République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique
Université Abderrahmane Mira - Béjaïa -
Faculté des Sciences Exactes
Département d'Informatique

Mémoire de fin de cycle
En vue de l'obtention d'un diplôme de master professionnel en informatique
Option : Administration et Sécurité des Réseaux

Thème

Contrôler l'accès à un réseau WiFi avec un code QR. Cas d'étude : Entreprise Portuaire de Bejaia

Réalisé par :

M^lle^ AIT CHALALT Linda.
M^lle^ BALOUL Anissa.

Evalué par le jury composé de :

Examinateur 1	**M^r^. MOKTEFI Mohand**	**M.A.A**	**U. A/Mira Béjaïa.**
Examinateur 2	**M^r^. FARAH Zoubeyr**	**M.C.B**	**U. A/Mira Béjaïa.**
Encadrant	**M^r^. KHANOUCHE M. Essaid**	**M.C.A**	**U. A/Mira Béjaïa.**

Année universitaire 2019–2020.

Remerciements

Ce travail fut accompli grâce à ALLAH vers lequel vont toutes les louanges.
Au terme de ce travail, nous aimerions exprimer notre gratitude et nos remerciements à notre encadrant Mr KHANOUCHE Mohamed Essaid ainis qu'au responsable de notre stage Mr TOUATI Baddredine de nous avoir encadré pour réaliser ce travail par leurs disponibilités leurs temps précieux, leurs encouragements, leurs aides, leurs conseils avisés et leur gentillesse.
Nous tenons, également, à remercier vivement les examinateurs pour l'honneur qu'ils nous ont fait en acceptant de juger ce travail.
Enfin, pour toute personne qui a contribué, de près ou de loin, à l'élaboration de ce mémoire. Veuillez bien trouver ici l'expression de nos sincères remerciements

Dédicaces

Je dédie ce travail, A ma famille, particuliérements mes parents que Dieu les protège, qui m'ont encouragé et aidé tout au long de la réalisation de notre projet mais aussi pendant toute ma scolarité,
A Mon frère et ma belle-soeur qui m'ont beaucoup soutenu aussi durant cette année,
A mon chèr et adorable neveu Assyl qui illumine ma vie,
A mes deux familles paternelles et maternelles.

Anissa.

Dédicaces

Je dédie cet humble travail,

A mes chers parents, qui ont toujours été là-derrière chaque pas pour me soutenir et m'encourager, je vous remercie pour votre éducation et tous les sacrifices que vous m'avez donné tout au long de ma vie. "Que Dieu vous accorde une longue vie ",

A mon adorable frère,

A mes très chères sœurs,

A tous les membres de ma famille,

A tous mes chers amis,

A toutes les personnes qui ont participé à la réalisation de ce modeste travail.

Linda.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

VPN	**V**irtual**P**rivate **N**etwork
BSA	**B**asic **S**ervice **A**rea
BSS	**B**asic **S**ervice **S**et
MAC	**M**edia **A**ccess **C**ontrol
DS	**D**istribution **S**ystem
WiFi	**W**ireless **F**idelity
WLAN	**W**ireless d'**L**ocal **A**rea **N**etwork
IEEE	**I**nstitute of **E**lectrical and **E**lectronics **E**ngineers
OFDM	**O**rthogonal **F**requency **D** ivision **M**ultiplexing
DSSS	**D**irect **S**equence **S**pread **S**pectrum
OFDM	**O**rthogonal **F**requency **D**ivision **M**ultiplexing
WEP	**W**ired **E**quivalent **P**rivacy
WPA	**W**iFi **P**rotected **A**cces
TKIP	**T**emporal **K**ey **I**ntegrity **P**rotocol
AES	**L**'Advanced **E**ncryption **S**tandard
EPB	**E**ntreprise **P**ortuaire de **B**ejaia
QR	**Q**uick **R**esponse
ISO	**I**nternational **O**rganization for **S**tandardization
CDD	**C**harged **C**oupled **D**evice
RC4	**R**ivest **C**ipher **4**
HTML	**H**ypertext **M**arkup **L**anguage
PHP	**H**ypertext **P**reprocessor
CSS	**C**ascading **S**tyle **S**heets
DNS	**D**omain **N**ame **S**ystem
DHCP	**D**ynamic **H**ost **C**onfiguration **P**rotocol
HTTP	**H**ypertext **T**ransfer **P**rotocol
HTTPS	**H**ypertext **T**ransfer **P**rotocol **S**ecure
SSL	**S**ecure **S**ockets **L**ayer
BCH	**B**ose, Ray-**C**haudhuri, **H**ocquenghem

Introduction Générale

Les réseaux informatiques sont devenus un atout indispensable au sein d'une entreprise quel que soit son secteur d'activité. Les individus peuvent facilement traiter des informations en se servant des logiciels et des réseaux informatiques. L'art de dissimuler l'information est devenu une question importante au cours des dernières années, car la sécurité de l'information est devenue une préoccupation majeure à l'ère d'internet. La maitrise et la mesure de la sécurité logique des réseaux basés sur les installations et les configurations des équipements réseaux deviennent une priorité majeure pour les administrateurs réseaux.

À l'ère de la technologie, rester connecté est un besoin pour chaque personne possédant un dispositif mobile (smartphone, tablette, ou ordinateur portable). La fonction primaire du WiFi (acronyme de Wireless Fidelity) est de simplifier cette tâche, il offre la possibilité à chacun de rester en ligne en toute circontances . Cette technologie peut être utilisée en interne (WiFi privé) ou être ouverte à des personnes extérieures (WiFi public). En interne, le WiFi permet de faciliter le travail de ses utilisateurs qui peuvent accéder au réseau local de l'entreprise via leurs smartphones et tablettes. Le WiFi public permet quant à lui d'apporter un service aux personnes extérieures à l'entreprise en leur offrant une connexion Internet gratuite

Les réseaux locaux sans fil WLAN (Wireless Local Area Network) envahissent notre quotidien, car la valeur ajoutée qu'ils offrent aux utilisateurs, à un coût raisonnable, est incontestable. Comme ces réseaux possèdent des frontières à géométrie variable et surtout difficilement contrôlables, il est indispensable de les sécuriser et de contrôler l'accès à ces réseaux.

L'entreprise portuaire de Bejaïa fait partie de ces entreprises qui offrent une connexion internet gratuite aux passagers de la gare maritime. Malheureusement, elle rencontre des problèmes quant au service proposé. Ayant un réseau ouvert, elle n'est pas à l'abri d'une surcharge du réseau et cela engendre une dégradation du service (bande passante faible, accès limité aux voyageurs), en plus des différentes menaces de sécurité quand le wifi est accessible à tous.

Ce mémoire est structuré en trois chapitres, le premier chapitre contient quelques généralités sur les réseaux d'entreprises, et sur le réseau WiFi. Dans le second chapitre, nous présentons l'organisme d'accueil et décrivons le fondement méthodique de la solution proposée qui consiste en un système de sécurité basé sur le code QR. Le dernier chapitre sera la mise en place et l'implémentation d'une authentification en utilisant un code QR, et enfin nous terminerons ce mémoire par une conclusion générale.

Chapitre 1

Les réseaux d'entreprise

1.1 Introduction

Le réseau en entreprise permet à l'entreprise de centraliser ses données, et de travailler en équipe de manière productive. Ce réseau peut être filaire,sans-fils ou une hybridation des deux.

Le développement d'utilisation d'internet a permis à beaucoup d'entreprises d'ouvrir leurs systèmes d'information à leurs partenaires ou leurs fournisseurs. Il s'avère donc essentiel de connaître les ressources de l'entreprise à protéger et ainsi maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information.

Dans ce chapitre, nous présentons les réseaux filaires et sans fil, ainsi que le WiFi, ses différentes normes et ses techniques de sécurité.

1.2 Les réseaux d'entreprise

Selon la définition du dictionnaire "le Petit Robert" : un réseau est « un ensemble de points communiquant entre eux ». Dans le monde numérique, ces « points » appelés également « nœuds » du réseau sont des équipements informatiques. Il peut s'agir d'ordinateurs, d'imprimantes, de systèmes de vidéosurveillance, de téléphones portables ou de tout autre matériel électronique [1].

Selon Philippe Gomez et Pierre Bichon : un réseau local d'entreprise représente un système de communication local reliant plusieurs ordinateurs (serveur, stations de travail, etc) permettant de transférer des données à des vitesses élevées, sur de courtes distances et dans les limites d'une enceinte privée. Les éléments constitutifs d'un réseau local sont : la station de l'utilisateur, le serveur du réseau et le média [4].

Plus précisément un réseau d'entreprise permet de relier ses ordinateurs via un serveur qui gère l'accès à Internet, les e-mails, les droits d'accès aux documents partagés et le travail collaboratif. Chaque utilisateur du réseau se connecte avec un nom d'utilisateur et un mot de passe avant d'être par le serveur. L'utilisateur peut accéder à ses données et au partage de fichiers. Le réseau d'entreprise est privé, protégé par un pare-feu et généralement géré par le service informatique. Certaines

entreprises disposant de plusieurs sites, les réseaux sont interconnectés par une technologie VPN (Virtual Private Network) afin de garantir la sécurité et la confidentialité des données de cette entreprise.

1.3 Types des réseaux

On distingue deux types : réseaux filaires et réseaux sans fils.

1.3.1 Réseaux filaires

Le réseau filaire comme son nom l'indique, est un réseau que l'on utilise grâce à un fil de connexion. Ce réseau utilise des câbles Ethernet pour relier des ordinateurs et des périphériques grâce à un routeur ou à un commutateur. On qualifie souvent ce réseau de rapide, fiable et sécurisé. En effet, s'il s'agit par exemple de relier deux ou trois ordinateurs situés dans une même pièce, il est souvent moins coûteux en temps et en argent de connecter les ordinateurs à un simple routeur, à l'aide de quelques câbles réseaux [1].

1.3.2 Réseaux sans-fil

Le réseau sans-fil est un réseau dans lequel au moins deux terminaux peuvent communiquer sans l'utilisation d'un fil, il est basé sur une liaison utilisant des ondes radio-électriques (radio et infrarouges) en lieu et place des câbles habituels [2].

Les réseaux sans-fil permettent de relier très facilement des équipements distants d'une dizaine de mètres à quelques kilomètres. De plus, l'installation de tels réseaux ne demande pas de lourds aménagements des infrastructures existantes comme c'est le cas avec les réseaux filaires. De plus les ondes hertziennes sont difficiles à confiner dans une surface géographique restreinte, il est donc facile pour un pirate d'écouter le réseau si les informations circulent en clair, ce qui nécessite de mettre en place les dispositions nécessaires de telle manière à assurer une confidentialité des données circulant sur les réseaux sans-fil [2].

Il existe plusieurs technologies qui utilise les réseaux sans-fil, telles que le WiFi, que nous présentons dans le prochain titre, l'infrarouge, le laser, le Bluetooth...
Nous notons deux types de réseaux sans fils :

- **Les réseaux Ad hoc :**

  Les réseaux « ad hoc » s'affranchissent de toute infrastructure. La communication a lieu directement de machine à machine. Une machine pouvant éventuellement servir de relais pour diffuser un message vers une station non vue (au sens électromagnétique du terme) par la station d'origine (routage).

  Les réseaux ad hoc ne fonctionnent qu'en mode point à point, lorsqu'une station veut en joindre une autre elle inonde le réseau, son message est répété par toutes les stations jusqu'à la station destination. Le destinataire acquitte le premier message reçu qui emprunte en

retour la même voie qu'à l'aller. Chaque machine apprend ainsi la route pour joindre le destinataire (la route est construite à l'envers) [3].

- **Les réseaux avec infrastructure :**

  Dans ce type de réseau sans fil, chaque périphérique est relié au réseau via un point d'accès (Access Point : AP). On dit que le périphérique est le « client » et l'AP le « maître ».

  Un réseau de ce type s'appelle un Basic Service Set (BSS) et couvre un espace qu'on appelle une « cellule » ou Basic Service Area (BSA). Chaque Basic Service Set (BSS) est identifié par un nombre composé de 48 bits appelé BSSID. En mode Infrastructure, ce BSSID correspond tout simplement à l'adresse MAC(Media Access Control) du point d'accès. Le point d'accès sert de relais entre les périphériques, mais il peut aussi servir de relais vers un réseau filaire, par exemple, un réseau d'entreprise.

  Ces BSS multiples peuvent être reliés par un système de distribution (Distribution System : DS) de façon à former un unique réseau sans fil étendu. Le DS peut être un réseau filaire Ethernet (cas le plus fréquent), un câble de point à point, ou encore une liaison sans fil. IL est alors possible à un utilisateur de se déplacer dans l'ensemble de la zone de couverture sans souffrir de ralentissement ou d'interruption de la connexion : en cas de besoin, la liaison bascule automatiquement selon le principe du hand-over vers le point d'accès offrant la meilleure connexion [1].

1.4 Réseaux WiFi

Selon le guide « Tout sur le réseau » de Fabrice LeMainque, le WiFi *(Wireless Fidelity)* est une technique de réseau informatique sans fil mise en place pour fonctionner en réseau interne et, depuis, devenu un moyen d'accès à haut débit à internet. Cette technique est fondée sur la norme IEEE 802.11. Le WiFi permet de créer des réseaux locaux sans fil à haut débit qui, en pratique permettent de relier des entités (ordinateurs, smartphones, etc) grâce à des ondes radio [7].
Les connexions sans fil sont largement répandues notamment **chez les particuliers**, on peut aussi les trouver [6] :

- À la maison (pour partager une connexion ADSL ou câble).
- En entreprise (pour un accès au réseau local en sans fil).
- Dans les lieux publics (hôtels, gares, aéroports, cafés, galeries marchandes, etc via des Hot Spots).

Le WiFi a été conçu comme une version sans fil du protocole Ethernet. Les deux d'ailleurs se marient très bien, si nous avons déjà monté un réseau Ethernet alors nous n'aurons aucune difficulté à comprendre et mettre en œuvre un réseau WiFi.

1.4.1 Présentation de la norme 802.11

La norme 802.11 est un ensemble de standards qui régissent les transmissions sur les WLAN (Wireless Local Area Network). Chaque standard ou sous standard est désigné par une lettre de

l'alphabet. Ceci ne correspond pas à une appellation empirique, mais désigne le groupe de travail de l'Institut des ingénieurs électriciens et électroniciens (Institute of Electrical and Electronics Engineers : IEEE) qui est chargé de l'étude et de la publication d'un standard ou sous standard de la famille 802.11.

De base, le 802.11 définit trois couches physiques : l'une sur infrarouge et deux autres sur les ondes radio de fréquence 2.4 GHz, avec un débit théorique de 1 ou 2 Mb/s [1]. Il est noté que le débit réel est loin d'être le même que le débit théorique, car dans la réalité nous faisons face à plus d'obstacles physiques.
Pour cette norme nous comptons beaucoup de versions les plus importantes sont [1] [5] :

1.4.1.1 802.11a

Moins connu que la norme 802.11b, 802.11a fut approuvée en 1999, mais les premiers produits n'apparurent qu'en 2002. Contrairement au standard d'origine, émet dans la bande 5 GHz, bien moins encombrée que la bande 2.4 GHz. Il annonce des débits théoriques de 54 Mbits/s. L'accès au média se fait en OFDM *(Orthogonal Frequency Division Multiplexing)*.

1.4.1.2 802.11b

La norme 8012.11b fut ratifiée en 1999. Il se développa plus rapidement et les premiers produits apparurent en 2000. Beaucoup plus proche du standard 802.11 d'origine, il reprend la bande de fréquences 2.4 GHz et utilise un accès au médium de communication en mode DSSS *(direct-sequence spread spectrum)*. Une amélioration des techniques de modulation lui permet d'atteindre des débits théoriques de 11 Mbits/s.

1.4.1.3 802.11g

Ratifiée en 2003, cette nouvelle version du standard fonctionne dans la bande 2.4 GHz, comme 802.11b, mais utilise l'OFDM comme 802.11a, ce qui lui permet d'atteindre le même débit théorique de 54 Mbits/s. Toutefois les débits utiles restent inférieurs à ceux de 802.11a. Un point d'accès 802.11g peut gérer des terminaux 802.11g mais sait se replier en mode 802.11b pour supporter des terminaux de génération antérieure. Cette particularité permet donc une migration « en douceur » des réseaux, sans avoir à intervenir immédiatement sur le parc de terminaux.

