République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université A. Mira de Bejaïa

Faculté des Sciences Exactes

Département d'Informatique

Mémoire de Fin de Cycle

En vue de l'obtention du diplôme de Master professionnel en Informatique

Option : Administration et sécurité des réseaux

Thème :

Sécurisation d'un serveur web apache

Cas d'étude : « CSRICTED » de l'université A. Mira Bejaia

Réalisé par :

M[lle] MAOUCHI NADJET

M[lle] BENIKHLEF FAIZA

Devant le jury composé de :

Examinateur 1 Mme ALOUI Soraya U.A/Mira Bejaia

Examinateur 2 Mr. MOHAMMEDI Mohamed U.A/Mira Bejaia

Encadrant Mr. TOUAZI Djoudi U.A/Mira Bejaia

Année universitaire 2021/2022

Remerciements

En tout premier lieu, nous remercions le bon dieu tout puissant de nous avoir donné courage, volante et patience pour terminer ce travail.

Nous tenons à exprimer notre gratitude pour notre encadreur Mr TOUAZI.Djoudi, pour le temps qu'il nous a accordé et pour nous avoir suivis dans nos démarches, pour nous avoir transmis les renseignements nécessaires à la réalisation de ce travail.

Nous remercions tout particulièrement Mr DJEBBARI.Y pour son aide précieuse et ses conseils avisés.

Nous remercions aussi le personnel de «CSRICTED», de nous avoir acceptés au sein de leur organisme pour effectuer notre stage et leur aimable accueil et pour leur disponibilité.

Nous remercions les membres de jury qui ont accepté de juger notre travail.

Enfin, notre gratitude s'adresse également à tous ceux qui nous ont soutenus de près ou de loin à achever ce modeste travail.

Dédicace

Je dédie ce mémoire :

A mes très chers parents ; qui ont tout fait pour m'encourager durant toutes mes études, et grâce à eux que je suis arrivé à réaliser ce résultat.

Mon très chers frère FAWZI pour qui je souhaite une vie pleine de joie, réussite et beaucoup de bonheur.

A mes sœurs AHLEM ET MAISSA pour leurs soutient moral indéfectible.

A mes très chères copines CHAFIA, WISSAM, MOUFIDA, ADJA, Siham avec qui j'ai passé des agréables et inoubliables moments.

A ma très chère tante AICHA qui n'a cessé de m'encourager.

Sans oublie ma binôme Melle BEN IKHLEF FAIZA et toute sa famille.

Enfin, mes dédicaces vont `a toute la famille MAOUCHI et BEN IKHLEF.

MAOUCHI NADJET.

Dédicaces

Je dédie ce modeste travail:

En premier lieu à mes très chers parents à qui j'offre toutes mes réussites et tous les mérites. Je leur serais éternellement dévoué. Et à mon père et qui n'a jamais cessé d'être à mes côtés par ces précieux conseils et orientation ainsi que son soutien moral.

A mon mari BOUBKEUR

A mes frères (HAMDI et Saïd).

A mes deux sœurs (Fifi et Najete).

A ma grand-mère Fatima

A tous mes oncles, tantes et cousin(e) s sans exception et toute la famille un par un.

A tous mes amis

Sans oublie ma binôme Najete et à toute sa famille.

A Toutes personnes qui m'ont soutenue tout au long de mes études.

Table des matières :

Liste des tableaux

Liste des Figures

Liste des abréviations :

ATS **A**pplied **T**ype **S**ystem.

BSD **B**erkeley **S**oftware **D**istribution.

CRS **C**ertificate **S**igning **R**equest.

CSRICTED **C**entre des **S**ystèmes et **R**éseaux d'**I**nformation, de **C**ommunication de **T**élé- enseignement et de l'**E**nseignement à **D**istance.

CA **C**ertification **A**uthority

DNS **D**omain **N**ame **S**ystem

DMZ **D**emilitarized **Z**one.

DV **D**omain **V**alidation

DHCP **D**ynamic **H**ost **C**onfiguration **P**rotocol.

EV **E**xtended **V**alidated

FTP **F**ile **T**ransfer **P**rotocol

GNS3 **G**raphical **N**etwork **S**imulator.

GLPI **G**estionnaire **L**ibre de **P**arc **I**nformatique

HTTP **H**yper**T**ext **T**ransfert **P**rotocol

HTTPS **H**yper**T**ext **T**ransfer **P**rotocol **S**ecure

IRC **I**nternet **R**elay **C**hat

IP **I**nternet **P**rotocol

ICMP **I**nternet **C**ontrol **M**essage **P**rotocol

IMAP **I**nternet **M**essage **A**ccess **P**rotocol.

IPSec **I**nternet **P**rotocol **S**ecurity

IETF **I**nternet **E**ngineering **T**ask **F**orce

IPv4 **I**nternet **P**rotocol **v**ersion 4**.**

LAN **L**ocal **A**rea **N**etwork

MAC **M**edia **A**ccess **C**ontrol.

NAT **N**etwork **A**ddress **T**ranslation.

OSPF **O**pen **S**hortest **P**ath **F**irst

OSI **O**pen **S**ystem **I**nterconnection

OV **O**rganisation **V**alidate

OS **O**perating **S**ystem

POP **P**ost **O**ffice **P**rotocol

RIP **R**outing **I**nformation **P**rotocol

RIB **R**elevé d'**I**dentité **B**ancaire

RFC **R**equests **F**or **C**omments

SMTP **S**imple **M**ail **T**ransfer **P**rotocol

SSL **S**ecure **S**ockets **L**ayer

SSH **S**ecure **S**hell

SI **S**ystème d'**I**nformation.

TCP **T**ransmission **C**ontrol **P**rotocol

TLS **T**ransport **L**ayer **S**ecurity

UDP **U**ser **D**atagramme **P**rotocol

URL	**U**niform **R**esource **L**ocator
VTP	**V**LAN **T**runking **P**rotocol
VLAN	**V**irtual **L**ocal **A**rea **N**etwork.
WAN	**W**ide **A**rea **N**etwork
WEB	**W**orld **W**ide **W**eb

Introduction général

Avec l'essor de l'informatique ces derniers années, le partage des informations entre les différents ordinateurs à travers les quatre coins du monde devient un besoin excréments important notamment pour les entreprises et les différentes organisations informatisées.

Le progrès dans la technologie informatique a abouti à faire des réseaux informatiques, des systèmes qui permettent à ces différentes entreprises et organisations de faire circuler leurs informations le plus rapidement avec des moindres coûts. C'est en connectant aux divers réseaux informatique à travers le monde de que la notion d'internet est apparue.

Internet donc est les plus grands réseaux planétaires qui permettent l'échange des informations entre tous les ordinateurs connectés à ces réseaux.

Le partage des informations entre les utilisateurs des réseaux peut avoir plusieurs objectif comme l'envoi des messages d'informations, qui est le cas de la messagerie électronique ; le transfert de données sous différents formats, la consultation des diverses page web qui est le cas de service web. C'est à cause de la diversité des objectifs visés en partageant des informations via internet qu'il est nécessaire de faire de celle-ci un moyen qui fournit des services, chaque service fonctionne selon son propre protocole.

Ses dernières années l'internet a connu un développement phénoménal. Selon [39], le nombre d'utilisateurs connectés à l'internet se situe actuellement à plus d'un milliards en mars 2007.en mai 2007, [Netcraft] a recensé plus de 120 millions de site web .dans le monde dont 66 millions sont hébergés sur les serveurs web apache. [39]

L'homme a toujours ressenti le besoin de dissimuler des informations, bien avant même l'apparition des premiers ordinateurs et de machines à calculer.

L'informatique est un monde en perpétuelle et rapide mutation, de nouveaux matériels, de nouveaux logiciels, de nouveaux sites Internet. Avec tout leur intérêt, certes …mais avec aussi leurs failles de sécurité, qui apparaissent chaque jour.

La sécurité informatique est de fait un sujet éminemment vaste et mouvant. La plupart des entreprises algériennes disposent d'un site internet et d'une messagerie électronique ce qui

Pousse à l'utilisation d'un accès internet. Ce sont là autant de portes d'entrée potentielles sur le réseau qui, compte tenu des risques encourus, devraient inciter à adopter une politique de sécurité. [39]

Pour cela nous avons partagé notre travail en quatre chapitres important. Dans le premier chapitre, nous allons parler des notions de base sur la sécurité des systèmes d'informatique.

Dans le second chapitre nous allons parler des généralités sur la sécurité d'un serveur web.

Dans le troisième chapitre, nous allons présenter la structure, les fonctionnalités ainsi de l'entreprise, la problématique et la solution.

Quant au quatrième chapitre, il sera consacré à la réalisation de notre solution.

Dans le cadre de ce travail, nous allons nous intéresser à la configuration, l'installation et la sécurisation d'un serveur web apache sous linux.

Chapitre 1 : Pré-requis théorique

Introduction :

La notion de réseau ancienne, mais elle restreinte au niveau de la télécommunication (téléphone, télégraphe).avec le développement technologique, surtout dans le domaine informatique (matériel et logiciel). Le réseau informatique (téléinformatique) permet de plus en plus de places aujourd'hui des millions de personnes sont reliées à l'internet : particuliers, petites et grandes, entreprises associations, écoles, université et gouvernements.

Parmi les services qu'offre l'internet : le courrier électronique (mail). L'IRC…etc .mais la composante la plus populaire de l'internet est Word wide web appelé aussi le web. La sécurité des réseaux est devenue de plus en plus importante ces dernières années, alors que des virus et des outils automatisés de plus en plus sophistiqués attaquent les réseaux. Cela comprend tous les aspects matériels et logiciel, les serveurs, les stations de travail, ainsi que l'implémentation des réseaux et le câblage, les systèmes d'exploitation, y compris ceux des réseaux, les programmes utilisateurs, et l'élément le plus important : les données utilisateurs.

Dans ce chapitre nous avons faisons une analyse théorique des concepts de base relatifs à la sécurisation .il comprend deux point dans la première point nous présentons un préambule sur les réseaux TCP /IP (leurs classification ainsi que leurs architecture client /serveur et la pile protocolaire TCP/IP) dans le second nous parlons sur quelque concepts clé de la sécurisation informatique. Dans ce qui suit, nous allons plus détail la sécurité d'un serveur web, le système client/serveur, notion sur HTTPS ou http ainsi échange entre SSL et HTTPS.

Partie 1 : Notion de base sur la sécurité des systèmes d'information

1.1 Généralité sur les réseaux TCP/IP :

1.1.1 Classification des réseaux

Les réseaux peuvent être classifiés en fonction de différents critères, parmi ces critères on cite l'ouverture qui donne :

- **Les Réseaux Internet :**

Sont Les réseaux publics, nationaux ou internationaux des entreprises de télécommunication (un ensemble d'ordinateurs interconnectés), permettant l'échange d'informations. Ces informations sont accessibles grâce à des protocoles de communication internet (HTTP, FTP, SMTP, NNTP). [1]

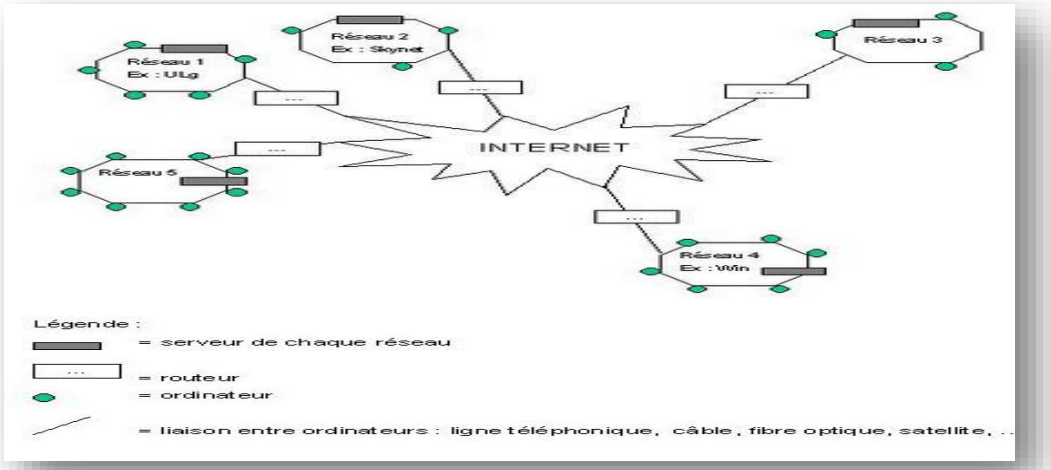

Figure 1.1: Le réseau Internet. [2]

- **Les réseaux Intranet** :

Un réseau intranet est un réseau local interne à une entreprise dont l'utilisation s'apparente à celle d'internet puisqu'il fonctionne avec la même technologie. Cependant, le réseau reste totalement privé et fermé aux connexions publiques (Les réseaux privés internes à l'intérieur d'une entrepris). [3]

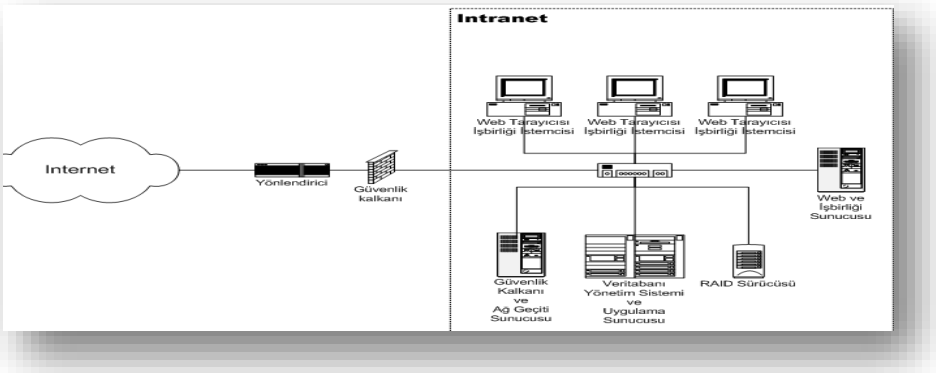

Figure 1.2:le réseau Intranet. [4]

- **Les réseaux Extranet** :

Un réseau extranet se destine quant à lui au partage d'informations avec des acteurs externes à l'entreprise. Son utilisation est filtrée grâce à une identification par mot de passe. L'extranet permet d'ouvrir le système d'informations d'une entreprise à des partenaires extérieurs : clients, fournisseurs, filiales…(Les réseaux privé internes et externes, ouvert vers l'extérieur). [3]

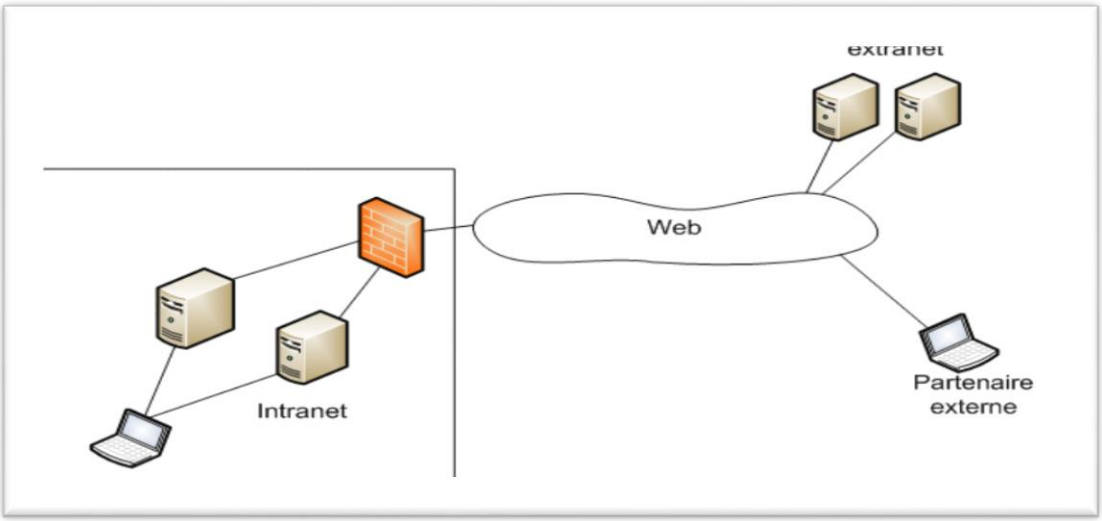

Figure 1.3: le réseau Extranet. [5]

1.2.2 Architecture réseau :

- **Architecture client /serveur :**

Une architecture client-serveur représente l'environnement dans lequel des applications de machine clients communiquent avec des applications de machines de type serveurs, une machine généralement très puissante en terme de capacités d'entrée-sortie, qui leur fournit des services. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion, etc. Un système client/serveur fonctionne selon le schéma suivant :

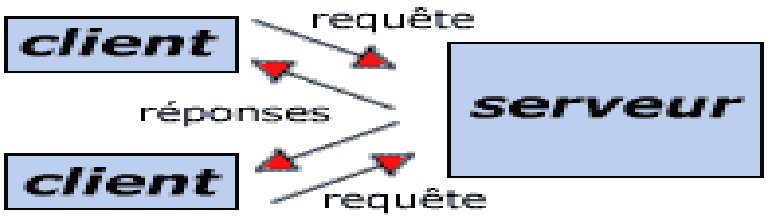

Figure 1.4: architecture client/serveur

- Le client émet une requête vers le serveur grâce à son adresse IP et le port, qui désigne un service particulier du serveur.

- Le serveur reçoit la demande et répond à l'aide de l'adresse de la machine cliente et son port.

Les premiers réseaux informatiques étaient architecturés autour d'un ordinateur central, appelé « mainframe Ss», qui représente ainsi un ordinateur central de grande puissance chargé de gérer les sessions utilisateurs des différents terminaux qui lui étaient reliés. [9]

1.2.3 La pile protocolaire TCP/IP :

TCP/IP Représente l'ensemble des règles communication sur l'internet et se fonde sur l'adressage IP c'est –à-dire il faut de fournir une adresse IP à chaque machine de réseau afin de pouvoir acheminer des paquets données.

La pile TCP/IP est donc l'ensemble des protocoles nécessaires pour faire dialoguer plusieurs machines entre elles, que ce soit au sein d'un réseau local ou via internet. [6]

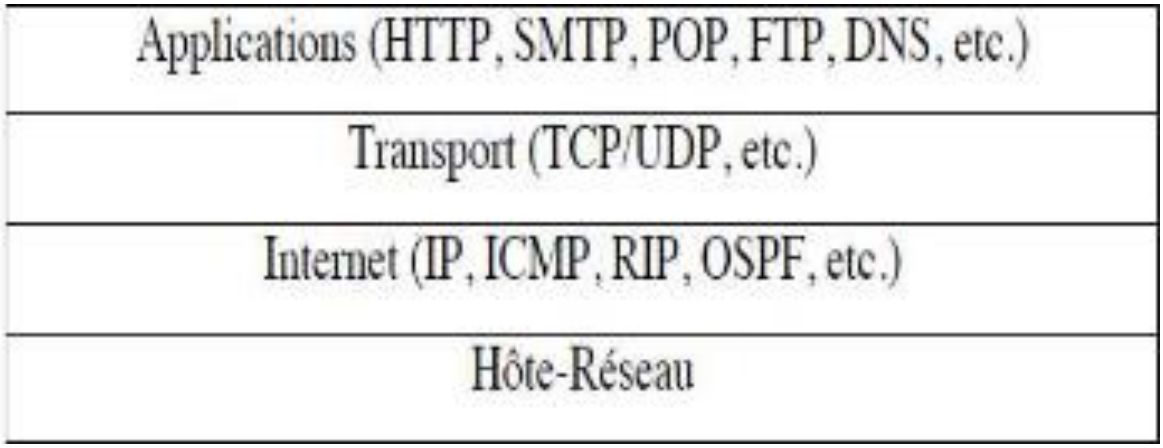

Figure 1.5: la pile TCP /IP. [6]

La couche hôte-réseau regroupe les fonctionnalités des couches liaison de données et physique du modèle OSI et où les couches transport et application sont des couches de bout en bout.

Une couche est dite de bout en bout si elle est implantée sur les entités terminales de communication mais pas sur les entités intermédiaires (routeur, switch). [6]

1.2 Généralité sur la sécurité des systèmes d'information

1.2.1 Définition de sécurité informatique :

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique. Elles caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard la sécurité. [8]

1.2.2. Les critères de la sécurité informatique :

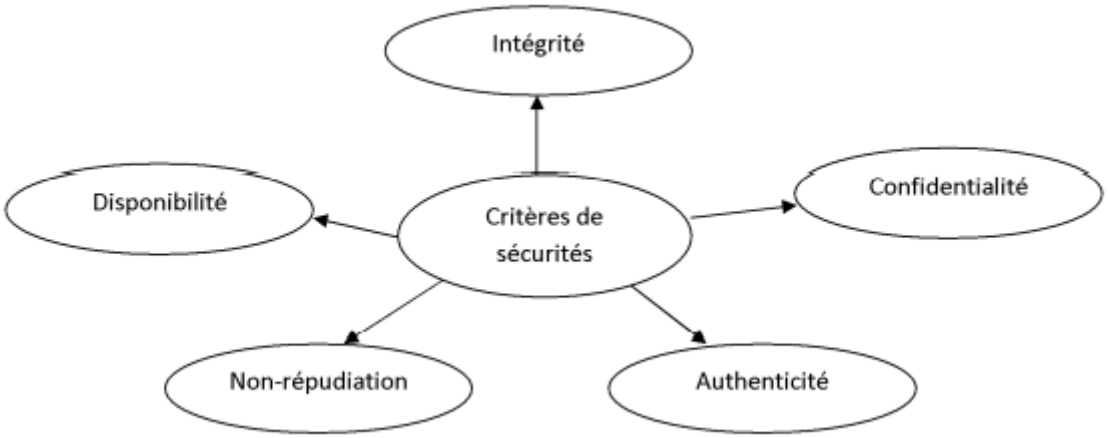

Figure 1.6: critères de sécurité.

- **Confidentialité** : Confidentialité est la capacité à garder un secret. Elle a comme rôle la protection des données contre les attaques non autorisées, ce qui assure l'arrivée du message envoyé au destinataire. [10]
- **Intégrités :** L'intégrité consiste à s'assurer que les données n'ont pas été falsifiées et qu'elles sont donc correctes, authentiques et fiables. [11]
- **Authentification :** L'authentification permet de s'assurer de l'identité des processus communicants, ce qui assure que le message envoyé a été reçu par le bon destinataire.
- **No répudiation:** Le non répudiation permet pour un message donné de bien spécifier l'émetteur et le récepteur, c'est-à-dire que ni l'émetteur ni le récepteur ne peuvent contester respectivement l'émission ou la réception d'un message donné. [10]
- **Disponibilité :** est l'assurance que les personnes autorisées ont accès à l'information quand elles le demandent ou dans les temps requis pour son traitement. [12]
- **Traçabilité :** garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables. [13]

1.2.3 Les attaques et vulnérabilités :

1.2.3.1 Vulnérabilité :

Ce sont les failles de sécurité dans un ou plusieurs systèmes. Tout système vu dans sa globalité présente des vulnérabilités, qui peuvent être exploitables ou non. [14]

1.2.3.2 Les attaques :

1. Définition d'attaque *:* Elles représentent les moyens d'exploiter une vulnérabilité. Il peut y avoir plusieurs attaques pour une même vulnérabilité mais toutes les vulnérabilités ne sont pas exploitables. [14]

2. Type d'attaque :

- **Attaque directe :**

L'attaque la plus simple, Hacker attaque sa victime directement depuis son ordinateur Via un script d'attaque faiblement configurable. Le programme de piratage qu'ils utilisent envoie directement paquets à la victime. Dans ce cas, il est généralement possible de tracer attaque pour identifier l'agresseur. [14]

Figure 1.7: attaque directe

- **Attaques par rebond**

Menée via un autre ordinateur qui se retrouve complice involontaire. Cet ordinateur expédie des messages d'attaque à la victime, masquant l'identité du pirate.

Figure 1.8: Attaque par rebond

- **Attaques à réponse indirecte :**

Attaques à réponse indirecte Cette attaque est un dérivé de l'attaque par rebond. Du point de vue d'un pirate informatique, il offre les mêmes avantages. Mais au lieu d'envoyer une attaque à un ordinateur intermédiaire Il le passe et l'attaquant lui enverra des requêtes. C'est cette réponse à la requête qui sera envoyée à l'ordinatrice victime. [14]

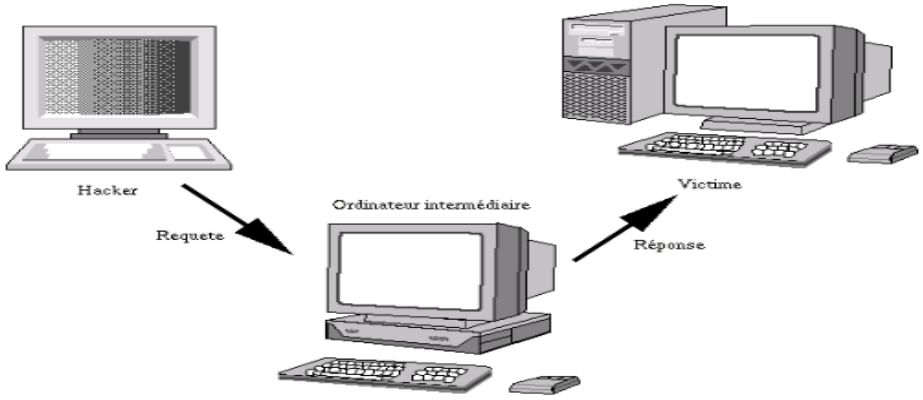

Figure 1.9: attaques à réponse indirecte

1.2.4 Les protocoles de sécurités :

- **SSL (Secure Sockets Layer) :**

SSL (Secure Sockets Layers) est un procédé de sécurisation des transactions effectuées via Internet. Il repose sur un procédé de cryptographie par clef publique afin de garantir la sécurité de la transmission de données sur Internet. Son principe consiste à établir un canal de communication sécurisé entre deux machines (un client et un serveur) après une étape d'authentification. Le système SSL est indépendant du

protocole utilisé, ce qui signifie qu'il peut aussi bien sécuriser des transactions faites sur le Web par le protocole HTTP que des connexions via le protocole FTP, POP ou IMAP. En effet, SSL agit telle une couche supplémentaire, permettant d'assurer la sécurité des données, situées entre la couche application et la couche transport (protocole TCP par exemple). [15]

- **TLS (Transport Layer Security) :**

  Est le successeur du protocole SSL. Est une nouvelle version de SSL. Cela fonctionne plus ou moins comme le SSL, utilisant le chiffrement pour protéger le transfert des données et de l'information. Les deux termes sont généralement utilisés de façon interchangeable dans l'industrie bien que SSL soit toujours largement utilisé. [16]

- **Le Protocol SSH :**

  SSH est à la fois un protocole et un ensemble de programmes. Il possède plusieurs fonctionnalités. Il permet par exemple d'établir des sessions sécurisées sur un ordinateur distant, de transférer des fichiers sécurisés ou d'établir des tunnels sécurisés. Pour ce qui concerne l'établissement de communications sécurisées, SSH se base sur le protocole SOCKS v5 intégré dans la plupart des équipements réseau. SSH apporte donc une amélioration indéniable aux protocoles non sécurisés tels que Telnet, Rlogin, FTP. [17]

- **IPSec (Internet Protocol Security) :**

Est un protocole de niveau 3. Il est très utilisé lors de la création de réseaux virtuels et pour la sécurisation des accès distants à un intranet. Les services IPSec sont basés sur des mécanismes cryptographiques qui leur confèrent un niveau de sécurité élevé. La sécurisation se faisant au niveau IP, IPSec peut être mis en œuvre sur tous les équipements du réseau et fournir un moyen de protection unique pour les échanges de données.

IPSec s'insère dans la pile de protocoles TCP/IP au niveau d'IP. Ceci présente l'avantage de le rendre exploitable par les niveaux supérieurs et d'offrir un moyen de protection unique pour toutes les applications. [18]

1.2.5 Les mécanismes défense :

- **Pare-feu :**

  Le pare-feu Un élément (logiciel ou matériel) du réseau informatique contrôlant les communications qui le traversent. Il a pour fonction de faire respecter la politique de

sécurité du réseau, celle-ci définissant quels sont les communications autorisés ou interdits. N'empêche pas un attaquant d'utiliser une connexion autorisée pour attaquer le système. Ne protège pas contre une attaque venant du réseau intérieur (qui ne le traverse pas). [19]

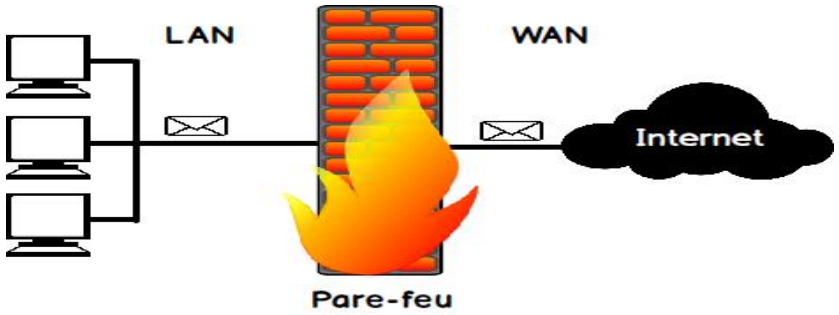

Figure 1.10: pare-feu.

- **Anti-virus :**

  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. [20]

- **Proxy :**

  Un serveur proxy (traduction française de «proxy server», appelé aussi «serveur mandataire») est à l'origine une machine faisant fonction d'intermédiaire entre les ordinateurs d'un réseau local et internet. La plupart du temps le serveur proxy est utilisé pour le web, il s'agit alors d'un proxy HTTP. Toutefois il peut exister des serveurs proxy pour chaque protocole applicatif (FTP, ...).

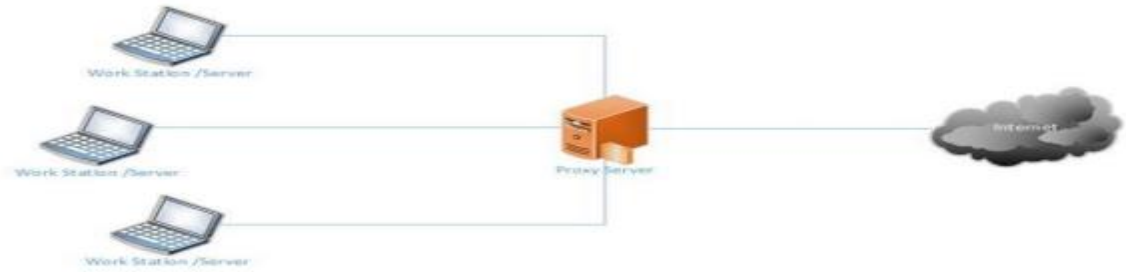

Figure 1.11: proxy

- **DMZ :**

  Une zone démilitarisée (ou DMZ, DeMilitarized Zone) est une zone de réseau privée ne faisant partie ni du LAN privé ni de l'Internet. À la manière d'une zone franche au-delà de la frontière, la DMZ permet de regrouper des ressources nécessitant un niveau de protection intermédiaire. Comme un réseau privé, elle est isolée par un firewall mais avec des règles de filtrage moins contraignantes. [22]

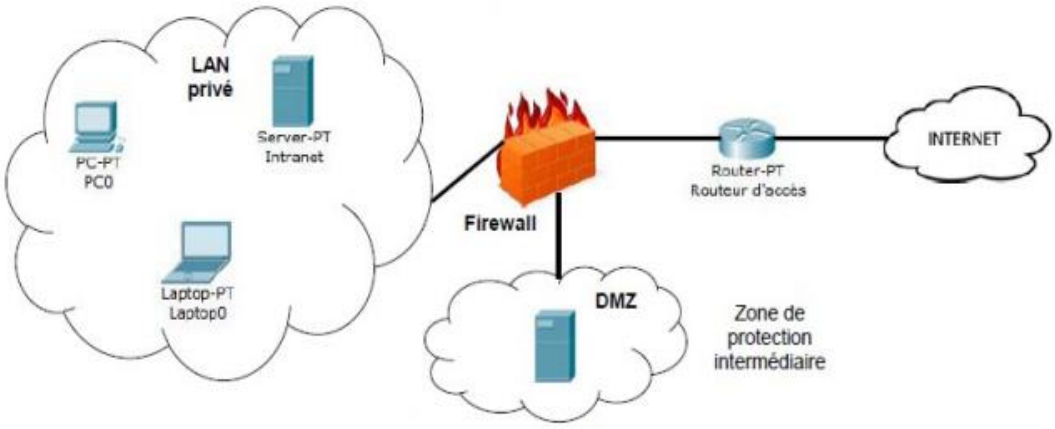

Figure 1.12: le DMZ.

Partie 2 : Généralité sur la sécurité d'un serveur web

2.1 Le système client /serveur :

Le web est un système d'information distribué vaste permettant au client d'accéder aux objets de données partagées sur différent serveur. Le web est basé sur le modèle client-serveur où la communication se fait sous la forme de requête-réponse, et elle est toujours initialisée

par le client, ce dernier accède aux documents web à l'aide browser, lorsque le client sélectionne le document demandé, le browser doit créer un requête équivalent et l'envoyer au serveur web correspondant. [23]

- **Client web :** c'est un programme, qui établit une connexion avec un serveur afin d'envoyer des demandes de service (requête), a ce dernier .le demandeur (client) de service commence par l'envoi d'une demande de connexion au serveur original, puis il envoie les requêtes, le client peut connecter DNS pour avoir adresse IP de serveur original dans chaque URL.
- **Serveur web :** c'est un programme qui accepte des connexions avec des clients (le demandeur des services) afin de le service en envoyant des réponses à leur requête. Un serveur web est un ordinateur qui joue le rôle de serveur informatique avec des logiciels du type serveur http. Il existe deux types de serveur :

  Serveur original (final) : où les ressources original sont créés et stockées comme : HTTP, ftp…etc.

  Serveur intermédiaire : qui peut jouer le rôle d'un serveur pour le client et le rôle d'un client pour un autre serveur (le serveur proxy).

- **Présentation de l'architecture client /serveur :** .Le World Wide Web parmi les applications qui sont bâties selon l'architecture client /serveur. Un serveur est un programme ou machine qui offre un service (application, accès à des sources de données ….etc.)Sur le réseau. Ces services sont fournir par le dialogue entre client et serveur, ce client va être demandeur de service qui est un navigateur web (IE, Firefox……).Pour fournir le service web, le serveur doit être connecté au réseau et exécute la démo HTTP (HTTP daemon) qui est le programme implémentant le Protocol http. [23]

Le principe de fonctionnement de client /serveur:

- Le navigateur se connecte à un serveur sécurisé : une clé de cryptage unique est mise en place tout au long de la transaction entre le serveur et le navigateur.
- Le navigateur envoie des données cryptées à destination du serveur, le seul à déchiffrer les informations reçues, grâce à la mise en place d'une clé d'échange unique.
- Le serveur envoie un avis de bonne réception de l'information.
- Le client vérifie la validité du certificat (donc l'authenticité du marchand),

- Il crée une clé secrète aléatoire, chiffre cette clé à l'aide de la clé publique du serveur, puis lui envoie le résultat (la clé de session).
- Le serveur est en mesure de déchiffrer la clé de session avec sa clé privée.
- Les deux entités sont en possession d'une clé commune dont ils sont seuls connaisseurs. Le reste des transactions peut se faire à l'aide de clé de session, garantissant l'intégrité et la confidentialité des données échangées. [24]

2.2 Notion sur HTTPS ou HTTP Secure :

HTTPS n'est pas l'opposé de HTTP mais plutôt son petit cousin. Tous deux sont des protocoles de transfert hypertexte qui permettent à des données web d'être affichées sur votre écran lorsque vous envoyez une requête. Cependant, HTTPS est légèrement différent, plus avancé et bien plus sécurisé.

Figure 1.13: à comparaison entre HTTP et HTTPS. [25]

2.2.1 Définition HTTPS :

HTTPS veut dire HyperText Transfer Protocol Secure (protocole de transfert hypertextuel sécurisé), et c'est une extension sécurisée du protocole HTTP. Il est utilisé pour sécuriser les communications sur internet ou sur un réseau. Le « S » à la fin est l'initiale du mot « Secure » (sécurisé) signifie que les données échangées entre le navigateur de

l'internaute et le site web sont chiffrées et ne peuvent en aucun cas être espionnées (confidentialité) ou modifiées (... et il fonctionne grâce au protocole TLS (Transport Layer Security), le successeur du protocole SSL (Secure Sockets Layer), la technologie de sécurité standard pour établir une connexion chiffrée entre un serveur web et un navigateur. Sans la présence de HTTPS, toutes les données que vous entrez sur un site (ex : nom d'utilisateur, mot de passe, carte bancaire, RIB ou tout autre information requise dans un formulaire) seront envoyées en format de texte brute et seront, par conséquent, vulnérables aux interceptions et à l'espionnage. C'est pour cette raison que vous devriez toujours vérifier qu'un site utilise bien HTTPS avant d'y entrer quelques données que ce soit.

En plus de chiffrer les données transmises entre un serveur et votre navigateur, le protocole TLS authentifie également le serveur auquel vous vous connectez et protège les données transmises de toute altération. [26]

2.2.2. Le principe HTTPS :

Le protocole HTTPS passe par un certificat SSL (Secure Socket Layer) qui permet de » poser » la couche TLS de sécurité. Ce certificat électronique s'applique au site pour sécuriser les échanges de données en assurant leur chiffrement à l'aide d'une clé de cryptage asymétrique. [26]

2.3 Le protocole SSL :

2.3.1 SSL (Secure Socket Layer) :

La clé publique de cryptage des données de l'utilisateur**.** Est une couche de chiffrement de protocole basée sur HTTPS. Il a été développé à l'origine par Netscape puis consolidé par l'IETF (Internet Engineering Task Force). RFC (Request for feedback), le RFC contient de nombreuses spécifications de technologie Internet. Permet la transmission de données chiffrées sur le réseau Internet. [27].

