Université Sidi Mohamed Ben Abdellah
Faculté des Sciences et Techniques Fès
Département Génie Electrique

Mémoire de Projet de fin d'étude

Préparé par

ZOUMHANE Fatimazahra

Pour l'obtention du diplôme

Ingénieur d'Etat en

SYSTEMES ELECTRONIQUES & TELECOMMUNICATIONS

Intitulé

Mise en place d'une solution Wifi sécurisée

Encadré par :

Pr ABARKAN El Hossein

Mr KOITA Moussa (DATAPROTECT)

Soutenu le 30 Juin 2015, devant le jury composé de :

Pr ABARKAN El Hossein ……..: Encadrant

Pr KOITA Moussa ……: Encadrant

Pr ZENKOUAR Khalid……..: Examinateur

Pr MRABTI Fatiha……: Examinateur

ANNEE UNIVERSITAIRE 2014- 2015

Remerciements

Je ne peux entamer ce présent rapport sans exprimer mes sincères remerciements à tous ceux qui ont contribué, de près ou de loin, à l'aboutissement de ce stage.

Je pense particulièrement à Mr. KOITA, mon encadrant, pour la finesse de ses attitudes sur le plan aussi bien humain que professionnel. Ses remarques successives ont permis d'améliorer les différentes versions de ce travail.

Je remercie également Mr. AMEZERIN pour m'avoir donné l'opportunité de passer ce stage chez Dataprotect.

J'adresse aussi mes remerciements à mon parrain industriel Mr. ABARKAN qui m'a prodigué de précieuses recommandations d'une grande utilité.

Mes sincères remerciements s'adressent à Mr. ZENKOUAR pour ses judicieuses directives et l'aide qu'il m'a octroyée.

Ma gratitude va aussi à l'endroit des membres du jury d'avoir examiné et noté mon travail.

Je tiens également à adresser mes sincères remerciements à l'ensemble du corps enseignant de la FST FES.

Enfin, qu'il me soit permis de remercier tout le personnel de DATAPROTECT, pour son soutien et pour sa générosité considérable quant à l'ore de l'information.

Résumé

Plusieurs entreprises s'intéressent de plus en plus à la mise en place d'un réseau sans fil, en vue des avantages que le Wifi permet à ses utilisateurs (facilité de déploiement, mobilité, connexion des périphériques portables aux ressources de l'entreprise…) tout en maintenant leur besoin de sécurité et de disponibilité de leurs données qui circulant sur ces réseaux.

Fournir les bonnes pratiques nécessaires à la mise en place d'infrastructure sans fils répondant aux normes de sécurité et de disponibilité à travers l'élaboration d'un document est le contexte dans lequel s'inscrit cette étude qui a été menée au sein de la société DATAPROTECT.

Dans ce document, nous avons présenté l'étude du projet qui consiste à rassembler des consignes et des équipements nécessaires pour mettre en place l'architecture finale sécurisée, et qui répond aux besoins de ses utilisateurs en termes de sécurité, fiabilité et force.

Pour atteindre le but final du projet, on a fait tout d'abord l'étude des normes : ANSSI, PCI-DSS, 27002, NIST, qui donnent les recommandations sur le déploiement du réseau sans fil, ensuite on a pris cinq technologies : RUCKUS, CISCO, ARUBA, FORTINET, AEROHIVE et on a fait la comparaison de leurs avantages et inconvénients afin de choisir la technologie qui répond aux besoins exprimés, après on a fait l'étude des failles des architectures existantes, et on a pris dans ce document le cas d'une moyenne entreprise et d'un hôtel ; et finalement, et après l'étude du besoin on a mis en place l'architecture Wifi sécurisée adoptée.

Mots clés : Sécurité – Wifi – Réseau sans fil – Architecture – LAN – Déploiement – Standard – Norme- WEP- Radius- WPA-Authentification.

TABLE DES MATIERES

Liste des tableaux

Liste des figures

INTRODUCTION GÉNÉRALE

Malgré les problèmes de sécurité intrinsèques, les réseaux sans fil continuent à se développer vu les avantages qu'ils permettent (coût faible, installation aisée, débit élevé…). Il est donc important de bien connaître les problèmes liés à la mise en place de ce type de réseaux afin d'en limiter les effets néfastes sur la sécurité des données. Il est également important de déterminer le niveau de sécurité souhaité, afin de mettre en place une solution adéquate, et de configurer les différents alternatifs de sécurité que le réseau sans fil dispose pour améliorer la confidentialité des communications.

Dans ce cadre **DATAPROTECT** souhaite élaborer un document qui comprend les consignes et les recommandations à suivre par ses clients, qui veulent déployer un réseau Wifi sécurisé dans leurs entreprises. Durant ce projet, on va faire une étude des normes qui supportent le Wifi, ainsi que les paramétrages et les règles de sécurité à utiliser pour protéger le réseau. Le but de cette étude est de proposer une architecture sécurisée et fiable destinée aux clients de Dataprotect pour assurer la sécurité de leurs données.

Ce rapport comprend les détails de cette étude qui est constituée de quatre chapitres présentés comme suit:

Le premier chapitre présente l'organisme d'accueil, puis présente le contexte du projet et le cahier des charges expliquant plus en détail le projet ainsi que la planification poursuivie et les tâches confiées au cours du stage; ensuite, le deuxième chapitre comprend les généralités sur la sécurité du réseau sans fil, et l'étude du projet qui expose les normes utilisées pour mettre en place l'architecture finale sécurisée et les technologies existantes sur le marché ; enfin, le dernier chapitre présente l'étape d'étude du besoin du client et la solution finale adoptée, ainsi qu'une démonstration de fonctionnement du projet qui garantit la pertinence de l'architecture proposée.

Chapitre 1 : Contexte général du projet

Ce chapitre présente une vue générale sur l'organisme d'accueil, puis une vision globale des sujets qui seront axes d'étude et de réalisation de notre cahier des charges

I. Présentation de l'entreprise d'accueil

1. Présentation de l'entreprise

DATAPROTECT est une entreprise spécialisée en sécurité des systèmes d'informations, fondée en 2009 par des experts en sécurité ayant mené plusieurs projets de conseils et d'intégration de solutions de sécurisation au Maroc et à l'étranger.

Appuyant son offre sur une vision unifiée de la sécurité, DATAPROTECT est dotée d'un réservoir de compétences pointues certifiées en sécurité lui permettant d'assurer une expertise unique sur le marché marocain.

DATAPROTECT est organisée autour de 5 pôles d'activités :

- **Le conseil** : Activité de conseil et d'assistance à maîtrise d'ouvrage dans la mise en œuvre de solutions de sécurité.
- **L'intégration:** Activité de maîtrise d'œuvre complète et d'ingénierie de solutions de sécurité.
- **L'infogérance :** Activité de supervision et d'administration des équipements de sécurité.
- **La recherche et le développement :** Activité de veille, de recherche et de développement de nouvelles solutions de sécurité.
- **La formation** : Activité de transfert de compétences sur des thèmes pointus de la sécurité.

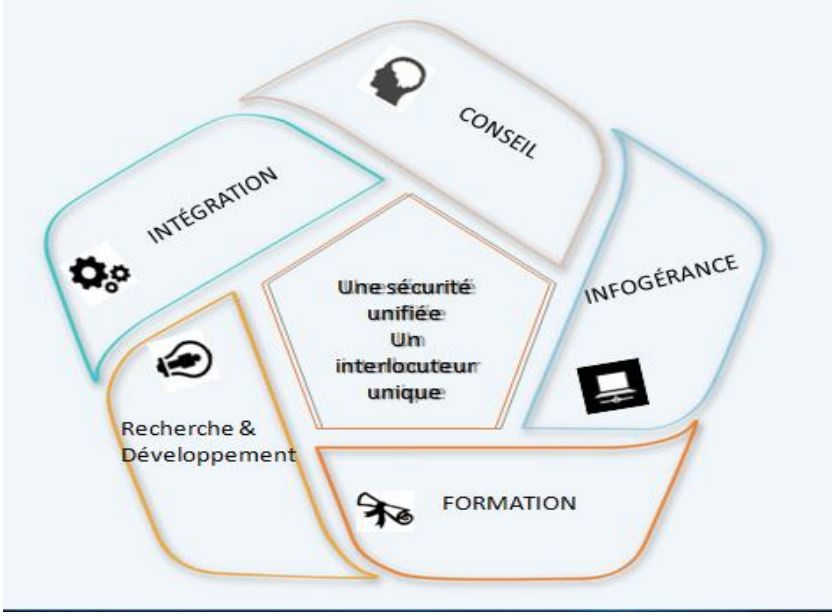

Figure 1.1 : Principaux pôles d'activités de l'entreprise

2. La mission de l'entreprise

DATAPROTECT a pour mission de faire bénéficier ses clients du retour d'expérience à forte valeur ajoutée de ses équipes.

Pour y parvenir, DATAPROTECT s'est lancée, depuis sa création, dans la constitution des équipes composées des ressources certifiées ayant conduit de nombreux projets liés à la sécurité de l'information aussi bien au Maroc qu'à l'étranger.

En combinant son expertise pointue au niveau technologique et sa compréhension complète et singulière de la chaîne des menaces informationnelles, DATAPROTECT se donne comme mission de ne fournir que des prestations spécialisées et concentrées uniquement autour de la sécurité de l'information.

3. Les activités et projets de DATAPROTECT

Le conseil :

Ayant mené une centaine de missions d'audit de sécurité et de certification des systèmes d'informations pour le compte d'organisations exerçants dans divers domaines d'activités, DATAPROTECT dispose d'un retour d'expérience très riche et varié en la matière.