1.4.1.4 802.11n

Ce standard a été ratifié en juillet 2009, mais des études du standard ont été publiées depuis 2006. Compatible avec les standards précédents, il permet, grâce à de nombreuses techniques d'atteindre des débits très élevés (>100 Mb/s), c'est la version la plus utilisée.

1.4.1.5 802.11ac

Cette norme a vu le jour en 2014. Cette évolution de 802.11n atteint des débits de l'ordre du Gbits/s, avec partage du canal radio par plusieurs utilisateurs. L'augmentation du débit se fera grâce à une meilleure efficacité de la modulation et une plus grande largeur du canal. La bande de fréquence sera compatible avec la bande 5 GHz utilisée par 802.11a et 802.11n.

1.4.2 Sécurité dans les réseaux WiFi

La sécurité est une question importante en matière de réseau sans fil, car il est pratiquement impossible de contrôler les ondes. En effet,une personne ayant un ordinateur peut accéder au réseau contrairement au réseau filaire ou il faut accéder au câble pour parvenir à ce résultat.

Souvent, au sein d'un réseau d'ordinateurs, les accès non autorisés représentent un risque pour la sécurité. Dans le cas où un grand nombre de personnes auraient accès à un réseau, la probabilité d'accès non autorisé est accrue, en particulier suite à la divulgation du mot de passe ou dans le cas où il n'y en a même pas. Le contrôle d'accès est un mécanisme fondamental de la sécurité des données qui détermine qui a le droit de consulter et d'utiliser des informations et ressources d'une entreprise. Via une authentification, les stratégies de contrôle d'accès vérifient que les utilisateurs sont bien ceux qu'ils prétendent être et qu'ils disposent d'un accès adapté au réseau de l'entreprise.

Pour l'améliorer des mécanismes ont été établis dont [1] :

1.4.2.1 Wired Equivalent Privacy (WEP)

Le mécanisme WEP a pour objectif de protéger toutes les communications WiFi en cryptant les paquets et pour ce faire :

- Tous les AP doivent être configurés avec une clé secrète, la « clé WEP », longue de 40 ou 104 bits.
- De même tous les utilisateurs doivent configurer leurs adaptateurs WiFi avec cette même clé.
- Par la suite tout le trafic WiFi entre les utilisateurs et les AP est crypté. Le cryptage repose sur un algorithme appelé Rivest Cipher 4 (RC4).

1.4.2.2 WiFi Protected Acces (WPA)

Lors de la conception de WEP, l'IEEE savait que cette solution ne serait que momentanée, car loin d'être parfaite elle ne répondait pas à toutes les attentes de sécurité des utilisateurs. Ainsi est né le WPA, considéré comme une version allégée de WPA2 (802.1i), il en existe 2 variantes : **WPA Personal**, également appelé WPA Pre-shared Key, et le **WPA Entreprise**.

- WPA repose sur le cryptage Temporal Key Integrity Protocol (TKIP) qui a été conçu de telle sorte qu'il soit possible de le mettre en œuvre dans les AP existants par une simple mise à jour.
- Repose aussi sur l'algorithme RC4.

1.4.2.3 WiFi Protected Access 2 (WPA2) /802.1i

Le WPA2 permet d'utiliser un nouvel algorithme de cryptage appelé Advanced Encryption Standard (AES), il est plus puissant en calcul que RC4, et nécessite un matériel plus puissant. L'algorithme AES existe aussi en deux variantes, qui reposent sur le protocole 802.1x et sur une

clé partagée entre tous les équipements du réseau.

Pour remédier aux problèmes de confidentialités dans les réseaux sans fils, il a vite fallu trouver des solutions [1] [7] :

- Définir un mot de passe complexe et le modifier régulièrement.
- Limiter les débordements : consiste à s'assurer que les ondes radio ne débordent pas sur l'extérieur de l'entreprise.
- Utiliser les Firewall intégrés dans le routeur.
- Masquer le SSID.
- Filtrer par adresses MAC : mécanisme qui consiste à limiter l'accès au réseau sans fil à une liste d'équipements donnée, identifiée par leurs adresses MAC.
- Isoler le réseau sans fil : traiter les utilisateurs du réseau sans fil comme s'ils venaient d'internet.

1.5 Conclusion

Même si les solutions de sécurité ne sont pas encore au point, le déploiement des réseaux sans fil est déjà effectif et va s'amplifier dans les années à venir dans les entreprises du fait des besoins croissants des utilisateurs en termes de mobilité, de flexibilité et de services. Pour se faire, le monde industriel et académique a pour mission de concevoir des mécanismes de sécurité adaptés aux réseaux sans fil.

Le contrôle d'accès étant le plus important, car la protection du réseau commence par l'inspection, puis le blocage de toute intrusion dans le réseau sans fil pour un meilleur service de sécurité.

Chapitre 2

Contexte & Objectifs du projet

2.1 Introduction

Ce chapitre est réservé à l'étude du réseau mis en place à l'Entreprise Portuaire de Bejaia (l'EPB) et à la solution proposéé pour améliorer leur gestion du réseau WiFi, d'abord nous évoquons un bref aperçu de l'entreprise pour mieux connaître sa structure et ses objectifs. Ensuite, nous étudions le réseau de cette entreprise et ses différents composants pour identifier les failles dans ce réseau WiFi et proposer une méthode pour sécuriser l'accès à ce dernier.

2.2 Présentation de l'organisme d'accueil

De par sa position stratégique, les qualités nautiques remarquables et les infrastructures performantes dont il dispose, le port de Béjaïa reste un moteur de développement économique pour la région et le pays. Principale plaque tournante du commerce du bassin méditerranéen, il constitue l'accès privilégié aux différentes industries, parce qu'il offre à ses clients des terminaux propices et compétitifs ainsi que des équipements modernes et performants, tous dédiés pour l'accueil et le traitement de tous types de marchandises [8]. En plus de ça, on peut noter ses principales activités comme étant les suivantes [9] :

- L'exploitation de l'outillage et des installations portuaires.
- L'exécution des travaux d'entretien, d'aménagement et de renouvellement de la super structure portuaire.
- L'exercice du monopole des opérations d'acconage et de manutention portuaire.
- L'exercice du monopole des opérations de remorquage, de pilotage et d'amarrage.

2.2.1 Structure de l'entreprise

L'Entreprise Portuaire de Béjaïa est composée d'une direction générale, avec un département marketing et d'une Cellule de Project d'Exploitation des activités commerciales, suivie de deux directions générales adjointes, fonctionnelles et opérationnelles, chacune d'elle est divisée en plusieurs sous directions :

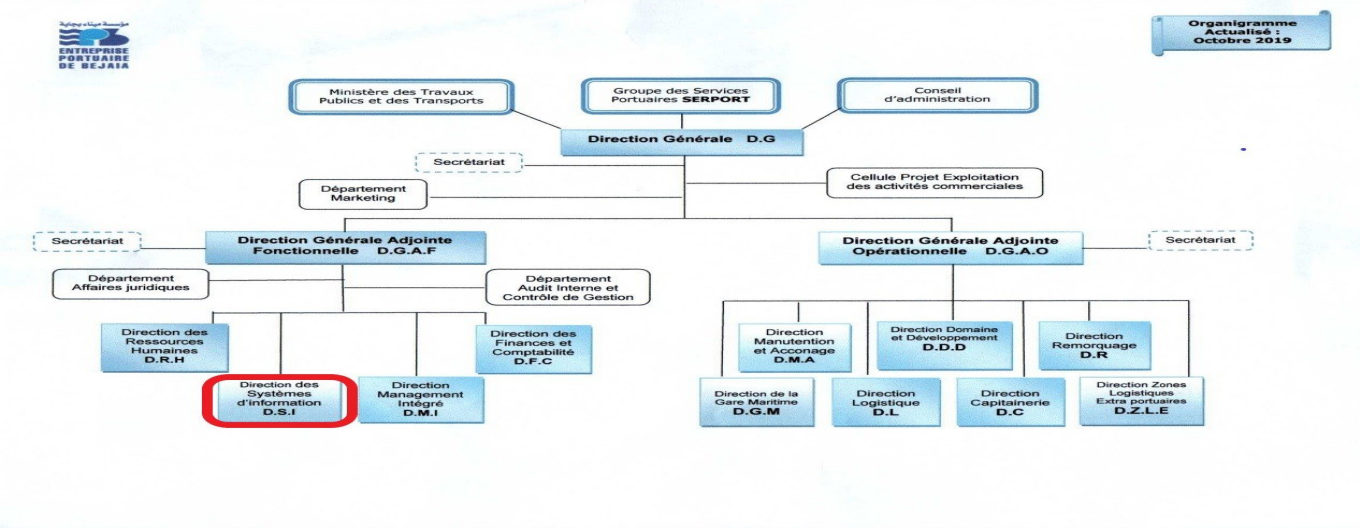

FIGURE 2.1 – Organigramme de l'EPB 2019 [11].

2.2.1.1 La direction générale adjointe opérationnelle

A) **Direction Manutention et Acconage** (**D.M.A**), qui assure la réception, la reconnaissance à terre des marchandises ainsi que leurs gardes jusqu'à leur embarquementou livraison au destinataire. Subdivisée en deux départements : département commerciu

B) **Direction Domaine et Développement** (**D.D.D**), qui met en oeuvre les programmes d'entretien et d'investissement de l'entreprise. Subdivisée en trois départements : Département des travaux, département de maintenance, et département approvisionnements.

C) **Direction Remorquage** (**D.R**), qui assure les opérations de remorquages des navires à l'entrée comme à la sortie.

D) **Direction de la Gare Maritime** (**D.G.M**), qui gère la communication avec les compagnies de navigations maritimes et de leurs passagers pour leurs entrées et sorties.

E) **Direction Logistique** (**D.L**), qui permet de moderniser la manutention mécanisée afin d'assurer des prestations à même de répondre à ses objectifs et aux soucis de la clientèle en offrant une meilleure qualité de services, dans les meilleurs délais et à moindre cout.

F) **Direction Capitainerie** (**D.C**), qui s'occupe de la sécurité au sein du port de Bejaia. On y retrouve les structures suivantes :

- Département police et sécurité.
- Service sécurité terrestre.
- Service facturation.
- Service CTMD et hydrocarbures.

G) **Direction Zones Logistiques Extra portuaires** (**D.Z.L.E**), qui se charge de la gestion des zones logistiques en dehors de la zone du port de Bejaia, nous en comptons deux à ce jour, Tixter : situé à environ 190 kilomètres du port de Béjaïa, dans la daïra de Aïn Taghrout, et à Ighil Ouberouak, sis dans la commune de Tala Hamza, à environ 5 kilomètres du port de Béjaïa.

2.2.1.2 La direction générale adjointe fonctionnelle

A) **Direction des Ressources Humaines**(**D.R.H**),qui se charge d'exécuter toutes les tâches liées à la gestion et au développement des structures, et d'appliquer rigoureusement les lois de gestions et réglements intérieurs de l'entreprise.

B) **Directions des Finances et Compatbilité**(**D.F.C**), qui gère les finances et les dépenses de l'entreprise, elle est constituée de deux départements, à savoir : département de comptabilité, et le département des finances.

C) **Direction des systèmes d'information** (**D.S.I**), qui a pour mission l'automatisation des métiers de l'entreprise portuaire de Béjaïa. Cela en mettant en place les logiciels et l'infrastructure nécessaire pour la gestion du système d'information.Nous y avons effectué notre stage professionnel afin de mieux étudier leurs besoins et failles.

2.2.2 Présentation du réseau informatique de l'EPB

Le réseau du port de Bejaia s'étend du port pétrolier (n°16) aux ports 13 et 16 (port à bois). La salle machine du réseau local de l'EPB contient principalement une armoire de brassage et une autre armoire optique de grande taille, l'ensemble des serveurs. Les deux armoires servent à relier les différents sites de l'entreprise avec le département informatique par des câbles de type 4, 6, 8 et 12 brins. Chaque site a une armoire de brassage contenant un ou plusieurs convertisseur(s) media, un ou plusieurs Switch auxquels sont reliés les différents équipements par des câbles informatiques.

Depuis quelques années, le réseau de l'EPB s'étend aussi à la gare maritime qui est entièrement gérée par l'EPB, cette dernière gère donc le serveur vidéo surveillance, serveur contrôle d'accès (pour s'assurer de donner l'accès seulement aux personnes qui y sont autorisées), serveur système de gestion parking, le serveur d'affichage (messages dédiés aux passagers majoritairement), ainsi que le réseau des agences maritimes et le WiFi ouvert mis à la disposition des passagers et des employés de l'EPB. Toutes ces manipulations se font au sein même de la direction système informatiques grâce à un pare-feu.

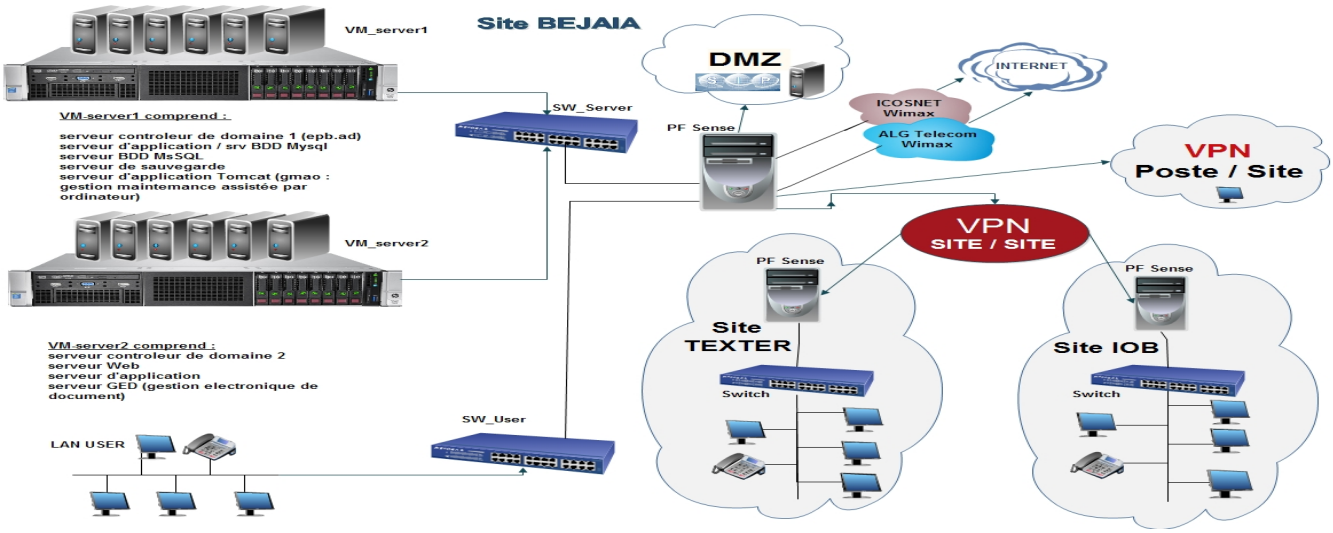

FIGURE 2.2 – Schéma de l'EPB 2019 [11]

2.2.2.1 Les missions du centre informatique

- Le centre informatique a pour mission l'automatisation des métiers de l'Entreprise Portuaire de Bejaia, et cela en mettant en place les logiciels et l'infrastructure nécessaires pour la gestion du système d'information.
- L'EPB déploie des systèmes d'information pour accroitre la productivité, automatiser les processus métiers et fournir un meilleur service aux clients. Ces systèmes intègrent de plus en plus des fonctionnalités réseau pour relier tous les utilisateurs à l'entreprise ou établir des liens avec la clientèle et les fournisseurs.
- Le réseau apporte aujourd'hui une réelle valeur ajoutée en permettant d'intégrer de nouveaux partenaires, fournisseurs et clients.

Suite à la mise en place de la nouvelle gare maritime, le service informatique s'est vu confié la mission de gestion informatique de la gare.[11] :

- Actualiser les serveurs d'affichages.
- Gestion du WiFi mis à la disposition des voyageurs.
- Mise en place d'un switch permettant l'accès à distance du firewall qui gère les points d'accès WiFi et le réseau de l'agence maritime.

2.2.3 Nouvelle gare maritime

FIGURE 2.3 – Gare maritime de Béjaia.

