#
```

FIGURE 4.22 – Affichage du certificat

Une fois ces étapes terminées, SSL sera installé sur votre serveur Debian. Vous pouvez ensuite configurer Apache pour utiliser le certificat SSL dans les fichiers de configuration appropriés, tels que les fichiers de site virtuel, afin de sécuriser les connexions HTTPS.

### 3. Appliquer la certificat sur Hôte virtuelle

On ouvre le fichier de configuration du site virtuel dans le répertoire `/etc/apache2/sites-available`. On ajoute les directives suivantes pour activer SSL :

```
<VirtualHost *:443>
  ServerName generalemballage.org
  ServerAlias www.generalemballage.org
  DocumentRoot /var/www/generalemballage.org
  <Directory /var/www/generalemballage.org>
    Require all granted
  </Directory>
  SSLEngine on
  SSLCertificateFile
  /etc/ssl/generalemballage.org/generalemballage.org.crt
  SSLCertificateKeyFile
  /etc/ssl/generalemballage.org/private/generalemballage.org.key
</VirtualHost>
```

Une fois que apache redémarrer et les modifications de configuration sont appliquer, Les connexions vers cette hôte virtuelle seront sécurisées à l'aide du certificat SSL.

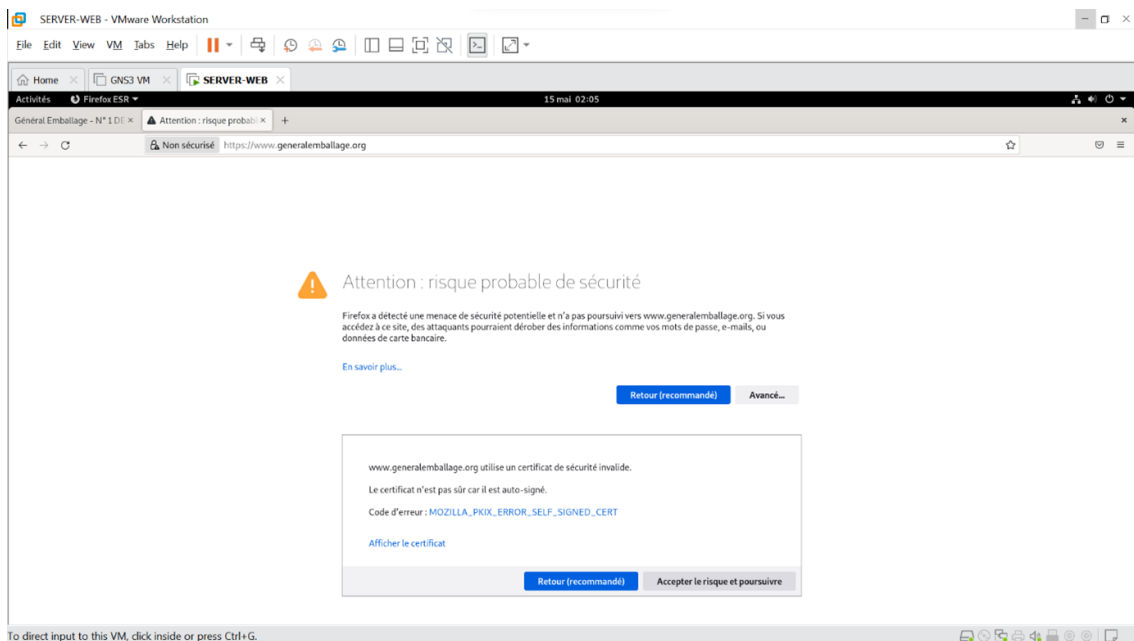


FIGURE 4.23 – test de l'ouverture avec https



Il est important de noter que les certificats SSL auto-signés ne sont pas considérés comme des certificats de confiance par les navigateurs web, ce qui signifie que les utilisateurs verront un avertissement de sécurité lorsqu'ils accèdent à votre site. Pour obtenir un certificat SSL valide et reconnu par les navigateurs, vous devrez acheter un certificat auprès d'une autorité de certification (CA).

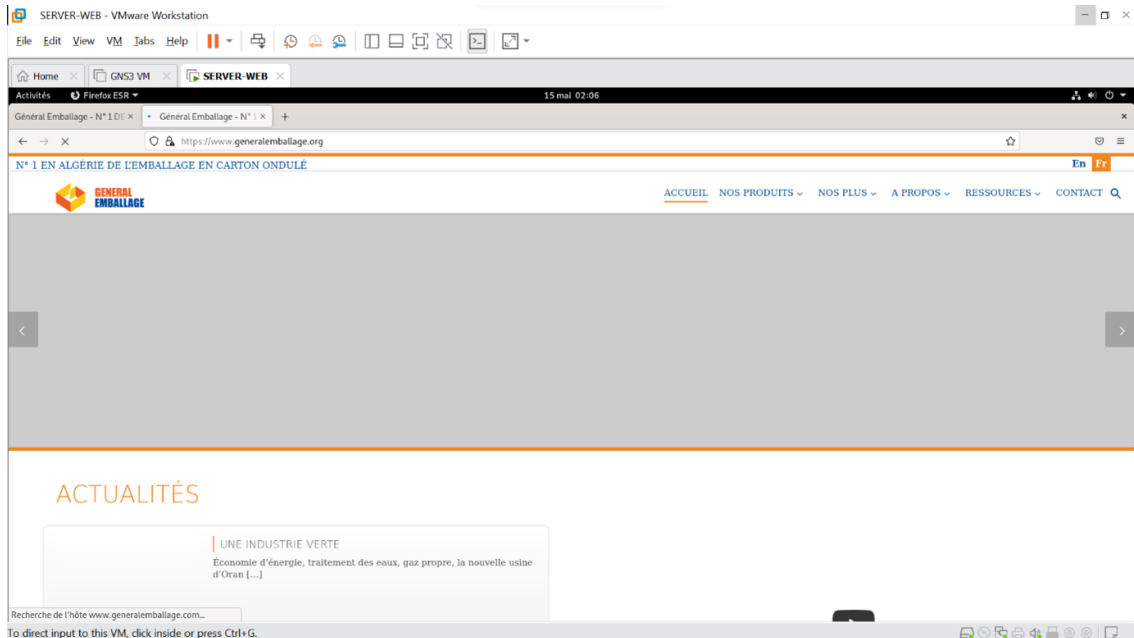


FIGURE 4.24 – Test de l'ouverture avec https en acceptons les risques

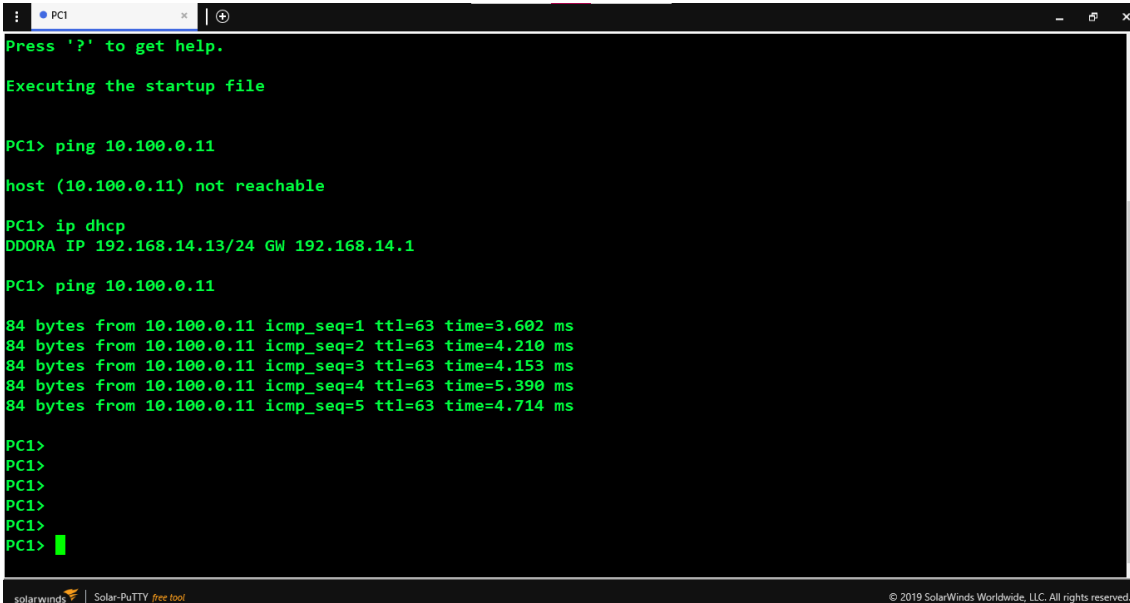
#### 4. Rediriger http vers https

Pour rediriger les clients vers HTTPS dans le fichier de configuration de l'hôte virtuelle dans Apache, on va remplacer Directory et DocumentRoot par mettre la commande RedirectPermanent à l'intérieur du bloc <VirtualHost> dans la section correspondant au port 80 (HTTP) :