2.3.2 Historique SSL :

Initialement développé par Netscape, le SSL sort en 1995 dans sa version SSL 2.0 (le SSL 1.0 n'étant jamais sorti). Mais après la découverte de plusieurs vulnérabilités en 1996, la version 2.0 est vite remplacée par le SSL 3.0. *Remarque :* les versions 2.0 et 3.0 sont parfois libellées ainsi *:* SSLv2 et SSLv3. Basé sur le SSL 3.0, le TLS est introduit en 1999 comme la nouvelle version du SSL. [28]

2.3.3 Comment fonctionne SSL:

Lorsque l'ordinateur est connecté à un site Web qui utilise SSL, le navigateur Web de l'ordinateur demandera le site Web et le serveur Web enverra une copie de son certificat SSL à l'ordinateur. Un certificat SSL est un petit certificat utilisé par l'identité d'un site Web. Il s'agit d'obtenir un certificat SSL. Après cela, il chargera les données après cela, puis le navigateur Web et le vérifiera, le navigateur Web et le serveur Web. [29]

2.4 Service offert par SSL :

SSL permet d'assurer les services de sécurité suivants : [30]

- **Confidentialité :** Le client et le serveur doivent garantir que leurs conversations ne peuvent pas être écoutées par des tiers. Cette fonctionnalité est assurée par un algorithme de chiffrement. [34]
- **Intégrité :** Les clients et les serveurs doivent être en mesure de vérifier que les messages transmis n'ont pas été tronqués ou altérés (intégrité) et proviennent de l'expéditeur prévu. Ces fonctions sont assurées par des signatures de données. [30]
- **Authentification :** Le client doit pouvoir vérifier l'identité du serveur. Depuis SSL 3.0, le serveur peut également demander au client de s'authentifier. Cette fonctionnalité est garantie par l'utilisation de certificats. [30]

2.5 Système de sécurisations utilisé par SSL :

Il existe deux parties dans une communication chiffrée : l'expéditeur, qui chiffre les données, et le destinataire, qui les déchiffre. [31]

2.5.1 Système de chiffrement symétrique :

On utilise la même clé pour chiffrer et déchiffrer un message. [32]

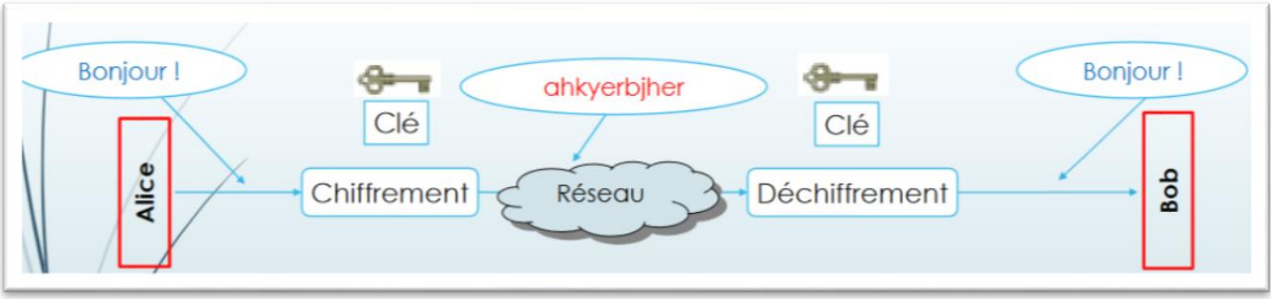

Figure 1.14: le chiffrement symétrique. [32]

2. 5.2. Système de chiffrement asymétrique :

Utilisation d'une paire de clés:

• Publique: Connue par tout le monde, utilisée généralement pour crypter ou vérifier la signature des messages.

• Privée: Connue uniquement par le détenteur, utilisée pour décrypter et signer des messages.

Un message chiffré avec une clé publique ne peut être déchiffré qu'avec la clé privée correspondante. [32]

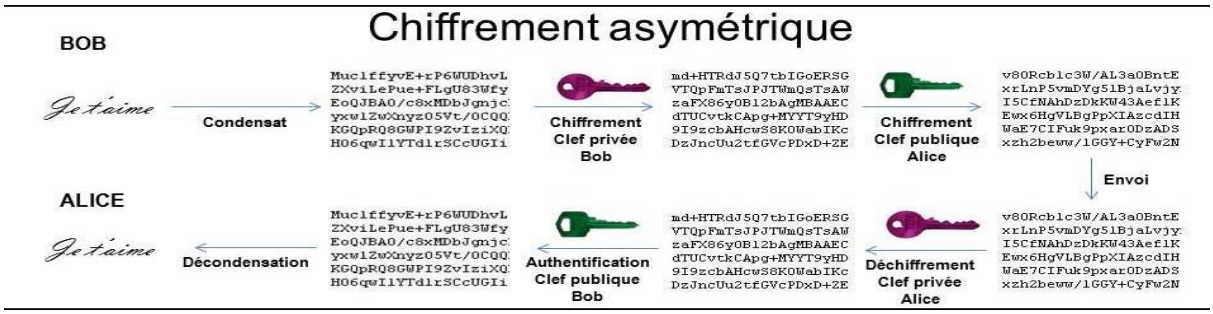

Figure 1.15: le chiffrement symétrique. [32]

2.5.3. Système de signature cryptographique :

La signature numérique est un mécanisme qui permet d'authentifier un message, autrement dit de prouver qu'un message provient bien d'un expéditeur donné, à l'instar d'une signature sur un document papier. Par exemple le certificat numérique.

- Les certificats numériques simplifient la tâche qui consiste à déterminer si une clé publique appartient réellement à son détenteur supposé.

- Un certificat est un document électronique émis par une tierce partie de confiance qui permet de garantir l'authenticité d'une clé publique. Un certificat contient notamment :

  1) l'identité de l'AC;

  2) L'identité du propriétaire;

  3) la clé publique du propriétaire;

  4) la date d'expiration du certificat;

  5) la signature de l'AC qui a délivré le certificat;

  6) d'autres informations qui n'entrent pas dans la portée de cet article.

- . L'organisme certifier est appelé CA: Certification Authority (autorité de certification).

- Un certificat correspond à une référence. Il peut s'agir par exemple de votre permis de conduire, de votress carte de sécurité sociale ou de votre certificat de naissance.

Validation du certificat : [33]

Quand Alice chiffre un message destiné à Bob, elle utilise le certificat de Bob. Avant d'utiliser la clé publique incluse dans le certificat de Bob, des étapes supplémentaires sont nécessaires pour valider le certificat de Bob. Il faut vérifier :

1. la période de validité du certificat de Bob;

2. que le certificat appartient bien à Bob;

3. que le certificat n'a pas été altéré;

4. que le certificat de Bob a été signé par une AC de confiance. De plus, si Alice doute de l'authenticité de l'AC de Bob, d'autres étapes seraient nécessaires pour valider le certificat de cette AC. Ces étapes sont identiques à celles requises pour valider le certificat de Bob.

Le destinataire vérifier un certain nombre d'aspects au sujet de l'émetteur pour s'assurer que le certificat est valide et qu'il appartient bien à la personne à qui il est censé appartenir. Il peut notamment :

1. comparer l'identité du propriétaire;

2. vérifié que le certificat est toujours valide;

3. vérifié que le certificat a été signé par un AC de confiance;

4. vérifier la signature du certificat de l'émetteur pour s'assurer que ce dernier n'a pas été altéré.

Bob peut maintenant vérifier le certificat d'Alice et avoir la certitude que c'est bien la clé privée d'Alice qui a servi à signer le message. Alice doit prendre des précautions avec sa clé privée et ne pas révéler comment y accéder; ce faisant, elle met en pratique une partie de la non-répudiation, une caractéristique associée à la signature numérique. Comme nous le verrons à la section 3.2, d'autres conditions sont essentielles au maintien de la non-répudiation. Notez que les certificats sont signés par une AC, ce qui signifie qu'ils ne peuvent être altérés. La signature de l'AC peut, à son tour, être vérifiée à l'aide du certificat de cette AC.

Dans l'exemple ci-dessous, il est présumé que Bob et Alice ont toute deux confiances en l'AC.

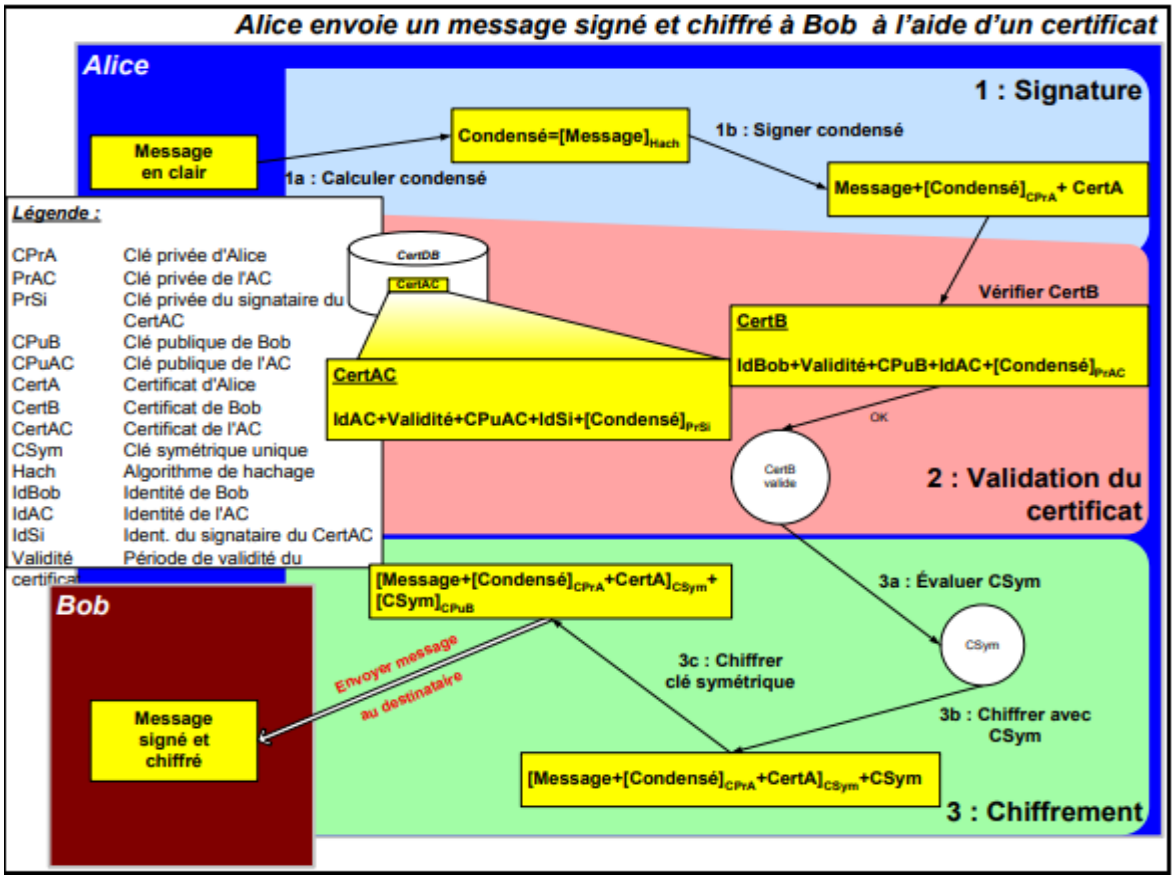

Figure 1.16: Processus détaillé de signature et de chiffrement à l'aide de certificats. [33]

Dans la figure 2.4 ci-dessus, une étape de validation de certificat a été ajoutée. Seuls les champs requis pour la validation d'un certificat sont affichés.

Alice veut s'assurer que la CPuB incluse dans le CertB appartient bien à Bob et qu'elle est toujours valide.

- Elle vérifie le champ Id et trouve IdBob, qui représente l'identité de Bob. En fait, la seule chose qu'elle sait réellement est que ce certificat semble appartenir à Bob

- Elle vérifie ensuite les champs de validité et constate que la date et l'heure actuelles entrent dans la période de validité. Jusque-là, le certificat semble bien appartenir à Bob et être valide. • La dernière vérification consiste à vérifier la signature du CertB à l'aide de la clé publique de l'AC (CPuAC incluse dans le CertAC) [10]. Si la signature du CertB est valide, cela signifie que :

1. Le certificat de Bob a été signé par l'AC en laquelle Alice et Bob ont pleinement confiance.

2. L'intégrité du certificat de Bob est prouvée et il n'y a donc eu aucune altération.

3. L'identité de Bob est assurée et la clé publique incluse dans le certificat est toujours valide et appartient bien à Bob. Par conséquent, Alice peut chiffrer le message et avoir la certitude que seul Bob pourra le lire. Bob exécutera les mêmes étapes pour le certificat d'Alice avant de vérifier la signature d'Alice. [33]

Parmi ces certificats on trouve le certificat SSL :

2.5.4. Les certificats SSL:

Un certificat SSL est un fichier de données qui lie une clé cryptographique aux informations d'une organisation. Installé sur un serveur, le certificat active le cadenas et le protocole « https », afin d'assurer une connexion sécurisée entre le serveur web et le navigateur. Le SSL est généralement utilisé pour sécuriser les transactions bancaires, le transfert de données et les informations de connexions. Il est récemment devenu la norme pour sécuriser la navigation sur les sites de réseaux sociaux. [34]

Les certificats SSL lient ensemble :

- Un nom de domaine, un nom de serveur et un nom d'hôte.
- L'identité de l'organisation (nom d'entreprise) et le lieu.
    - **Fonctionnement d'un certificat SSL :**

Les certificats SSL utilise ce qu'on appelle la cryptographie à clé publique.
Ce type de cryptographie exploite la puissance de deux clés qui sont de longues chaînes de nombres générés de manière aléatoire. L'une est appelée clé privée et l'autre clé publique, Une clé publique est connue de votre serveur et disponible dans le domaine public. Elle peut être utilisée pour chiffrer n'importe quel message. Si Alice envoie un message à Bob, elle le verrouillera avec la clé publique de Bob, mais la seule façon de le décrypter est de le déverrouiller avec la clé privée de Bob. Bob est le seul propriétaire de sa clé privée et il est par conséquent le seul à pouvoir l'utiliser pour déverrouiller le message d'Alice. Si un pirate

informatique intercepte le message avant que Bob ne le déverrouille, tout ce qu'il obtiendra est un code cryptographique qu'il ne pourra pas déchiffrer, même avec la puissance d'un ordinateur.

Dans le contexte d'un site web, la communication a lieu entre un site et un serveur. Votre site web et votre serveur sont Alice et Bob.

- **Les différents types de certificats SSL** :

Il existe trois types de certificats SSL : les certificats à validation de domaine (DV), les certificats à validation d'organisation (OV) et les certificats à validation étendue (EV). Les niveaux de chiffrement sont les mêmes pour chaque type de certificat. Ce qui diffère, ce sont les processus d'audit et de vérification nécessaires pour obtenir le certificat.

Le nombre d'entreprises utilisant des certificats SSL a considérablement augmenté au cours des dernières années, et les cas d'application du SSL se sont diversifiés. Par exemple :

- vous pourriez avoir besoin du SSL pour assurer la confidentialité des communications (afin de ne pas être espionné),
- où vous pourriez vouloir prouver que vous pouvez faire confiance à votre interlocuteur (identité au niveau de la communication privée).

- **Certificats SSL à validation étendue EV (**"Extended validated") permet une sécurité renforcée de votre site par la présence d'une barre verte sur la ligne d'URL du browser.
- **Certificats SSL à validation de domaine DV** (Domain validated") permet de sécuriser un site internet.
- **Certificats SSL à validation de l'organisation OV (**"Organisation validated") sécurise le site internet institutionnel de votre organisation.
- **Certificat RGS*** : Ce certificat s'adresse aux organisations du secteur public. Il respecte la norme RGS et est reconnu par l'administration française

2.6 Fonctionnement d’un protocole sécurisé :

2.6.1 Authentification du serveur :

Le serveur envoie son certificat au client et lui liste les algorithmes cryptographiques. Le client vérifie la validité du certificat à l'aide de la clé publique du CA (Certificate Authority) contenue dans le navigateur. Les données échangées par la suite entre le client et le serveur sont chiffrées et authentifiées à l'aide de clés dérivées de la clé maître. [37]

2.6.2 Authentification du client :

Le serveur peut exiger que le client s'authentifie en demandant d'abord son certificat. Le client répond en envoyant ce certificat puis en signant un message avec sa clé privée (Ce message contient des informations sur la session et le contenu de tous les échanges précédents. [37]

2.6.3 Chiffrement des données :

Le cryptage des données est une méthode de conversion des données du texte brut (non crypté) en texte chiffré (crypté), les données sont plus vulnérables en raison du besoin de décryptage avant la transmission et des faiblesses de la méthode de transmission elle-même. Le cryptage des données en transit ou le cryptage de bout en bout assure leur confidentialité même si elles sont interceptées**.** [38]

2.7 Les sous-protocoles SSL :

Le protocole SSL est constitué de quatre sous-protocoles:

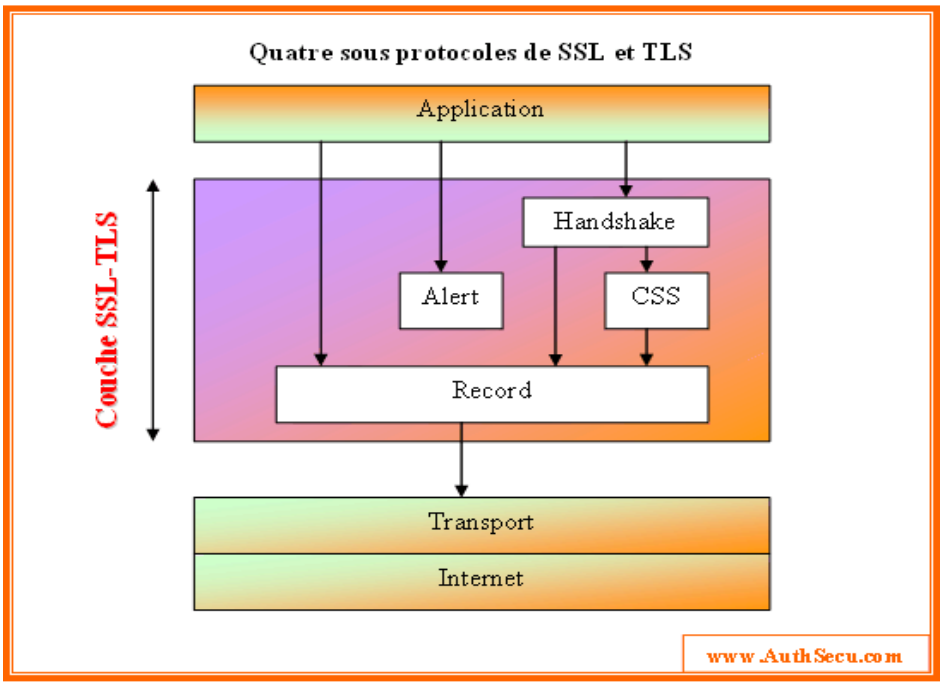

Figure 1.17: sous protocoles SSL.

2.7.1 Le protocole Handshake :

Ce protocole permet au serveur et au client de s'authentifier mutuellement ; ce protocole permet au client et au serveur de s'authentifier mutuellement, de négocier les algorithmes de chiffrement, de négocier les algorithmes de MAC et enfin de négocier les clés symétriques qui vont servir au chiffrement. [35]

2.7.2. Le protocole Change Cipher Spec :

Ce protocole contient un seul m2.essage, Il est utilisé pour indiquer le protocole de journalisation pour implémenter les algorithmes cryptographiques qui viennent d'être négociés. [36]

2.7.3 Le protocole Alert:

Ce protocole spécifie les messages d'erreur que peuvent s'envoyer clients et serveurs. Les messages sont composés de 20 octets, le premier étant soit fatal soit warning. Si le niveau de criticité du message est fatal, la connexion SSL est abandonnée. Le deuxième octet est utilisé pour le code d'erreur. [35]

2.7.4 Le protocole SSL Record :

Ce protocole intervient après l'émission du message ChangeCipherSpec.il permet de garantir:

- la confidentialité à l'aide de chiffrement des données
- l'intégrité à l'aide de génération d'un condensât. [36]

2.8 Echange entre SSL et HTTPS :

HTTPS et SSL sont connectés l'un à l'autre, et vous ne pouvez pas avoir l'un sans l'autre; Quant à HTTP, qui est le préfixe de lien d'origine.

L'installation d'un certificat SSL (Secure Socket Layer) sur votre site le sécurise, et lorsqu'un certificat SSL ou TLS valide est installé sur votre site, le préfixe du lien passera de HTTP à HTTPS.

Lorsqu'un navigateur accède à un site Web, il demande un certificat de confiance au serveur pour créer un canal de communication sécurisé. Ensuite, le serveur et l'appareil commencent à créer un protocole d'échange de chiffrement sécurisé qui contient les clés pour démarrer le processus de communication et d'envoi de données.

Si le serveur répond aux demandes du navigateur, il commence à ouvrir le site en toute sécurité et place l'icône (cadenas) à côté du domaine dans la barre de recherche. Cela signifie que le site est sécurisé et que les données sont protégées par cryptage (HTTPS) et (SSL/TLS).

Cependant, HTTPS et SSL sont deux choses distinctes, mais ils partagent une connexion solide. Pour mieux le comprendre, imaginons que HTTPS soit le pont sécurisé qui permet aux données de passer entre le serveur et l'utilisateur. Alors qu'un certificat SSL est un moyen de crypter ces données et de les cacher aux harceleurs.

Figure 1.18: échange entre SSL et HTTPS

Conclusion :

Dans ce chapitre nous avons présenté les réseaux et la sécurité informatique d'une façon générale, nous avons cité les classifications des réseaux et architecture réseau, dans ce qui suit nous allons présenter également les critères et les protocoles de sécurité, on parler aussi sur les mécanismes de défense, le chapitre suivant sera consacré pour la généralité sur la sécurité d'un serveur web. Nous avons défini la sécurité d'un serveur web. Le prochain chapitre sera consacré à la présentation de l'organisme d'accueil.

2.1 Introduction

Dans ce chapitre nous allons présenter l'entreprise Centre des Systèmes et Réseaux d'Information, de Communication de Télé-enseignement et de l'Enseignement à Distance (CSRICTED) dans laquelle nous avons effectué notre stage pour la réalisation de notre projet de fin de cycle, et qui nous permettra d'étudier les problèmes de l'entreprise. Ainsi de mètre une solution.

2.2 Présentation de l'université

L'Université de Bejaïa, crée en octobre 1983, est un établissement public pluridisciplinaire. Elle compte aujourd'hui plus de 45 700 étudiants, 1714 enseignants et 1227 personnels techniques et administratifs, répartis sur huit facultés : Technologie - Sciences Exactes - Droit et Sciences Juridiques et Administratives - Sciences de Nature et de la Vie - Lettres et Langues - Sciences Humaines et Sociales - Sciences Economiques, Sciences de Gestion et Sciences Commerciales - Sciences Médicales.

2.3 Visite Expresse de l'Université

L'université de Bejaia a réussi à mettre sur pied des formations de plus en plus en phase avec le monde du travail. Cette démarche lui a permis d'être mieux à l'écoute des besoins de ses partenaires économiques en matière de ressources humaines et de compétences.

L'Université de Bejaïa dispose actuellement une trentaine de laboratoires de Recherche, agréés par le Ministère de l'Enseignement Supérieur et de la Recherche Scientifique portant sur plusieurs domaines : Modélisation et Optimisation des Systèmes - Technologie des Matériaux et du Génie des Procédés-Matériaux organiques - Génie et de l'environnement – Hydraulique -Technologie Industrielle et de l'Information-Génie Electrique - Biomathématique, Biophysique Biochimie - Mathématiques Appliquées -Physique Théorique - Ecologie et Environnement - Economie et Développement - Microbiologie Appliquée - Biochimie Appliquée - Formation en langues Appliquées et Ingénierie des Langues en milieu Multilingue - Ecosystèmes Marin et l'Aquacole).

L’Université de Béjaïa a entrepris un travail de structuration important pour que la recherche puisse s’inscrire dans la compétition nationale et internationale et constituer une dynamique favorable à son essor et son rayonnement. En effet, elle a inscrit plusieurs projets de développement de la recherche en particulier: un incubateur technologique - un Centre d’Innovation et de Transfert de Technologie - un Centre National de Recherche en Technologie de l’Agroalimentaire.

2.4 Fonctionnement et Organisation de l'Université

L'université de Bejaia est composée d'un rectorat, d'organes décisionnels et pédagogiques, de facultés et départements. Elle comporte des services administratifs et techniques communs.

Le rectorat placé sous l'autorité du recteur de l'université comprend:

Des vice-rectorats placés sous la responsabilité de vice-recteurs.

Un secrétariat général de l'université chargé du fonctionnement et de la gestion administrative et financière des structures placées sous son autorité.

Une bibliothèque centrale de l'université placée sous la responsabilité d'un directeur chargé du fonctionnement et de la gestion des structures.

- **Les organes décisionnels:**

Le conseil d'administration étudie et propose toute mesure susceptible d'améliorer le fonctionnement de l'université et de favoriser la réalisation de ses objectifs.

Le conseil scientifique propose les orientations des politiques de recherche et de documentation scientifique et technique de l'université et donne son avis sur toute autre question d'ordre pédagogique et scientifique qui lui est soumise par son président.

- **Les organes pédagogiques:**

Conseil de discipline

Equipe de formation

Comité pédagogique par matière

Equipe pédagogique

2.5 Présentation de CSRICTED:

Le CSRICTED est l'un des services communs de l'université de Bejaïa, il se charge de la gestion de toutes les ressources informatiques de l'université ainsi que de l'assurance de la continuité des services informatiques et de leurs maintenances, tels que le service pédagogique, la disponibilité de la connexion aux réseaux intranet et internet et l'exploitation des différents services offerts, et enfin la maintenance du parc informatique de l'université. [40]

2.6 Organisation :

Le CSRICTED se constitue de quatre sections : la section système d'information, la section réseau, la section e-learning et la section maintenance. [40]

- **Organigramme :**

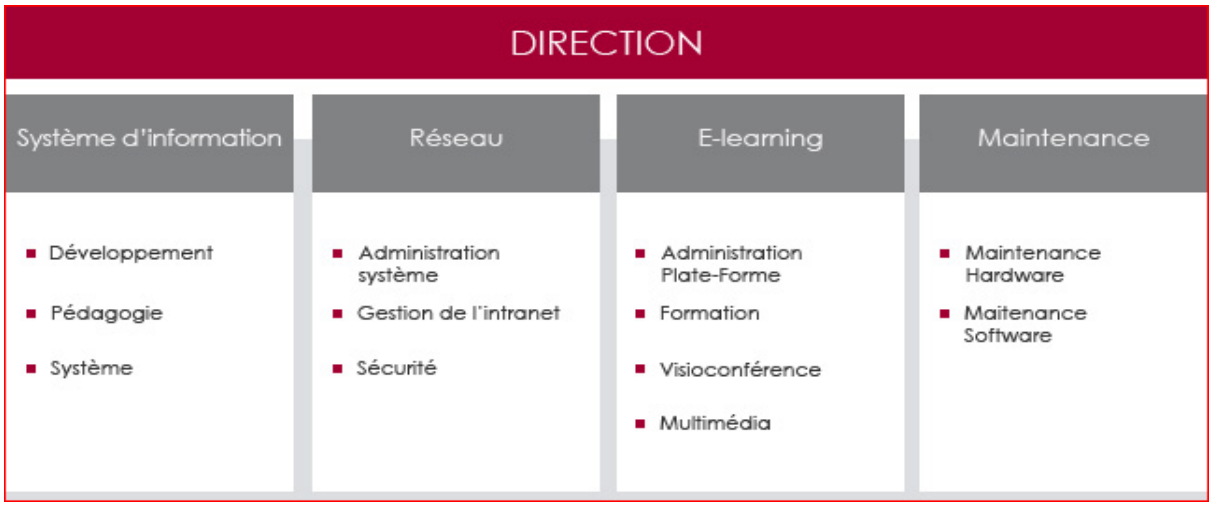

Figure 2.1: la direction

- **Description et Rôles de chaque section :**

1) Section Système d'Information :

La Section Système d'Information (S.I), a pour mission de mettre en œuvre la politique des systèmes d'information et des technologies de l'information et de la communication, la gestion d'une manière plus générale à tout ce qui touche au traitement automatique de l'information. [40]

La section se compose de trois cellules qui sont :

- **Cellule de développement** : elle se charge du développement et de la gestion des sites web de l'université et du développement d'applications de gestion.

- **Cellule pédagogique** : assure la maintenance des salles de TP, installation des systèmes et logiciels pédagogiques, planification des séances de TP et gestion du pack informatique (GLPI).
- **Cellule Système** : assure d'une manière plus efficace la gestion des utilisateurs des stations au sein de l'université (contrôleur de domaine).

***2*) Section Réseau :**

La section réseau a pour missions de maintenir le fonctionnement normal du réseau intranet de l'université, d'assurer la sécurité des équipements réseaux et des services offerts par le réseau au système d'information et aux applications et enfin de fournir des services de connexion internet, de messagerie électronique, de support utilisateur, d'étude et de suivi des projets réseau de l'université de Bejaia.

3) Section chargée du Télé-enseignement (e-learning) :

La section chargée du télé-enseignement est composée de 4 cellules:

- la cellule chargée de l'administration de la plateforme de télé-enseignement,
- la cellule chargée du multimédia et de l'infographie,
- La cellule chargée de la visioconférence.
- la cellule chargée de la formation.

Cette section a pour mission de prendre en charge toutes les opérations liées au e-learning à l'université de Bejaia. Son champ d'intervention concerne au moins deux domaines: le domaine pédagogique et le domaine technique.

Le domaine pédagogique englobe la formation des enseignants, des responsables et du personnel ATS de l'université sur l'usage des technologies de l'information et de la communication.

Le domaine technique englobe la mise en place d'une solution e-learning répondant à la fois aux besoins et aux ambitions de cette université. Il s'agit notamment de l'installation, de l'administration et de la maintenance des plates-formes de e-learning. En plus de cela, cette cellule gère une salle de visioconférence.

4) Section Maintenance :

Comme son nom l'indique, cette section assure le maintien en bon état des équipements informatiques des différents services de l'université. Elle est chargée de :

● installation Soft et Hard (conception et installation du système des micros ordinateurs) :

elle s'occupe du montage du microordinateur de bureau (montage d'une unité centrale complète), ensuite installation du système d'exploitation (Windows XP par exemple), logiciels et utilitaires nécessaires (Micro Soft Office, Adobe Accrobat, anti-virus…etc.)

● réparation Soft et Hard : l'objectif de la section est d'assurer la maintenance des

équipements informatiques de l'université. elle se charge donc de la réparation à savoir :

onduleurs, imprimantes, écrans et unités centrales lorsqu'il s'agit d'une panne électronique

(réparation des blocs d'alimentations à titre d'exemple), ainsi que les équipements réseau :

grands onduleurs (10KVA….), Switch, armoires …etc. [40]

2.7 Problématique et solution :

- **Problématique :**

La sécurité des réseaux informatique est un sujet essentiel pour favoriser le développement des échanges dans tous les domaines vu l'expansion et l'importance grandissante des réseaux informatiques lesquels ces derniers ont engendré le problème de sécurité des systèmes d'information. Dans la plupart d'organisations informatisées, partager les données directement entre machines est leur souci majeur. Il s'avère indispensable de renforcer les mesures de sécurités dans le but de maintenir la confidentialité, l'intégrité et le contrôle d'accès au réseau pour réduire les risques d'attaques. Afin d'assurer le bon

fonctionnement global de l'entreprise, on utilise une technique de la décomposition du réseau en zone de sécurités séparées est l'une des solutions les plus fiables que l'entreprise peut adapter pour protéger ses matérielles et logicielles.

Vu ses caractéristiques, est un moyen de lutter contre la violation potentielle du système de sécurité et les attaques contre la confidentialité. La bonne gestion de cette zone permet de minimiser les attaques venant du réseau externe, en autorisant les services dont l'entreprise a besoin. Cette décomposition appelée (DMZ) nécessite la mise en place d'un firewall pour pouvoir l'administrer.

- **solution**

La DMZ est sous réseau isole à la fois du réseau local et de l'internet, c'est en quelque sorte une zone tampon, entre un réseau sécurisé et un réseau non sécurisé, ou sont stockées les ressources les plus précieuses.

2.8 Conclusions :

Au terme de ce troisième chapitre consacré à la présentation de l'organisme d'accueil, et la détermination de la problématique liée à la sécurisation d'un serveur web apache. Le chapitre suivant sera consacré à la finalisation de notre projet qui consiste à la sécurisation d'un serveur web apache.

3.1 Introduction

Ce chapitre sera consacré à la sécurisation d'un serveur web apache de l'entreprise, l'Université Abderrahmane Mira de Bejaïa. Nous allons décrire les déférentes étapes suivies lors de la sécurisation de serveur web apache proposé par GNS3.

3.2 Environnement de travail (présentation des outils de travail) :

3.2.1 GNS3 :

GNS3 (Graphical Network Simulator) est un logiciel libre, est une solution open-source qui permet d'émuler des équipements informatiques (routeur, switch, PC…) et qui permet de simuler leurs fonctionnements.de réseaux informatiques. Il est la suite logique de paquet Tracer. [41]

Figure 3.1:GNS3.

3.2.2 VMware Workstation *:*

VMware Workstation est une solution logicielle professionnelle, est une gamme de produits d'hyperviseur de poste de travail qui permettent aux utilisateurs d'exécuter des machines virtuelles, des conteneurs et des clusters Kubernetes.

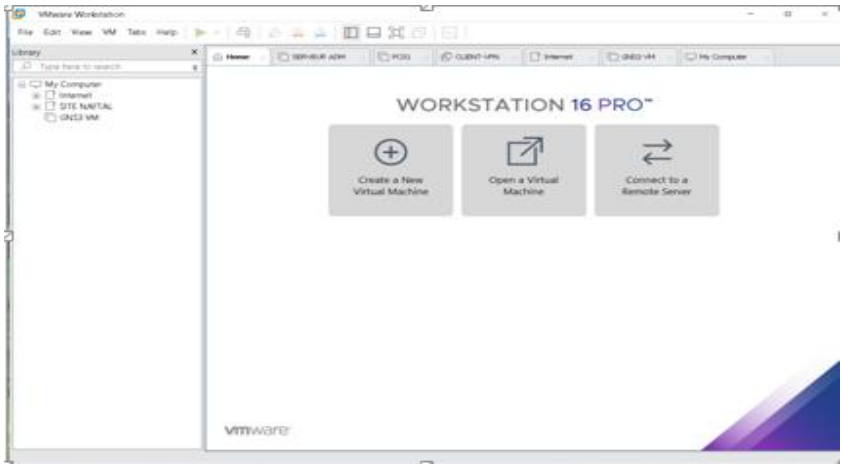

Figure 3.2: L'interface graphique de VMware Workstation pro 16.

3.2.3 Les machines virtuelles :

Windows 10 : Windows 10 est le dernier système d'exploitation de Microsoft, qui ramène de nombreuses fonctionnalités perdues des éditions précédentes et introduit des fonctionnalités longuement attendues qui étaient déjà disponibles sur les logiciels rivaux depuis un bon moment déjà. [42]

Windows serveur 2022 : Windows Server 2022 est l'actuel système d'exploitation commercialisé par Microsoft et destiné aux serveurs, La sécurité multicouche avancée de Windows Server 2022 offre la protection complète dont les serveurs ont actuellement besoin.

Debian 11 : Debian est un système d'exploitation et une distribution de logiciels libre. Le système d'exploitation Debian a annoncé le 14 août 2021 la sortie de sa nouvelle version stable en version **11** nommée "Bullseye".

DMZ : les DMZ ont pour objectif de renforcer le niveau de sécurité du réseau local de l'entreprise. Dans ce système, un nœud de réseau protégé et surveillé, tourné vers l'extérieur, a accès aux éléments exposés au sein de la zone dématérialisée tandis que le reste du réseau est protégé par un pare-feu.

3.3 Equipement (hard&soft) :

Le hardware (ou hard) qualifie le matériel informatique en général (les composants physiques), Software est un logiciel qui englobe à la fois le système d'exploitation et

l'application informatique qui parcourt l'ordinateur. Ils sont tous les deux indispensables au fonctionnement de votre appareil. [43]

- **Pc ou ordinateur :** c'est un équipement terminal, PC signifie personnel computer et désigne aujourd'hui l'ordinateur de bureau ou le micro-ordinateur.

- **Commutateur (switch)** : ressemble à hub et envoi des données et contrôlé, Contrairement au concentrateur qui envoie l'information à l'ensemble des ordinateurs connectés au réseau, le commutateur va établir une liaison seulement entre les ordinateurs intéressés par l'information. [44]
- **Le routeur** : est un équipement qui permet :

✓ L'interconnexion des réseaux.
✓ L'échange des informations entre deux réseaux,
✓ Il dispose d'un port (connecteur RJ45) par réseau, d'un système d'exploitation, et d'un logiciel chargé d'aiguiller (router) les informations.
✓ Permet d'assurer le routage des paquets afin de déterminer le chemin le plus adéquat qu'un paquet de données doit emprunter. [44]

- **Serveur :** Un serveur informatique offre des services accessibles via un réseau. Il les requêtes effectuées par un autre ordinateur appelé « client ». C'est pourquoi on entend souvent parler de relation « client/serveur ». [45]

  Serveur web : c'est ce qui permet à un navigateur web d'afficher un site internet.

  Serveur DNS (Domain Name system) : Un système de noms de domaine, ou DNS, traduit les noms de domaine lisibles par l'homme (par exemple www.amazon.com) en adresses IP lisibles par une machine (par exemple, 192.0.2.44).

- **Firewall:** *Un* firewall (ou pare-feu) est outil informatique (matériel et/ou logiciel) conçu pour protéger les données d'un réseau (protection d'un ordinateur personnel relié à Internet par exemple, ou protection d'un réseau d'entreprise). Il permet d'assurer la sécurité des informations d'un réseau en filtrant les entrées et en contrôlant les sorties selon des règles définies par son administrateur.

- **Navigateur web :** le navigateur web (ou browser en anglais) sont des logiciels qui permettent de consulter des pages web et des sites Internet.

- ✓ **Navigateur Firefox :** est un navigateur web libre et gratuit disponible pour PC (Windows, MacOs, Linux, BSD, etc.) et mobiles (Android, IOS), développé et distribué par la Mozilla Fondation depuis 2003, avec l'aide de milliers de bénévoles. L'entreprise Mozilla Corporation est créée en 2005 pour se charger du développement.

3.4 Architecture proposée :

La figure 4.6 : présente l'architecture que nous avons proposée sous GNS3.

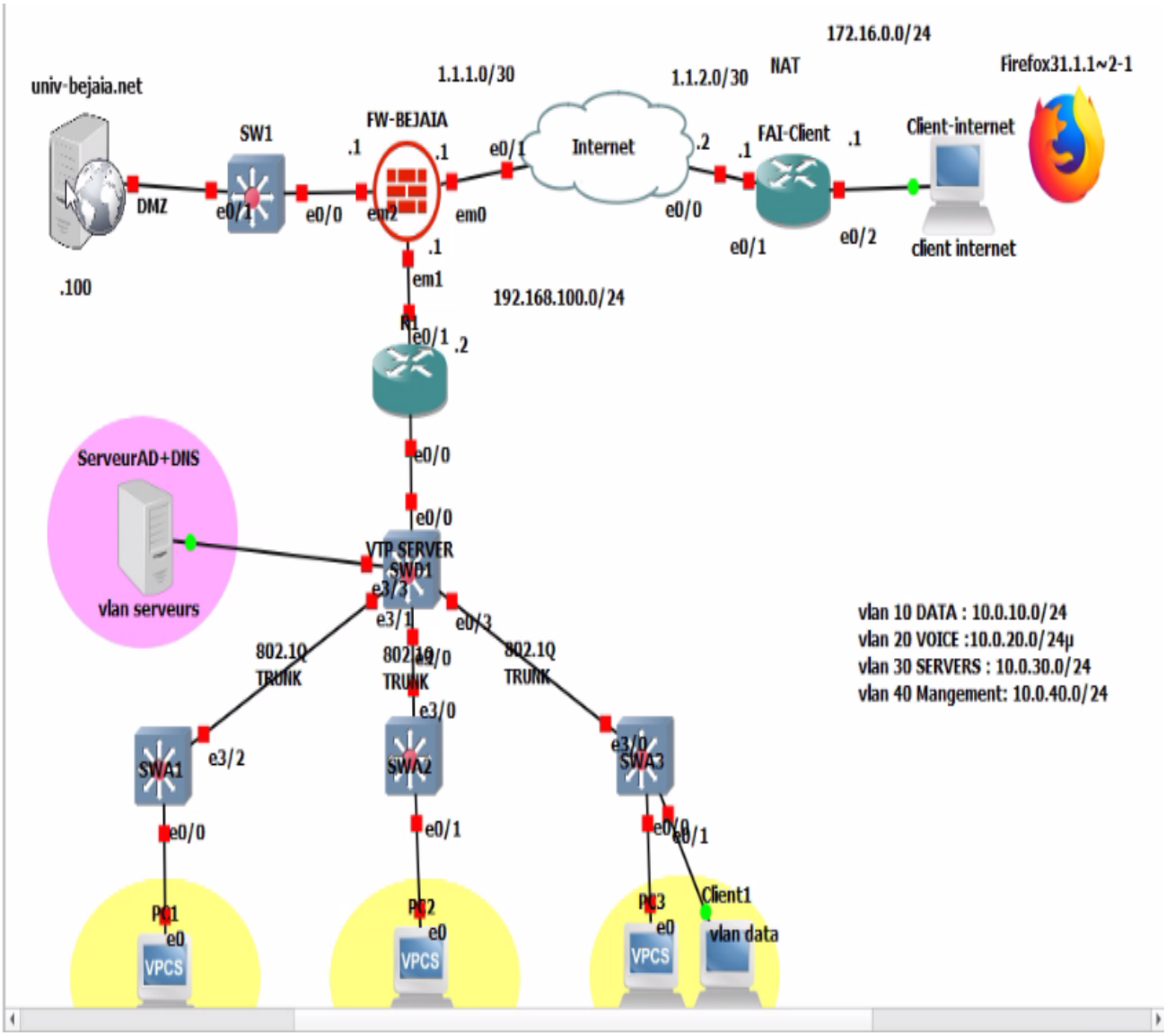

Figure 3. 3:Architecture proposée.