Dans l'objectif de développer le trafic passager, une nouvelle infrastructure spécialement dédiée pour l'accueil et le transit des passagers dans les meilleures conditions, a été conçue. Ce nouveau terminal à passagers répond aux normes internationales d'accueil et de transit des voyageurs et des véhicules, et s'inscrit dans l'optique de modernisation des infrastructures pour offrir les meilleures prestations aux usagers.
Prenant pied à la fois sur la façade maritime et sur la zone urbaine, ce nouveau terminal à passagers s'étale sur une superficie de 34.145 m^2 et il est se compose de deux blocs intérieur (du port) et extérieur (du port) [10] :

1. **Le bloc extérieur** se compose d'un parking a étage pour véhicule, d'espace commercial, et de l'accès a l'étage de débarquement et embarquement piétons situé au 2éme niveau du bloc intérieur via une passerelle.
2. **Le bloc intérieur** se compose de 4 niveaux :
   — Rez-de-chaussée pour l'embarquement véhicule.
   — Le 1er étage pour le débarquement des véhicules.
   — Le 2eme étage pour l'embarquement et débarquement des piétons, et d'un espace public(commercial).
   — Le 3eme étage salle de conférence et restauration.

Etage 1	**Etage 2**	**Etage3**
Transit des véhicules au débarquement, avec accès par rampes sur une surface de 5 545 m².	Transit des passagers (piétons) comprenant un hall d'enregistrement pour l'embarquement et le débarquement des passagers, halls pour formalités police et douane, salle d'embarquement, ainsi qu'une coursive pour l'acheminement vers la passerelle d'accès au navire, sur une surface de 5 695 m².	Salle de conférence et restaurant, sur une surface de 2 870 m².

TABLE 2.1 – La structure de la gare maritime.

2.3 Problématique et motivation

Surfer sur le net est devenu le passe-temps numéro 1 de toute personne possédant un smartphone, tablette, ou ordinateur portable. Vidéos, livres, réseaux sociaux, appels, chacun l'utilise à sa guise. L'Entreprise Portuaire de Bejaïa propose à ses voyageurs un service WiFi ouvert à tout public pour rendre l'attente plus agréable durant l'embarquement ou le débarquement du navire.

Avec une **capacité annuelle** de 1.000.000 de passagers et 100.000 véhicules, nombre de **passagers traités au débarquement et à l'embarquement** équivalent à 240 Passagers/heure, et nombre de **véhicules traités au débarquement et à l'embarquement** équivalent à 200 Véhicules/heure, et le service étant ouvert à tous, les voyageurs se retrouvent donc à le partager avec les agents de sécurités, douaniers, garde-côte, et autres employés de l'entreprise. Ils ne sont donc pas entièrement satisfaits du service proposé vu qu'ils sont parfois dans l'incapacité d'appeler un proche pour annoncer leur arrivée ou leur départ imminent.

Nous avons donc pensé à plusieurs façons de sécuriser et contrôler l'accès du réseau WiFi pour leur offrir le meilleur des services afin de les aider à être prioritaires en ce qui concerne l'accès à internet. Après concertation avec le service informatique de l'EPB et étude des besoins, nous sommes arrivés à la proposition d'une solution, qui consiste à : mettre en place une authentification QR pour les personnes détenant une carte d'embarquement pour un voyage prévu.

2.4 CODE QR

Le QR code (Quick Response) est un code matriciel 2D conçu en tenant compte de deux points, c'est-à-dire qu'il doit stocker une grande quantité de données par rapport aux codes-barres 1D et il doit être décodé à grande vitesse à l'aide de n'importe quel appareil portable comme les smartphones [14]. Il a été inventé en 1994 par Denso, l'une des principales sociétés du groupe Toyota, et approuvé en tant que norme internationale ISO (ISO/IEC18004) en juin 2000. Ce symbole en deux dimensions a été initialement destiné à être utilisé pour le contrôle de la production de pièces automobiles, mais il s'est répandu dans d'autres domaines. Aujourd'hui, le code QR est vu et utilisé quotidiennement pour les raisons suivantes [12] :

- Plusieurs caractéristiques supérieures aux codes à barres linéaires : un code QR contient des centaines de fois plus d'informations et peut contenir davantage d'informations dans un espace plus petit, il peut aussi contenir des caractères Kanji/Chinois , etc...
- Il peut être utilisé gratuitement, car Denso a mis le brevet dans le domaine public.
- La norme de structure des données n'est pas une condition préalable aux utilisations actuelles.

2.4.1 Caractéristique du code QR

Le code QR offre une capacité de stockage de données élevée : 7089 caractères numériques, 4896 caractères alphabétiques et signes, 2953 caractères binaires (données codées sur 8 bits) et 1817 données en kanji (Caractère chinois de l'écriture japonaise), l'enregistrement à haute densité (environ 100 fois plus élevée en densité que les symboles linéaires) et la lecture à grande vitesse [12] [13].

Le QR Code présente d'autres supériorités tant sur le plan des performances que des fonctionnalités [12] [13] :

1. **Lecture à grande vitesse dans toutes les directions (360°) :** Les symboles bidimensionnels prenaient beaucoup de temps pour détecter la position/angle/taille du symbole, et avaient un problème que leurs lectures étaient moins précises par rapport à celles des symboles linéaires. Le code QR a résolu ce problème en ajoutant des modèles de notification de la position du symbole disposés dans trois de ses coins pour permettre une lecture rapide dans toutes les directions (360°). En disposant les motifs de détection dans les trois coins du symbole, la vitesse de décodage du code QR peut être rendue 20 fois plus rapide que celle des autres symboles de la matrice. De plus, la détection des modèles de recherche peut être facilement mis en œuvre par le matériel, et peut également être accélérée.

2. **Résistance aux symboles déformés :** Les symboles sont souvent déformés lorsqu'ils sont fixés sur une surface courbe ou lorsque le lecteur est incliné (incliné entre la face du capteur CCD (Charged Coupled Device) et la face du symbole). Pour corriger cette distorsion, le code QR comporte des motifs d'alignement disposés avec un intervalle régulier à l'intérieur de la portée du symbole. L'écart entre la position centrale du motif d'alignement estimé à partir de la forme extérieure du symbole et de la position centrale réelle du modèle d'alignement, sera calculé pour pouvoir corriger les cartographies (pour identifier la position centrale de chaque cellule). Cela rendra la distorsion linéaire des symboles non linéaires lisibles (voir Figure 2.4).

FIGURE 2.4 – Correction des symboles déformés.

3. **Correction des erreurs :** La technologie des codes QR s'est avérée être un succès même si le code est partiellement endommagé. Cela est possible en raison de la correction d'erreurs qui est basée sur les codes Reed-Salomon, qui sont disposés dans la zone de données du code QR. Le code QR comporte quatre niveaux de correction d'erreur ; Faible (L) qui peut tolérer jusqu'à 7% de dommages, Moyen (M) qui peut tolérer jusqu'à 15% de dommages, le quartile (Q) peut tolérer jusqu'à 25% de dommages et le haut (H) peut tolérer jusqu'à 30% de dommages. Le niveau de correction des erreurs peut être configuré par l'utilisateur lorsqu'il crée le symbole. Ainsi, si le code est fortement susceptible de se salir dans son environnement d'utilisation, il est recommandé de fixer à 30% ce niveau de correction.

4. **Relier les fonctionnalités des symboles :** Le QR Code dispose d'une fonctionnalité de liaison qui permet de représenter un symbole unique en plusieurs symboles en le divisant. Un seul symbole peut être divisé en 16 symboles au maximum, et chaque symbole comporte un indicateur indiquant combien de symboles le symbole original avait été divisé et dans quel ordre ce symbole spécifique serait parmi tous ceux qui ont été divisés. Cela permettra d'éditer l'ensemble des données et de les soumettre à l'ordinateur, quel que soit l'ordre dans lequel les symboles ont été lus par le lecteur. Grâce à cette fonctionnalité de liaison, le code QR pourra être imprimé même si l'espace d'impression n'est pas assez large pour qu'un seul code QR soit imprimé.

5. **Marquage direct :** Le QR Code offre une lisibilité supérieure, même pour les symboles qui sont directement marqués au laser ou à l'aide de marqueurs de points. Si les symboles sont directement marqués, la forme de la cellule ne doit pas nécessairement être carrée. Elle peut aussi être sous forme circulaire. Même si la partie blanche (à forte réflectance) et la partie noire (à faible réflectance) sont inversées. En raison de l'angle du rayon lumineux, le code peut encore être lu avec précision. Il est également possible de lire de la face arrière du symbole lorsqu'il est marqué sur un matériau transparent tel que le verre, etc.

6. **Processus de masquage :** En ayant des motifs spéciaux pour traiter le masquage, le code QR permet d'avoir des cellules noires et blanches bien disposées dans un ordre équilibré.
Pour baliser avec précision les données qui ont été lues, il est nécessaire de disposer les cellules blanches et noires de manière équilibrée. Pour ce faire, un calcul EX-OR sera effectué entre la cellule de la zone de données et la cellule du modèle de masque (template) lors de l'encodage

des données stockées et de leur disposition dans la zone de données. Ensuite, le nombre de modèles uniques existants et l'équilibre entre les cellules blanches et les cellules noires seront évalués par rapport à la zone de données où le calcul a été effectué.
Il y a huit motifs de masque (voir figure 2.5). L'évaluation sera faite pour chaque motif de masque, et le motif de masque ayant le résultat d'évaluation le plus élevé ainsi que le résultat du calcul EX-OR seront stockés dans la zone de données.

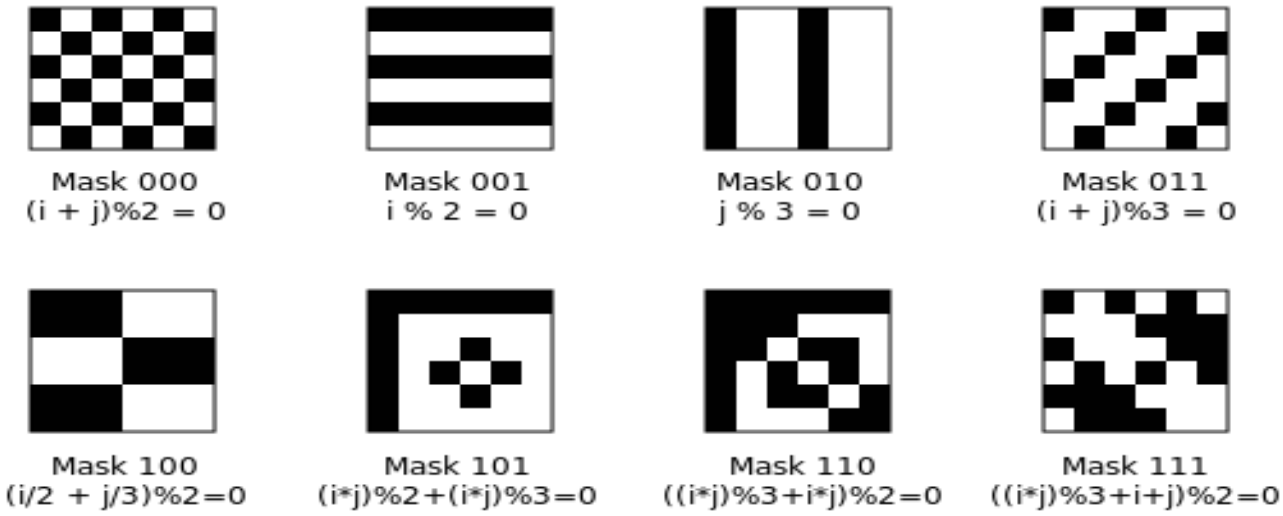

FIGURE 2.5 – Les huit motifs de masque QR

2.4.2 Structure du code QR

Le QR Code est un symbole de type matriciel avec une structure cellulaire disposée dans un carré. Il se compose des motifs de fonctionnalité pour faciliter la lecture et la zone de données où les données sont stockées. Le code QR a des motifs de recherche, des motifs d'alignement, des schémas de temporisation et une zone tranquille [12] :

A) **Finder Pattern :** le **modèle de positionnement** permet de détecter la position du code QR. En plaçant ce motif aux trois coins d'un symbole, la position, la taille et l'angle du symbole peuvent être détectés. Ce schéma de recherche consiste en une structure qui peut être détecté dans toutes les directions (360°) (voir la figure 2.6).

B) **Alignment Pattern :** le **modèle d'alignement** permet de corriger la distorsion du code QR. Il est très efficace pour corriger les distorsions non linéaires. La coordonnée centrale du modèle d'alignement sera identifiée pour corriger la distorsion du symbole. À cette fin, une cellule noire isolée est placée dans le modèle d'alignement pour faciliter la détection de la coordonnée centrale du modèle d'alignement (voir la figure 2.6).

C) **Timing Pattern :** le **schéma de temporisation** permet d'identifier la coordonnée centrale de chaque cellule dans le code QR avec des motifs en noir et blanc disposés en alternance.

Il est utilisé pour corriger la coordonnée centrale de la cellule de données lorsque le symbole est déformé ou lorsqu'il y a une erreur dans l'emplacement de la cellule. Elle est disposée à la fois dans le sens vertical et horizontal (voir la figure 2.6).

D) **Quiet Zone :** La **zone de calme** est un espace en marge nécessaire à la lecture du code QR. Cette zone de silence permet de détecter plus facilement le symbole parmi l'image lue par le capteur CCD (Charged Coupled Device). Quatre cellules ou plus sont nécessaires pour la zone de silence (voir la figure 2.6).

E) **Data Area :** Les données du code QR seront stockées (encodées) dans la **zone de données**. La partie grise de la figure 2.6 représente la zone de données. Les données seront encodées en nombres binaires de 0 et 1 selon la règle d'encodage. Les nombres binaires 0 et 1 seront convertis en cellules noires et blanches et seront ensuite arrangés. La zone de données comportera des codes Reed-Solomon incorporée pour les données stockées et la fonctionnalité de correction des erreurs.

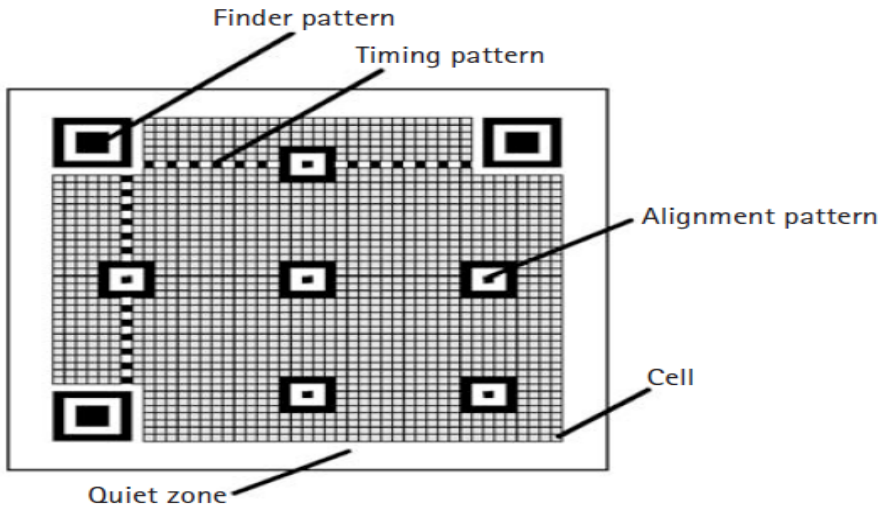

FIGURE 2.6 – La structure du code QR [12]

2.4.3 Versions du code QR

Les versions de symboles du code QR vont de la version 1 à la version 40. Chaque version a une configuration de modules ou un nombre de modules différents, le module fait référence aux points noirs et blancs qui composent le QR Code [17]. La configuration des modules désigne le nombre de modules contenus dans un symbole, à partir de la version 1 (21×21 modules) jusqu'à la version 40 (177×177 modules). Chaque numéro de version supérieure comprend 4 modules supplémentaires par côté [17]. Chaque version de symbole de code QR a la capacité maximale de données en fonction de la quantité de données, du type de caractère et du niveau de correction des erreurs. En d'autres termes, plus la quantité de données augmente, plus il faut de modules pour composer le QR Code, ce qui se traduit par des symboles QR Code plus grands.