```
<VirtualHost *:80>
  ServerName generalemballage.org
  ServerAlias www.eneralemballage.org
  RedirectPermanent / https://generalemballage.org
  RedirectPermanent / https://www.generalemballage.org
</VirtualHost>
```

Une fois que apache redémarer et les modifications de configuration sont appliquer.

#### 4.3.5 Etape 7 : Test DHCP et Vérification de la connectivité



```
Press '?' to get help.
Executing the startup file

PC1> ping 10.100.0.11
host (10.100.0.11) not reachable

PC1> ip dhcp
DDORA IP 192.168.14.13/24 GW 192.168.14.1

PC1> ping 10.100.0.11
84 bytes from 10.100.0.11 icmp_seq=1 ttl=63 time=3.602 ms
84 bytes from 10.100.0.11 icmp_seq=2 ttl=63 time=4.210 ms
84 bytes from 10.100.0.11 icmp_seq=3 ttl=63 time=4.153 ms
84 bytes from 10.100.0.11 icmp_seq=4 ttl=63 time=5.390 ms
84 bytes from 10.100.0.11 icmp_seq=5 ttl=63 time=4.714 ms

PC1>
PC1>
PC1>
PC1>
PC1>
PC1>
```

FIGURE 4.25 – Assignation des adresses IPs

```
PC1
ping 8.8.8.8
*172.16.1.5 icmp_seq=1 ttl=254 time=7.007 ms (ICMP type:11, code:0, TTL expired in transit)
*172.16.1.5 icmp_seq=2 ttl=254 time=6.382 ms (ICMP type:11, code:0, TTL expired in transit)
*172.16.1.5 icmp_seq=3 ttl=254 time=7.475 ms (ICMP type:11, code:0, TTL expired in transit)
*172.16.1.5 icmp_seq=4 ttl=254 time=6.092 ms (ICMP type:11, code:0, TTL expired in transit)
*172.16.1.5 icmp_seq=5 ttl=254 time=6.284 ms (ICMP type:11, code:0, TTL expired in transit)
PC1> ping 8.8.4.4
*172.16.1.5 icmp_seq=1 ttl=254 time=8.662 ms (ICMP type:11, code:0, TTL expired in transit)
*172.16.1.5 icmp_seq=2 ttl=254 time=5.625 ms (ICMP type:11, code:0, TTL expired in transit)
*172.16.1.5 icmp_seq=3 ttl=254 time=6.495 ms (ICMP type:11, code:0, TTL expired in transit)
*172.16.1.5 icmp_seq=4 ttl=254 time=6.033 ms (ICMP type:11, code:0, TTL expired in transit)
*172.16.1.5 icmp_seq=5 ttl=254 time=6.748 ms (ICMP type:11, code:0, TTL expired in transit)
PC1> █
```

FIGURE 4.26 – test de connectivité entre le LAN et internet

```
PC4> ip dhcp
DDORA IP 192.168.12.10/24 GW 192.168.12.1
PC4> ping 192.168.14.13
84 bytes from 192.168.14.13 icmp_seq=1 ttl=63 time=2.369 ms
84 bytes from 192.168.14.13 icmp_seq=2 ttl=63 time=3.197 ms
84 bytes from 192.168.14.13 icmp_seq=3 ttl=63 time=4.406 ms
84 bytes from 192.168.14.13 icmp_seq=4 ttl=63 time=2.980 ms
84 bytes from 192.168.14.13 icmp_seq=5 ttl=63 time=4.927 ms
PC4> ping 10.100.0.11
84 bytes from 10.100.0.11 icmp_seq=1 ttl=63 time=5.359 ms
84 bytes from 10.100.0.11 icmp_seq=2 ttl=63 time=6.272 ms
84 bytes from 10.100.0.11 icmp_seq=3 ttl=63 time=4.402 ms
84 bytes from 10.100.0.11 icmp_seq=4 ttl=63 time=3.497 ms
84 bytes from 10.100.0.11 icmp_seq=5 ttl=63 time=3.724 ms
```

FIGURE 4.27 – Tester la connectivité inter-VLAN

```
PC6> ip dhcp
DDORA IP 192.168.10.11/24 GW 192.168.10.1

PC6> ping 10.100.0.1

84 bytes from 10.100.0.1 icmp_seq=1 ttl=64 time=1.186 ms
84 bytes from 10.100.0.1 icmp_seq=2 ttl=64 time=1.501 ms
84 bytes from 10.100.0.1 icmp_seq=3 ttl=64 time=1.823 ms
84 bytes from 10.100.0.1 icmp_seq=4 ttl=64 time=2.016 ms
84 bytes from 10.100.0.1 icmp_seq=5 ttl=64 time=1.880 ms

