الجمهورية الجزائرية الديمقراطية الشعبية

République Algérienne démocratique et populaire

وزارة التعليم العالي والبحث العلمي

Ministère de l'enseignement supérieur et de la recherche scientifique

جامعة سعد دحلب البليدة

Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا

Faculté de Technologie

قسم إلكترونيك

Département d'Électronique

Mémoire de Master

En Télécommunication

Spécialité : Réseaux & Télécommunications

Présenté par

SAIDANI YAMINA

&

ZERKOUK NARIMANE

Mise en place d'une maquette HOTSPOT Wi-Fi au niveau de l'université de Blida 1 pour une connectivité efficace et sécurisée

Proposé et Encadré par :

Mr. Zerkouk Ahmed & Mr. Hebib Sami

Année Universitaire 2022-2023

Remerciements

Nous tenons à remercier "ALLAH" le tout puissant de nous avoir accordé la santé, le courage ainsi que la volonté d'entamer et de terminer notre projet de fin d'étude.

Nous remercions très chaleureusement nos promoteurs Mr. Zerkouk Ahmed, Mr. Mechakra Abdel Rachid et Mr. Hebib Sami pour avoir dirigé nos travaux. Merci pour vos échanges scientifiques vos conseils et votre rigueur.

Nous tenons à exprimer notre profonde gratitude à tous les enseignants de la spécialité réseaux et télécommunications en générale.

Nous voudrions aussi remercier toute l'équipe de ICOSNET qui nous ont apporté leur soutien au long de ce projet de fin d'étude.

Nous remercions également tous les membres du jury pour nous avoir honorées par leur présence et pour avoir accepté d'évaluer ce travail de mémoire.

Nous tenons aussi à remercier nos parents respectifs, nos frères et sœurs sans oublier nos amis.

Enfin, nous remercions tous ceux qui ont participé de près ou de loin à l'achèvement de ce travail

Dédicace

A ma chère mère,

A mon cher père,

Qui n'ont jamais cessé, de formuler des prières à mon égard, de me soutenir

Et de m'épauler pour que je puisse atteindre mes objectifs.

A mes chers frères,

A mes chères sœurs,

Pour ses soutiens moraux et leurs conseils précieux tout au long de mes études.

A ma chère grand-mère,

Qui je souhaite une bonne santé.

A ma famille,

A mon cher binôme,

A tous mes proches,

A tous mes collègues,

A tous mes amis,

A tous ceux qui m'aiment,

A tous ceux que j'aime.

Je dédie ce mémoire.

Saidani Yamina

Dédicace

Je dédie ce travail à mes proches qui ont joué un rôle important dans ma réussite académique :

À mon père, Abderrahmane, tu es mon modèle éternel, mon soutien moral et ma source de joie. Tes sacrifices pour me voir réussir resteront gravés dans mon cœur. Que Dieu te garde pour nous.

À ma mère, Amina, tu es la lumière de ma vie. Ton dévouement et ton amour indéfectible ont été mes sources d'inspiration et de motivation. Je t'adore de tout mon être.

À ma chère grand-mère,Fatma, tu incarnes l'amour, la sagesse et le réconfort. Ta force et ta résilience m'ont inspirée tout au long de mon parcours. Je suis honorée d'être liée à toi.

À mes chères tantes, Wahiba, Razika, Nadira et Lila, votre soutien et vos conseils ont été d'une valeur inestimable pour moi. Votre présence bienveillante a été un véritable soutien tout au long de mes études.

À mon mari, Mehdi, tu es mon roc, mon soutien constant et ma motivation. Ton soutien m'a permis de persévérer et de réussir mes études. Je te remercie du fond du cœur.

À ma sœur, Manar, et mes frères, Abdellah et Adnan, vous êtes mes complices, mes alliés et mes sources d'inspiration. Votre amour et votre soutien m'ont encouragée à donner le meilleur de moi-même.

À Monsieur Rachid et à mon binôme Yamina, merci à vous pour votre précieuse collaboration.

Zerkouk Narimane

ملخص: HOTSPOTهي نقطة وصول لاسلكية تتيح للمستخدمين الاتصال بالإنترنت من أجهزتهم المحمولة عبر تقنية Wi-Fi، وتوفر اتصالاً ملائمًا بالإنترنت في الأماكن العامة، مما يسمح للمستخدمين بالبقاء على اتصال والوصول إلى الخدمات عبر الإنترنت. الهدف الرئيسي من عملنا هو توفير ميزات إدارة وإدارة الوصول إلى الإنترنت المركزية لمؤسسة ICOSNET، مثل إدارة المستخدم والتتبع والمراقبة والفوترة وتخصيص الشبكة. من HOTSPOTS. بفضل حل HSNM، تمكنا من تنفيذ جميع الوظائف المذكورة سابقًا. كتطبيق لهذا المشروع، أجرينا سيناريوهات اختبار في جامعة البليدة 1 من أجل التحقق من صحة الحل المقترح.

كلمات المفاتيح: هوت سبوت; ICOSNET; Wi-Fi; HSNM ; جامعة البليدة 1; سيناريوهات الاختبار

Résumé : Un HOTSPOT est un endroit qui permet aux utilisateurs de se connecter à Internet à partir de leurs appareils mobiles via la technologie Wi-Fi. Il offre une connectivité Internet pratique dans des lieux publics, permettant aux utilisateurs de rester connectés et d'accéder aux services en ligne. L'objectif principal de notre travail est de fournir une gestion d'accès Internet centralisée et des fonctionnalités d'administration pour l'entreprise ICOSNET, tel que la gestion des utilisateurs, le suivi et la surveillance, la facturation et de la personnalisation du réseau de HOTSPOTS. Grâce à la solution HSNM, nous avons pu mettre en œuvre toutes les fonctionnalités mentionnées précédemment. Comme application de ce projet, nous avons conduit des scénarios de tests au niveau de l'université de Blida 1 afin de valider la solution proposée.

Mots clés : HOTSPOT ; HSNM ; Wi-Fi ; ICOSNET ; scénarios de tests ; université de Blida 1

Abstract: A HOTSPOT is a wireless access point that allows users to connect to the Internet from their mobile devices using Wi-Fi technology. It provides convenient Internet connectivity in public places, enabling users to stay connected and access online services. The main objective of our work is to provide centralized Internet access management and administrative features for the company ICOSNET, such as user management, tracking and monitoring, billing, and customization of the HOTSPOT network. Thanks to the HSNM solution, we were able to implement all the aforementioned features. As part of this project, we conducted test scenarios at Blida 1 University to validate the proposed solution.

Keywords: HOTSPOT; HSNM; Wi-Fi; ICOSNET; scenarios; University of Blida 1

Listes des acronymes et abréviations

ADSL : Asymmetrica **D**igital Subsidier **L**ine

AP: Access **P**oint

BLR: Boucle **L**ocale **R**adio

BSS: Basic **S**ervice **S**et

BSA: Base **S**tation **A**rea

CSS: **C**ascading **S**tyle **S**heets

DSSS: Direct **S**equence **S**pread **S**pectrum

ESXI: Eleastic **S**ky **I**ntegrated

FAI : Fournisseur d'**A**ccès **I**nternet

FHSS: Frequency **H**opping **S**pread **S**pectrum

HGW: Home **G**ateway

HTML: Hypertext **M**arkup **L**anguage

HTTP: Hypertext **T**ransfer **P**rotocol

HTTPS: Hypertext **T**ransfer **P**rotocol **S**ecure

HSNM: Hotspot **N**etwork **M**anagement **S**ystem

HTML: Hypertext **M**arkup **L**anguage

IBSS: Independent **B**asic **S**ervice **S**et&

IEEE: Institute of **E**lectrical and **E**lectronics **E**ngineers

IR : Infra Rouge

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

ISM: Industrial **S**cientific and **M**edical

ISP: Internet **S**ervice **P**rovider

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

OVA: Open **V**irtualization **F**ormat

PDA: Personal **D**igital **A**ssistant

PME/PMI : Petite ou **M**oyenne **E**ntreprise

RLC : **R**adio **R**essources **C**ontrol

SMS: **S**hort **M**essage **S**ervice

SSL: **S**ecure **S**ocket **L**ayer

VOIP: **V**oice **o**ver **I**nternet **P**rotocol

VM: **V**irtual **M**achine

VMDK: **V**irtual **M**achine **D**isk.

VLAN: **V**irtual **L**ocal **A**rea **N**etwork

WAN: **W**ireless **A**rea **N**etwork

WLAN: **W**ireless **L**ocal **A**rea **N**etwork

WiMAX: **W**orldwide **I**nteroperability for **M**icrowave **A**ccess

Wi-Fi: **W**ireless **F**idelity

WMAN: **W**ireless **M**etropolitan **A**rea **N**etwork

WPAN: **W**ireless **P**ersonal **A**rea **N**etwork

WPA2: **W**i-Fi **P**rotected **A**ccess 2

WWAN: **W**ireless **W**ide **A**rea **N**etwork

xDSL: **D**igital **S**ubscriber **L**ine

Table des matières

Liste des figures

Liste des tableaux

Introduction générale

Dans le cadre des réseaux sans fil, les HOTSPOTS jouent un rôle important en offrant une connectivité Internet sans fil, exploitant la technologie des réseaux sans fil pour créer des points d'accès pratiques où les utilisateurs peuvent se connecter et profiter d'Internet sans contraintes filaires.

Les HOTSPOT se sont rapidement développés à l'échelle mondiale mais ce n'est pas le cas de l'Algérie. Ces HOTSPOT permettant ainsi à des utilisateurs mobiles disposant d'équipements adaptés (ordinateurs ou téléphones portables compatibles, PDA et autres) de se connecter à Internet de partout avec beaucoup de simplicité. Si ces connexions Internet sont ouvertes au grand public, cela ne veut pas dire qu'il n'existe aucune protection à l'accès et pour les utilisateurs. Nous savons bien qu'une fois connectés sur un même réseau, les utilisateurs deviennent potentiellement vulnérables. La première des protections qui a été mise en place au sein des HOTSPOT est le portail captif avec une authentification par fichier local ou bien un serveur à distance.

ICOSNET, un fournisseur d'accès Internet (FAI) spécialisé dans les services aux entreprises, envisage une stratégie de diversification afin de s'implanter sur le marché grand public. Étant donné que le cahier des charges pour l'ouverture de la boucle locale nécessaire pour proposer des offres xDSL et FTTX n'est pas encore disponible, l'entreprise explore une alternative viable : le déploiement de HOTSPOTS Wi-Fi pour répondre aux besoins des différents clients. Le but de ce projet est de développer une maquette de HOTSPOT Wi-Fi basée sur la solution HSNM à destination de l'université Blida 1.

Ce mémoire est composé d'une introduction, de cinq chapitres et d'une conclusion. Les contenus des chapitres sont donnés comme suit.

Le premier chapitre présente un aperçu des concepts clés des réseaux sans fil tel que les différents types de réseau sans fil, les normes du Wi-Fi, les fréquences utilisées, le mode de fonctionnement et les avantages ainsi que le problème associé à la technologie wifi

Le deuxième chapitre porte sur les HOTSPOTS, en étudiant leurs concepts généraux, les règles essentielles et les risques associés à leur utilisation. Ensuite, nous analysons en détail le fonctionnement des HOTSPOTS et le processus d'authentification via un portail captif. Nous présentons également différentes solutions open source pour la gestion des HOTSPOTS. Par la suite, nous mettons en avant l'entreprise ICOSNET, qui nous a recommandé spécifiquement d'adopter la solution HSNM. Enfin, nous détaillons les caractéristiques de cette solution.

Le troisième chapitre est divisé en deux parties distinctes. La première partie aborde les notions essentielles de la virtualisation. La deuxième partie décrit en détail les étapes nécessaires pour installer la machine virtuelle HSNM sur l'hyperviseur VMWARE ESXi

Le quatrième chapitre est dédié à l'implémentation de la solution HSNM. Cela a impliqué la configuration de la plateforme HSNM, suivie de la configuration de la Gateway MIKROTIK et enfin la configuration du point d'accès.

Le cinquième et dernier chapitre est consacré à la validation du fonctionnement de notre projet et à la présentation des résultats finaux.

Chapitre I : Introduction aux communications sans fil

I.1 Introduction

Depuis leur émergence dans les années 1990, les réseaux locaux sans fil ont connu un succès mitigé en raison du grand nombre de solutions propriétaires offrant des vitesses de transmission faibles. Cependant, après la standardisation de l'IEEE 802.11 en 1997 et surtout l'approbation de l'amendement 802.11b en 1999, qui a augmenté la vitesse maximale de transmission à 11 Mbits/s par rapport aux 2 Mbits/s précédents, ces réseaux ont commencé à connaître un succès durable [1].

Un réseau sans fil est un réseau dans lequel au moins deux appareils peuvent communiquer sans avoir besoin de câbles. Grâce à ces réseaux, les utilisateurs peuvent rester connectés tout en se déplaçant dans une zone géographique plus ou moins étendue, d'où le terme de "mobilité" souvent utilisé. Les réseaux sans fil utilisent des ondes radioélectriques plutôt que des câbles traditionnels. Différentes technologies existent, se distinguant par la fréquence d'émission, le débit et la portée des transmissions [1].

Dans ce chapitre, nous mettons en avant la communication sans fil, en particulier la technologie Wi-Fi (802.11), ainsi que les diverses bandes de fréquences utilisées dans les réseaux Wi-Fi. Enfin, nous examinons les problèmes spécifiques aux réseaux sans fil basés sur la norme IEEE 802.11.

I.2 Les réseaux sans fil

I.2.1 Définition d’un réseau sans fil

D’une manière générale, le terme communications sans fil (réseaux sans fil) fait référence à des communications mettant en jeu des signaux infrarouges ou radiofréquences permettant le partage d’informations et de ressources entre les déférentes entités d’un réseau. Ces entités sont de nos jours de déférents types (PDAs, capteurs sans fil, récepteurs satellitaires, terminaux mobiles, etc[2].. La figure I.1 représente la structure d’un réseau sans fil par rapport à un réseau câblé

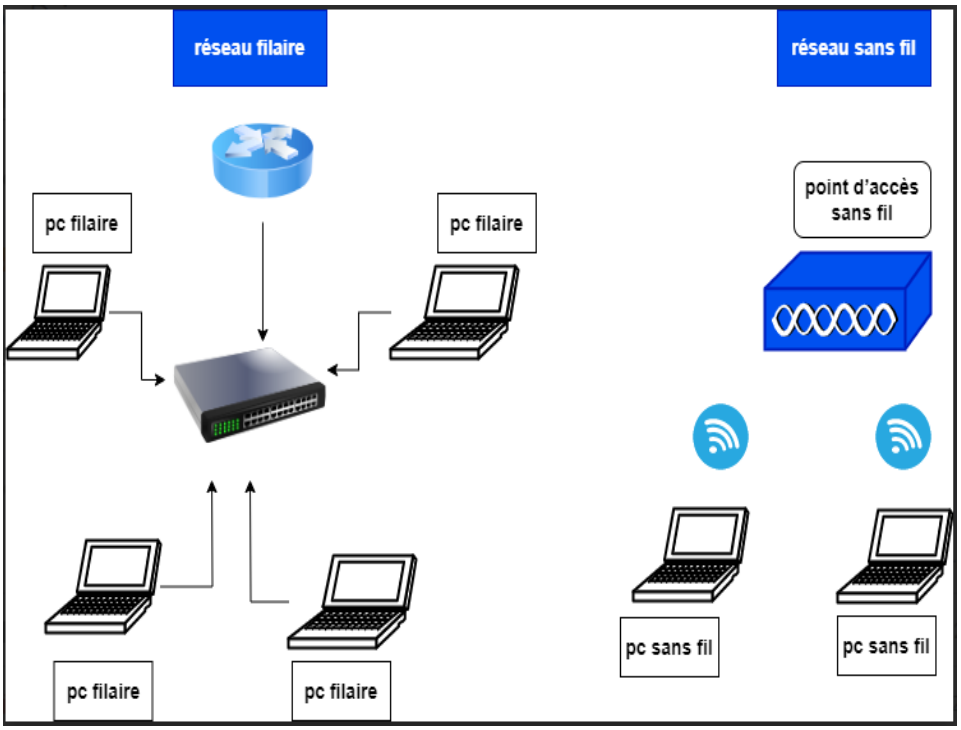


Figure I.2 : Réseau câblé associé à un réseau sans fil.

I.2.2. Caractéristiques des réseaux sans fil

Du fait de la nature du canal de transmission, les réseaux sans fil se distinguent des réseaux filaires par les propriétés suivantes[3].

- Mobilité : Les dispositifs connectés à un réseau sans fil peuvent se déplacer librement dans la zone de couverture du réseau, sans perdre leur connexion. Cela offre une flexibilité significative par rapport aux réseaux filaires, qui sont généralement limités par la longueur des câbles.

- Facilité d'installation : Les réseaux sans fil ne nécessitent pas de câblage complexe pour connecter les périphériques. Cela simplifie l'installation et permet une mise en place rapide du réseau.

- Extensibilité : Il est relativement facile d'ajouter des nouveaux dispositifs à un réseau sans fil existant. Il suffit généralement de configurer les nouveaux appareils pour se connecter au réseau sans fil existant, sans avoir à installer de nouveaux câbles physiques.

I.3 Classification des réseaux sans fils

Une première distinction entre les réseaux sans fils dépend de leur champ d'action. Suivant leur portée, selon le périmètre géographique offrant une connectivité (appelé zone de couverture) comme le montre la figure I.3.

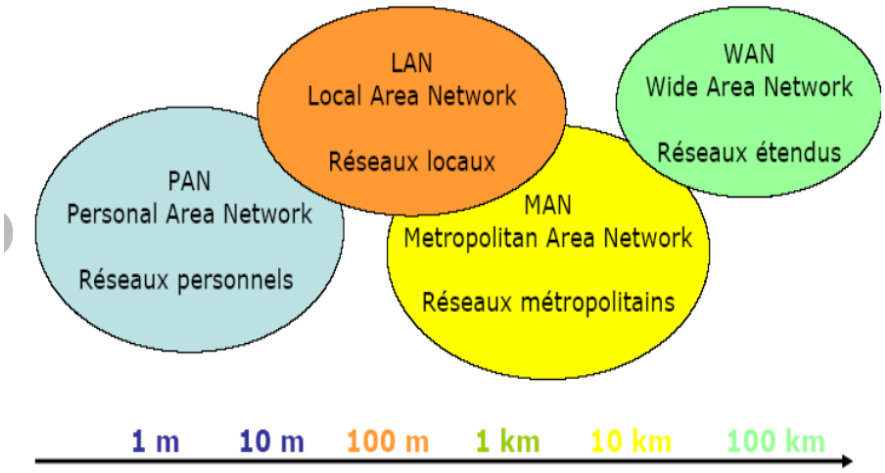


Figure I.4: Classification des réseaux sans fils selon l'étendue géographique[4].

- **Les réseaux personnels sans fil (WPAN)**

Appelé aussi réseaux domestique, Ils assurent l'interconnexion entre des terminaux distants à quelques dizaines de mètres, c'est des réseaux à faible portée. Ils servent généralement à relier des périphériques (PC, Imprimante…etc.) ou un assistant personnel (PDA) à un ordinateur sans liaison filaire[5].

- **Les réseaux locaux sans fil (WLAN)**

Correspond au périmètre d'un réseau local installé dans une entreprise, un foyer ou encore dans les espaces publics (HOTSPOT). Tous les terminaux (PC, assistant PDA…etc.) situés dans la zone de couverture du WLAN peuvent s'y connecter[5].

- **Réseaux métropolitains sans fils (WMAN)**

Le réseau métropolitain sans fils (WMAN pour Wireless Métropolitain Area Network) est Connu sous le nom de Boucle Locale Radio (BLR). Les WMAN sont basés sur la norme IEEE 802.16. La boucle locale radio offre un débit utile de 1 à 10 Mbit/s pour une portée de 4 à 10 kilomètres, ce qui destine principalement cette technologie aux opérateurs de télécommunication. Et ce sont des réseaux qui couvrent partiellement ou totalement la superficie d'une ville[5].

- **Réseaux étendus sans fil (WWAN)**

Le réseau étendu sans fils (WWAN pour Wireless Wide Area Network) Est également connu sous le nom de réseau cellulaire mobile, il s'agit des réseaux sans fil les plus répondu, puisque tous les téléphones mobiles sont connectés à un WWAN[5].

Le tableau I.2 récapitule les différentes catégories des réseaux sans fil.

Catégorie	Description	Bande de Fréquence	Débit Maximal	Portée
WPAN (Personal Area Network)	Réseaux de proximité des communications entre appareils personnels.	2 ,4 GHz, 5 GHz	Jusqu'à 3 Mbps	Quelques mètres
WLAN (Local Area Network)	Réseaux locaux pour des zones telles que bâtiments, campus ou HOTSPOT public.	2 ,4 GHz, 5 GHz	Jusqu'à 10 Gbps	Jusqu'à 100 mètres
WMAN (Métropolitain Area Network)	Réseaux métropolitains pour des zones urbaines plus larges	2 ,4 GHz, 5 GHz	Jusqu'à 1 Gbps	Jusqu'à quelques kilomètres
WWAN (Wide Area Network)	Réseaux étendus à grand échelle couvrant des régions national ou mondiale	Différentes bandes	Jusqu'à 10 Gbps	Plusieurs kilomètres à des centaines kilomètres

Tableau I.3: Les catégories des réseaux sans fil. **[5]**

I.4 Définition du réseau Wi-Fi

I.4.1 Principe

Le Wi-Fi est une technique de réseau informatique sans fil mise en place pour fonctionner en réseau interne devenu un moyen d'accès à haut débit à Internet. Il est basé sur la norme IEEE 802.11 (ISO/CEI 8802.11) correspondant au standard international décrivant les caractéristiques d'un réseau local sans fil (WLAN)[6].

Le Wi-Fi est utilisé par différent types d'utilisateurs que l'on peut regrouper ainsi[6] :

Home spot : Réseau pour les particuliers : il permet de partager sa connexion Internet sans utiliser les câbles.

Work spot : Réseau d'entreprise : s'associe à un réseau filaire Ethernet ou le remplace.

Hot spot : Réseau publique en accès libre accessibles dans les lieus publics fréquentés (gares, aéroport, hôtels …) par un ordinateur ou PDA... ; La figure I.3 présente le principe de Fonctionnement d'un réseau Wi-Fi.

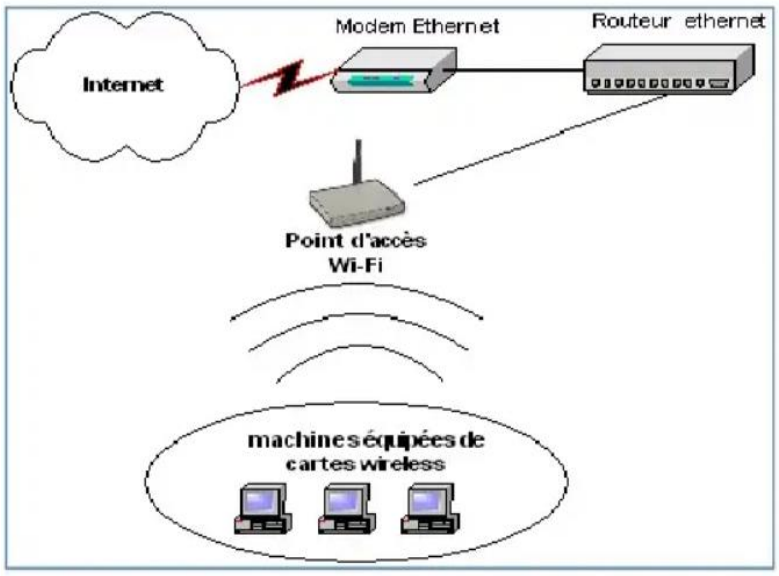


Figure I.5: Fonctionnement d'un réseau Wi-Fi[6].

I.4.2 Standard

La norme 802.11 s'attache à définir les couches basses du modèle OSI (Open System Interconnexion) pour une liaison sans fil utilisant des ondes électromagnétiques, c'est-à-dire :

- **La couche physique** (notée parfois couche PHY), proposant des types de codage de l'information.
- **La coche liaison de données** constituée de deux sous – couches : le contrôle de la liaison logique (Radio Ressources Control ou RLC) et le contrôle d'accès au support (Media Access Control ou MAC) [7]. La figure I.6 présenté les couches basent du modèle OSI.

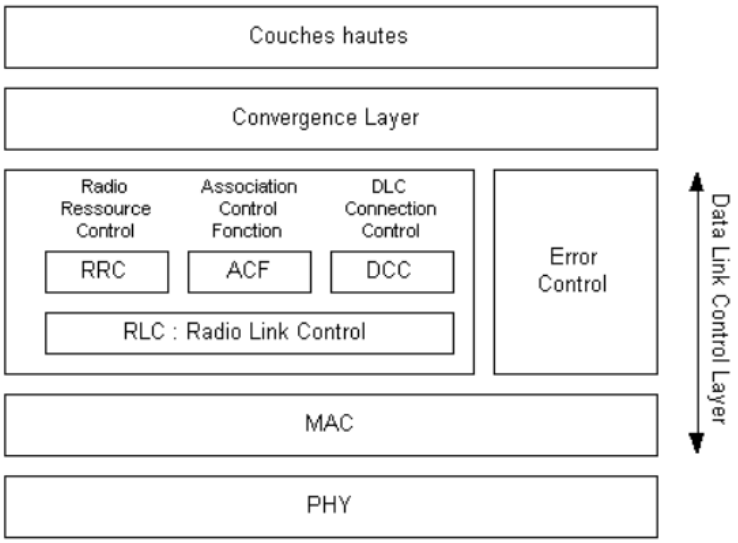


Figure I.7: Modèle en couches de l'IEEE 802.11 [7].

I.4.3 Les différentes normes Wi-Fi

La norme IEEE 802.11 est en réalité la norme initiale offrant des débits de 1 ou 2Mbps. Des révisions ont été apporté à la norme originale afin d'optimiser le débit (c'est le cas des normes 802.11a, 802.11b et 802.11g, appelées normes 802.11 physique) ou bien préciser des éléments afin d'assurer une meilleure sécurité ou une meilleure interopérabilité**.**[7] **;** la figure I.5 présente les révisions des normes 802.11.