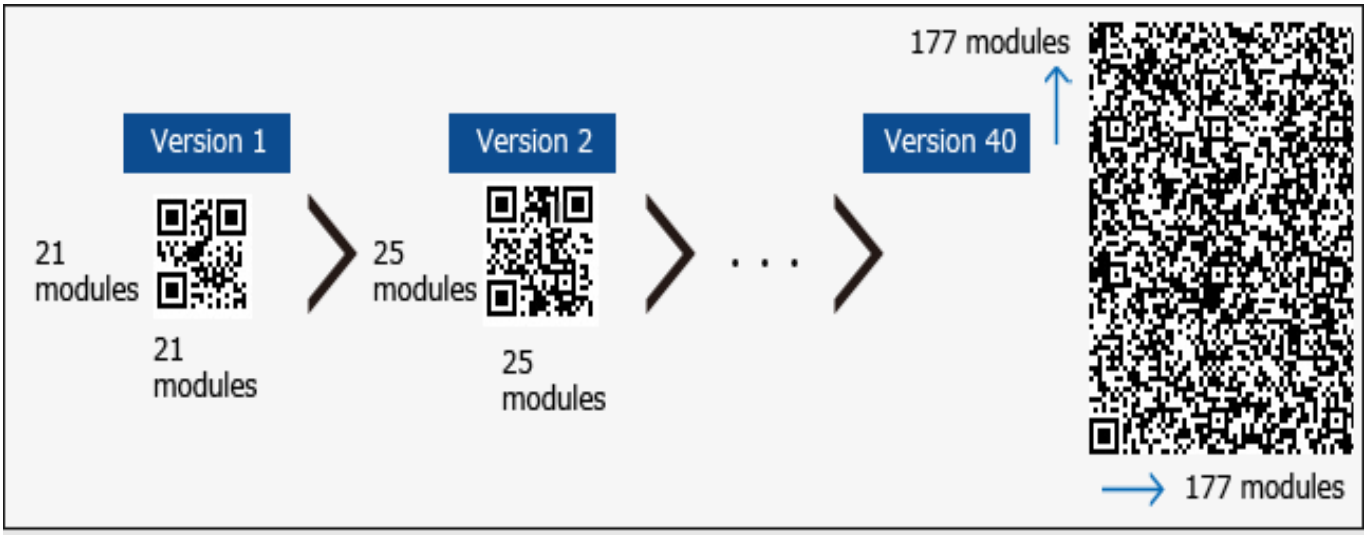

FIGURE 2.7 – La version 1 et 2 et 40 du code QR

2.4.4 Usage du code QR

Un code QR est appliqué dans différents flux d'applications liés au marketing, à la sécurité, etc. et gagne en popularité à un rythme très élevé. Jour après jour, de plus en plus de gens prennent conscience de cette technologie et l'utilisent en conséquence. La popularité du code QR croît rapidement avec la croissance des utilisateurs de smartphones et donc le code QR arrive rapidement à des niveaux élevés d'acceptation dans le monde entier.
Les codes QR sont proposés pour [14] :

- Fournir un texte, celui-ci est alors inclus dans le code QR qui devient plus complexe. Ce texte ne peut être modifié, ce qui est différent du texte proposé sur une page web.
- Visiter un site web classique ou mobile, y lire l'information, participer à un concours, à un sondage, remplir un formulaire de demande de renseignements.
- Envoyer un SMS,qui est pré-encodé avec le numéro du destinataire et le sujet, ou envoyer un email.
- Encoder un numéro de téléphone ou les coordonnées d'une carte de visite électronique (éviter ainsi un risque d'erreur d'encodage et intégrer facilement les coordonnées parmi les contacts).
- Accéder directement à une vidéo.
- Annoncer un évènement.
- Géolocaliser (à partir d'une adresse, on peut obtenir sa latitude et sa longitude avec un outil comme GPSfrance.net3).
- Se connecter au réseau WiFi, ce qui est le but de notre projet.

2.4.5 Générateurs de codes QR

La procédure de codage du Code QR comprend les étapes suivantes. Tout d'abord, les données d'entrée sont encodées selon le mode le plus efficace ce qui forme un flux binaire. Les flux binaires sont divisés en mots de code. Ensuite, les mots de code sont divisés en blocs, et des mots de code de

correction d'erreur sont ajoutés à chaque bloc. Tous ces mots de code sont placés dans une matrice et sont masqués par un motif de masque. Enfin, des motifs de fonction (modèle de positionnement, modèle d'alignement, modèle timing) sont ajoutés au symbole QR [15].

Il existe plusieurs outils de création de codes QR qui sont disponibles en ligne et gratuitement. Ils se distinguent les uns des autres par [14] :

- Leurs capacités de production : texte, URL, appel téléphonique, SMS, vCard...
- Correction des erreurs du code produit.
- La possibilité de personnaliser les couleurs des pixels, du fond et de la bordure.
- Le format des images (jpeg, png, eps, tiff, svg), un code QR ainsi vectorisé peut être agrandi sans déformation par exemple pour être imprimé sur une bâche.

Les générateurs de codes QR ont été recensés sur le site 2d code QR 9 [14] :

- GOQR.ME 10 : outil simple permettant d'aboutir à un texte, une URL, un SMS, une vCard.
- Mobile Fish 12 : générateur permettant de localiser un lieu.
- MOJI-Q 13 : avec possibilité d'intégrer un texte dans le code. La version japonaise de ce générateur permet de davantage varier les couleurs et de créer un effet miroir.
- QR Code and 2D Code Generator 14 : cet outil propose une vingtaine d'actions et permet de générer des codes QR vectorisés.
- QReate & Track 15

Des générateurs de codes QR sont proposés sous forme d'applications mobiles. Par exemple QRS+16, QR Code Generation, etc.

2.4.6 Lecture du code QR

La lecture des symboles de la matrice sera réalisée à l'aide d'un capteur CCD (capteur de surface). Les données de la ligne de balayage capturées par le capteur seront stockées dans la mémoire. Ensuite, à l'aide du logiciel, les détails seront analysés, les modèles de positionnement identifiés, et la position/taille/angle du symbole détecté, et le processus de décodage sera mis en œuvre.

Le rapport entre le noir et le blanc de la ligne de balayage qui traverse les trois **modèles de positionnement (Finder Pattern)** qui sont positionnés dans les trois coins du code est toujours 1 :1 :3 :1 :1 lorsqu'il est vu de n'importe quelle direction parmi les 360°qui l'entourent. En détectant ce rapport spécifique, le modèle de positionnement peut être détecté parmi l'image capturée par le capteur CCD pour identifier la position du code QR dans un court laps de temps. En outre, en identifiant les relations de position des trois motifs de positionnement énumérés à la figure 2.6 parmi le champ d'image du capteur CCD, la taille, l'angle et la forme extérieure du symbole peuvent être détectés simultanément [12].

Il existe plusieurs applications qui permettent de lire un code QR en utilisant la caméra intégrée du smartphone, cette lecture se fait en 3 étapes :

Etape 1 : Ouvrir l'application d'appareil photo, soit depuis l'écran de verrouillage soit depuis l'icône de l'écran d'accueil.

Etape 2 : Stabiliser l'appareil pendant 2-3 secondes en direction du code QR.

Etape 3 : Cliquer sur la notification pour ouvrir le contenu du code QR. En fonction du code QR scanné, une action différente sera demandée. Par exemple, les codes d'URL demanderont d'ouvrir le lien avec Google Chrome.

Exemple d'applications : QR Code Reader, Lightning QR Scanner, etc.

2.4.7 Sécurisation du réseau WiFi via le code QR

Pour éviter qu'un réseau WiFi se fasse pirater, le premier réflexe qui vient à l'esprit est de compliquer le plus possible son mot de passe. D'autres techniques moins compliquées permettent d'avoir de meilleurs résultats, il en est ainsi de l'utilisation des codes QR.

Les Codes QR présentent de nombreux avantages pour protéger l'accès à un réseau WiFi. L'avantage principal est sa simplicité et sa praticité ; ça ne prend que quelques secondes pour le scanner. Un autre avantage procuré par l'utilisation des codes QR est son efficacité. Malgré le fait qu'il soit très simple à utiliser, cela ne l'empêche pas d'être l'un des moyens les plus efficaces pour sécuriser son réseau. Un Code QR est unique et ne peut être dupliqué ou copié.

Néanmoins le code QR peut être utilisé pour pirater les utilisateurs. En septembre 2011, Kaspersky Lab a détecté le premier code QR malveillant du genre. La méthode d'attaque utilisée dans le code QR était la suivante : lorsqu'un utilisateur scanne le code, il est dirigé vers un site web, puis un fichier malveillant se télécharge dans l'appareil de l'utilisateur à son insu. C'est la seule méthode d'attaque connue sur les codes QR malveillants. les spécialistes en sécurité informatique ont détecté plusieurs sites web malveillants contenant des codes QR pour des applications mobiles qui comprenaient un cheval de Troie capable d'envoyer des messages texte à des numéros courts surtaxés [16].

2.5 Cahier des charges

La décision d'engager un travail sur l'authentification QR a été motivée par le besoin de proposer une solution pour contrôler et sécuriser l'accès au réseau WiFi de la gare maritime de l'Entreprise Portuaire de Bejaïa (l'EPB), dans le but de mettre à disponibilité des voyageurs un meilleur service internet. Nous allons procéder à ce travail en utilisant un code QR, il est unique et sécurisé ce qui est l'idéal pour atteindre notre objectif qui est de renforcer la sécurité d'un réseau.

L'usage des codes QR reste simple, efficace et ludique. Cette technique se révèle particulièrement utile pour partager une connexion internet. La solution proposée sera réalisée en deux étapes :
• La première étape consiste à générer un code QR contenant les informations des utilisateurs(nom d'utilisateur et mot de passe) grâce à un générateur QR, pour ensuite les scanner grâce au lecteur QR inséré dans la page d'authentification WiFi de l'EPB.
• La deuxième étape consiste à programmer la page d'authentification en utilisant les langages HTML, CSS, PHP, et javascript. Les deux premiers serviront à donner une structure à la page, php se chargera de l'aspect connexion à la base de donnée, quant à javascript son utilité sera la mise en oeuvre d'un programme qui permettra d'intégrer un lecteur QR à cette page. Suite au scan du code, les données seront automatiquement insérées aux champs adéquats pour la vérification.

2.6 Conclusion

De nos jours, un code QR est appliqué dans différents flux d'applications liés au marketing, à la sécurité, aux universitaires, etc. et gagne en popularité à un rythme très élevé. Jour après jour, de plus en plus de gens prennent conscience de cette technologie et l'utilisent en conséquence. La popularité du code QR croît rapidement avec la croissance des utilisateurs de smartphones et donc le code QR arrive rapidement à des niveaux élevés d'acceptation dans le monde entier.

Nous avons présenté dans ce chapitre l'organisme d'accueil. Nous avons également posé la problématique de la gare maritime et détaillé le code QR. Enfin, nous avons établi le cahier des charges résumant les objectifs de notre projet.

Chapitre 3

Mise en oeuvre de la solution

3.1 Introduction

Dans ce chapitre, nous présentons les différents langages de programmations, outils et algorithmes utilisés tout en expliquant toutes les étapes suivies du début à la fin de la conception et réalisation du projet.

3.2 Outils et langages de préparation de l'environnement

3.2.1 Javascript

Le principal langage de script pour les navigateurs Web et il est essentiel aux applications Web modernes. Les programmeurs ont commencé à l'utiliser pour écrire des applications complexes. Ce langage, initialement créé par la société Netscape, permet de rendre une page HTML bien plus interactive, en y insérant du code réagissant, par exemple, aux évènements de l'utilisateur, ou encore à valider les données saisies dans un formulaire HTML. Ces scripts vont être gérés et exécutés par le navigateur lui-même sans devoir faire appel aux ressources du serveur. Ces instructions seront donc traitées en direct et sans retard par le navigateur [18].

3.2.2 HTML (HyperText Markup Language)

Langage de balisage utilisé pour la création de pages web. Il s'agit d'un langage dont les standards permettent à tous les Webmasters de créer des sites Internet en liant des pages HTML les unes avec les autres par des hyperliens [18].

3.2.3 CSS (Cascading Style Sheets)

Langage informatique utilisé pour appliquer des styles à un contenu et le mettre en forme. Ainsi, avec le CSS, on pourra changer la couleur ou la taille d'un texte, positionner tel contenu à tel endroit de notre page web ou ajouter des bordures ou des ombres autour d'un contenu [22].

3.2.4 Php (Hypertext Preprocessor)

C'est un langage de scripts multiplateformes incorporé dans des pages HTML. Il a été spécifiquement conçu pour résoudre le problème du web [19]. Il est utilisé pour la conception de sites web dynamiques.

3.2.5 PfSense

Pfsense est une distribution gratuite et personnalisée de FreeBSD (un support d'exploitation pour une variété de plateformes, qui se concentre sur les caractéristiques, la vitesse et la stabilité) [21]. Ce support est un outil très flexible et puissant qui peut s'adapter à de nombreuses applications, d'un routeur domestique à un pare-feu, pour un grand réseau d'entreprise. Il possède également de nombreuses caractéristiques que l'on trouve généralement que dans les routeurs commerciaux coûteux. Il convient pour la sécurisation d'un réseau domestique ou d'une entreprise [21]. Pfsense a plusieurs fonctionnalités, il peut être utilisé comme : un routeur LAN ou WAN, un hotstop sans fil, un routeur VPN, un Serveur DHCP ou DNS, un pare-feu, un portail captif [21].

3.2.5.1 Pare-feu

Un pare-feu est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celles-ci définissant quels sont les types de communications autorisées sur ce réseau informatique, Il surveille et contrôle les applications et les flux de données (paquets) [20]. PfSense peut être configuré comme un pare-feu open source basé sur le système d'exploitation FreeBSD. Il utilise le pare-feu à états packetFilter, des fonctions de routage et de NAT lui permettant de connecter plusieurs réseaux informatiques. Il comporte l'équivalent libre des outils et services utilisés habituellement sur des routeurs professionnels propriétaires. pfSense convient pour la sécurisation d'un réseau domestique ou petite entreprise [21]. Après une brève installation manuelle pour assigner les interfaces réseaux, il s'administre ensuite à distance depuis l'interface web et gère nativement les VLAN [20].

3.2.5.2 Portail Captif

Un portail captif est une structure permettant un accès rapide et sécurisé à Internet. Lorsqu'un utilisateur cherche à accéder à Internet pour la première fois, le portail capte sa demande de connexion grâce à un routage interne et lui propose de s'identifier afin de pouvoir recevoir son accès [20]. Cette demande d'authentification se fait via une page web stockée localement sur le portail captif grâce au serveur HTTP (Hypertext Transfer Protocol). Ceci permet à tout ordinateur équipé d'un « Web browser » ou navigateur web et d'un accès WiFi de se voir proposer un accès à Internet. La connexion au serveur est sécurisée par SSL (Secure Sockets Layer) grâce au protocole HTTPS (HyperText Transfer Protocol Secure) ce qui garantit l'inviolabilité de la transaction. Les identifiants de connexion (Login et Mot de passe) sont stockés dans une base de données qui est hébergée localement ou sur un serveur distant. Une fois l'utilisateur authentifié, les règles de firewall (pare-feu) le concernant sont modifiées et celui-ci se verra autorisé à utiliser son accès Internet pour une durée fixée par l'administrateur. A la fin de la durée fixée, l'utilisateur se verra redemander ses identifiants de connexions afin d'ouvrir une nouvelle session.