PC6> ping 10.100.0.11

84 bytes from 10.100.0.11 icmp_seq=1 ttl=63 time=5.641 ms
84 bytes from 10.100.0.11 icmp_seq=2 ttl=63 time=5.673 ms
84 bytes from 10.100.0.11 icmp_seq=3 ttl=63 time=4.681 ms
84 bytes from 10.100.0.11 icmp_seq=4 ttl=63 time=5.202 ms
84 bytes from 10.100.0.11 icmp_seq=5 ttl=63 time=5.049 ms
```

FIGURE 4.28 – Test de connectivité entre le LAN et le serveur

## 4.4 Conclusion

En conclusion, nous avons mis en place des mesures de sécurité essentielles pour protéger notre serveur web. Nous avons configuré un pare-feu, activé SSL/TLS, renforcé les politiques de mots de passe, détecté les intrusions et effectué des tests de validation. Ces actions nous ont permis de renforcer la sécurité de notre serveur web et de garantir la confidentialité et l'intégrité des données échangées.

## Conclusion générale

En conclusion, ce projet nous a offert une expérience enrichissante sur les plans personnel et professionnel. Nous avons consolidé nos connaissances et compétences en matière de configuration dans un environnement virtuel, notamment avec l'utilisation de VMware. De plus, nous avons approfondi notre expertise dans le domaine de la sécurité des réseaux d'entreprise grâce à la mise en place d'un réseau virtuel privé et d'un pare-feu pfsense.

Nous avons également approfondi notre compréhension de la sécurité d'un serveur web en étudiant l'architecture client/serveur du web, le protocole HTTPS et le protocole SSL/TLS. Nous avons mis en évidence l'importance des certificats SSL pour l'authentification et le chiffrement des données.

En appliquant nos connaissances théoriques, nous avons présenté l'organisme d'accueil de notre étude, General Emballage, et ses problématiques spécifiques en matière de sécurité informatique. Nous avons proposé des solutions telles que l'utilisation de la DMZ, des pare-feu, des certificats SSL et des VLANs pour renforcer la sécurité de leur système.

En réalisant une étude pratique, nous avons configuré un environnement de travail avec des outils tels que GNS3 et VMware Workstation. Nous avons détaillé les étapes de mise en place de la solution proposée, en configurant les interfaces, les VLANs, les routeurs, la DMZ, le pare-feu, le serveur web, le DHCP et en effectuant des vérifications de la connectivité.

Ce projet nous a permis d'acquérir une expérience concrète et d'appliquer nos connaissances universitaires dans un contexte réel. Nous espérons que les solutions proposées contribueront à renforcer la sécurité des serveurs web de General Emballage et garantiront la confidentialité, l'intégrité et la disponibilité de leurs données.