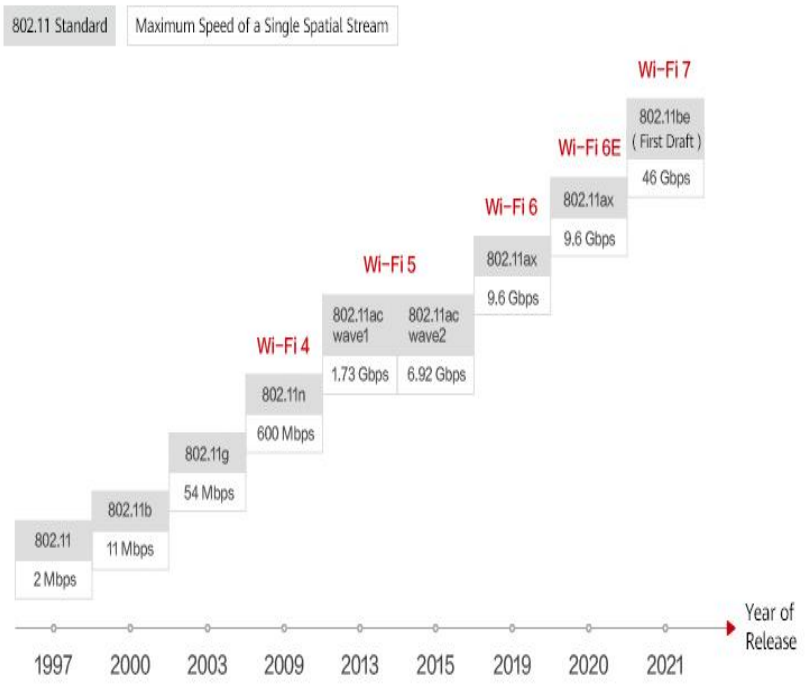


Figure I.8: La révolution de la norme 802.11[8]**.**

I.4.4 Les bandes de fréquences utilisées dans la norme IEEE 802.11

Le Wi-Fi utilise deux principales fréquences, à savoir 2,4 GHz et 5 GHz. La fréquence de 2,4 GHz offre une portée étendue et une meilleure pénétration des obstacles, ce qui la rend idéale pour les environnements nécessitant une large couverture. Cependant, elle peut être sujette aux interférences en raison de nombreux autres appareils utilisant cette fréquence. D'un autre côté, la fréquence de 5 GHz offre une bande passante plus large et des vitesses de transmission plus élevées. Elle est moins sujette aux interférences car moins d'appareils l'utilisent, mais sa portée est généralement plus courte et elle peut rencontrer plus de difficultés à traverser les obstacles physiques.[9] ; La figure I.6 présente les deux fréquences Utilisées par le Wi-Fi.

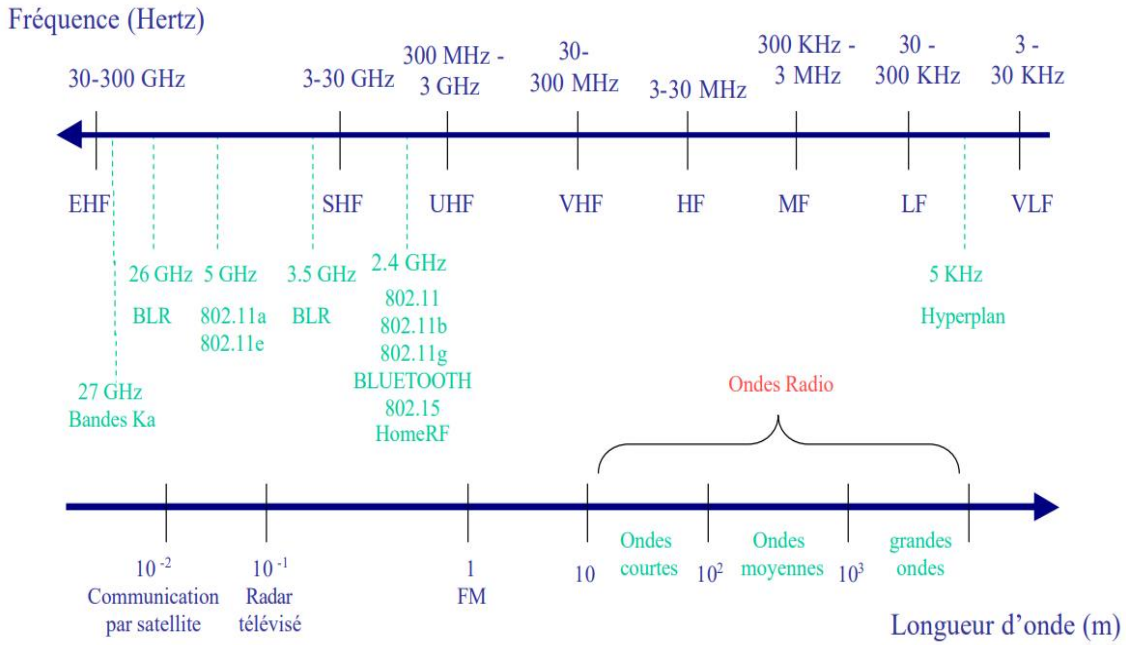


Figure I.9: Les bandes de fréquences de 2,4 GHz et 5 GHz[9].

I.5. Le mode de fonctionnement

On distingue deux modes de fonctionnement.

I.5.1 Le mode infrastructure

Dans ce mode, une station de base appelée Access Point (point d'accès) gère toutes les stations terminales à portée radio. Il permet aux stations terminales de communiquer entre elles et avec des stations d'un réseau filaire existant. L'ensemble constitué par le point d'accès et les stations sous son contrôle forme un BSS (Basic Service Set/Ensemble de services de base) ; la zone ainsi couverte est appelée BSA (Base Set Area)[10].

Figure I.10:Mode infrastructure[11].

I.5.2 Le mode ad hoc

En mode ad hoc, il n'y a pas de gestion centralisée. Il n'y a pas de point d'accès. Les stations terminales se connectent directement les unes aux autres via des liaisons point à point ou point à multipoints. Ces stations constituent une cellule appelée IBSS (Indépendant Basic Service Set) [10].

Figure I.11: Mode ad hoc[11].

I.6 Problèmes spécifiques aux réseaux sans fils de type IEEE 802.11

I.6.1 Support de transmission

Malgré leurs nombreux avantages, les réseaux sans fil posent d'énormes problèmes liés au Support de transmission. Les ondes radio se propagent dans l'air, en ligne droite, à la vitesse de la lumière et peuvent être déviées par réflexion, réfraction ou diffraction à cause des obstacles rencontrés sur leur trajectoire. Les ondes radio peuvent même être totalement absorbées.

L'existence d'interférences, principalement dues aux réflexions multiples, des Conséquences néfastes sur les paramètres de la liaison c'est-à-dire sur le taux d'erreur, la portée ainsi que le débit, qui sont des grandeurs étroitement liées.

Parallèlement aux problèmes dus au support de propagation, la sécurité, la mobilité ainsi que la qualité de service (fonction de l'application utilisée) restent les maillons faibles des réseaux sans fil [12].

I.6.2 Sécurité

Bien que les réseaux sans fil offrent la mobilité ainsi que la rapidité et la facilité de déploiement, la sécurité demeure un réel problème. La propagation dans l'espace fait que

n’importe quel individu ayant des équipements d’écoute appropriés (adaptateur radio, antenne directive, scanné) peut écouter le trafic sur le réseau (écoute passive).

D’autres attaques menacent l’intégrité d’un réseau comme l’intrusion ou la dissimulation d’identité. Avec l’intrusion, un étranger pénètre un système de communication puis accède au système d’information de l’entreprise. Dans la dissimulation d’identité, un destinataire reçoit un message en provenance d’une personne qu’il croit connaître mais dont l’identité a été usurpée[12] ; Le tableau I.2 représente les solutions préconisées pour les types d'attaques mentionnées précédemment .

Type d’Attaque	**Solution préconisée**
Intrusion	Contrôle d’accès
Dissimulation	Identification

Tableau I.4: Types d’attaques et solutions préconisées [12] .

I.7 Conclusion

Dans ce chapitre, nous avons abordé plusieurs sujets liés aux réseaux sans fil. Tout d'abord, nous avons traité les classifications des réseaux sans fil, en mettant l'accent sur la technologie Wi-Fi et l'apparition du standard 802.11. Ensuite, nous avons expliqué les différentes bandes de fréquences utilisées dans les réseaux Wi-Fi. Enfin, nous avons cité les problèmes spécifiques aux réseaux sans fil basés sur la norme IEEE 802.11

Dans le chapitre à venir, nous consacrerons une attention particulière à la technologie HOTSPOT et nous examinerons de manière approfondie son fonctionnement.

Chapitre II : Généralités sur la Technologie HOTSPOT

II.1 Introduction

La dénomination exacte d'un HOTSPOT est Wireless Internet HOTSPOT. Il s'agit d'un lieu où la connexion vers un réseau Internet est possible via une connexion sans fil et grâce à un ensemble de technologies et de protocoles mis en œuvre. On parle également de borne Wi-Fi ou de point d'accès Wi-Fi[13].

Les HOTSPOTS se sont rapidement développés à l'échelle mondiale permettant ainsi à des utilisateurs nomades disposant d'équipements adaptés (ordinateurs ou téléphones portables compatibles, PDA et autres) de se connecter à Internet de partout avec beaucoup de simplicité. Si ces connexions Internet sont ouvertes au grand public, cela ne veut pas dire qu'il n'existe aucune protection à l'accès et pour les utilisateurs[13].

Dans ce chapitre, nous allons définir les HOTSPOTS en abordant leurs concepts généraux, les règles essentielles et les risques associés à leur utilisation. Ensuite, nous allons examiner en détail leur fonctionnement et le processus d'authentification via un portail captif. Puis, nous allons présenter des solutions open source pour la gestion des HOTSPOTS, en mettant en avant l'entreprise ICOSNET et sa recommandation de la solution HSNM. Enfin, nous allons détailler les caractéristiques de cette solution.

II.2 Définition du HOTSPOT Wi-Fi

HOTSPOT est un endroit physique où les gens peuvent accéder à l'Internet, généralement en utilisant le Wi-Fi, via un réseau local sans fil (WLAN) avec un routeur connecté à un fournisseur d'accès Internet. La plupart des gens appellent ces endroits "points d'accès Wi-Fi " ou "connexions Wi-Fi ".

Il s'agit alors d'un lieu public à forte affluence et clairement délimité (par exemple : café, hôtel, gare...) donnant accès à un réseau sans fil qui permet aux utilisateurs de terminaux mobiles de se connecter facilement à Internet[13].

II.3 Historique de HOTSPOT Wi-Fi

Les HOTSPOTS Wi-Fi sont un développement relativement récent dans l'histoire de la technologie sans fil. Voici un bref aperçu de l'histoire des HOTSPOTS.

Les premiers HOTSPOTS Wi-Fi sont apparus dans les années 1990, lorsqu'un groupe de chercheurs de Lucent Technologies a développé la première technologie de réseau local sans fil (WLAN) basée sur la norme 802.11. Ces chercheurs ont créé des HOTSPOTS Wi-Fi dans les bâtiments de Lucent pour permettre aux employés de se connecter à internet sans fil.

Le premier HOTSPOT Wifi public a été installé à l'aéroport international de Dallas-Fort Worth en 2000. L'installation a connu un succès immédiat, des milliers de voyageurs se connectant au HOTSPOT chaque mois.

Au cours des années 2000, les HOTSPOTS Wi-Fi sont devenus de plus en plus populaires, des HOTSPOTS entreprises comme STARBUCKS, McDonald's et d'autres chaînes de restauration rapide offrant des HOTSPOTS Wi-Fi gratuits ou payants à leurs clients.

Au fil du temps, les HOTSPOTS Wi-Fi sont devenus plus fréquents dans les lieux publics tels que les aéroports, les hôtels, les centres commerciaux et les bibliothèques. Les points d'accès mobiles sont également devenus populaires, les fournisseurs de services mobiles proposant des HOTSPOTS Wi-Fi portables à utiliser en déplacement.

Aujourd'hui, les HOTSPOTS Wi-Fi sont largement utilisés dans le monde entier pour fournir une connectivité Internet sans fil pratique et facilement accessible. Ils ont transformé la manière dont nous interagissons avec l'internet, en permettant aux utilisateurs de se connecter à l'internet de manière transparente depuis pratiquement n'importe quel endroit[13] ;la figure II.1 représente le déploiement des HOTSPOT Wi-Fi dans le Monde

Figure II.1:Les HOTSPOT Wi-Fi dans le Monde [14] .

II.4 Les types des HOTSPOTS Wi-Fi

Il existe différents types de HOTSPOTS Wi-Fi, chacun ayant ses propres caractéristiques et utilisations. Voici une liste des principaux types de HOTSPOTS Wi-Fi :

- **HOTSPOT Wi-Fi mobiles** : ce sont des appareils portables qui permettent aux utilisateurs de se connecter à Internet via un réseau cellulaire. Les HOTSPOTS Wi-Fi mobiles peuvent être achetés auprès des fournisseurs de services mobiles et sont souvent utilisés pour fournir une connectivité Internet lors des déplacements.

- **HOTSPOT Wi-Fi publics** : ce sont des HOTSPOTS disponibles dans des endroits publics tels que les aéroports, les cafés, les hôtels et les bibliothèques. Les HOTSPOTS Wi-Fi publics permettent aux utilisateurs de se connecter à l'internet gratuitement ou moyennant des frais, et sont souvent utilisés pour accéder à l'internet lors de déplacements.

- **HOTSPOT Wi-Fi prépayé** : Ce troisième type de HOTSPOT est très similaire aux HOTSPOTS mobiles, mais limiter la quantité de données que vous pouvez consommer ou utiliser avec cette connexion. Pour pouvoir utiliser ce type de connexion, vous devez payer une certaine quantité de données à l'avance et, lorsque vous la consommez, le paiement pour plus de données est automatiquement renouvelé. C'est donc quelque chose qui va nous coûter de l'argent. C'est quelque chose que nous pouvons trouver dans de nombreux pays, courant dans des endroits tels que les bateaux, les aéroports ou les gares, même dans certains hôtels[15].

II.5 Avantages et inconvénients d'un HOTSPOT Wi-Fi

II.5.1 Avantages

Un HOTSPOT Wi-Fi offre plusieurs avantages [16] .

- Accès à Internet : Un HOTSPOT Wi-Fi permet d'accéder à Internet depuis n'importe quel endroit où il y a une connexion sans fil. Cela peut être utile pour les voyageurs, les travailleurs à distance, les étudiants et les personnes qui ont besoin d'accéder à Internet en déplacement.

- Mobilité : Avec un HOTSPOT Wi-Fi, vous pouvez vous déplacer librement tout en étant connecté à Internet. Vous pouvez utiliser un Smartphone, une tablette ou un ordinateur portable pour vous connecter à Internet via le HOTSPOT Wi-Fi.

- Partage de connexion : Vous pouvez partager votre connexion Internet avec plusieurs appareils simultanément. Cela peut être utile lorsque vous voyagez avec des amis ou des collègues et que vous avez besoin de partager une connexion Internet.

- Sécurité : Les HOTSPOTS Wi-Fi sont souvent sécurisés avec des protocoles de chiffrement tels que WPA2. Cela signifie que vos informations sont protégées contre les pirates informatiques et les cybercriminels.

- Économie : Les HOTSPOTS Wi-Fi sont souvent moins chers que les plans de données cellulaires, ce qui peut être avantageux si vous avez besoin d'une connexion Internet temporaire ou si vous voyagez à l'étranger et que vous ne voulez pas payer des frais d'itinérance élevés.

II.5.2 Inconvénients

Bien qu'il y ait des avantages à utiliser un HOTSPOT Wi-Fi, il y a aussi quelques inconvénients potentiels à considère [16].

- Connexion instable : La qualité de la connexion peut être affectée par des facteurs externes tels que la distance entre l'appareil et le HOTSPOT Wi-Fi, la présence d'obstacles ou d'interférences dans l'environnement, la charge du réseau, etc. Il est donc possible que la connexion soit instable ou lente dans certaines circonstances.

- Limitations de données : Certains HOTSPOTS Wi-Fi ont des limites de données, ce qui signifie que vous ne pourrez pas transférer autant de données que vous le souhaitez. Cela peut être un inconvénient si vous devez télécharger ou transférer des fichiers volumineux.

- Disponibilité : Les HOTSPOTS Wi-Fi ne sont pas toujours disponibles dans toutes les zones géographiques, en particulier dans les zones rurales ou éloignées. Il est donc possible que vous ne puissiez pas accéder à Internet via un HOTSPOT Wi-Fi dans certaines circonstances.

II.6 Risques concrets d'usage de la connexion internet en accès Wi-Fi

L'usage d'une connexion internet en accès Wi-Fi provoque des risques d'utilisation qui peuvent causer des problèmes avec les autorités judicieuses. Parmi ces risques il y a[16] .

- Téléchargements illégaux.
- Connexion à des sites d'échanges de fichiers.
- Usurpation d'identité sur des forums ou des messageries instantanées....
- Diffusion de propos diffamatoires, xénophobe sur internet.
- Usage de l'accès internet pour des actions de Spam, de piratage, de diffusion de virus.

II.7 Règle pour la mise en place d'un HOTSPOT

La mise en place d'un HOTSPOT conforme à la législation Algérienne implique plusieurs étapes :

- Créer un accès (compte) individuel pour chaque utilisateur, établir le lien entre ce compte et la personne physique, par exemple en demandant une carte d'identité, ou carte d'étudiant et en relevant le numéro de téléphone de cette dernière.
- Ensuite il est nécessaire d'enregistrer les heures d'accès de ce visiteur, ceci est fait directement par le portail captif.
- Finalement l'université enregistre l'activité Internet des utilisateurs, le contenu n'est ici pas archivé, uniquement les adresses IP visités.

Veuillez-vous référer à **l'annexe 1** pour consulter tous les détails de la réglementation concernant la mise en place du HOTSPOT Wi-Fi.

II.8 Fonctionnement d'un HOTSPOT

Le principe de fonctionnement d'un HOTSPOT repose sur la transmission de signaux radio à partir d'un routeur ou d'un point d'accès Wi-Fi vers les dispositifs à proximité [17].

Lorsqu'un HOTSPOT est activé, il émet un signal Wi-Fi qui peut être détecté par les appareils compatibles à portée. Les utilisateurs peuvent alors sélectionner le HOTSPOT dans la liste des réseaux Wi-Fi disponibles et se connecter en entrant les informations d'identification nécessaires, comme un mot de passe si celui-ci est sécurisé.

Une fois connectés, les utilisateurs peuvent accéder à Internet via le HOTSPOT, en utilisant la bande passante et la connectivité du réseau auquel le HOTSPOT est connecté. Les HOTSPOTS peuvent être configurés pour offrir un accès Internet gratuit ou payant, en utilisant des portails captifs pour l'authentification des utilisateurs et la gestion des sessions.

La gestion d'un HOTSPOT Wi-Fi implique des tâches telles que la configuration du réseau, la gestion des utilisateurs, le contrôle de la bande passante, la personnalisation du portail captif et la surveillance du trafic. Les solutions logicielles de gestion de HOTSPOTS offrent des fonctionnalités avancées pour simplifier ces tâches et garantir une expérience utilisateur fluide et sécurisée.

II.9 Portail captif

Le portail captif d'un HOTSPOT est une interface web ou une page spécifique qui s'affiche lorsqu'un utilisateur se connecte à un réseau Wi-Fi public ou à un HOTSPOT. Il agit comme une passerelle entre l'utilisateur et l'accès à Internet.

Le portail captif du HOTSPOT est conçu pour authentifier les utilisateurs, collecter des informations d'identification telles que des identifiants ou des codes d'accès, et fournir des informations supplémentaires telles que les conditions d'utilisation, les politiques de confidentialité ou les offres spéciales. Il peut également offrir des options de paiement pour les forfaits premium ou les temps d'accès supplémentaires[18] ; La figure II.2 explique le fonctionnement de portail captif.

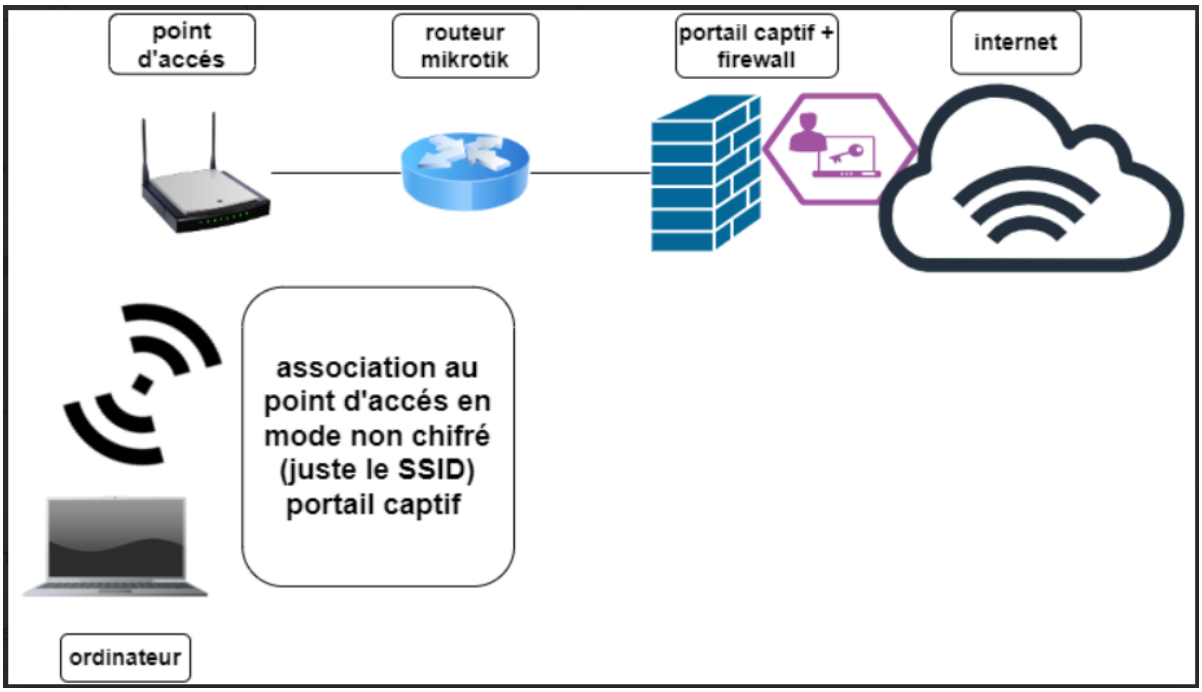


Figure II.2: Portail captif WEB

Un portail captif est un système qui contrôle l'accès à un réseau sans fil en demandant aux utilisateurs de s'authentifier ou de s'inscrire avant de pouvoir accéder à Internet.la figure II.3 explique la fonction d'un portail captif.

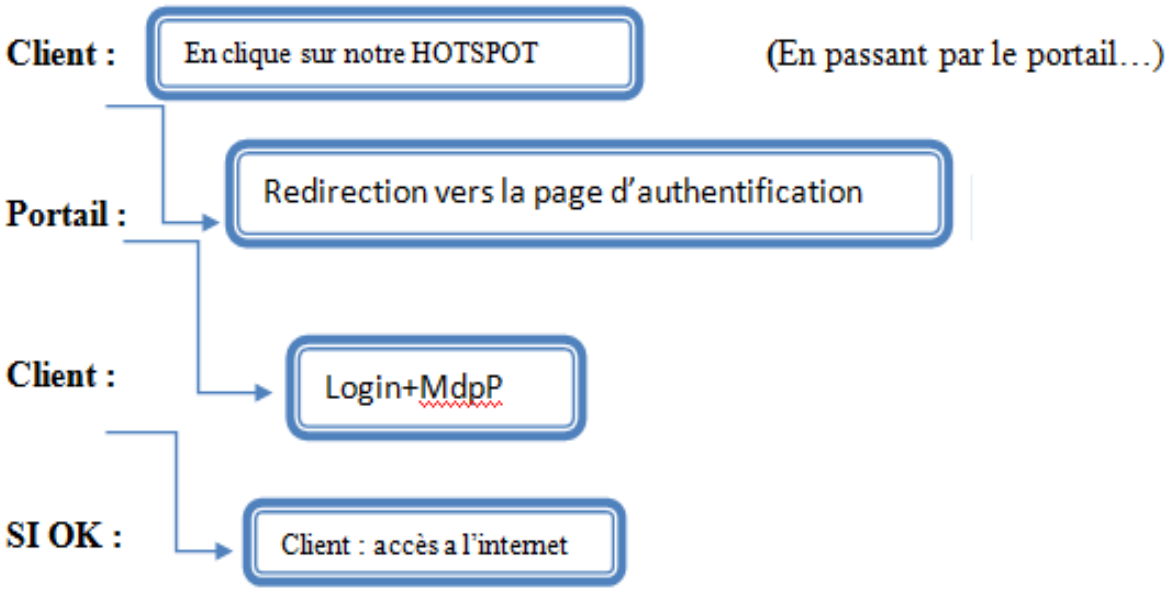


Figure II.3: Fonction type d'un portail captif.

II.10 Les différentes solutions de gestion des HOTSPOTS

Voici quelques logiciels populaires qui permettent d'installer un portail captif pour la gestion des HOTSPOTS Wi-Fi :

- **HSNM (HOTSPOT Network Manager)**

  HSNM est une solution de gestion de HOTSPOT qui offre des fonctionnalités avancées de contrôle d'accès et de gestion des utilisateurs. Il prend en charge plusieurs méthodes d'authentification telles que le code d'accès, l'authentification sociale et les tickets prépayés.

  HSNM offre également des options de personnalisation du portail captif pour l'authentification des utilisateurs. Il dispose d'un tableau de bord intuitif pour surveiller l'utilisation du réseau, gérer les utilisateurs connectés et analyser les données.

  HSNM propose une intégration avec des systèmes de paiement tiers pour faciliter la monétisation des HOTSPOTS.[19]

- **Cloud4Wi**

  Cloud4Wi est une entreprise spécialisée dans la fourniture de solutions de gestion et d'analyse de l'expérience client basées sur le Cloud. Leur plateforme permet aux entreprises de créer et de gérer des HOTSPOTS Wi-Fi personnalisés, offrant ainsi une connectivité sans fil aux utilisateurs finaux.