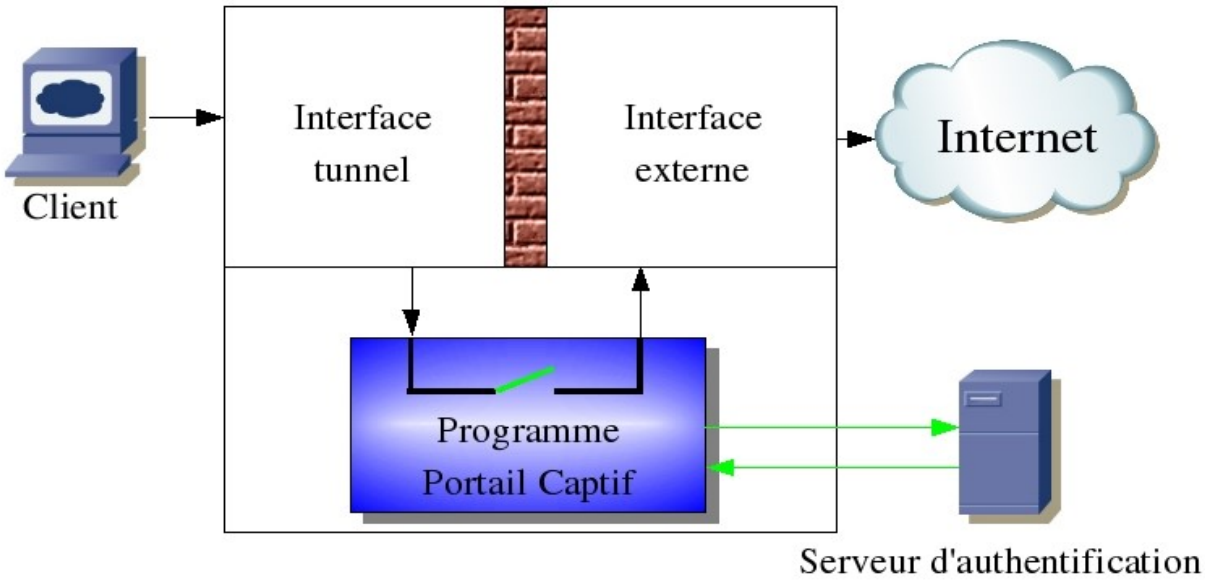

FIGURE 3.1 – Fonctionnement d'un portail captif.

3.3 Algorithmes utilisés

La lecture du code QR est complexe et contrairement à ce qu'il parait, sa lecture nécessite l'utilisation de quelques algorithmes. Voici les algorithmes que nous utiliserons afin de déchiffrer ce code QR :

3.3.1 Algorithme de Bresenham

Un algorithme de contrôle informatique d'un type de traceur numérique qui est maintenant couramment utilisé avec les ordinateurs numériques. Le traceur considéré est capable d'exécuter, en réponse à une implémentation appropriée, n'importe lequel des huit mouvements linéaires indiqués à la figure 3.2. Ainsi, le traceur peut se déplacer linéairement d'un point sur un maillage à n'importe quel point adjacent sur le maillage[23].

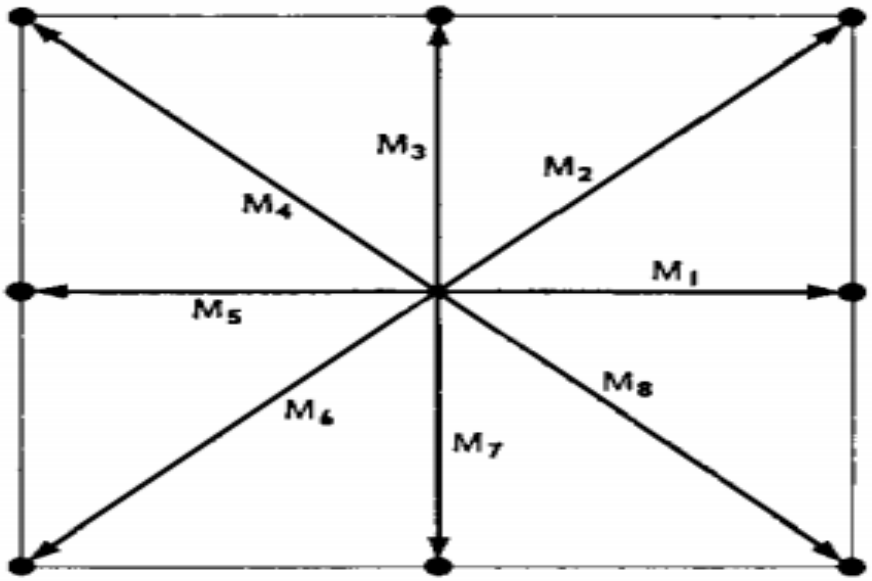

FIGURE 3.2 – Les maillages de l'algorithme de Bresenham.[23]

3.3.2 La distance de Hamming

Le code de Hamming est un code correcteur, son objectif est la détection ou la correction d'erreurs après la transmission d'un message. Cette correction est permise grâce à l'ajout d'informations redondantes. Le message est plongé dans un ensemble plus grand, la différence de taille contient la redondance, l'image du message par le plongement est transmise. En cas d'altération du message, la redondance est conçue pour détecter ou corriger les erreurs. La détection d'une erreur se fait par le calcul de la distance de Hamming entre deux mots du message transmis [24].

3.3.3 Algorithme Euclidien

L'algorithme euclidien ou son équivalent peut être utilisé pour trouver le polynôme de localisation d'erreur et le polynôme d'évaluateur d'erreur dans l'équation clé de Berlekamp qui est nécessaire pour décoder un code Reed-Solomon (RS) [25].

3.3.3.1 Algorithme de recherche de Chien

La recherche Chien, du nom de Robert Tienwen Chien, est un algorithme qui est couramment utilisé pour trouver les racines des polynômes de localisation d'erreur rencontrés dans le décodage des codes Reed-Solomon et des codes BCH(reprenant les initiales de ses inventeurs : Bose, Ray-Chaudhuri et Hocquenghem) [26].

3.3.4 Code de Reed-Solomon

Les codes de Reed – Solomon sont des codes correcteurs d'erreurs utilisés dans tous les domaines requérant des données fiables. Typiquement, dans les communications spatiales, télévision numérique et stockage de données. Ils permettent de corriger des erreurs et des effacements grâce

à des symboles de contrôle ajoutés après l'information, ces symboles sont générés à l'aide de polynômes particuliers, appelés polynômes générateurs [27].Ce code de Reed-Solomon est basé sur un principe mathématique qui a pour objectif de construire un polynôme à partir des messages à transmettre, les messages sont divisés en blocs, et des informations redondantes sont ajoutées à chaque bloc, le résultat est alors envoyé, au lieu des messages originaux. La redondance permet au récepteur du message encodé de reconstruire le polynôme source même s'il y a eu des erreurs pendant la transmission.

3.4 Configuration et réalisation

Le projet réalisé consiste à contrôler le réseau WiFi de l'EPB de sorte à ce que l'accès soit possible juste après le scan du code QR. Malheureusement, suite à nos recherches, nous avons découvert que modifier l'état du réseau d'un smartphone, tablette ou ordinateur portable via une page dynamique n'est pas faisable, car si un simple code HTML ou Javascript suffisait à changer l'état du réseau, cela résulterait en une faille de sécurité et tout appareil accédant au site serait compromis. Pour remédier à ce problème tout en respectant l'idée initiale du projet qui est l'utilisation d'un code QR pour accéder à un réseau WiFi. Nous avons décidé de résoudre la problématique traitée d'une autre façon, qui est la configuration du portail captif avec authentification, la solution se fera donc comme suit :

1. Configuration d'un portail captif avec authentification.
2. Création des utilisateurs avec le privilège « captif portal login ».
3. Création d'un code QR correspondant à cet utilisateur. Suite à cela, l'authentification se fera en scannant le code QR dans la page du portail captif, après la saisie des données le voyageur n'aura qu'à confirmer avec le bouton **connexion**.

Afin de concrétiser ce projet, nous avons suivi un ordre précis pour la réalisation d'un portail captif, ces étapes sont les suivantes :

3.4.1 Création de la page HTML du portail captif

Cette page web dynamique est la page vers laquelle le voyageur sera dirigé suite à sa tentative d'accès au réseau WiFi de la gare maritime, elle est conçue grâce aux deux langages HTML (Hyper Text Markup Language) et CSS (Cascading Style Sheets). Quant à la partie PHP (HypertextPreprocessor) du code, elle servira à la vérification des données saisies, et se fera grâce à un formulaire servant de lien avec la base de données. La figure ci-dessous représente le formulaire grâce auquel la vérification des données saisies du code QR est possible.

```
<form class="box" action="$PORTAL_ACTION$" method="post" name="login">
<h1 class="box-title">Connexion</h1>
<input type="password" class="box-input" name="username" id="username" placeholder="Nom d'utilisateur">
<input type="password" class="box-input" name="password" id="PSW" placeholder="Mot de passe">
<input name="auth_voucher" type="text">
<input name="redirurl" type="hidden" value="$PORTAL_REDIRURL$"
<input type="submit" value="Connexion" name="submit" class="box-button">
```

FIGURE 3.3 – Formulaire d'authentification du code QR.

3.4.2 Création du lecteur QR en Javascript

Le code que nous avons programmé afin de scanner un code QR, comprend les étapes suivantes :

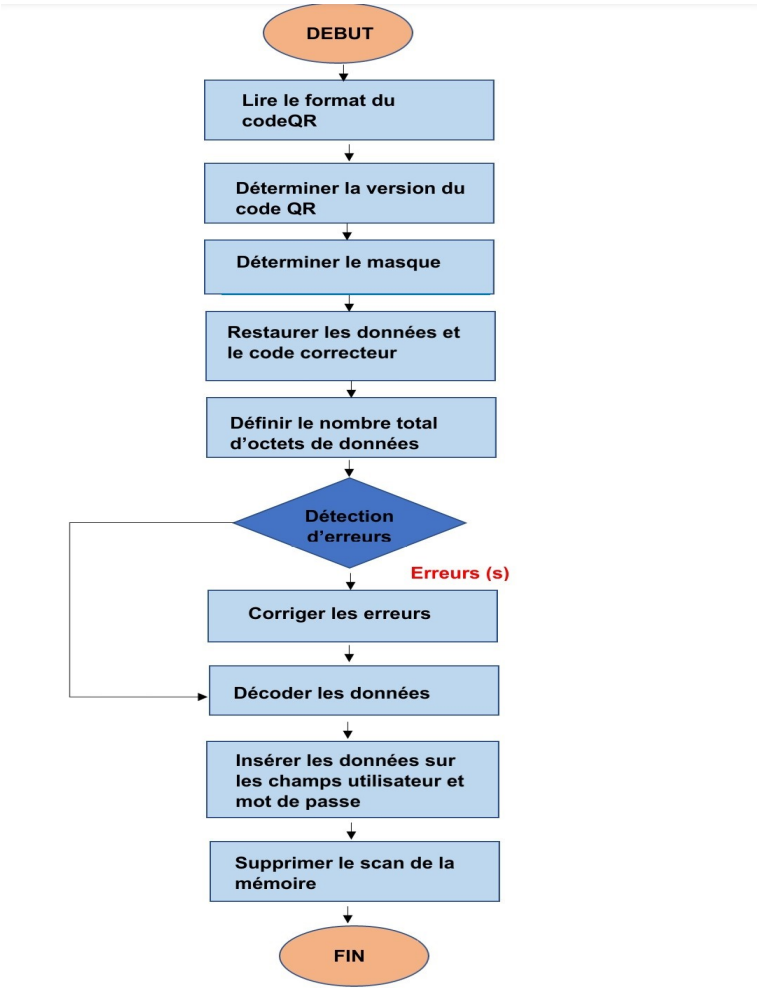

FIGURE 3.4 – Organigramme du déchiffrement du code QR.

1. Lire le format en détectant la position exacte des trois **Finder Pattern**, puis identifier les **Alignment Pattern** ainsi que les **Timing Pattern** en utilisant l'algorithme de Bresenham pour se déplacer dans le code QR.
2. Déterminer la version du code QR.
3. Déterminer le masque utilisé, puis démasquer les données qui signifie séparer le masque des données.
4. Compter le nombre total d'octets de données.
5. Corriger les erreurs et copier les blocs de données ensemble dans un flux d'octets.
6. Décoder le contenu du flux d'octets.
   Les étapes 4, 5 et 6 sont faites grâce aux algorithmes de Reed Solomon, de Bresenham, la distance de Hamming, Euclidien et de recherche Chien.
7. Insérer le contenu du code QR dans les deux champs utilisateur et mot de passe du portail captif.
8. Supprimer le scan de la mémoire et arrêt du scan.

Le code nécessite un navigateur compatible avec la méthode **getUserMedia()**, afin d'utiliser la fonction **Navigator.mediaDevices.getUserMedia()** qui demande à l'utilisateur la permission d'utiliser une entrée vidéo (ex : une webcam ou un écran partagé) ou audio (ex : un microphone) de son appareil. La majorité des navigateurs sont compatibles avec **getUserMedia** comme : google chrome, Mozilla Firefox et la dernière version de Internet Explorer.

3.4.3 Configuration de Pfsense/Portail captif

Nous arrivons à la dernière étape du projet qui consiste à mettre en place le portail captif et l'adapter à nos besoins. Pour cela, nous avons tout d'abord commencé par le créer dans la partie « **Services** –> **Portail captif** », suite à cela, nous avons défini les propriétés que l'on juge importantes. Tout d'abord :

- Choisir l'interface LAN : car nous gérons les connexions du réseau local LAN.
- Idle timeout : le temps d'inactivité après lequel l'utilisateur sera déconnecté. Dans ce cas là, l'utilisateur sera automatiquement déconnecté s'il reste plus de 30 minutes sans activité sur le réseau.
- Hard timeout : le temps de connexion permis. Cette option détermine le temps de connexion auquel le voyageur a le droit. Dans notre cas ce temps est de 60 minutes, la session de l'utilisateur aura expiré après ce délai.
- Maximum concurrent connections : les connexions simultanées autorisées. Dans notre cas, il n'y a pas de limite pour celle-ci, plusieurs appareils peuvent se connecter avec le même nom d'utilisateur et mot de passe.

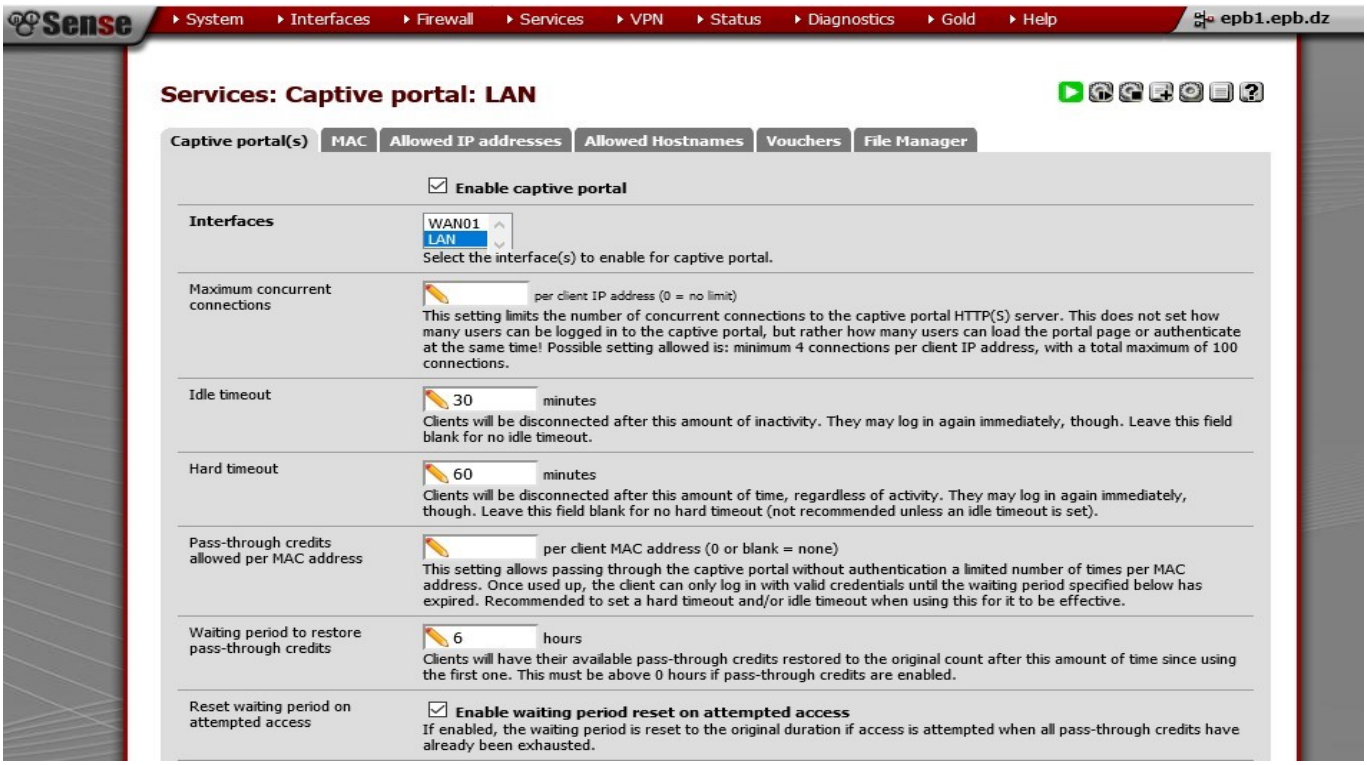

FIGURE 3.5 – Configuration des contraintes temporelles du portail captif.