Unique prestataire Marocain autorisé par le consortium PCI SSC à mener des missions de certification PCI DSS, et doté de compétences certifiées en audit de sécurité (CISA, CEH, OSCP, CISSP, Lead Implementer & Lead Auditor ISO 27001, Risk Manager ISO 27005, PA QSA, PCI QSA, etc…), l'activité conseil de DATAPROTECT couvre les prestations ci-après

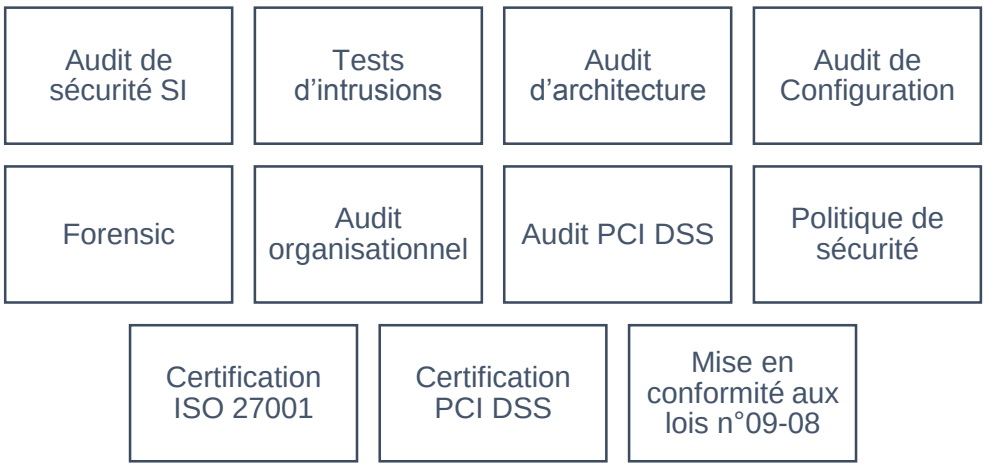

Figure 1.2 : Les prestations couvertes par le pole conseil

L'intégration :

De la sécurité périmétrique jusqu'à la corrélation des logs de sécurité en passant par la sécurité des postes de travail et des accès distant, divers outils existent sur le marché pour assurer diverses fonctions de sécurité. Fort de son retour d'expérience dans la mise en place de solutions de sécurité, DATAPROTECT dispose des ressources qualifiées en intégration de solutions de sécurité des systèmes d'informations, certifiées sur les différentes technologies et solutions: (KASPERSKY, SAFENET, CYBEROAM, BEEWARE, TRIPXIRE, RUCKUS, WEBSENSE, QUALYS, PGP, McAfee, SPLUNK, GALLEON, SYMANTECT, …).

L'activité d'intégration de DATAPROTECT couvre les prestations suivantes :

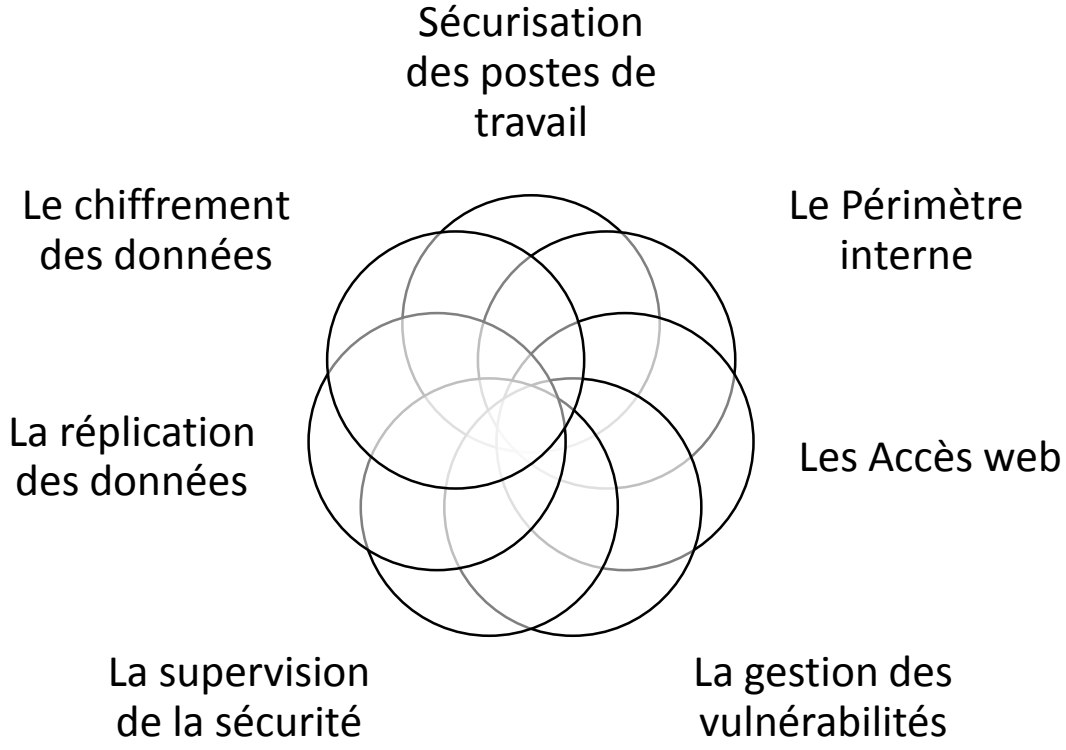

Figure 1.3 : Les prestations couvertes par le pole intégration

L'infogérance

- Infogérance des solutions de sécurité (Firewall, UTM, IPS/IDS, Gestion des logs, etc.)
- Offre Mars : Maintenance, Administration, Reporting, Supervision.
- Security Operations Center (SOC).
- Management des vulnérabilités.

Recherche et Développement

- Développement de solutions sécurisées.
- Recherches et veille de vulnérabilités.
- Développement sécurisé des applications souveraines.
- Recette de sécurité des applications critiques.

La formation :

Destinées aux dirigeants d'entreprises et aux collaborateurs souhaitant appréhender les nouvelles approches en matière de sécurité, les formations proposées par DATAPROTECT sont particulièrement adaptées aux besoins du marché.

Leader dans son domaine d'activité, DATAPROTECT dispose de salles parfaitement équipées et d'une équipe de formateurs hautement qualifiés dont la plupart ont acquis une expérience à l'international et sont dotés de certificats reconnus à l'échelle internationale dans le domaine de la sécurité. L'approche de DATAPROTECT est la suivante :

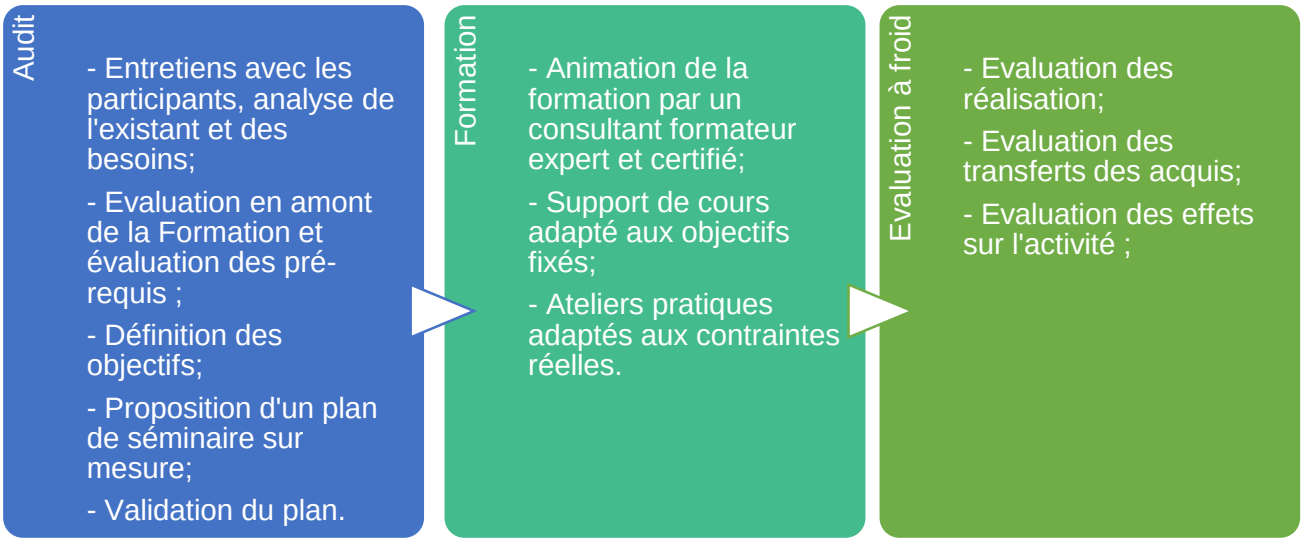

Figure 1.4 : L'approche de DATAPROTECT

4. Organigramme

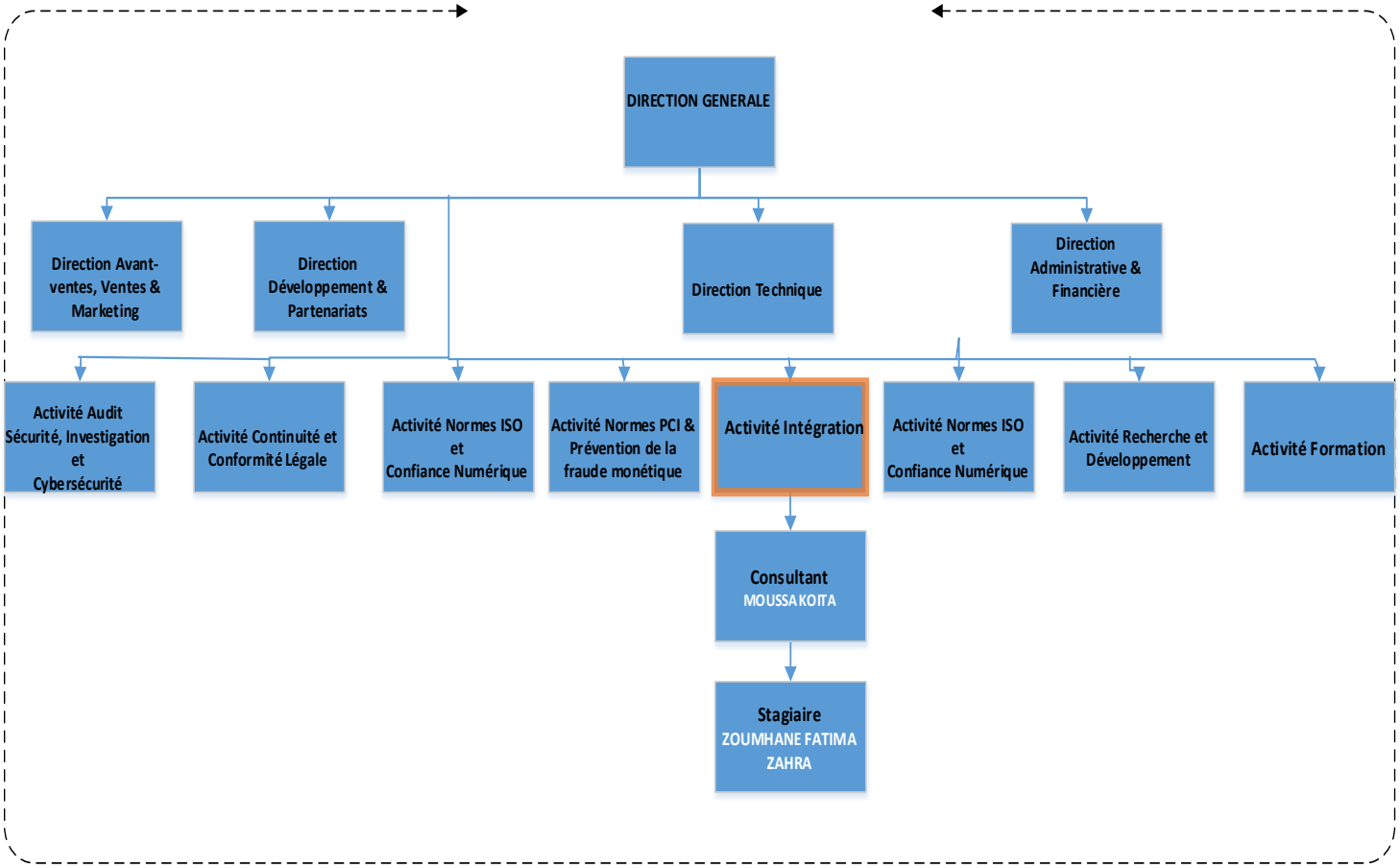

Figure 1.5 : Organigramme de DATAPROTECT

5. Présentation de l'environnement de travail

Le présent projet s'est déroulé au sein de l'équipe intégration dont fait partie l'encadrant de stage, Mr **KOITA MOUSSA.** Leur travail consiste à auditer l'architecture SI existante du client, analyser ses besoins fonctionnels et techniques afin de mettre en place des solutions de sécurisation des systèmes d'information suivant les meilleures pratiques.