- **Cisco MERAKI**

  Cisco MERAKI est une plateforme de gestion Cloud qui offre une solution complète pour la gestion et le déploiement de réseaux informatiques. Elle permet aux entreprises de gérer leurs réseaux filaires et sans fil, leurs appareils et leurs applications, le tout à partir d'une interface centralisée basée sur le Cloud.[20]

- **UNIFI Controller**

  UNIFI Controller est une application logicielle développée par Ubiquité Networks, conçue pour gérer et contrôler les dispositifs de réseau UNIFI, tels que les points d'accès sans fil, les commutateurs Ethernet et les caméras de surveillance.[21]

Le tableau II.1 présente une comparaison entre les différentes solutions citées précédemment :

Plate-forme	HSNM	Cloud4Wi	Cisco MERAKI	UNIFI Controller
Caractéristiques Principales	Portails captifs personnalisables, authentification des utilisateurs, Gestion centralisée, analyse de localisation, Outils marketing (avancé)	Portails captifs personnalisables, authentification des utilisateurs, analyse de localisation, outils marketing (basique)	Gestion centralisée, authentification des utilisateurs, contrôles d'accès, utilisation Analytique	Authentification des utilisateurs, portail captif
Matériel pris En charge	Prend en charge plusieurs fournisseurs de matériel	Prend en charge plusieurs fournisseurs de matériel	Points d'accès sans fil MERAKI	Points d'accès sans fil Ubiquité UNIFI
Options de Déploiement	Sur site, Basé sur le Cloud	Basé sur le Cloud	Basé sur le Cloud	Sur site, basé sur le Cloud
Méthodes d'authentification	Portail captif, connexion sociale, Envoi/réception de SMS, CARD VOCHER	Portail captif, RADIUS, Active Directory, connexion sociale	Portail captif, RADIUS, Active Directory, connexion sociale	Portail captif, RADIUS, connexion sociale
Prise en charge multi-locataires	OUI	OUI	OUI	Oui (Gestion multi sites)
Prise en charge de la marque	OUI	OUI	OUI	OUI

Tableau II.1: Comparaison entre les différentes solutions de HOTSPOT.

Nous voulons offrir un accès internet rapide et facile (y a compris minimum de configuration par l'utilisateur) qui assure la mobilité (y a compris le réseau sans fils) au niveau de notre département d'électronique de l'université Blida 1.

Après avoir analysé les comparatifs précédents et en tenant compte des besoins de notre projet ainsi que des exigences de l'entreprise ICOSNET, il est clair que la solution HSNM se distingue en termes de performance et de scalabilité. Elle offre une réponse complète aux

critères de sécurité et d'authentification nécessaires (sécurité de l'authentification et de la communication). De plus, cette solution répond parfaitement aux critères suivants :

- Sécurité de l'authentification et de la communication : HSNM offre des mécanismes robustes pour garantir l'authentification sécurisée des utilisateurs et assurer une communication fiable et protégée.

- Disponibilité : La solution HSNM est conçue pour assurer une disponibilité élevée en intégrant des fonctionnalités qui permet une répartition équilibrée de la charge entre les différents composants du système.

- Confidentialité : HSNM assure la confidentialité des données en offrant des fonctionnalités telles que l'utilisation du protocole HTTPS pour l'interface Web, l'authentification HTTPS.

- Simplicité d'administration et d'installation : HSNM est conçu pour être convivial et facile à administrer, avec une interface intuitive et des processus d'installation simplifiés, facilitant ainsi la gestion quotidienne du système.

Ces critères font de la solution HSNM un choix attractif pour répondre aux besoins de sécurité, de performance et de facilité d'administration dans divers contextes d'utilisation.

II.11 La solution proposée par ICOSNET

II.11.1Présentation de l'entreprise ICOSNET

Crée en 1999, ICOSNET se positionne comme un opérateur d'accès internet et de solutions de télécommunication et s'impose aujourd'hui sur le marché de la convergence voix et données pour les PME/PMI et les grands comptes multinationaux installés en Algérie.

ICOSNET a su capitaliser une importante expérience et nouer un relationnel conséquent avec les différents acteurs du secteur des télécommunications en Algérie et à l'étranger.

ICOSNET se différencie par son approche technique et qualitative. La société a ainsi montré son savoir-faire et sa maîtrise, notamment auprès des entreprises multi sites.

Sur le marché algérien, ICOSNET est un opérateur à part entière (autorisation ISP, VOIP et WIMAX). Ce positionnement nous permet de s'adresser à une clientèle large, de convaincre des clients de taille significative et de pouvoir proposer des solutions de connexion et de communication économiquement plus avantageuse et plus abouties.

Les raisons de son succès sont multiples, elles sont tout d'abord humains, combinant l'expérience et l'implication de ces collaborateurs et la forte expertise de ces partenaires, elles sont aussi stratégiques, car à partir de 2009 toute notre connectivité internet et acheminé depuis Londres, ce qui a largement contribué à la fiabilité du réseau ICOSNET.

Aujourd'hui plusieurs entreprises algérienne et grand groupes internationaux implanté en Algérie luis font confiance. ICOSNET ambitionne d'étendre son implantation sur le territoire national.

Au-delà de ses nouvelles ambitions de croissance, ICOSNET ne perdre pas de vue ses valeurs : qualité de service, satisfaction client, anticipation, veille technologique et innovation sont autant d'objectifs qui reste et resteront priorités.

Figure II.4: Historique d'ICOSNET.

II.11.2 La solution HSNM

HSNM HOTSPOT Manager est un logiciel de gestion de HOTSPOT développé par HSNM, une entreprise spécialisée dans la fourniture de solutions de gestion de réseau pour les entreprises.

Le logiciel HSNM HOTSPOT Manager permet aux entreprises de gérer efficacement leur HOTSPOT Wi-Fi, en offrant une plate-forme de gestion centralisée pour les points d'accès, les utilisateurs, les forfaits, les transactions et les analyses[19].

II.11.2.1 Les principales caractéristiques de HSNM

La solution HSNM propose plusieurs caractéristiques, qui sont énumérées ci-dessous :

- Connexion au système à plusieurs niveaux : administrateur, revendeur, gestionnaire, annonceur.
- Définition des produits avec leurs prix de vente, achetables directement par l'utilisateur en utilisant différents modes de paiement.
- Enregistrement des utilisateurs selon différentes méthodes d'authentification, également avec envoi/réception de SMS.
- Comptabilisation de l'utilisateur en associant un produit à volonté, avec toutes les limitations de temps et de trafic quotidien, mensuel et total.
- Génération automatique d'un script pour la configuration des passerelles HOTSPOT basées sur MIKROTIK ROUTER OS.
- Affichage/analyse graphique des données de trafic, temps, ventes revendeur, manager et utilisateur.
- Création d'applications personnalisées qui s'intègrent au portail captif, engageant les utilisateurs, fournissant des contenus, promouvant des produits, affichant des promotions, etc.
- Mise à jour automatique du logiciel de l'appareil grâce à une mise à jour en direct.
- Afficher la bannière publicitaire et la vidéo au moment où les utilisateurs se connectent au portail[19].

II.11.2.2 Marchés cibles des services HSNM

HSNM est en mesure de satisfaire un large éventail de propositions commerciales ; Le tableau II.2 qui donne quelques scénarios dans lesquels HSNM peut offrir ses services.

TYPE	DESCRIPTION
Hospitalité	Les clients ont besoin de se connecter et de surfer sur le net. Les hébergements tels que les hôtels, les centres de villégiature, les campings, les plages, les restaurants, les bars, etc. peuvent augmenter la valeur de leur offre.
Entreprises privées	Elles doivent permettre aux invités de se connecter à leur réseau d'entreprise.
Événements	Les spectacles, les événements sportifs, les concerts, etc. peuvent fournir des informations, des scores et des résultats.
Municipalité	Placez des points d'accès pour les citoyens et les touristes dans les parcs, les places et les rues
Magasins et centres commerciaux	Offrent un service supplémentaire aux clients et peuvent publier des dépliants, des promotions, des publicités, etc.
Éducation	Écoles et campus universitaires pour permettre l'accès aux enseignants, étudiants, invités, etc.
Administration publique	Nécessité de permettre aux invités de se connecter au réseau municipal
Divertissement	Accès à Internet dans les parcs d'attractions et les parcs à thème.

Tableau II.2: Les services qui offrent HSNM[19].

La figure II.5 qui montre un exemple de déploiement de la solution HSNM dans un Hôtel

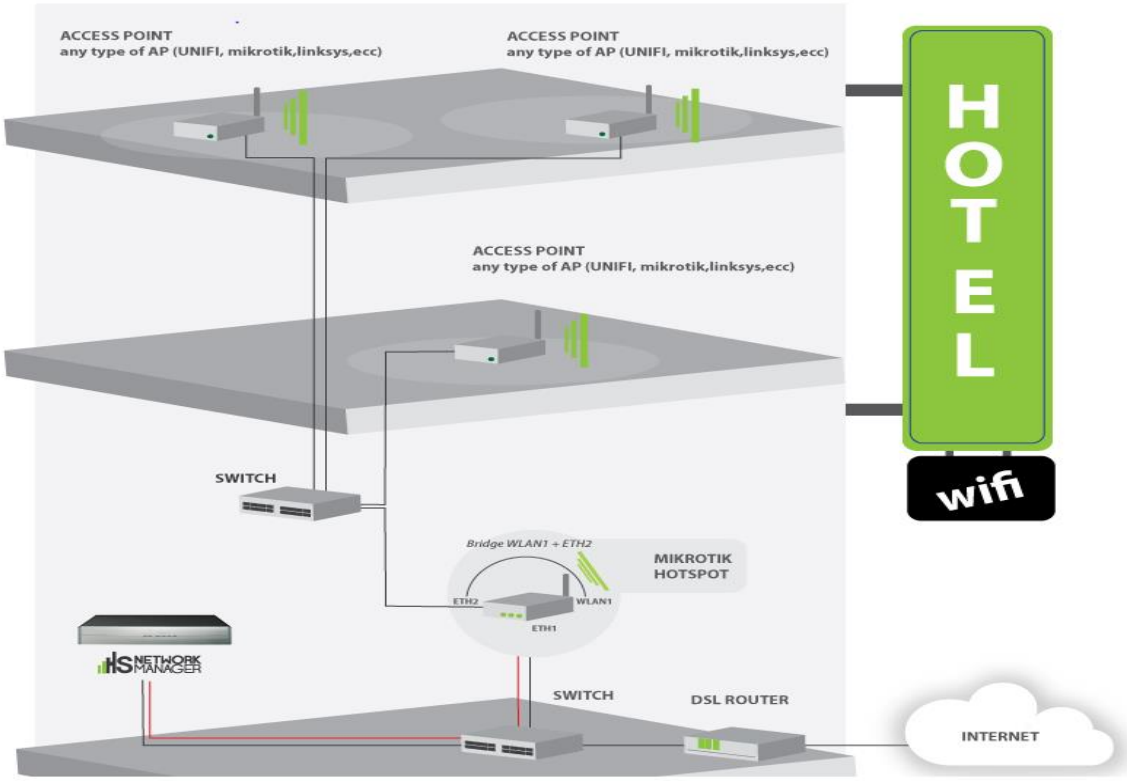


Figure II.5: Déploiement d'un HOTSPOT dans un hôtel [22].

II.11.2.3 Les versions du HSNM

Il existe deux versions de HSNM :

- **Hardware**

- Hardware (SUBSYSTEM=2.0)

- Hardware (SUBSYSTEM<=1.9)

- **Virtual Appliance**

Nous allons travailler avec la deuxième version de produit HSNM : VMWARE **;** Il est fourni en tant qu'Appliance virtuelle et fonctionne sur VMWARE Player, VMWARE Workstation Player ou VMWARE VSPHERE ou convertible sur d'autres systèmes virtuels. L'avantage est la possibilité de placer la machine dans une structure de serveur existante avec une réduction visible de l'investissement du premier produit. La liste suivante décrit les exigences minimales pour le serveur qui exécute la machine virtuelle :

- Au moins **3 Go de RAM** à dédier à HSNM.
- **De 35 Go** (espace minimum requis pour l'installation) **à 250 Go** (occupation maximale atteinte lors de l'augmentation des données) **d'espace disque**. Il est recommandé d'installer la machine virtuelle sur un disque avec une disponibilité de 250 Go, car lorsque les données augmentent, s'il n'y a pas assez d'espace, la machine peut se bloquer.
- **Processeur Dual-Core**[19]**.**

II.12 Conclusion

La technologie des HOTSPOTS Wi-Fi joue un rôle essentiel dans la fourniture de connectivité Internet sans fil dans les lieux publics. Afin d'offrir une expérience utilisateur de qualité, une gestion efficace de ces HOTSPOTS est primordiale. En optant pour la bonne solution logicielle, il est possible d'assurer la sécurité du réseau, la personnalisation du portail captif et la gestion centralisée. Dans ce contexte, l'entreprise ICOSNET, présentée précédemment, nous recommande l'utilisation de la solution HSNM en raison de ses caractéristiques avantageuses.
Il est temps de se pencher sur une étude de planification et d'optimisation afin de faire fonctionner ce HOTSPOT dans les meilleures conditions possibles.

Chapitre III : Installation de HSNM environnement hyperviseur

III.1 Introduction

Le logiciel HSNM HOTSPOT Manager permet aux entreprises de gérer efficacement leur HOTSPOT Wi-Fi, en offrant une plate-forme de gestion centralisée pour les points d'accès, les utilisateurs, les forfaits, les transactions et les analyses.

La plateforme HSNM est proposée sous forme d'un appareil physique et peut être utilisée avec des logiciels tels que VMWARE Player, VMWARE Workstation Player, VMWARE VSPHERE ou autres. Cela signifie qu'elle doit être intégrée à une infrastructure de serveur existante.

Dans ce chapitre, nous explorerons les concepts fondamentaux de la virtualisation, puis nous détaillerons les étapes nécessaires pour installer la machine virtuelle HSNM sur l'hyperviseur VMWARE ESXi.

III.2 Principe de fonctionnement de la virtualisation

III.2.1 Définition de la virtualisation

La virtualisation est une technologie qui permet de créer des versions logiques ou virtuelles de ressources informatiques, telles que des serveurs, des systèmes d'exploitation, des réseaux ou des applications. Elle vise à séparer la couche logicielle de la couche matérielle, permettant ainsi de maximiser l'utilisation des ressources physiques disponibles.

En utilisant la virtualisation, une seule machine physique peut être utilisée pour exécuter plusieurs machines virtuelles indépendantes, chacune d'entre elles fonctionnant avec son propre environnement logiciel. Ces machines virtuelles peuvent partager les ressources matérielles, telles que le processeur, la mémoire et le stockage, de manière efficace, en permettant l'exécution simultanée de différents systèmes d'exploitation et applications sur une même machine physique.[23] ; La figure III.1 montre le fonctionnement de la virtualisation.

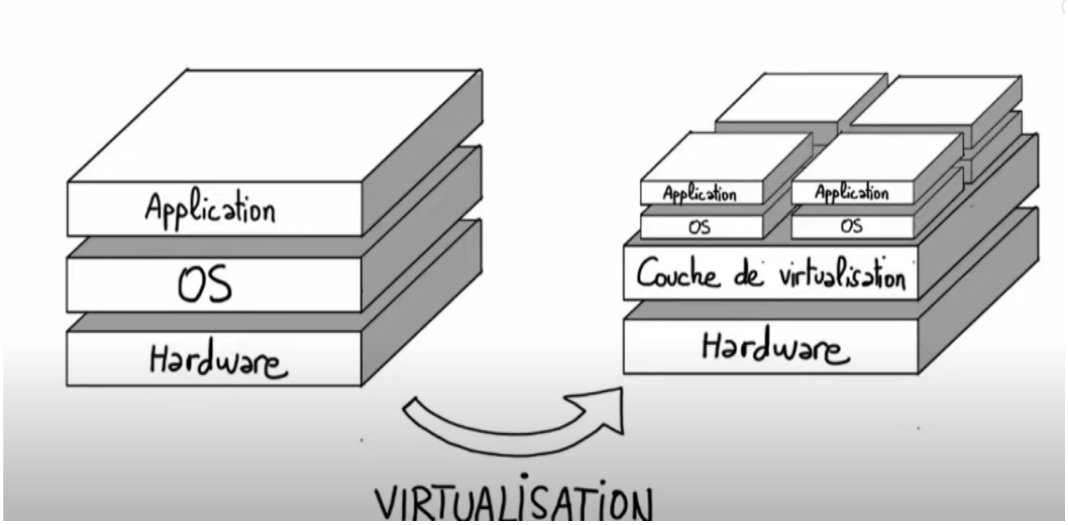


Figure III.1: Le fonctionnement de la virtualisaion [24].

III.2.2 Présentation de la machine virtuelle

Connu sous l'appellation « machine virtuelle » (Virtual machine ou VM), un système informatique virtuel est un conteneur de logiciels parfaitement isolé intégrant un système d'exploitation et des applications. Chaque VM autonome est entièrement indépendante. L'installation de plusieurs VM sur un ordinateur permet d'exécuter différents systèmes d'exploitation et applications sur un seul et même serveur physique, ou hôte.

Une fine couche logicielle, appelée "hyperviseur", dissocie les machines virtuelles de l'hôte et alloue dynamiquement des ressources informatiques à chaque machine selon les besoins[23].

III.2.3 L'hyperviseur

L'hyperviseur est une technologie clé pour la virtualisation de système, qui permet de créer des machines virtuelles complètes, chacune avec leur propre système d'exploitation, applications et services. Il existe 2 types d'hyperviseurs [23].

L'hyperviseur de type 1 ou « barre-métal » : Il s'exécute directement sur le matériel physique, sans nécessiter de système d'exploitation hôte. Il est également appelé hyperviseur natif. Les exemples courants d'hyperviseurs de type 1 sont VMWARE ESXI, Microsoft Hyper-V et XEN.

L'hyperviseur de type 2 ou « Host métal » : C'est un logiciel qui s'exécute à l'intérieur d'un autre système d'exploitation l'OS HOTE un système d'exploitation invité, il s'exécute en troisième niveau au-dessus du matériel. Les exemples d'hyperviseurs de type 2 incluent

VMWARE Workstation, Oracle Virtual Box et Microsoft Virtual PC ; La figure III.2 montre les types d'hyperviseur.

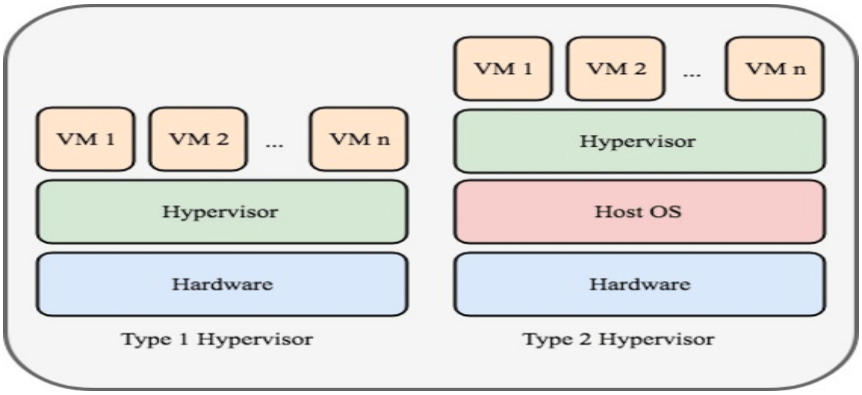


Figure III.2: Type 1 et type 2 hyperviseur[25].

Le rôle de l'hyperviseur consiste à :

- Contrôler le processeur et les ressources de la machine physique.
- Attribuer à chaque machine virtuelle son besoin de ressources.
- S'assurer qu'il n'y aura pas d'interactions entre les machines virtuelles[23].

III.2.4 Avantages et inconvénients des machines virtuelles

III.2.4.1 Avantages

- Options de reprise d'activité et de provisionnement des applications.
- Les machines virtuelles sont simples à gérer et à entretenir et sont disponibles partout
- Plusieurs environnements de systèmes d'exploitation peuvent être exécutés sur un même ordinateur physique [26].

III.2.4.2 Inconvénients

- L'exécution de plusieurs machines virtuelles sur une seule machine physique peut être à l'origine de performances instables.
- Les machines virtuelles sont moins efficaces et plus lentes qu'un ordinateur physique[26].

III.3 Présentation de VMWARE VSPHERE ESXI

VMWARE VSPHERE est un produit de virtualisation de serveurs de l'entreprise VMWARE, qui permet de consolider plusieurs machines virtuelles sur un seul serveur physique.

VSPHERE est une plate-forme de virtualisation de Cloud COMPUTING. Elle ne doit pas être considérée comme un produit, mais plutôt comme une famille de produits contenant des logiciels de soutien et des outils de gestion[27].

ESXI est une partie spécifique de la plateforme VSPHERE. ESXI est un hyperviseur de type 1, également appelé "barre-métal", conçu pour être installé directement sur un serveur physique. Il permet de créer et de gérer des machines virtuelles (VM) sur ce serveur, comme illustré dans la figure III.3.

Figure III.3:VMWARE VSPHERE ESX [28].

ESXI présente plusieurs avantages [27], il permet, entre autres, de :

- Offrir une expérience conviviale
- Offrir une sécurité renforcée et protège les données importantes
- Réduire l'empreinte informatique
- Offrir des performances fiables et prévisibles.

III.4 Installation de l'ESXI

Pour installer l'hyperviseur ESXI (barre-métal) sur notre serveur, nous suivons les étapes suivantes :

1- Nous préparons une clé USB multiboot en copiant l'image ISO de l'hyperviseur ESXI. Ensuite, nous démarrons la machine en utilisant cette clé USB. Une fois la machine allumée, nous arrivons à l'écran de démarrage de L'ESXI, comme illustré dans la Figure III.4

Figure III.4: L'écran de démarrage de l'ESXI

2- Le système ESXI se charge dans la mémoire RAM de la machine, permettant l'exécution de l'hyperviseur.

3- Après le chargement du système, l'écran affichant le contrat de licence apparaît. Pour continuer l'installation, nous acceptons les termes en cliquant sur F11

4- Une fois que le système est installé, nous retirons la clé USB et procédons à un redémarrage. Ensuite, nous renseignons les informations nécessaires telles que le nom d'utilisateur, le mot de passe et l'adresse IP.

Nous retournons sur notre navigateur Internet et saisissons l'adresse IP suivante : 192.168.2.170. La page suivante s'affiche alors, conformément à ce qui est montré dans la Figure III.5

Figure III.5: Affichage de la page de VMWARE

5- Nous saisissons le nom d'utilisateur et le mot de passe que nous avons définis lors de l'installation, ce qui nous permet d'accéder à notre logiciel VMWARE ESXI.

6- Les informations de notre serveur sont affichées en haut de l'interface web de VMWARE ESXI, comme illustré dans la Figure III.6.

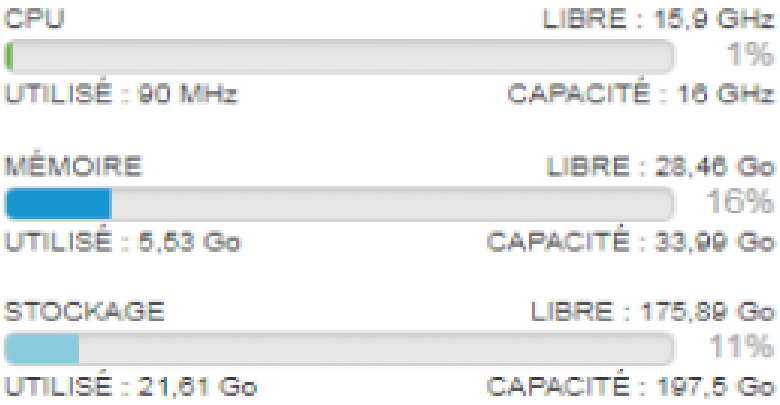


Figure III.6 : Les informations de serveur.

7- Pour créer une machine virtuelle, nous cliquons sur l'option "Machine virtuelle". Ensuite, nous sélectionnons "Déployer une machine virtuelle à partir d'un fichier OVA" en cliquant sur "Sélectionner un type de création".

8- Nous avons téléchargé le fichier OVA à partir du site HSNM, qui nous a été envoyé par courrier électronique, comme indiqué dans la Figure III**.**7

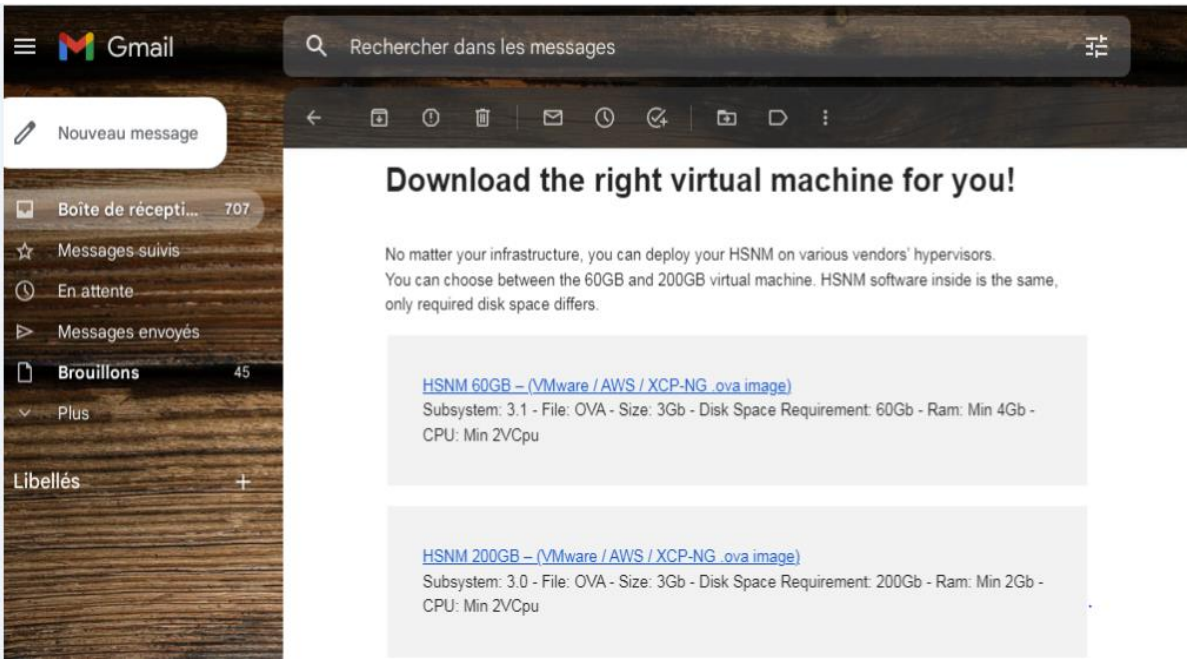


Figure III.7: Les liens des fichiers OVA.