Dans cette étape, nous définissons la page vers laquelle sera redirigé l'utilisateur après une authentification valide avec l'option **After authentification redirection URL**.

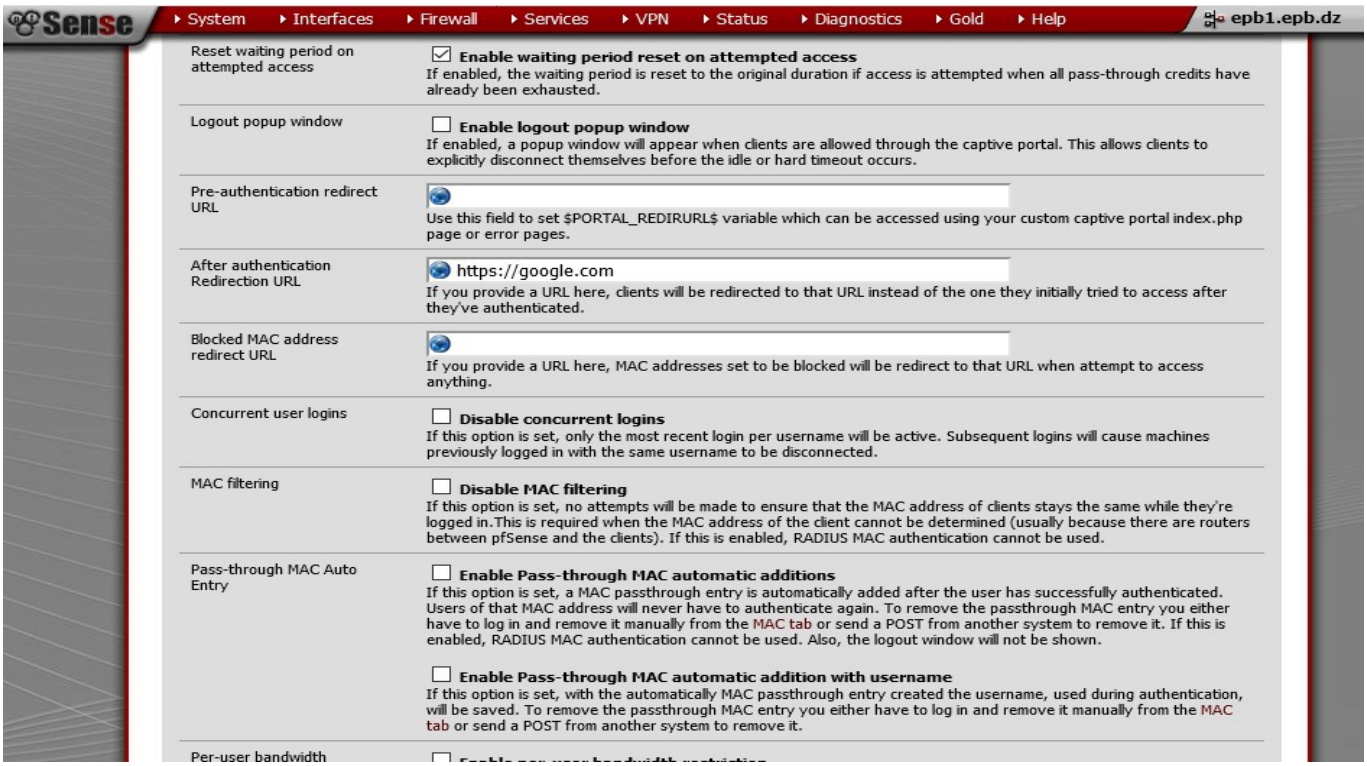

FIGURE 3.6 – Configuration de la page post-authentification réussie.

Ici, nous modifions le mode d'authentification qui était auparavant sur « No Authentification » à « Local User Manager/Voucher », où seuls les utilisateurs ayant comme privilège « **Captive portal login** » pourront s'y authentifier.

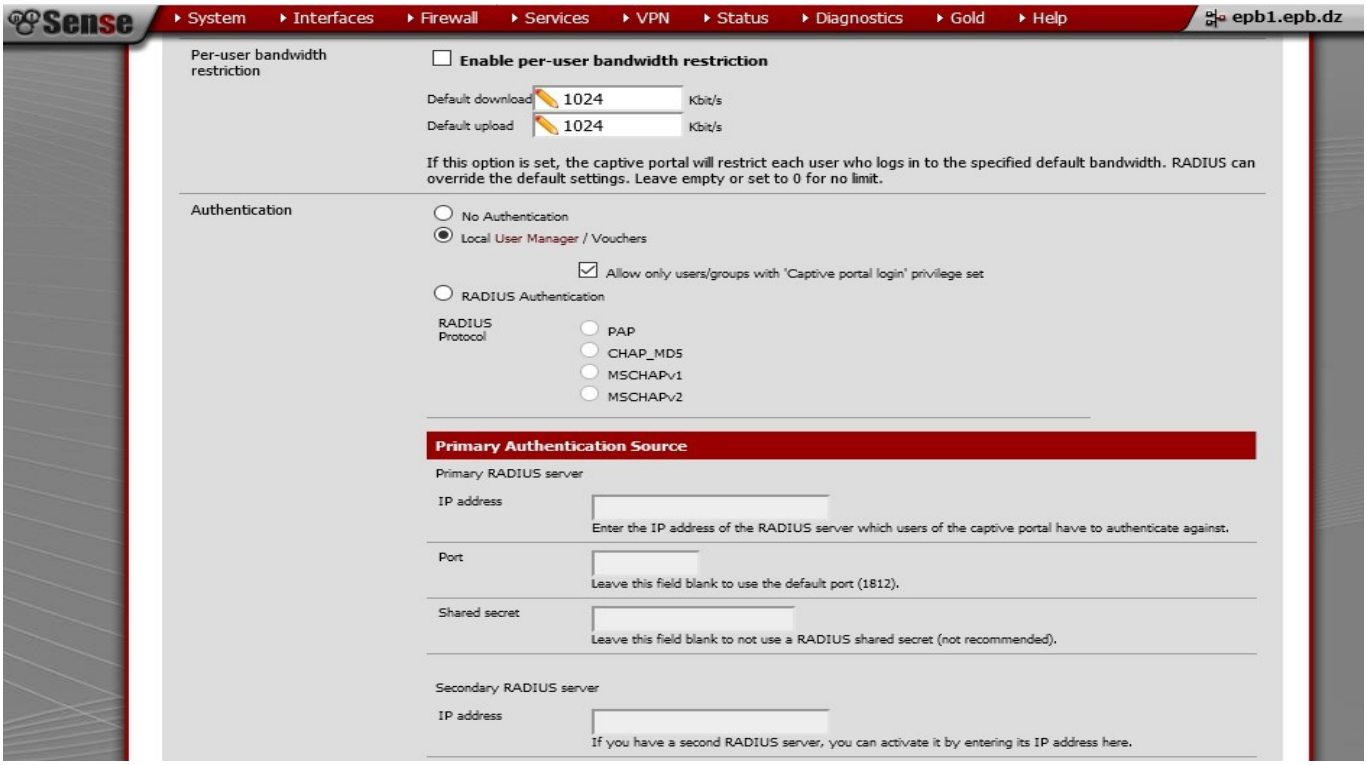

FIGURE 3.7 – Configuration du mode authentification "Local user manager/Voucher".

Dans la dernière étape de la configuration du portail captif, nous insérons le code source que nous avons conçu avec HTML, CSS, PHP, et javascript. Et cela en sélectionnant **parcourir** dans l'option « **Portal page contents** ».

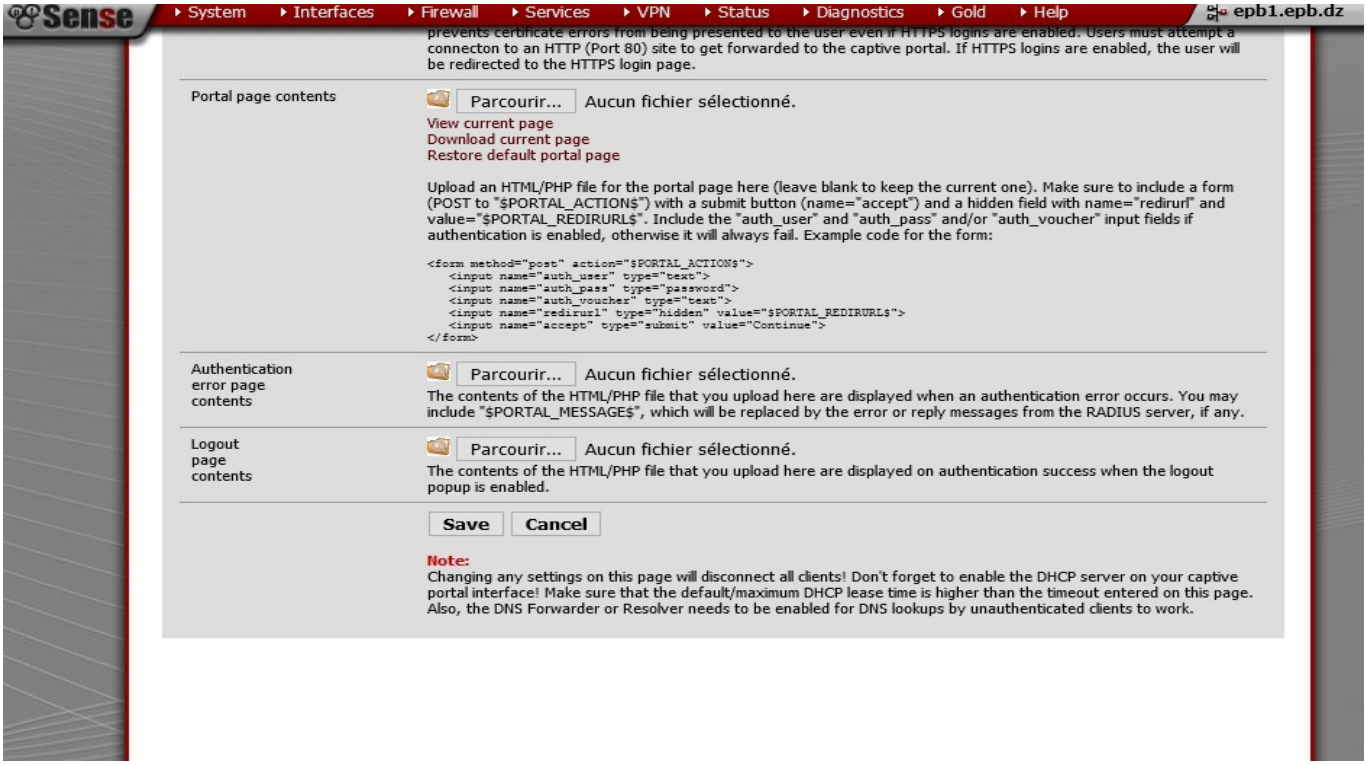

FIGURE 3.8 – Configuration de la page du portail captif.

Nous passons maintenant à la création des utilisateurs. Pour cela, nous devons nous rendre à " **System** –> **User Manager**", puis ajouter un utilisateur.

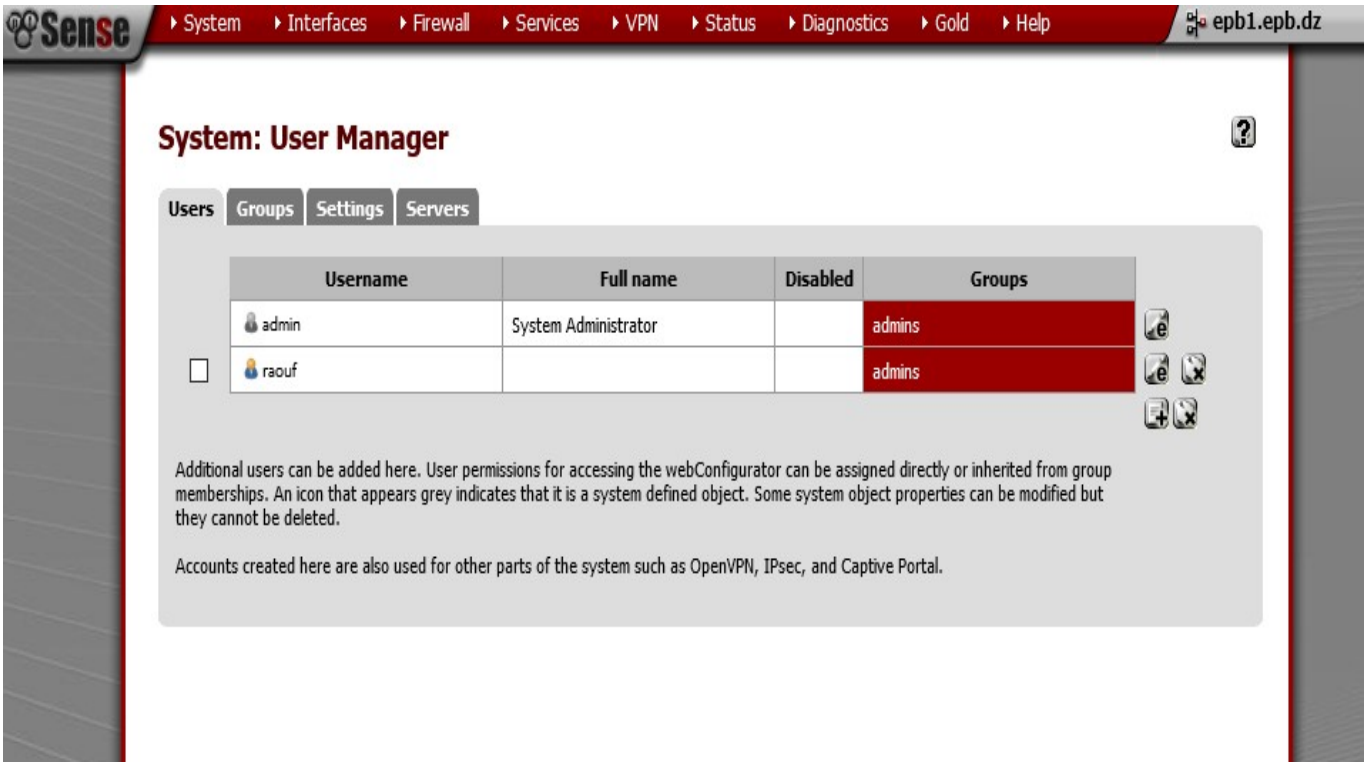

FIGURE 3.9 – Page de tous les utilisateurs.

Nous donnons un nom significatif à l'utilisateur « garemaritime » tout en ne l'affectant à aucun groupe.