Leur offre d'intégration de solutions se matérialise par :

- ✓ La mise en place de l'antivirus.
- ✓ La mise en place de solution de gestion de vulnérabilités.
- ✓ La mise en place de solution de gestion des correctifs.
- ✓ La mise en place de solution de prévention de fuite d'informations sensibles.
- ✓ La mise en place d'outils de cryptage de données.
- ✓ La mise en place de solution d'authentification forte.

II. Analyse du contexte

1. Le rôle de la technologie dans le développement

Nous assistons à une révolution des méthodes de travail. Celles-ci sont de plus en plus introduites dans nos vies. Aujourd'hui, en tant que particulier ou professionnel, nous sommes tous sujets à l'utilisation des nouvelles technologies. Elles se sont forgés une place indispensable dans nos vies et dans le fonctionnement des l'entreprises notamment.

La mise en place de ces technologies et leur utilisation personnalisée ont encore accéléré la mondialisation des échanges, dès lors que les frontières terrestres sont devenues virtuelles et les distances ont été totalement réduites, voire supprimer par la simple action d'un clic de souris. Le monde professionnel a donc dû s'adapter afin de se préparer à évoluer avec ces nouveaux outils et se les approprier le plus rapidement possible.

Les nouvelles technologies ont permis à bon nombre d'entreprises de s'affirmer par des gains de compétitivité, au sein du marché de plus en plus exigeant. L'investissement dans les nouvelles technologies apparaît clairement comme l'un des principaux moteurs de compétitivité au sein des entreprises, quelle que soit leur taille. Les entreprises qui ont su surfer sur la vague sont celles qui ont su garder la tête hors de l'eau pendant les années de récession économique**. [7]**

2. Analyse de la situation

Atouts et opportunités de la situation	✓ Grande quantité d'informations de tout genre ouvertes à tout le monde. ✓ La technologie dans l'éducation permet de dépasser les limites, d'aller vers des situations d'apprentissages réelles et signifiantes pour les élèves. ✓ Facilite plusieurs tâches et permet de gagner le temps.
Faiblesses et points de vigilance de la situation	✓ Risque lié à la sécurité de nos informations que la technologie gère. ✓ Mal utilisation de ces technologies peut emmener à des situations non voulues (guerre par exemple).

Tableau 1. 1 : Atouts et faiblesses de la situation

3. Les risques envisagés :

Le risque sur le système d'information s'est accru avec le développement du travail à distance et des nouvelles technologies : vols, destruction de données ou de matériel, indisponibilité du système, etc. avec une origine qui peut être externe, mais souvent interne (malveillance ou négligence).

L'entreprise est soumise donc à la nécessité de veiller à l'intégrité, la confidentialité, la disponibilité, et la traçabilité de ses informations et de mettre en place les moyens adaptés tant d'un point de vue technique qu'organisationnel.

III. Problématique

Nous remarquons ces dernières années la montée en puissance des réseaux locaux sans fil ou encore Wifi, qui sont devenus l'une des principales solutions de connexion pour de nombreuses entreprises à cause du fort développement de l'effectif nomade. En effet, les employés sont équipés d'ordinateurs portables et passent plus de temps à travailler au sein d'équipes géographiquement dispersées et plurifonctionnelles. Le marché du sans fil se développe alors rapidement à cause de la bonne productivité que les entreprises constatent.

1. Analyse de l'existant

Le Wifi est un outil très pratique qui permet à un utilisateur de se connecter à Internet depuis n'importe qu'elle pièce de son local s'il est équipé du matériel adéquat. Cette technologie facilite grandement la création de réseaux locaux entre plusieurs ordinateurs reliés sans fil à un seul et même modem-routeur. De plus il est facile à installer et souple à utiliser et il ne nécessite pas un gros investissement, il est donc la solution idéale pour partager une connexion ADSL avec tous les ordinateurs du domicile ou du bureau des utilisateurs.

Concrètement, le Wifi trouve son utilité dans la liberté qu'il offre aux internautes. Les câbles gênants et disgracieux ne sont plus nécessaires pour profiter des joies du haut débit. En pratique, le Wifi répond aux besoins des mobilités des internautes : il permet de relier des ordinateurs portables, des PC de bureau, des Smartphones et des tablettes ainsi que des périphériques mobiles à une liaison haut débit ou à des appareils électroniques communiquant dans un rayon de plusieurs dizaines de mètres en intérieur à plusieurs centaines de mètres à l'extérieur.

Avec cette évolution rapide de ce type dématérialisé de réseaux, les exigences en termes de sécurité deviennent de plus en plus sévères.

2. Dysfonctionnement

Ce qu'il faut savoir c'est qu'une connexion Wifi non sécurisée peut s'avérer très dangereuse non seulement pour votre ordinateur, mais aussi pour vos données personnelles.

Si quelqu'un se connecte via votre connexion Wifi non sécurisée et si la personne de l'autre côté est mal intentionnée, elle peut introduire un virus dans les fichiers publics en y notant un nom de dossier attrayant et votre ordinateur se retrouve infecté, vous serez dans ce cas accusé à sa place s'il effectue des actions illégales : pirater des sites web, télécharger des œuvres protégées…etc., ce qui pourrait vous engendrer de nombreux problèmes, car cela viendra de votre connexion et donc de votre ordinateur, bien que ce ne serait pas vous.

Les hackers sont aussi capables de récupérer les données qui transitent via le réseau Wifi piraté. Toutes les données peuvent être interceptées. N'importe quel pirate, même débutant, avec un logiciel de sniff réseau, peut capturer et lire les données échangées comme les emails reçus ou envoyés, les pages visitées, les conversations Skype, les identifiants et mots de passe utilisés sur les pages qui ne sont pas sécurisées en HTTPS/SSL.

Par exemple un internaute en train d'effectuer des achats en ligne par l'intermédiaire de sa tablette, court ainsi le risque de voir ses coordonnées bancaires interceptées par les pirates. Une simple connexion à sa boîte email de type Gmail permet au pirate de récupérer l'identifiant et le mot de passe. À partir de là, l'hacker a accès à des dizaines d'autres accès, pour récupérer les mots, les accès, etc.

Tout comme il y a plusieurs façons d'infiltrer un réseau sans fil, il existe également plusieurs moyens de sécuriser un réseau et de faire face aux menaces. De ce fait, beaucoup de travaux et d'efforts ont été consentis ces dernières années afin d'aboutir à des solutions pour sécuriser ces réseaux.

IV. Cahier des charges

Le principal problème des réseaux Wifi est leur fragilité vis-à-vis des attaques externes, et malgré les travaux qui ont été faits pour sécuriser les réseaux, des vulnérabilités persistent encore et il est toujours possible de monter des attaques plus ou moins facilement.

Le but de ce projet est la mise en place d'une architecture Wifi sécurisée.

L'objectif de ce document est de proposer aux clients de DATAPROTECT qui veulent déployer un réseau sans fil dans leur entreprise (hôtel, entreprise, hôpital…) des normes et des recommandations à suivre afin de sécuriser leurs données.

Il faut étudier les différentes failles du réseau sans fil, les différentes solutions existantes, rassembler les bonnes configurations à faire afin de sécuriser le réseau. Il faut aussi faire une étude comparative des équipements qui existent et qui vont nous permettre de respecter les normes de sécurité et le débit souhaité pour finalement proposer un exemple d'architecture Wifi sécurisée qui indique les consignes à suivre par les utilisateurs du réseau sans fil.

V. Macro planning du projet

Pour comprendre le concept de la sécurité des systèmes d'information, il fallait collecter les informations sur le thème de réseau informatique, ce qui va servir par la suite pour réussir l'action qui a été demandée.

Ensuite il était nécessaire de commencer l'étude du projet en essayant de saisir la problématique, diviser le travail en plusieurs tâches élémentaires avec l'estimation de la durée que va prendre chaque tâche.

Le temps pour avoir le résultat désiré était très court donc il fallait une bonne gestion du temps et l'utilisation des bonnes méthodes, c'est pour cela que le recours au diagramme de gant comme illustré ci-dessous.

Au cours du projet, il y avait des réunions journalières ou le standup Meeting avec l'encadrant chaque matin qui consiste à préciser l'état d'avancement du projet, son principal objectif est de connaitre les tâches effectuées et de détecter les problèmes émergents et les

objectifs pour la journée ; et afin d'éviter l'écartement entre ce que le client attend et le but final, il y avait toujours l'implication du client dans ces réunions.