9- Après avoir téléchargé le fichier OVA, nous retournons dans le logiciel VMWARE ESXI. Nous cliquons sur "Sélectionner des fichiers OVA et VMDK" et glissons le fichier OVA que nous avons téléchargé. Nous attribuons à la machine virtuelle le nom "HSNM", comme illustré dans la Figure III.8**.**

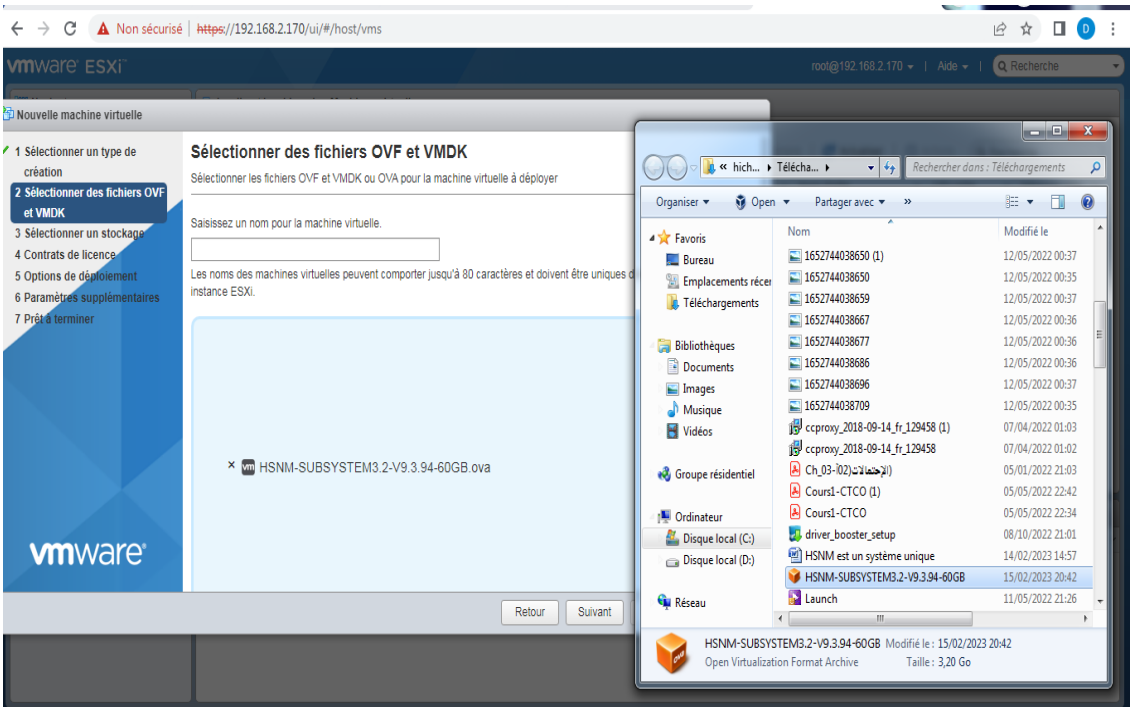


Figure III.8: Glissement de fichier OVA.

10- Notre machine virtuelle "HSNM" est maintenant installée, comme le montre la Figure III.9

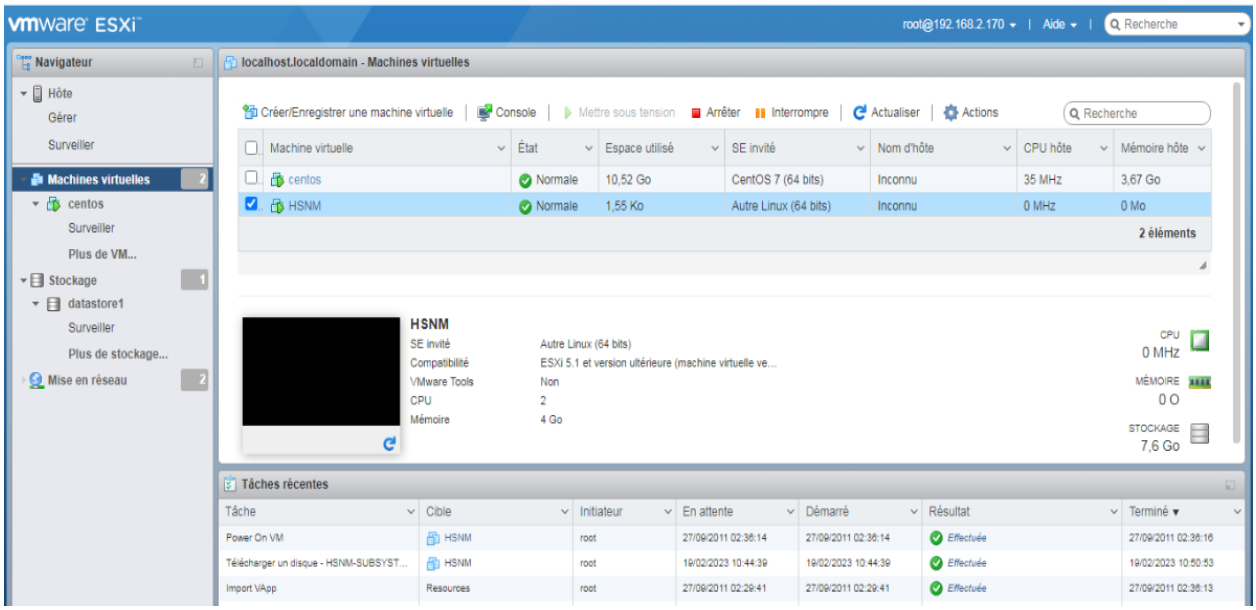


Figure III.9: La machine virtuelle HSNM.

11- Nous pouvons accéder à la plateforme HSNM à partir d'un navigateur web en utilisant les adresses IPv4 suivantes : 192.168.10.10 et 192.168.0.250, comme illustré dans la Figure III.10

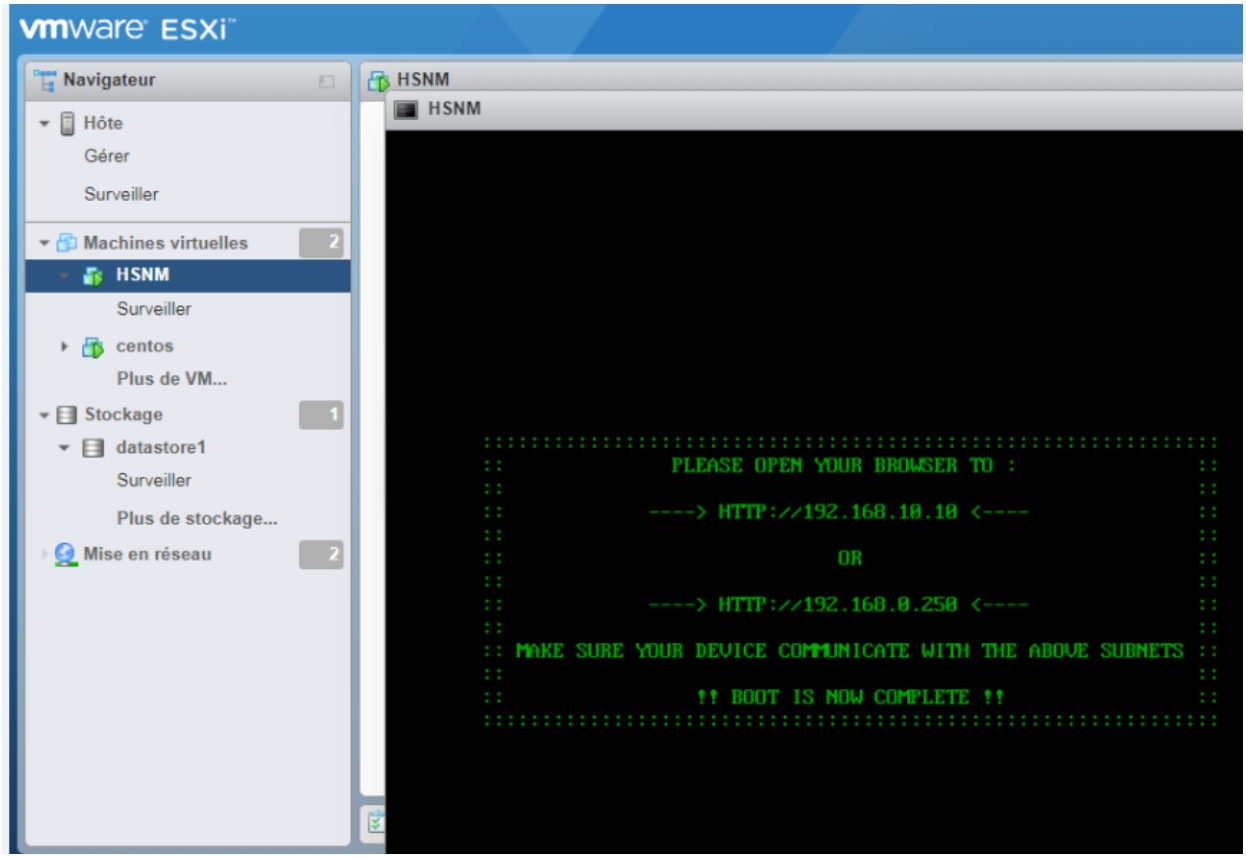


Figure III.10: Les adresses IP de la plateforme de HSNM.

III.5 Conclusion

Dans ce troisième chapitre, nous avons abordé le fonctionnement de la virtualisation. Après la définition de la machine virtuelle (VM) et le rôle de l'hyperviseur ESXI, nous avons procédé à l'installation d'ESXI sur un serveur, suivi de la création d'une machine virtuelle à l'aide de VMWARE ESXI. Enfin, nous avons accédé à la plateforme HSNM HOTSPOT Manager en utilisant une adresse IP spécifique dans un navigateur web.

Dans le prochain chapitre, nous aborderons les configurations nécessaires pour la création d'un HOTSPOT Wi-Fi à l'aide de la plateforme HSNM.

Chapitre IV : Implémentation de la solution HSNM

IV.1 Introduction

Au cours des trois chapitres précédents, nous avons présenté tout d'abord les différents types de réseaux sans fil. Ensuite, nous avons exploré la technologie Wi-Fi ainsi que les HOTSPOTS. Enfin, nous avons examiné les outils indispensables pour mettre en œuvre la solution HSNM.

Dans ce chapitre, nous allons effectuer la configuration des paramètres système. Nous débuterons par ajuster les paramètres en fonction de nos besoins spécifiques, en déterminant les produits disponibles (gratuits, partiellement gratuits ou payants), les revendeurs (Reseller), les gestionnaires (Manager), les domaines, les passerelles (Gateway), les annonceurs et les campagnes publicitaires.

Ensuite, nous procéderons à la création des « TEMPLATES ». En effet, lorsque les utilisateurs se connecteront à une passerelle, ils seront redirigés vers un portail d'accueil personnalisé, éventuellement avec des éléments graphiques, où ils pourront accéder aux applications disponibles, s'inscrire ou s'authentifier en utilisant la méthode d'authentification préalablement définie.

Enfin, nous procéderons à la configuration des passerelles (Gateway) et des points d'accès en suivant le guide de configuration approprié.

IV.2 Identification des composants matériels

IV.2.1 Point d’accès (AP)

Un point d'accès est un périphérique qui crée un réseau sans fil local ou WLAN, habituellement dans un bureau ou dans un grand bâtiment. Un point d'accès se connecte à un routeur câblé, un commutateur ou un concentrateur par câble Ethernet ; il retransmet le signal Wi-Fi vers une zone désignée.

Les points d'accès peuvent fonctionner dans différents modes, tels que le mode point d'accès, le mode répéteur ou le mode pont, et ils peuvent prendre en charge différentes normes sans fil, en fonction des besoins du réseau [29] ; La figure IV.1 montre un modèle de point d'accès.

Figure IV.1: Point d'accès [29].

IV.2.2 Switch

Le Switch est un composant central du réseau local, car il permet aux ordinateurs et autres appareils de communiquer entre eux en acheminant les paquets de données directement entre les appareils connectés. Contrairement à un concentrateur qui envoie tous les paquets de données à tous les appareils connectés, le commutateur ne transmet que les paquets de données destinés à un appareil spécifique[30].

Un Switch transfère les trames de données en conservant un tableau indiquant quelles adresses MAC (Media Access Control) ont été observées et sur quel port du commutateur ; La figure IV.2 montre la table MAC dans un Switch.

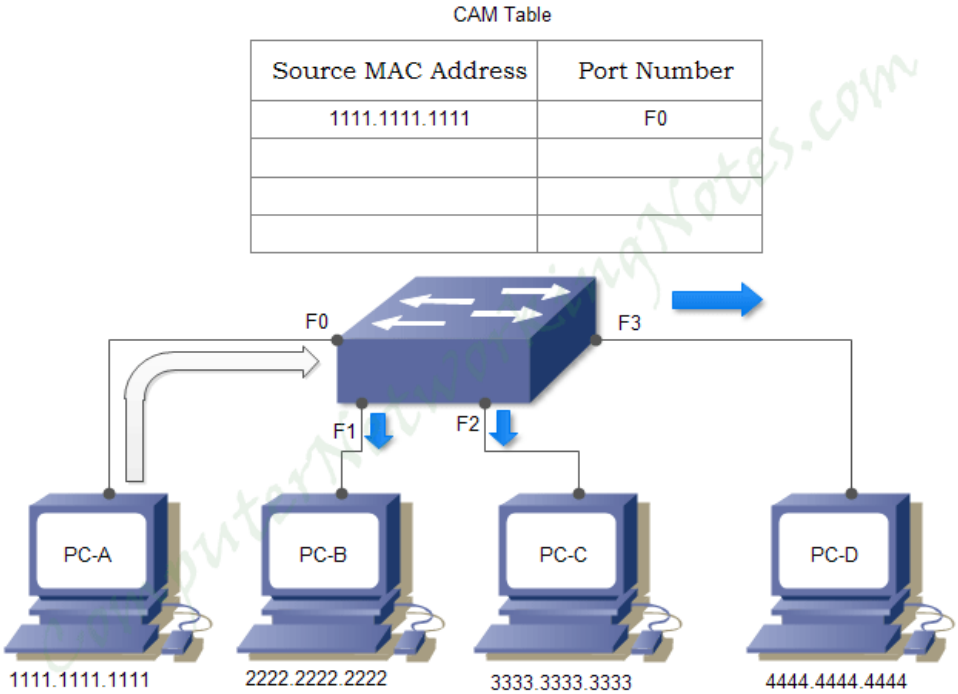


Figure IV.2: Table MAC d'un Switch [31].

IV.2.3 Routeur

Un routeur est un dispositif utilisé dans les réseaux informatiques pour diriger le trafic des données entre différents réseaux. Il s'agit essentiellement d'un appareil qui connecte plusieurs appareils ou réseaux informatiques et permet le transfert de données entre eux.

Dans ce travail, nous avons utilisé un routeur de la marque MIKROTIK. Ce dernier fonctionne sur un système d'exploitation appelé RouterOS. Il s'agit d'un système d'exploitation riche en fonctionnalités qui offre des capacités avancées de routage, de pare-feu et de gestion de réseau[32] ; la figure IV.3 montre le routeur MIKROTIK utilisé .

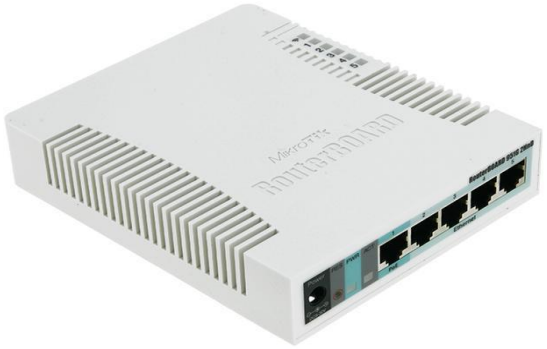


Figure IV.3: Routeur MIKROTIK[33].

IV.2.4 Modem

Un modem est un dispositif utilisé pour établir une connexion entre un réseau informatique et un réseau de communication externe, tel que le réseau Internet. Le nom "modem" est en réalité une contraction des termes "modulateur" et "démodulateur", qui sont les principales fonctions du dispositif[34] ; La figure IV.4 présente le modem TP Link.

Figure IV.4: modem TP Link.[35].

IV.2.5 Le serveur

Le serveur utilisé a les caractéristiques citées dans le tableau IV.1.

Caractéristiques	
Processeur	2.4 GHz
Mémoire vive	2 Go
Carte réseaux	2 cartes réseaux Ethernet
Disque dur	320 Go

Tableau IV.1: Caractéristique du serveur**.**

IV.3 Topologie utilisée

Le schéma suivant nous montre comment les différents équipements sont raccordés dans la topologie utilisée.

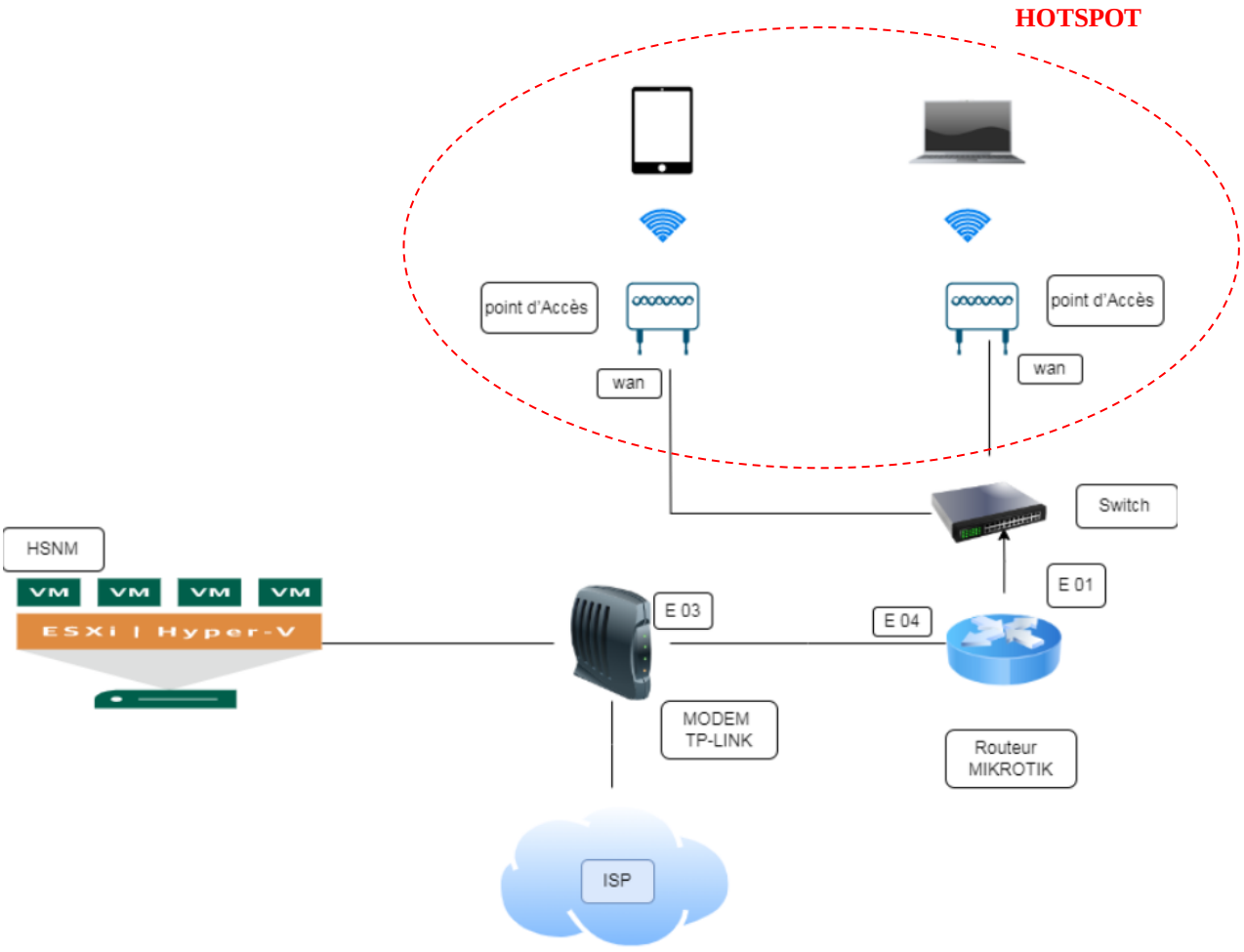


Figure IV.5: Architecture générale de fonctionnement d'un HOTSPOT

IV.4 Configurations de HSNM

IV.4.1 Configuration de la structure de branches

HNSM est fourni avec une structure de branches existante (Reseller, Manager, Domain, Gateway).

- **Reseller**

Ils sont les revendeurs des services proposés par HSNM et gèrent commercialement les régisseurs et les annonceurs.

Le revendeur a accès via ses propres informations d'identification et est autorisé à afficher uniquement ses propres données. Il n'a pas de connexion à la configuration du système ni aux données des autres revendeurs.

- **Manager**

La personne qui héberge physiquement les passerelles dans ses sites, espaces ou zones. Le gestionnaire a accès au système par le biais de ses propres identifiants et ne peut consulter ou modifier, si cela est autorisé, que ses propres données.

Il n'a pas accès à la configuration du système ni aux données des autres gestionnaires ou revendeurs.

Le gestionnaire peut également gérer ses propres campagnes publicitaires qui cibleront les utilisateurs de sa passerelle.

- **Domain**

Les domaines regroupent plusieurs HOTSPOTS qui partagent les mêmes méthodes d’authentification, noms d'utilisateur et mots de passe. Cela est particulièrement Pratique dans le cas où les utilisateurs finaux peuvent utiliser Les mêmes identifiants. C’est également à ce niveau que nous sélectionnons les méthodes de connexion au Service HOTSPOT pour les utilisateurs, telles que par SMS, enregistrement manuel, Auto enregistrement, connexion via les réseaux sociaux, etc. De plus, nous Déterminons les produits disponibles pour les utilisateurs.

- **Gateway**

Les passerelles HGW sont des équipements placés entre le réseau du point d’accès et Internet, elles acheminent les demandes anonymes des Utilisateurs vers le portail d'accueil ou la page de connexion pour L’enregistrement ou l'authentification.

La création de cette structure de branches est réalisée en suivant les étapes suivantes :

Étape 1 : Nous avons mis en place le revendeur (Reseller) en effectuant les actions suivantes :

Dans le menu déroulant Système, nous avons sélectionné l'option "Ajouter un revendeur (Reseller)".

Ensuite, nous avons saisi les informations requises et cliqué sur le bouton Enregistrer situé en haut à droite de la page ; La figure IV.6 illustre le processus de création du revendeur

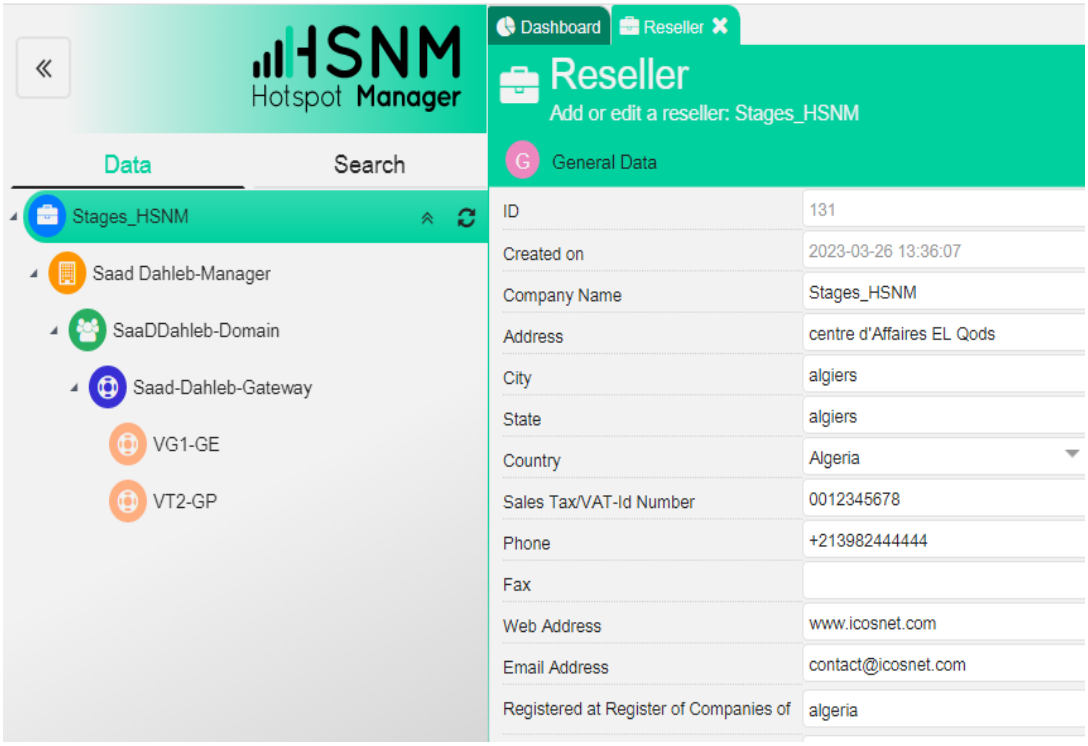


Figure IV.6 : Création de revendeur « Reseller ».

Étape 2 : Dans le menu déroulant Revendeur (Reseller), nous avons sélectionné l'option "Ajouter un gestionnaire (Manager)".

Ensuite, nous avons saisi les informations nécessaires et cliqué sur le bouton enregistrer situer en haut à droite de la page, tel qu'illustré dans la figure IV.7.