3.5 Méthodologie :

La définition du mode trnuk : Le mode trunk (la norme 802.1Q) est utilisé dans le cas ou plusieurs VLANs doivent circuler sur un même lien. C'est par exemple le cas de la liaison entre deux switchs ou bien le cas d'un serveur ayant une interface appartenant à plusieurs VLANs. Il est surtout avantageux pour les communications en interne étant donné que les appels téléphoniques, qui passent seulement par le réseau internet (WAN), sont gratuit.

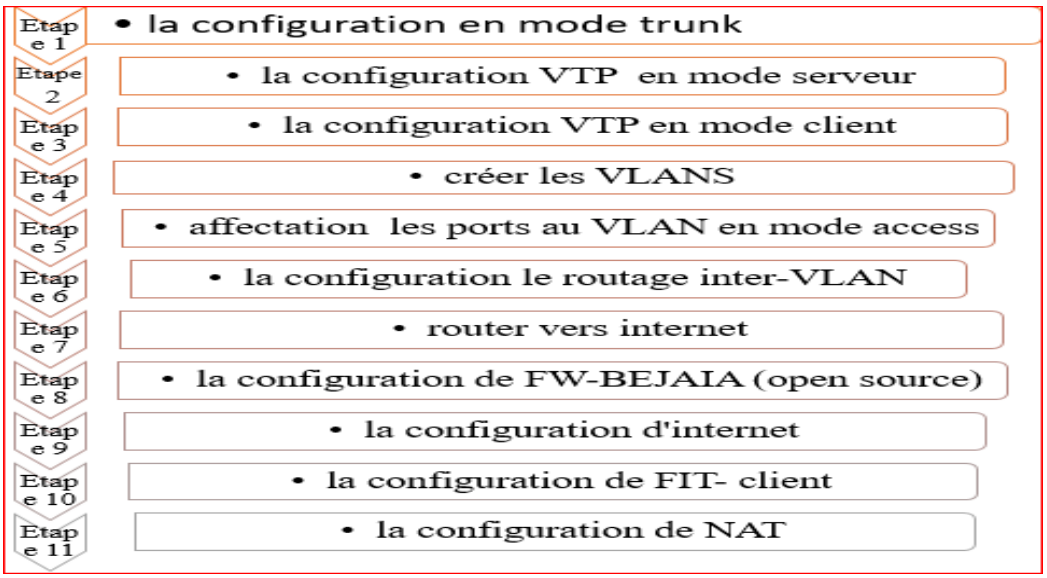

Figure 3.4 : diagramme des Etapes de configuration

Etape 1 : la configuration les interfaces en mode trunk :

SWD1 (distributeur) :

Tout abord on montre les voisins de notre serveur SWD1 avec la commande show cdp Neighbors :

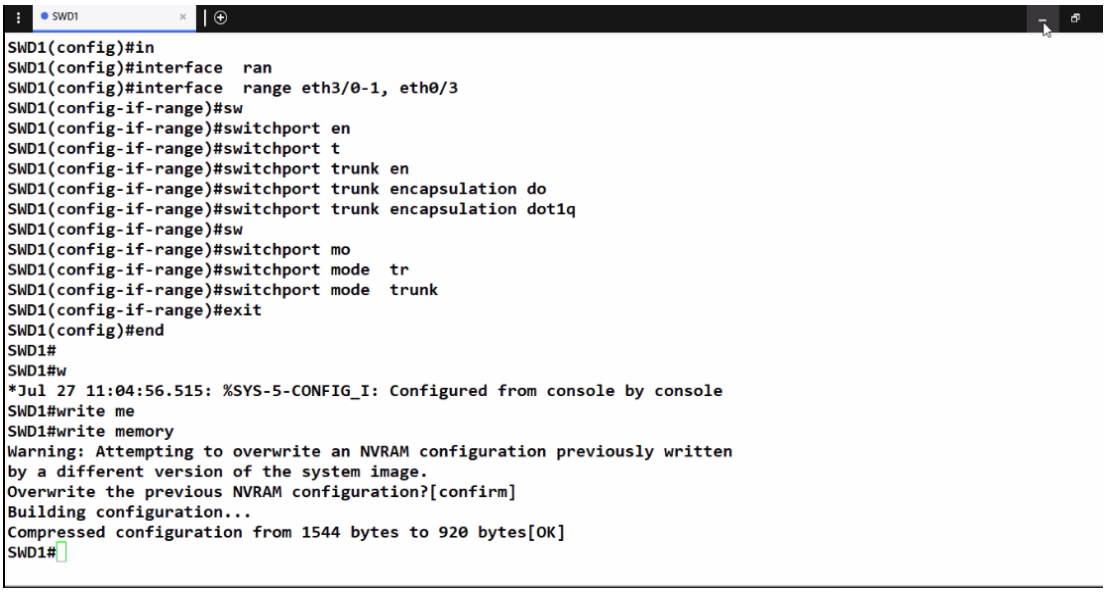

Figure 3.5: la configuration en mode trunk de SWD1

SWA1 :

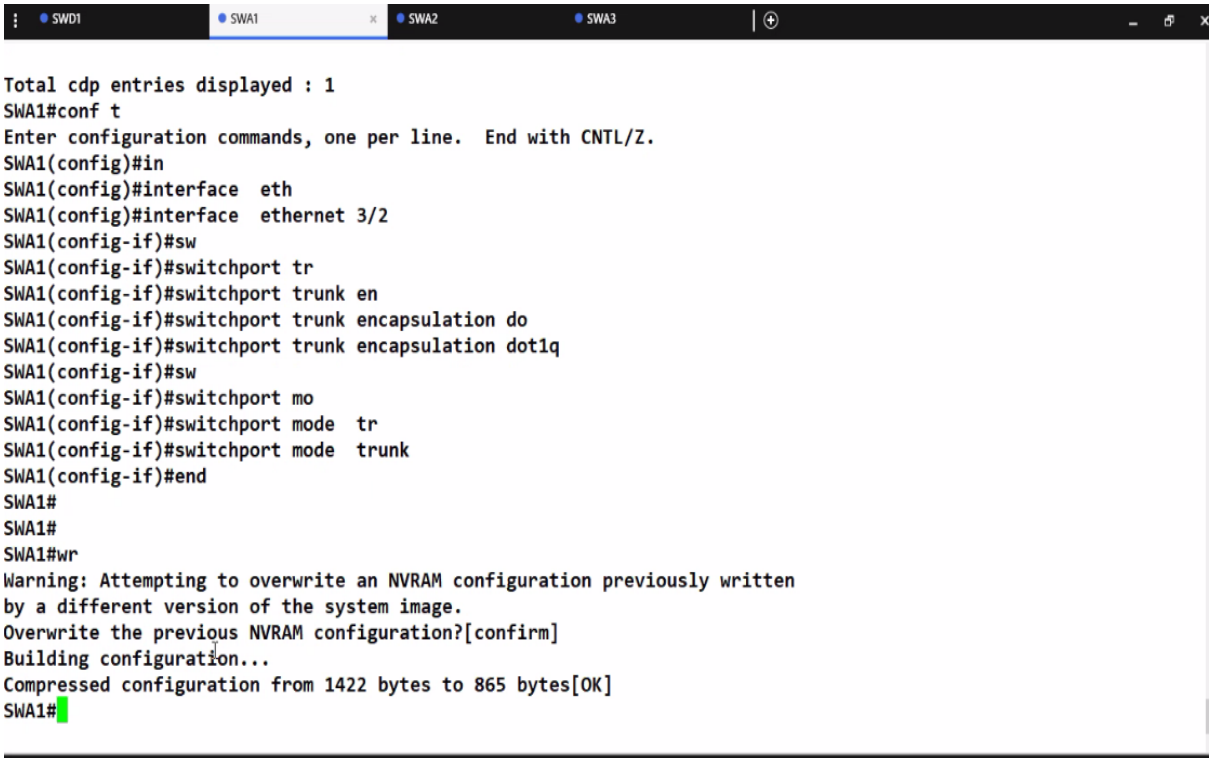

Figure 3.6: la configuration en mode trunk de SWA1.

SWA2 :

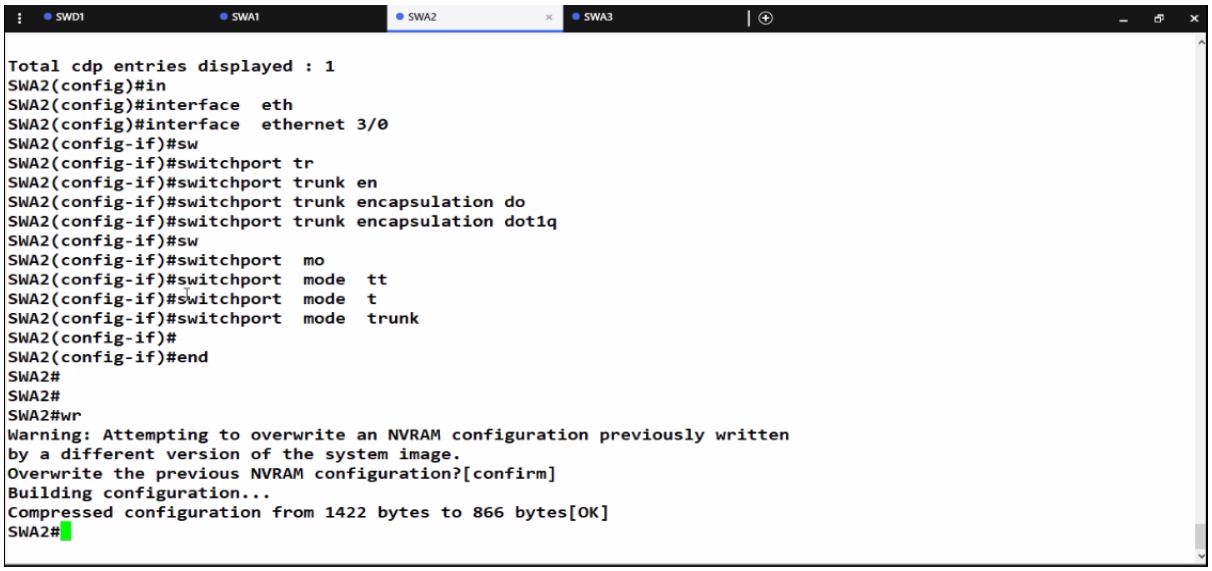

Figure 3.7: la configuration en mode trunk de SWA2.

SWA3 :

Interface connecté vers SWD1 :

On tape la commande show cdp neighbors:

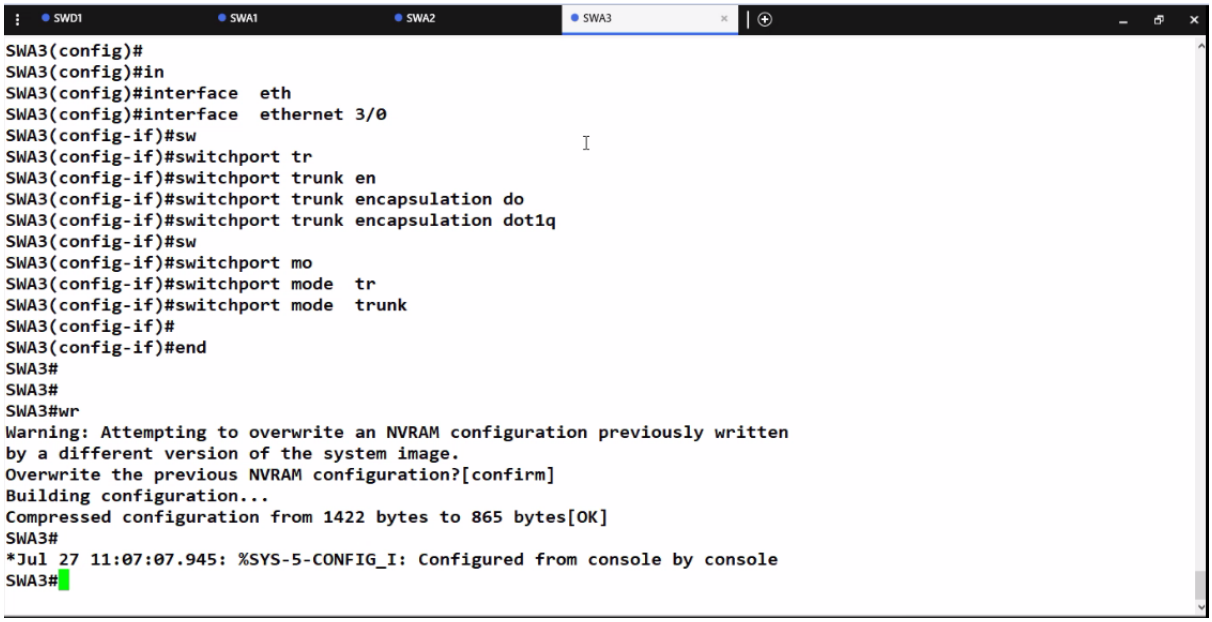

Figure 3.8: la configuration en mode trunk de SWA3

Configuration VTP : VTP ou VLAN Trunking Protocol est un protocole de niveau 2 utilisé pour configurer et administrer les VLAN sur les périphériques, en mode trunk .Il a trois type mode VTP serveur, client, transparence.

Etape 2 : la configuration VTP en mode serveur :

Pour administrer tous, le serveur qui va gérer les clients.

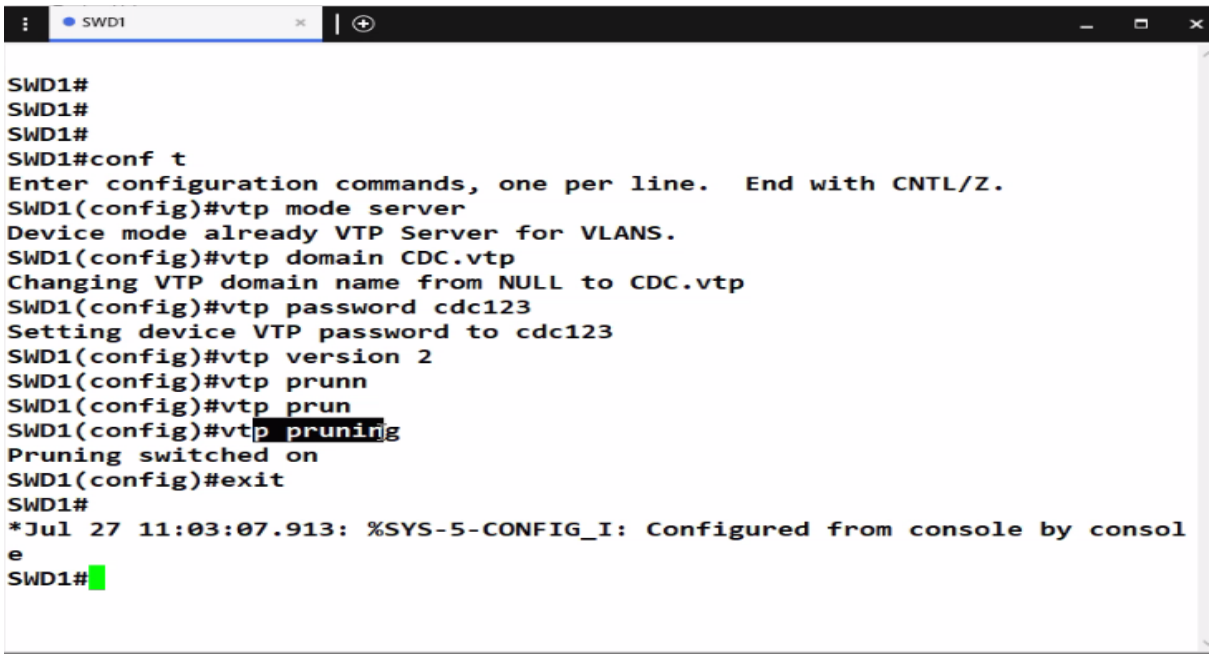

Figure 3.9:la configuration VTP en mode serveur.

Etape 3 : la configuration VTP en mode client : pour appliquer les VLANs, et pour faciliter la gestion des VLANs.

SWA1 :

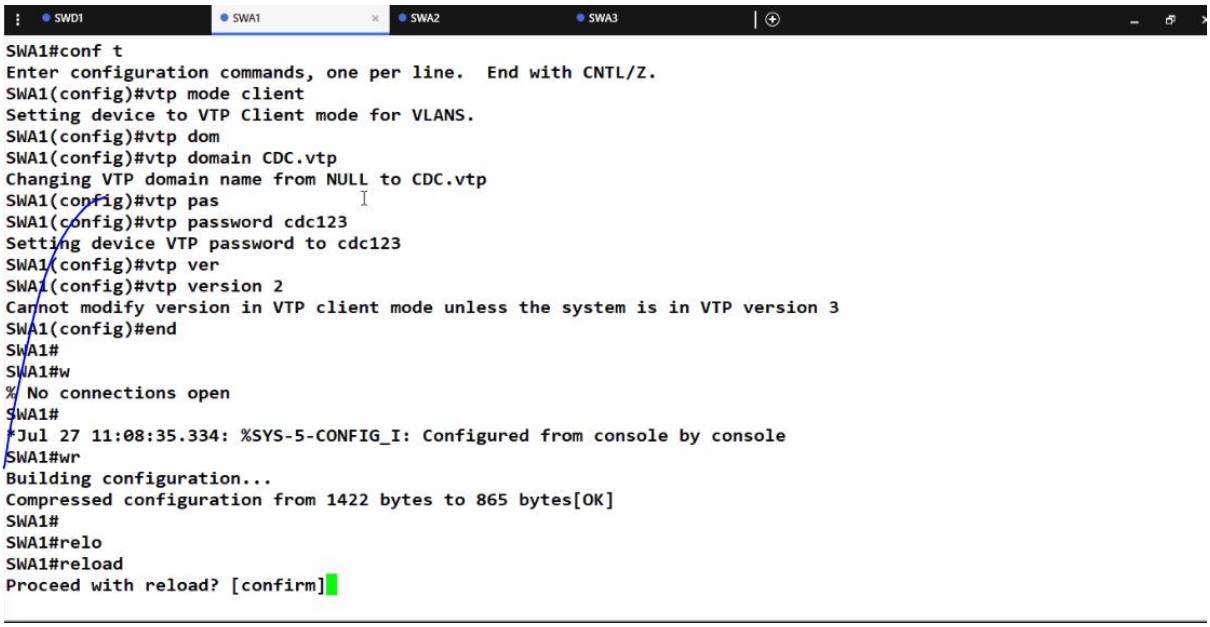

Figure 3.10: configuration VTP de SWA1.

SWA2 :

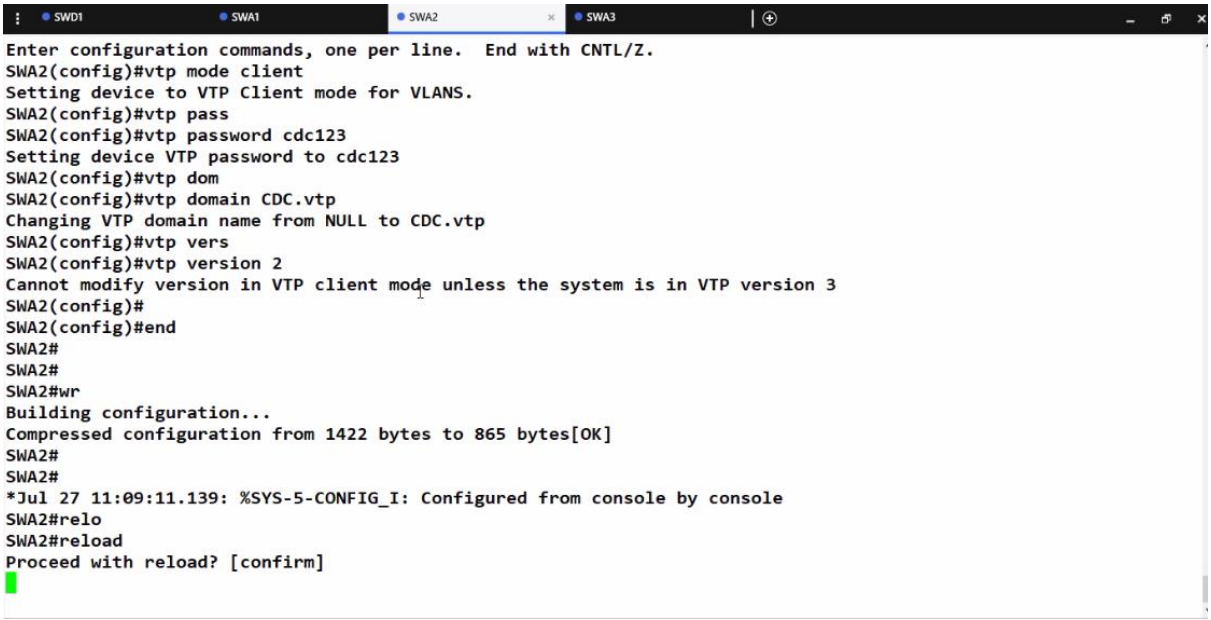

Figure 3.11 : la configuration VTP de SWA2.

SWA3

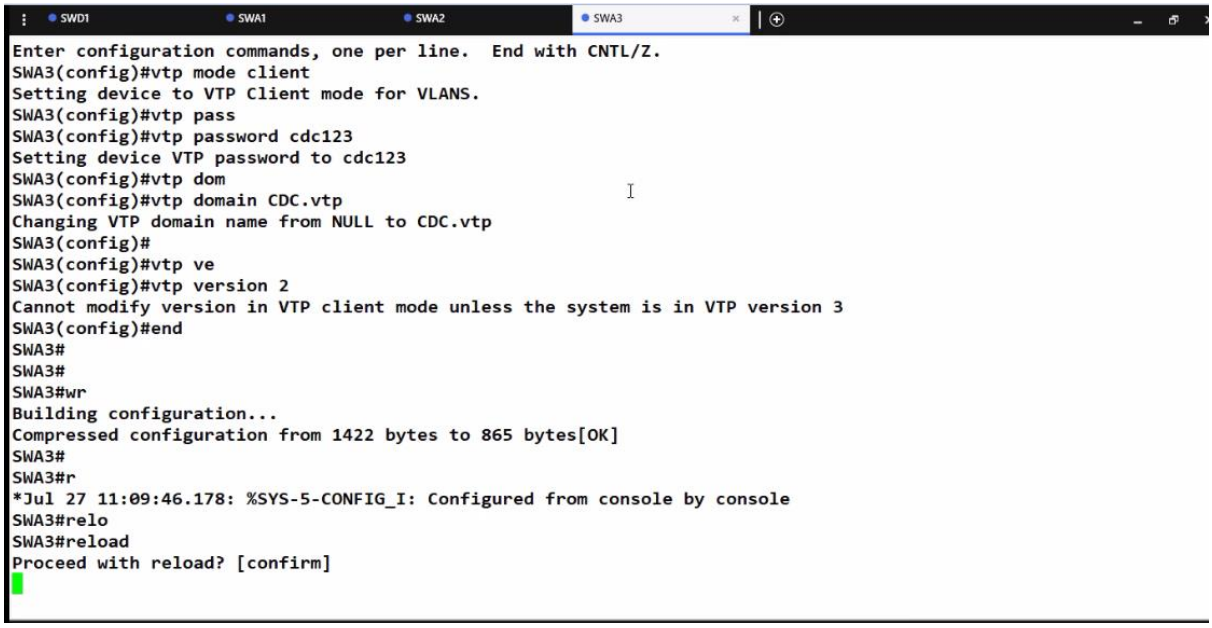

Figure 3.12: à configuration VTP de SWA3.

Etape 4 : créer les VLANs :

La définition VLANS : Vlan veut dire Virtual local area network … en d'autres mots : réseau local virtuel. Le concept de VLAN est utilisé afin d'avoir plusieurs réseaux indépendants sur le même équipement réseau physique. Cela évite d'avoir des équipements réseaux différents dans une entreprise lorsque nous voulons que deux départements ou fonctionnalités ne soient pas sur le même réseau ou vu l'un de l'autre.

Switch distributeur (SWD1) :

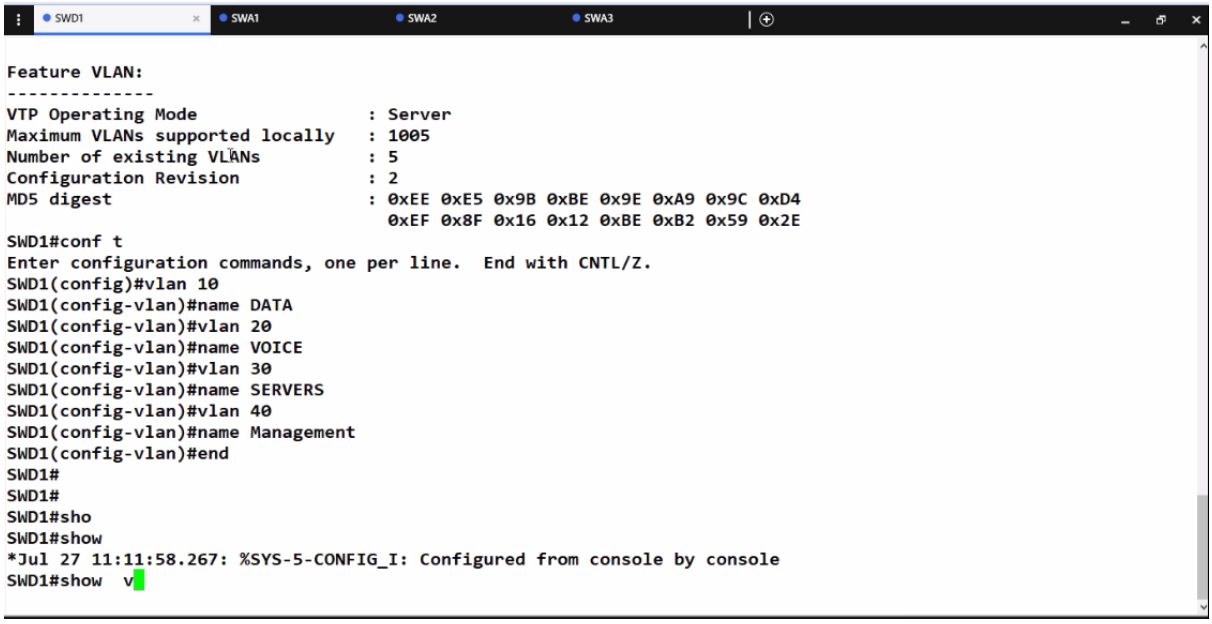

Figure 3.13: la création des VLANs.

Etape 5 : affectation les ports au VLAN en mode Access :

Une fois les VLAN créés, vous devez affecter les ports au VLAN approprié. Vous pouvez configurer des ports à l'aide de la commande switchport et spécifier si le port doit être en mode accès ou trunk.

SWA1 :

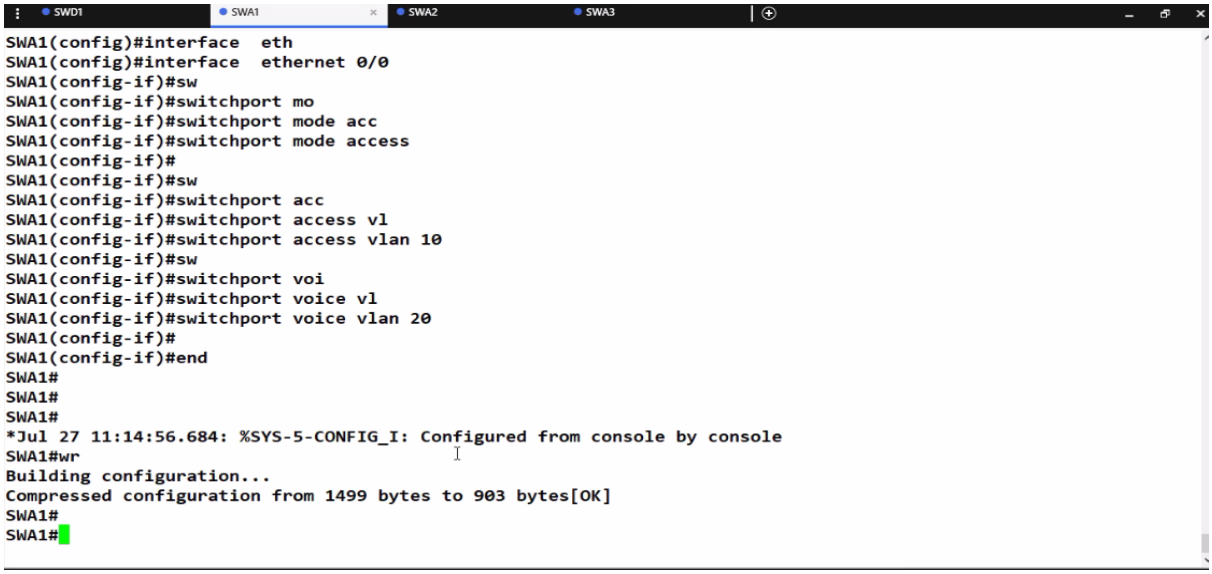

Figure 3.14: affectation les ports au VLAN pour SWA1.

SWA2 :

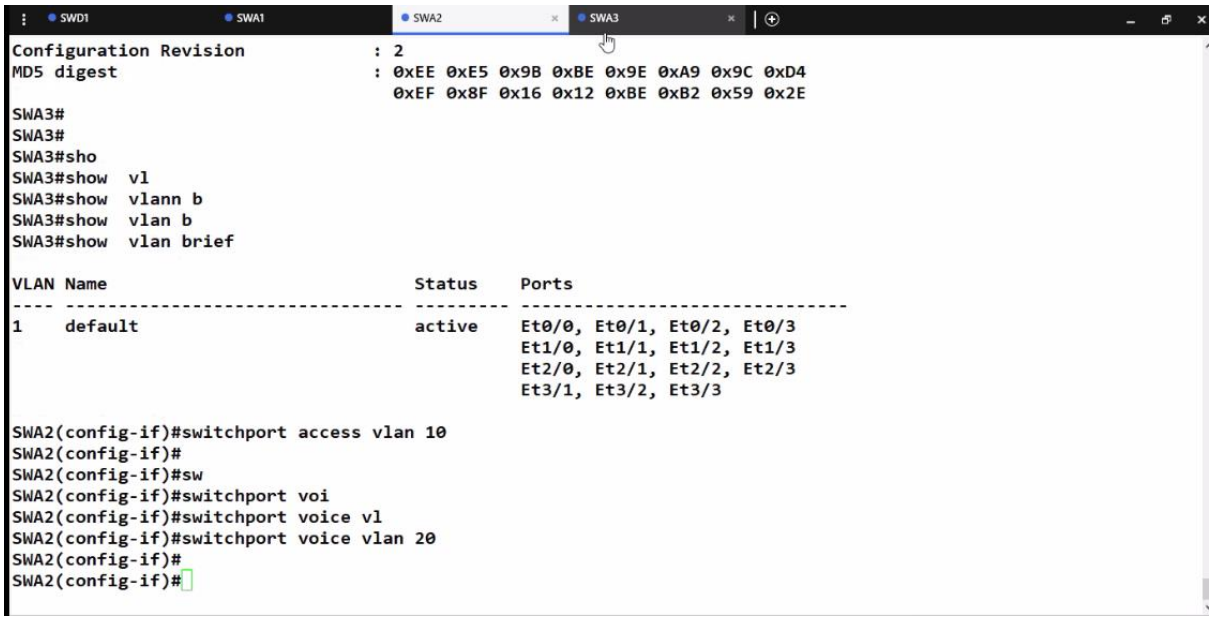

Figure 3.15: affectation les ports au VLAN pour SWA2.

SWA3 :

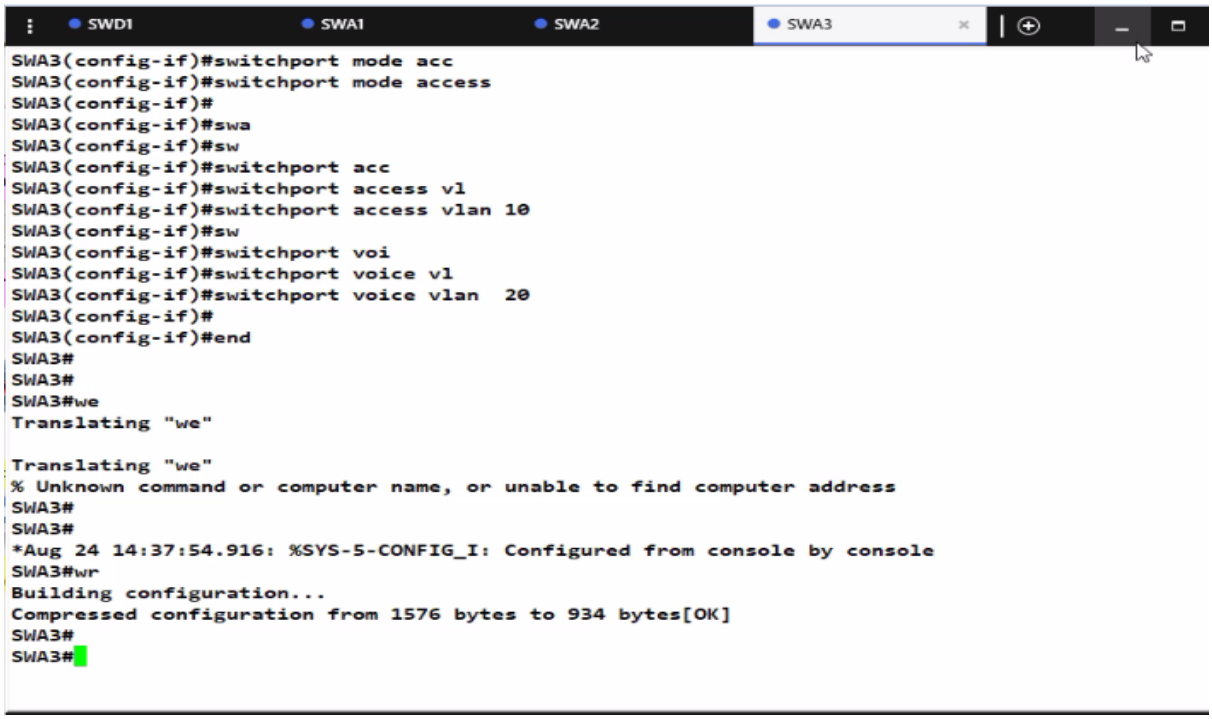

Figure 3.16:affectation les ports au VLAN pour SWA3.

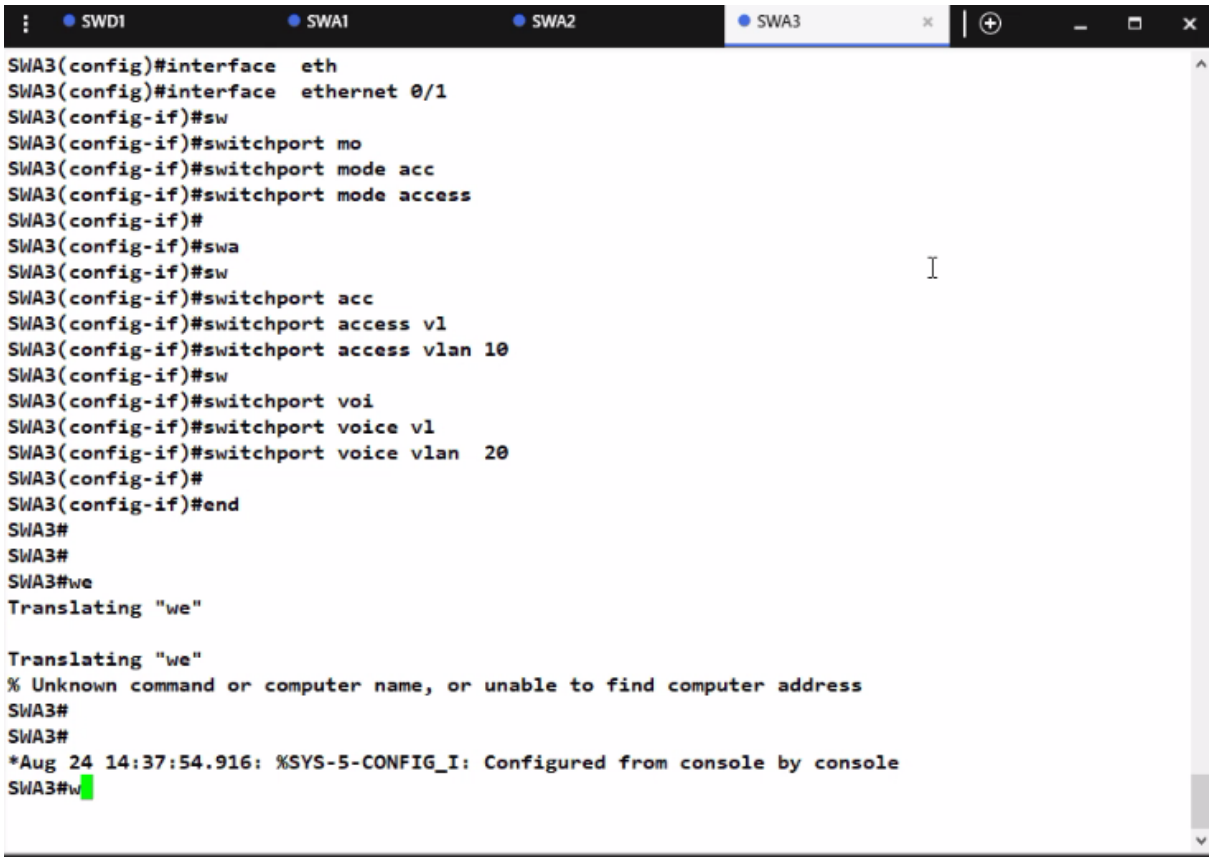

Figure 3.17:affectation les ports au VLAN pour interface e0/1 SWA3.