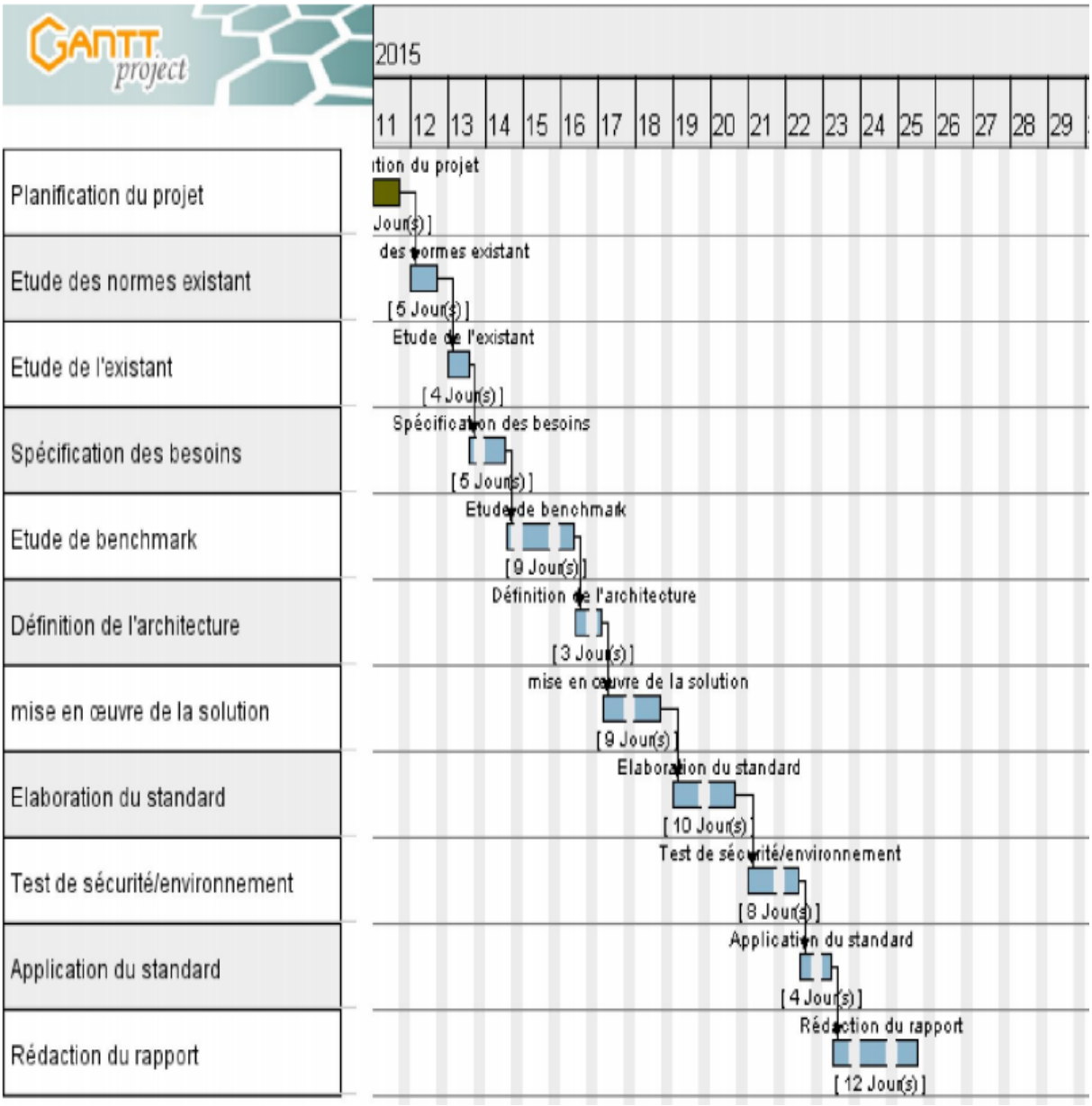

Figure 1.6 : Planning du projet

VI. Tâches et responsabilités confiées au cours du stage

Durant le stage, je suis intervenu sur plusieurs taches ayant pour but de m'aider à développer mes connaissances générales sur les réseaux informatiques, mais aussi à faire mon premier pas dans les activités professionnelles en menant à bout les responsabilités confiées.

Tache	Description
Mise en place de solutions de virtualisation «VMWARE»	Il s'agissait de prendre contact avec le concept de la virtualisation, de comprendre le principe de fonctionnement d'un hyperviseur, de mettre en place des machines virtuelles tant sur l'ESXI, que sur la version Cliente (VMWare Workstation)
Hacking de réseau sans fil	Ayant pour but principal de comprendre le concept de la sécurité sans fils, cette tâche consistant à la découverte de la distribution (KALI LINUX) utilisée par les professionnels de la sécurité, tout comme les Hackers malveillants pour casser la sécurité des réseaux sans fil.
Mise en place Windows server 2012 R2	Découvrir l'environnement le plus utilisé sur le marché en termes d'annuaire LDAP, était une des taches importantes que j'ai menées également. Le but étant de découvrir comment sont organisés les systèmes d'informations au sein des entreprises, la gestion des actifs, utilisateurs et authentifications. Le but de ce travail est de comprendre l'attribution des droits d'accès aux utilisateurs du réseau selon un annuaire déjà établi.
Design d'architecture avec Microsoft Visio 2013	Solution de design utilisée par les ingénieurs afin de schématiser des architectures complexes, la découverte de cette application que j'ai par la suite utilisée tout au long de mon stage m'a permis de comprendre plus en détail l'organisation des architectures réseau.

Tableau 1. 2 : Tâches confiées au cours du stage

VII. Connaissances à acquérir pour traiter le sujet du mémoire :

Le projet demande une bonne connaissance technique, organisationnelle et managériale pour traiter les phases du projet qu'on va traiter dans le chapitre trois, et atteindre l'objectif final.

a) Sur le plan technique

- Faire des recherches sur le sujet choisi pour constituer une sorte de revue de presse.
- Apprendre les différents concepts de sécurité d'un réseau.

- Se documenter pour savoir quelles sont les solutions qui ont été menées, par quelles structures, pour quels publics, et tirer les failles.
- connaitre les outils nécessaires pour sécuriser une infrastructure Wifi.

b) Sur le plan organisationnel

- Formuler des objectifs en décrivant la démarche à suivre ce qui va permettre de concrétiser une idée pour atteindre le résultat visé.
- Découper le déroulement du projet en plusieurs phases successives.
- Organiser et prévoir le temps de travail.
- Découper en plusieurs tâches.
- Utiliser les méthodes de gestion du projet : méthode agile qui consiste à impliquer au maximum le demandeur (client), ces méthodes permettent une grande réactivité aux demandes, visent la satisfaction réelle du besoin du client.
- Se méfier de l'effet tunnel en utilisant des jalons qui vont permettre de scinder le projet en phases clairement identifiées.

Le jalon matérialise la clôture officielle d'une phase, et le démarrage de la phase suivante. Il peut être la production d'un document, la tenue d'une réunion ou bien encore un livrable du projet.

c) Sur le plan managérial

- Réfléchir aux ressources matérielles et humaines qui pourront aider durant tout le processus d'élaboration et de réalisation du travail.
- Savoir travailler en équipe.
- Savoir gérer le temps.

Chapitre 2 : Étude des méthodes et technologies

Ce chapitre présente les principales bases à maîtriser pour choisir la solution convenable. Il présente aussi les normes supportant le Wifi et les technologies existantes

I. Généralité

1. Type d'architecture du réseau WIFI

Le mode ad hoc : tous les clients (terminaux ou postes) des réseaux Wifi communiquent entre eux sans passer par un équipement central [Figure 3.1].

Le mode Infrastructure : dans ce mode un équipement central appelé access point est indispensable pour gérer la communication entre les différents clients Wifi.

Les protocoles de sécurité fonctionnent seulement dans le mode infrastructure.

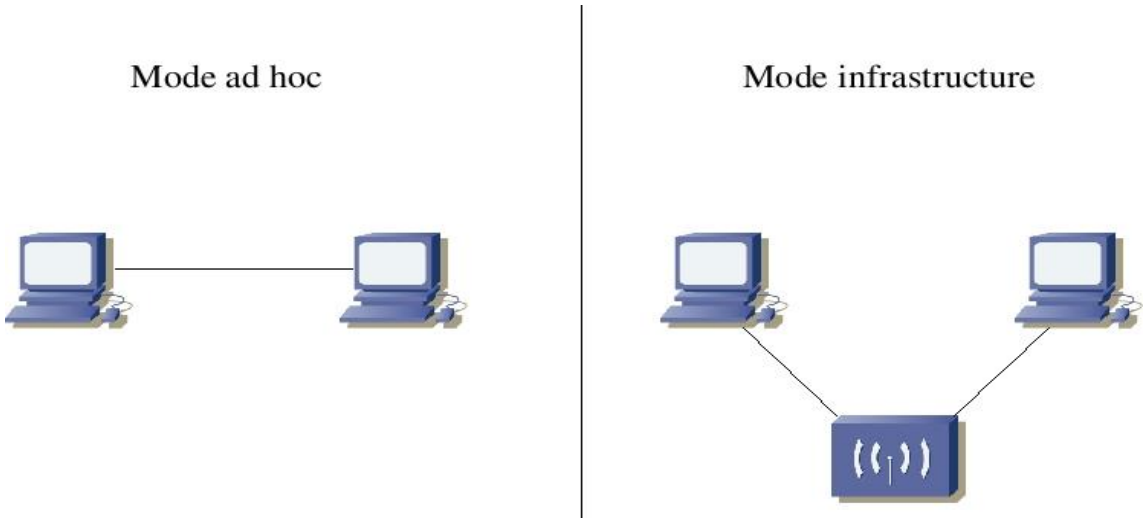

Figure 2. 1 : Types d'architecture Wifi

2. Les normes WIFI

La norme 802.11 fait référence à une famille de spécifications développées par l'IEEE pour la technologie des réseaux locaux sans fil (RLR). La norme 802.11 stipule une interface radioélectrique entre un client sans fil et une station de base ou entre deux clients sans fil, utilisant un système à saut de fréquence et à étalement du spectre (FHSS, pour Frequency Hopping Spread Spectrum) ou à étalement du spectre en séquence directe (DSSS, pour Direct Sequence Spread Spectrum).

802.11a : La norme 802.11a (baptisé Wifi 5) permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels) et une fréquence de fonctionnement de 5 GHz. La norme 802.11a spécifie 52 canaux de sous-porteuses radio dans la bande de fréquence des

5 GHz. Il utilise une méthode de transmission de multiplexage par répartition orthogonale de la fréquence (OFDM, pour Orthogonal Frequency Division Multiplexing).

802.11 b : La norme 802.11 b propose un débit théorique de 11 Mbps (6 Mbps rééls) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquence utilisée est la bande des 2.4 GHz, il utilise DSSS (Direct Sequence Spread Spectrum).

802.11 g : La norme 802.11g offre un haut débit (54 Mbps théoriques, 30 Mbps réels) sur la bande de fréquence des 2.4 GHz. La norme 802.11g a une compatibilité ascendante avec la norme 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b.