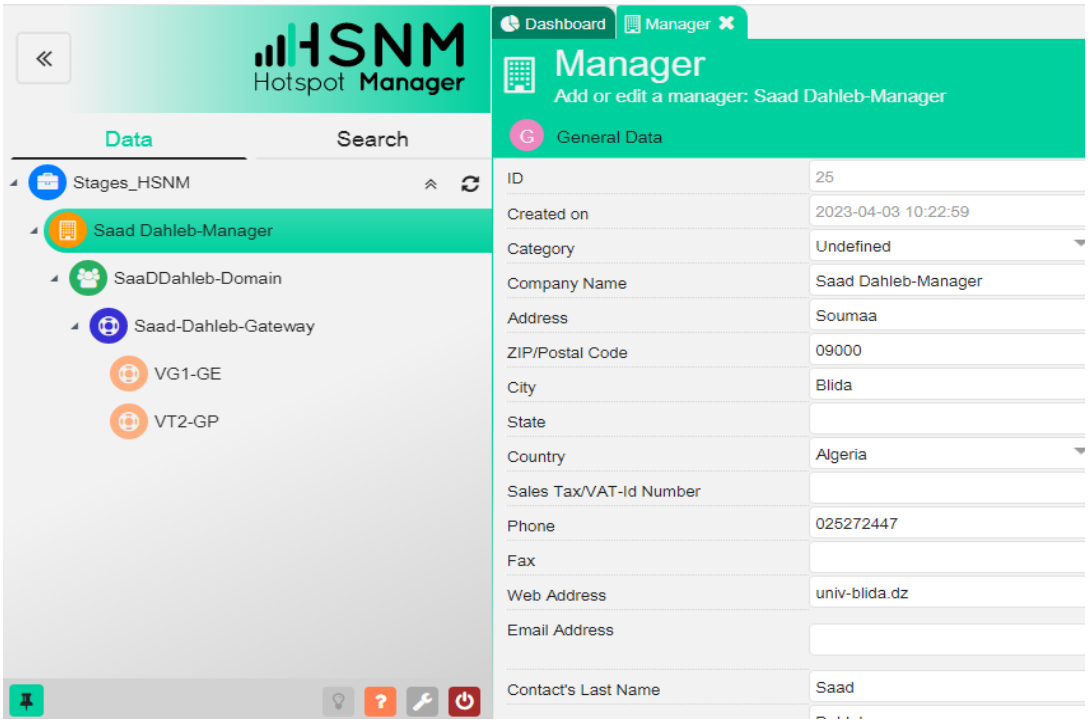


Figure IV.7: Création de gestionnaire « Manager ».

Étape 3 : Dans la liste déroulante Gestionnaire (Manager), nous avons sélectionné l'option "Ajouter un domaine (Domain)".

Ensuite, nous avons saisi les informations nécessaires et cliqué sur le bouton enregistré situé en haut à droite de la page. Ceci est illustré dans la figure IV.8.

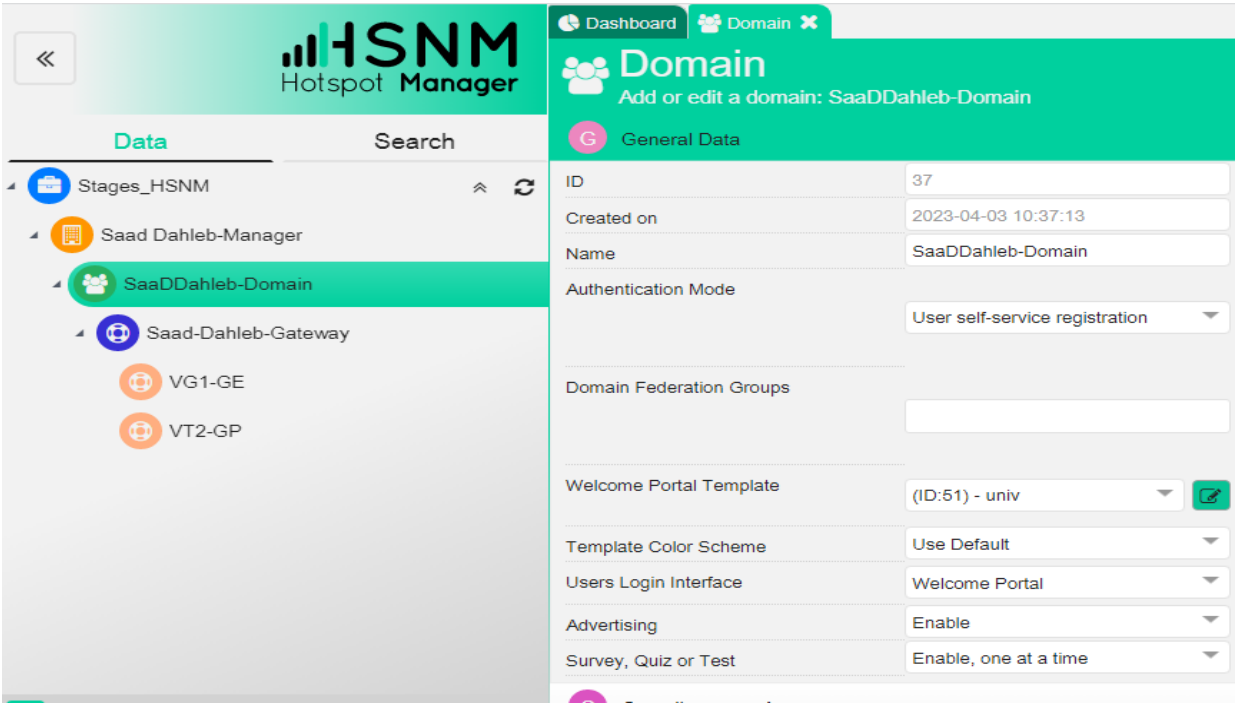


Figure IV.8: création de « Domain ».

Étape 4 : Dans le menu déroulant domaine, nous avons sélectionné l'option "Ajouter une Gateway ".

Ensuite, nous avons saisi les informations nécessaires et cliqué sur le bouton enregistré situé en haut à droite de la page, Vous pouvez voir cette étape illustrée dans la figure IV.9.

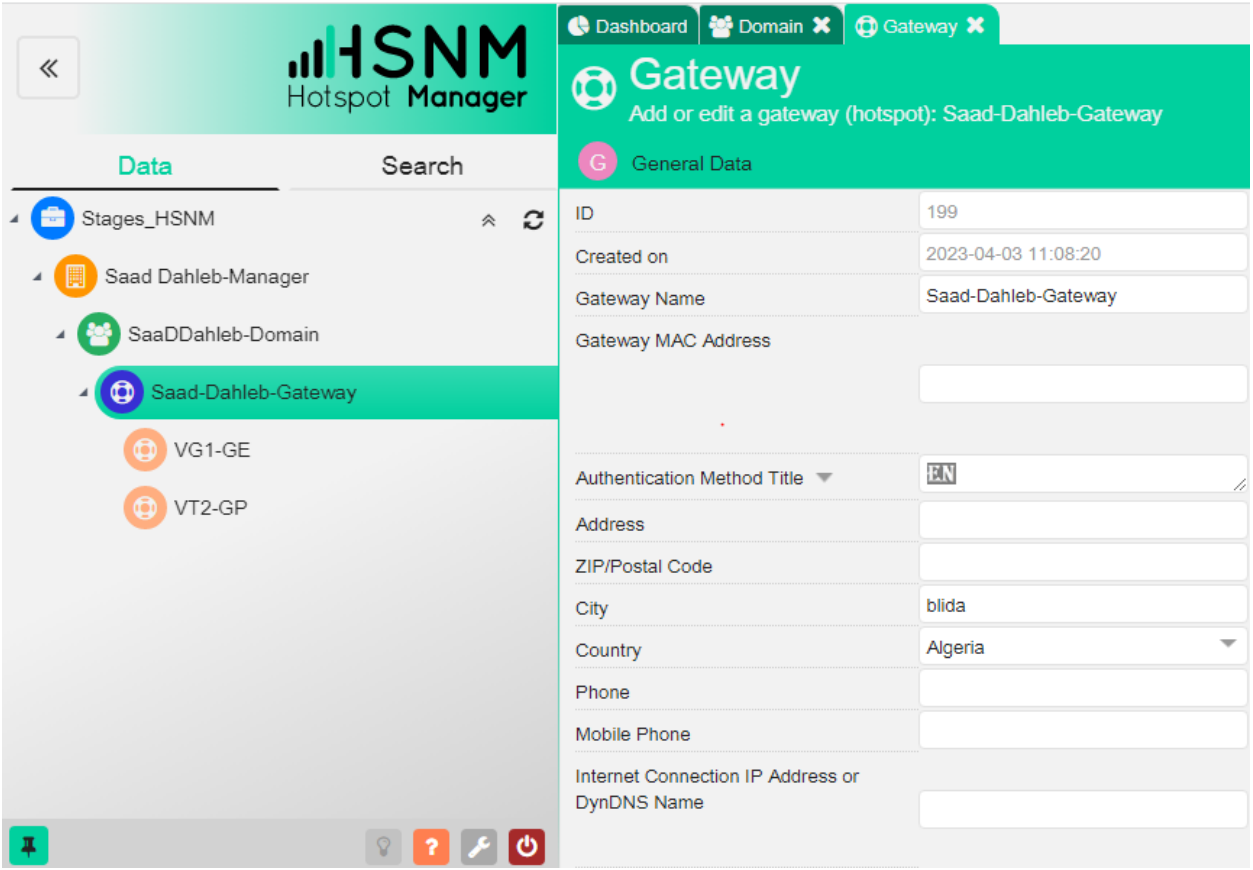


Figure IV.9: Création de « Gateway ».

IV.4.2 Création de portail Captif

Pour créer le portail captif, nous devons d'abord créer une « TEMPLATE ».

IV.4.2.1 Création de « TEMPLATE »

Dans le menu déroulant " Domaine ", nous avons sélectionné l'option "TEMPLATE". Ensuite, nous avons cliqué sur "Créer un TEMPLATE" et saisi les détails requis. Cette étape est illustrée dans la figure IV.10.

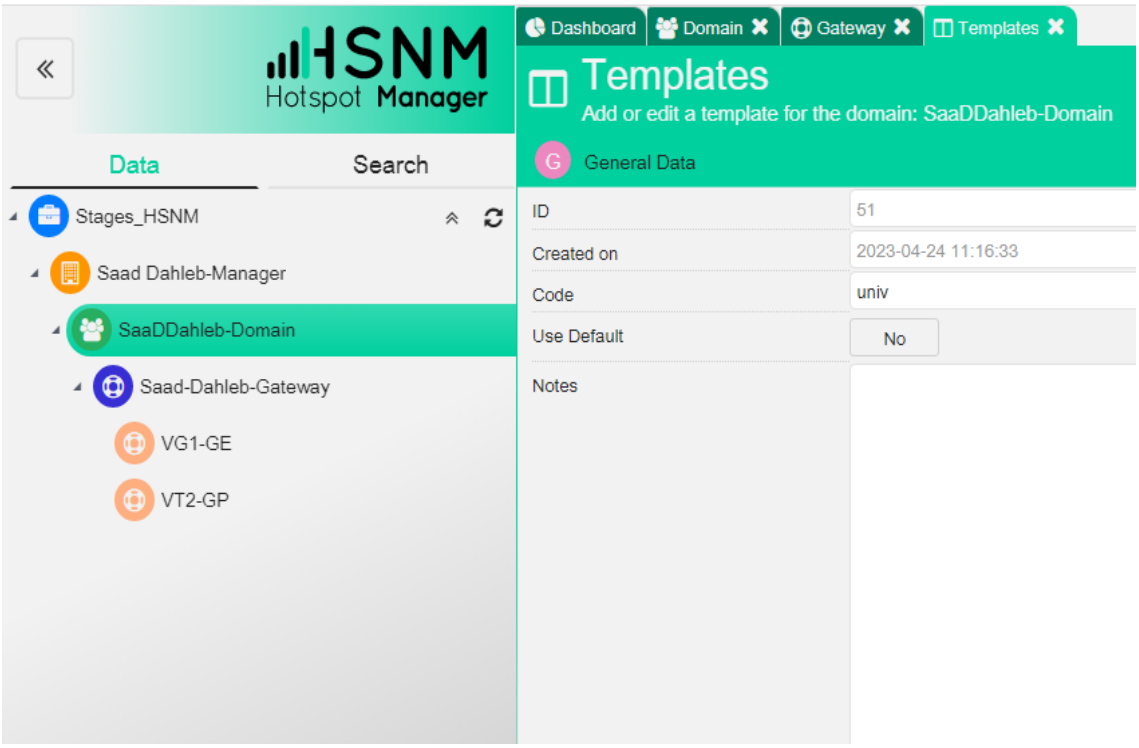


Figure IV.10: Création de « TEMPLATE ».

Nous allons maintenant configurer les paramètres du portail d'accueil, y compris le titre, le sous-titre, le logo personnalisé, l'introduction et les couleurs de fond. Ces éléments sont illustrés dans les figures ci-dessous.

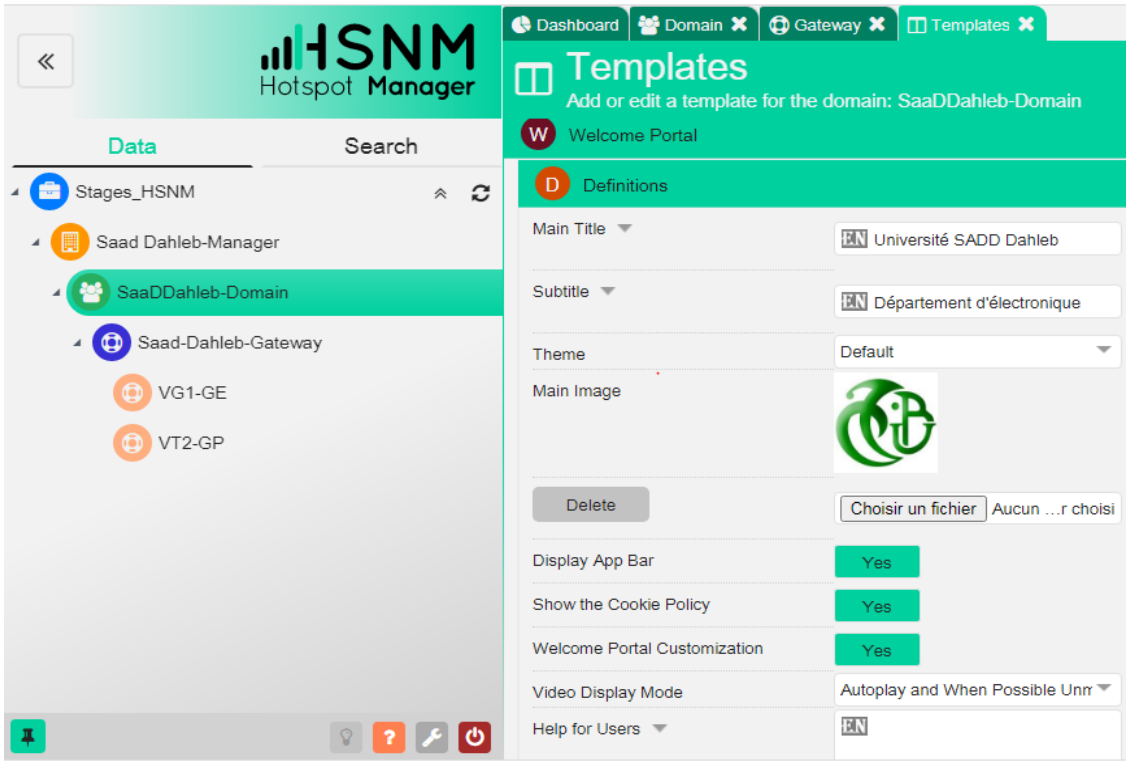


Figure IV.11 : Les paramètres du portail captif.

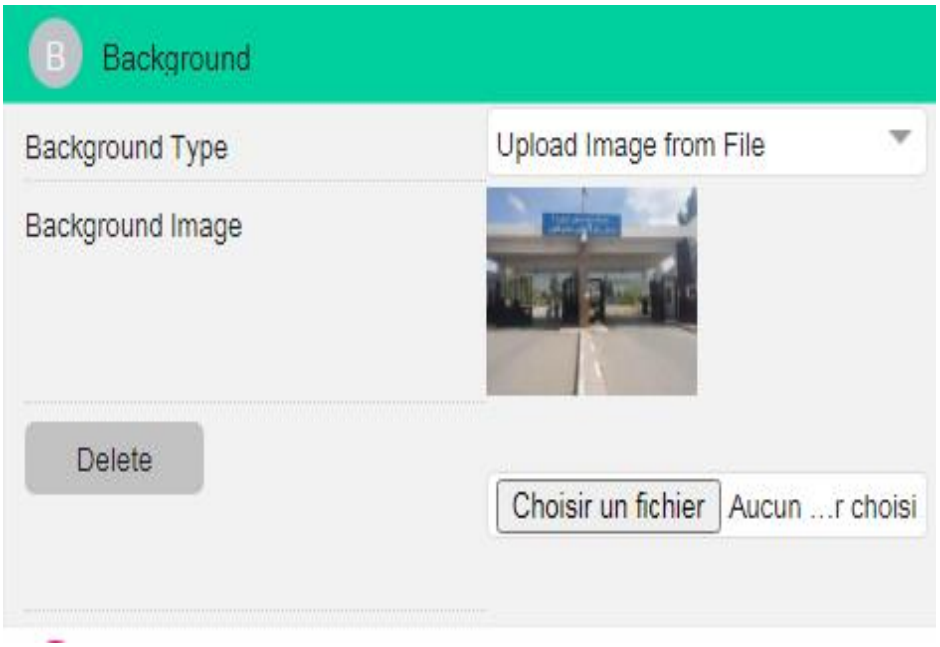


Figure IV.12: Arrière-plan du portail captif**.**

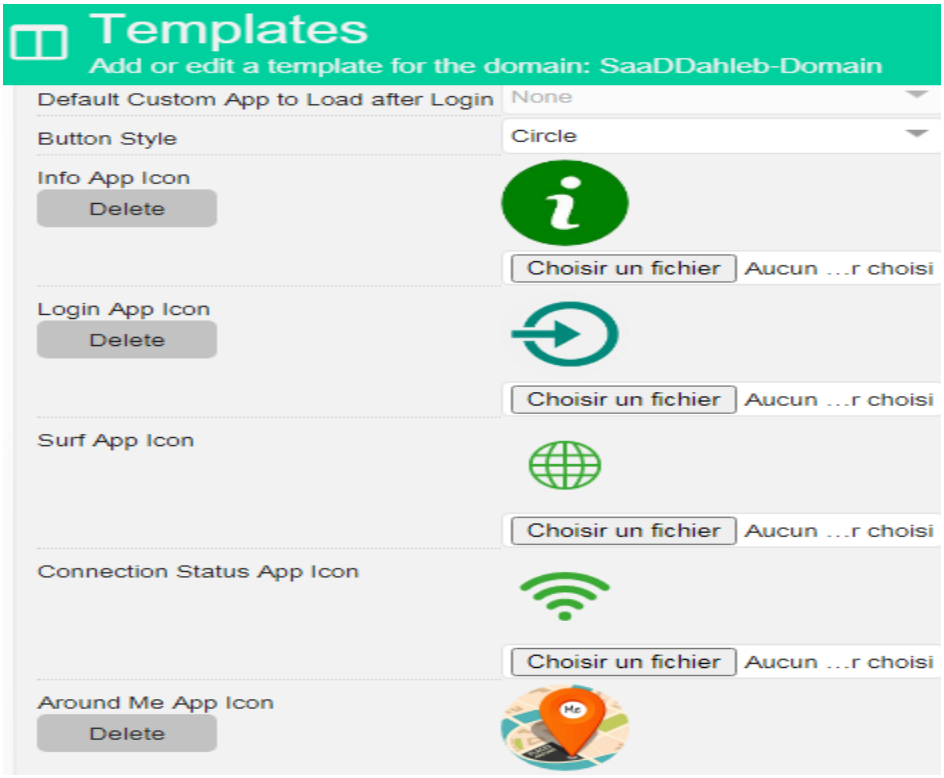


Figure IV.13: Les applications qui chargent à l'ouverture de portail captif.

Figure IV.14: La modification des couleurs de portail captif.

- Dans « Login APPS » du « TEMPLATE », on clique sur « Custom CSS » et on a saisi le code CSS pour la transformation en gris :

#AppContentFormsLoginFormTableSurfButton

{
Background : Grey

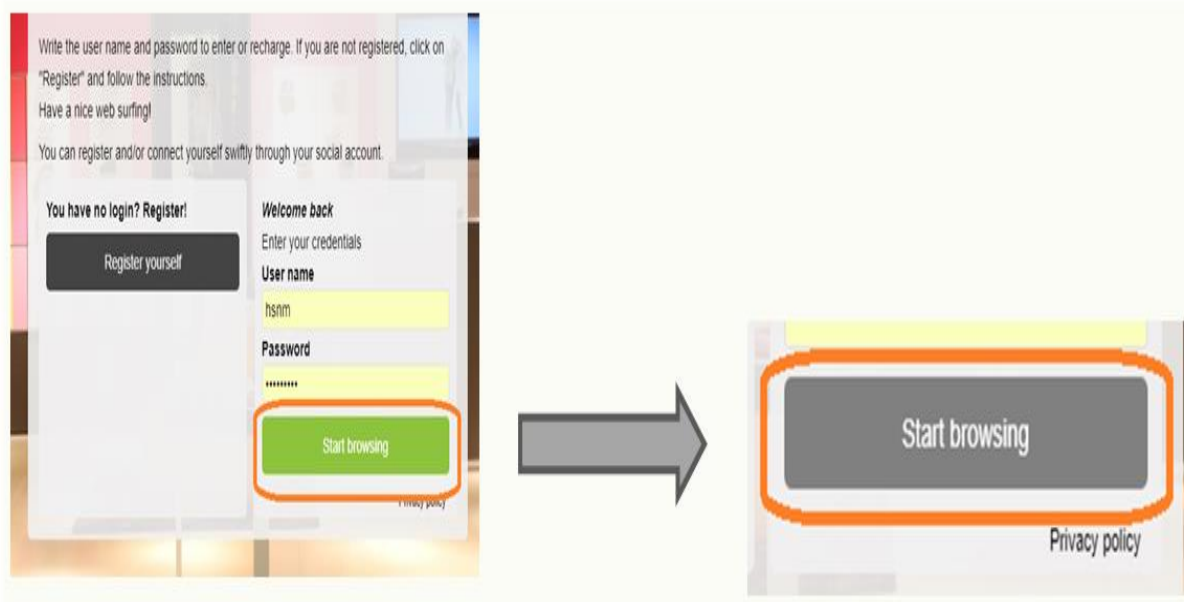


Figure IV.15: Modification de la couleur du bouton « START BROWSING »

Figure IV.16: L'interface de portail captif.

Ensuite, nous devons télécharger ce "TEMPLATE" à la fois au niveau du "Domain" et au niveau de la "Gateway" :

1. Nous avons appliqué le "TEMPLATE" dans le domaine, comme illustré dans la figure IV.17.

Figure IV.17 : Téléchargement le « TEMPLATE » dans le « Domain ».

2. Nous avons appliqué le "TEMPLATE" à la Gateway, comme illustré dans la figure IV.18.

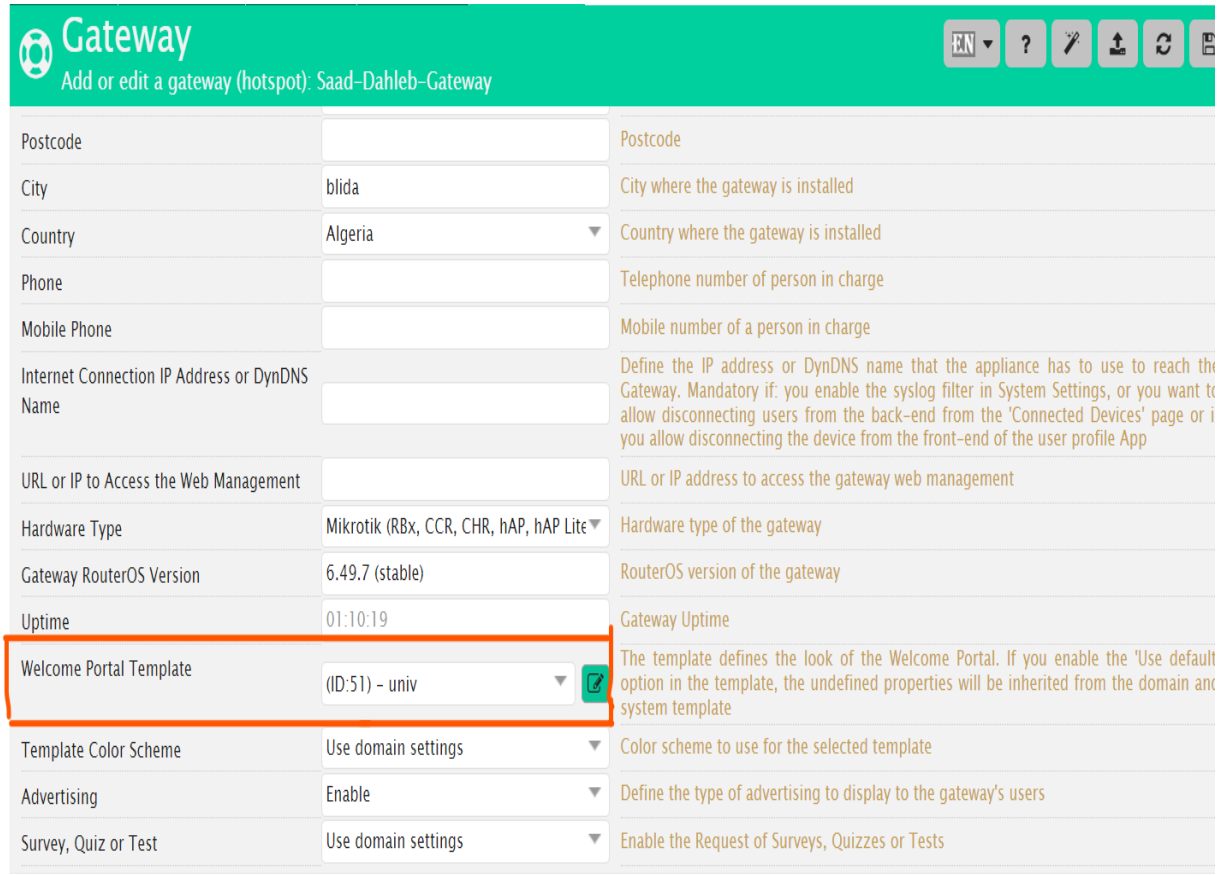


Figure IV.18 : Téléchargement de « TEMPLATE » aux niveaux de « Gateway ».

IV.4.3 Création de produit

Pour créer un produit, nous suivons les étapes suivantes :

Étape 1 : Ajout d'une politique de produit

Nous avons créé la politique de produit au niveau de "Reseller" en cliquant sur "Product Policies" et en remplissant les informations nécessaires, comme illustré dans la figure IV.19.