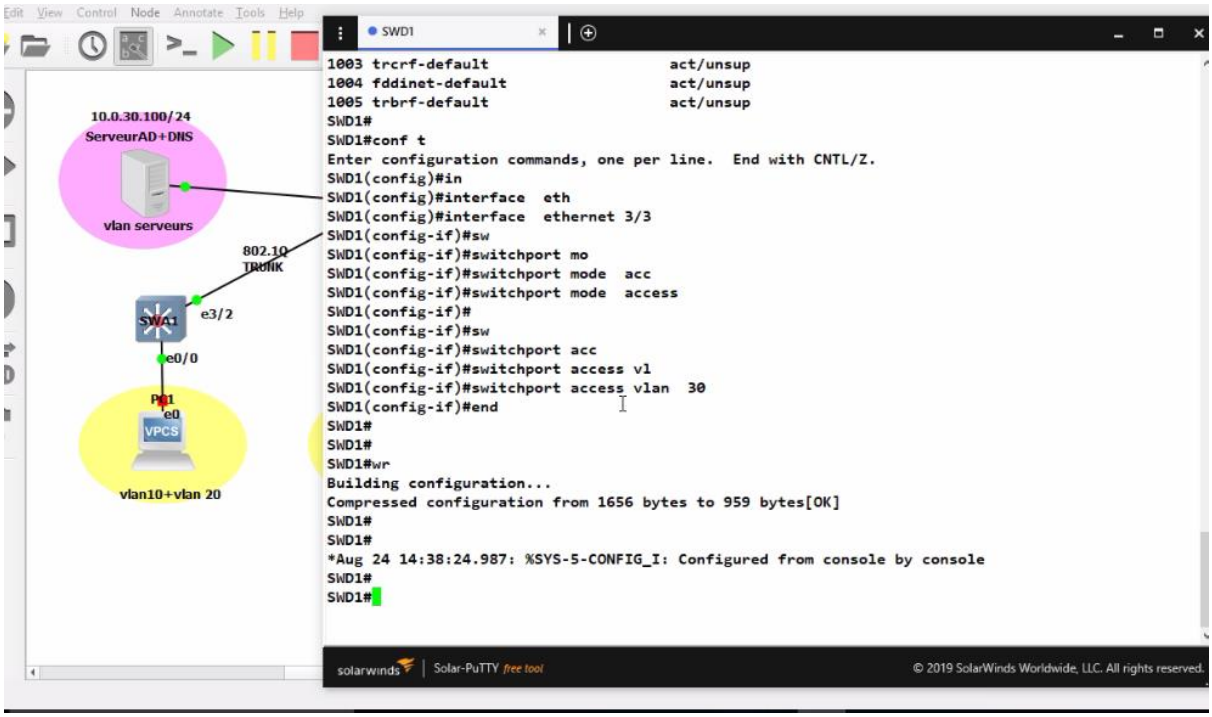

Figure 3.18: affectation les ports au VLAN pour interface e3/3 SWD1.

Etape 6 : la configuration le routage inter-VLAN :

Le routage inter-VLAN : est un processus qui permet de transférer du trafic réseau d'un VLAN à un autre à l'aide d'un périphérique de couche 3 comme un routeur. Il réaliser la communication entre tous les VLANs qui existent notre réseau à travers un routeur.

Les étapes des configurations comme suite :

- Création des sous interfaces pour chaque vlan.
  - Configuration de l'encapsulions 802.1Q pour chaque interface.
  - Configuration des adresses « passerelle par défaut pour chaque vlan »

On doit activer d'abord l'interface e0/0

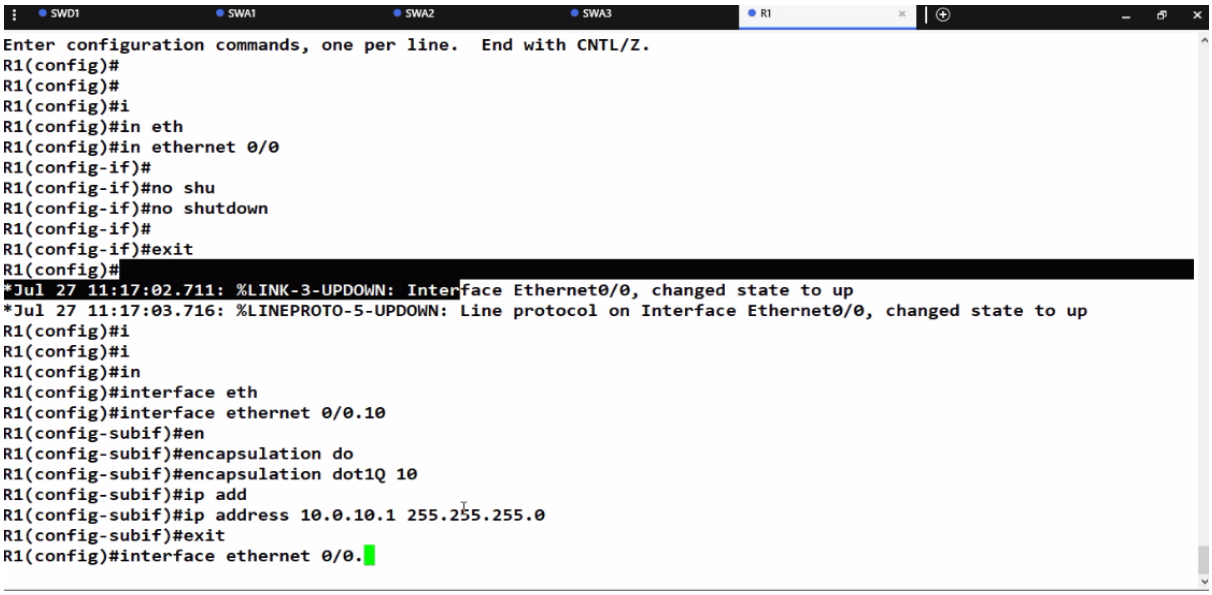

Figure 3.19: activation du l'interface e0/0 de routeur.

R1

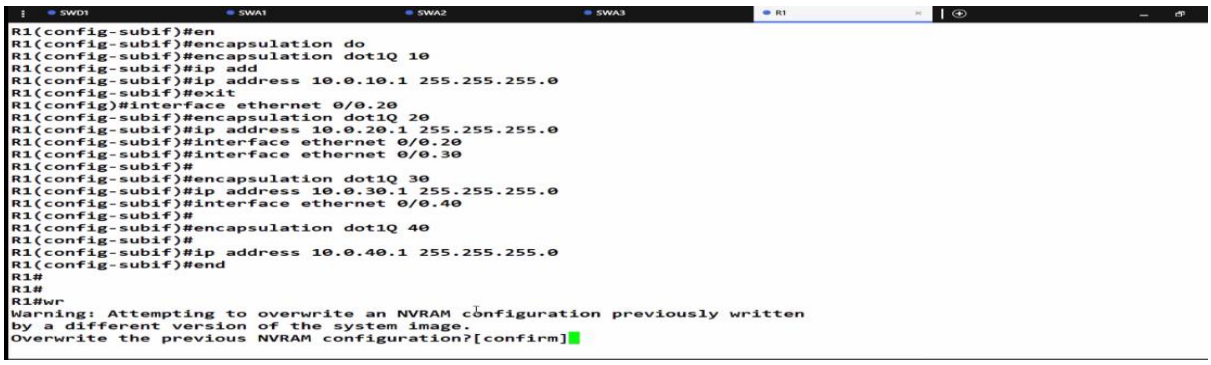

Figure 3.20: la configuration de routage inter-VLAN R1.

Etape 7 : router vers internet :

Nous devons configurer la route par défaut pour router les VLANs vers l'internet en utilisant la commande IP route 0.0.0.0 0.0.0.0 et indique l'interface de sortie vers internet.

R1 :

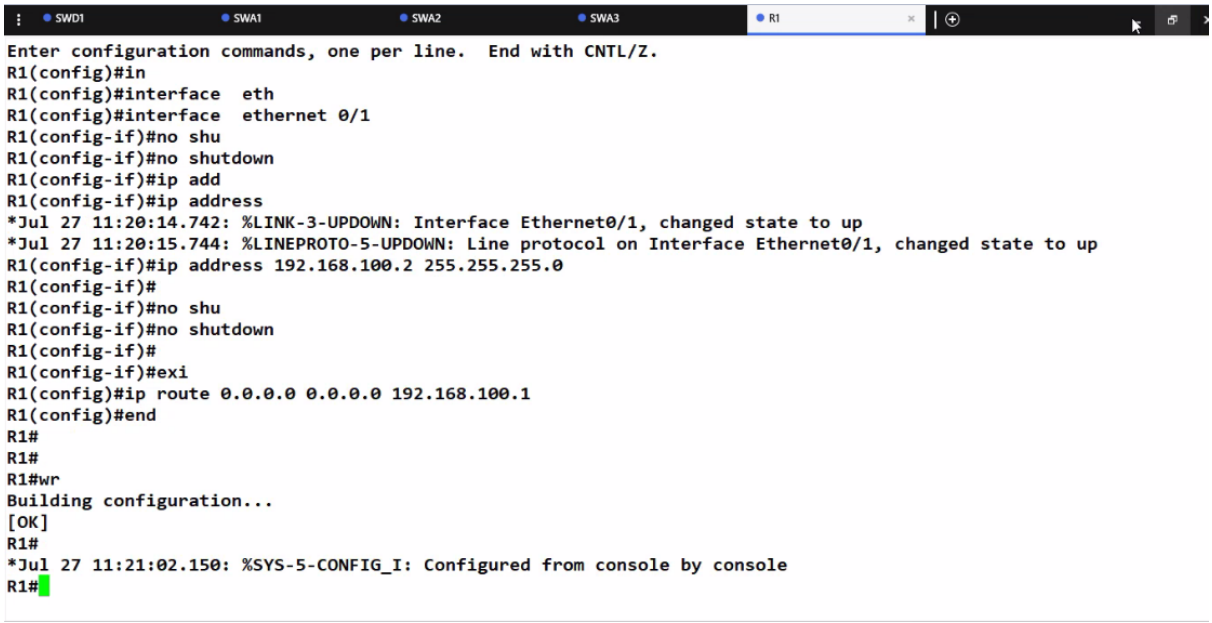

Figure 3.21: routage des VLANs vers internet.

Etape 8 : la configuration de FW-Bejaia (open source) :

1. Affectation l'adresse pour firewall :

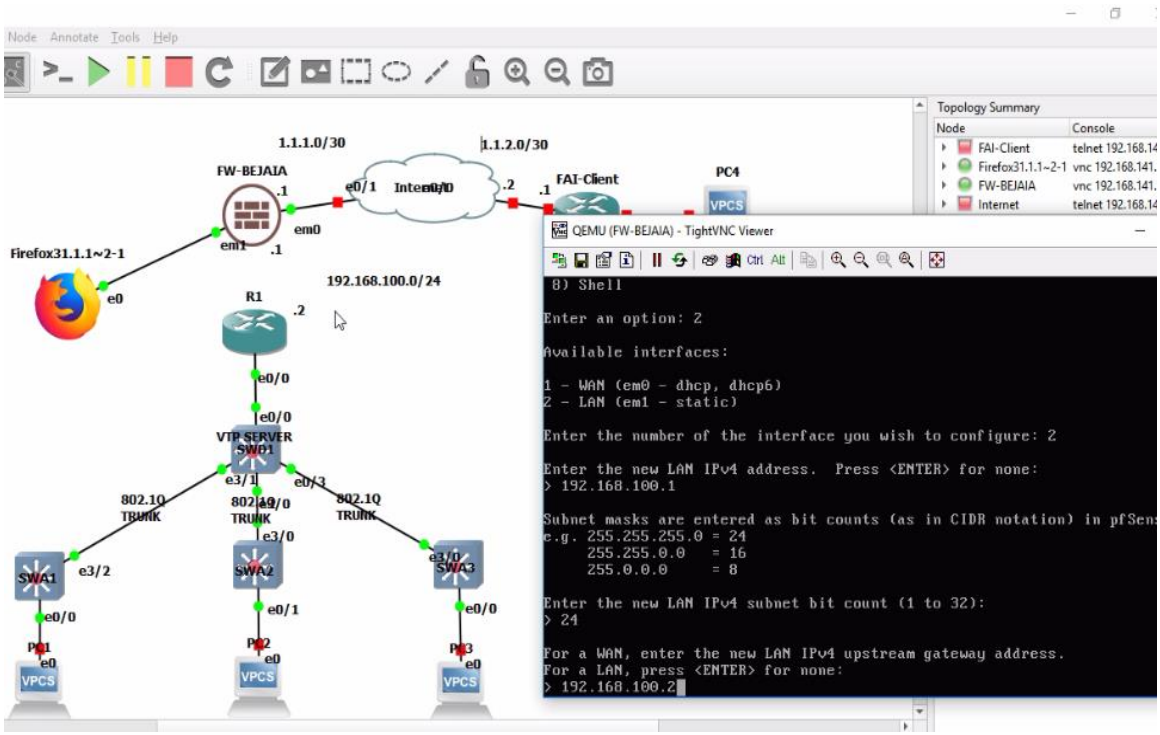

Figure 3.22: l'adresse firewall.

2. Affectation adresse IP public pour firewall :

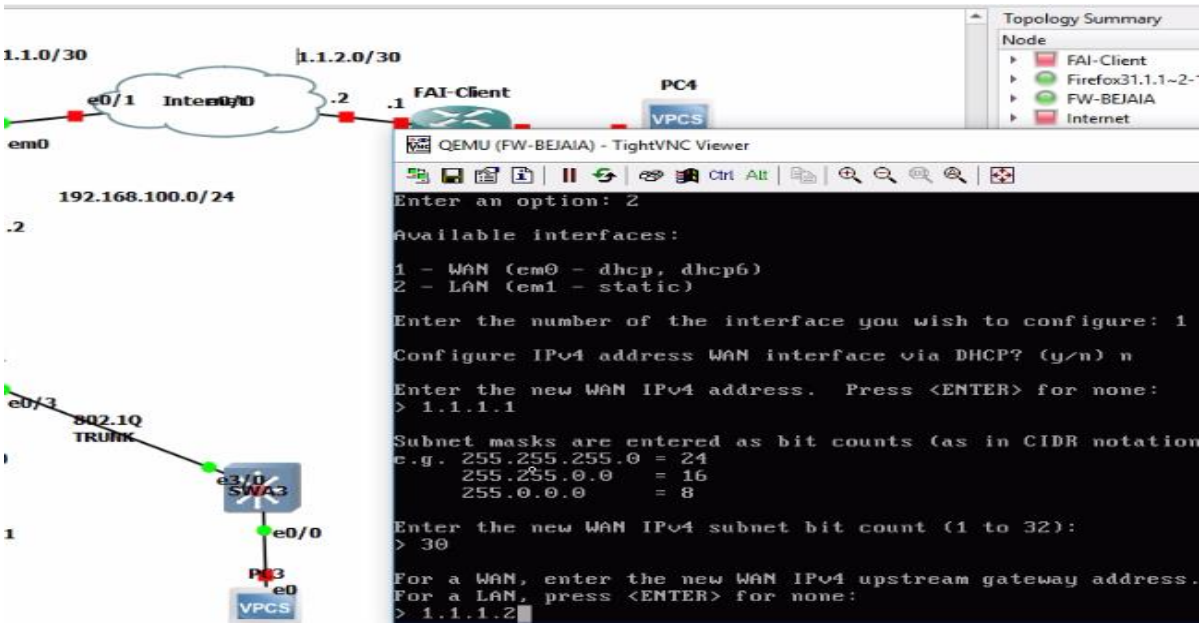

Figure 3.23 : l'adresse publique firewall.

3. Affectation adresse IP pour le navigateur web (Firefox) : pour accéder en http notre firewall.

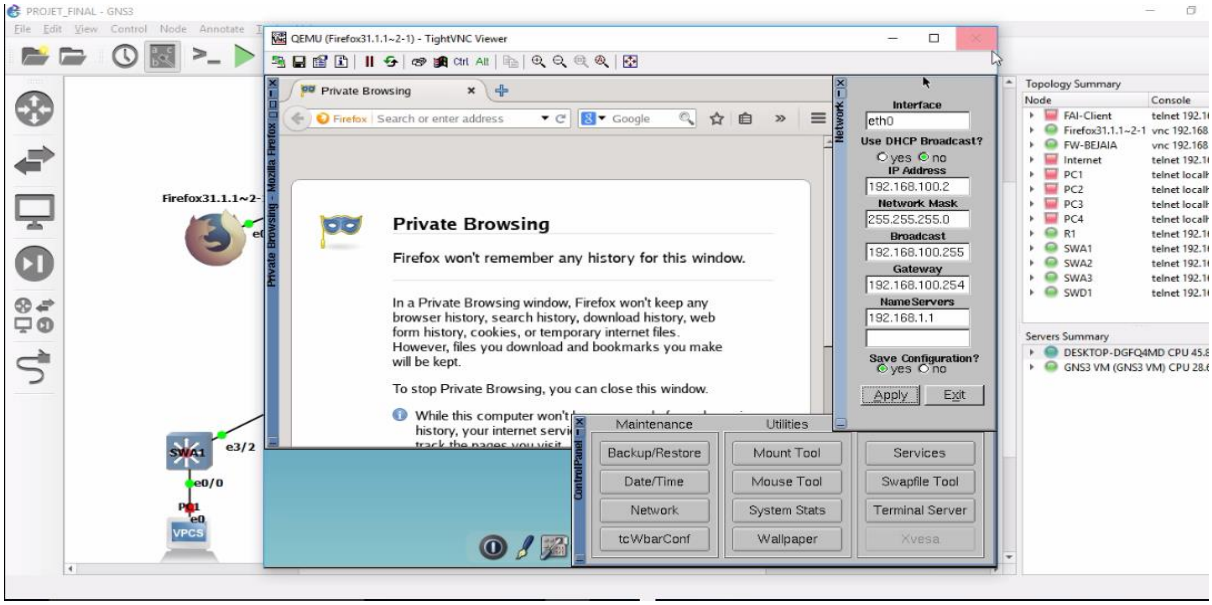

Figure 3. 24: l'adresse IP pour Firefox.

4. Accéder au pfsense à partir le navigateur web : on taper adresse de pfsense.

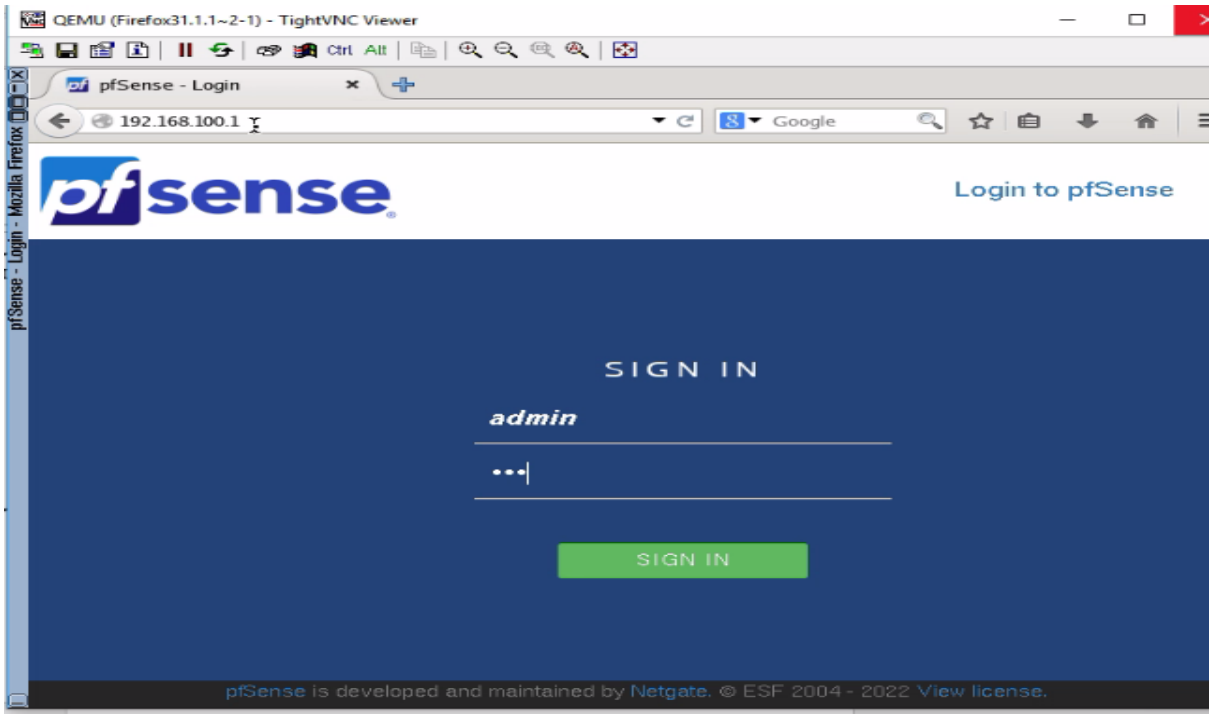

Figure 3.25: page d'accueil de pfsense.

4 : Les étapes à suivre pour l'autorisation de trafic : dans le LAN.

Autoriser any (tout trafic) : Dans cette étape on va mentionnée les vlans sur la partie firewall car il les connait pas, ensuit on va autoriser le IPV4 puis en change la source au lieu LAN net on mit any.

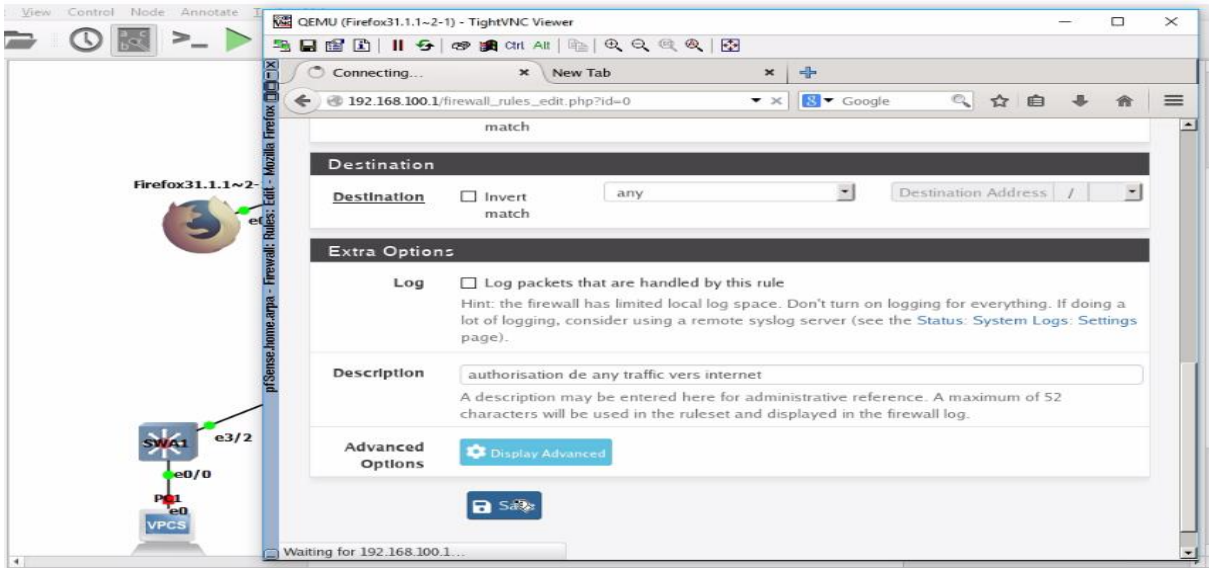

Figure 3.26: autorisation tout trafic.

5 : Router vers les VLANS

a) La route par défaut il faut être à WAN

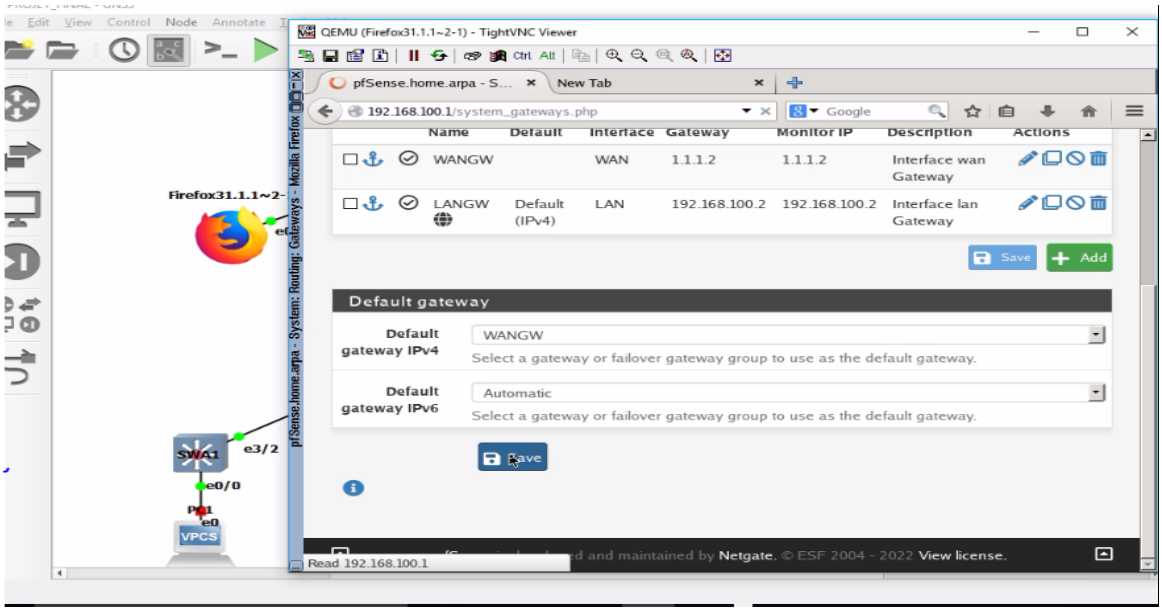

Figure 3.27: default Gateway ipv4 en WAN.

b) La création d'une alias se vlan pour regrouper les VLANs :

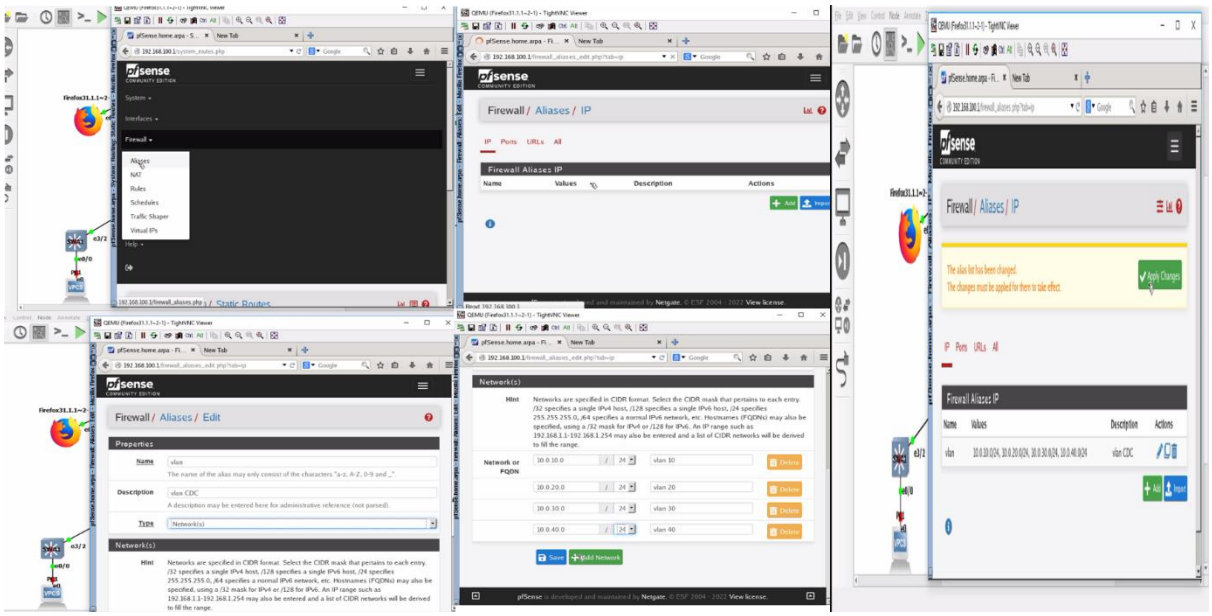

Figure 3.28 : regrouper les VLANs dans alias vlan

c) Création d'une route statique vers alias vlan :

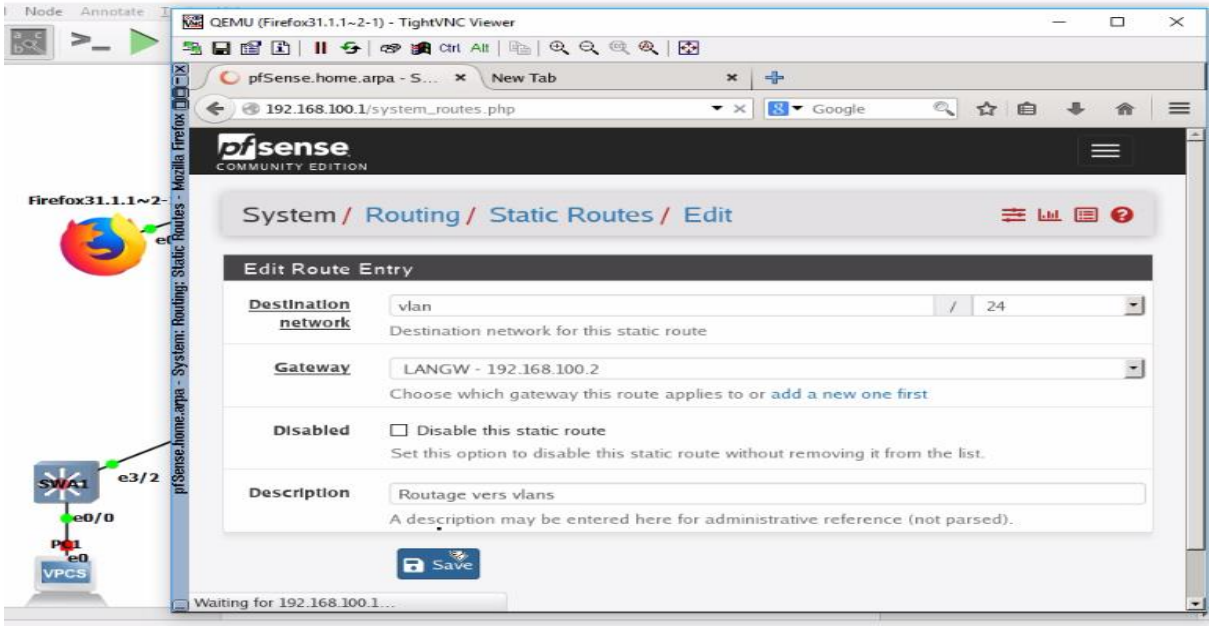

Figure 3.29:router vers les VLANs.

6 .1 : Tester Ping de R1 vers firewall :

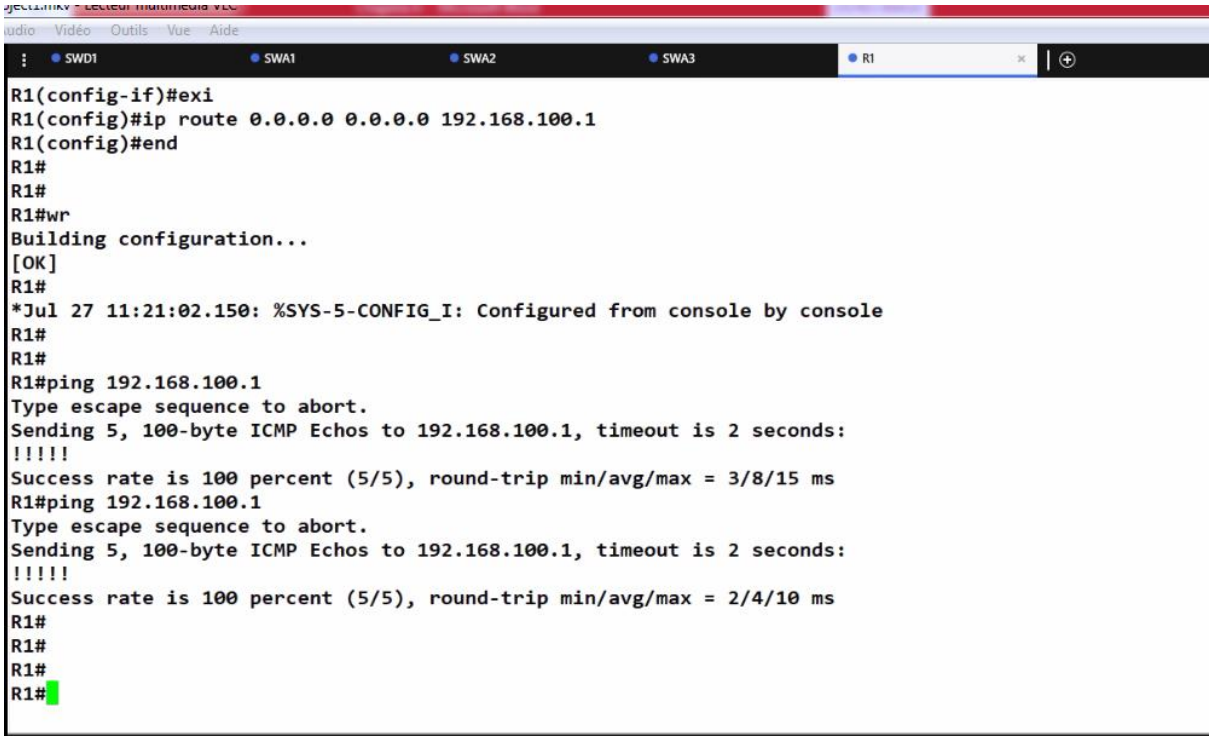

Figure 3.30: vérification la connectivité de R1 vers firewall

6.2 : Tester Ping de pc2 vers firewall :

```
cs.sf.net.
For more infor
mation, please
 visit wiki.fr
eecode.com.cn.

Press '?' to g
et help.

Executing the
startup file


PC2>
PC2>
PC2> ip 10.0.10.10/24 10.0.10.1
Checking for duplicate address...
PC1 : 10.0.10.10 255.255.255.0 gateway 10.0.10.1

PC2> ping 192.168.100.1
84 bytes from 192.168.100.1 icmp_seq=1 ttl=63 time=4.483 ms
84 bytes from 192.168.100.1 icmp_seq=2 ttl=63 time=3.192 ms
84 bytes from 192.168.100.1 icmp_seq=3 ttl=63 time=6.405 ms
84 bytes from 192.168.100.1 icmp_seq=4 ttl=63 time=5.211 ms
84 bytes from 192.168.100.1 icmp_seq=5 ttl=63 time=3.597 ms
```

Figure 3.31: teste la connectivité de pc2 vers firewall.

Etape 9 : la configuration d'internet :

1 : Interface vers firewall :

SWD1 SWA1 SWA2 SWA3 R1 PC2 Internet

```
Internet(config-if)#INterface  ethernet 0/1
Internet(config-if)#
*Jul 27 14:50:12.303: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Jul 27 14:50:13.308: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
Internet(config-if)#
Internet(config-if)#no shu
Internet(config-if)#no shutdown
Internet(config-if)#
Internet(config-if)#
Internet(config-if)#
Internet(config-if)#
*Jul 27 14:50:17.676: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
*Jul 27 14:50:18.679: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to up
Internet(config-if)#ip add
Internet(config-if)#ip address 1.1.1.2 255.255.255.252
Internet(config-if)#
Internet(config-if)#
Internet(config-if)#no shu
Internet(config-if)#no shutdown
Internet(config-if)#
Internet(config-if)#des
Internet(config-if)#description // connexion vers firewall//
Internet(config-if)#
Internet(config-if)#exit
Internet(config)#
Internet(config)#
```

Figure 3.32: configuration l'interface Ethernet 0/1.

2 : interface vers FAI-Client :

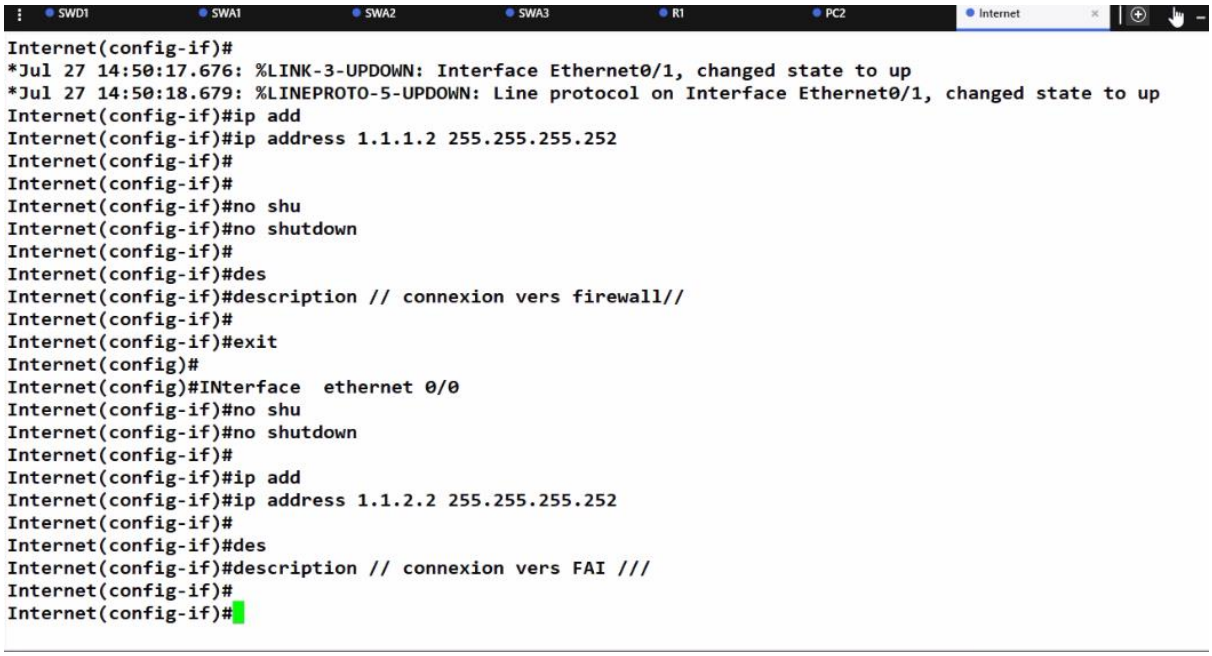

Figure 3.33: configuration l'interface Ethernet 0/0.

Etape 10 : la configuration de FAI-Client :

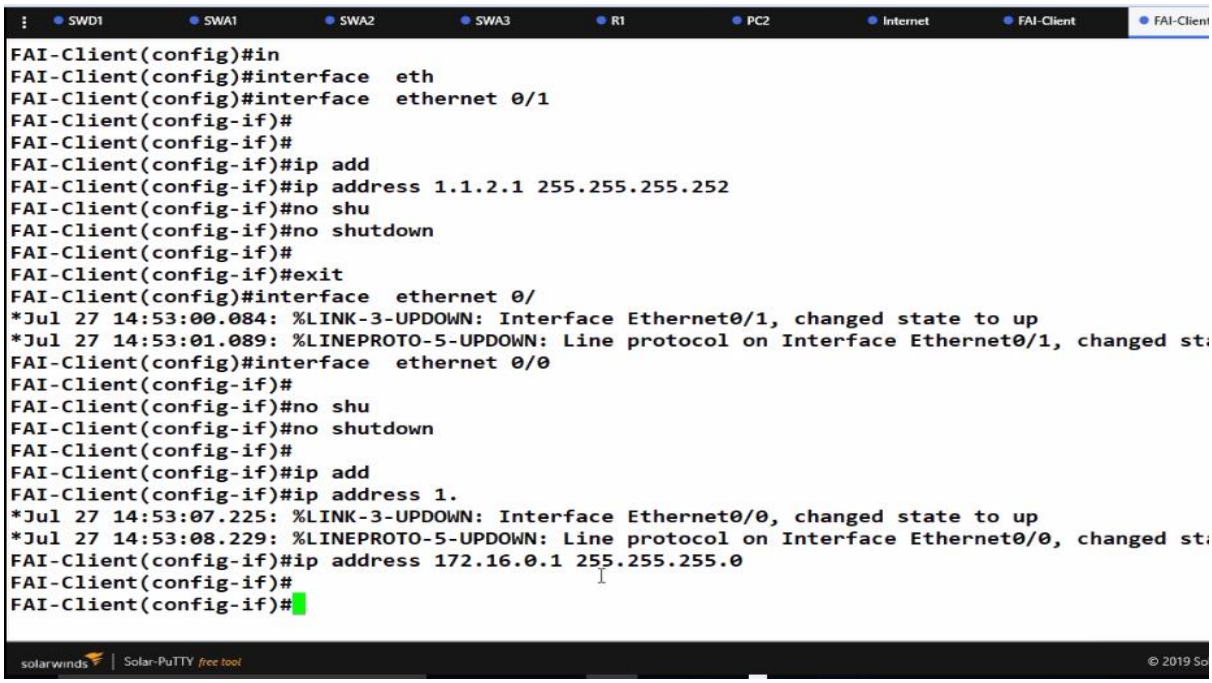

Figure 3.34: configuration FAI-Client

Création d'une route de FAI-Client vers l'internet :

```
FAI-Client#wr
*Jul 27 14:53:21.850: %SYS-5-CONFIG_I: Configured from console by console
FAI-Client#wr
Warning: Attempting to overwrite an NVRAM configuration previously written
by a different version of the system image.
Overwrite the previous NVRAM configuration?[confirm]
Building configuration...
[OK]
FAI-Client#
FAI-Client#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
FAI-Client(config)#
FAI-Client(config)#ip route 0.0.0.0 0.0.0.0 1.1.2.2
FAI-Client(config)#
FAI-Client(config)#
FAI-Client(config)#
FAI-Client(config)#end
FAI-Client#
FAI-Client#
FAI-Client#wr
Building configuration...

*Jul 27 14:53:45.585: %SYS-5-CONFIG_I: Configured from console by console[OK]
FAI-Client#
FAI-Client#
```

Figure 3.35: Création d'une route de FAI-Client vers l'internet.