802.11n : Un groupe de travail du Comité IEEE 802.11 a défini un nouveau projet de spécification en prévision de l'augmentation du débit jusqu'à des vitesses de 540 Mbps. Pour améliorer les performances, la spécification utilise la technologie Multiple-Input-Multiple-Output (MIMO), ou l'utilisation de plusieurs récepteurs et de plusieurs émetteurs sur le client et le point d'accès.

802.11i : La norme IEEE 802.11i a été ratifiée en juin 2004 et met l'accent sur la sécurité en proposant des mécanismes de contrôle d'intégrité, d'authentification et de chiffrement.

802.11e : La norme 802.11e vise à donner des possibilités en matière de qualité de service au niveau de la couche « liaison de données ». Ainsi, cette norme a pour but de définir les besoins des différents paquets en termes de bande passante et de délai de transmission de manière à permettre, notamment, une meilleure transmission de la voix et de la vidéo.

802.11ac : est la dernière évolution du standard de transmission sans fil 802.11, qui permet une connexion sans fil haut débit dans la bande de fréquences 5 GHz. Le 802.11ac offre jusqu'à 1 300 Mbit/s de débit théorique, en utilisant des canaux de 80 MHz, soit jusqu'à 7 Gbit/s de débit global dans la bande des 5 GHz [8].

Nous avons préféré de travailler pendant ce projet avec 802.11ac vu le débit qui nous permet. Donc le matériel que nous allons choisir par la suite doit répondre à cette norme.

802.1x : Un standard lié à la sécurité des réseaux informatiques, permettant d'authentifier un utilisateur souhaitant accéder à un réseau (filaire ou non) grâce à un serveur d'authentification.

L'authentification IEEE 802.1x est basée sur des protocoles EAP comme EAP-TLS/TTLS ou PEAP.

EAP (Extensible Authentication Protocol) est juste le protocole de transport des informations d'identification des utilisateurs.

3. Les protocoles de sécurité

WEP : Il utilise le protocole de chiffrement RC4 et une clé de chiffrement symétrique et statique. Chaque intervenant dispose d'une même clé WEP. Le point d'accès envoie un message en clair au client qui répond avec un message crypté avec la clé WEP, donc l'identification se fondra seulement sur les périphériques et non sur les utilisateurs.

Le WEP est considéré comme cryptographiquement cassé : l'utiliser pour connexion Wifi est donc déconseillé car il n'offre pas une protection suffisante.

WPA : Il a été proposé par la Wifi Alliance en 2003. Il améliore la sécurité offerte par l'ancien protocole WEP vu qu'il était désormais cassé et il fallait donc un nouveau protocole de sécurité. C'est pourquoi des faiblesses ont été remarquées dès son introduction. Mais la première attaque efficace publiée contre WPA1 date de 2008.

WPA utilise en général le protocole de chiffrement TKIP. Le protocole TKIP permet la génération aléatoire de clés et offre la possibilité de modifier la clé de chiffrement plusieurs fois par seconde, pour plus de sécurité.

WPA2 : C'est le successeur de WPA, il remplace le chiffrement TKIP par AES pour plus de sécurité. L'utilisation de WPA2 ne garantit pas à elle seule un bon niveau de sécurité, l'utilisateur doit choisir soigneusement son mot de passe.

Pour rappel, TKIP et AES peuvent être utilisés par WPA, mais WPA2 n'utilise qu'AES.

WPA et WPA2 permettent deux types d'authentification :

- **Entreprise :**

La méthode d'authentification entreprise est utilisée dans des environnements professionnels parce qu'il demande des configurations relativement complexes et du matériel coûteux.

Dans cette authentification, les clients doivent s'authentifier auprès d'un serveur appelé radius pour recevoir leurs codes d'accès au réseau. L'authentification ne se fait pas par le point d'accès, ce dernier relaie les messages d'authentification entre le client et le RADIUS.

- **Personnel (Personal)** :

C'est une solution plus légère, plus facile à mettre en place, prévue pour les particuliers et les petites entreprises. Le point d'accès et le client partagent une clé similaire appelée clé partagée (shared key) ou mot de passe (passphrase). C'est un mode dans lequel les clients utilisent tous une « passphrase » commune.

WPS : Le Wifi Protected Setup (WPS) est un standard de la Wifi Alliance créé en 2007, qui a pour but d'établir une connexion Wifi de manière simplifiée. Ce n'est pas un système de chiffrement et d'authentification, mais il est destiné à être un complémentaire.

Mais la sécurité n'est pas garantie ; ce mode est activité par défaut dans la plupart des équipements récents, et le PIN qu'il donne peut être facilement contournable, vu qu'avec cette méthode, on évite à ce que l'utilisateur détermine une méthode de sécurisation et choisit un mot de passe complexe, donc il doit être désactivé sur les points d'accès. [1]

Filtrage MAC : Consiste à donner au point d'accès les adresses MAC ayant le droit de s'associer. Cette liste peut être répétée sur tous les points d'accès pour assurer la mobilité.

4. Méthode d'authentification basée sur des certificats

Dans le cadre de l'authentification en environnement sans fil basée sur le protocole 802.1X, différentes variantes d'EAP sont disponibles aujourd'hui dont les plus connues sont:

- Protocole EAP-MD5 (EAP - Message Digest 5) : authentification du client par login/mot de passe.
- Protocole EAP-TLS (EAP - Transport Layer Security) : crée par Microsoft. Méthodes d'authentification mutuelles entre le serveur et le client par certificat.
- Protocole EAP-TTLS (EAP - Tunneled Transport Layer Security) : développé par Funk Software et Certicom, utilise des certificats uniquement sur le serveur d'identification.

- Protocole PEAP (Protected EAP) : développé par Microsoft, Cisco et RSA Security, le client est authentifié par un login/mot de passe tandis que le serveur est authentifié par son certificat. [2]

	EAP-MD5	EAP-TLS	EAP-TTLS	PEAP
Authentification du serveur	Aucune	Clé publique (certificat)	Clé publique (certificat)	Clé publique (certificat)
Authentification du client	Password hash	Clé publique (certificat à carte puce)	CHAP,PAP, MS-CHAP(v2), EAP	EAP (EAP MS-CHAP v2 ou clé publique)
Distribution dynamique des clés	Non	Oui	Oui	Oui
Risque sécurité	Vol de session, attaque par dictionnaire, Obtention du login client et Attaque MiM	Obtention de l'identité client	Attaque MiM	Attaque MiM

Tableau 2.1 : Méthode d'authentification basée sur des certificats

5. Le protocole RADIUS

L'authentification est l'opération par laquelle le destinataire et/ou l'émetteur d'un message s'assure de l'identité de son interlocuteur. L'authentification est une phase cruciale pour la sécurisation de la communication. Les utilisateurs doivent pouvoir prouver leur identité à leurs partenaires de communication et doivent également pouvoir vérifier l'identité des autres utilisateurs.

Le fonctionnement de RADIUS est basé sur un système client/serveur chargé de définir les accès d'utilisateurs distants à un réseau. Le protocole RADIUS repose principalement sur

un serveur (le serveur RADIUS), relié à une base d'identification (base de données, Active Directory, annuaire LDAP, etc.) et un client RADIUS, appelé NAS (*Network Access Server*), faisant office d'intermédiaire entre l'utilisateur final et le serveur. L'ensemble des transactions entre le client RADIUS et le serveur RADIUS sont chiffrées et authentifiées grâce à un secret partagé.

Le scénario du principe de fonctionnement est le suivant :

- Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance ;
- Le NAS achemine la demande au serveur RADIUS ;
- Le serveur RADIUS consulte la base de données d'identification afin de connaître le type de scénario d'identification demandé pour l'utilisateur. Soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur. Le serveur RADIUS retourne ainsi une des quatre réponses suivantes :

  - **ACCEPT** : l'identification a réussi ;
  - **REJECT** : l'identification a échoué ;
  - **CHALLENGE** : le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un « défi » (en anglais « *challenge* ») ;
  - **CHANGE PASSWORD** : le serveur RADIUS demande à l'utilisateur un nouveau mot de passe.

Suite à cette phase dite d'authentification, débute une phase d'autorisation où le serveur retourne les autorisations de l'utilisateur. [9]

II. Méthodes habituellement utilisées pour Une Situation présentant des similitudes

1. Les méthodes existantes :

Il était nécessaire d'élaborer des normes qui vont garantir la protection des données personnelles et la mise en place d'un environnement numérique digne de confiance. La sécurité du réseau sans fil fait l'objet de plusieurs normes, par exemple : ANSSI, ISO/CEI 27002**,** NORME PCI-DSS**,** Norme NIST.

a) Norme ANSSI :

En France, l'ANSSI (Agence nationale de la sécurité des systèmes d'information) est un service du Secrétariat général de la défense et de la sécurité nationale (SGDSN). Elle assiste le premier ministre sur tous les sujets relatifs à la cyberdéfense, et développe de nombreuses actions (prévention, réglementation, assistance, conseil, formation, etc.) pour prévenir ou résoudre les risques de sécurité informatique et réseau. Avec 250 effectifs en 2012, la structure de l'ANSSI peut sembler limitée par rapport à ses voisins allemands et britanniques (500 et 700 agents), mais elle ne cesse de prendre de l'ampleur [10].

Dans le guide qu'ANSSI a publié le 3 avril 2013 un guide 23 recommandations qui vont guider l'utilisateur du Wifi pour un choix des meilleurs paramètres pour la bonne sécurisation d'un réseau Wifi

Recommandation 1 :	N'activer l'interface Wifi que lorsqu'elle celle-ci doit être utilisée
Recommandation 2 :	Afin de garder le contrôle sur la connectivité du terminal, désactiver systématiquement l'association automatique aux points d'accès Wifi configurés dans le terminal.
Recommandation 3 :	Maintenir le système d'exploitation et les pilotes Wifi du terminal en permanence à jour des correctifs de sécurité.
Recommandation 4 :	Éviter tant que possible de se connecter à des réseaux sans fil inconnus ou qui ne sont pas de confiance.
Recommandation 5 :	Bloquer, par configuration du pare-feu local, les connexions entrantes via l'interface Wifi
Recommandation 6	Respecter la politique de sécurité de l'entité, en particulier s'agissant des moyens cryptographiques d'authentification ainsi que de protection en confidentialité et en intégrité qui doivent être mis en œuvre.
Recommandation 7 :	Ne pas brancher de bornes Wifi personnelles sur le réseau de l'entité.
Recommandation 8 :	En situation de mobilité, lors de toute connexion à des points d'accès Wifi qui ne sont pas de confiance (par exemple à l'hôtel, la gare ou l'aéroport), préalablement à tout échange de données, utiliser systématiquement des moyens de sécurité complémentaires (VPN IPsec par exemple).
Recommandation 9 :	Plus largement, lorsque des données sensibles doivent être véhiculées via un réseau Wifi, l'utilisation d'un protocole de sécurité spécifique, tel que TLS ou IPsec, doit être mis en œuvre.