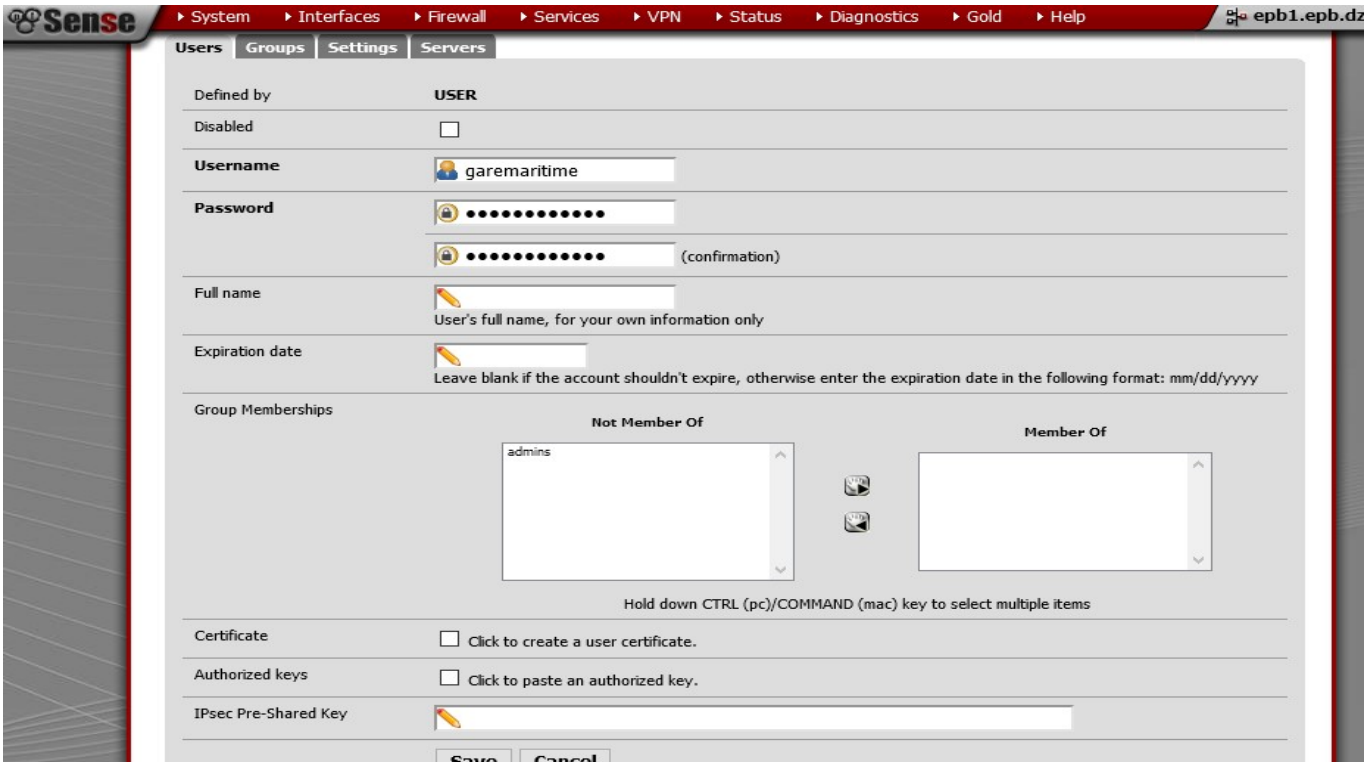

FIGURE 3.10 – Création de l'utilisateur "garemaritime".

Nous attribuons le privilège "**Captive portal login**", qui est la condition d'authentification au portail captif.

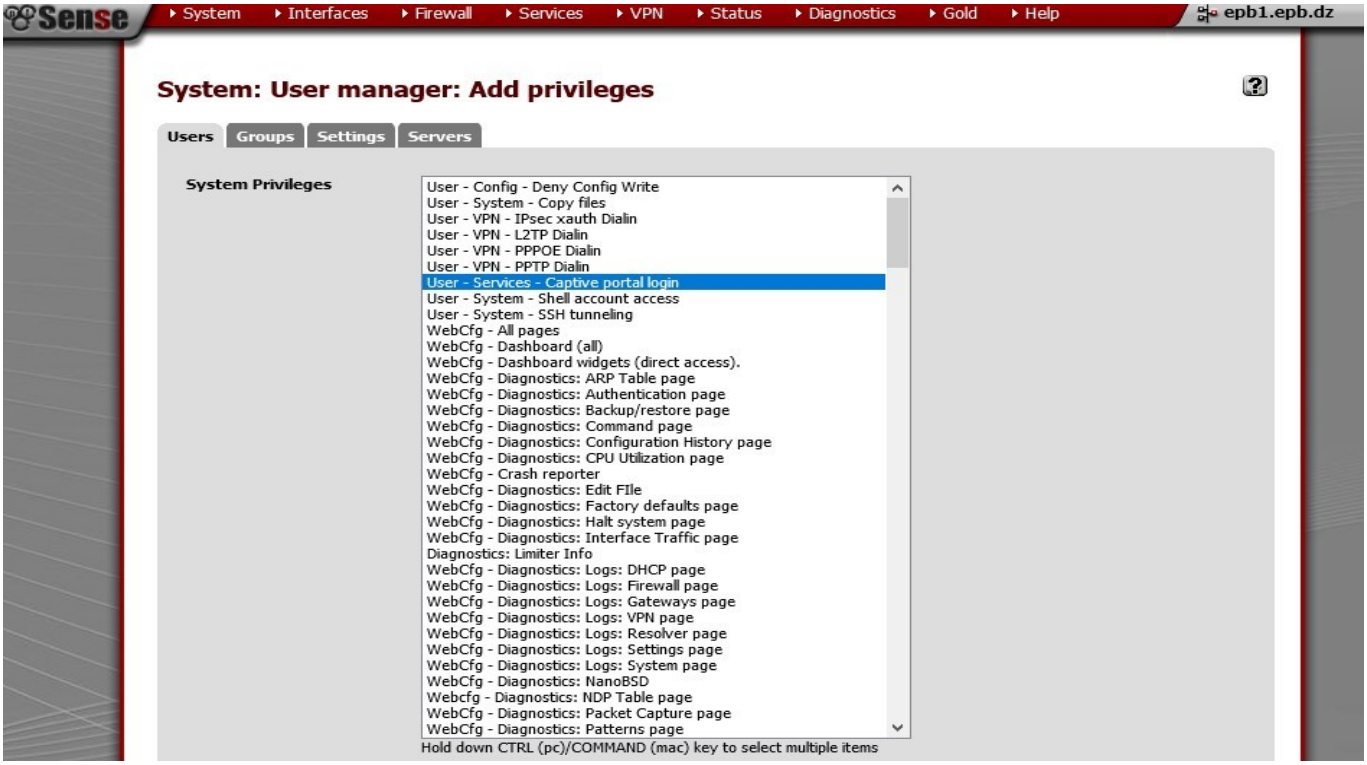

FIGURE 3.11 – Attribution des privilèges à l'utilisateur.

La dernière étape avant la validation de l'ajout de l'utilisateur est de s'assurer d'avoir ajouté le privilège "**Captive portal login**" qui lui permettra de s'authentifier si les données entrées sont correctes. Suite à cela, nous validons l'ajout de l'utilisateur.

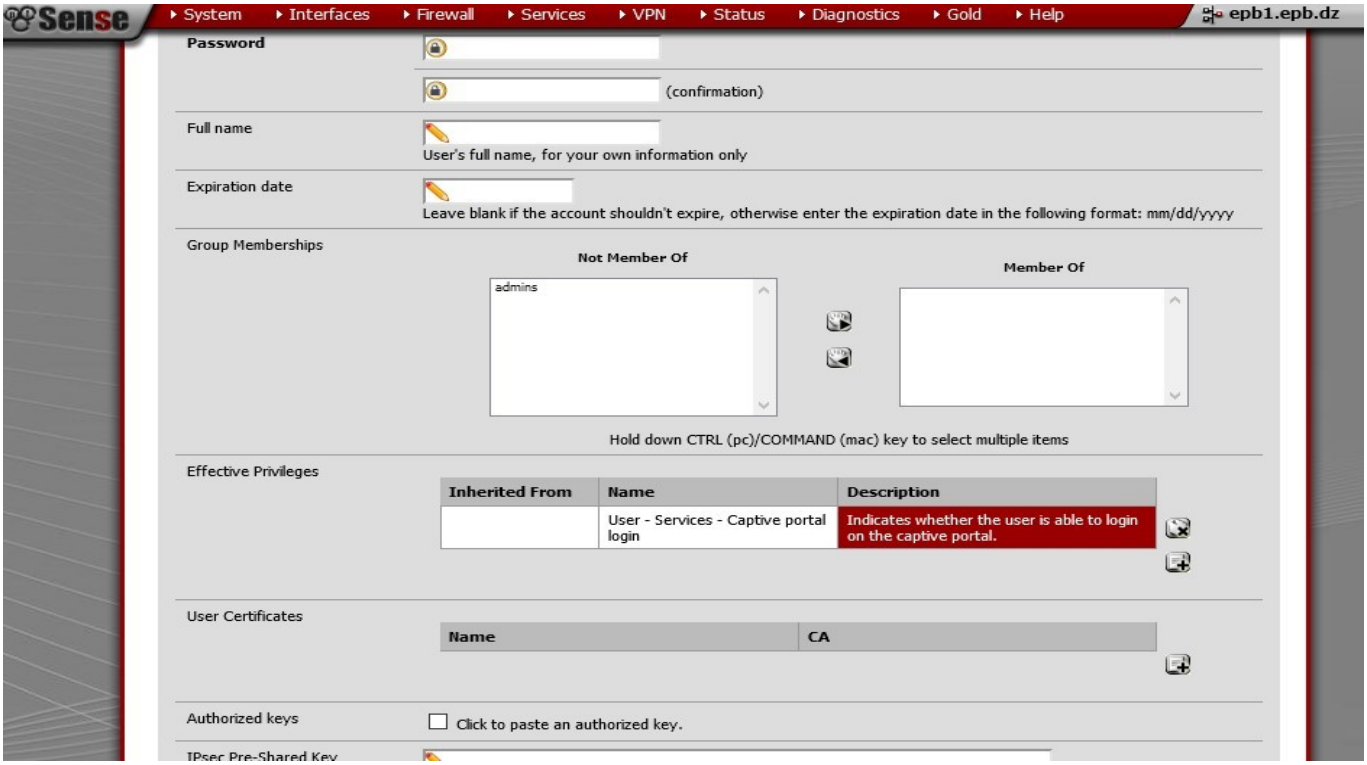

FIGURE 3.12 – Création du profil de l'utilisateur terminé.

Le code QR utilisé est ensuite généré par le site "**www.goqr.me**". Nous utilisons le type **text** afin de coder le mot "**garmaritime** qui est le nom utilisé pour notre compte utilisateur. Puis, nous téléchargeons le code.

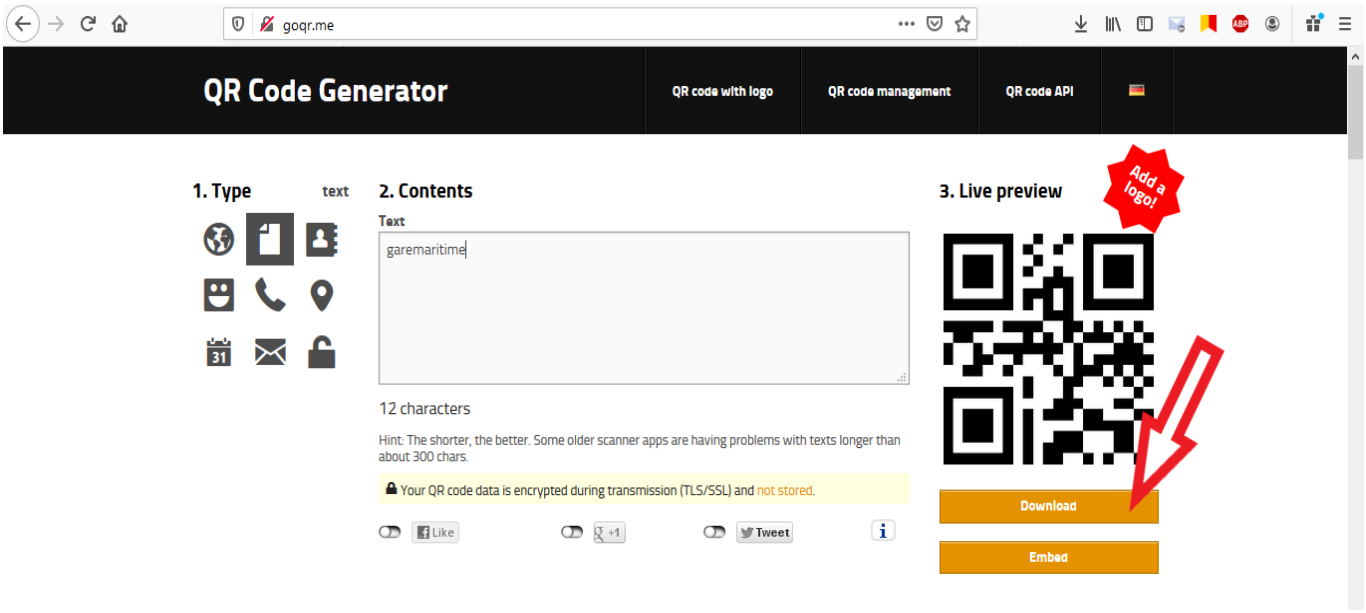

FIGURE 3.13 – Création du code QR correspondant à l'utilisateur"garemaritime".

Le code utilisé est le code ci-dessous.

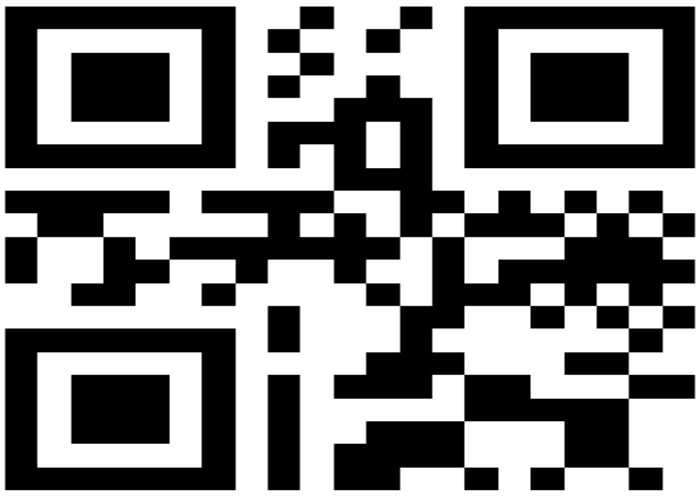

FIGURE 3.14 – Code QR correspondant à "garemaritime".

Enfin, suite à toutes ces étapes nous arrivons à ce résultat :

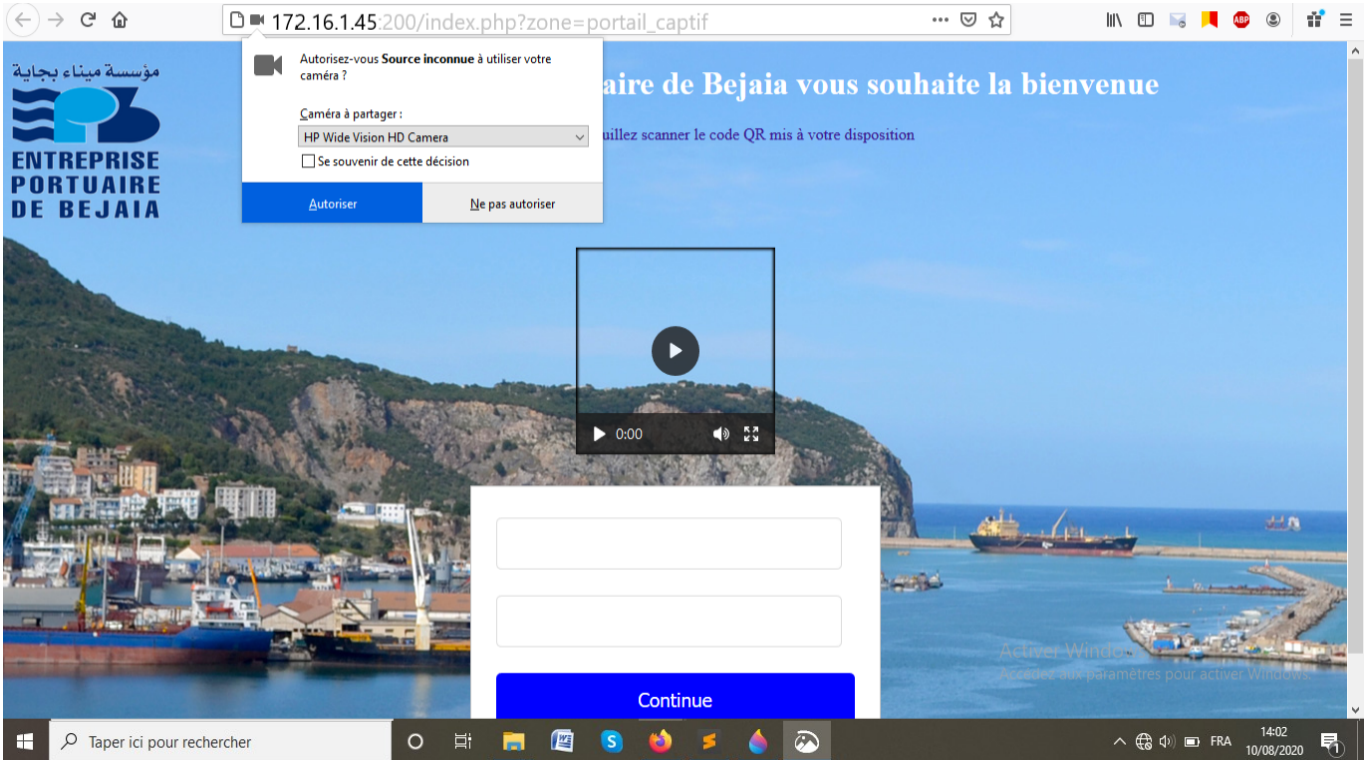

FIGURE 3.15 – Page web du portail captif.