Etape 13: la configuration de NAT :

```
FAI-Client
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
 transport input none
!

FAI-Client(config)#acc
FAI-Client(config)#access-list 1 p
FAI-Client(config)#access-list 1 permit 172.16.0.0 0.0.0.255
FAI-Client(config)#ip nat
FAI-Client(config)#ip nat so
FAI-Client(config)#ip nat source i
FAI-Client(config)#ip nat i
FAI-Client(config)#ip nat inside sou
FAI-Client(config)#ip nat inside source li
FAI-Client(config)#ip nat inside source list 1 i
FAI-Client(config)#ip nat inside source list 1 interface eth
FAI-Client(config)#ip nat inside source list 1 interface ethernet 0/1 o
FAI-Client(config)#$de source list 1 interface ethernet 0/1 overload
FAI-Client(config)#
FAI-Client(config)#
FAI-Client(config)#end
FAI-Client#
FAI-Client#
FAI-Client#w
```

Figure 3.36: la configuration de NAT.

Configuration le routeur1 en DHCP relais

- Configuration de l'agent relais pour chaque sous interface afin de permettre les diffusions des messages DHCP en indiquant à chaque sous interface l'adresse IP du serveur avec la commande IP helper-address 10.0.30.100.

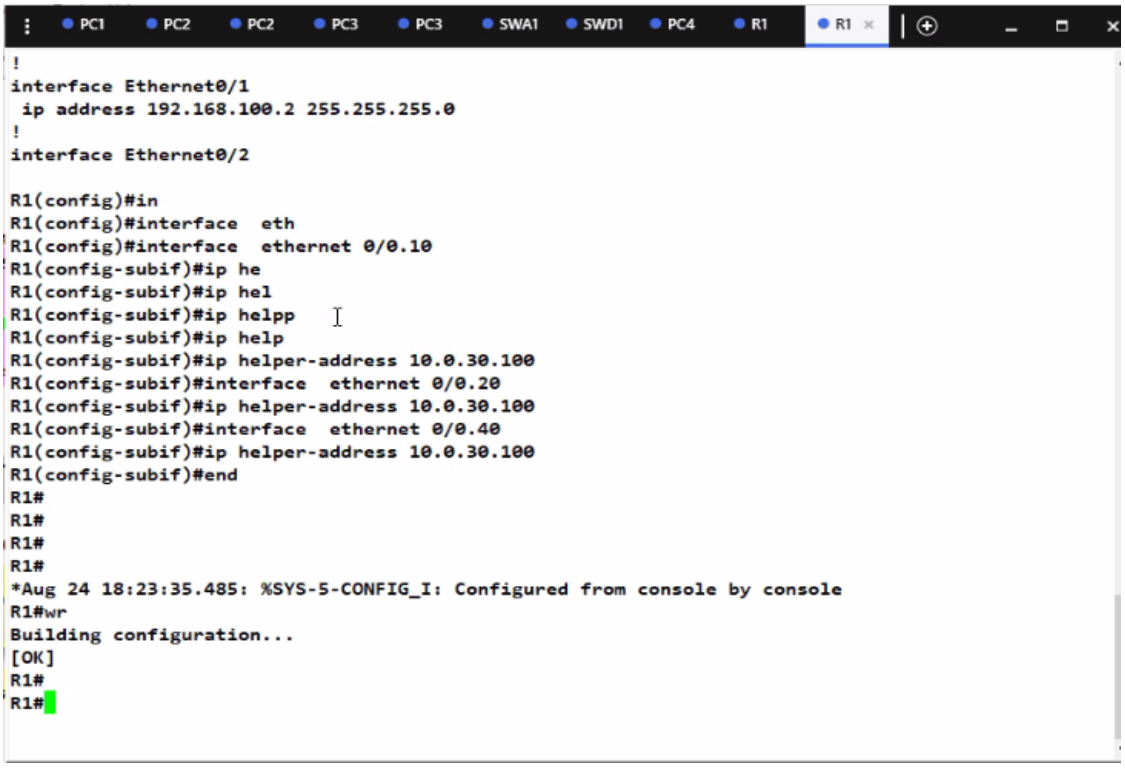

Figure 3.37 : La configuration le routeur R1 en DHCP relais.

3.6 Tableau d'adressage général :

Device	Interface	Adresse ip	description	passrelle
R1	E0/0	sous interface	Connecter au SWD1	//
	E0/1	192.168.100.2 / 24	Connecter au pfsense	//

Switch distributeur SWD1	E0/0	En mode trunk	Connecter au R1	//
	E3/3	VLAN serveur	Connecter au serveur AD+DNS	//
	E3/1	En mode trunk	Connecter au SWA1	//
	E3/0	En mode trunk	Connecter au SWA2	//
	E0/3	En mode trunk	Connecter au SWA3	//
Serveur AD+DNS	E0	10.0.30.100/24	Connecter au SWD1	//
Switch accès SWA1	E3/2	En mode trunk	Connecter au SWD1	//
	E0/0	En mode accès	Connecter au VLAN10+VLAN20	//
Switch accès SWA2	E3/0	En mode trunk	Connecter au SWD1	//
	E0/0	En mode accès	Connecter au VLAN10+VLAN20	//
Switch accès SWA3	E3/0	En mode trunk	Connecter au SWD1	//

	E0/0	En mode accès	Connecter au VLAN10+VLAN20	//
	E0/1	En mode accès	Connecter au VLAN10+VLAN20	//
Pfsense	Em0	1.1.1.1/30	Connecter à l'internet	1.1.1.2
	Em1	192.168.100.1/24	Connecter au R1	192.168.100.2
	Em2	192.168.16.1/24	Connecter au SW_DMZ	//
FAI-Client	E0/0	172.16.0.1/24	Connecter au client-internet	//
	E0/1	1.1.2.1/30	Connecter à internet	//
Client – internet	E0	172.16.0.10/24	Connecter au FAI-Client	172.16.0.1
Internet	E0/1	1.1.1.2/30	Connecter au FAI-Client	//
	E0/0	1.1.2.2/30	Connecter au pfsens	//
PC1	E0	10.0.10.11/24	Connecter au	10.0.10.1

			VLAN10+VLAN20	
PC2	E0	DHCP	Connecter au VLAN10+VLAN20	//
PC3	E0	DHCP	Connecter au VLAN10+VLAN20	//
Client1	E0	DHCP	Connecter au VLAN10+VLAN20	//

Tableau 3. 1: tableau d'adressage général.

3.7 Tableau d'adressage des VLANs :

Nom VLAN	IP VLAN	Réseau /préfix
VLAN Data	10	10.0.10.0 /24
VLAN VOICE	20	10.0.20.0 /24
VLAN SERVERS	30	10.0.30.0/24
VLAN Mangement	40	10.0.40.0/24

Tableau 3.2 : tableau d'adressage des VLANs.

3.8 Tableau d’adressage de routage inter-vlan

Equipements	Encapsulation 802.1q	Interface	Adresse IP /préfixe
R1	10	0/0.10	10.0.10.1/24
	20	0/0.20	10.0.20.1/24
	30	0/0.30	10.0.30.1/24
	40	0/0.40	10.0.40.1/24

Tableau 3.3 : tableau d’adressage inter-vlan.

3.9 Phase 1 : installation

3.9.1 Installation Debian 11 sur VMware:

- Cliquez sur le bouton "Créer une nouvelle machine virtuelle".
- Depuis le menu Fichier / New Virtual machine.

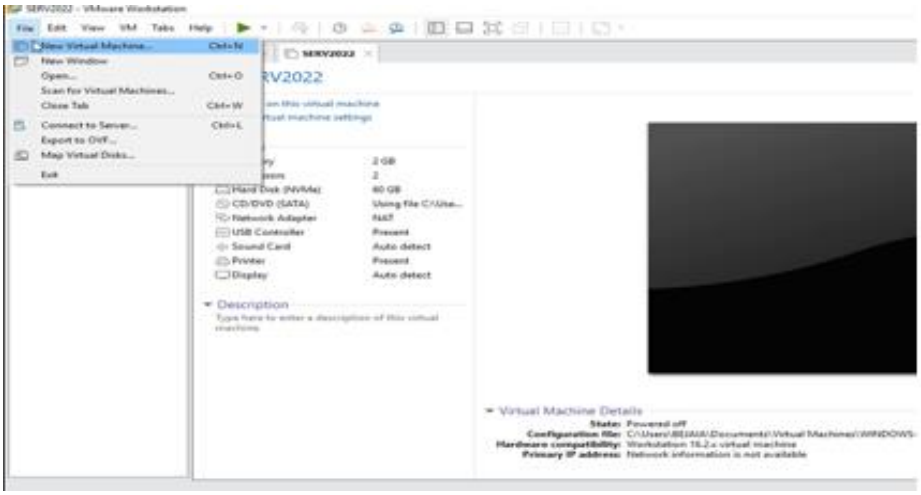

Figure 3.38: interface VMware Workstation.

- Sélectionner ‘ typical (recommended)’.

- Cliquer ‘next’.
- Vous cliquez sur «browse» et sélectionnez votre fichier ISO puis cliquez sue «next».
- nous attribuons le nom de la machine et son emplacement soit vous laissez le nom de base ou alors vous pouvez le changer et ensuite vous pouvez choisir ou enregistré votre machine virtuelle, cela dépend de vous. Puis cliquez sur «Next».
- Nous attribuons la taille et le type de stockage Maintenant vous devez choisir la capacité du disque de votre machine. Ensuite cliquez sur «split virtual disk as a single file» puis sur «next».
- 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»
- On le démarre en cliquant sur la ligne "Power on this virtual machine" et on sélectionne la méthode d'installation :
- nous sélectionnons la langue d'installation :
- Nous définissons notre emplacement :
- Nous sélectionnons la langue du clavier :
- Après cela, le réseau sera configuré puis nous attribuons le nom de l'équipement :

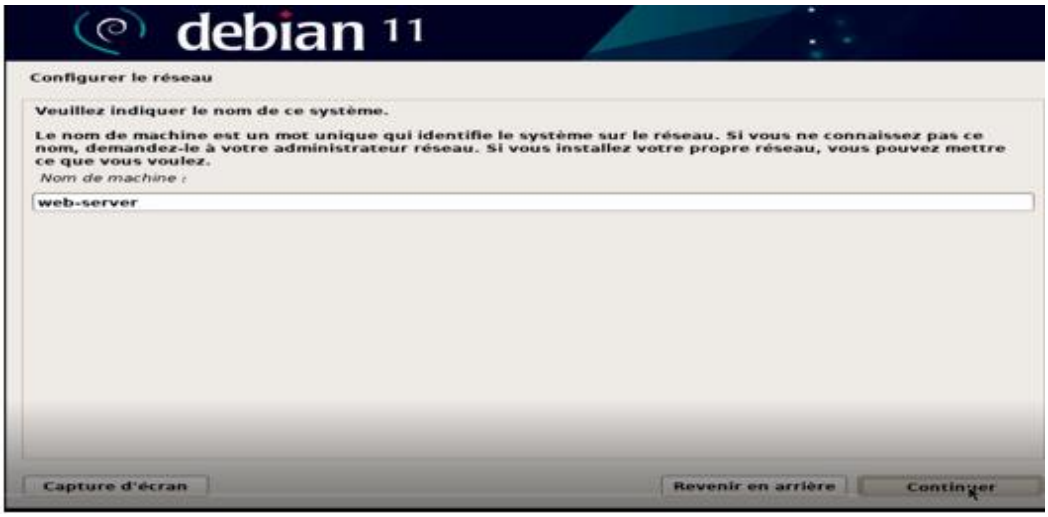

Figure 3.39: configuration le réseau 1

- Nous pouvons attribuer un domaine si nous l'avons :
- Nous procédons à l'attribution du mot de passe de l'utilisateur root :

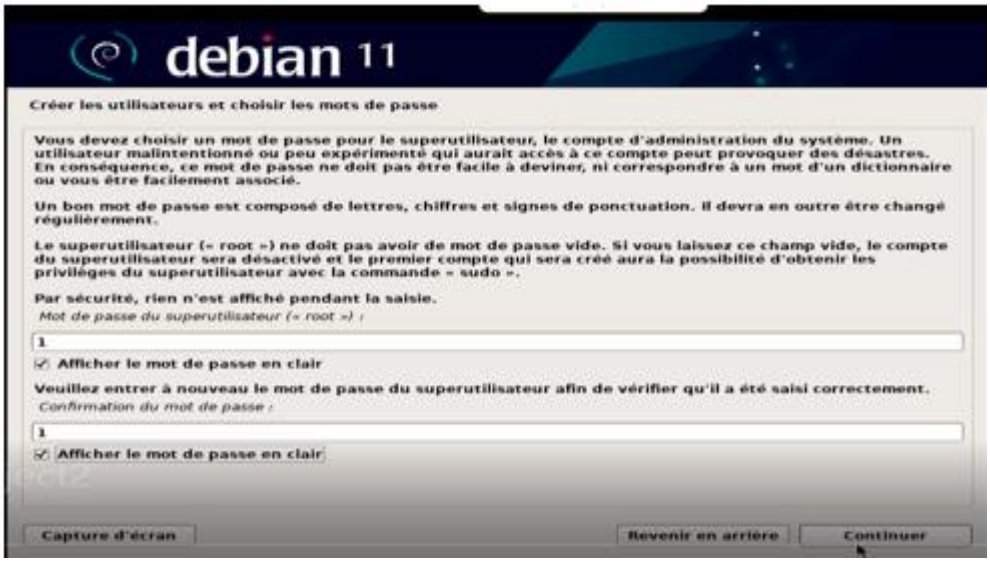

Figure 3.40: créer les utilisateurs et choisir les mots de passe

- Nous créons l'utilisateur administrateur :

Figure 3.41:le compte utilisateur.

- Nous cliquons sur Continuer et les composants Debian 11 seront chargés
- 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’.
- Nous sélectionnons le disque à utiliser :

- Nous définissons la manière dont les partitions sont gérées :
- Après cela, nous verrons ce qui suit :

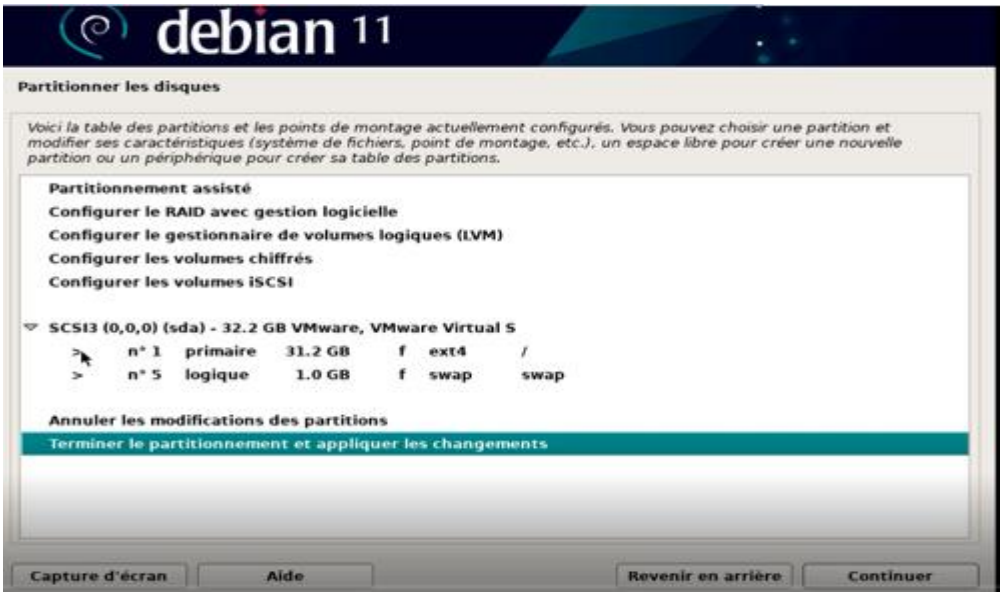

Figure 3. 42: partitionner les disques 4.

- Nous confirmons le processus de partition : cliquer sur ‘oui
- Nous cliquons sur Continuer pour continuer le processus :
- .Au cours de ce processus, nous verrons ce qui suit :

Figure 3. 43: configurer le gestionnaire de paquets.

- Là, nous définissons si nous utilisons ou non un miroir Debian 11, dans ce cas nous ne l'utiliserons pas et Debian continuera à ajuster les valeurs apt, nous verrons qu'il demande si nous voulons participer à l'enquête :
- Nous définissons maintenant ce qui doit être installé sur Debian 11
- Nous procédons au téléchargement et à l'installation de ce logiciel :
- Ensuite, nous devons configurer GRUB :
- Nous sélectionnons "Oui" et maintenant nous définissons où installer
- Ensuite, nous verrons ce qui suit :

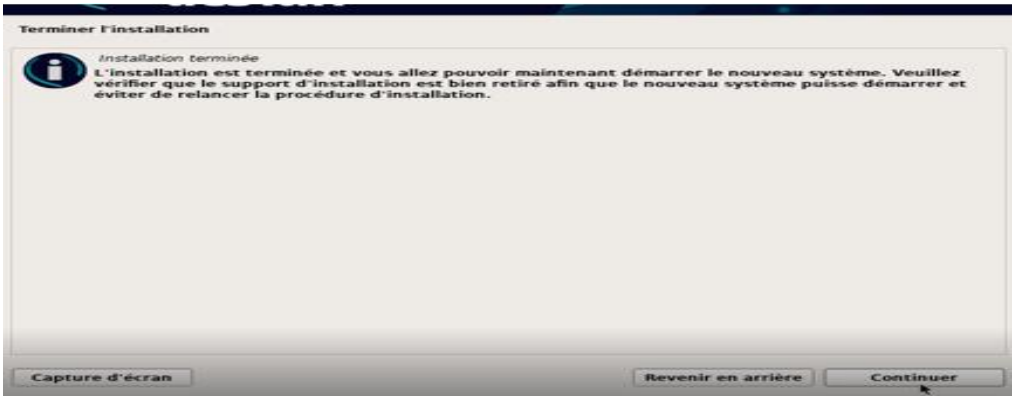

Figure 3.44: terminer l'installation.

- 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.

- Debian est installé :

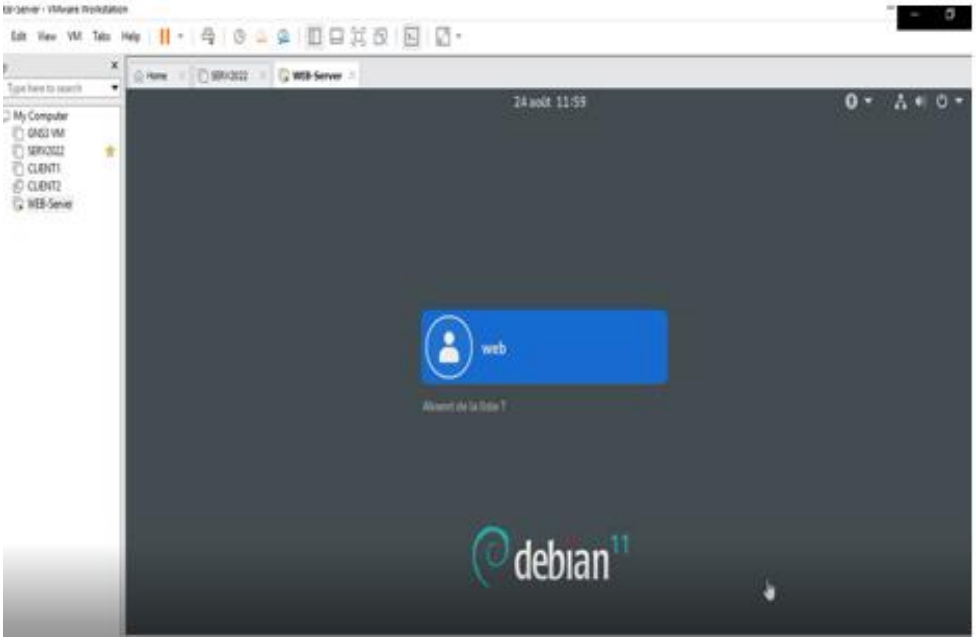

Figure 3.45: l'installation terminée.

3.9.2 Installation SSH sur web-server

Etape 1 : Mettre à jour le système.

Tout d'abord, nous devrons mettre à jour les référentiels de packages dans notre système d'exploitation. Pour cela, exécutez la commande suivante dans Terminal en tant que sudo.

Figure 3.46: Mettre à jour le système

Etape 2 : installation SSH : pour accéder à distance.

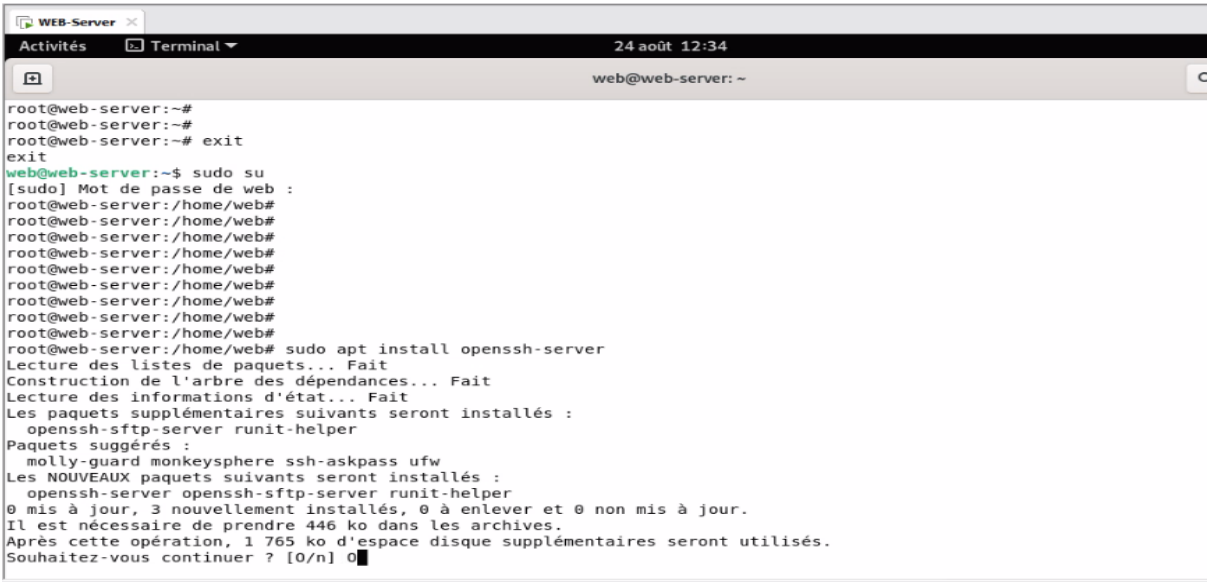

Figure 3.47: Installation SSH

Etape 3 : vérifier l'adresse serveur web : Pour cela, exécutez la commande suivante dans Terminal ifconfig, son adresse c'est 192.168.241.133.

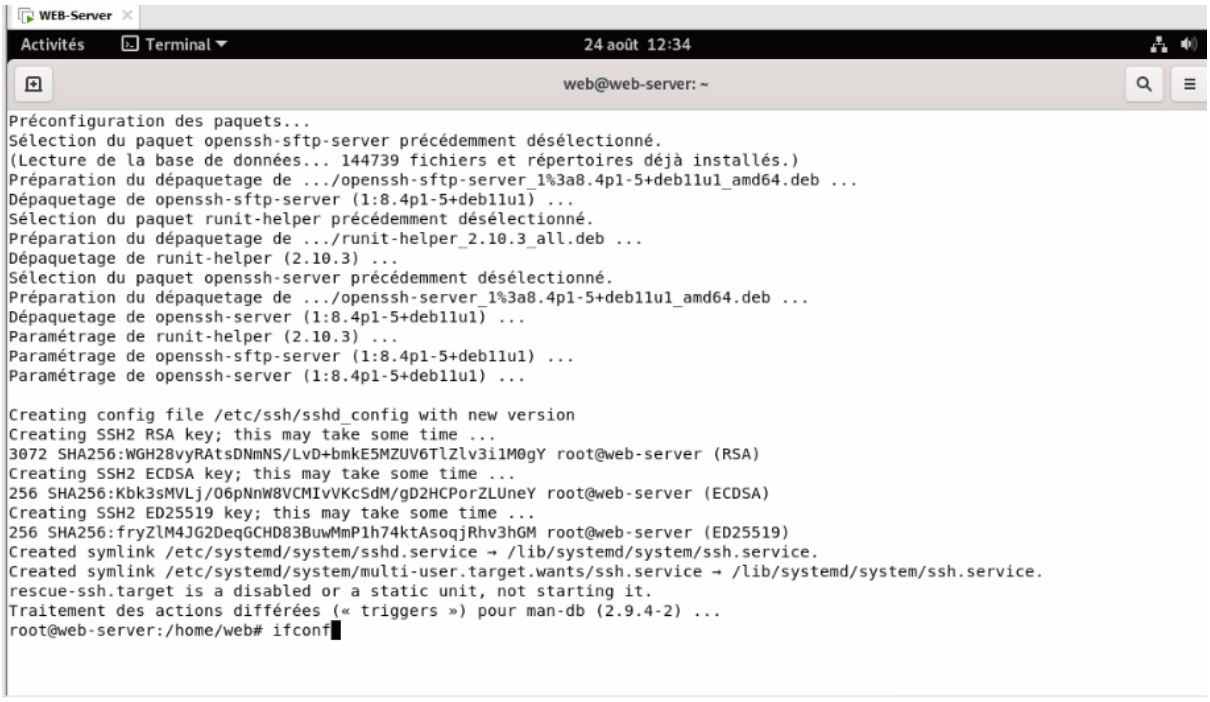

Figure 3.48: Adresse web-server.

Etape 4 : accéder au web-server à partir SSH : on taper adresse de web-server sur puTTY. Nom l'utilisateur c'est web, mot de passe 1, adresse 192.168.241.133.

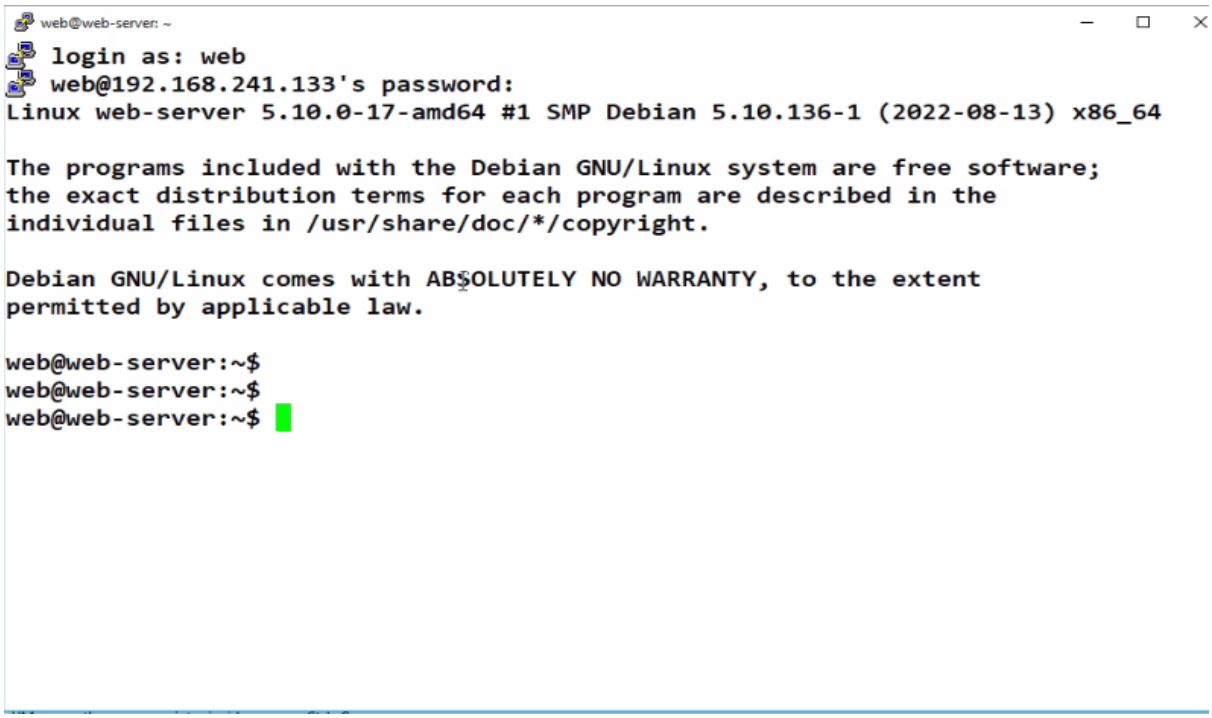

Figure 3.59:accéder au web-server à partir PUTTY.

Etape 5 : Accéder au fichier hosts : pour créer les noms de Domain.

On tape la commande nano/etc /host

Etape 6 : Création les noms Domain : les noms Domain notre site c'est univ-bejaia.net, www.univ-bejaia.net.

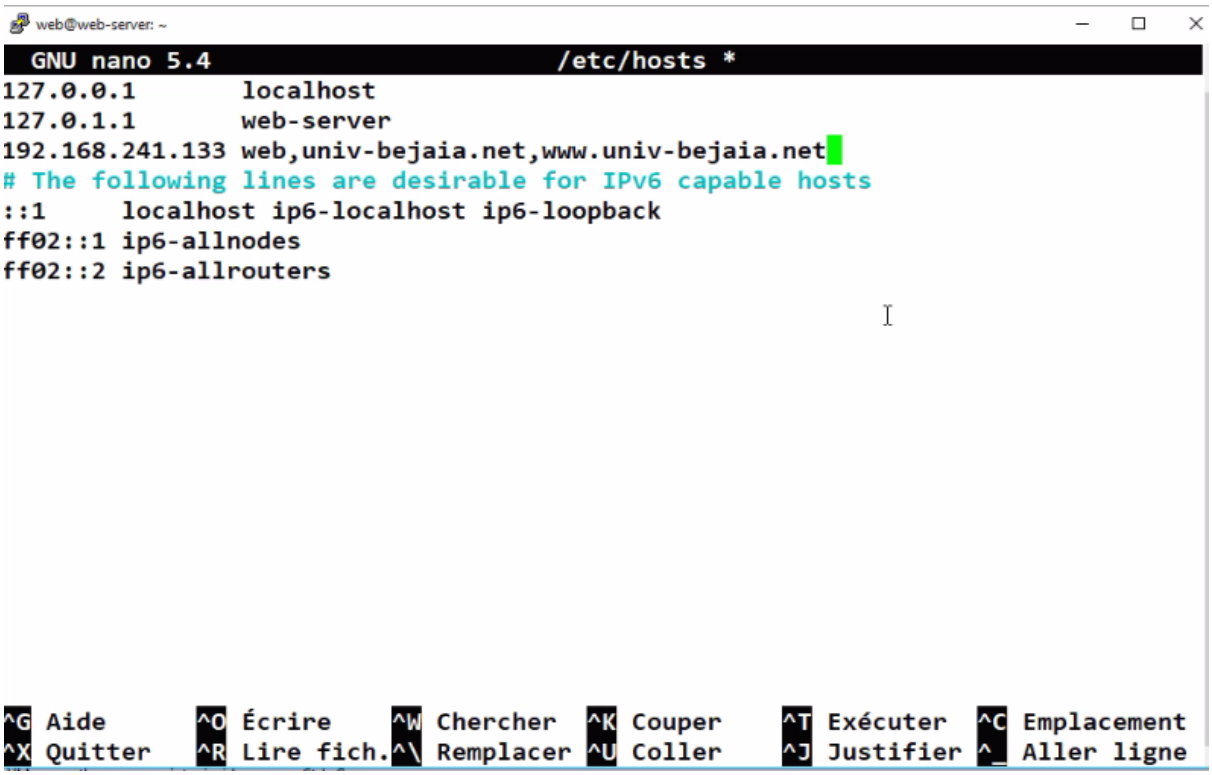

Figure 3.50:Création le nom des Domain.

3.9.3 Serveur apache

- **Définition Serveur apache :**

Apache est le serveur web le plus répandu (environ 70% des sites web selon netcrafit) sur l'internet. Apache est de loin l'application de serveur Web la plus utilisée dans les systèmes d'exploitation Linux, mais il peut être utilisé sur presque toutes les plates-formes de système d'exploitation telles que Windows, MAC OS, OS/2, etc. Il permet aux développeurs de publier leur contenu sur Internet.

- **Installation serveur apache :** la figure ci-dessous explique comment installer serveur apache à l'aide de la commande apt install:

Figure 3.51: Installation serveur apache2.

3.10 Phase 2 : configuration

3.10.1 Configurer les paramètres du serveur Web Apache :

Etape 1 : Vérifiez que le service Apache est en cours d'exécution Après l'installation, le service Web Apache démarre automatiquement. Cependant, pour vous en assurer, exécutez la commande suivante dans Terminal :

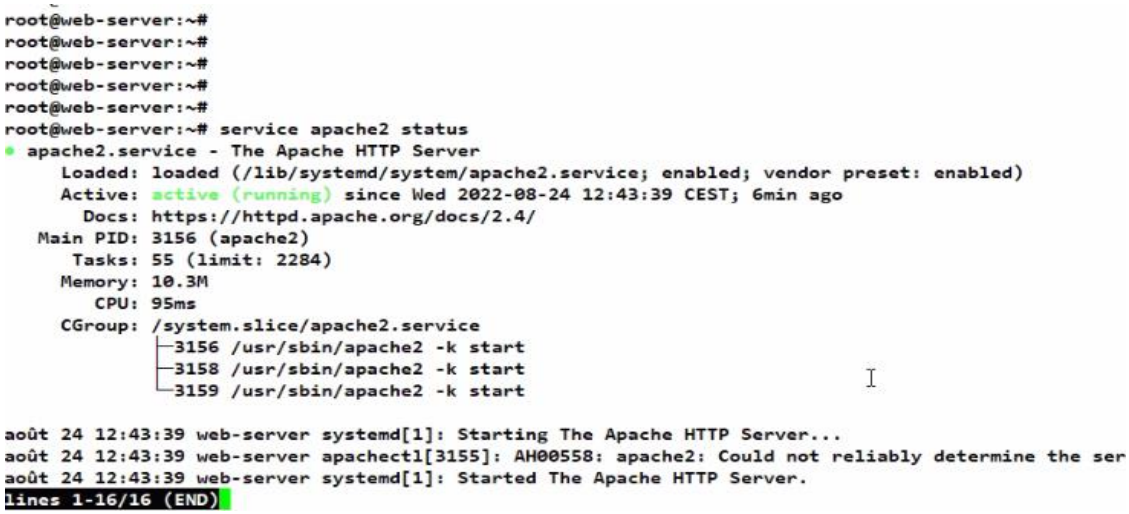

Figure 3.52 : Activation de serveur apache2.

Vérifier le serveur Web Apache : vérifier si le serveur Web Apache fonctionne correctement en demandant une page Web au serveur Web Apache. En entrant l'adresse IP 192.168.241.133 ci-dessus, vous verrez la page Apache par défaut suivante.

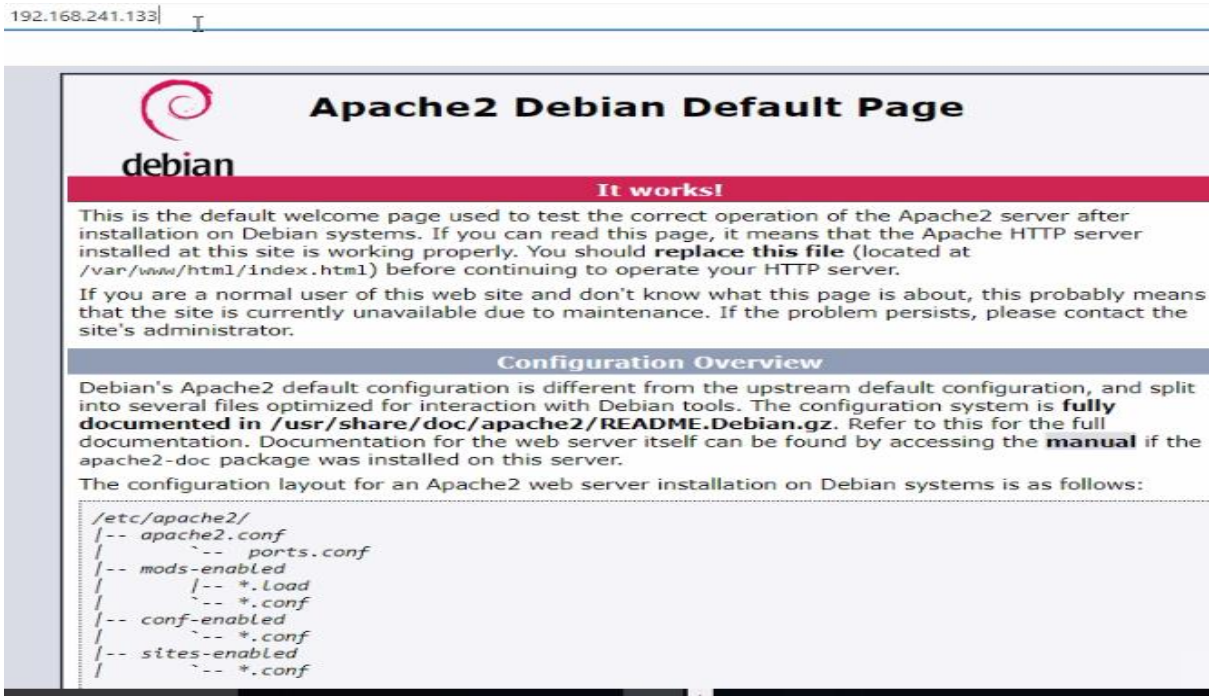

Figure 3.53: Page par défaut de serveur apache2.

Configurer des hôtes virtuels dans Apache :

Les hôtes virtuels d'Apache vous permettent d'exécuter plusieurs sites Web sur un seul serveur. Nous allons configurer ici un hôte virtuel dans le serveur Web Apache. Pour cela, nous allons d'abord créer un site web nommé **univ-bejaia.net** en utilisant le bloc serveur disponible par défaut dans Apache.