Recommandation 10 :	Configurer le point d'accès pour utiliser un chiffrement robuste. Le mode WPA2 avec l'algorithme de chiffrement AES-CCMP est fortement recommandé. Pour les points d'accès personnels, utiliser le mode d'authentification WPA-PSK (WPA-Personnel) avec un mot de passe long (une vingtaine de caractères par exemple) et complexe, d'autant plus que ce dernier est enregistré et n'a pas besoin d'être mémorisé par l'utilisateur.
Recommandation 11 :	Lorsque l'accès au réseau Wifi n'est protégé que par un mot de passe (WPA-PSK), il est primordial de changer régulièrement ce dernier, mais également de contrôler sa diffusion. En particulier, il convient de : – ne pas communiquer le mot de passe à des tiers non autorisés (prestataires de services par exemple) ; – ne pas écrire le mot de passe sur un support qui pourrait être vu par un tiers non autorisé ; – changer le mot de passe régulièrement et lorsqu'il a été compromis.
Recommandation 12 :	Pour les réseaux Wifi en environnement professionnel, mettre en œuvre WPA2 avec une infrastructure d'authentification centralisée en s'appuyant sur WPA-Entreprise (standard 802.1x et protocole EAP), ainsi que des méthodes d'authentification robustes.
Recommandation 13 :	Configurer le Private VLAN invité en mode isolated lorsque le point d'accès Wifi prend en charge cette fonctionnalité.
Recommandation 14 :	Ne pas conserver un nom de réseau (SSID) générique et proposé par défaut. Le SSID retenu ne doit pas être trop explicite par rapport à une activité professionnelle ou une information personnelle.
Recommandation 15 :	Désactiver systématiquement la fonction WPS (Wifi Protected Setup) des points d'accès.
Recommandation 16 :	Sécuriser l'administration du point d'accès Wifi, en : – utilisant des protocoles d'administration sécurisés (HTTPS par exemple) ; – connectant l'interface d'administration à un réseau filaire d'administration sécurisé, a minima en y empêchant l'accès aux utilisateurs Wifi ; – utilisant des mots de passe d'administration robustes.
Recommandation 17 :	Configurer le point d'accès pour que les événements de sécurité puissent être supervisés. En environnement professionnel, il est préférable de rediriger l'ensemble des événements générés par les points d'accès vers une infrastructure centrale de supervision.
Recommandation 18 :	Maintenir le microgiciel des points d'accès à jour.
Recommandation 19 :	Ne jamais sous-estimer la zone de couverture d'un réseau Wifi. Ne jamais penser être à l'abri de tout risque du fait de l'isolement géographique du point d'accès Wifi.
Recommandation 20 :	En environnement professionnel, isoler le réseau Wifi du réseau filaire et mettre en place des équipements de filtrage réseau permettant l'application de règles strictes et en adéquation avec les objectifs de sécurité de l'organisme. Comme pour le point d'accès, l'équipement de filtrage doit

	être paramétré pour que puissent être supervisés les événements de sécurité.
Recommandation 21 :	Si un réseau Wifi « visiteurs » doit être mis en place, il est recommandé de déployer une infrastructure dédiée à cet usage, isolée des autres et ne donnant accès à aucune ressource du réseau interne. Ce réseau doit par ailleurs avoir sa propre politique de sécurité beaucoup plus restrictive.
Recommandation 22 :	Mettre en œuvre les GPO nécessaires à l'application de stratégies de sécurité verrouillant les configurations Wifi des postes clients Windows, de manière à appliquer techniquement différentes recommandations indiquées dans ce document.
Recommandation 23 :	Afin de ne pas les communiquer aux utilisateurs, déployer sur les postes Windows les informations de connexion au Wifi par GPO (nom de réseau, clé d'accès, certificats éventuels si la méthode EAP le nécessite, etc.).

Tableau 2.2 : Recommandations de la norme ANSSI [3]

b) Norme ISO/CEI 27002

La norme ISO/CEI 27002 est une norme internationale concernant la sécurité de l'information destinée à être utilisées par des organisations qui désire de sélectionner les mesures nécessaires dans le cadre du processus de mise en œuvre d'un système de management de la sécurité de l'information (SMSI) selon l'ISO/CEI 27001; de mettre en œuvre des mesures de sécurité de l'information largement reconnues; et d'élaborer leurs propres lignes directrices de management de la sécurité de l'information.

L'ISO 27002:2013 donne des lignes directrices en matière de normes organisationnelles relatives à la sécurité de l'information et des bonnes pratiques de management de la sécurité de l'information, incluant la sélection, la mise en œuvre et la gestion de mesures de sécurité prenant en compte le ou les environnements de risques de sécurité de l'information de l'organisation. Le chapitre 13 de la norme nous donne des consignes qu'on doit suivre pour garder le réseau d'un établissement sécurisé au cas du déploiement d'un réseau sans fil [11].

Chapitre 13 : sécurité des communications 13.1.1 Contrôle des réseaux	Dans le cas des environnements sensibles, il convient de veiller à traiter l'ensemble des accès sans fil comme des connexions externes et de séparer ces accès des réseaux internes jusqu'à franchissement de la passerelle conformément à la politique de contrôle des réseaux avant d'accorder l'accès aux systèmes internes.
	Les technologies d'authentification, de chiffrement et de contrôle d'accès réseau au niveau utilisateur propres aux

	réseaux sans fil modernes normalisés peuvent être suffisantes pour permettre une connexion directe au réseau interne de l'organisation, lorsqu'elles sont correctement mises en œuvre.
	Il convient de définir des mesures spéciales pour préserver la confidentialité et l'intégrité des données transmises sur les réseaux publics ou les réseaux sans fil et de protéger les systèmes et applications connectés.

Tableau 2.3 : Recommandations de la norme 27002 [4]

c) NORME PCI-DSS

La norme PCI DSS est l'acronyme anglais de Payment Card Industry Data Security Standard a été élaborée par les sociétés de carte de paiement, c'est-à-dire American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc, pour aider à faciliter une large adoption de mesures de sécurité des bases de données. C'est une norme globale qui a créé un standard commun pour la sécurité de tous les circuits de paiement touchant les cartes bancaires. Toute organisation qui émet, conserve, ou traite des données de carte de paiement est tenue de se conformer à la Norme PCI DSS ; le non-respect de ce cadre réglementaire peut entraîner des amendes et frais élevés. L'impact négatif des cyber-attaques sur la confiance des clients et sur l'activité financière rend la protection des données de carte de paiement non seulement importante, mais essentielle, et ce, quelque soit le type de commerce. Les grands détaillants en ligne ne sont pas les seules organisations ciblées. L'attention du public est souvent focalisée sur des pertes de sociétés importantes, mais il s'avère que de plus en plus d'actions criminelles visent des sites e-commerce de petite taille. La norme PCI DSS a 12 exigences précises. Il est énoncé dans ce document celles qui ont un rapport avec le réseau sans fil [12].

1ère exigence : installer et gérer une configuration de pare-feu afin de protéger les données des titulaires de carte	1.1.2 Mettre en place des normes de configuration de pare-feu incluant un diagramme du réseau à jour, avec toutes les connexions à des données de titulaires de carte, y compris tous réseaux sans fil. 1.3.8 L'installation de pare-feux de périmètre entre tous réseaux sans fil et l'environnement de données de titulaires de carte, et la configuration de ces pare-feux de manière à bloquer tout trafic provenant de l'environnement sans fil, ou pour contrôler tout trafic (lorsqu'il est nécessaire à des fins commerciales) ;
2ème exigence : ne pas utiliser les paramètres par défaut du fournisseur pour les mots de passe et les autres paramètres de sécurité du système	2.1.1 Dans le cas des environnements sans fil, modifier les réglages par défaut du fournisseur sans fil, y compris notamment les clés Wired Equivalent Privacy (WEP), le Service Set IDentifier (SSID) par défaut, les mots de passe et les chaînes communautaires SNMP. Désactiver les émissions en clair du SSID sur le réseau. Mettre en place une technologie d'accès Wifi protégé (WPA et WPA2) pour le cryptage et

	l'authentification lorsqu'il existe une capacité WPA.
3ème exigence : protéger les données des titulaires de carte en stock	3.4 Rendre le PAN, au minimum, illisible où qu'il soit stocké (y compris des données sur support numérique portable, support de sauvegarde, journaux et données reçues de, ou stockées par des réseaux sans fil)
4ème exigence : crypter la transmission des données des titulaires de carte sur les réseaux publics ouverts	4.1.1 Dans le cas des réseaux sans fil transmettant des données de titulaire de carte, crypter les transmissions en utilisant la technologie d'accès protégé au Wifi (WPA ou WPA2), IPSEC VPN ou SSL/TLS. Ne jamais se fier uniquement au protocole WEP (Wired Equivalent Privacy) pour protéger la confidentialité et l'accès à un réseau LAN sans fil
10ème exigence : suivre et surveiller tous les accès aux ressources du réseau et aux données des titulaires de carte	10.5.4 Copier les journaux relatifs aux réseaux sans fil sur un serveur registre du LAN interne.