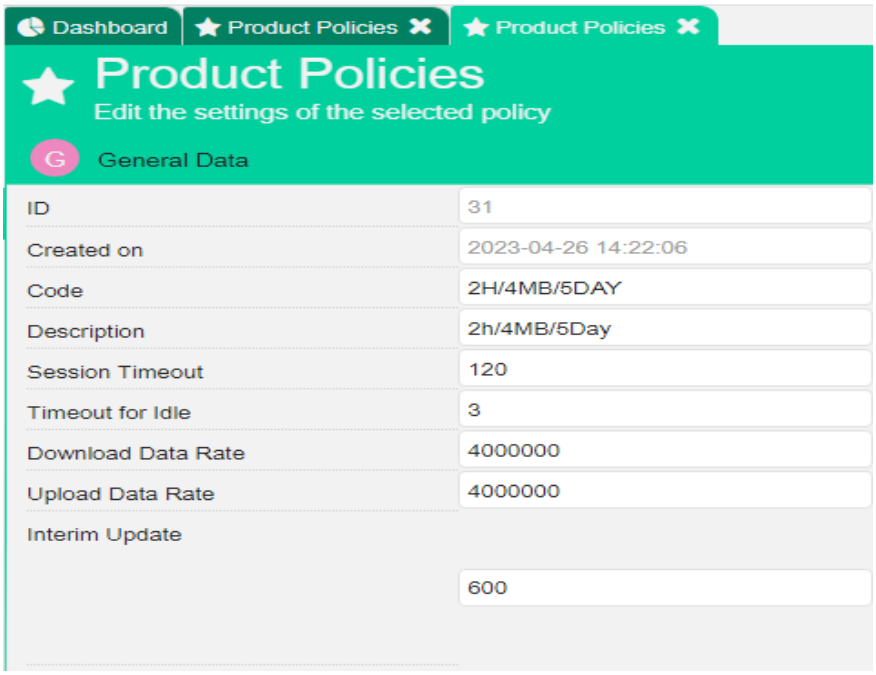


Figure IV.19: La création de « Product Policies ».

Étape 2 : Ajout de produit

Le produit a été créé en sélectionnant l'option "Reseller" et en cliquant sur "Product". Ensuite, nous avons saisi les informations nécessaires, comme illustré dans la figure IV.20

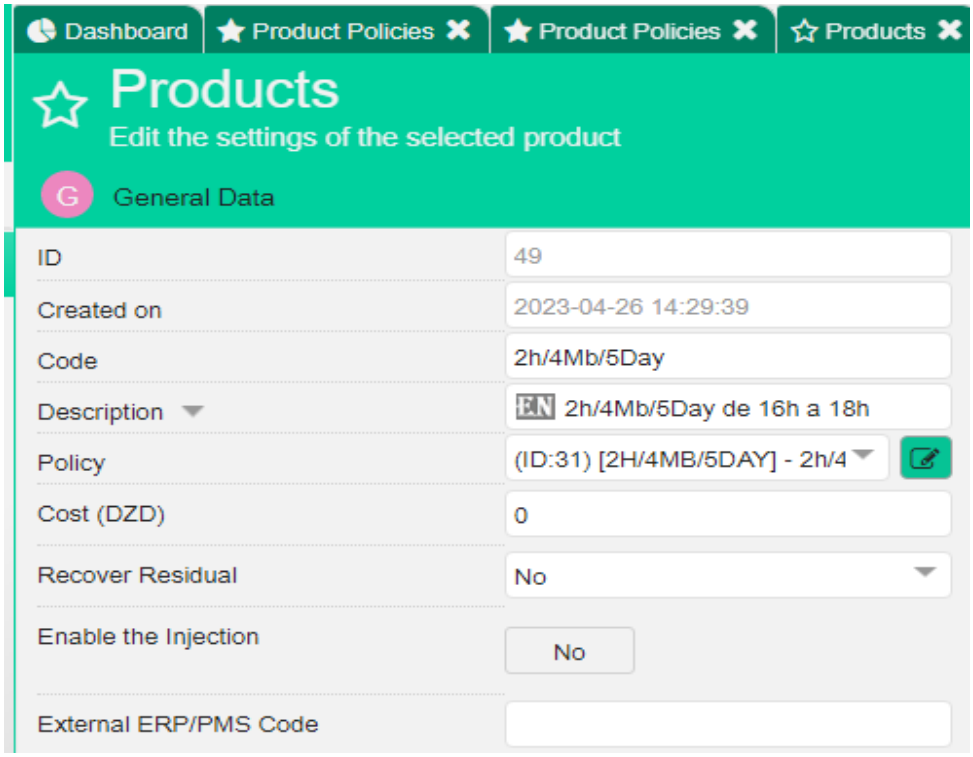


Figure IV.20 : La création de « Product ».

Étape 3 : Téléchargement de « produit »

Il est nécessaire de télécharger le produit au niveau de "Domain", comme indiqué dans la figure IV.21.

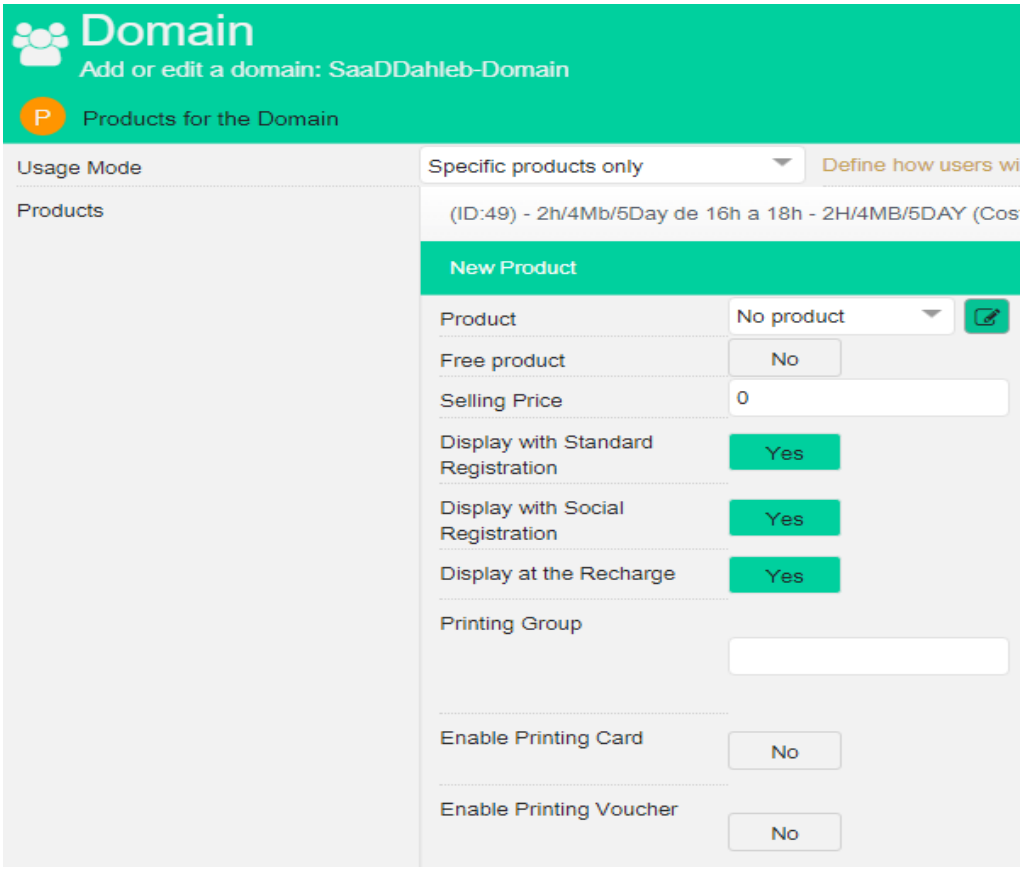


Figure IV.21 : Téléchargement de « Product » aux niveaux du « Domain ».

IV.5 Configuration manuelle de la Gateway MIKROTIK

On peut configurer la Gateway MIKROTIK de deux manières différentes

1- La configuration manuelle de la Gateway MIKROTIK.

2- La configuration automatique de la Gateway MIKROTIK.

Dans notre cas, nous avons opté pour la méthode de configuration manuelle. Nous avons suivi les étapes suivantes

Étape 1 :

Nous avons sélectionné notre Gateway et choisi l'option "Download Gateway Configuration Files" dans le menu déroulant, comme illustré dans la figure IV.22.

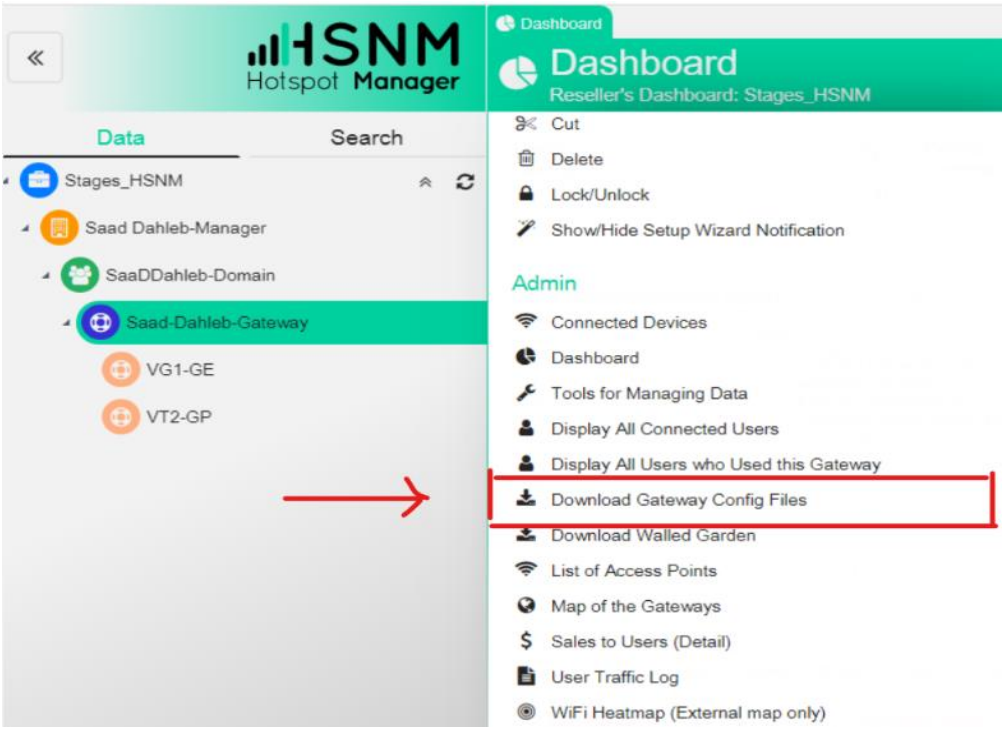


Figure IV.22 : Téléchargement de fichier de configuration.

Étape 2 :

Nous avons décompressé les fichiers et les avons sauvegardés, comme indiqué dans la figure IV.23.

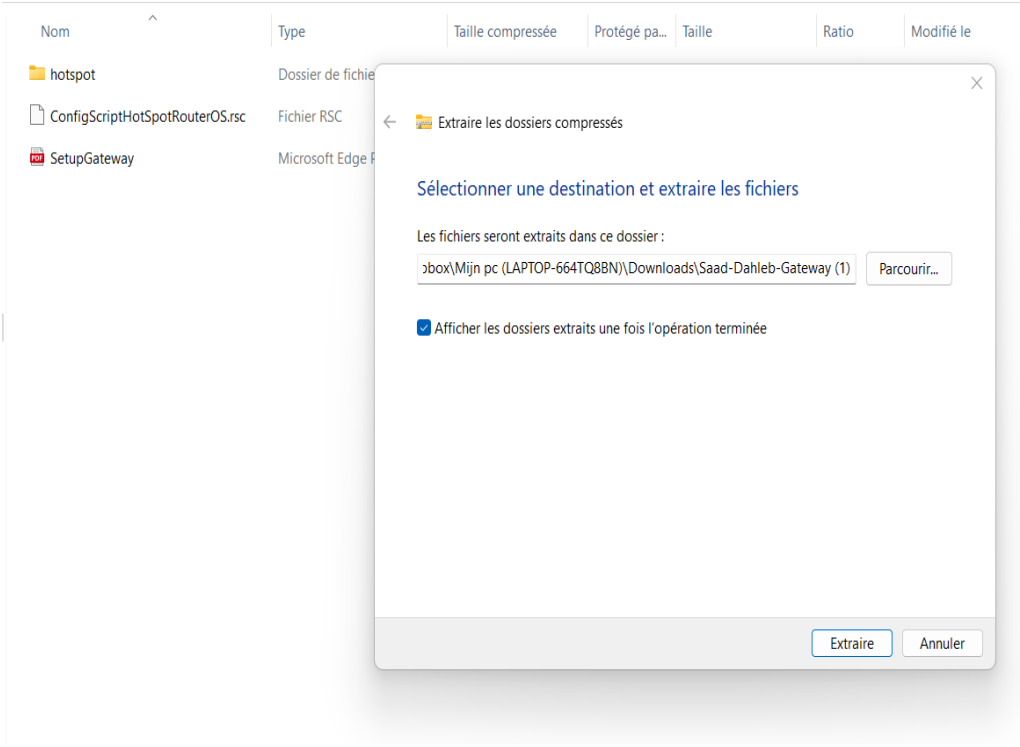


Figure IV.23: Décompression des fichiers de la configuration.

Ensuite, pour télécharger nos fichiers de configuration sur notre routeur mikrotik, nous devons suivre les étapes suivantes :

Étape 1 : on Allume notre routeur mikrotik.

Étape 2 : on a Téléchargé WINBOX à partir du site suivant : https://mikrotik.com/download.

Étape 3 : nous avons Sélectionné notre routeur en cliquant sur son adresse MAC (Login= admin sans mot de passe).

Ensuite, on a cliqué sur le bouton de connexion situé à droite.

Étape 4 : nous avons cliqué sur "Nouveau terminal" et saisi la commande suivante : "system reset-configuration no-defaults=YES". Cette étape est illustrée dans la figure IV.24.

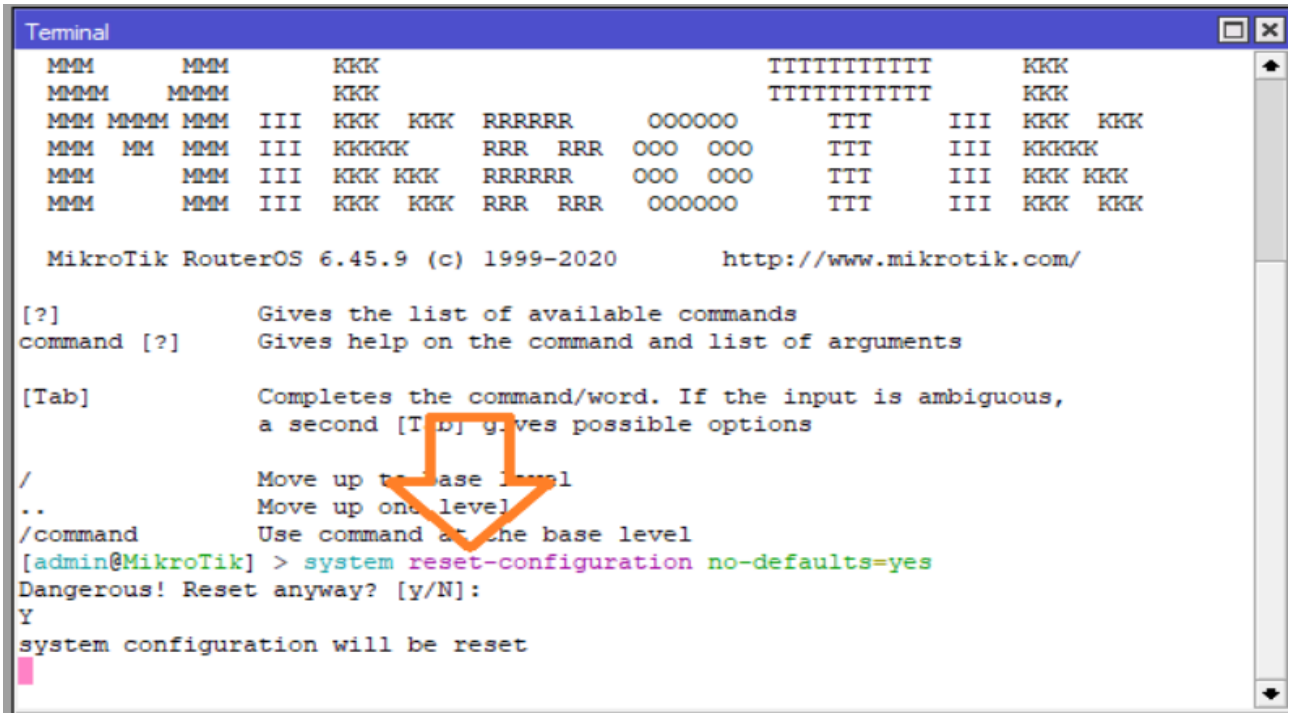


Figure IV.24: Réinitialisation du système.

Étape 5 : il est nécessaire de faire un glisser-déposer du dossier "HOTSPOT" et du fichier "RCS" que nous avons préalablement décompressés. Comme illustrée dans la figure IV.25**.**

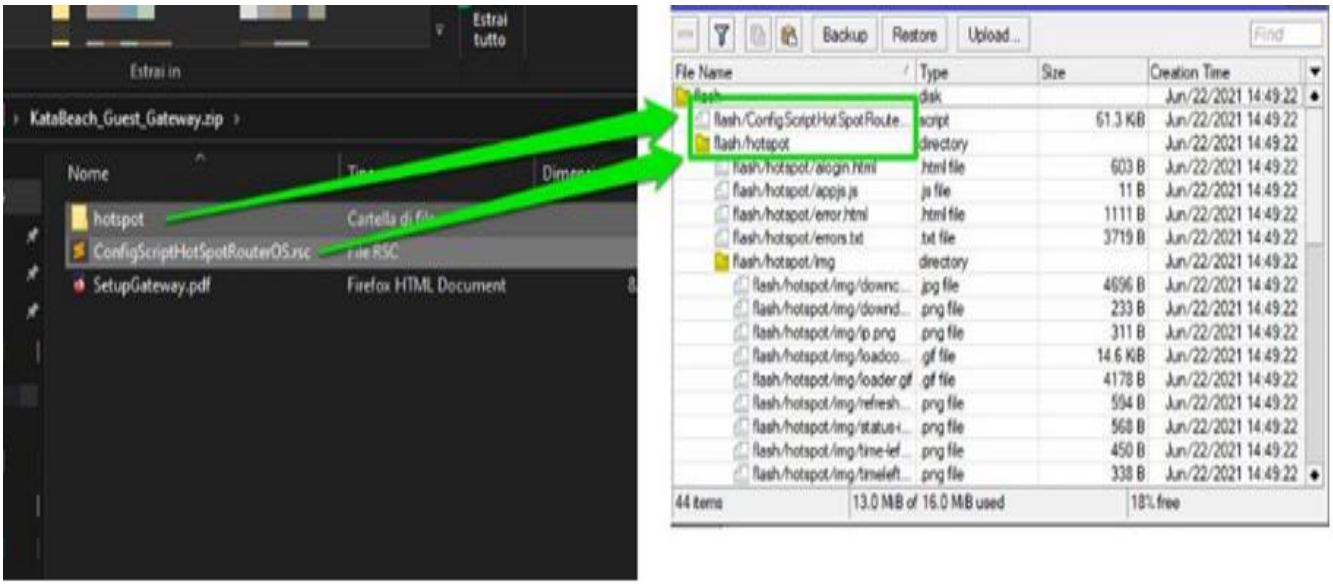


Figure IV.25: Glissement des fichiers décompressé.

Étape 6 : nous avons cliqué sur "New terminal" et saisi la commande suivante : "import ConfigScriptHotSpotRouterOS.rsc". Cette étape est illustrée dans la figure IV.26.

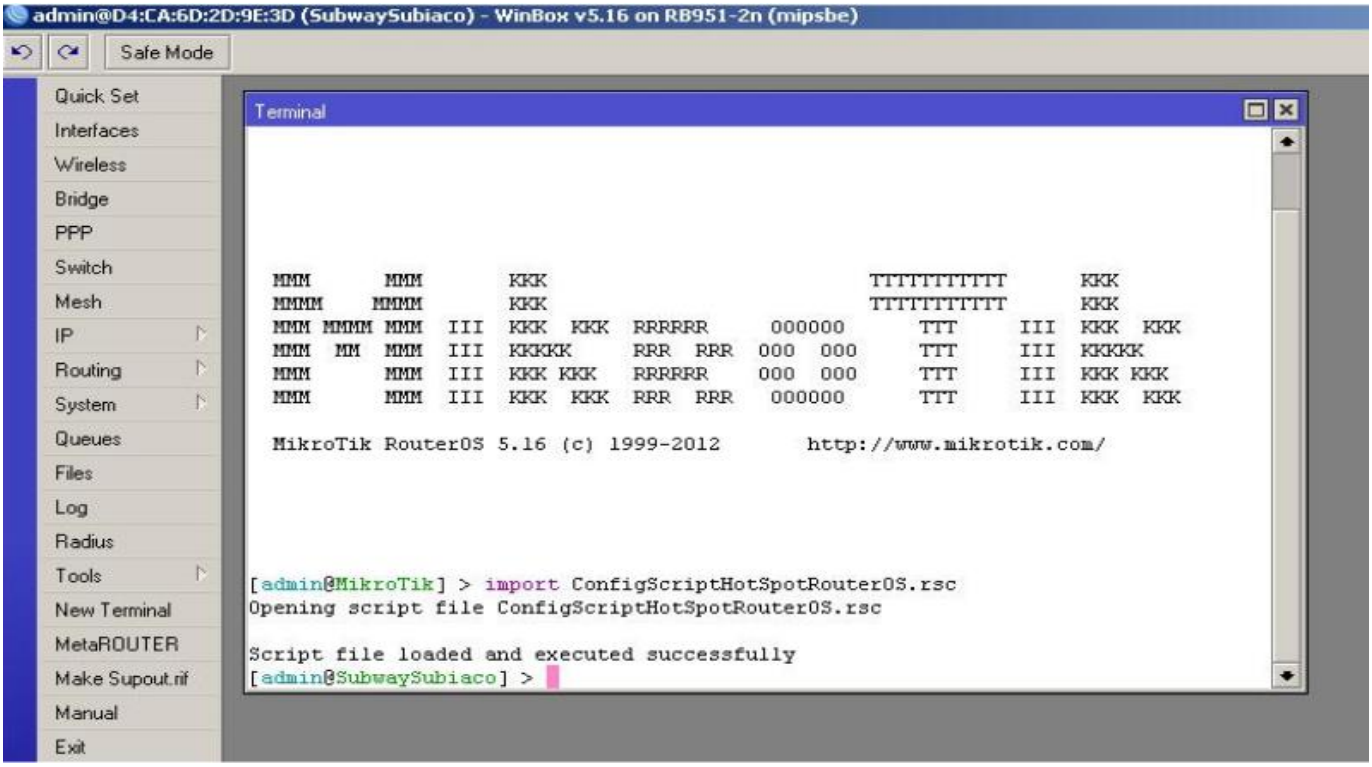


Figure IV.26: Importation de la configuration.

Enfin notre routeur mikrotik est bien configuré.

IV.6 Configuration du point d’accès

Nous avons configuré notre point d'accès en suivant les étapes ci-dessous.

Étape 1 : Pour accéder à notre modem TP-LINK, nous devons ouvrir notre navigateur web et entrer l'adresse '192.168.0.1'.

Étape 2 : Une fois que nous avons saisi le nom d'utilisateur et le mot de passe, nous pouvons configurer notre modem en tant que point d'accès. Comme illustré dans la figure IV.27.

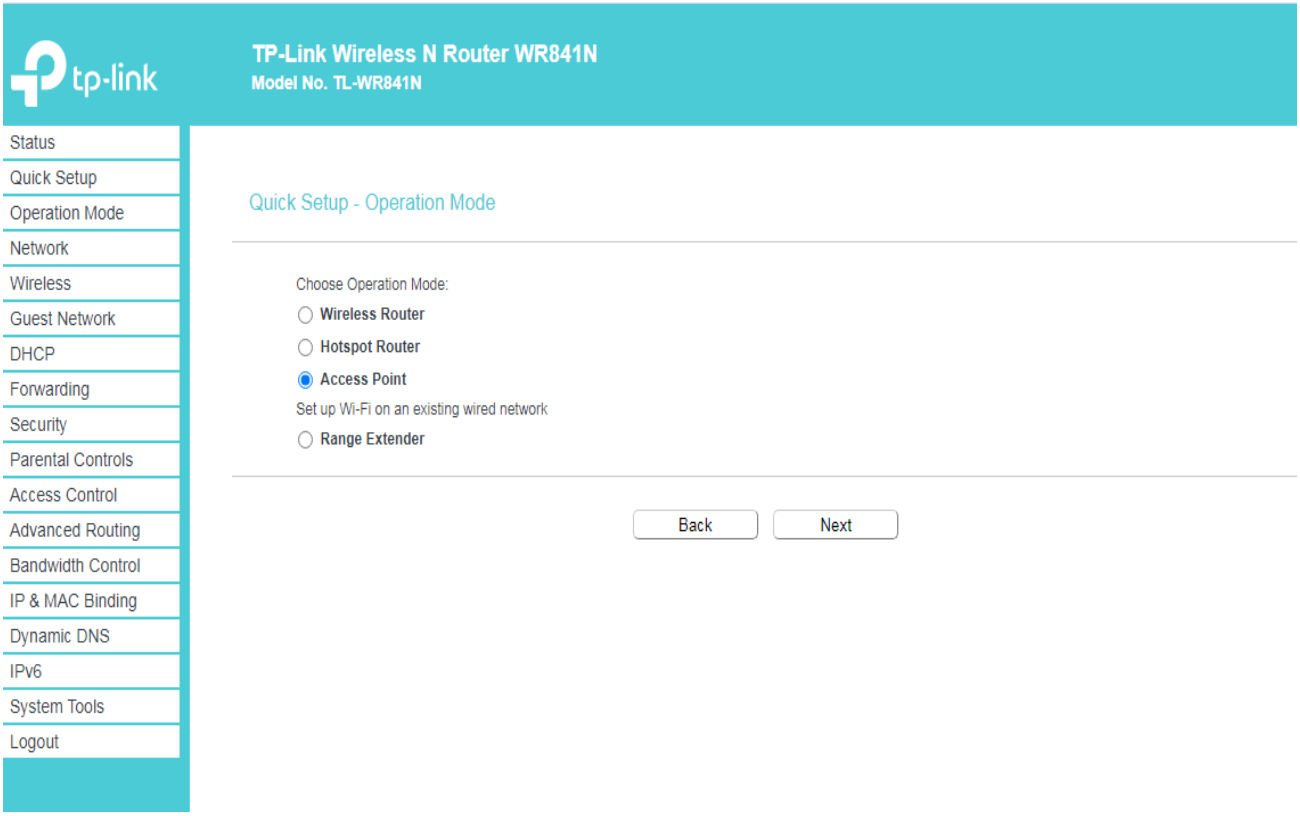


Figure IV.2712: Paramétrage du mode de point d’accès.