Enfin, la sécurisation des serveurs web sous Linux est un enjeu crucial pour les entreprises et les organisations dans un monde de plus en plus connecté. Il est essentiel de prendre des mesures de sécurité adéquates pour protéger les informations sensibles et prévenir les attaques. Ce mémoire offre des connaissances approfondies et des recommandations pratiques pour renforcer la sécurité des serveurs web et assurer une gestion efficace des systèmes d'information.

# Annexe A

## Installation de VMware

### A.1 Les étapes d'installations VMware Workstation

Afin de créer les machines utilisateurs virtuelles au sein du même pc, nous sommes appelés à installer VMware Workstation en suivant les étapes ci-dessous :

#### A.1.1 Téléchargement du logiciel

##### A.1.1.1 Étape 1

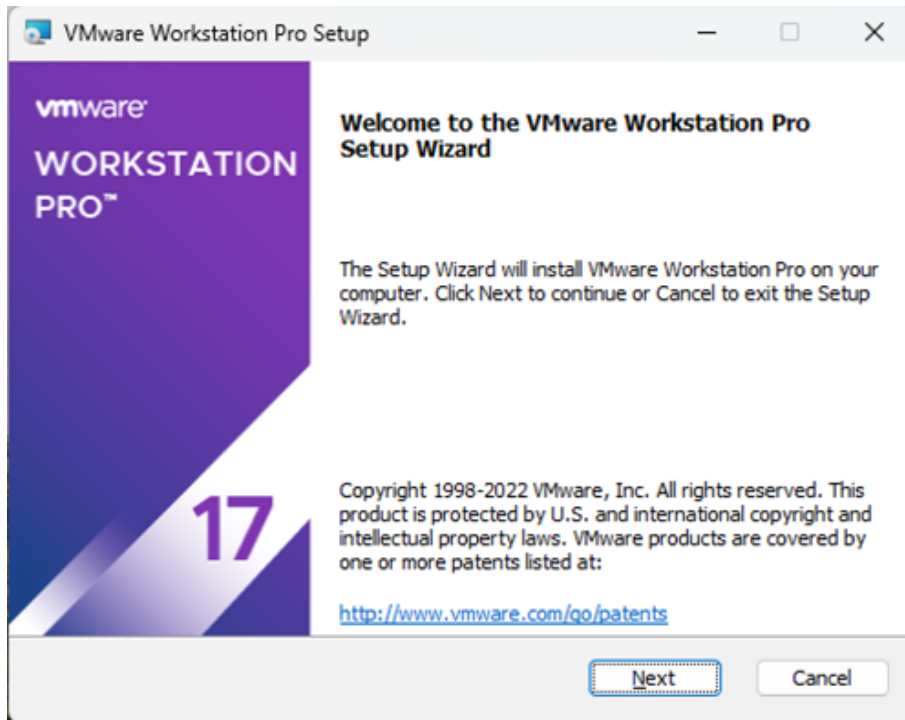
Accédez au site officiel de VMware (<https://www.vmware.com/>) et téléchargez la version de VMware Workstation Pro 17 compatible avec le système d'exploitation Windows.

##### A.1.1.2 Étape 2

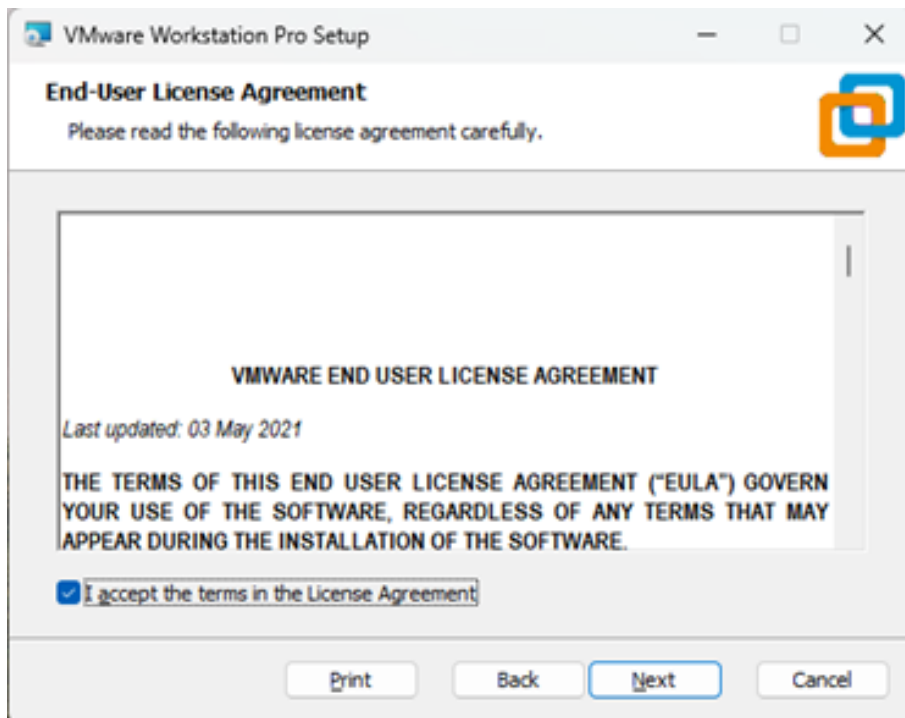
Exécution du programme d'installation : Double-cliquez sur le fichier d'installation téléchargé pour lancer le processus d'installation de VMware Workstation Pro 17

#### A.1.2 Configuration des options d'installation

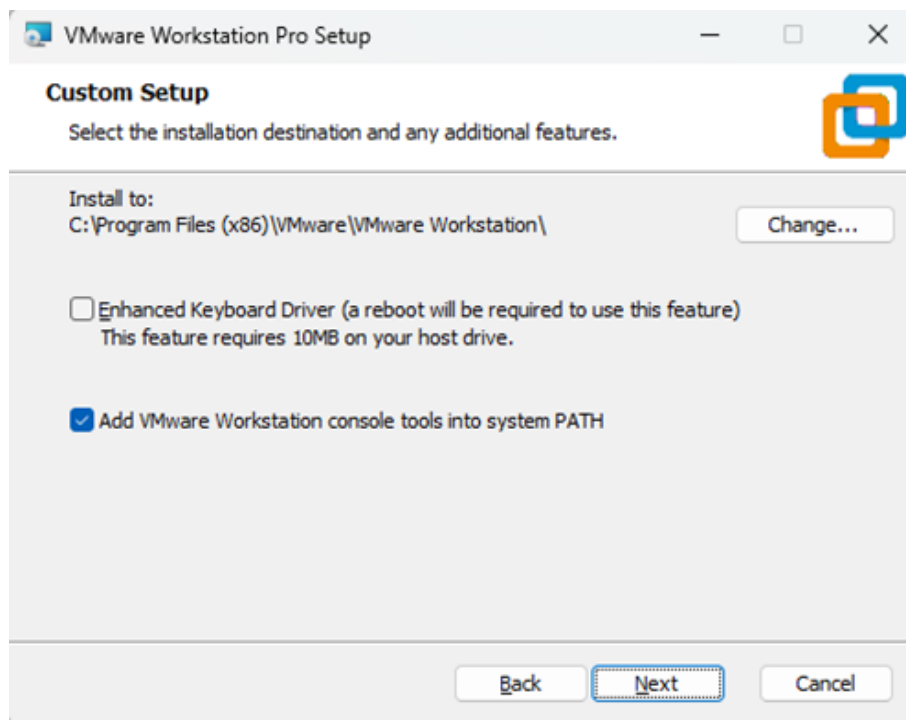
- **Étape 1** :Ouvrez le fichier d'installation de VMware Workstation Pro.
- **Étape 2** :À la première étape, cliquez sur "Next" pour continuer.



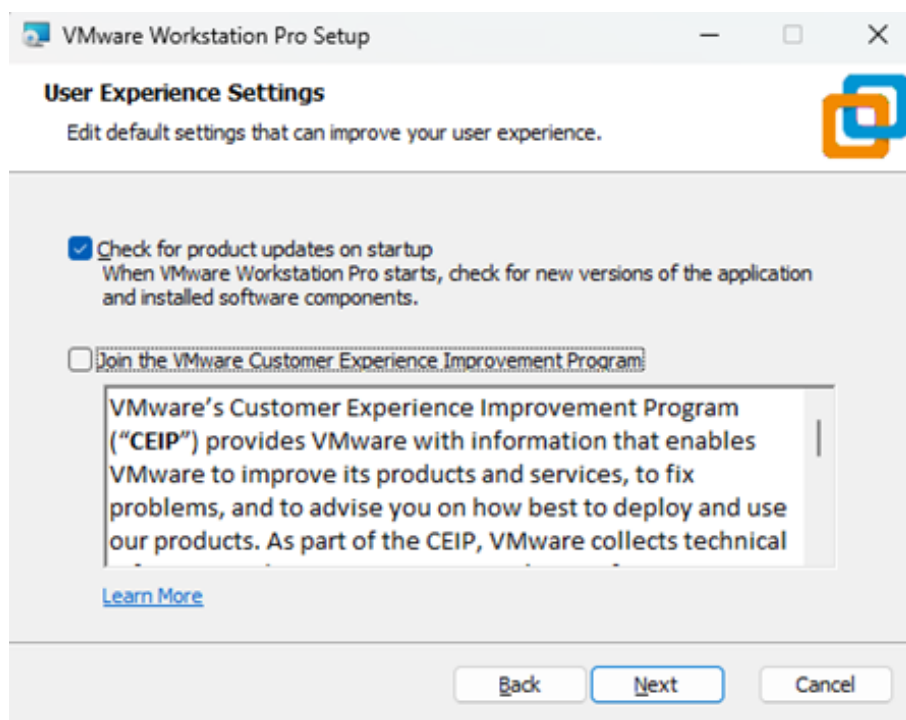
- **Étape 3** :Acceptation des termes de licence



- **Étape 4 :** Choisissez le lieu souhaité pour l'installation et cliquez sur «Next». Coché l'option "Add VMware Workstation console tools into system PATH" si vous souhaitez utiliser l'outil en ligne de commande vctl.exe.

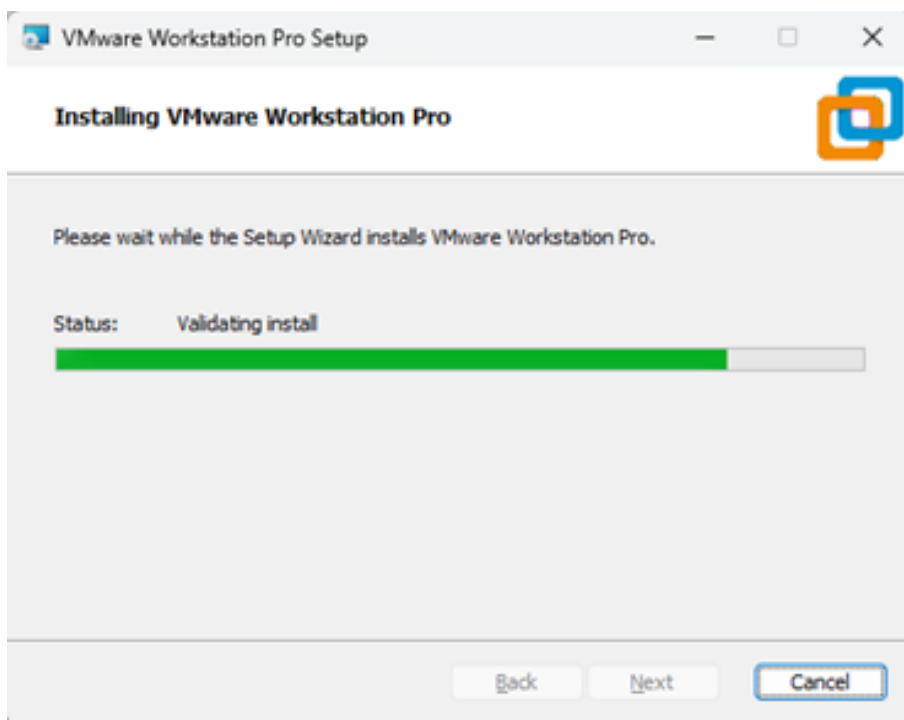
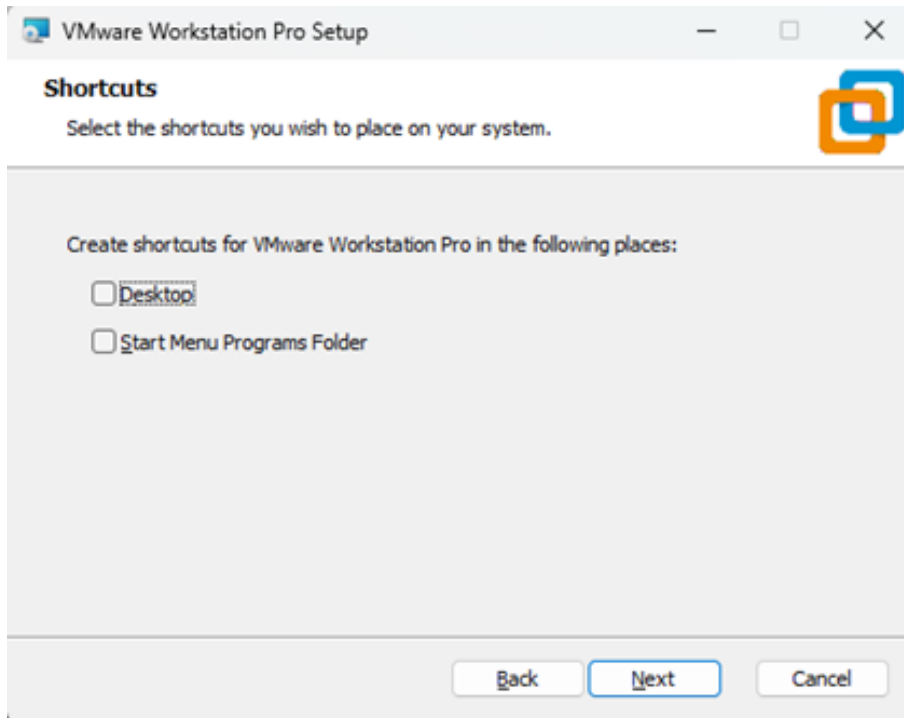


- **Étape 5 :** Cochez les options si vous le souhaitez et cliquez sur Next. Cochez la première option pour vérifier les mises à jour au démarrage de l'application et désactivez la deuxième option si vous ne souhaitez pas participer au programme d'amélioration de VMware Workstation. Cliquez sur "Next".

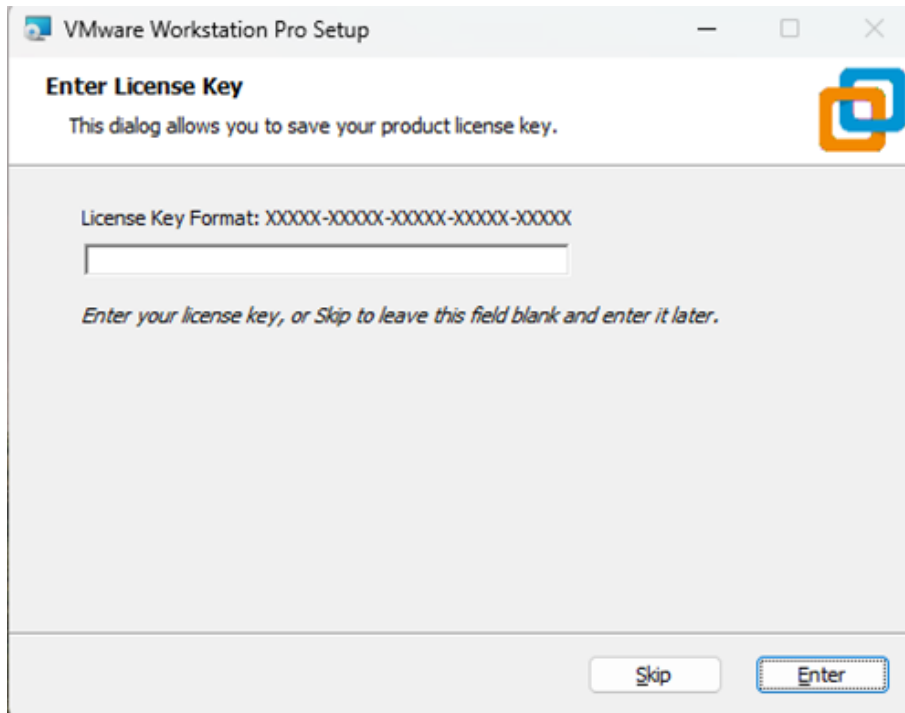




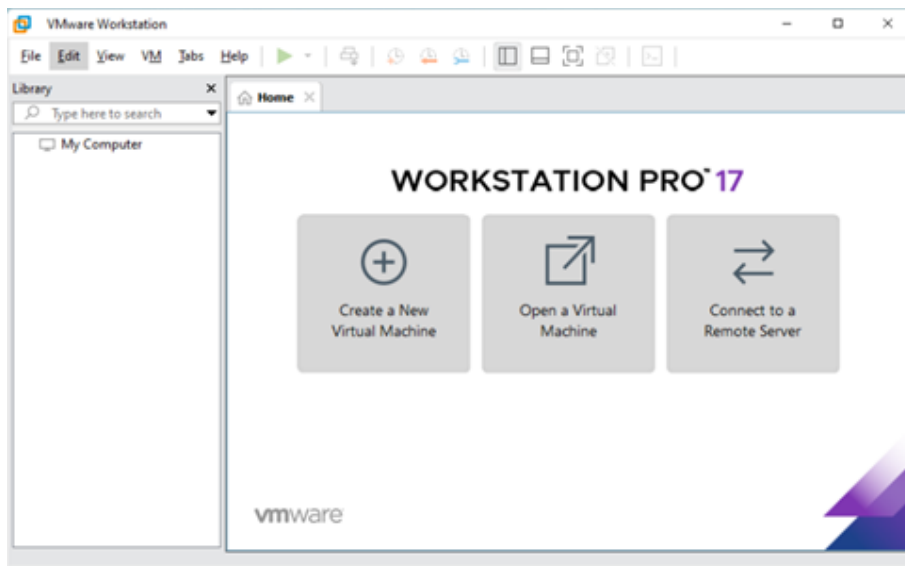
- **Étape 6** : Cochez les options pour créer des raccourcis sur le bureau et dans le menu Démarrer, puis cliquez sur "Next".



- **Étape 7** : Cliquez sur Install. La durée de l'installation dépend de la puissance de votre ordinateur :  
Saisissez votre clé de licence personnelle pour activer votre installation de VMware Workstation Pro, ou vous pouvez choisir de le faire ultérieurement. Cliquez sur "Enter".



- **Étape 8 :** À la fin, vous verrez la boîte de dialogue d'installation terminée. Cliquez sur **Finish** et vous avez terminé le processus d'installation. Vous pouvez être invité à redémarrer votre ordinateur. Cliquer sur **Oui** recommencer.