Étape 1 : configurer un nom de domaine

Tout d'abord, nous allons créer un répertoire à **/var/www** pour notre hôte virtuel **univ-bejaia.**net .Pour cela, nous utiliserons la commande suivante :

```
root@web-server:/var/www/html# exit
exit
web@web-server:~$
web@web-server:~$
web@web-server:~$ cd /home/
web@web-server:/home$ ls
web
web@web-server:/home$ cd /web
-bash: cd: /web: Aucun fichier ou dossier de ce type
web@web-server:/home$ cd /home/web/Bureau/
web@web-server:~/Bureau$
web@web-server:~/Bureau$ ls
univ-bejaia.net
web@web-server:~/Bureau$
web@web-server:~/Bureau$
web@web-server:~/Bureau$
web@web-server:~/Bureau$
web@web-server:~/Bureau$ cp -r univ-bejaia.net/  /var/www/
cp: impossible de créer le répertoire '/var/www/univ-bejaia.net': Permission non accordée
web@web-server:~/Bureau$ sudo cp -r univ-bejaia.net/  /var/www/
web@web-server:~/Bureau$ cd /var/www/
web@web-server:/var/www$ ls
html  univ-bejaia.net
web@web-server:/var/www$
web@web-server:/var/www$
web@web-server:/var/www$
web@web-server:/var/www$
```

Figure 3.54: Création répertoire var/www.

Nous allons maintenant créer un exemple de page d'index pour tester notre site **univ-bejaia.net**. Pour ce faire, nous allons créer un fichier HTML.

```
web@web-server:~/Bureau$
web@web-server:~/Bureau$ rm -r univ-bejaia.
web@web-server:~/Bureau$
web@web-server:~/Bureau$
web@web-server:~/Bureau$ LS
-bash: LS : commande introuvable
web@web-server:~/Bureau$ ls
web@web-server:~/Bureau$
web@web-server:~/Bureau$
web@web-server:~/Bureau$
web@web-server:~/Bureau$
web@web-server:~/Bureau$ cd /var/www/
web@web-server:/var/www$ ls
html  univ-bejaia.net
web@web-server:/var/www$
web@web-server:/var/www$
web@web-server:/var/www$ ls
html  univ-bejaia.net
web@web-server:/var/www$ cd univ-bejaia.net
web@web-server:/var/www/univ-bejaia.net$ ls
index_files  index.html
```

Figure 3.55 : index.HTML.

Nous allons maintenant créer un fichier d'hôte virtuel qui servira le contenu de votre serveur à l'aide de la commande suivante : etc/ apache2/site-available /et la commande sudo nano uviv-bejaia.net.conf

Figure 3.56:Création fichier hôte virtuelle.

Les détails de configuration suivants de notre nom de domaine :

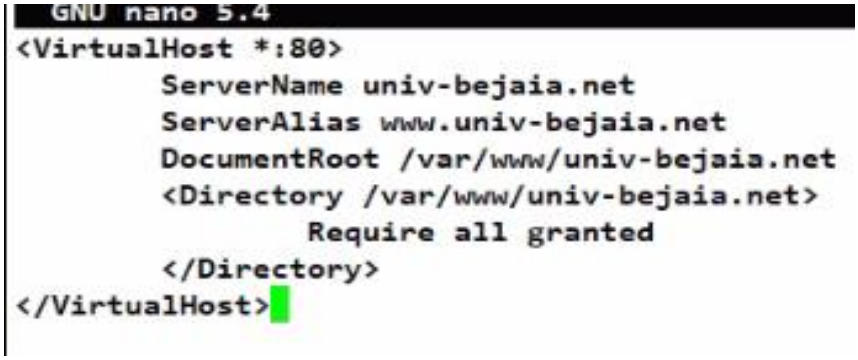

Figure 3.57: Les détails de nom Domain.

Étape 2 : Activez le fichier de configuration du domaine

On Active maintenant le fichier d'hôte virtuel à l'aide de la commande suivante :

```
sudo a2ensite univ-bejaia.net.conf
```

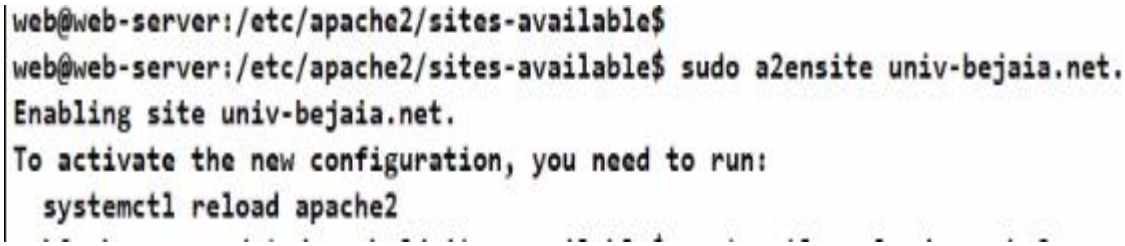

Figure 3.58:Activation fichier d'hôte.

Etape 3 : vérification serveur apache : vérifier si le serveur Web Apache fonctionne correctement en demandant une page Web au serveur Web Apache. En entrant nom de notre site web univ-bejaia.net ci-dessus, vous verrez la page de notre site suivante :

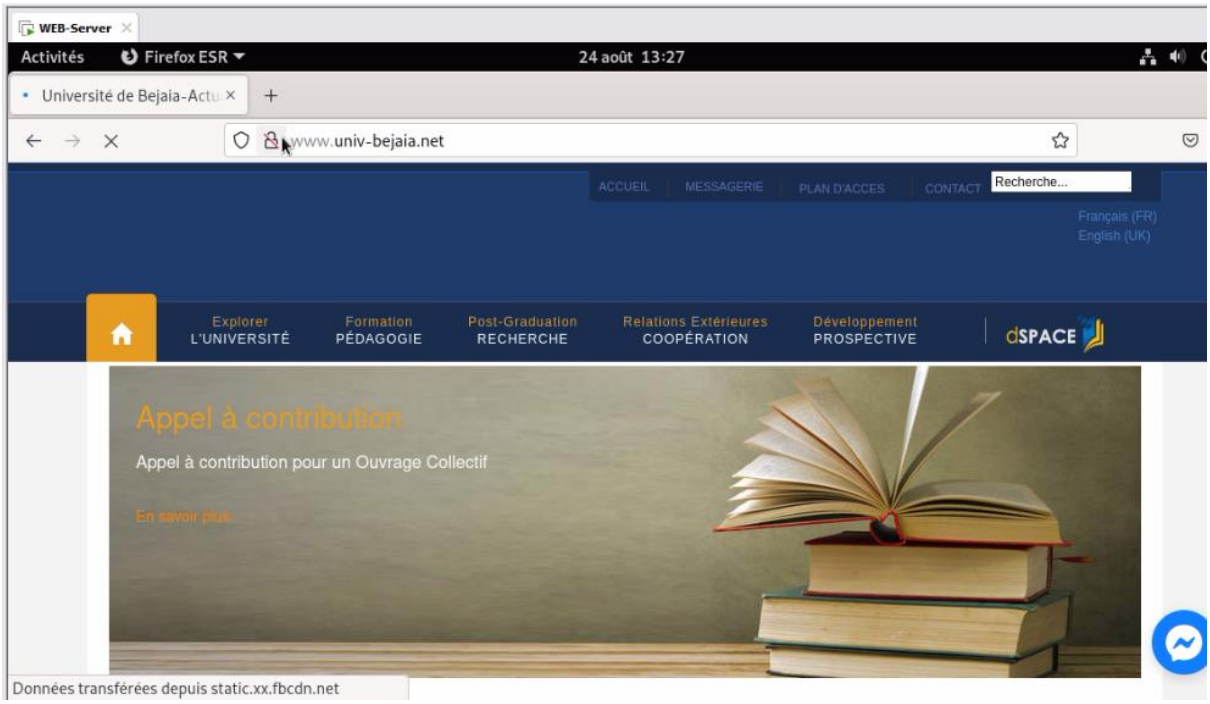

Figure 3.59:La page de site univ-bejaia.net.

4.10.2 Sécurisation serveur apache univ-bejaia.net.

Installation SSL : à l'aide de la commande sudo apt install openssl.

```
certs  openssl.cnf  private
root@web-server:/etc/ssl#
root@web-server:/etc/ssl#
root@web-server:/etc/ssl# sudo apt install openssl
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances... Fait
Lecture des informations d'état... Fait
openssl est déjà la version la plus récente (1.1.1n-0+deb11u3).
openssl passé en « installé manuellement ».
0 mis à jour, 0 nouvellement installés, 0 à enlever et 0 non mis à jour.
root@web-server:/etc/ssl# ls -la
total 44
```

Figure 3.60:installation SSL.

Création de certificat CRS (certificate signing request) : est un certificat qui n'est pas délivré par une autorité de certification réputée

Etape 1 : créer un nouveau sous dossier SSL : nous avons créé sous dossier ssl : univ-bejaia.net à l'aide de la commande sudo mkdir

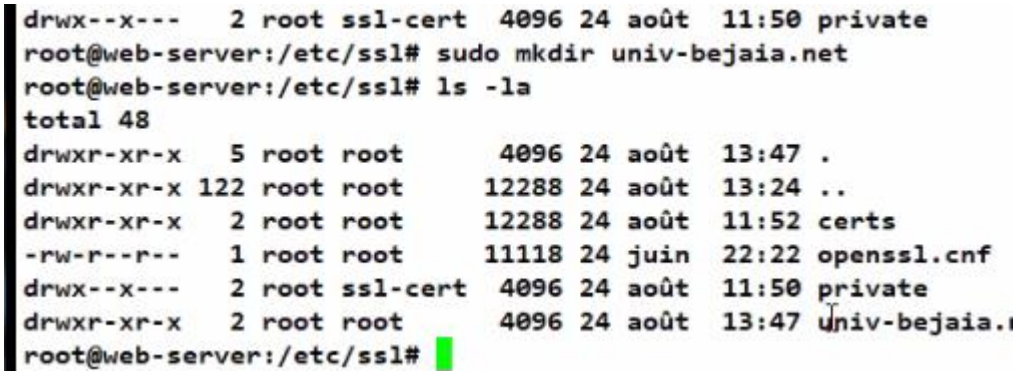

Figure 3.61: Création sous dossier SSL univ-bejaia.net.

Etape2 : créer un nouveau sous dossier univ-bejaia.net : nous avons créé sous dossier s'appelle private pour stoker la clé privée :

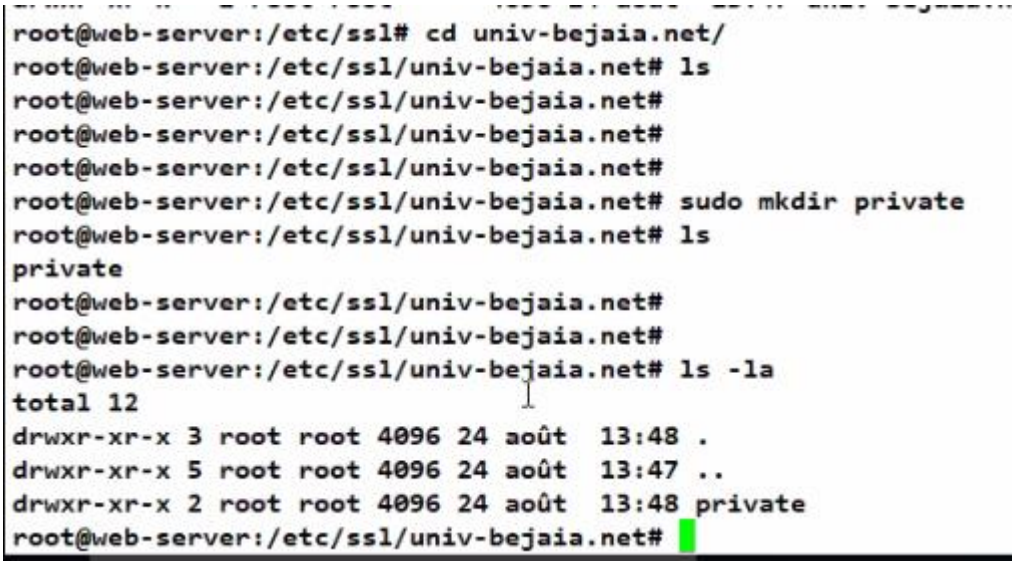

Figure 3.62: Création sous dossier private.

Etape 3 : création des fichiers : à l'aide de la commande sudo openssl req-x509-nodes-day 365-newkey rsa : 2048 –keyout /etc/ssl/univ-bejaia.net. Key –out/etc/univ-bejaia.net.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: novelle 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.

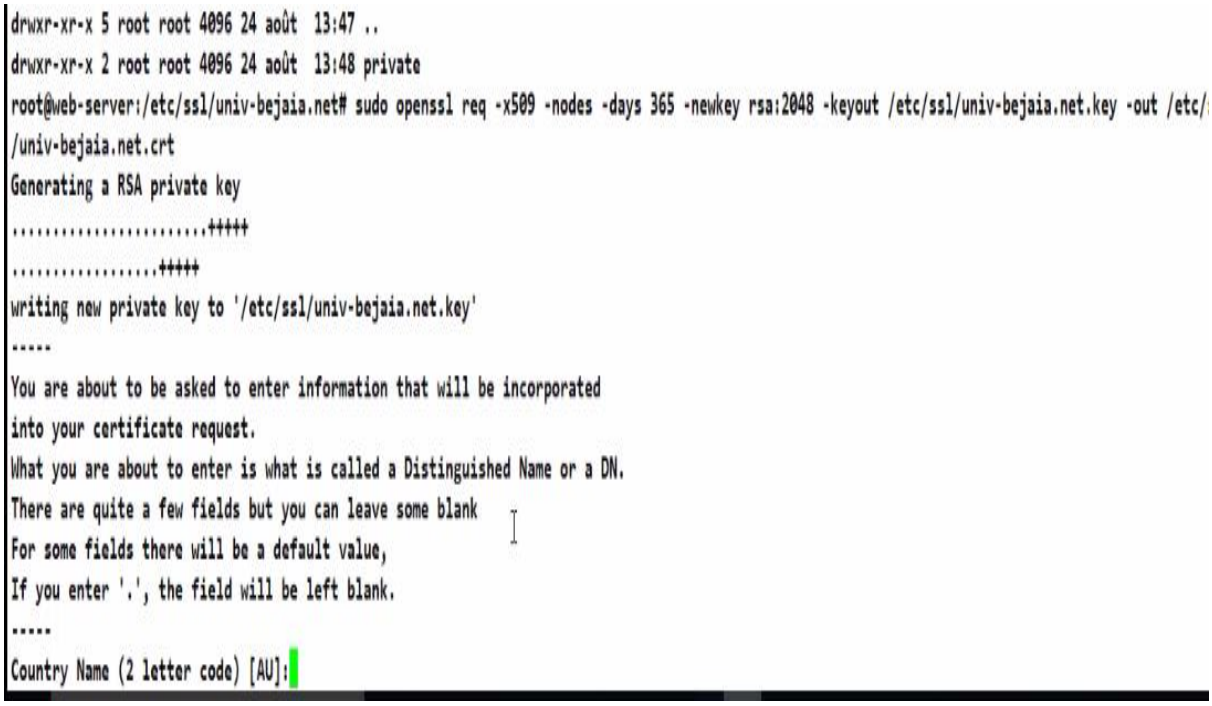

Figure 3.63:création des fichiers.

Etape 4 : rempiler le fichier ou stoker la clé privée :

Le code : DZ.

Le nom : Bejaia.

La cité : Bejaia.

La compagne : uviv-bejaia.net.

Le nom de serveur : univ-bejaia.net.

Adresse email : faiza.nadjet@univ-bejaia.net.

```
.....+++++
writing new private key to '/etc/ssl/univ-bejaia.net.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:DZ
State or Province Name (full name) [Some-State]:BEJAIA
Locality Name (eg, city) []:BEJAIA
Organization Name (eg, company) [Internet Widgits Pty Ltd]:univ-bejaia.net
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:univ-bejaia.net
Email Address []:faiza.nadjet@univ-bejaia.net
```

Figure 3.64:Remplissage du fichier.

Etape 5 : générer le certificat CRS :

```
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:univ-bejaia.net
Email Address []:faiza.nadjet@univ-bejaia.net
root@web-server:/etc/ssl/univ-bejaia.net#
root@web-server:/etc/ssl/univ-bejaia.net#
root@web-server:/etc/ssl/univ-bejaia.net# cd ..
root@web-server:/etc/ssl# ls
certs  openssl.cnf  private  univ-bejaia.net  univ-bejaia.net.crt  univ-bejaia.net.key
root@web-server:/etc/ssl# cp univ-bejaia.net.crt /etc/ssl/univ-bejaia.net
root@web-server:/etc/ssl# cd univ-bejaia.net
root@web-server:/etc/ssl/univ-bejaia.net# ls
private  univ-bejaia.net.crt
root@web-server:/etc/ssl/univ-bejaia.net# cd ..
root@web-server:/etc/ssl# cp univ-bejaia.net.key  /etc/ssl/univ-bejaia.net/private/
root@web-server:/etc/ssl# ls
certs  openssl.cnf  private  univ-bejaia.net  univ-bejaia.net.crt  univ-bejaia.net.key
root@web-server:/etc/ssl# rm univ-bejaia.net.key
root@web-server:/etc/ssl# rm univ-bejaia.net.crt
root@web-server:/etc/ssl# cd univ-bejaia.net
root@web-server:/etc/ssl/univ-bejaia.net# ls
private  univ-bejaia.net.crt
root@web-server:/etc/ssl/univ-bejaia.net# cd private/
root@web-server:/etc/ssl/univ-bejaia.net/private# ls
univ-bejaia.net.key
root@web-server:/etc/ssl/univ-bejaia.net/private#
root@web-server:/etc/ssl/univ-bejaia.net/private# cd ..
root@web-server:/etc/ssl/univ-bejaia.net# ls
private  univ-bejaia.net.crt
root@web-server:/etc/ssl/univ-bejaia.net#
```

Fi0gure 3.65: générer le certificat CRS.

Vérification le certificat CRS :

```
root@web-server:/etc/ssl/univ-bejaia.net# ls
private  univ-bejaia.net.crt
root@web-server:/etc/ssl/univ-bejaia.net# cat univ-bejaia.net.crt
-----BEGIN CERTIFICATE-----
MIIEAzCCAuugAwIBAgIUB3gcUrtI2sXiOpR2Tb7kadVd070wDQYJKoZIhvcNAQEL
BQAwgZAxCzAJBgNVBAYTAkRaMQ8wDQYDVQQIDAZCRUpBSUExDzANBgNVBAcMBkJF
SkFJQTEYMBYGA1UECgwPdW5pdi1iZWphaWEubmV0MRgwFgYDVQQDDA91bml2LWJ1
amFpYS5uZXQxKzApBgkqhkiG9w0BCQEWHGZhaXphLm5hZGp1dEB1bml2LWJlamFp
YS5uZXQwHhcNMjIwODI0MTE1NjEwWhcNMjMwODI0MTE1NjEwWjCBkDELMAkGA1UE
BhMCRFoxDzANBgNVBAgMBkJFSkFJQTEPMA0GA1UEBwwGQkVKQU1BMRgwFgYDVQQK
DA91bml2LWJ1amFpYS5uZXQxGDAWBgNVBAMMD3VuaXYtYmVqYW1hLm51dDErMCkG
CSqGSIb3DQEJARYcZmFpemEubmFkamV0QHVuaXYtYmVqYW1hLm51dDCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBANEqDctVkr2tjFjJF3s1hc/iNXVOVuYv
Mw5rRjK3Dc6HOjOUiMRGMs1nKZS53u8CdFGi3IuCdNVX9zEmMSYTBDV050yWZ4+P
QDR/TJt2ecze52qm0OAZ/p1uAXTIL3ID9VTLdXjADM5JDtSgGYi61DxtSR/AJqOG
EsjkHbBRp7d8WSjxX63agd+LptJUTeyiuJe/gKI86KrpTRoW9sRoMH/pN+6ifAiZ
QJB/kFvg5ItYHMM/SIBN+tzxQ6haT5LoWL5AA/5zYeJp7SIu03o8V2alECofODMp
nZAPaZEvcvicjtcQi4XzPkuY/Mxdeec7xCzAO+pVH+I1B5aHXQ6djhUCAwEAAaNT
MFEwHQYDVR0OBBYEFN7swpdmLGKOTEn+qhW97SRBYqopMB8GA1UdIwQYMBaAFN7s
wpdmLGKOTEn+qhW97SRBYqopMA8GA1UdEwEB/wQFMAMBAf8wDQYJKoZIhvcNAQEL
BQADggEBAEMgh2m85e3WUAwAEVHxIwEKVyvia/7xhFAROqRErDueptgkMMfWXs0o
1zEhmv8DdsZuF/wfI712TEpca6uHaE1fLA81VVkmN/6632aHYE5+1uH1gAVD2aPc
tXyOISBI2XOYwciYn6urgqptX9oM3bgS1qP6fss5UKN+McVvjMvrkpvsAardy2QU
u6S3BJkaRbQf9oXF1MFI+56zsQ9skBFJs97ULuBEnxr+Rm8GOHOchPLbnuCof+yG
6k+TSCxBl3crPsQlgVAO1nEeeS/RxTvzmaxqxtbEJ6+5GyxHSUAk7YMXYPMsObf8
J2Pz+EwD1e4vFC4WPMskuCLgY/WmM78=
-----END CERTIFICATE-----
root@web-server:/etc/ssl/univ-bejaia.net#
```

Figure 3.66: Le certificat CRS.

Vérification la clé privée :

```
-----END CERTIFICATE-----
root@web-server:/etc/ssl/univ-bejaia.net# cd private/
root@web-server:/etc/ssl/univ-bejaia.net/private# ls
univ-bejaia.net.key
root@web-server:/etc/ssl/univ-bejaia.net/private# cat univ-beja
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDRKg3LVZK9rYx
yRd7JYXP4jV1T1bmLzMOa0Yytw3Ohzoz1IjERjLJZymUud7vAnRRotyLgnTVV/c
JjEmEwQ1dOdM1mePj0A0f0ybdnnM3udqptDgGf6ZbgF0yC9yA/VUy3V4wAzOSQ7
oBmIutQ8bUkfwCajhhLI5B2wUae3fFko8V+t2oHfi6bSVE3soriXv4CiPOiq6U0
FvbEaDB/6TfuonwImUCQf5Bb4OSLWBzDP0iATfrc8UOoWk+S6Fi+QAP+c2Hiae0
LtN6PFdmpRAqHzgzKZ2QD2mRL3L4nI7XEIuF8z5LmPzMXXnnO8QswDvqVR/iJQe
h10OnY4VAgMBAAECggEBAKFdUEcOPacXvK7CdNsM169JVPSq+1+aCkmVeRKnJn+
07f3X4wMnCHE9M9I1jTOL+7LN1pqyrfMpWfFjyVQhm63QbpUTpDycxYNH4zQWic
0FT3XS2G4GR9+aGezvunEh3Y2UfO4hJDSq2+1fQmLpZvuXpFQ4nkZZmWY1EjrcB
R/1EItQ1/VX6+cgEgDbdeUiuMxVH8OXcIYuPexs9AeKdo5xATBoEE11cuJtfrWw
jEorQki1WRRikpJL1r4WXDV2z/RYUpqZPAM9kDdDmmbaoz9hw3EfR0zUwJQcc5m
NhzE7NBnL7CAeHYuD9vfZ6UjW8VcgLGVPr17XdHOkAECgYEA/MpHv6s8jP5RvjyL
Y3z1R6XHAeOTbrQTTnWCIofZw/q9MUCrTE9fxOKY3GrfzHvqDtz/vQ5CMErNIq3U
OWBwKqrdNmRqAXrmCHKcr40tANO1/ZdYBr1wfsKaCnKGL3gMHB19XVf6XSdkLByI
2d2mtaGOos+oKgNDIYRC5Weg7wkCgYEA09H2m1mpNaEaZVRK1gt1Qha2aQQIt01I
nY0AYU5rR2sWm3Mhbse5lRwp/oNaKdL1/fD8FEF7F/g9NSBIoiMCvZH+Uet+UtxC
iILiaAiA/ZGxc6gj232mCin+s312Bk6LgfiTx6vtNpIjwdPR3tpbCLAUbcyeWPVC
cvBFoBeIHa0CgYBzJEPYBswWwIRFLV2mxTUHxHfH4Xu28ejVVOrIha5n+N6R/43C
vWS2ziuoQjnb7xkmWf1WhJcbXgbf4+OFmuqcVKVb8BLkx7Ddai76O0ijVstPTc8I
irQh2MvHNHDwUDLb3bRffwI3yghzmzxvS+1yU7sfZ4yGTmQWcSLzUOdZ2QKBgAsp
xbb1n/kcTJm0MvZJxPkS3mRn/Nk8a0YZqUJzbz1iS97AzqnWPk6yGxau6ea2mLSc
m3Co/AGHXhfTaV1zP2qcJ+M/3vQVdHMphSF4CObJZ6wu0ituz3FLQYFGfxPXvoa
e6UKyDyMsuo06ZqumAe90GTwUgVUZ9i9/LprYhBFAoGAT+XWcvkJNeduh1xsI1fA
I37xSaRHIasL29LoNEPr06QmAKrT/nz89GGB755aG591vPUGYDhwky5OHHs5UFdV
8S5ZjIDYs9M7Nc59FAKpt9nOzqJOSSP405f76XcF1SqxThxADZAnE+AAvfkzIzpC
XwWiNWfCZWP6XcHdhO4KMq4=
-----END PRIVATE KEY-----
root@web-server:/etc/ssl/univ-bejaia.net/private#
```

Figure 3.67: La clé privée

Appliquer le certificat CRS sur Hôte virtuelle :

Etape1 : accéder au fichier ou on a stocké le local host : on accéder a le fichier à l'aide la commande cd/etc/apache2/sites-available/ el ls : le fichier c'est univ-bejaia.net.conf.

```
e6UKyDyMsuo06ZqumAe90GTwUgVUZ9i9/LprYhBFAoGAT+XWcvkJNeduh1xsIlfc
I37xSaRHIasL29LoNEPr06QmAKrT/nz89GGB755aG591vPUGYDhwky5OHHs5UFdV
8S5ZjIDYs9M7Nc59FAKpt9nOzqJOSSP405f76XcF1SqxThxADZAnE+AAvfkzIzpQ
XwWiNWfCZWP6XcHdhO4KMq4=
-----END PRIVATE KEY-----
root@web-server:/etc/ssl/univ-bejaia.net/private# cd
root@web-server:~# cd /etc/apache2/sites-available/
root@web-server:/etc/apache2/sites-available# ls
000-default.conf  default-ssl.conf  univ-bejaia.net.conf
root@web-server:/etc/apache2/sites-available# nano univ-bejaia.net.conf
```

Figure 3.68 : Le fichier stockage du local host.

Etape 2 : validation de fichier : à l'aide la commande nano

```
 GNU nano 5.4                                    univ-bejaia.net.conf
<VirtualHost *:80>
        ServerName univ-bejaia.net
        ServerAlias www.univ-bejaia.net
        DocumentRoot /var/www/univ-bejaia.net
        <Directory /var/www/univ-bejaia.net>
                Require all granted
        </Directory>
</VirtualHost>
```

Figure 3.69:Validité de fichier local host.

Etape 5 : rajouter le port 443 et activer le certificat sur local host :

Figure 3.70: ajouter le port 80et activation du certificat.

Activer le module SSL : on active le mode SSL a l'aide la commande sudo a2nmod SSL :

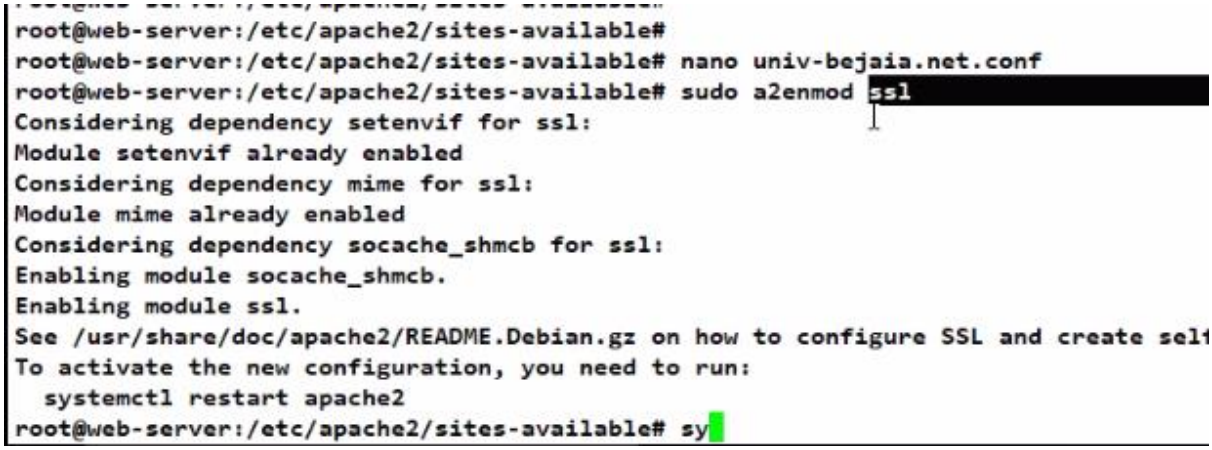

Figure 3.71: Activation module SSL.

Redémarrer le serveur apache : à l'aide de la commande : systemctl restart apache2.

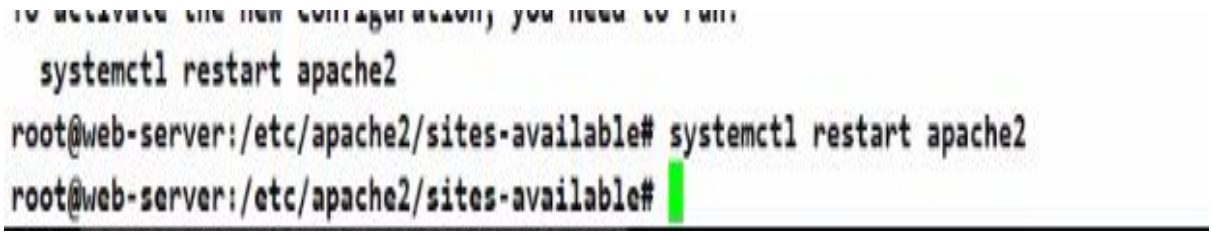

Figure 3.72: Redémarrage serveur apache2.

3.11 : Phase 3:Tests

Teste 1 : accéder au site avec https à partir web-server : on accède à notre site avec https.

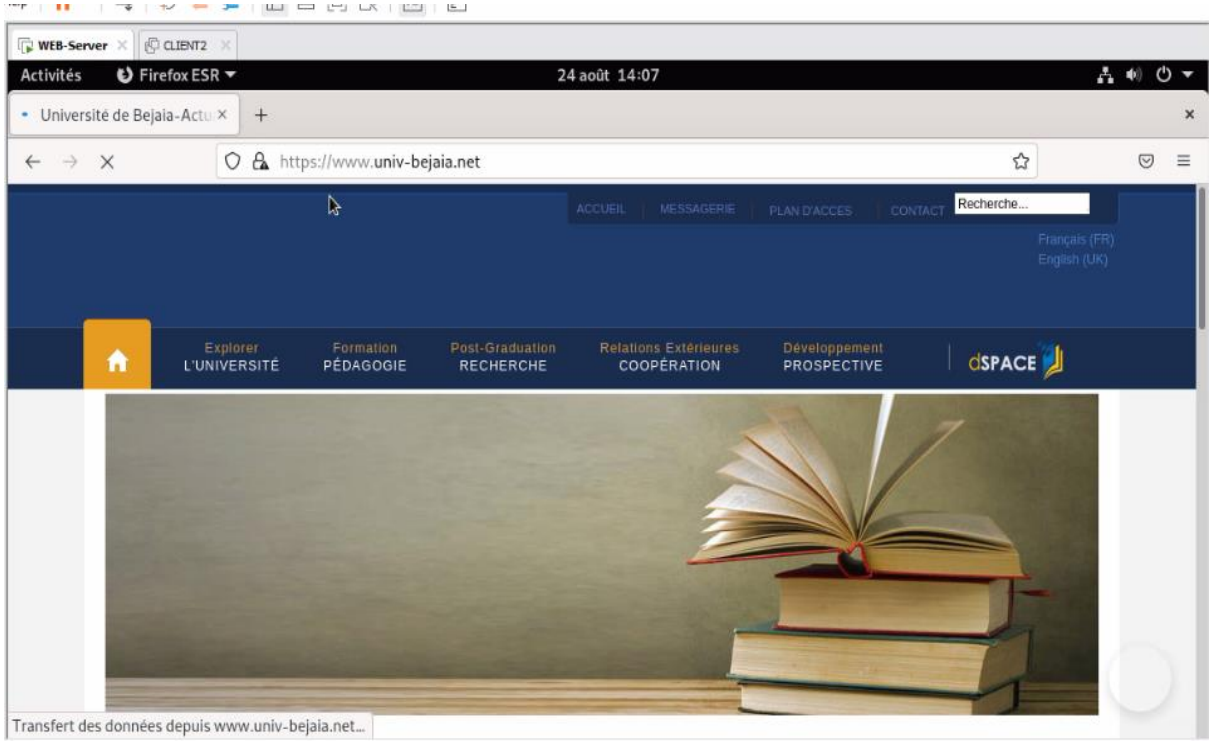

Figure 3.73: accéder au site avec https.

Rediriger les clients vers https : dans fichier configuration on va supprimer notre Directory et DecumentRoot et mettre la commande RedirectPermanent /https://univ-bejaia.net.

```
<VirtualHost *:80>
        ServerName univ-bejaia.net
        ServerAlias www.univ-bejaia.net
        RedirectPermanent / https://univ-bejaia.net
        RedirectPermanent / https://www.univ-bejaia.net
</VirtualHost>
<VirtualHost *:443>
        ServerName univ-bejaia.net
        ServerAlias www.univ-bejaia.net
        DocumentRoot /var/www/univ-bejaia.net
        <Directory /var/www/univ-bejaia.net>
                Require all granted
        </Directory>
        SSLEngine on
        SSLCertificateFile /etc/ssl/univ-bejaia.net/univ-bejaia.net.crt
        SSLCertificateKeyFile /etc/ssl/univ-bejaia.net/private/univ-bejaia.net.key
</VirtualHost>
```

Figure 3.74: rediriger les clients vers https.

Puis activer mode SSL et redémarrer le serveur.

Recharger le serveur apache : à l'aide de la commande systemctl reload apache2.

Figure 3.75: recharger le serveur apache.

La configuration de client2 (client internet):

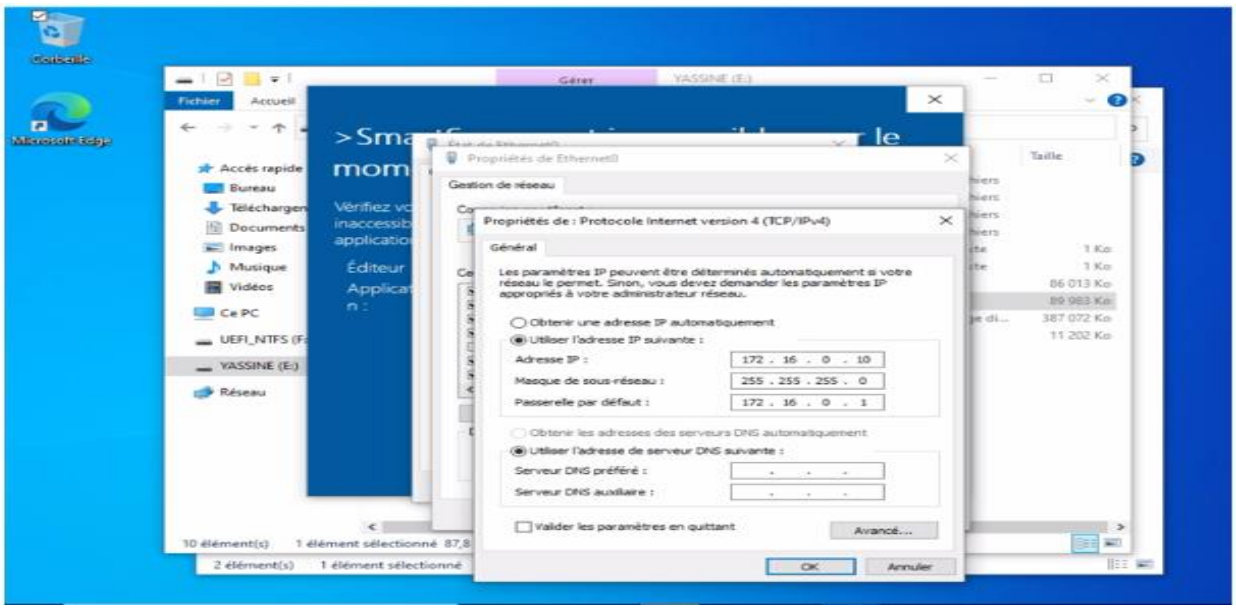

Figure 3.76: la configuration de client-internet.

Création local host pour client-internet et client 1:

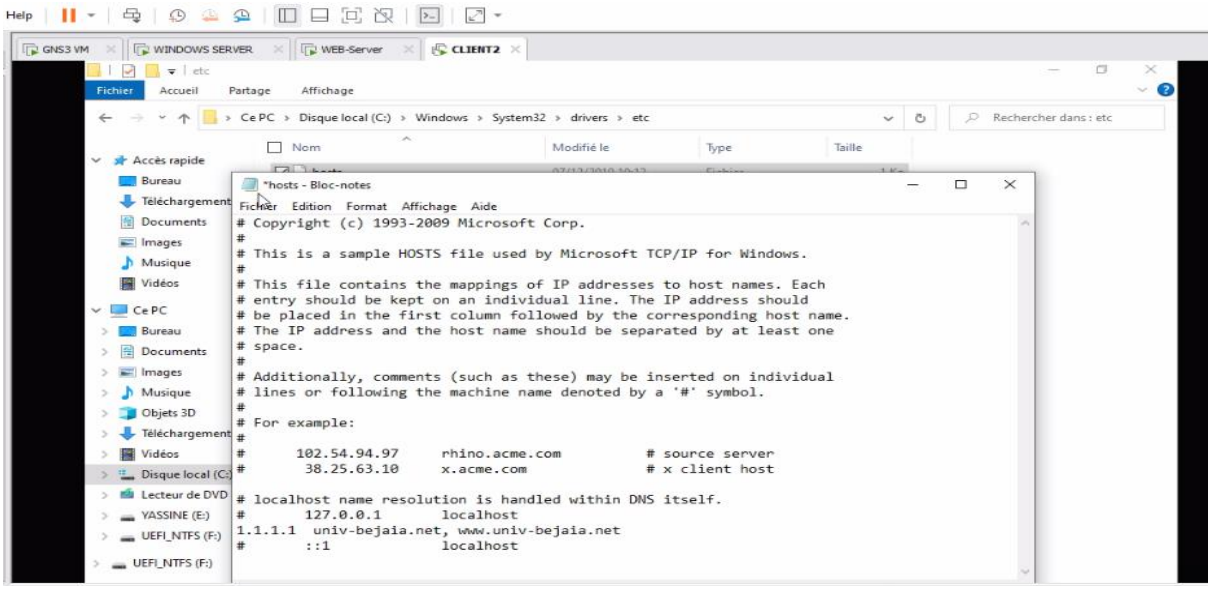

Figure 3.77 : création local host pour client-internet.