Tableau 2.4 : Recommandations de la norme PCI-DSS [5]

d) Norme NIST

Le « National Institute of Standards and Technology » connu sous le sigle **NIST**, est une agence du Département du Commerce des États-Unis. Son but est de promouvoir l'économie en développant des technologies, la métrologie et des standards de concert avec l'industrie [13]. Les sections qui ont traité la sécurité dans les réseaux sans fil sont les suivantes :

Section 2 : Configuration de la sécurité WLAN	Les organisations devraient procéder à des évaluations de risque pour identifier les menaces contre leurs réseaux locaux sans fil et de déterminer l'efficacité des contrôles de sécurité existants lutter contre ces menaces
Section 2 : Configuration de la sécurité WLAN Pour tous leurs périphériques clients WLAN:	désactiver toutes les interfaces réseau qui ne sont pas autorisées pour toute utilisation (y compris pendant les plans d'urgence pour la continuité des activités, la reprise après sinistre, etc.), et configurer l'appareil de sorte que l'utilisateur ne peut pas les activer ou contourner les restrictions autrement
Section 2 : Configuration de la sécurité WLAN Pour tous leurs périphériques clients WLAN non autorisés pour deux connexions:	Mettre en œuvre les contrôles appropriés techniques de sécurité de telle sorte que toutes les configurations connectées doubles sont interdites.
	Si possible, configurer les périphériques pour désactiver pontage (passage du trafic entre les réseaux). C'est une précaution au cas où une double connexion non autorisée se produit

Section 2 : Configuration de la sécurité WLAN Pour tous les appareils client Wifi autorisés pour deux connexions	Mettre en œuvre les contrôles de sécurités techniques appropriés pour que les configurations doubles connectées autorisées ne soient actives que lorsque cela est nécessaire et que toutes les autres configurations connectées doubles sont interdites.
	Configurer les périphériques pour désactiver pontage (passage du trafic entre les réseaux), sauf si absolument nécessaire.
Section 3 : Surveillance de la sécurité WLAN Les Organisations avec WLAN devraient mettre en œuvre des solutions de surveillance continue pour leurs réseaux locaux sans fil qui offrent toutes les capacités de détection suivantes:	Dispositifs WLAN non autorisés, y compris les points d'accès indésirables et périphériques clients non autorisés
	Périphériques WLAN qui sont mal configuré ou en utilisant des protocoles WLAN faibles et les implémentations du protocole
	Les habitudes d'utilisation de WLAN inhabituelles, comme un nombre extrêmement élevé de dispositifs clients à l'aide d'un AP particulier, volumes anormalement élevés de trafic WLAN impliquant un dispositif client particulier, ou de nombreuses tentatives infructueuses pour rejoindre le WLAN dans un court laps de temps
	L'utilisation de scanners WLAN actifs (par exemple, la guerre conduite outils) qui génèrent du trafic WLAN. L'utilisation de capteurs passifs ne peut pas être détectée par les contrôles de surveillance.
	Attaques DoS et conditions (par exemple, les interférences de réseau). Beaucoup des attaques par déni de service sont détectées par comptage des événements pendant les périodes de temps et d'alerte lorsque les valeurs seuils sont dépassées.
	Usurpation d'identité et les attaques man-in-the-middle.
Section 3 : Surveillance de la sécurité WLAN les organisations devraient envisager lors de la planification de la fréquence et de l'ampleur des évaluations périodiques	L'emplacement de l'installation en cours de numérisation, parce que la proximité physique d'un bâtiment à un espace public (par exemple, les rues et les espaces communs publics) ou son emplacement dans une région métropolitaine occupée peut augmenter le risque de menaces WLAN
	Le niveau de sécurité de données à transmettre sur le réseau local sans fil
	Les changements physiques aux installations, tels que les projets de construction qui pourraient influer sur la force et la propagation des signaux WLAN

Tableau 2.5 : Recommandations de la norme NIST [6]

2. Analyse de leurs avantages et inconvénients par rapport au projet à mettre en œuvre

Normes	Avantage par rapport au projet à mettre en œuvre	Inconvénient par rapport au projet à mettre en œuvre
ANSSI	Donne les précautions et les solutions à mettre en place pour protéger les usagers d'internet.	----------
ISO 27002	Insiste sur la nécessité de mettre en place les protocoles de sécurité et des processus de gestion des accès.	Donne uniquement des recommandations. N'indique pas nommément les solutions techniques à mettre en place.
PCI-DSS	S'intéresse à protéger le réseau sans fil afin de garantir la sécurité des données des utilisateurs de carte bancaire.	Précise seulement quelques protocoles de sécurité à mettre en place, sans faire allusion à des actions à éviter lorsqu'on utilise un réseau Wifi.
NIST	Permet une prise de conscience des failles de sécurité dans les réseaux sans fil.	Ne donne pas la solution technique pour y remédier.

Tableau 2.6 : Comparaison entre les normes supportant la sécurité du WIFI

3. Les solutions et technologies de connexion sécurisées via réseau sans fil

Cette partie concerne l'étude des points d'accès existant sur le marché et qui supportent le standard 802.11ac, ce standard permet une connexion sans fil haut débit à un réseau local.il existent plusieurs entreprises qui produisent ce type de matériel, mais qui diffèrent dans les propriétés : Il existe comme exemple: FORTINET [14], CISCO-MERAKI [15], ARUBA [16], RUCKUS [17] et AEROHIVE [18].

	FORTINET AP-221C	FORTINET AP-223C	FORTINET AP-320C	FORTINET AP-321C	AEROHIVE AP-130	AEROHIVE AP-230	AEROHIVE AP-370	ARUBA AP-220	ARUBA AP-228	ARUBA AP-210
Puissance de transmission	20 dBm	17 dBm	21 dBm	20 dBm			20 dBm	18 dBm	•Sur 2.4-GHz: +23 dBm (18 dBm par chaine) •Sur 5-GHz: 23 dBm (18 dBm par chaine)	18 dBm
DÉBITS	•300Mbit/s pour 2,4GHZ • 867Mbit/s pour 5GHZ	•300Mbit/s pour 2,4GHZ •867Mbit/s pour 5GHZ	•450Mbit/s pour 2,4GHZ • 1300Mbit/s pour 5GHZ	•450Mbit/s pour 2,4GHZ • 1300Mbit/s pour 5GHZ	•300Mbit/s pour •2,4GHZ 867 Mbit/s pour 5GHZ	•450Mbit/s pour 2,4GHZ • 1300Mbit/s pour 5GHZ	•450Mbit/s pour 2,4GHZ • 1300Mbit/s pour 5GHZ	•600 Mbit/s (2,4 GHz) • 1 300 Mbit/s (5 GHz)	•600 Mbit/s (2,4 GHz) • 1 300 Mbit/s (5 GHz)	•450 Mbps(2.4-GHz) • 1 300 Mbps (5 GHz)
NORMES	802.11 a/b/g/n/ac	802.11 a/b/g/n/ac	802.11 a/b/g/n/ac	802.11 a/b/g/n/ac	IEEE 802.11a/b/g/n/ac	IEEE 802.11a/b/g/n/ac	IEEE 802.11a/b/g/n/ac	802.11 a/b/g/n/ac	IEEE 802.11a/b/g/n/ac	IEEE 802.11a/b/g/n/ac
CHAÎNES RADIO / FLUX	2 x 2:2	2 x 2:2	3 x 3:3	3 x 3:3	2x2	3 x 3	3 x 3	3 x 3 : 3	3 x3:3	3 x3:3
802.1X POUR PORTS ETHERNET	Authentificateur & Demandeur	Authentificateur & Demandeur	Authentificateur & Demandeur	Authentificateur & Demandeur	Authentificateur & Demandeur	Authentificateur & Demandeur	Authentificateur & Demandeur	pris en charge	pris en charge	pris en charge
TUNNELLISAN								VPN avec ipsec	VPN avec IPsec	VPN avec IPsec
802.11^{e}	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge	Pris en charge

	FORTINET AP-221C	FORTINET AP-223C	FORTINET AP-320C	FORTINET AP-321C	AEROHIVE AP-130	AEROHIVE AP-230	AEROHIVE AP-370	ARUBA AP-220	ARUBA AP-228	ARUBA AP-210
SÉCURITÉ SANS FIL	AES-CCMP, WPA2-PSK, RC4, TKIP, TLS, TTLS, WEP, WPA, WPA-PSK, WPA2	AES-CCMP, WPA2-PSK, RC4, TKIP, TLS, TTLS, WEP, WPA, WPA-PSK, WPA2	AES-CCMP, WPA2-PSK, RC4, TKIP, TLS, TTLS, WEP, WPA, WPA-PSK, WPA2	AES-CCMP, WPA2-PSK, RC4, TKIP, TLS, TTLS, WEP, WPA, WPA-PSK, WA2	WPA and WPA2, 802.11i, WEP, 802.1x, PSK, Aerohive PPSK, CCMP, TKIP, et RC4 (WEP seulement)	WPA(TM) and WPA2 (TM), 802.11i, WEP, 802.1x, PSK, CCMP, TKIP, and RC4 (WEP seulement)	WPA(TM) and WPA2 (TM), 802.11i, WEP, 802.1x, PSK, CCMP, TKIP, and RC4 (WEP seulement)	•abonnement au service OpenDNS • Trusted Platform Module (TPM)	•abonnement au service OpenDNS • Trusted Platform Module (TPM)	•abonnement au service OpenDNS • Trusted Platform Module (TPM)
BSSID	16	16	16	16				16		

Tableau 2.7 : Caractéristiques des points d'accès supportant 802.11ac

	ARUBA AP-200	MERAKI AP-MR32	MERAKI AP-MR34	RUCKUS R700	RUCKUS R600	RUCKUS R500	RUCKUS H500	RUCKUS T300
Puissance de transmission	18 dBm	15 dBm sur 2,4 GHz; •20 dBM sur 5 GHz		29 dBm sur 2,4 GHz; 27 dBM sur 5 GHz	28 dBm pour 2.4GHz†/ 27 dBm pour 5GHz†	26 dBm pour 2,4 GHz†/25 dBm pour 5GHz†	19 dBm sur 2,4 GHz ; 22 dBm sur 5,0 GHz	26 dBm pour 2,4 GHz ; 25 dBm pour 5,0 GHz
DÉBITS	300 Mbps	1200 Mbps max rate	1750 Mbit/s	•450 Mbit/s (2,4 GHz) • 1 300 Mbit/s (5 GHz)				• 2,4 GHz :300 Mbit/s • 5 GHz : 867 Mbit/s
NORMES	IEEE 802 .11a/b/g /n/ac	IEEE 802.11a/b /g/n/ac	IEEE 802.11 a/b/g/n/ac • une radio dédiée à l'analyse du spectre et au WIPS bi-bande	IEEE 802.11a/ b/g/n/ac	IEEE 8 02.11a / b/g / n /a c	IEEE 802.11a/ b/g/n/ac	IEEE 802.11 a/b/g/n/ac	• 5 GHz IEEE 802.11 ac • 2 GHz IEEE 802.11 g/n
CHAÎNES RADIO / FLUX	2 x2:2	2 x 2:2	3 x 3:3	3 x 3:3	3 x 3	2 x 2	2 x 2 : 2	2 x2:2