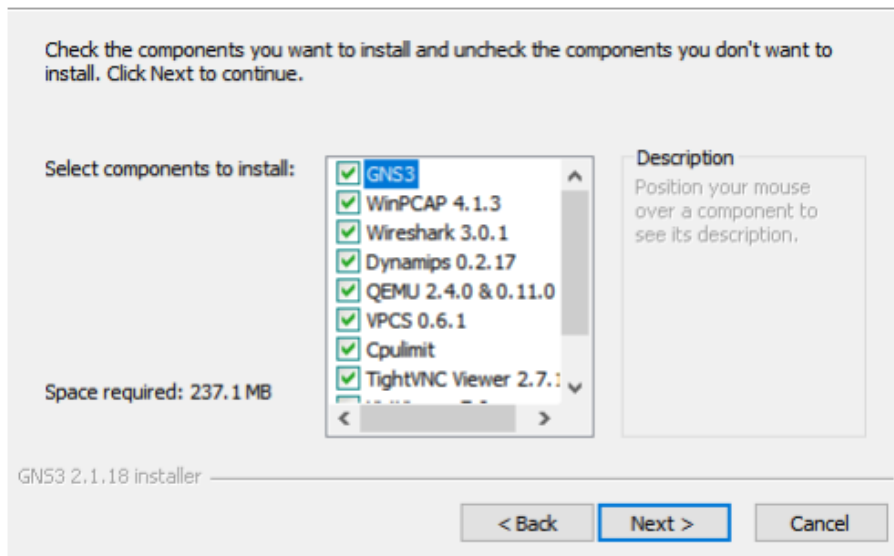
# Annexe B

## Installation de GNS3

### B.1 Les étapes d'Installation de GNS3 sous Windows

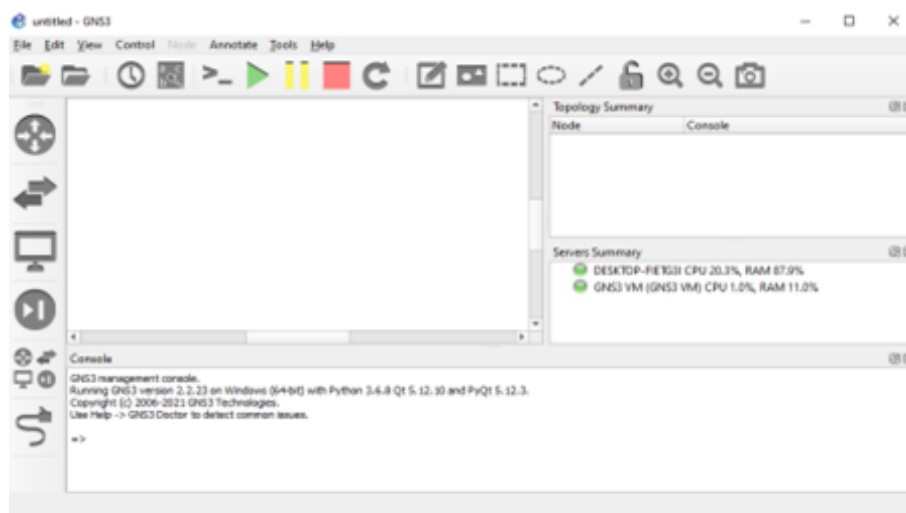
Pour installer GNS3, il faut tout d'abord télécharger le fichier exécutable, ensuite le lancer et suivre les étapes d'installation :

1. Téléchargez l'installateur Windows depuis le lien fourni ([www.GNS3.com](http://www.GNS3.com)).
2. Lancer l'exécution de l'installateur.
3. Lorsque la fenêtre de bienvenue s'affiche, appuyez sur « next ».
4. Acceptez les termes de la licence.
5. Ne modifiez pas le répertoire du menu démarrer au travers duquel GNS3 est accessible.
6. Laissez la liste des composants à installer inchangée.
7. A l'apparition de l'écran de bienvenue de Wireshark, appuyez sur « next ».
8. Acceptez les termes de la licence.
9. Laissez la liste des composants à installer inchangée et validez.
10. Laissez la liste des tâches additionnelles inchangée et validez.
11. Ne modifiez pas le répertoire dans lequel Wireshark sera installé et validez.
12. A l'apparition de l'écran de bienvenue de Winpcap, appuyez sur «OK».
13. Acceptez les termes de la licence.
14. Autorisez le module winpcap à s'exécuter au démarrage.
15. Lorsque l'installation se termine, cliquez sur « Finish ».
16. Après l'installation de GNS3, cliquez sur « Next ».
17. A la demande d'inscription à la mailing-list de GNS3, cliquez sur « next » puis sur « No » à la fenêtre demandant de confirmer.



18. Décochez « Start GNS3 » et cliquez sur « Finish ».

19. L'installation est terminée.



20. Attendez que l'installation se termine. Une fois terminée, redémarrez la machine virtuelle.

21. Vous pouvez maintenant utiliser Debian 11 sur votre machine virtuelle VMware Workstation.

# Annexe C

## Configuration de la partie client extérieur

### C.1 configuration des routeurs

Le rôle du R-Client est de router les paquets de données provenant du réseau local vers le routeur R-ISP pour qu'ils puissent être acheminés vers leur destination finale sur Internet. Le R-Client permet ainsi aux utilisateurs du réseau local de bénéficier de la connectivité et des services fournis par l'ISP.

- **Configuration des interfaces**

Configurer des adresses IP statiques pour chaque interface suivant le tableau suivant :

Device	Interface	Adresse ip	Description	Passerelle
R-ISP	Eth0/0	172.16.1.5/30	connecter a R-client	172.16.1.6
	Eth0/1	172.16.1.2/30	connecter a Pfsense	172.16.1.1
	Nat	DHCP	connecter a Internet	//
R-client	Eth0/0	172.16.1.6/30	connecter a R-ISP	172.16.1.5
	Eth0/1	192.168.200.1/24	connecter a Client	//

TABLE C.1 – Adressage des routeurs