Même chose pour client1.

- **La configuration DMZ :**

1. accéder au pfsense a partir windows server :

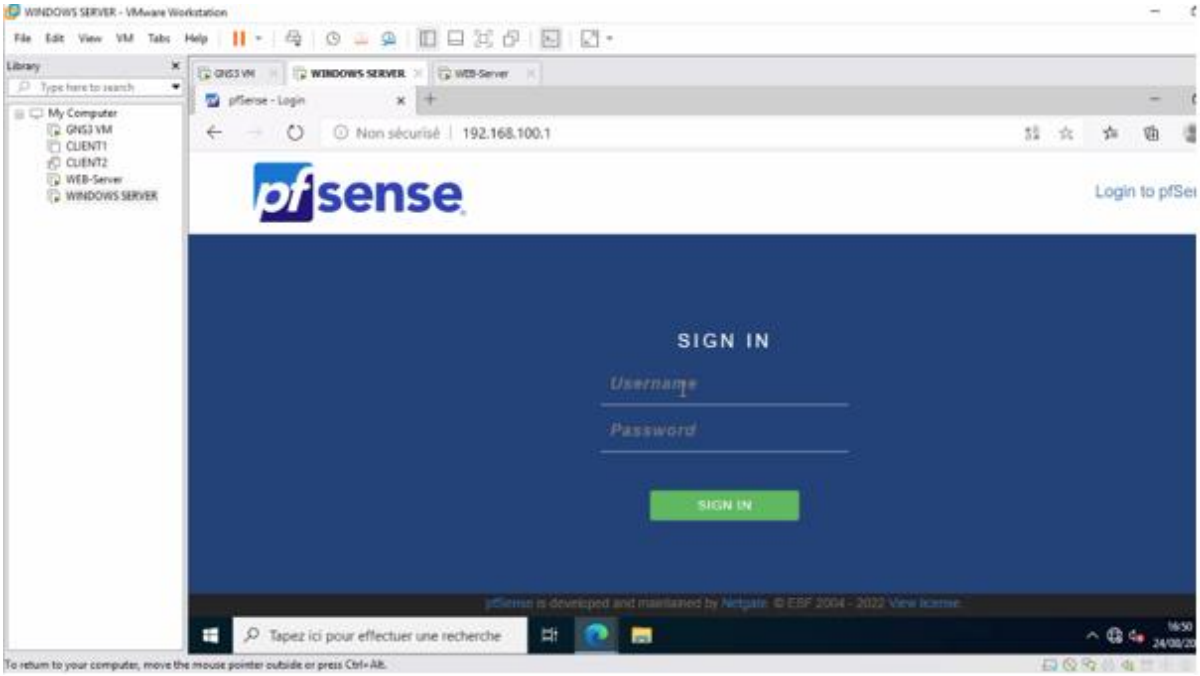

Figure 3.78: Pfsense.

2. créer la rode action pour firewall: autoriser une règle dans WAN depuis any adresse vers notre serveur avec HTTPS.

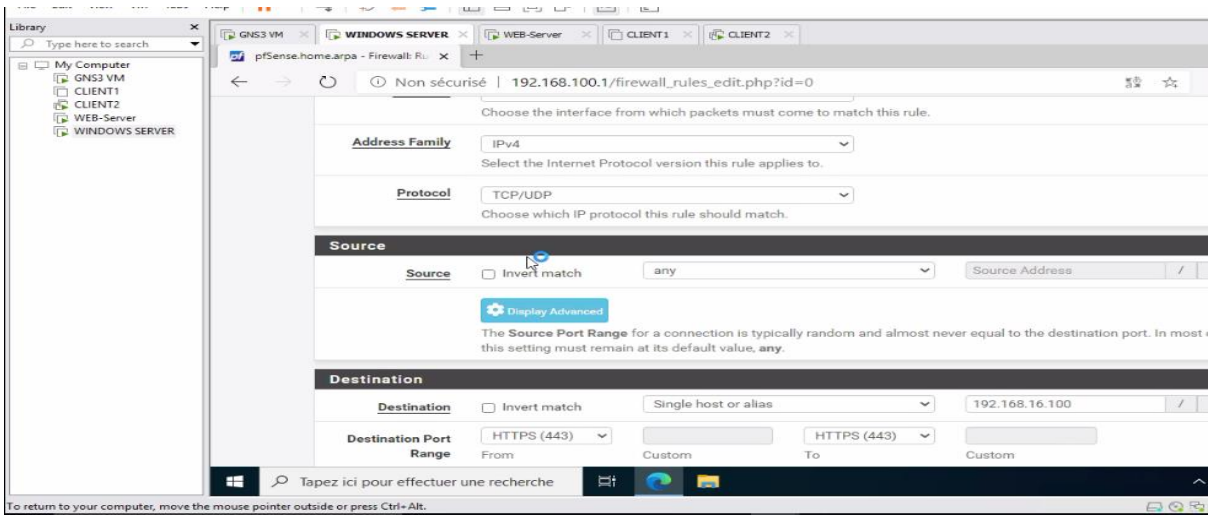

Figure 3.79: création rode action HTTPS pour firewall.

3. autoriser la règle http pour firewall :

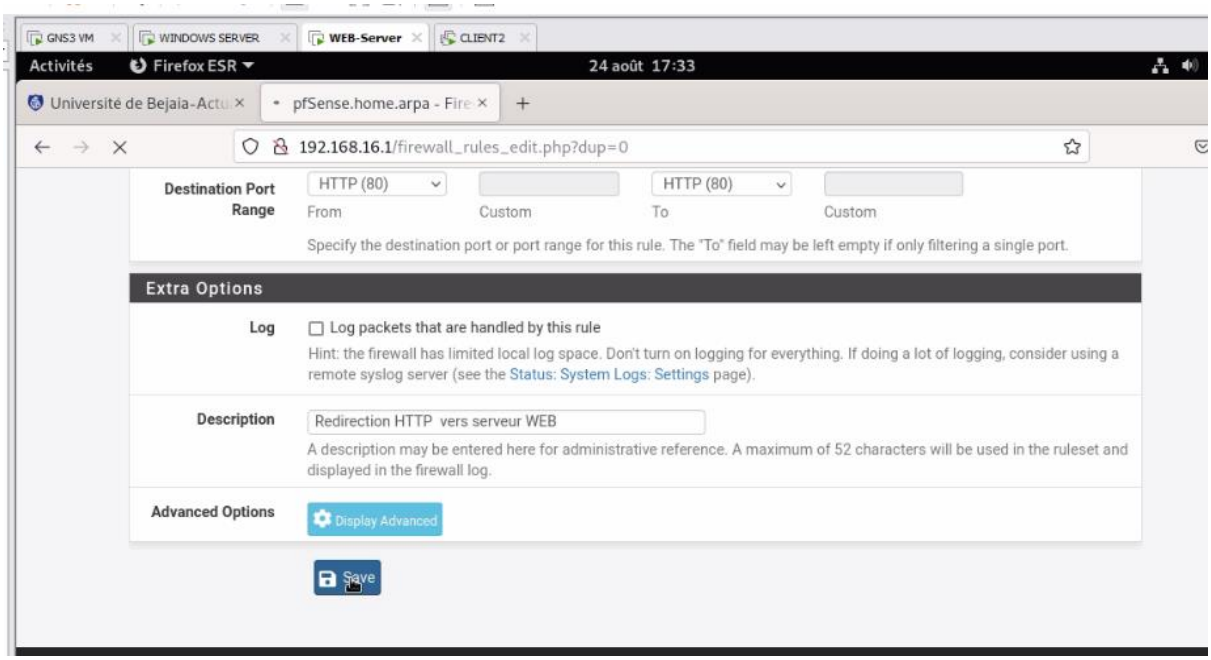

Figure 3.80: autoriser http.

- **Froidir FW-BEJAIA :**

Après effective de NAT on doit froide les ports notre serveur à partir firewall :

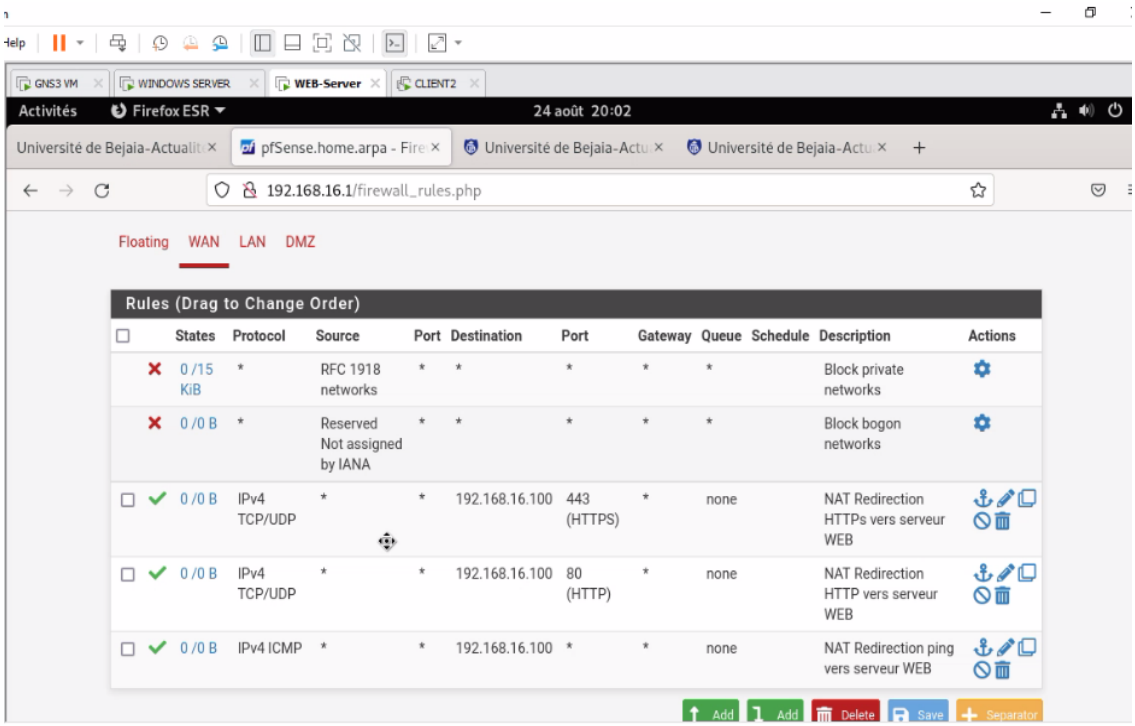

Figure 3.81:les règles http et https et Ping pour firewall.

Teste2 : accéder au site à partir d'intérieur :

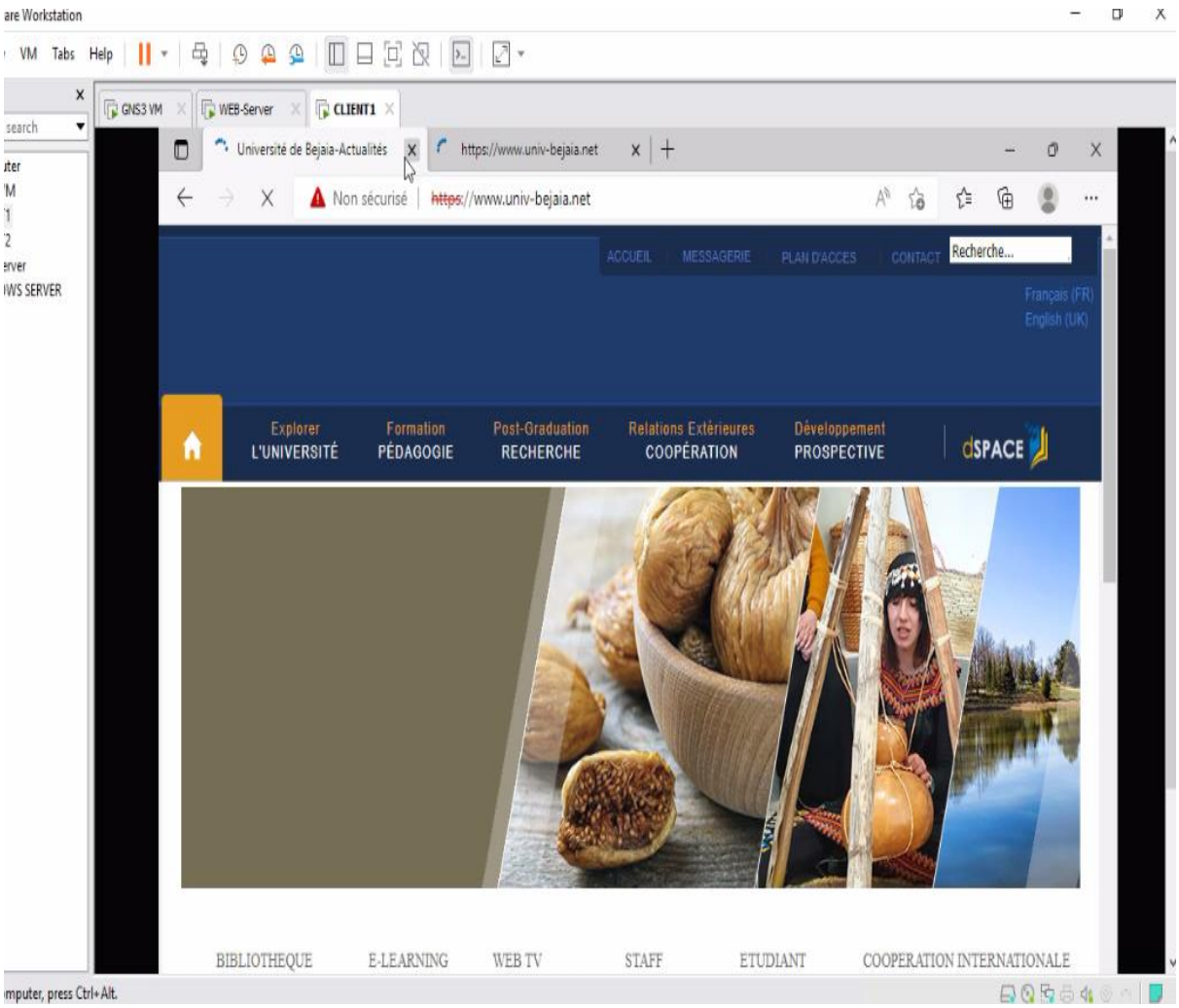

Figure 3.82: accéder au site avec https à partir d'intérieur.

Teste 3 : accéder au site à partir d'extérieur :

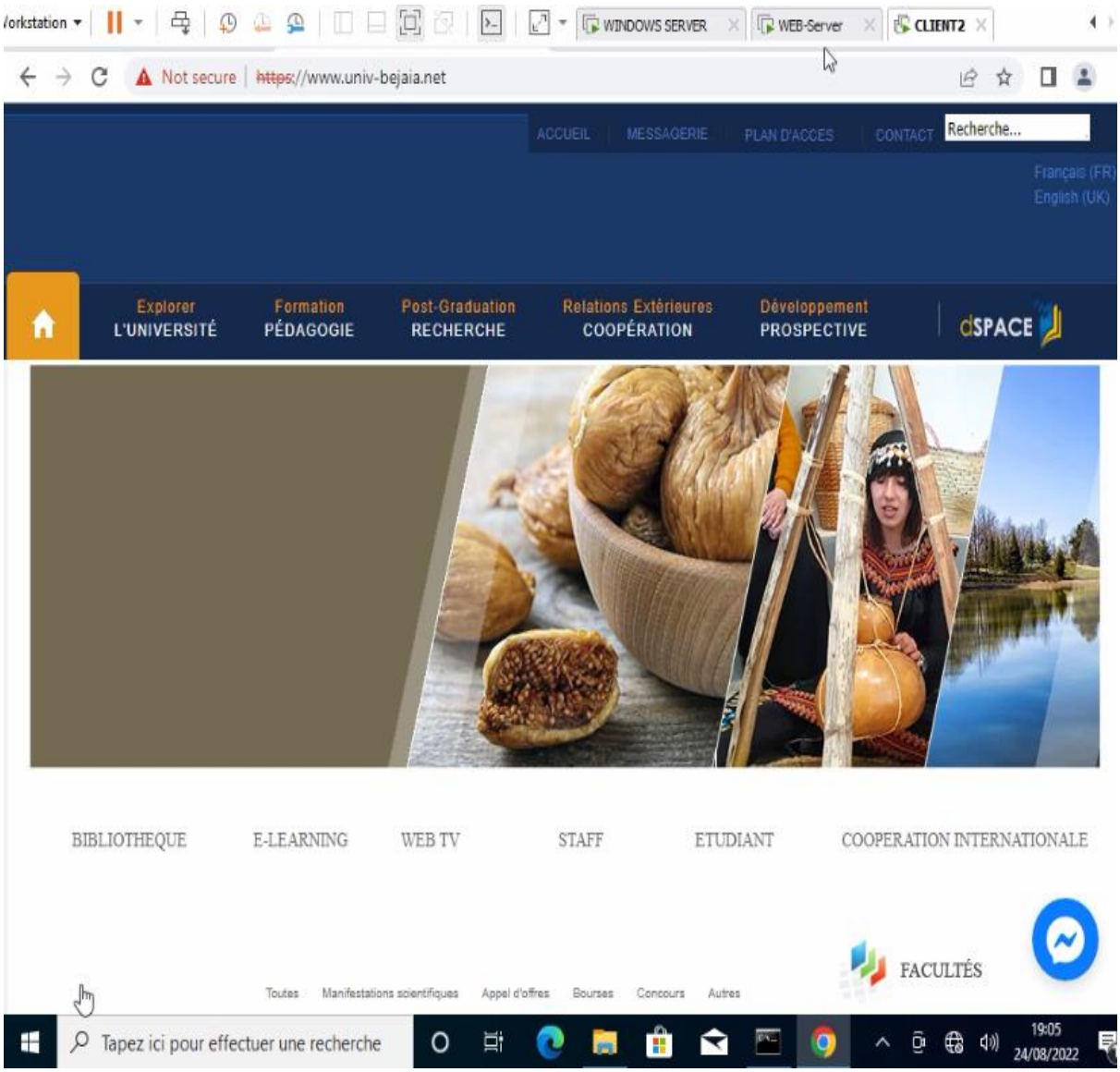

Figure 3.83: accéder au site avec https à partir l'extérieur.

3.12 Conclusion :

Dans ce chapitre, nous avons traité un ensemble de tâches à effectuer pour sécuriser le serveur web et nous avons présenté la solution mise en place et les tests de validation pour nous assurer que notre objectif a bien attiennent.

Conclusion général :

Sécuriser un système est une tâche difficile, surtout lorsque ledit système informatique est connecté à Internet. En fait, le World Wide Web grouille de pirates qui interfèrent avec le bon fonctionnement de vos systèmes.

La sécurité se fera avant tout au niveau du serveur web pour le protéger des attaques extérieures, mais aussi pour ne pas déranger les utilisateurs éventuels qui utilisent la même machine en parallèle pour d'autres raisons. : Restreindre Apache à consommer dans les ressources disponibles permettant ainsi d'autres utilisateurs/applications de la machine pour qu'ils fonctionnent/s'exécutent correctement.

L’objectif de notre travail était de sécuriser un serveur web apache.

Ce projet nous a permis d’acquérir des connaissances dans de nombreux domaines. En effet il nous à initier au monde de la recherche sur les réseaux informatique surtout en ce qui concerne la sécurité, ainsi les différents modes de communication, leur application ainsi que les protocoles qui les gèrent. Grâce à notre modeste travail, nous avons eu l’occasion de voir beaucoup de choses de plus près et d’enrichir nos connaissances, nous avons aussi eu la chance de mettre nos capacités en valeur et de faire face aux situations critiques et obstacles et apprendre comment procéder pour s’en sortir.

Comme perspectives, mettre en place un certificat numérique d’un fournisseur agréé pour cette dernière, mettre en place un firewall dédié pour le service WEB tel que fortiweb de fortinet.

Annexe A

➢ Les étapes d'installations VMware Workstation :

Étape 1 : Ouvrez le fichier d'installation de VMware Workstation Pro.

Étape 2 : Cliquez sur « NEXT ».

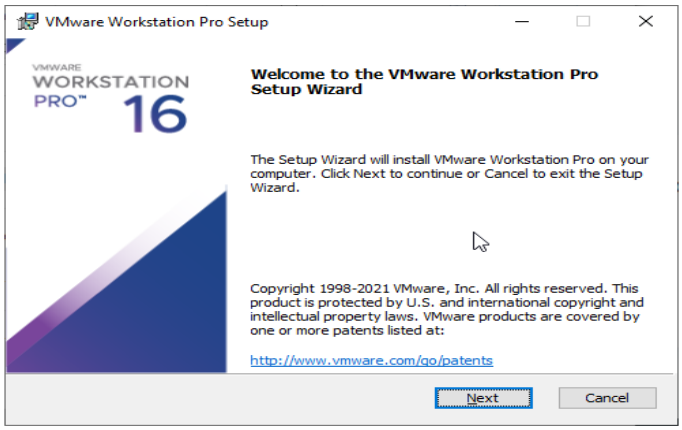

Figure A.1 : Démarrage d'installation d'une VM

Étape 3 : Acceptez le contrat de licence

Étape 4 : Choisissez le lieu souhaité pour l'installation et cliquez sur « Next ».

Étape 5 : Cochez les options si vous le souhaitez et cliquez sur Next.

Étape 6 : Cliquez sur « Next ».

Étape 7: Cliquez sur Install. La durée de l'installation dépend de la puissance de votre ordinateur

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.

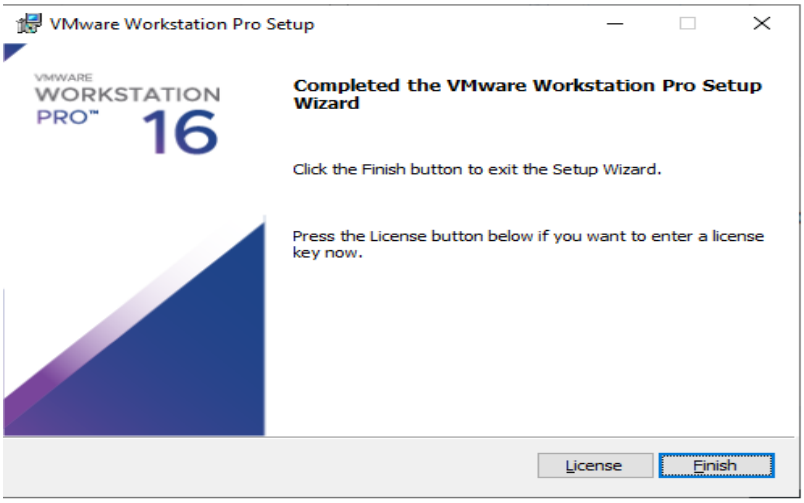

Figure A.2 : Fin des étapes d'installation d'une VM

Annexe B

➢ 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'installeur Windows depuis le lien fourni (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 taches additionnelles inchangée et validez.

11. Ne modifiez pas le répertoire dans lequel Wireshark sera installé et validez.

12. 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'exécute 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.

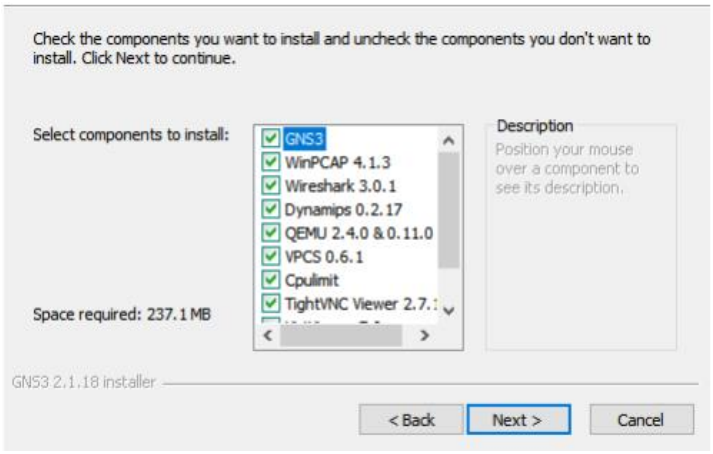

Figure B.1 : Répertoire de GNC3

18. Décochez « Start GNS3 » et cliquez sur « Finish ». 19. L'installation est terminée.

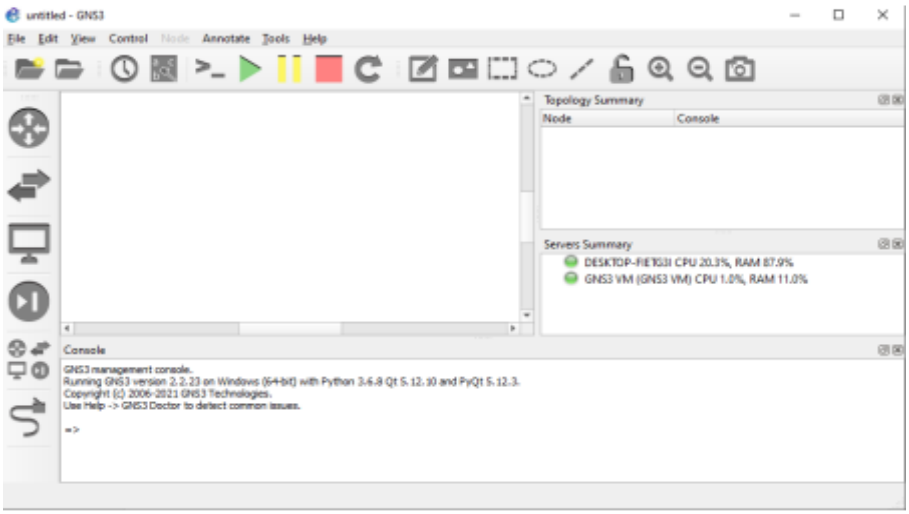

Figure B.2: l'interface de GNS3

ANNEXE C

➢ Les étapes d'Installations Windows serveur :

1 / Ouvrez VMware et créez la machine virtuelle depuis le menu "Fichier - Nouvelle machine virtuelle" :

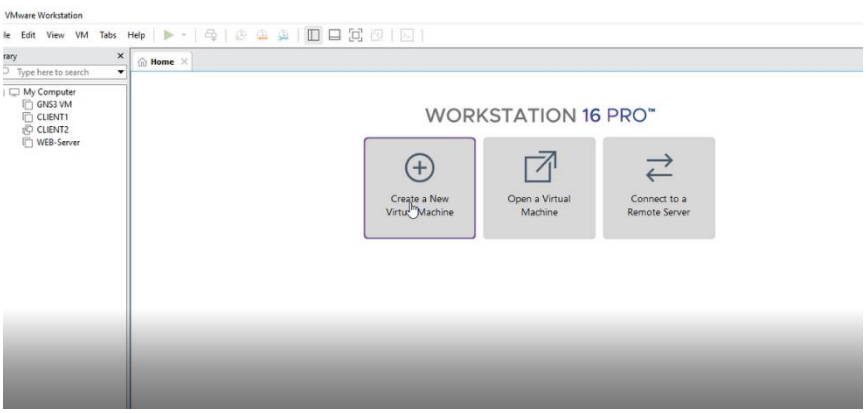

Figure C.1 : l'interface VMware Workstation

2 / Alternativement, nous pouvons utiliser les touches Ctrl + N ou cliquer sur "Créer une nouvelle machine virtuelle".

Les éléments suivants seront affichés :

3 / Sélectionnez l'option Typique, puis nous sélectionnons l'option pour installer le système plus tard :

4 / Cliquez sur Suivant et sélectionnez le système et l'édition, dans ce cas ce sera Windows Server 2021-2022 :

5/ Nous entrons le nom de la machine et son emplacement local :

6/ Cliquez sur « Next » et nous définirons la taille du disque et le type de stockage à utiliser :

7/ Nous cliquons sur Suivant pour voir les éléments suivants :

8/ On clique sur "Customize Hardware" et dans la fenêtre de configuration on va attribuer le réseau adapté :

9/ Dans Nouveau CD, sélectionnez l'image ISO que nous avons téléchargée

10/ Cochez la case "Utiliser le fichier image ISO", cliquez sur Parcourir et choisissez l'ISO :

11/ Cliquez sur Ouvrir pour le voir intégré :

12/ Appliquer les modifications.

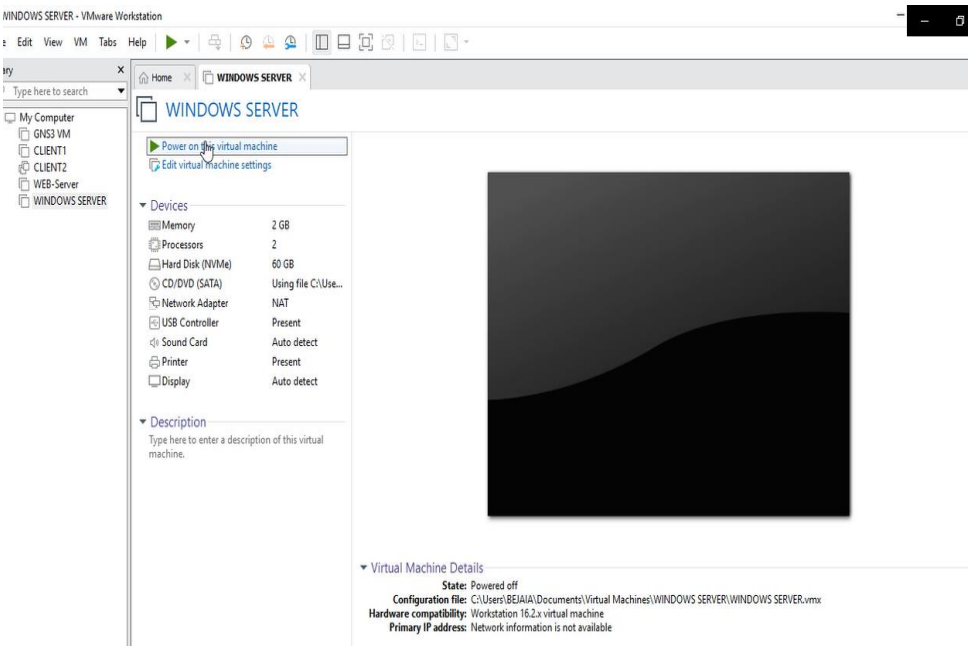

Figure C.2 : l'interface VMware

13/ Cliquez sur "Power on this virtual machine" et il faut appuyer sur une touche pour charger l'assistant Windows Server 2022 :

14/ Cliquez sur Suivant puis sur "Installer maintenant":

15/ Maintenant, nous sélectionnons l'édition à utiliser, celles avec la légende CORE sont développées pour être travaillées dans le terminal :

16/Cliquez sur Suivant et nous acceptons la licence d'utilisation :

17/ Ensuite, nous allons choisir le type d'installation à utiliser :

18/Enfin, nous sélectionnons le disque et lançons le processus d'installation de Windows Server 2022 :

19/ Cliquez sur Suivant pour démarrer l'installation de Windows Server 2022

20/ Cela installera les mises à jour et fonctionnalités disponibles

21/ Le système sera redémarré pour terminer le processus :

22/ Saisissez le mot de passe administrateur et cliquez sur « Terminer » :

23/ Pour accéder à Windows Server, nous allons dans le menu "VM - Send Ctrl + Alt + Del":

24/ Saisissez le mot de passe créé pour accéder au système :

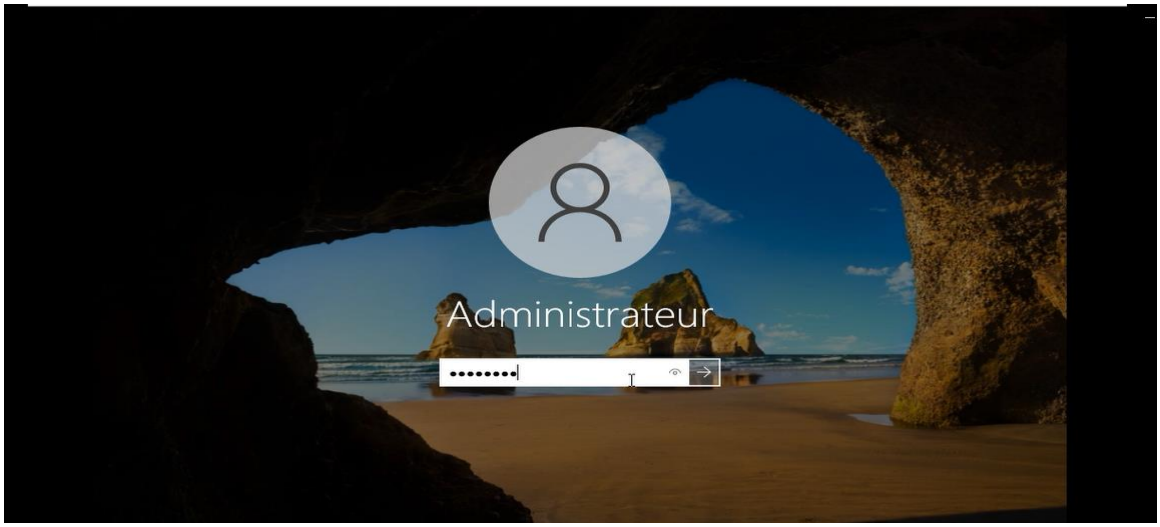

Figure C.3 : l'interface de Windows server

Annexe D

➢ Configuration de base sur le serveur :

Distribuer une adresse IP fixe au serveur :

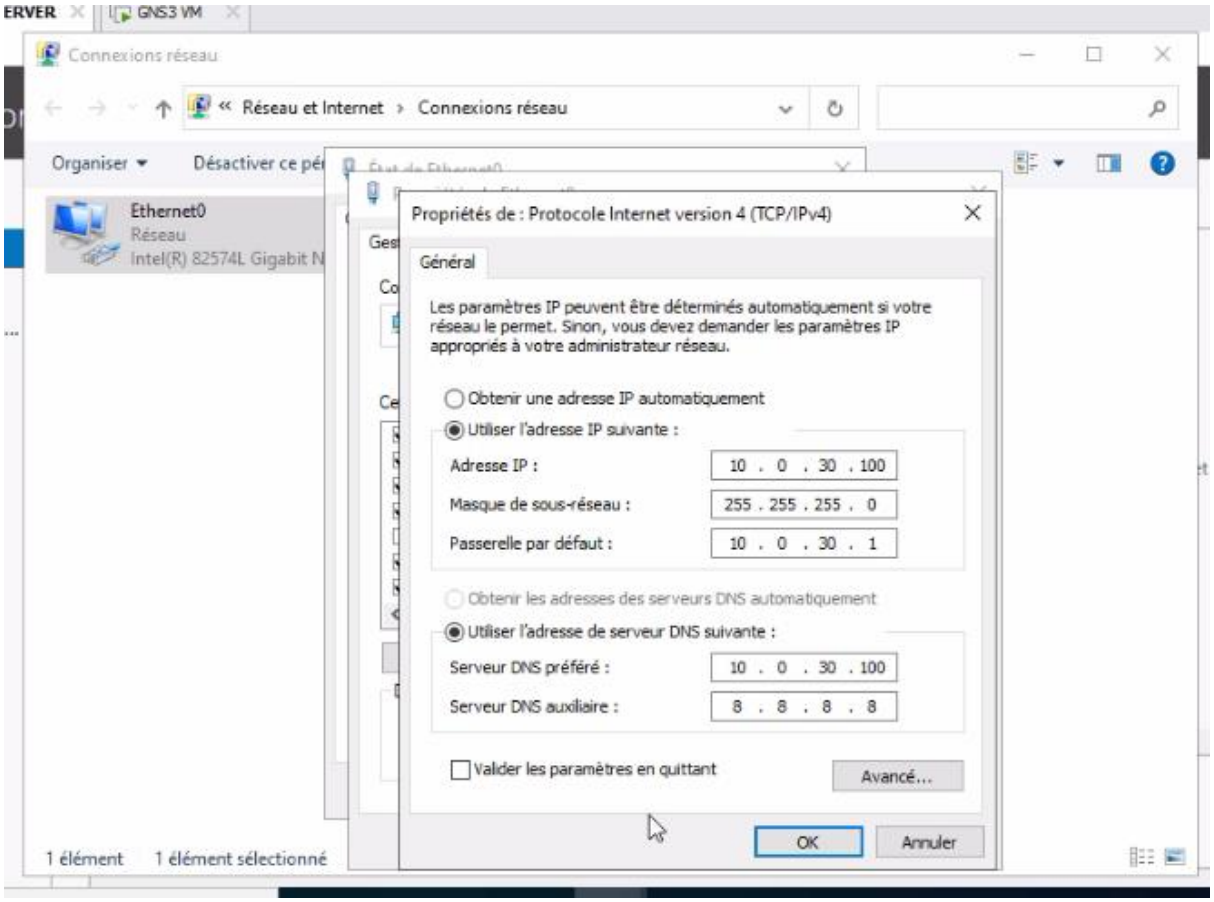

Figure D.1: configuration de serveur.

➢ Installer active directory dans le serveur :

Sur la machine Windows serveur 2022 nous avons installé un contrôleur de domaine dont le nom de domaine est univ-bejaia.local.

Pour commencer l'installation, il va falloir ajouter les rôles de service Active Directory. Lancer l'installation et ajouter les fonctionnalités qui nous manquent.

Voici les étapes d‘installation active directory :

- dans la gestionnaire de serveur on choisit ajouter des rôles et fonctionnalités.
- sélectionné le serveur destination.
- Choisi le rôle active directory.
- Lancer l’installation.

➢ Configuration l’active directory dans le serveur :

Maintenant nous allons commencer la configuration de notre Active Directory. Le domaine créé univ-bejaia.local est notre premier contrôleur de domaine catalogue global activé. Lorsque les services seront installés et configurés, cliquant sur FIN le système devra redémarrer. A la fin de l’installation on aura les trois rôles installés comme le montre la figure D.2.

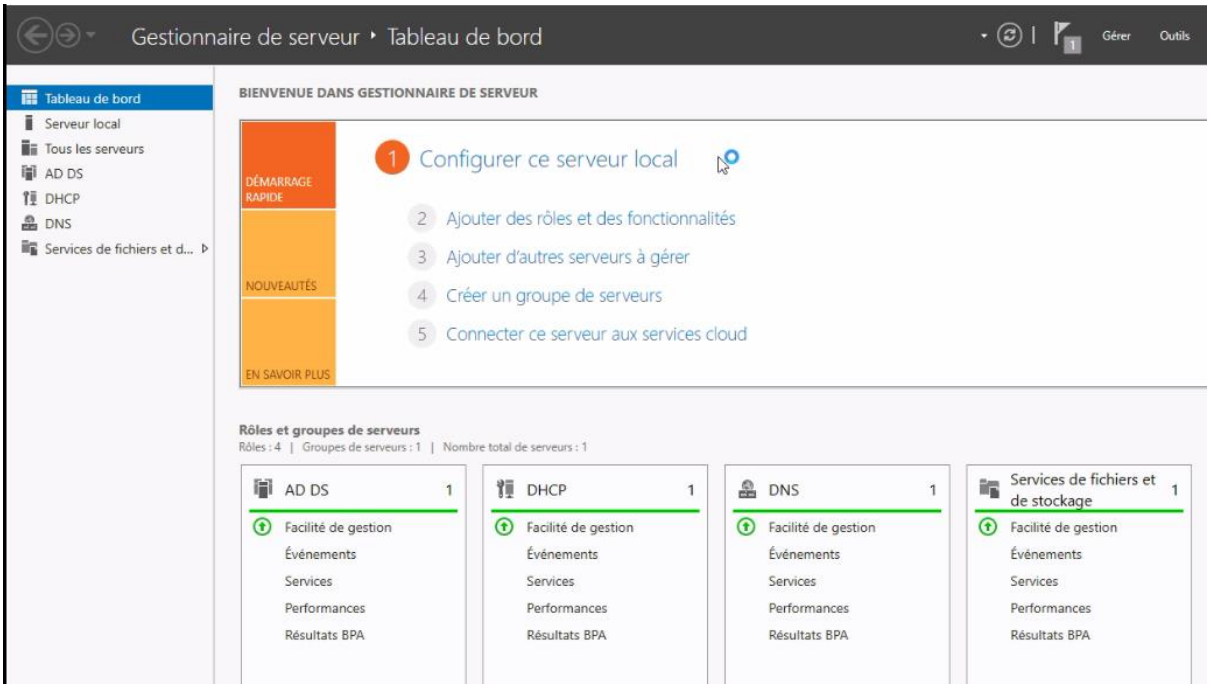

Figure D. 2: Les rôles AD DS et DNS et DHCP.