Étape 3 : Notre modem a été configuré en tant que point d'accès**.** Conformément à ce qui est illustré dans la Figure IV.28**.**

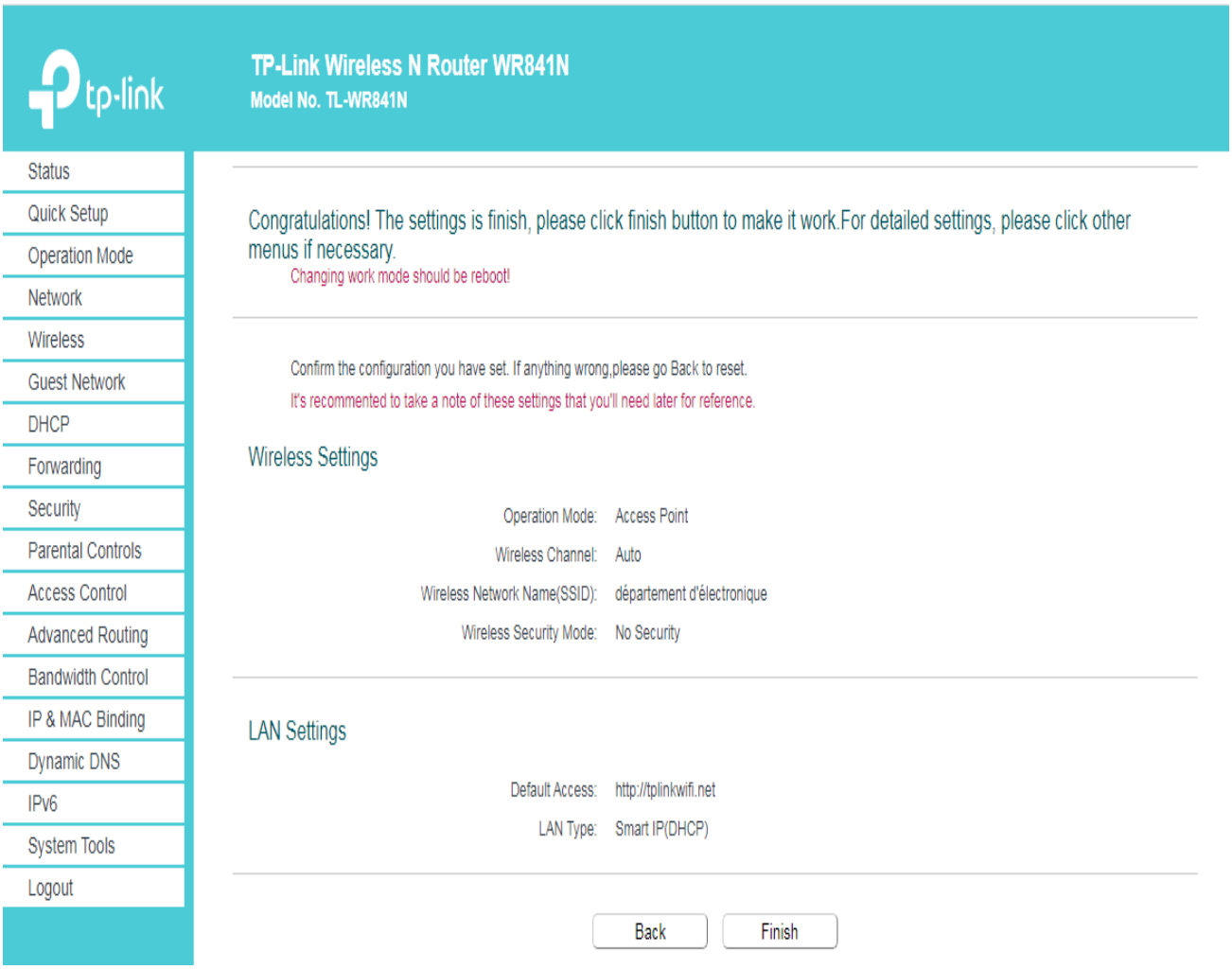


Figure IV.28: Configuration de point d'accès.

IV.7 Conclusion

Ce chapitre se concentre principalement sur l'implémentation des différents composants de la solution, tels que la plate-forme HSNM, la passerelle MIKROTIK, les points d'accès et leur interconnexion. Dans le chapitre à venir et à l'aide d'une approche méthodique, nous allons mettre en œuvre plusieurs scénarios de tests afin d'identifier et de comprendre les caractéristiques essentielles de la solution HSNM proposée. Cette dernière permettra d'enrichir le portfolio des services proposés aux clients d'ICOSNET.

Chapitre V : Tests et validation

V.1 Introduction

Dans ce chapitre, nous aborderons l'étape finale de notre projet, qui consiste à vérifier le bon fonctionnement de notre HOTSPOT. Pour ce faire, nous utiliserons la plateforme HSNM, qui permet de gérer les points d'accès. Nous mettrons en place des tests et des scénarios réalistes afin de mieux comprendre le fonctionnement de notre projet. Cette étape de vérification est cruciale pour s'assurer que notre HOTSPOT fonctionne correctement et répond aux attentes des utilisateurs. En utilisant la plateforme HSNM et en réalisant des tests et des scénarios pertinents, nous pourrons évaluer la performance, la fiabilité et la convivialité de notre approche.

V.2 Les scenarios

Nous avons la possibilité de restreindre et gérer plusieurs HOTSPOTS grâce à la plateforme HSNM, qui offre plusieurs fonctionnalités (limitation de temps, de jour et de bande passante, personnalisation du portail captif, choix de mécanisme d'authentification : SMS, réseaux sociaux, carte voucher…).

Nous avons sélectionné quelques scénarios représentés ci-dessous dans le but de tester la solution proposée.

V.2 .1 Scenario 1

Dans le premier scénario, nous avons mis en place des restrictions de temps, de jours et de bande passante. Les utilisateurs peuvent se connecter pendant 5 jours de la semaine, du dimanche au jeudi, de 16h à 18h, avec un débit de 4 MB. En ce qui concerne le mode d'authentification, nous avons opté pour la connexion par SMS. Plus de détails sur le mode d'authentification par SMS sont donnés dans l'annexe 2.

V.2 .1.1 Etapes de configuration

Etape1 : Nous avons créé ce produit dans le domaine avec les spécifications suivantes : durée de 2 heures, débit de 4 mégabits (MB) et une disponibilité de 5 jours, de 16h à 18h. Les figures ci-dessous illustrent ces informations.

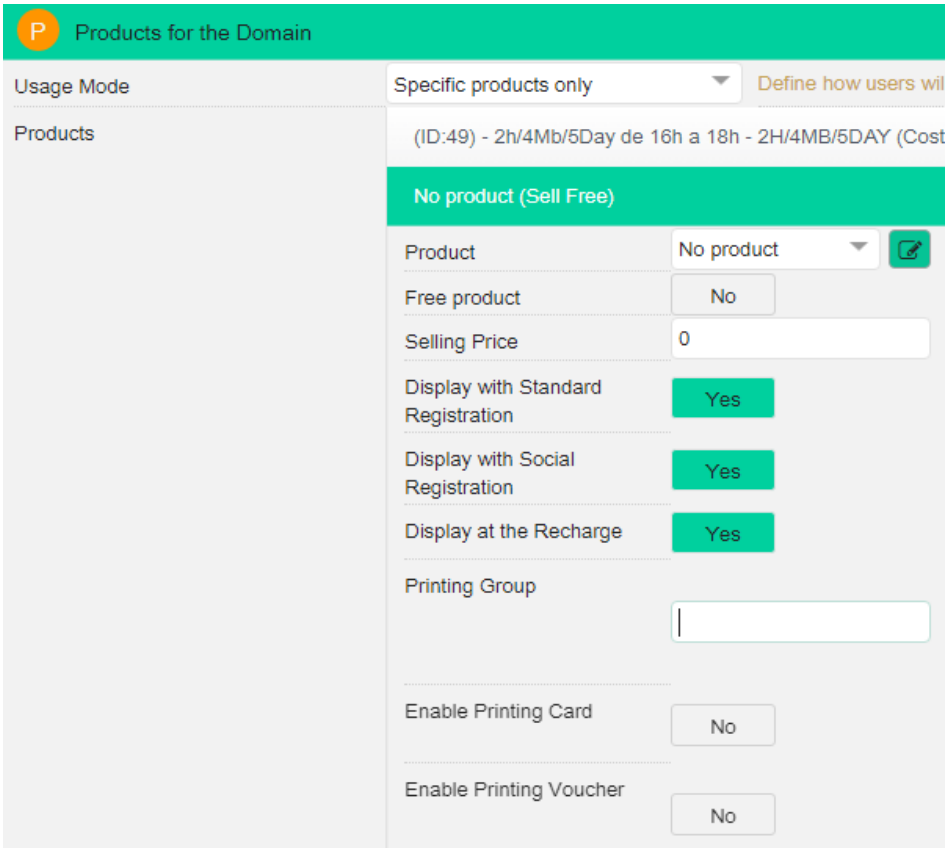


Figure V.1: Création de produit.

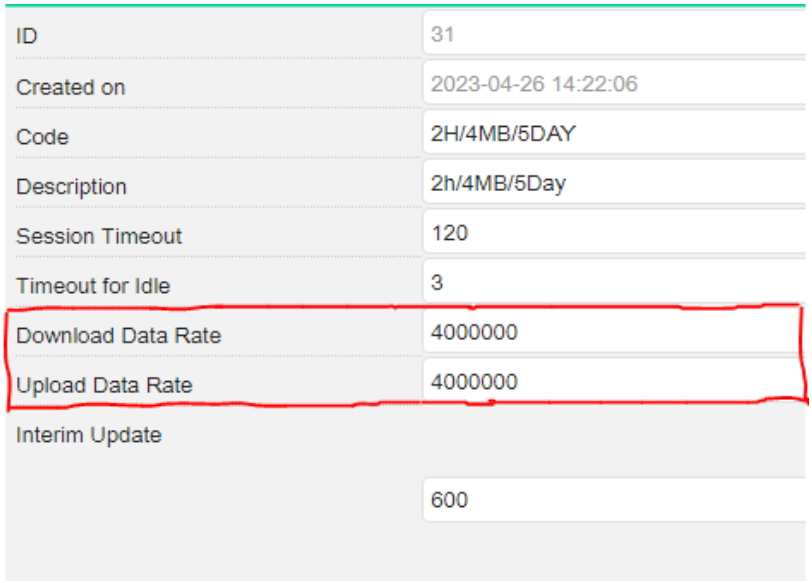


Figure V.2: Limitation de la bande passante.

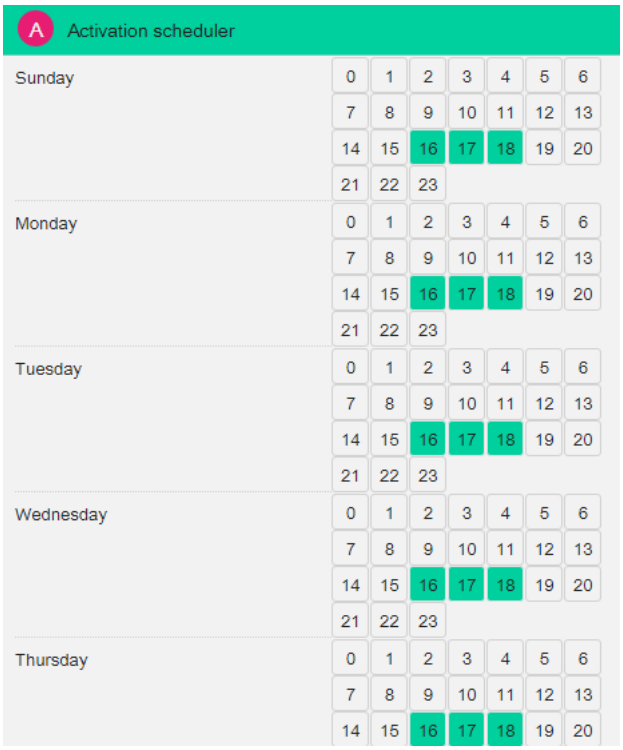


Figure V.3: Limitation des jours et des heures.

Etape2 : Nous avons choisi de mettre en place un mode d'authentification par SMS, en conformité avec les conditions d'exploitation des services d'accès à Internet en Algérie

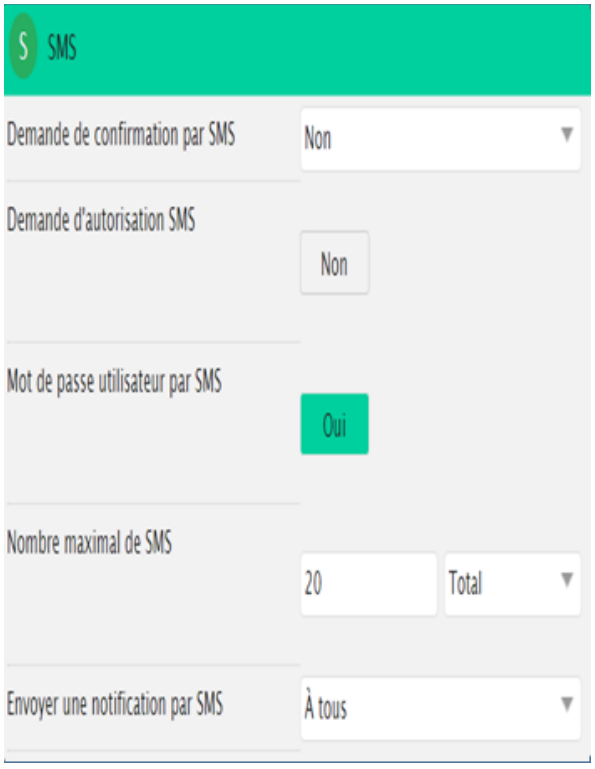


Figure V.4: Le mode d'authentification.

Une fois les étapes de réalisation achevées, nous passons maintenant aux résultats obtenus.

V.2 .1.2 Résultats

Lorsque l'utilisateur souhaite accéder à Internet, il lui est demandé de saisir son numéro de téléphone afin de recevoir un SMS contenant un mot de passe. Voici les figures V.5 et V.6 qui illustrent ce processus.

Figure V.5 : Formulaire de mode d'authentification.

Figure V.6: SMS contenant un mot de passe.

Une fois que nous avons saisi le numéro de téléphone, il nous faut sélectionner le produit que nous avions préalablement déterminé. Comme montre la figure V.7.

Figure V.7: Sélection de produit.

Enfin, nous avons pu accéder à Internet, comme montre la figure V.8**.**

Figure V.8: Accès à l'internet.

Si quelqu'un tente d'accéder à Internet en dehors de son créneau autorisé, il se verra refuser l'accès. Comme montre la figure V.9.

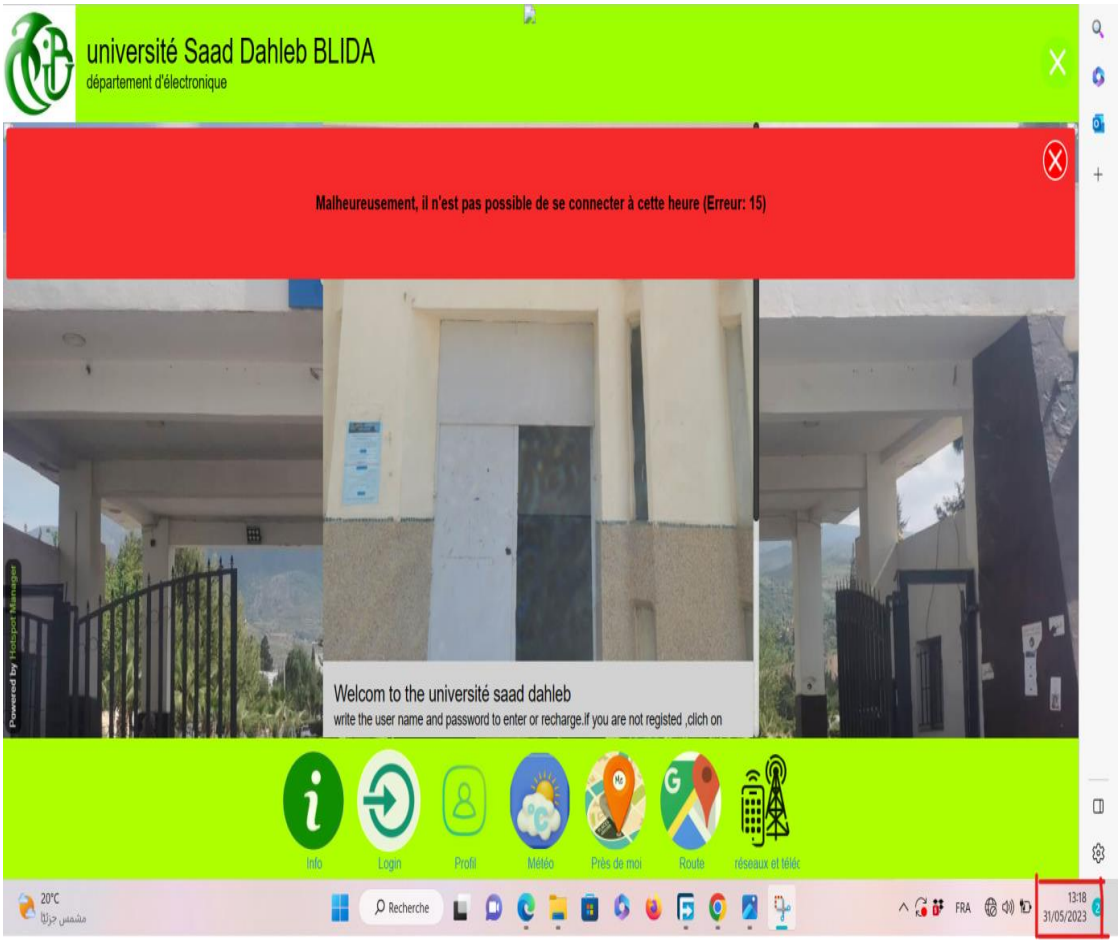


Figure V.9: Le refus d'accès à internet.

Nous avons effectué un test de bande passante afin de vérifier qu'elle ne dépasse pas 4 MB, conformément à la configuration que nous avions précédemment établie via un speed test comme montre la figure V.10.

Figure V.10: Test de la bande passante**.**

V.2.2 Scenario 2

Nous souhaitons désormais créer deux HOTSPOTS pour deux lieux différents. Chaque lieu possède ses propres caractéristiques, donc nous avons mis en place deux passerelles virtuelles. Chaque passerelle virtuelle est équipée d'un portail captif personnalisé

V.2.2.1 Etapes de configuration

Etape 1 : Nous avons mis en place deux passerelles virtuelles et avons attribué un modèle pour chaque passerelle virtuelle, comme illustré dans les figures V.11 et V.12.

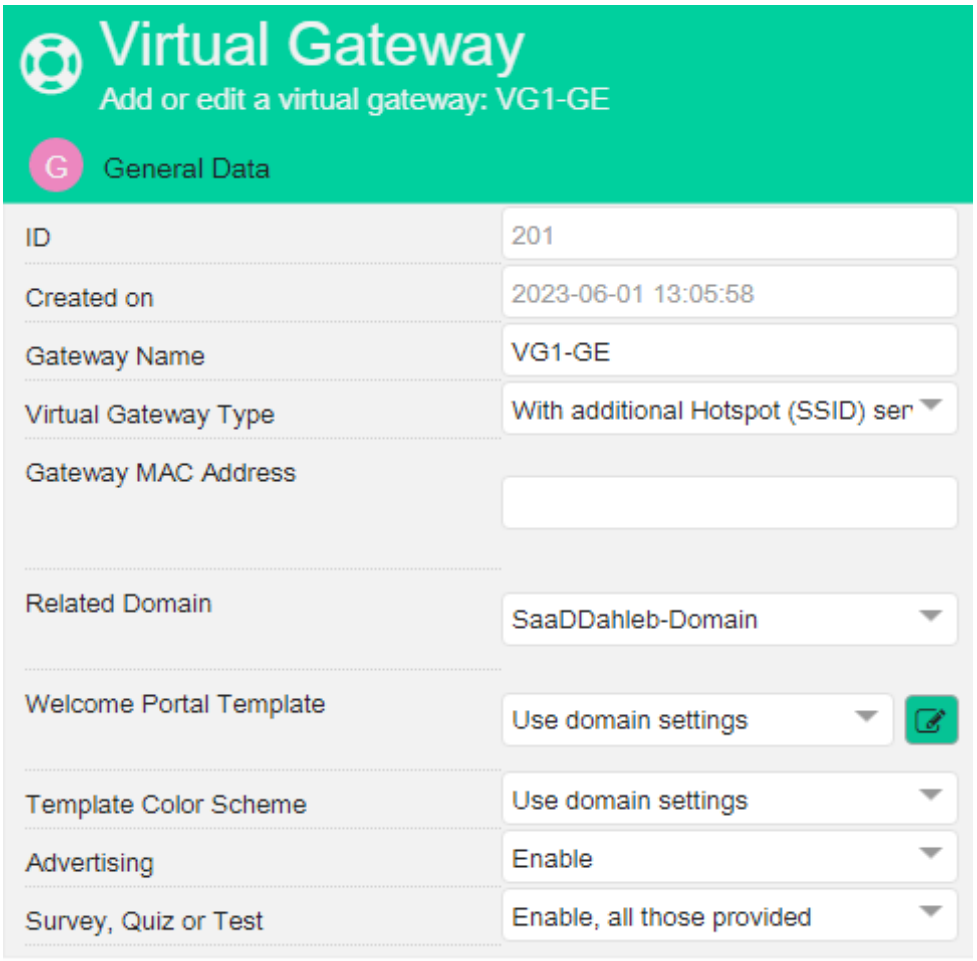


Figure V.11: Création de la première « virtuelle Gateway ».

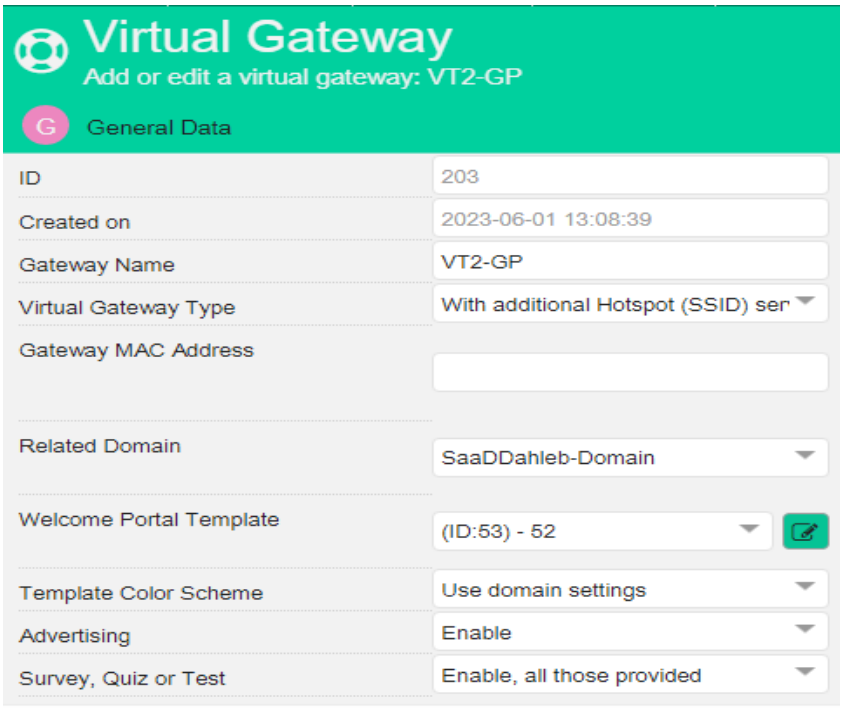


Figure V.12: Création de la deuxième « virtuelle Gateway ».

Etape 2 : Nous avons créé deux VLAN pour chaque passerelle virtuelle, ainsi qu'un réseau d'utilisateurs distincts pour chaque passerelle virtuelle, comme illustré dans les figures V.13 et V.14.

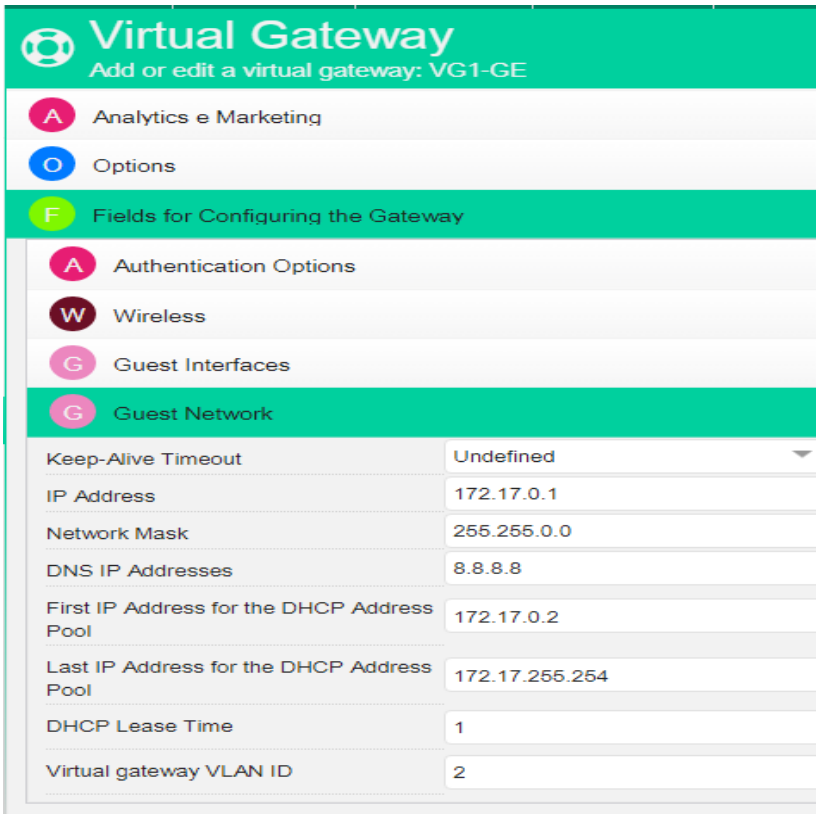


Figure V.13: Réseau d'utilisateur de la première « virtuelle Gateway ».