```
R-ISP(config)#interface ethernet 0/1
R-ISP(config-if)#no shutdown
R-ISP(config-if)#ip address 172.16.1.2 255.255.255.252
```

Appliquer la configuration d'adresses IP statiques sur l'ensemble des interfaces.

- **Configuration de routage statique**

Le routage est mis en place dans le but de faciliter la connectivité entre des réseaux distincts en acheminant de manière efficace et optimale le trafic vers sa destination appropriée.

```
R-Client(config-if)#ip route 0.0.0.0 0.0.0.0 172.16.1.5
```

- **Configuration de DHCP dans le R-Client**

La configuration du service DHCP dans le routeur R-Client permet de fournir dynamiquement des adresses IP aux clients du réseau.

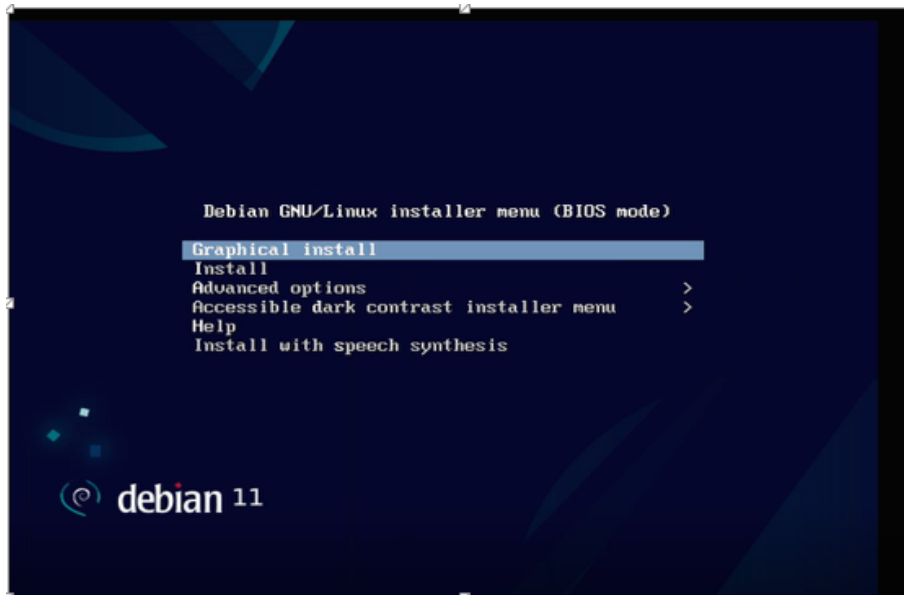
```
R-Client(config)#ip dhcp pool LAN
R-Client(dhcp-config)# network 192.168.200.0 255.255.255.0
R-Client(dhcp-config)# default-router 192.168.200.1
R-Client(dhcp-config)# dns-server 8.8.8.8
R-Client(dhcp-config)#ip dhcp excluded-address 192.168.200.1 192.168.200.10
```

# Annexe D

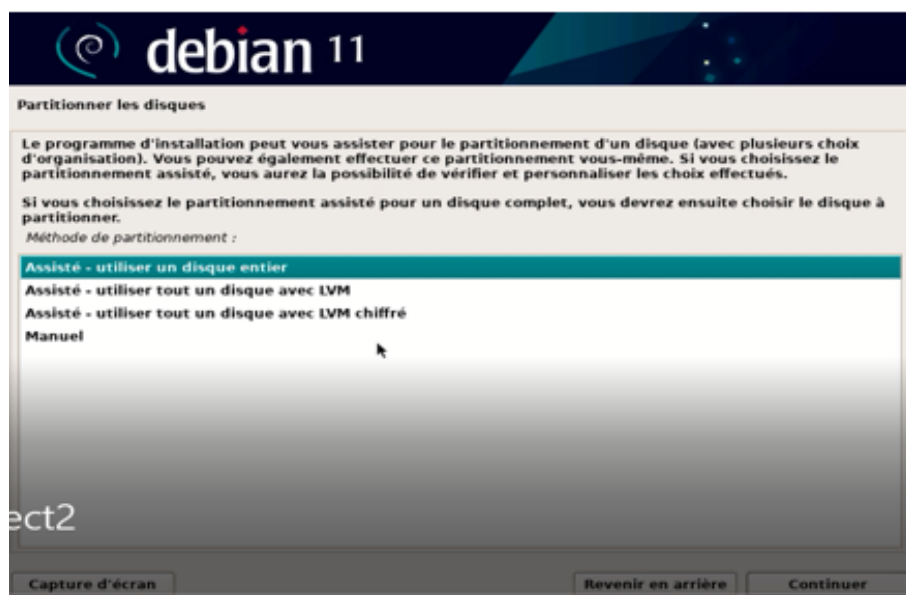
## Installation de linux debian

### D.1 Les étapes d'Installation de Debian 11 sur VM-ware

- **Étape 1** : Lancez VMware Workstation Pro et cliquez sur "Create a new virtual machine" pour créer une nouvelle machine virtuelle.
- **Étape 2** : Téléchargez l'image ISO de Debian 11 à partir du site officiel (<https://www.debian.org>) en choisissant la version correspondant à votre architecture (32 bits ou 64 bits).
- **Étape 3** : Sélectionnez "Installer disc image file (iso)" et cliquez sur "Browse" pour sélectionner l'image ISO de Debian 11 que vous avez téléchargée. Cliquez sur "Next" pour continuer.
- **Étape 4** : Choisissez "Linux" comme système d'exploitation et "Debian 10.x or later" comme version. Cliquez sur "Next".
- **Étape 5** : Spécifiez le nom et l'emplacement de la machine virtuelle, puis définissez la taille du disque dur virtuel. Vous pouvez utiliser les paramètres par défaut ou ajuster selon vos besoins. Cliquez sur "Next".
- **Étape 6** : Sur l'écran de configuration matérielle, vous pouvez ajuster les paramètres selon vos préférences, tels que la quantité de mémoire RAM allouée à la machine virtuelle. Ensuite cliquez sur « split virtual disk as a single file » puis sur « next ».
- **Étape 7** : Ensuite l'on vous demande si la configuration actuelle de votre machine vous convient. Pour tout changement vous pouvez cliquer sur. « customize Hardware » puis via l'interface de droite réglé votre mémoire grâce au curseur et cliquez sur « finish ».
- **Étape 8** : On le démarre en cliquant sur la ligne "Power on this virtual machine" et on sélectionne la méthode d'installation. Choisissez "Graphical install" pour une installation avec interface graphique ou "Install" pour une installation en mode texte. Suivez les étapes d'installation en fournissant les informations requises, telles que le nom d'utilisateur, le mot de passe et les paramètres de réseau.

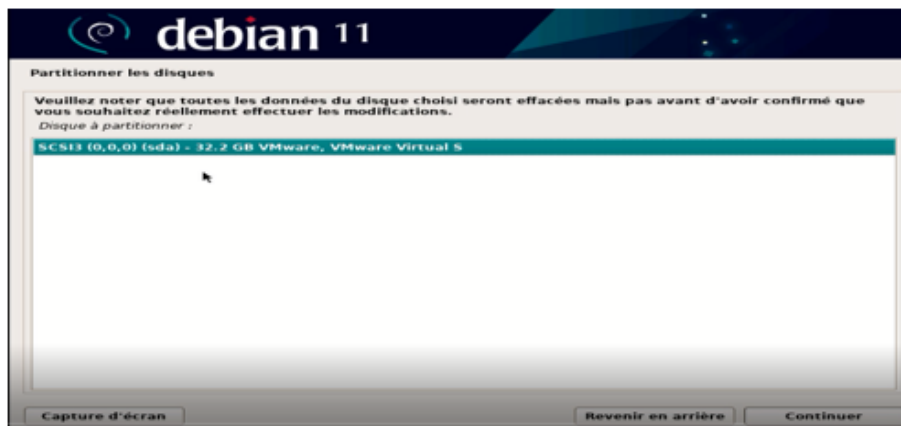


- **Étape 9** : Nous cliquons sur Continuer et les composants Debian 11 seront chargés.
- **Étape 10** : Une fois celle-ci validée, on accède, comme nous l'avons déjà vu, à la configuration du disque. Cliquer sur 'assisté-utiliser un disque entier puis cliquer sur 'continuer'.

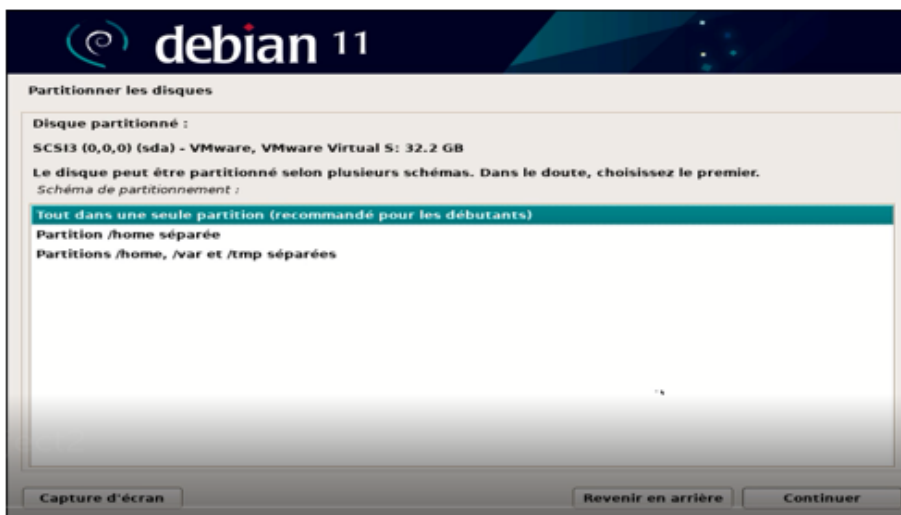




- **Étape 11** : Nous sélectionnons le disque à utiliser :



- **Étape 12** : Nous définissons la manière dont les partitions sont gérées :

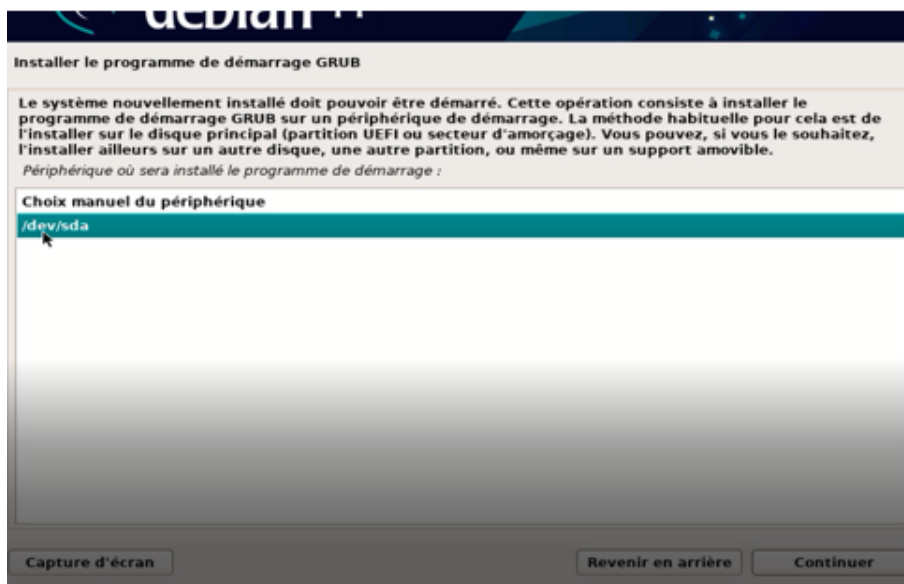


- **Étape 13** : Après cela, on clique sur terminer le partitionnement et appliquer les changements.
- **Étape 14** : Nous confirmons le processus de partition : cliquer sur 'oui'.
- **Étape 15** : Nous cliquons sur Continuer pour continuer le processus.
- **Étape 16** : Au cours de ce processus, nous définissons si nous utilisons ou non un miroir Debian 11 et aussi d'autre support d'installation, dans ce cas nous ne l'utiliserons pas.

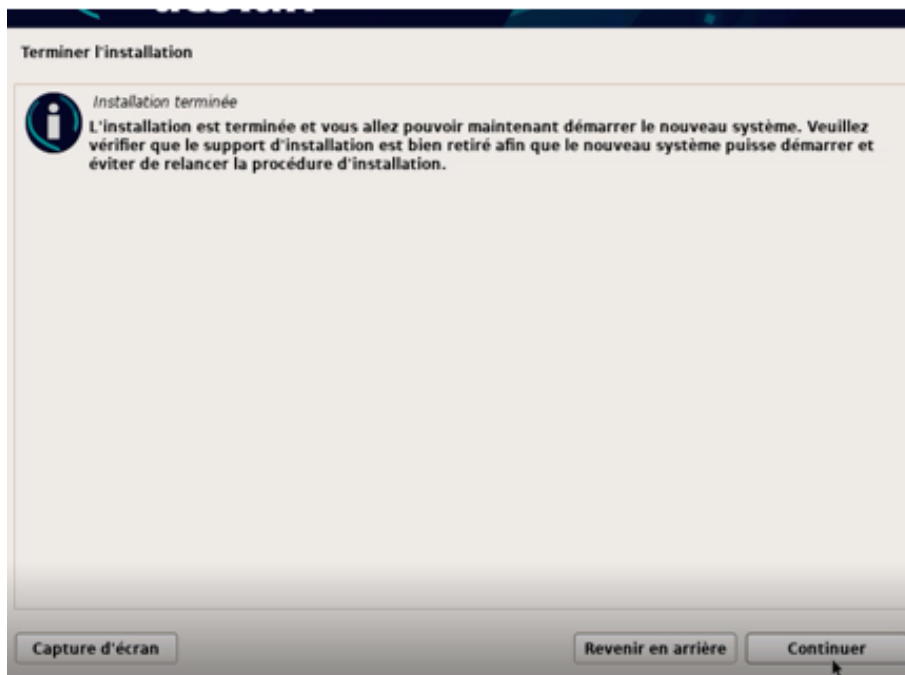
- **Étape 17** : Nous procédons au téléchargement et à l'installation de ce logiciel :



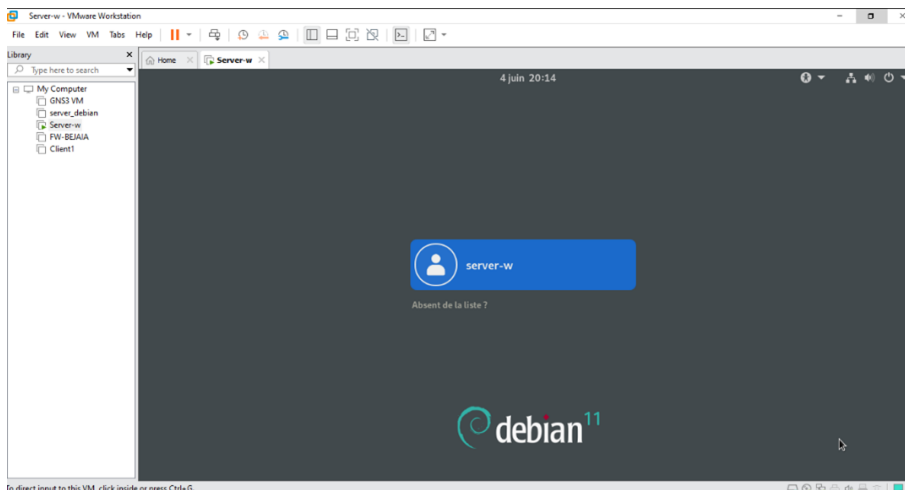
- **Étape 18** : Ensuite, nous devons configurer GRUB
- **Étape 19** : Nous sélectionnons "Oui" et maintenant nous définissons où installer



- **Étape 20** : Ensuite, nous verrons ce qui suit :



- **Étape 21** : Nous appuyons sur Continuer pour redémarrer le système et accéder à la connexion Debian 11. Enfin, dans VMware, il sera possible d'installer Guest Additions et VMware Tools pour augmenter les fonctionnalités de chaque machine virtuelle.