Après avoir autorisé l'accès à la caméra, cette dernière s'allume et nous positionnons le code QR devant elle.

FIGURE 3.16 – Scan du code QR.

Le code QR est décrypté grâce au code et le contenu est inséré dans les deux champs utilisateurs et mot de passe. L'utilisateur n'a qu'à valider en cliquant sur le bouton continuer pour vérifier les informations entrées. L'utilisateur "garemaritime" aura le même nom d'utilisateur et mot de passe pour faciliter le scan, le code QR contenant le texte « garemaritime » sera scanné et inséré dans les deux champs nom d'utilisateur et mot de passe, ces deux champs seront de type « password » pour garder la confidentialité du compte.

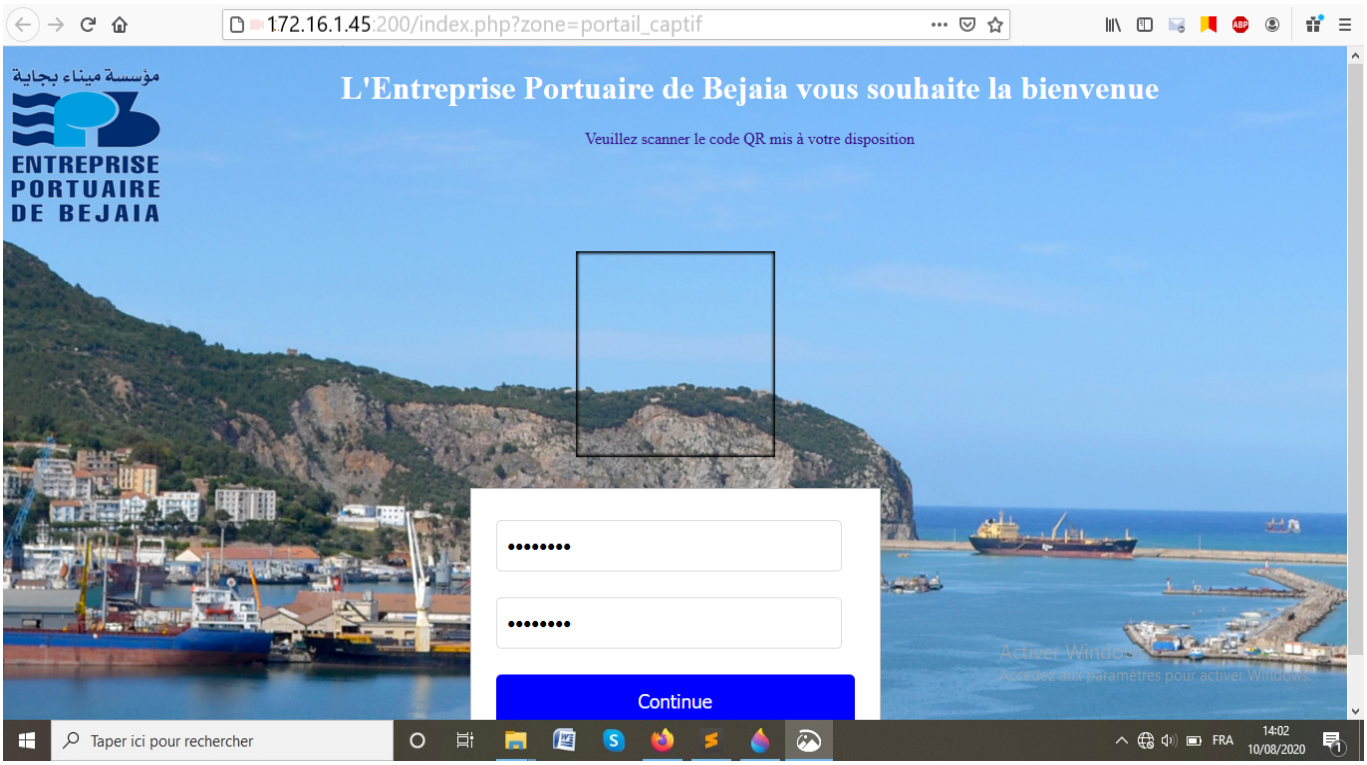

FIGURE 3.17 – Insertion des données dans leurs champs.

Dans cette dernière capture d'écran, nous constatons que l'authentification est valide, par conséquent notre machine est redirigée vers la page de google et est maintenant connectée au réseau de la gare maritime.

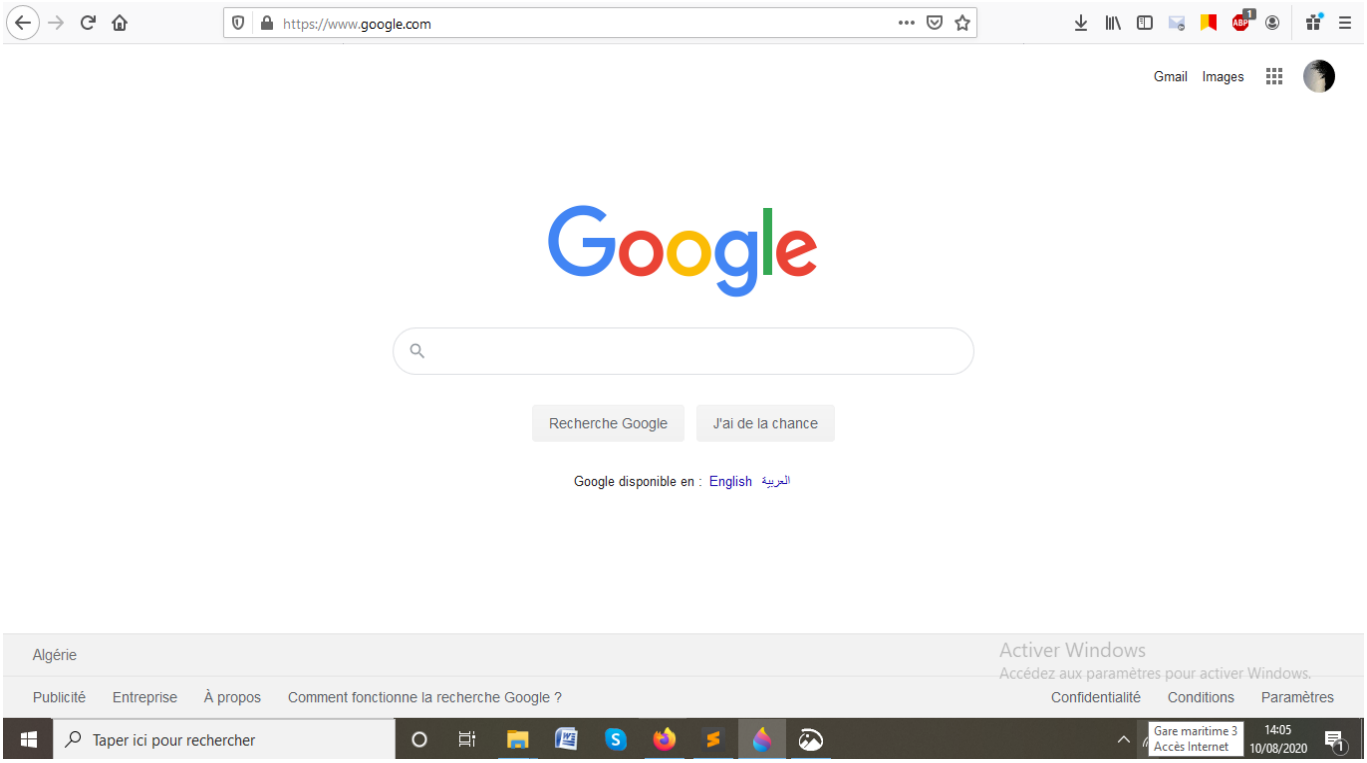

FIGURE 3.18 – Authentification réussie.

3.5 Conclusion

Tout au long de ce chapitre, nous avons abordé les différentes étapes de réalisation et les résultats des tests de l'authentification QR à un réseau WiFi, mais aussi les difficultés rencontrées en réalisant un portail captif à authentification QR.
Suite aux tests effectués, les résultats obtenus sont satisfaisants et ceci malgré la complexité du projet et des algorithmes utilisés pour le décodage et la lecture d'un code QR.

Conclusion Générale

Le projet réalisé a pour but de trouver une solution au problème que rencontre l'entreprise portuaire de Bejaïa en termes de sécurité et de contrôle d'accès de leur réseau WiFi afin que ce dernier soit réservé aux voyageurs de la gare maritime seulement.

Durant ce projet, nous avons pu mettre en œuvre les connaissances théoriques et pratiques acquises durant notre cursus. Nous avons réalisé ce travail en combinant programmation et configuration réseau pour répondre aux besoins de l'entreprise portuaire de Bejaïa.

Le code QR, bien que peu utilisé en Algérie, est la solution qui nous parait la plus adéquate aux besoins de la gare maritime, il rassemble les deux critères les plus importants d'une bonne solution car il est simple et très efficace. Même après avoir fait face à certaines difficultés quant à la mise en œuvre de notre idée, cela ne nous a pas empêchés d'obtenir le résultat attendu.

Bien qu'il fût court, notre stage pratique au sein de cette entreprise nous a permis de mettre en œuvre et en pratique nos idées ainsi que nos connaissances tout en découvrant le monde du travail en entreprise. Notre stage qui s'est déroulé à la direction système d'informations et à la gare maritime consistait à en apprendre plus sur l'entreprise portuaire de Bejaia, son système informatique plus précisément le fonctionnement de leur pare-feu Pfsense.

L'intérêt principal que nous avons tiré de cette étude est que nous avons bien affronté la vie professionnelle du domaine de l'informatique. Nous avons évalué les différentes étapes de réalisation d'un projet ainsi que les techniques développées par les spécialistes du domaine pour assurer l'efficacité et la bonne réalisation des travaux en se limitant aux ressources et à des durées de temps exactes. Nous avons pu voir la complexité de la mise en route d'un nouveau projet et de sa rapide évolution qui nous a appris à mieux nous organiser afin d'être capable de finaliser notre travail.

Bibliographie

[1] Aurélien Géron Préface de Marc Taieb.“ WIFI professionnel. La norme 802.11, le déploiement, la sécurité ”. Dunod. Paris. 2009. 3ème édition. (p 8 – 219).

[2] Di Gallo Frédéric.“ WiFi L'essentiel qu'il faut savoir ”. Dunod. Paris. 2003. (p 5).

[3] Claud Servin.“ Réseaux et télécom ”. Dunod. Paris. 2003. 4ème édition. (p 418).

[4] Philippe Gomez et Pierre Bichon. “ Comprendre les réseaux d'entreprise ”. CHIHAB-EYROLLES. 1996. (p 11).

[5] Michèle Germain. 802.11 DANS TOUS SES ÉTATS. Version 3. 2011. (p 2 - 8).

[6] Gwendal LE GRAND, Artur HECKER, et Franck SPRINGINSFELD. Architecture flexible de réseau sans fil WiFi sécurisé. 2004. (p 1).

[7] Fabrice Lemainque. Comment ça marche : Tout sur les réseaux sans fil. DUNOD. 2009. (p 2).

[8] http ://portdebejaia.dz/qui-sommes-nous/.

[9] http ://portdebejaia.dz/activites-du-epb/.

[10] http ://portdebejaia.dz/nouvelle-gare-maritime/.

[11] Documents internes de l'EPB.

[12] Tan Jin Soon. 2008. section Three. QR Code. synthesis journal. (p 59- 67).

[13] M. Mary Shanthi Rani, K.Rosemary Euphrasia. 2016. DATA SECURITY THROUGH QR CODE ENCRYPTION AND STEGANOGRAPHY. Advanced Computing : An International Journal (ACIJ). (p 2).

[14] Philippe Allard. 2011. Cahiers de la documentation. CODES QR Un gadget ou un nouvel outil ?. ABD-BVD.(p 31,32).

[15] Kinjal H. Pandya, Hiren J. Galiyawala. 2014. A Survey on QR Codes : in context of Research and Application. International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, ISO 9001 : 2008 Certified Journal). (p 258,259).

[16] A. Sankara Narayanan. 2012. QR Codes and Security Solutions. International Journal of Computer Science and Telecommunications. (p 70,71).

[17] Iris Uitz, Michael harness.2012. “ Der QR-Code – aktuelle Entwicklungen und Anwendungsbereiche”. Springer Science+Business Media. (p 339,340).

[18] Philippe Chaléat, Daniel Charnay. “ HTML et JavaScript”. Eyrolles. Paris. 2002. (p1,2).

[19] RasmusLerdorf. “ Php, Précis et concis ”. O'Reilly. Etats-Unis. 2002. 2eme édition. (p1).

[20] AryehF, Asante M,Danso, A E Y.2016. “Securing Wireless Network UsingpfSense Captive Portal withRADIUSAuthentication”.GhanaJournal of Technology. (p.40-45).

[21] ManujAggarwal.“ Network Security withpfSense : Architect, deploy, and operateenterprise-grade firewalls”. Packt.Inde. 2018. (p 6-10).

[22] Pierre Giraud. « Apprenez à coder en HTML5 et CSS3 ». 2020.(p9).

[23] J. E. Bresenham. 1965. “ Algorithm for computer control of a digital plotter”. IBM SYSTEMS JOURNAL• (p 25).

[24] Roman Kolpakov, Gregory Kucherov. 2003. “ FindingapproximaterepetitionsunderHamming distance ”.heoretical Computer Science. (p 136).

[25] T K Truong, I S Hsu, W L Eastman, I SReed. 1988. “Simplified procedure for correcting both errors and erasures of Reed-Solomon code using Euclidean algorithm”. IEE Proceedings E (Computers and Digital Techniques). (p 318).

[26] Stephen.B. Wicker, “Error control systems for digital communication and storage”. US Ed Edition.États-Unis.1995. Ch 9 : “The Decoding of BCH andReed–Solomon Codes". (p 203).

[27] SamueleDietler. 2006. “Implémentation de codes deReed-Solomon sur FPGA pourcommunications spatiales / Code correcteurd’erreurs”.Projet de diplôme :TélécommunicationsTraitement et transmission de l’information.haute école d’ingénierie et de gestion du canton de vaud. (p 82).

Résumé

Dans ce travail, nous proposons une solution de gestion du réseau WIFI de la gare maritime à l'entreprise portuaire de Béjaïa, une solution sécurisée et adaptée à leurs besoins. Etant donné qu'ils possèdent un pare-feu pour gérer la totalité de leur réseau, l'idée du portail captif semble évidente car elle répond aux critères recherchés pour un bon contrôle du réseau.
Après l'étude de ce dernier et la détection des problèmes rencontrés nous sommes en mesure de proposer une idée qui va répondre à leurs attentes. Nous établissons une authentification QR pour moderniser le réseau et notre choix est encouragé par la popularité et la simplicité du code QR car les QR Codes présentent de nombreux avantages et semblent être un bon moyen pour protéger son réseau des attaques des pirates, dans notre cas il permet de donner l'accès aux personnes autorisées seulement.
Mots clés : réseau, sécurité, code qr, wifi, EPB.

Abstract

In this work, we propose a solution for managing the WIFI network of the ferry terminal to the port company of Béjaïa, a secure solution adapted to their needs. Given that they have a firewall to manage their entire network, the idea of a captive portal seems obvious because it meets the criteria sought for good network control.
After the study of the latter and the detection of the problems encountered, we are able to propose an idea that will meet their expectations. We establish a QR authentication to modernize the network and our choice is encouraged by the popularity and simplicity of the QR Code because QR Codes have many advantages and seem to be a good way to protect one's network from hacker attacks, in our case it allows to give access only to authorized persons.
Key words : network, security, qr code, wifi, EPB.