➢ Configuration de serveur DHCP :

Distribution des adresses de manière dynamique on clique sur ipv4.

Etape1 : créer pour chaque VLAN étendue **:**

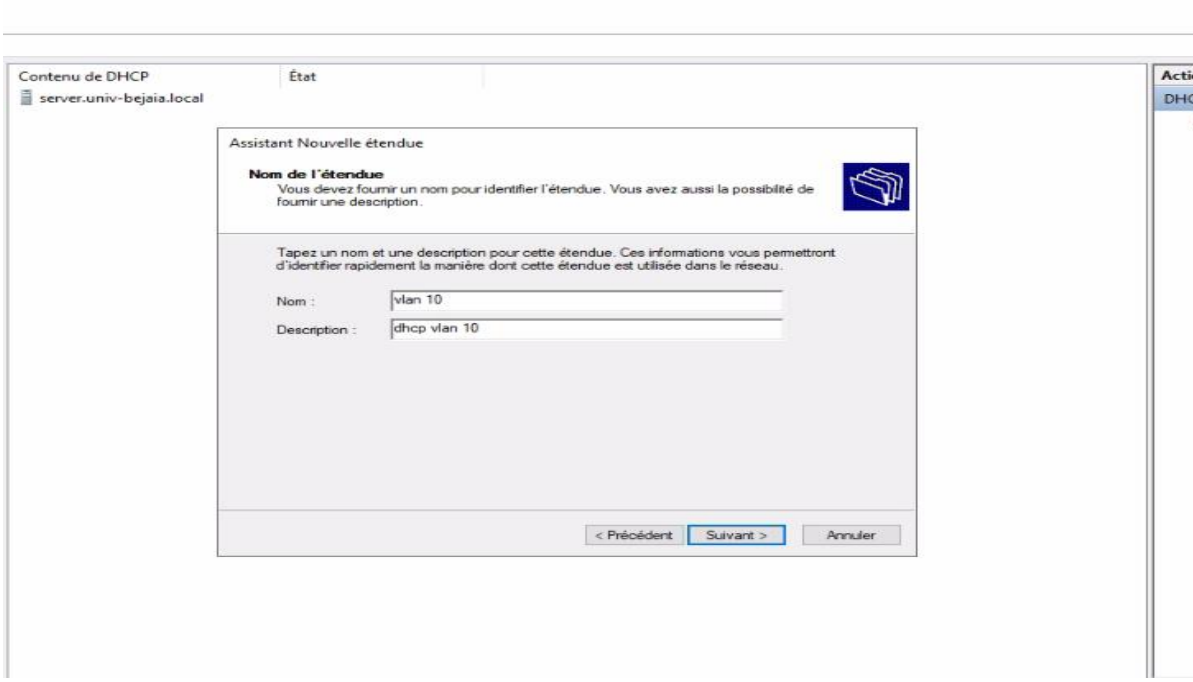

Figure D.3 : Le nom et la description de cheque VLAN.

Etape2 : la distribution des adresses pour les vlans :

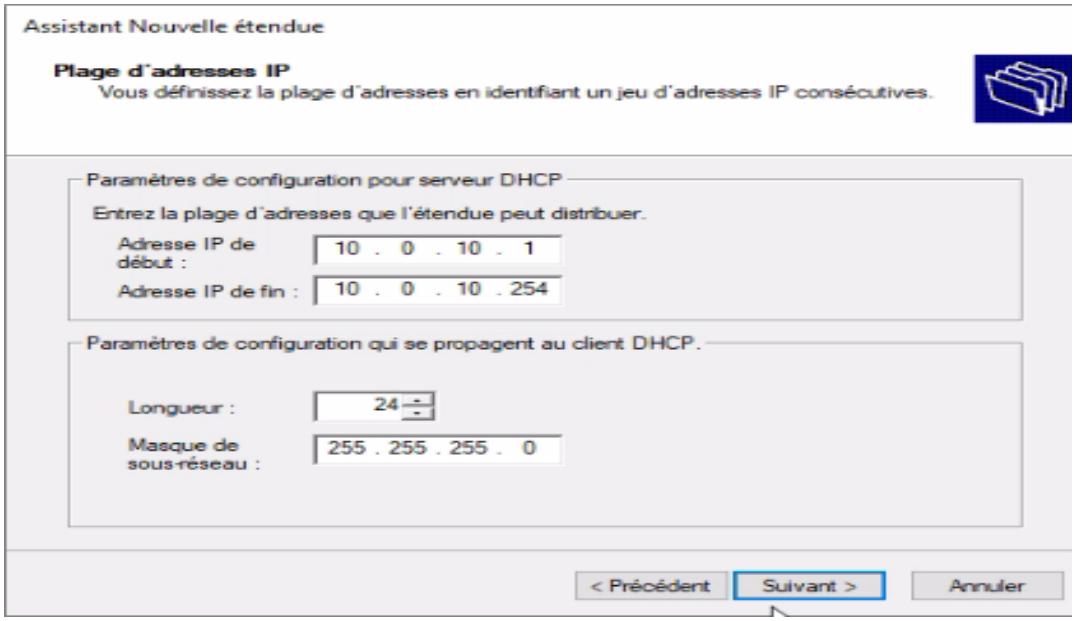

Figure D.4. : paramétrer les adresses des Vlan.

Etape3 : On va exclure les 10 premières adresses :

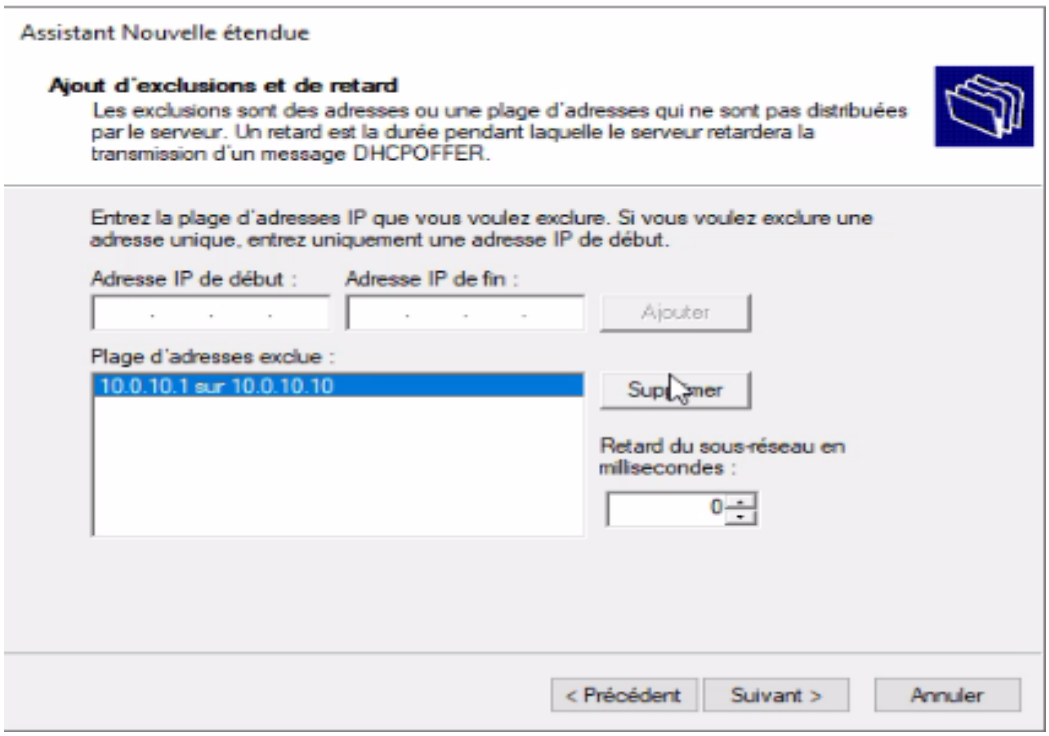

Figure D.5. : Exclusion des 10 premières adresses.

Ensuit on active l'étendu et configurer les options.

- Configurer la passerelle 10.0.10.1.
- Notre non demain c'est univ-bejaia.local.
- 8.8.8.8 pour les connectés sur internet.
- Configurer Un autre NetBOIS c'est serveur WINS avec adresse 10.0.30.100.
  Ses la même chose pour les autre VLAN. Comme ça tous les étendus sont Activer car on configurer tous les VLANs sur le serveur DHCP.

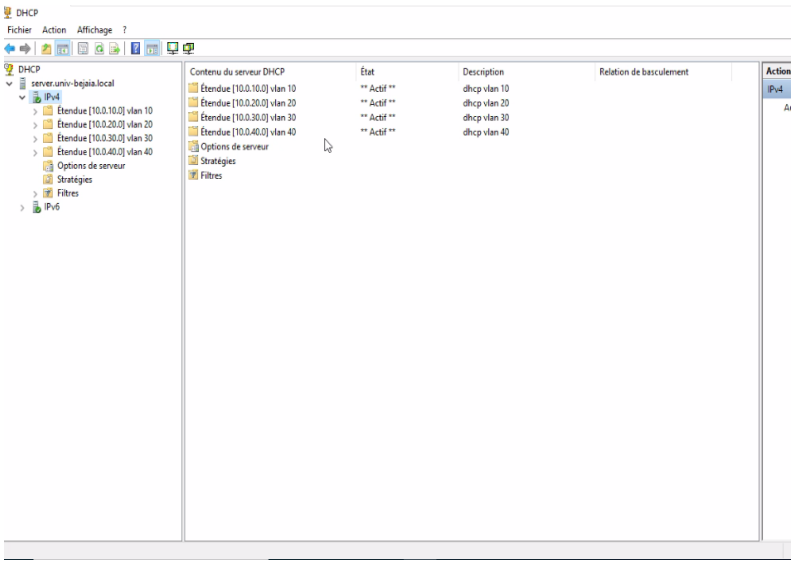

Figure D.6: Les étendus des VLANs configurer.

➢ Configuration le serveur DNS :

Pour que le client, il peut accéder directement au serveur web. Clique sur la zone directe

Etape1 : créer une nouvelle principale son nom c'est univ-bejaia.net.

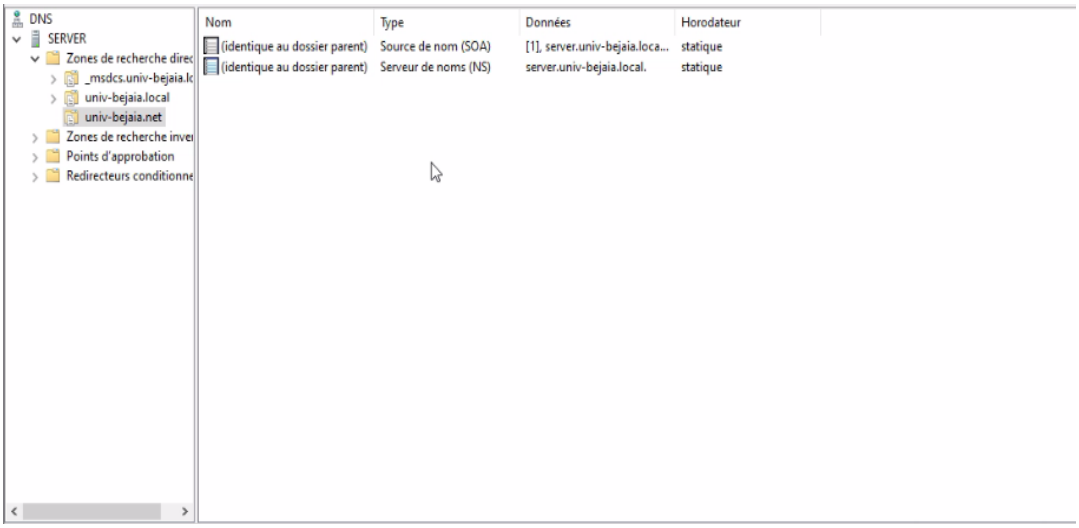

Figure D.7 : Création la zone principale.

Etape2 : création les hôtes :

Avec le nom web et adresse IP 192.168.16.100.

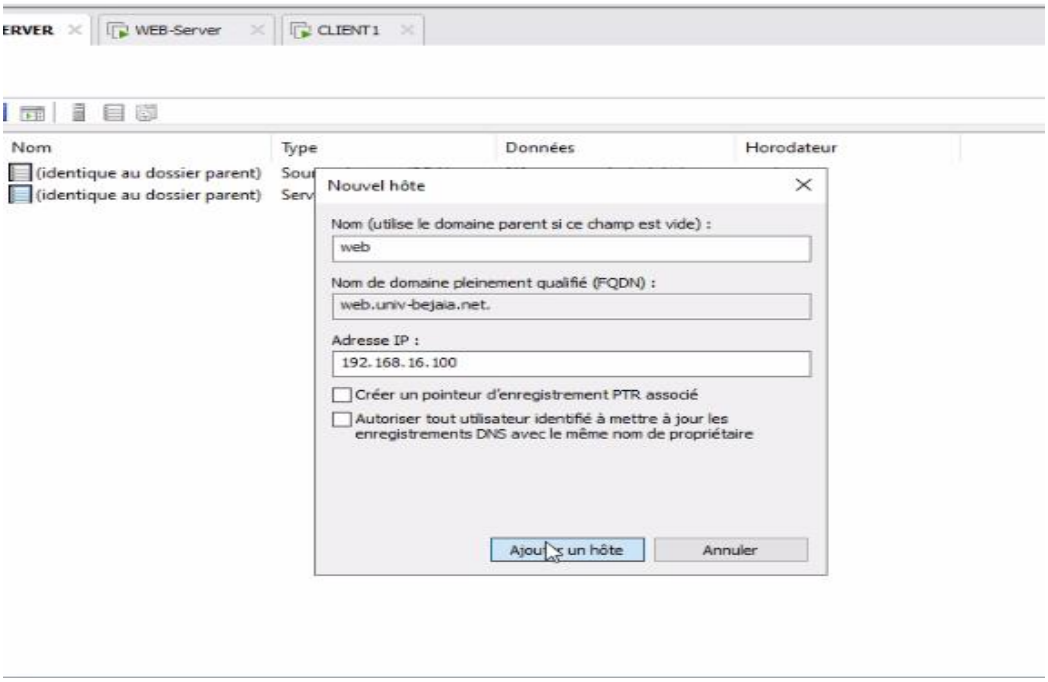

Figure D.8 : Création d'hôte.

Annexe E

➢ Étapes pour installer Windows 10 sur VMware Workstation

1/ Cliquez sur le bouton Fichier>Nouvelle machine virtuelle pour créer une nouvelle machine virtuelle.

2/ Sélectionnez Configuration personnalisée (avancée) et cliquez sur **Suivant.**

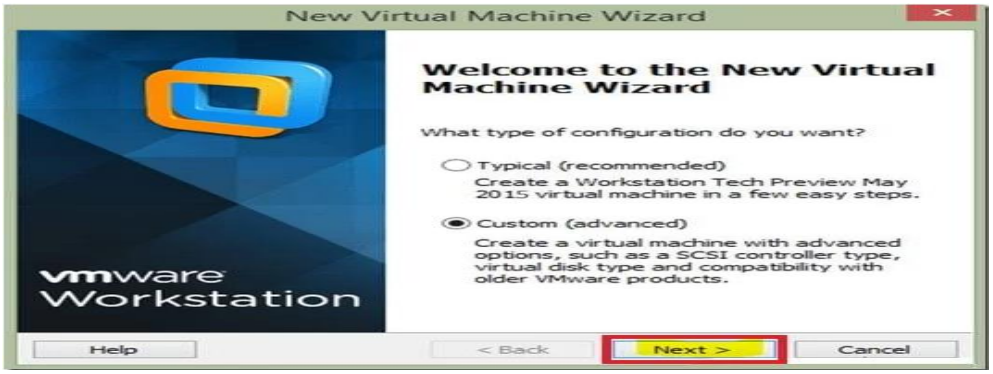

Figure E.1 : **Démarrage d'installation d'une nouvelle machine Virtual**

3/Dans l'assistant Nouvelle machine virtuelle, spécifiez un chemin pour votre fichier ISO Windows 10 et cliquez sur **Suivant.**

4/ Sélectionnez le système d'exploitation invité comme Microsoft Windows.

5/ Choisissez la version du système d'exploitation comme Windows 8 x64 et cliquez sur **Suivant**.

6/ Spécifiez le nom de la machine virtuelle (par exemple : Windows 10) et cliquez sur Suivant.

7/ Spécifiez le nombre de processeurs et le nombre de cœurs par processeur.

8/Ensuite, cliquez sur Suivant.

9/ Maintenant, spécifiez la mémoire de votre machine virtuelle en tant que 2 Go (donnez-la en Mo).

10/ Sélectionnez le type de réseau comme **Traduction d'adresses réseau (NAT)** et cliquez sur Suivant.

11/Spécifiez la capacité du disque de votre machine virtuelle. La taille recommandée pour Windows 8 est de 60 Go

12/ Cliquez sur Terminer et votre machine virtuelle est créée.

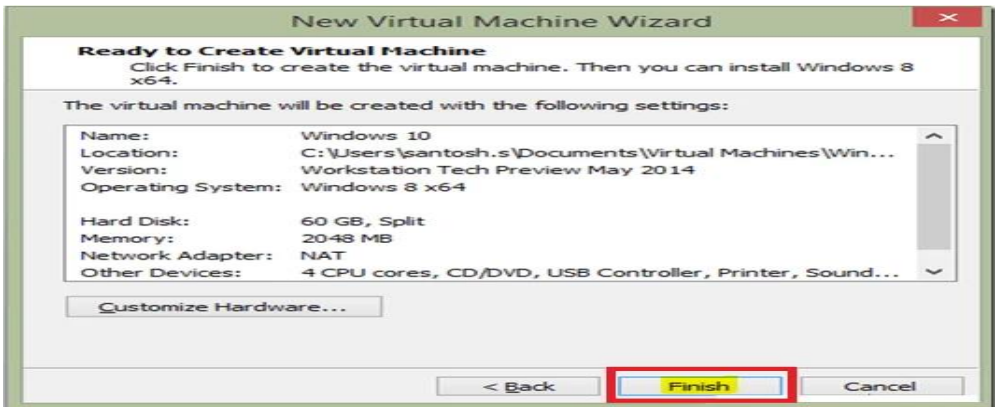

Figure E.2 : fin d'installation d'une nouvelle machine Virtual

13/ Suivez normalement le processus d'installation de Windows 10. Sélectionnez votre langue et la disposition du clavier, puis cliquez sur **Suivant** continuer.

Figure E. 3: démarrage d'installation Windows 10

14/Il suffit de cliquer sur **Installer maintenant** afin de poursuivre le processus d'installation.
15/ Choisissez le type d'installation parmi les deux options comme indiqué dans l'image ci-dessous.

16/La mise à niveau est utilisée pour mettre à niveau votre système Windows 7 ou 8 existant vers le nouveau système d'exploitation Windows 10. Personnalisé vous permet d'installer Windows 10 avec une copie existante de Windows.

17/Cliquez sur Personnaliser : **Installer l'installation Windows uniquement (avancée)** option

18/Allouez de l'espace pour Windows 10 et cliquez sur Suivant.

19/Vous pouvez maintenant exécuter Windows 10 dans VMware Workstation.

20/Maintenant, le processus d'installation démarre pour Windows 10 sur VMware Workstation et il faut un certain temps pour copier et installer la nouvelle version. Un écran de bienvenue s'affiche une fois l'installation terminée.

Figure E.4 : fin d'installation de Windows 10

Annexe F

➢ Les étapes d'installations winscp :

Etape 1 : cliquer sur le bouton 'télécharger WinSCP' pour télécharger le logiciel.

Le téléchargement commence immédiatement**.**

Etape 2 : le fichier est stocké dans téléchargement.

Etape 3 : cliquez sur WinSCP. Cliquer sur 'oui'

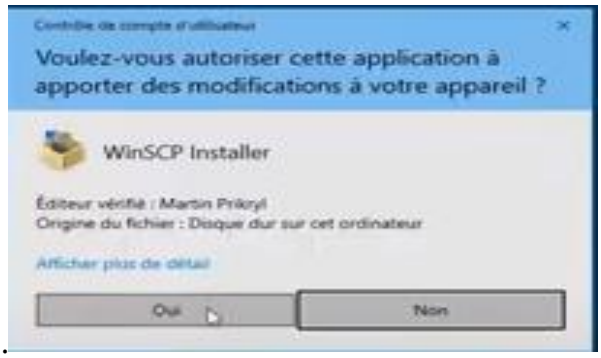

Figure F.1: le fichier WinSCP

Etape 4 : lisez et acceptez l'accord de de licence. Cliquez sur ' Accepter'.

Etape 5 : choisissez la manière d'installation. L'installation typique est (recommandé).

Cliquer sur 'suivant'.

Etape 6 : choisissez la manière d'utilisation.

Etape 7 : cliquer sur 'installer

Etape 8 : commencer l'installation :

Etape 9 : fin d'installation :

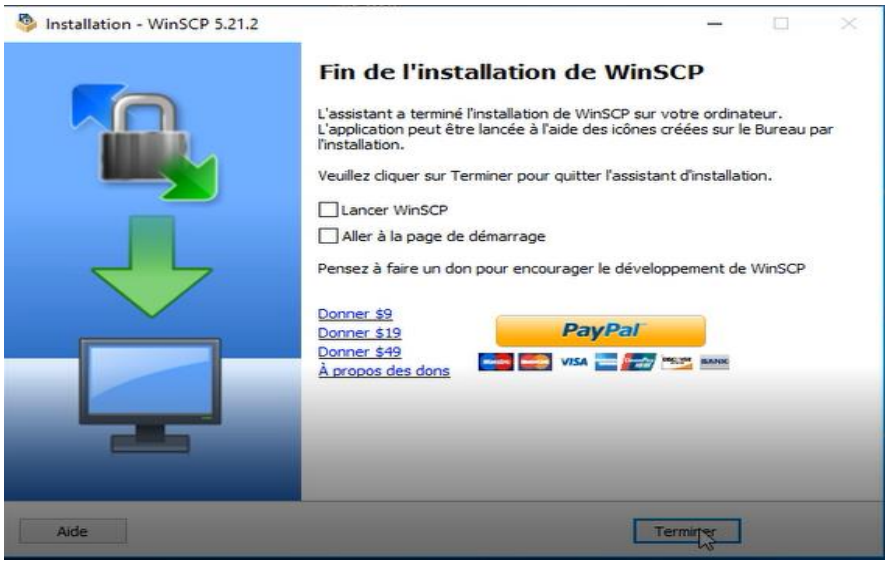

Figure F.2: fin d'installation**.**

Annexe G

➢ Les étapes d'installation putty

1. Double-cliquez sur le **fichier MSI** téléchargé pour lancer l'installation.

2. Cliquez sur' **Suivant'** sur l'écran de bienvenue pour poursuivre l'installation.

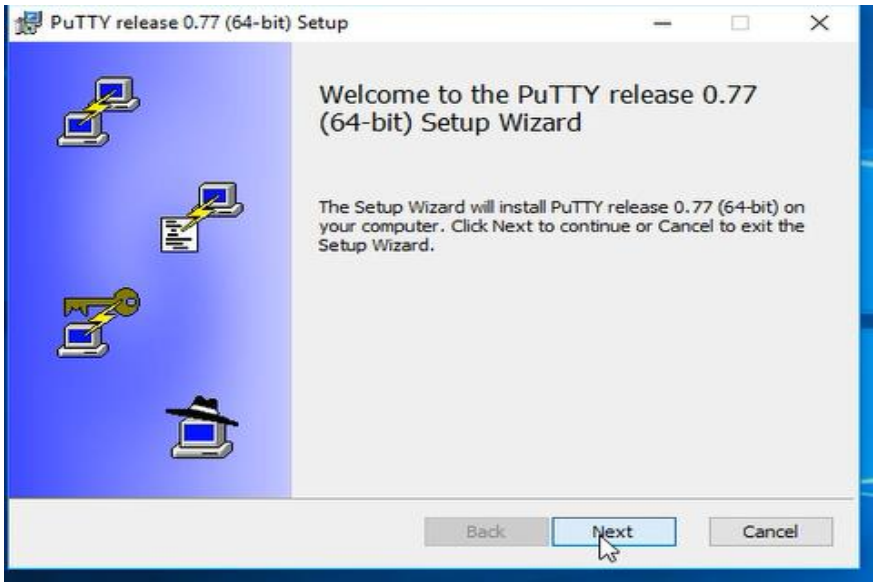

Figure G.1: répertoire putty.

3. Cliquez sur « **Suivant**» si vous n'avez pas besoin de modifier le chemin d'installation.

4. Sélectionnez les fonctionnalités du produit que vous souhaitez installer. Cliquez sur « **Installer** ».

5. Une fois l'installation terminée, le programme affiche un écran « Configuration terminée ». Cochez/décochez l'option « **View README file** »si vous souhaitez voir les notes du développeur. Cliquez sur « finish »pour quitter le programme d'installation.

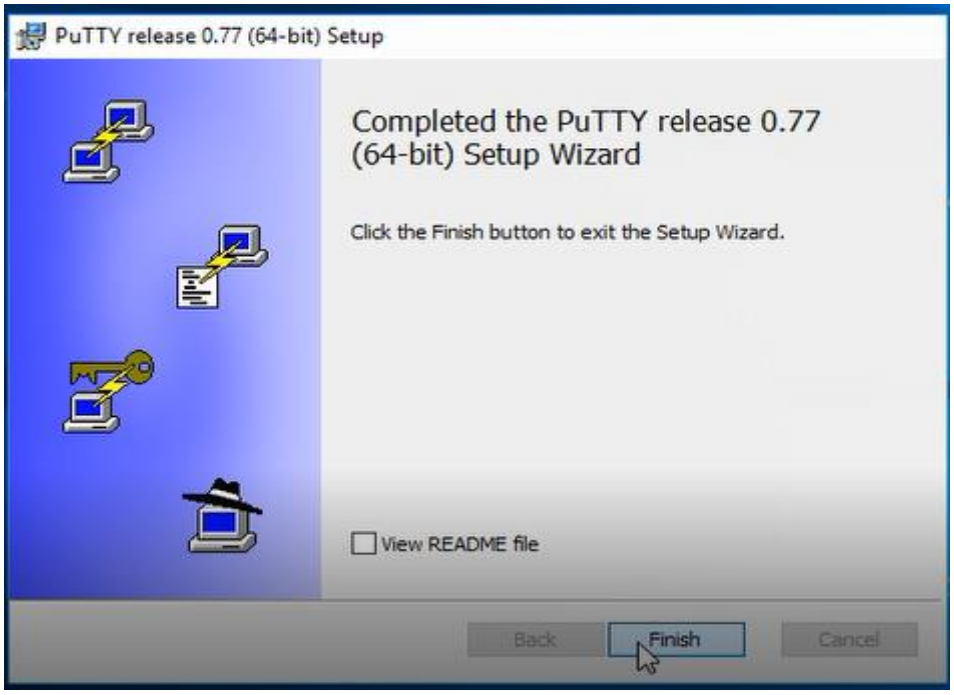

Figure G.2 : fichier putty

Exécutez Putty

- Après l'avoir installé, lancez Putty.
- Dans le champ Host Name (or IP adress) saisissez votre serveur FTP.
- Dans le champ Port saisissez 22 s'il n'est pas déjà rentré.
- Cochez SSH.
- Cliquez sur Open

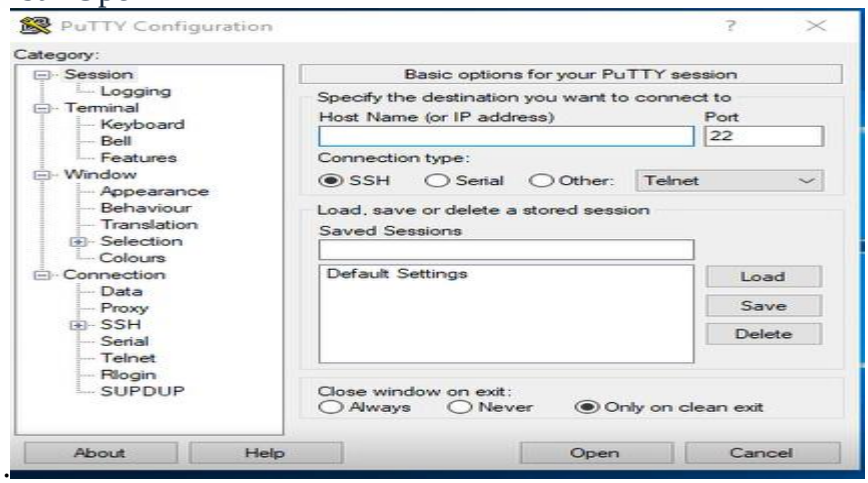

Figure G.3: l'interface de configuration putty

Annexe H

➢ Les étapes Installations firewall :

Pour commencer l'installation de firewall, nous cliquons sur power on this vertual machine

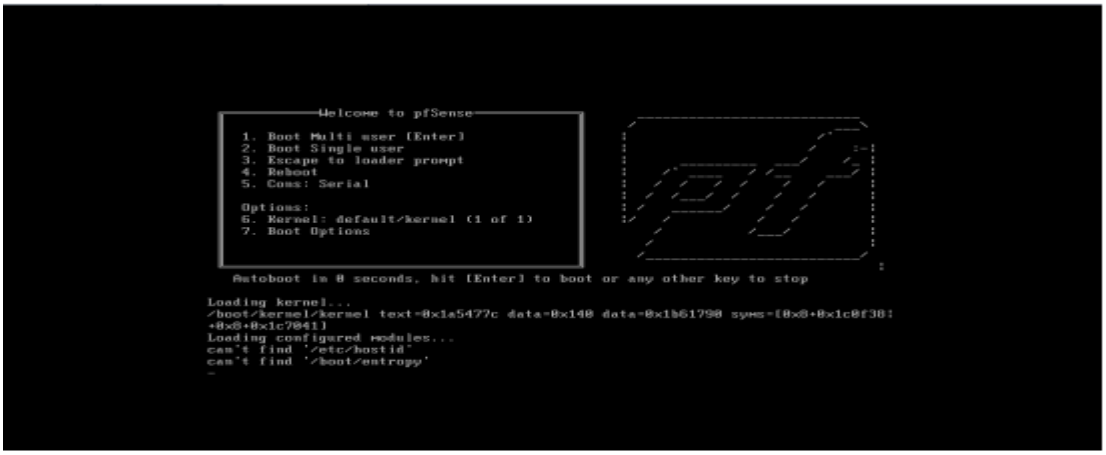

Figure H.1 : Ecran de démarrage de l'installation de firewall.

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

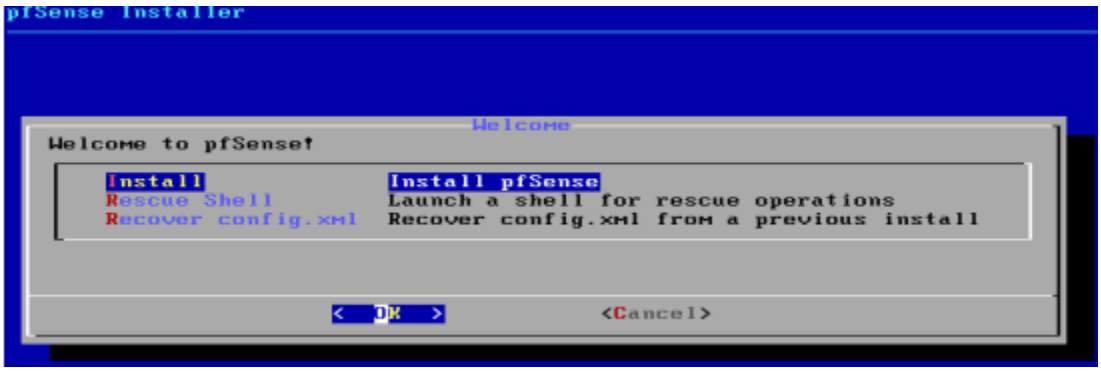

Figure H.2 : Début de l'installation de firewall.

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 (la figure 2).

Figure H.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 :

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] https://www.insee.fr/fr/metadonnees/definition/c1864

[2] https://www.crifa.ulg.ac.be/archives/kitnet/Ressources_eleves/Definition.html

[3 https://www.noodo-wifi.com/faq/difference-entre-intranet-et-extranet/

[4] https://fr.wikipedia.org/wiki/Fichier:Intranet.png

[5] https://fr.vikidia.org/wiki/Fichier:Extranet-intranet.png.

[6] A.SIDER, HOUHA.A Cours Technologie d'internet master2. Université de Bejaia, 2022.

[7] https://www.google.com/search?client=firefox-b-d&q=la+pile+protocolaire+tcp%2Fip

[8] ACISSIé. Sécurité informatique Ethical Hacking apprendre l'attaque pour mieux se défendre [3e édition]. 2012.

[9] https://www.google.com/search?q=architecture+client+%2Fserveur&oq=architecture+client+%2Fserveur&aqs=chrome..69i57j0l7.11901j0j7&sourceid=chrome&ie=UTF-8

[10] nesmas ourdia, zikiou nadia, optimisation et ealisation d'un réseau local sécurisé au seinde l'IAP de boumerdes, 2008/2009

[11] https://www.axido.fr/quels-sont-les-5-criteres-de-la-securite-it/,consulté le 17 juillet 2022.

[12] Jean-François Carpentier, La sécurité informatique dans la petite entreprise Etat de l'art et Bonnes Pratique, Edition ENI, Avril 2009.

[13]:https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_des_syst%C3%A8mes_d%27information,consulté le 19juillet 2022.

[14]: Lourent Bloch-Christophe Wolfhugel, EYROLLES, 2éme édition. 2005.

[15] Imad Bou Akl, Etude des protocoles et infrastructures de sécurité dans les réseaux, Coopération dans les sciences de traitement de l'information, 2005/2006

[16**]** https://www.websecurity.digicert.com, Consulté le 17 juillet 2022.

[17] https://repo.zenk-security.com/Protocoles_reseaux_securisation/Avantages%20et%20faiblesses%20du%20protocole%20SSH.pdf, consulté le 19 juillet 2022.

[18] **:** chenene katia, fedaul saloua, mise en placce d'une politique de sécurité dans un réseau cas d'une banque, l'obtention du diplome de master deux en informatique ,2012/2013.

[19] **:** Mickel Choisnard, Réseaux et Sécurité informatique, Université De Bourgogne, Cours MIGS, novembre 2015, In : https://blog.u-bourgogne.fr/migs/wp

[20] : https://www.futura-sciences.com/tech/definitions/informatique-antivirus-10999/, consulté le 19/07/2022.

[21] : http://n.grassa.free.fr/cours/proxy.pdf, Consulté le 17 juillet 2022.

[22] : http://projet.eu.org/pedago/sin/ISN/8-securite_reseaux.pdf, Consulté le 19 juillet 2022

[23] : Nadjette BEN HAMIDA, « les politiques de gestion du cache d'un serveur web », Université de Bejaia, mémoire de magistère en informatique, 2007.

[24] : http://ensat.ac.ma/Portail/wp-content/uploads/2020/03/Le-protocole-SSL.pdf

[25] **:** https://fr.semrush.com/blog/definition-https/

[26] : https://www.globalsign.com/fr/blog/la-difference-entre-http-et-https

[27] **:** https://arabicprogrammer.com/article/95921766978/, consulté le 28/08/2022.

[28] **:** https://www.globalsign.com/fr/blog/difference-entre-ssl-et-tls#:~:text=Initialement%20d%C3%A9velopp%C3%A9%20par%20Netscape%2C%20le,libell%C3%A9es%20ainsi%20%3A%20SSLv2%20et%20SSLv3.

[29] **:** https://arabicprogrammer.com/article/6179754922/, consulté le 28/08/2022.

[30] **:** https://www.frameip.com/ssl-tls/, consulté le 28/08/2022.

[31] : https://www.cloudflare.com/fr-fr/learning/ssl/what-is-asymmetric-encryption/

[32] **:** Nadia.Battat, Les systèmes de sécurité, master2. Université de Bejaia, 2022.

[33] **:** https://www.cgi.com/sites/default/files/white-papers/cgi_whpr_35_pki_f.pdf.

[34] **:** https://www.globalsign.com/fr/centre-information-ssl/definition-certificat-ssl

[35] **:** https://www.frameip.com/ssl-tls/, consulté le 28/08/2022.

[36] **:** https://www.frameip.com/ssl-tls/, consulté le 28/08/2022.

[37] **:** https://www.securiteinfo.com/cryptographie/ssl.shtml,consulté le 28/08/2022.

[38] **:** https://www.kaspersky.fr/resource-center/definitions/encryption,consulté le 28/08/2022.

[39] : Brono favre, Guide pratique de sécurité informatique mis en œuvre sous Windows et linux, peirre-alian Goupille, 2010.

[40] : univ-bejaia.dz.

[41]
https://www.google.com/search?q=GNS3+d%C3%A9finition&oq=gns&aqs=chrome.1.69i59l3j69i57j69i59j69i60.5189j0j7&sourceid=chrome&ie=UTF-8.

[42] : https://www.clubic.com/telecharger-fiche431147-windows-10.html.

[43] :https://www.google.com/search?q=equipement+(hard+et+soft)&oq=equipement+&aqs=chrome.1.69i59l2j69i57.6992j0j7&sourceid=chrome&ie=UTF-8.

[44] file:///C:/Users/PC%20MC/Downloads/Support%20%20de%20Cours_r%C3%A9seau_Fst_Chp3.pdf.

[45] https://www.syloe.com/glossaire/serveur-informatique/

Résumé :

Le web est le service internet le plus répandu dans le monde entier, il est utilisable par tous les domaines. Un serveur web est un simple ordinateur capable de gérer les entrées sorties fait par les internautes qui se sert de sa base de données, et qui interprète les requêtes http. Il permet également d'héberger un ou plusieurs sites. Grâce à des logiciels, il permet au client d'avoir les fichiers qu'il demande. Il existe plusieurs types de serveurs et il est important de tenir compte de certains critères pour choisir celui qui vous convient le mieux. Par ailleurs, des individus malintentionnés peuvent s'en prendre à votre serveur web.

Notre projet de fin d'études sera axé sur la sécurisation d'un serveur web sous linux. Pour cela, on a installé un serveur Apache, le certificat crs (auto-signé) et les protocoles SSH, SSL.

Mot-clé : WEB, Internet, Linux, HTTP, Serveur, SHH, SLL.

Abstract

The web is the most common Internet service worldwide, it is used in all areas and especially for sharing and information.

A web server is a simple computer that can handle inputs outputs made by net surfers that uses its database and interprets HTTP requests. It also allows you to host one or more sites. Thanks to software, it allows the customer to have the files he requests. There are several types of servers and it is important to take into account certain criteria to choose the one that suits you best. In addition, malicious individuals can attack your web server.

Our graduation project will focus on security a web server on Linux .For this, we installed an Apache server, self-signed certificate and SSH and SSL protocols.

Keyword: WEB, Internet, Linux, HTTP, Server, SHH, SLL.