- **Étape 22** : Debian est installé :



# Annexe E

## Installation de PfSense

### E.1 Les étapes Installations firewall

Une fois l'image ISO de pfSense est téléchargée à partir du site officiel (<https://www.pfsense.org>), nous cliquons sur power on this virtual machine

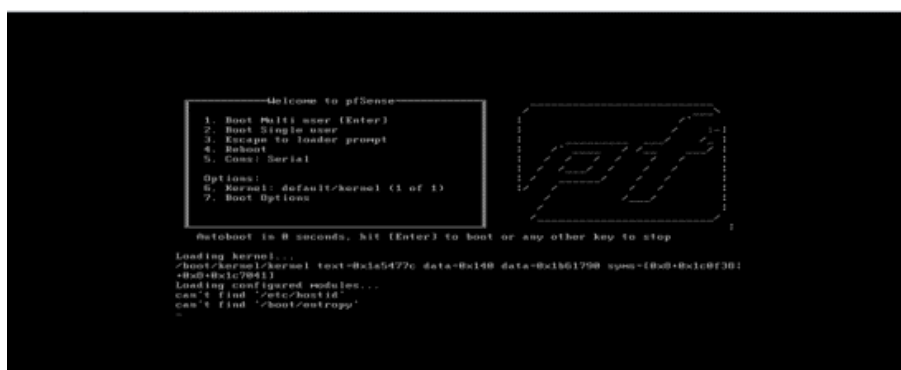


FIGURE E.1 – Ecran de démarrage de l'installation de firewall.

On laisse le système démarrer de lui-même et après quelques secondes, on arrive à l'écran suivant :

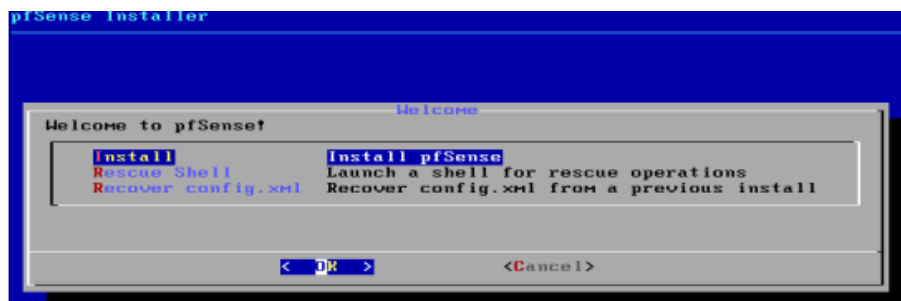


FIGURE E.2 – Début de l'installation de firewall

On accepte le type d'installation puis en validant par la touche «Entrée». Après quelque étape préliminaire, on procède maintenant au redémarrage du système pour

que ça prenne en compte toutes nos manipulations.



FIGURE E.3 – Fin de l’installation de firewall.

Si l’installation s’est bien déroulée, la machine démarre sur le nouveau système, et après configuration des différentes interfaces on obtient l’écran suivant :

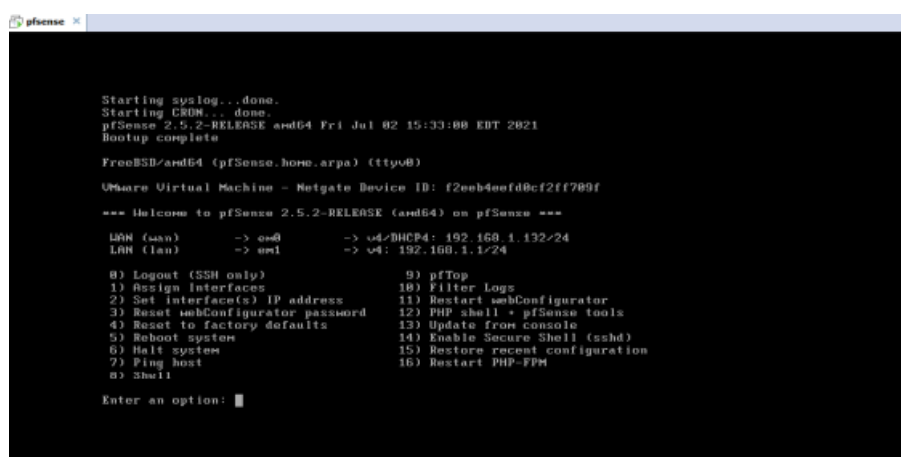


FIGURE E.4 – Menu de configuration de firewall.

Nous sommes maintenant sur la console principale de firewall. Il s’agit d’un menu qui nous donnant l’accès à certaines options pour configurer notre pare-feu. A partir de ce point, le firewall est installé et fonctionnel.

# Bibliographie

- [1] Lemainque, Fabrice, et Jean-François Pillou. Tout sur les réseaux et Internet - 5e éd. 5e édition. Malakoff : Dunod, 2020.
- [2] « Internet et le Web - JeSuisCultive.com ». Consulté le 6 avril 2023. <http://www.jesuiscultive.com/spip.php?article50>.
- [3] Opte. « THE INTERNET ». Consulté le 8 mai 2023. <https://www.opte.org/the-internet>.
- [4] FLYMAN TECHNOLOGY LIMITED. « internet intranet and extranet ». 09 :56 :01 UTC. <https://www.slideshare.net/DOMINICEDGE/chp-4internet-intranet-extranet>.
- [5] Syloe. « Qu'est-ce que l'intranet ? Définition - Expert Linux ». Consulté le 6 avril 2023. <https://www.syloe.com/glossaire/intranet/>.
- [6] User, Super. « Intranets et extranets ». Pulsar - Formations et créations sites, extranets et intranets. Consulté le 6 avril 2023. <https://www.pulsar-agency.com/creation-site-internet/pourquoi-creer-un-site-internet/les-types-de-sites-web/intranets-et-extranets>.
- [7] « Les réseaux INTERNET, INTRANET, EXTRANET - PDF Téléchargement Gratuit ». Consulté le 8 mai 2023. <https://docplayer.fr/17674145-Les-reseaux-internet-intranet-extranet.html>.
- [8] Ambrosy, Mathieu. « Architecture client-serveur ». Consulté le 6 avril 2023. <https://www.geonov.fr/architecture-client-serveur/>.
- [9] « client-server-small.png (325×261) ». Consulté le 6 avril 2023. <https://www.geonov.fr/fig/client-server/client-server-small.png>.
- [10] « Tutoriel : Comprendre la messagerie électronique ». Consulté le 28 avril 2023. <http://sdz.tdct.org/sdz/comprendre-la-messagerie-electronique.html>.
- [11] « Serveur de messagerie : comment ça fonctionne ? - Hosteur.com ». Consulté le 28 avril 2023. <https://www.hosteur.com/ressources/articles/serveur-de-messagerie>.
- [12] « Chap-12- Le client-serveur.pdf » BTS IG 1ère année ALSI. Consulté le 6 avril 2023. <http://perso.modulonet.fr/placurie/Ressources/BTS1-ALSI/Chap-12-%20Le%20client-serveur.pdf>.
- [13] « Sécurité des systèmes d'information ». In Wikipédia, 25 mars 2023. [https://fr.wikipedia.org/w/index.php?title=S%C3%A9curit%C3%A9\\_des\\_syst%C3%A8mes\\_d%27information&oldid=202614770](https://fr.wikipedia.org/w/index.php?title=S%C3%A9curit%C3%A9_des_syst%C3%A8mes_d%27information&oldid=202614770).
- [14] Poinsot, L. (s.d.). Chap. I : Introduction à la sécurité informatique. Cours "Sé- crypt". UMR 7030 - Université Paris 13 - Institut Galilée.

- [15] « Les mécanismes de sécurité informatique – Apprendre en ligne ». Consulté le 7 avril 2023. <https://www.clicours.com/les-mecanismes-de-securite-informatique/>.
- [16] « Attaque informatique : en quoi ça consiste? » Consulté le 7 avril 2023. <https://www.cyberuniversity.com/post/attaque-informatique-en-quoi-ca-consiste>.
- [17] IPE. « Quels sont les différents types d’attaques informatiques? - IPE Informatique », 6 novembre 2018. <https://www.ipe.fr/quels-sont-les-differents-types-dattaques-informatiques/>.
- [18] « Les protocoles sécurisés : Principes et fonctionnements | SYNETIS », 11 août 2015. <https://www.synetis.com/les-protocoles-securises-principes-et-fonctionnements/>, <https://www.synetis.com/les-protocoles-securises-principes-et-fonctionnements/>.