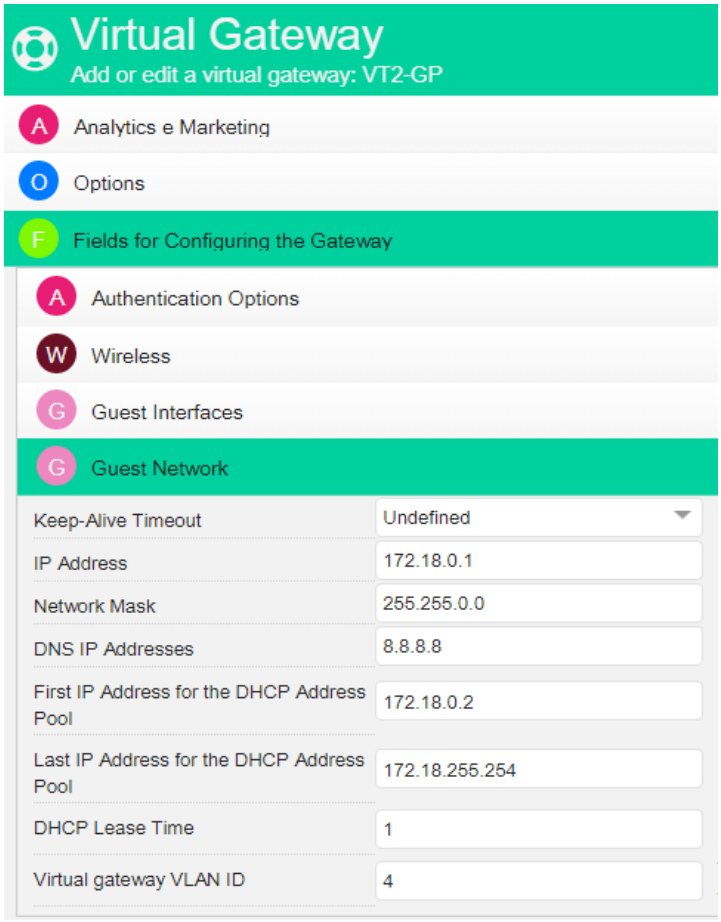


Figure V.14: Réseau d'utilisateur de la deuxième « virtuelle Gateway ».

Etape 3 : Une fois les VLAN créés, Nous avons configuré les deux VLANs (2 et 4) sur le Switch. Le Port G0/5 a été assigné au VLAN 2 pour la Virtual Gateway 1, tandis que le port

G0/7 a été assigné au VLAN 4 pour la Virtual Gateway 2. Ensuite, nous avons Configuré le port G0/9 en mode TRUNK afin qu'il puisse recevoir le trafic des Deux VLANs.

La configuration des VLANS est la suivante :

Switch #show run int G0/5

Building configuration...

Current configuration:

!

Interface GigaEthernet0/5

Description Virtual_GW_1

Switch port pvid 2

Switch #show run int G0/7

Building configuration...

Current configuration:

!

Interface GigaEthernet0/7

Description Virtual_GW_2

Switch port pvid 4

Switch #show run int G0/9

Building configuration...

Current configuration:

!

Interface GigaEthernet0/9

Description TO_MIKRTOIK_LAN

Switch port mode trunk

V.2 .2.2 Résultats

Après avoir achevé les différentes étapes de configuration, nous avons obtenu deux portails captifs distincts pour chaque HOTSPOT. Chacun de ces portails captifs possède ses propres caractéristiques spécifiques, cependant, ils utilisent tous le même mode d'authentification ; les figures V.15 et V.16 représentent les deux portails captifs pour chaque HOTSPOT.

Figure V.15: Portail captif de département d'électronique.

Figure 13: Portail captif de la bibliothèque centrale**.**

V.3 Conclusion

Dans ce dernier chapitre, nous avons abordé les étapes finales de notre projet et présenté les résultats obtenus. Nous avons examiné deux scénarios destinés à l'université Blida 1 incluant des tests et visant à vérifier si le système fonctionne conformément aux spécifications et aux exigences prédéfinies. Les résultats obtenus valident le bon fonctionnement du HOTSPOT proposé basé sur la solution HSNM.

Conclusion générale

L'utilisation de la solution HSNM (HOTSPOT Network Manager) pour l'installation d'un HOTSPOT Wifi peut être un choix bénéfique pour les entreprises et les organisations souhaitant offrir un accès Internet fiable et sécurisé à leurs clients ou invités. HSNM propose un ensemble complet de fonctionnalités qui permettent une gestion et un contrôle faciles du réseau Wi-Fi.

HSNM offre une gamme de fonctionnalités pour gérer la bande passante et le temps de connexion dans les réseaux Wi-Fi. Il permet un contrôle efficace de la répartition de la bande passante en définissant des limites de vitesse pour les utilisateurs, donnant ainsi la priorité aux utilisateurs payants pour des vitesses plus élevées tout en limitant celles des utilisateurs gratuits. De plus, il est possible de définir des limites de temps de connexion, ce qui permet de déconnecter automatiquement les utilisateurs une fois leur temps imparti écoulé. Ces fonctionnalités contribuent à une utilisation équitable du réseau et évitent la monopolisation de la connexion Wi-Fi par un seul utilisateur. En utilisant les capacités de gestion de la bande passante et du temps de connexion d'HSNM, vous pouvez créer des produits Wi-Fi qui améliorent l'expérience utilisateur, permettent de contrôler l'utilisation du réseau et offrent des options de tarification flexibles adaptées aux besoins spécifiques de votre entreprise.

En conclusion, nous sommes convaincus que ce projet contribuera à faciliter l'accès et à approfondir les connaissances des futures promotions d'étudiants sur les HOTSPOTS Wi-Fi. En respectant les réglementations en vigueur en Algérie et en utilisant une méthode d'authentification par numéro de téléphone via des SMS, nous garantissons une connexion sécurisée et un accès facile au réseau Wi-Fi. De plus, l'utilisation de HSNM offre une gamme complète de fonctionnalités pour gérer la bande passante, le temps de connexion et personnaliser le portail captif, améliorant ainsi l'expérience des utilisateurs. Nous sommes impatients de continuer notre travail dans ce domaine et nous espérons que cette initiative inspirera d'autres institutions à adopter des solutions similaires pour offrir une connectivité Wi-Fi optimale et accessible à l'Université de Blida 1 et au-delà.

Bibliographie

[1] Michel Terré "WI-FI" https://easytp.cnam.fr/terre/images/WiFi.pdf (consulté le 8 juin 2023).

[2] « Add wireless network » ; cisco entreprise https://www.cisco.com/c/dam/en/us/support/docs/smb/wireless/cisco-small-business-100-series-wireless-access-points/images/rjs-04122017-addwirelessnetwork(consulté le 8 juin 2023).

[3] Nadia Adrar ;"Les technologies sans fil le Wi-Fi et la Sécurité" ; article ; https://www.memoireonline.com/07/09/2324/m_Les-technologies-sans-fil-Le-Wi-Fi-et-la-Securite1.html.

[4] Monjal-Sfez, « Les réseaux sans fils » article ; publié le 7 Avril 2013 ; http://reseaux-filaire-ou-wifi.over-blog.com/le-wi-fi-correspond-%C3%A0-une-norme-visant-un-certain-type-de-r%C3%A9seau-local-sans-fil.-on-parle-de-wlan-pour-wireless-local-area-network-.-pour (consulté le 8 juin 2023).

[5] Jean-Luc Montagnier," Construire son réseau d'entreprise" ; livre ; https://fntic.univ-ouargla.dz/images/biblio/InfoPDF/578.pdf.

[6] Techno-Science.net, « Wi-Fi : définition et explications », article deTechno-Science.net. https://www.techno-science.net/definition/3915.html (consulté le 8 juin 2023).

[7] http://www.guill.net/view.php?cat=5&arc=3&rsf=4.

[8] Huawei Enterprise « Wi-Fi 6 : rapide, mais à quel point ? » ; article ; publié le 18/08/2022. https://e.huawei.com/fr/knowledge/enterprise-networking/wifi-6-how-fast-is-it.

[9] Paul Mühlethaler « 802.11 et les reseaux sans fil » ; livre. https://www.eyrolles.com/Informatique/Livre/802-11-et-les-reseaux-sans-fil-9782212111545/le 28/08/2002.

[10] Chris Hoffman, "What's the Difference between AdHoc and Infrastructure Mode Wi-Fi? »; article; publié le 22/09/2006; https://www.howtogeek.com/180649/htg-explainswhats-the-difference-between-ad-hoc-andinfrastructure-mode/

[11] Karima Belhadj & Amina Abid " Etude et réalisation d'un réseau WiFi HOTSPOT dans le service public » ; mémoire de fin d'étude ; soutenue en 2012 ; https://www.ummto.dz/dspace/bitstream/handle/ummto/8235/BelhadjKarima_AbidA.pdf?sequence=1&isAllowed=y.

[12] Samir ATHMANI "protocole de sécurité pour les réseaux de capteurs sans fils «; mémoire de magistère ; soutenue le 15/07/2010 ; http://eprints.univ-batna2.dz/189/1/Samir%20ATHMANI.pdf.

[13] « Qu'est-ce qu'un HOTSPOT wifi et comment ça marche », Net Spot entreprise, publié le 26 mai 2021. https://www.netspotapp.com/hardware/fr/wifi-hotspot/ (consulté le 8 juin 2023).

[14] « Google Earth ». https://www3.google.com/intl/fr/earth/ (consulté le 8 juin 2023).

[15] Pablo Sanchez ;« Qu'est-ce qu'un HOTSPOT et quels sont ses types»;article ;https://androidayuda.com/fr/android/que-es/hotspot-que-es-y-tipos/ (consulté le 8 juin 2023).

[16] Manuel, « Les avantages et les risques des HOTSPOT wifi », article, publié le 2 novembre 2019. https://www.vadconext.com/les-avantages-et-les-risques-des-hotspot-wifi/

[17] Margaux Couturier « Comment fonctionne un HOTSPOT ou borne Wifi ? », article, https://www.zoneadsl.com/dossiers/maison-connectee/comprendre-fonctionnement-un-hotspot-ou-borne-wifi.html (consulté le 8 juin 2023).

[18] Mohamed Yassine GACEM & Abdelrezak OUGHLIS " Déploiement d'un réseau sécurisé sans fil Wifi pour un campus universitaire sous un fournisseur d'identité Shibboleth » ; Mémoire de fin d'études ; soutenue en juin 2009 http://repository.enp.edu.dz/jspui/bitstream/123456789/2826/1/GACEM.Mohamed%20Yassine_OUGHLIS.Abdelrezak.pdf

[19] « Administrator Manual », HOTSPOT Manager Wi-Fi ; Manuel de l'administrateur ; https://wiki.hsnetworkmanager.com/?manuale=administrator-manual (consulté le 8 juin 2023).

[20] « Solutions by Industrie - Enterprise WiFi », Cloud4Wi entreprise ; https://cloud4wi.com/by-industry/ (consulté le 8 juin 2023).

[21] « HOTSPOT 2.0 », Cisco Meraki entreprise, publié le 5 octobre 2020 ; https://documentation.meraki.com/MR/Other_Topics/Hotspot_2.0.

[22] « Technical Partner Training Manual », Hotspot Manager Wiki; https://wiki.hsnetworkmanager.com/?manuale=technical-partner-training-guide (consulté le 8 juin 2023).

[23] Thierry Longeau « La virtualisation des systèmes d'information " ; Société ALCANTIS ; http://www.alcantis.fr/index_fichiers/virtualisation_systemes_information.pdf (consulté le 8 juin 2023).

[24] Arnaud & Amelina &Alain Patrick AINA " virtualisation & Partage de Charge" https://www.ws.afnog.org/afnog2014/ssf/docs/ssf_virtualisation-opensource.pdf (consulté le 8 juin 2023).

[25] AbdulrahmanAlnaim « Type 1 and type 2 hypervisors », ResearchGate; https://www.researchgate.net/figur.

[26] Oussama Stiti " Étude de l'Urbanisation des Accès Virtuels et Stratégie de Métamorphose de Réseaux « ; THESE DE DOCTORAT ; Université Pierre et Marie Curie - Paris VI, 2015. https://theses.hal.science/tel-01343298v1/document.

[27] J. MacPherson; « VMware vSphere vs. vCenter vs. ESXi – Différences, Benefits, and More », article, 30 août 2022. https://www.parkplacetechnologies.com/blog/vmware-vsphere-vs-vcenter-vs-esxi/

[28] « What is VMware vSphere - Beginners Guide to VMware Virtualization »; article; 31 juillet 2017. https://www.vmwarearena.com/what-is-vmware-vsphere-beginners-guide-to-vmware-virtualization.

[29] Bradley Mitchell « », article, Septembre 10, 2021. https://www.lifewire.com/wireless-access-point-816545(consulté le 8 juin 2023).

[30] Worton « Quelle est la différence entre hub, switch et routeur ?» ; depuis le 29 décembre, 2021.https://community.fs.com/fr/blog/whats-the-difference-hub-vs-switch-vs-router.html.

[31] « How Switches Forward Frames Explained »; Computer Networking Notes. https://www.computernetworkingnotes.com/ccna-study-guide/how-switches-forward-frames-explained.html (consulté le 8 juin 2023).

[32] « Apprendre à administrer un routeur mikrotik | 2022 | Udemy ». https://www.udemy.com/course/apprendre-a-administrer-un-routeur-mikrotik/ (consulté le 8 juin 2023).

[33] « Mikrotik rb951ui-2hnd – Votre partenaire hi-tech ! » ; https://wifi-algerie.com/produit/mikrotik-rb951ui-2hnd/ (consulté le 8 juin 2023).

[34] « Modem : définition, fonctionnement et modèles ». https://www.journaldunet.fr/web-tech/dictionnaire-du-webmastering/1445268-modem-definition-fonctionnement-et-modeles/ (consulté le 8 juin 2023).

[35] « TP-Link Routeur 4G LTE Archer MR200 V5 – Votre partenaire hi-Tech ! » https://wifi-algerie.com/produit/tp-link-routeur-4g-lte-archer-mr200/ (consulté le 8 juin 2023).

Annexe 1 : Conditions d'exploitation des services d'accès à Internet

CHAPITRE 3

CONDITIONS D'EXPLOITATION DES SERVICES D'ACCES A INTERNET

Art. 23. — Identification et protection des usagers

23.1 Identification

Tout client doit faire l'objet d'une identification précise comportant notamment, les éléments suivants :

— prénom(s) et nom et la copie d'une pièce d'identité officielle pour les personnes physiques ;

— extrait du registre du commerce ou des statuts pour les personnes morales.

Cette identification doit être faite avant la fourniture de tout service, conformément à l'article 161 de la loi.

Le Titulaire est tenu d'établir et de maintenir une base de données numérique contenant pour l'ensemble de ses abonnés, les informations suivantes :

— prénom(s) et nom ;

— date et lieu de naissance ;

— numéro d'identification national ou le numéro du passeport ;

— adresse ;

— dénomination sociale pour les personnes morales ;

— date de souscription ;

— le(s) service(s) fourni(s).

Le Titulaire est tenu de mettre en place les moyens matériels et logiciels permettant d'identifier techniquement et authentifier, au moment de la souscription, tous les utilisateurs qui se connectent via son infrastructure.

Lorsqu'il s'agit de la fourniture de service d'accès à Internet par la technologie Wi-Fi cité à l'article 4 ci-dessus, la souscription au service s'effectue, soit directement sur le site web du titulaire soit auprès d'un de ses points de présence commerciale. Dans tous les cas, le Titulaire doit garantir l'exactitude des informations fournies par le souscripteur (nom, prénom, numéro de téléphone).

La souscription au service s'effectue selon deux (2) modes :

— soit sur le site web du Titulaire à travers un lien direct sur la page d'authentification d'un portail captif où l'usager doit fournir :

• prénom(s) et nom ;

• son numéro de téléphone mobile lui permettant ainsi de recevoir les paramètres d'identification via le service de messagerie court (SMS).

— soit auprès d'un point de présence qui lui délivrera les paramètres d'identification moyennant le dépôt de la copie de la pièce d'identité officielle.

23.2 Confidentialité des communications

Le Titulaire s'engage à prendre les mesures permettant d'assurer la confidentialité des informations qu'il détient sur ses abonnés et la confidentialité de leurs communications et ne pas permettre la mise en place de dispositifs en vue de l'interception ou du contrôle des communications, échanges électroniques ou données sans l'autorisation préalable de l'autorité judiciaire, conformément à la législation en vigueur.

Le Titulaire est tenu de porter à la connaissance de ses agents, les obligations auxquelles ils sont assujettis et les sanctions qu'ils encourent en cas de non-respect du secret des communications, des échanges électroniques et des données.

23.3 Neutralité des services

Le Titulaire garantit la neutralité de ses services vis à-vis du contenu des informations transmises sur son infrastructure.

Il s'oblige, également, à prendre toutes les mesures nécessaires pour garantir la neutralité de son personnel vis-à-vis du contenu des messages transmis via son infrastructure. A cet effet, il offre les services sans discrimination, quelle que soit la nature ou la forme des communications électroniques transmises et la technologie utilisée et il prend les dispositions utiles pour en assurer l'intégrité.

Art. 24. — Protection des enfants et des personnes vulnérables

Le Titulaire est tenu de mettre en place des solutions afin de proposer à ses abonnés et de promouvoir un service qui leur permet de protéger les enfants ou les personnes vulnérables sous leur tutelle par restriction d'accès aux contenus indésirables.

CHAPITRE 4

RESPONSABILITE ET CONTROLE

Art. 25. — Responsabilité

Le Titulaire est responsable du bon fonctionnement du service, du respect des obligations contenues dans le présent cahier des charges, ainsi que du respect des principes et des dispositions législatives et réglementaires en vigueur.

Le Titulaire est seul responsable vis-à-vis des tiers, conformément aux dispositions de la loi, de fourniture du service et des dommages éventuels qui peuvent résulter, notamment, des défaillances du Titulaire ou de son personnel ou des défaillances du service.

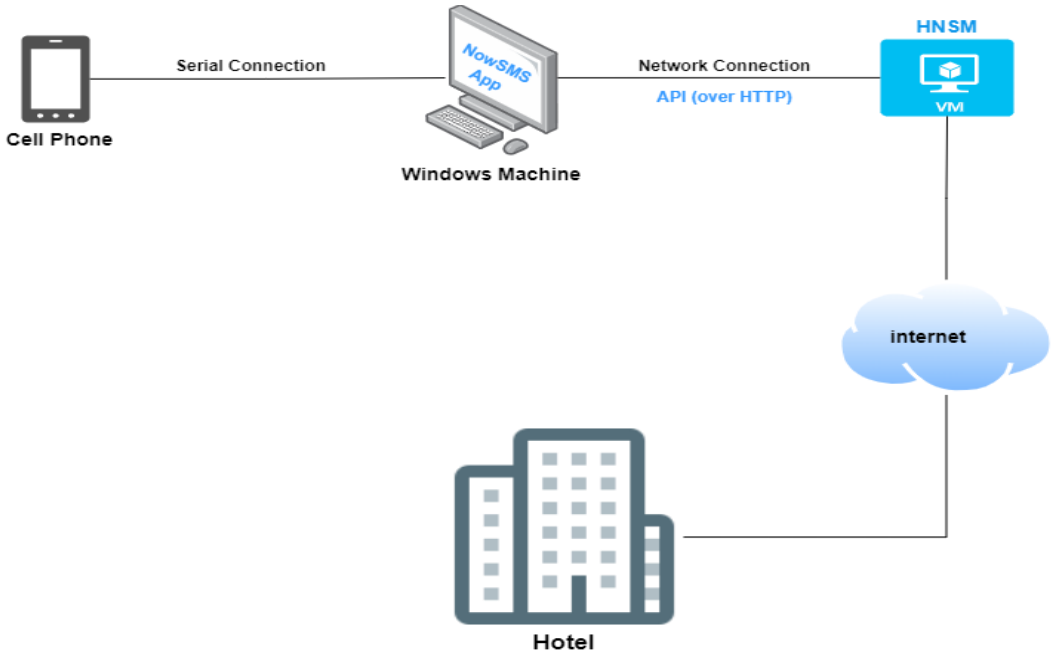
Annexe 2 : Présentation et configuration de la solution « Now SMS »

A.2.1 Présentation de la solution now SMS

NowSMS est une solution de passerelle de messagerie qui permet l'envoi et la réception de messages SMS, MMS et autres types de messages via diverses interfaces de communication.

Cependant, NowSMS utilise des identifiants d'objet pour gérer et suivre les différentes tâches et objets dans son système. Ces identifiants d'objet sont généralement attribués par le système lui-même et sont utilisés pour identifier de manière unique les objets tels que les messages, les utilisateurs, les groupes, les connexions, etc.

A.2.2 Authentification via la topologie Now SMS



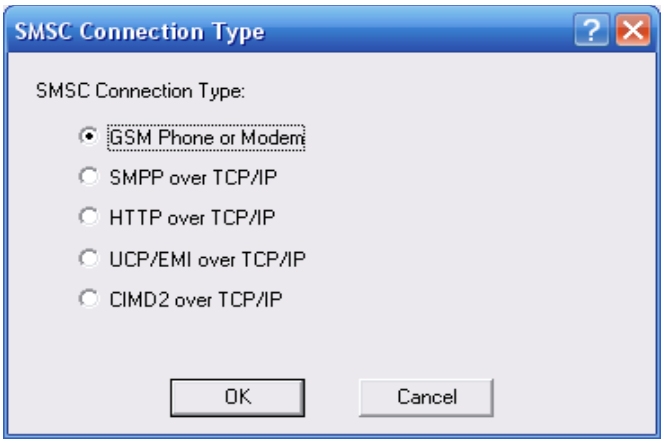
A.1: Topologie de fonctionnement de la solution Now SMS

A.2.3 Configuration de Now SMS

Etape1 :

Pour définir les modems qui seront utilisés par la passerelle, sélectionnez la boîte de dialogue de configuration "SMSC" dans la boîte de dialogue de configuration de la passerelle.

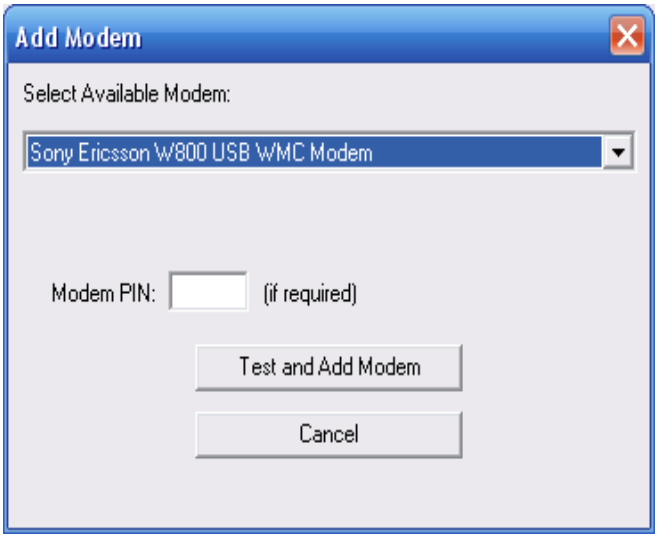
Sélectionnez "Ad", puis "GSM Phone or Modem" pour afficher la liste des pilotes de modem disponibles sur votre ordinateur.



A.2: Type de connexion SMCS

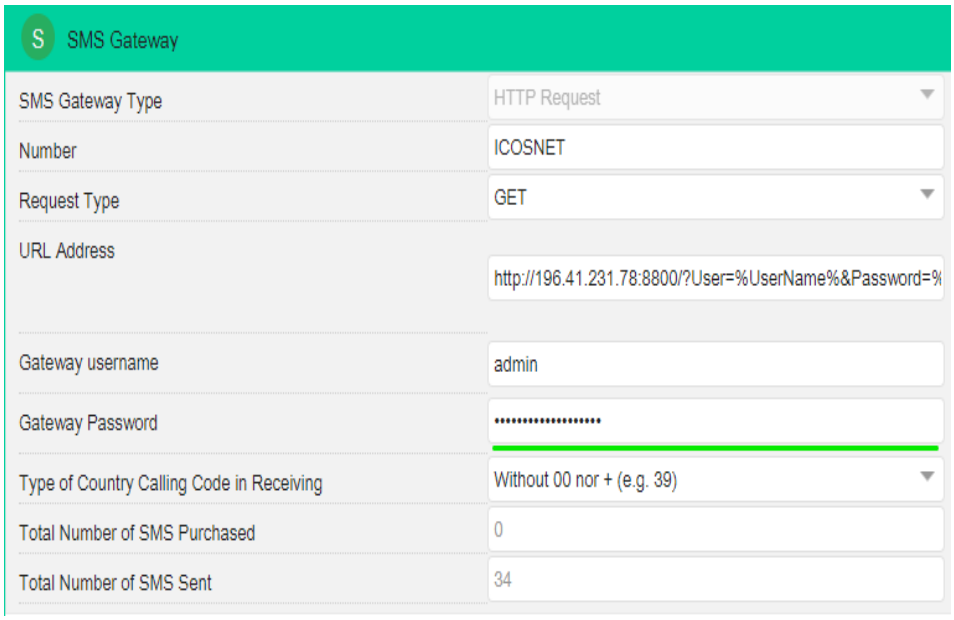
Etape 2 :

Sélectionnez un modem disponible et appuyez sur le bouton "Test and Ad Modem". La passerelle tente alors d'initialiser le modem et de confirmer qu'il prend en charge les interfaces nécessaires à l'envoi et à la réception de messages SMS.



A.3: Sélectionnent du modem disponible

Etape 3 : Nous avons configuré la Gateway SMS HSNM au niveau du « **Manager** »



A.4 : Configuration du SMS Gateway

URL complète :

http://196.41.231.78:8800/?User=%UserName%&Password=%Password%&PhoneNumber=%Number%&Text=%Message%