- [19] « CHAPITRE III - Les Attaques Et Mécanismes de Défense 2 | PDF | Attaque par déni de service | Système d’exploitation » Institut des Sciences Appliquées ISA . Consulté le 7 avril 2023. <https://fr.scribd.com/presentation/443023073/CHAPITRE-III -Les-attaques-et-mecanismes-de-defense-2>.
- [20] [https://commons.wikimedia.org/wiki/File%3ADMZ\\_network\\_diagram\\_2\\_firewall.svg](https://commons.wikimedia.org/wiki/File%3ADMZ_network_diagram_2_firewall.svg)
- [21] Gluck, O. (s.d.). Introduction aux Réseaux et au Web. Site web de l’Université Claude Bernard Lyon 1. <https://perso.univ-lyon1.fr/olivier.gluck/supports-enseig.html>
- [22] Brissaud, P.-O. (2020). Analyse de trafic HTTPS pour la supervision d’activités utilisateurs. [Mémoire de Master, Université de Lyon].
- [23] Journal du Net (2021). HTTPS (Hypertext Transfert Protocol Secure) - Définition. Journal du Net. <https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1203459-https-hypertext-transfert-protocol-secure-definition/>
- [24] A Comprehensive Survey on SSL/TLS and their Vulnerabilities. Mohammad Nauman, Ahmad Karim, Syed Zafarul Hussain, Kamran Ali, and Khalid Bashir Bajwa. Journal of Network and Computer Applications, Volume 86, Pages 1-42, 2017. Disponible sur : <https://www.researchgate.net/publication/310761924-A-Comprehensive-Survey-on-SSL-TLS-and-their-Vulnerabilities>.
- [25] C. D. François-Xavier Aguessy, « Interception des échanges dans une connexion SSL/TLS Application à l’analyse des données de géolocalisation envoyées par un smartphone, » Mémoire de Master, Université de Limoges, France, 2012.
- [26] Kheirr-dinne Mouhamed Ali. (2015). Etude et implémentation d’une solution de sécurisation des communications par SSL/TLS (Mémoire de Master en Télécommunications, Réseaux Mobiles et Services de Télécommunications). Université de Tlemcen.
- [27] Sekar, M., et Iguchi-Cartigny, J. (2018). Partition HTTP/TLS Pour Pépin. Rapport de projet de fin d’études, Polytech Lille, France.
- [28] SSL.com. (s. d.). Qu’est-ce que la cryptographie à clé publique? SSL.com. <https://www.ssl.com/fr/faq/qu%27est-ce-que-la-cryptographie-%C3%A0-cl%C3%A9-publique/>.

- [29] IBM. (S. d.). Service client-serveur. Récupéré de <https://www.ibm.com/fr-fr/topics/client-server-services>
- [30] FrameIP. (S.d.). SSL/TLS : Protocoles et chiffrements - 4.1 Le protocole de handshake. FrameIP. Récupéré à partir de <https://www.frameip.com/ssl-tls/#41-8211le-protocole-hanshake>.
- [31] Delmas, Y. (2021). Architecture des réseaux informatiques. [online] Available at : <https://delmas-rigoutsos.nom.fr/documents/YDelmas-ArchiWeb/YDelmas-ArchiWeb.html#id2506313>
- [32] Ristic, I. (2014). Bulletproof SSL and TLS : Understanding and deploying SSL/TLS and PKI to secure servers and web applications. Feisty Duck.
- [33] SSL/TLS - Fonctionnement et failles de sécurité" publié sur le site FrameIP.com. Disponible en ligne : <https://www.frameip.com/ssl-tls/#13-8211fonctionnement>.
- [34] Apache Software Foundation. (s. d.). SSL/TLS Strong Encryption : An Introduction [Introduction à SSL/TLS : cryptage fort]. Récupéré à partir de <https://httpd.apache.org/docs/trunk/fr/ssl/ssl-intro.html>
- [35] <http://www.redisgate.com/redis/network/ssl.php>
- [36] DigiCert. (s.d.). Comment fonctionnent les certificats SSL/TLS. Récupéré le 11 mai 2023, à partir de <https://www.digicert.com/fr/how-tls-ssl-certificates-work>
- [37] <https://www.google.com/search?sxsrf=APwXEddFb7N-a9g7OGCs2-S6a-tllO4c7g:1683760449976&q=Figure+:+structure+d27un+certificat+X.509&tbm=isch&sa=X&ved=2ahUKEwjvYe88OvAhXk-rsIHRn8BsEQ0pQJegQICBAB&biw=638&bih=580&dpr=1.5#imgrc=MU8JmjLuOQUyPM>
- [38] Dupont, M. (2021). Définition de HTTPS : Pourquoi et comment passer en HTTPS. Semrush. <https://fr.semrush.com/blog/definition-https/>



## Résumé

Le projet de fin d'études se concentre sur la sécurisation d'un serveur web sous Linux. Le serveur web utilisé est Apache, et des mesures de sécurité telles que l'installation d'un certificat CRS auto-signé et l'utilisation des protocoles SSH et SSL ont été mises en place. L'objectif principal de ce projet est d'assurer la confidentialité et l'intégrité des données échangées entre le serveur web et les utilisateurs. Des techniques telles que la gestion des certificats et la configuration des protocoles sécurisés sont mises en œuvre pour atteindre cet objectif. Cette étude permettra de renforcer la sécurité du serveur web et de prévenir les potentielles vulnérabilités liées aux échanges d'informations sur Internet.