	ARUBA AP-200	MERAKI AP-MR32	MERAKI AP-MR34	RUCKUS R700	RUCKUS R600	RUCKUS R500	RUCKUS H500	RUCKUS T300
802.1X POUR PORTS ETHERNET	pris en charge	Authentificateur & Demandeur	Authentificateur & Demandeur	Authentificateur & Demandeur			Authentificateur & Demandeur	
TUNNELLISATION	pris en charge	VPN télétravailleur avec Ipsec	VPN télétravailleur avec Ipsec	L2TP, PPPoE			L2TP, PPPoE	
STATIONS SIMULTANÉES				Jusqu'à 500	500 clients par AP	500 clients par point d'accès	Jusqu'à 100	jusqu'à 500 clients par AP
802.11^{e}	Pris en charge	Pris en charge	Pris en charge	Pris en charge			Pris en charge	
SÉCURITÉ SANS FIL	• abonnement au service OpenDNS • Trusted Platform Module (TPM)	Stratégie de pare-feu intégrée • Système de détection d'intrusion sans fil (WIPS) • WEP, WPA, WPA2-PSK, WPA2-Enterprise avec 802.1X • Chiffrement TKIP et AES • Isolation des invités • Confinement des points d'accès non autorisés	Stratégie de pare-feu intégrée • Système de détection d'intrusion sans fil (WIPS) • WEP, WPA, WPA2-PSK, WPA2-Enterprise avec 802.1X • Chiffrement TKIP et AES • Isolation des invités • Confinement des points d'accès non autorisés	WPA-PSK,WPA-TKIP,WPA2 AES, 802.11i •Authentification via 802.1X avec le ZoneDirector, base de données d'authentification locale, prise en charge pour RADIUS et Active Directory	WPA-PSK,WPA-TKIP,WPA2 AES, 802.11i •Authentification via 802.1X avec le ZoneDirector, base de données d'authentification locale, prise en charge pour RADIUS, LDAP et Active Directory	WPA-PSK,WPA-TKIP,WPA2 AES, 802.11i •Authentification via 802.1X avec le ZoneDirector, base de données d'authentification locale, prise en charge pour RADIUS et Active Directory	• WPA-PSK, WPA-TKIP, WPA2 AES, 802.11i •Authentification via 802.1X, base de données d'authentification locale, prise en charge de RADIUS, de LDAP et d'Active Directory	
BSSID							8 BSSID par radio	• Jusqu'à 32 en 2,4 GHz • Jusqu'à 16 en 5 GHz

Tableau 2.8 : Caractéristiques des points d'accès supportant 802.11ac

4. Etude Comparative des solutions de point d'accès existant sur le marché

Le tableau ci-dessous est une comparaison entre les différentes technologies, il va nous permettre par la suite de choisir le bon point d'accès selon le besoin exprimé par le client.

EXIGENCES /TECHNOLOGIES	CISCO-MERAKI	RUCKUS	ARUBA	AEROHIVE	FORTINET
Chiffrement WPA2/WPA	✓	✓	✓	✓	✓
Authentification via radius	✓	✓	✓	✓	✓
802.11 e	✓	✓	✓	✓	✓
NORME 802.11ac	✓	✓	✓	✓	✓
Débit très élevé	✓	—	—	—	—
Tunnelisation	✓	✓	✓	—	—
WIPS	✓	—	✓	✓	—
CLOUD	✓	✓	✓	✓	✓
Durée de fonctionnement long	—	—	✓	—	—
Focalisation de rayonnement	—	✓	—	—	—

Tableau 2.9 : Comparaison entre les points d'accès supportant 802.11ac

Chapitre 3 : Étude de la solution à mettre en ouvre

Ce chapitre étudie les protocoles de sécurité et les configurations à mettre en place dans le projet, puis la dernière partie est consacrée à la mise en œuvre de la solution de l'architecture sécurisée.

L’étude du projet est divisée en deux phases comme illustrées ci-dessous :

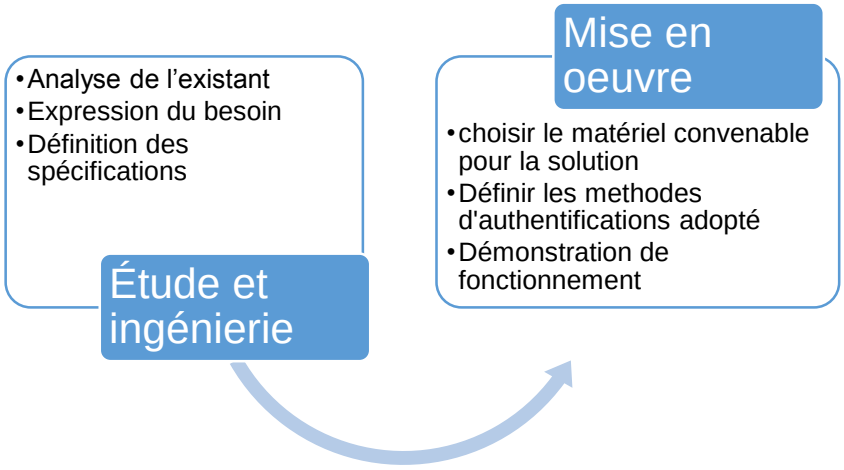

Figure 3. 1 : Les phases d’étude du projet

I. Étude et Ingénierie

1. Analyse de l’existant

L’analyse de l‘existant consiste à analyser les solutions déjà déployer pour aboutir à une critique de l'existant qui analyse les points positifs et négatifs, et dégage les améliorations à apporter pour l’architecture qu’on va mettre en place. Il est présenté ci-dessous des exemples de cas de déploiement dans un hôtel et une moyenne entreprise.

a) Exemple 1

Dans cet exemple c’est le cas de déploiement d’un réseau sans fil dans une moyenne entreprise.

Fonctionnement :

Le réseau interne de l’entreprise est protégé par des firewalls. Les deux réseaux ; d’administration et des commerciaux sont séparés avec des VLAN et dans chaque Vlan est connecté des points d’accès. Et afin de sécuriser l’accès aux différents serveurs et applications métiers, l’accès est limité à quelque employé.

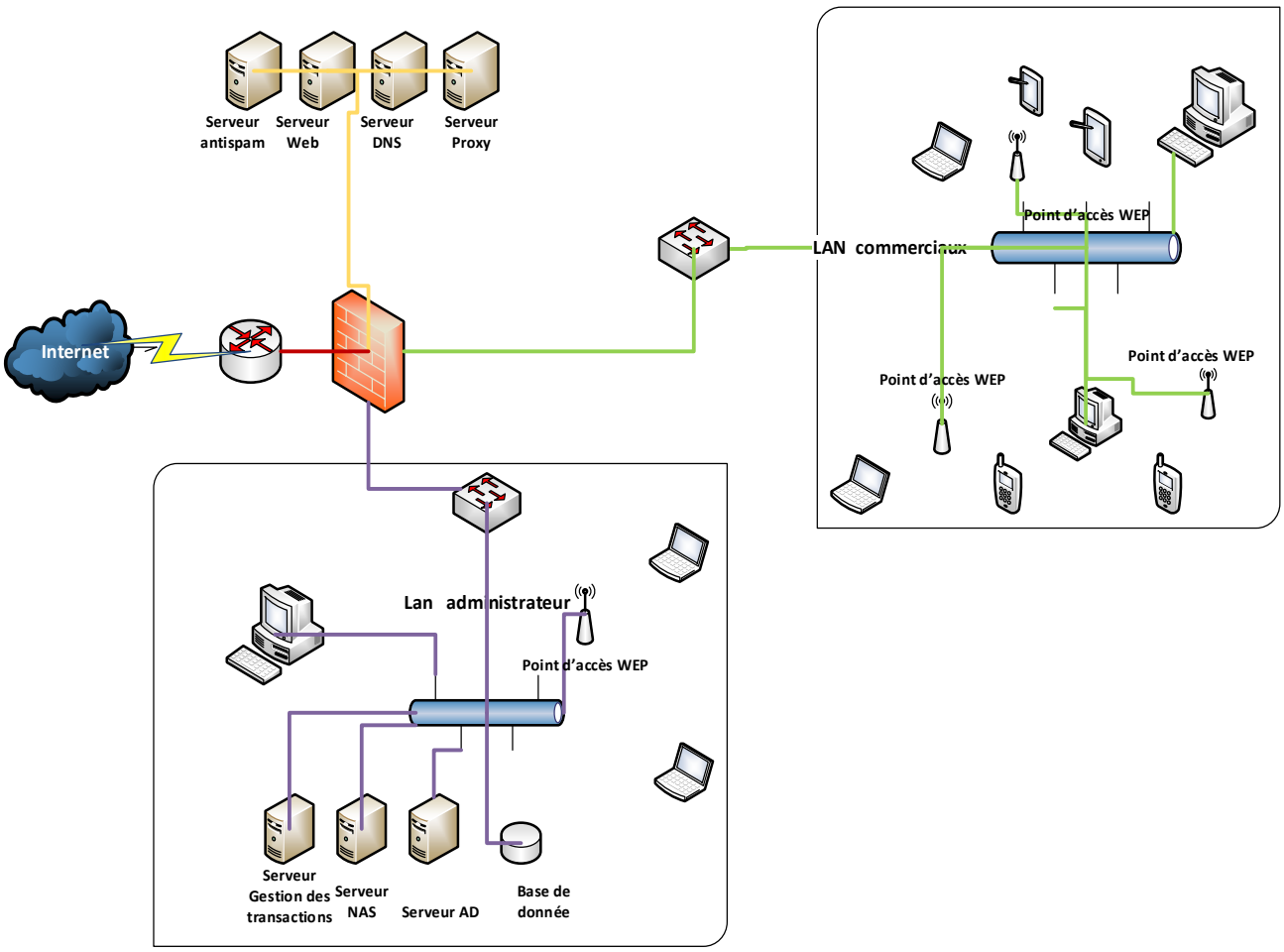

Figure 3.2 : Architecture d'une entreprise

Avantages:

- Permet de se connecter au réseau sans fil après l'authentification.
- La bande passante dédiée à chacun d'entre eux est limitée pour ne pas saturer la connexion internet.
- Les réseaux sont séparés par des VLAN.
- Bornes câblées au réseau via un commutateur gigabit POE permettant d'assurer l'alimentation électrique des bornes et la connexion au réseau du bâtiment.
- Bornes installées au plafond pour une meilleure diffusion.

Inconvénients :

- Utilise le mode d'authentification WEP.
- N'utilise pas une authentification via serveur Radius.

- N'utilise pas le filtrage MAC pour limiter les équipements connectés.
- Il n'y a pas de VLAN visiteurs pour empêcher à ce dernier d'accéder aux données circulant dans le réseau de l'entreprise.
- Interférence du rayonnement des points d'accès dans les zones de recouvrement.
- Ne limite pas la puissance des bornes pour limiter la diffusion en dehors du bâtiment.

b) Exemple 2 :

C'est l'exemple d'un déploiement d'un réseau sans fil dans un hôtel.

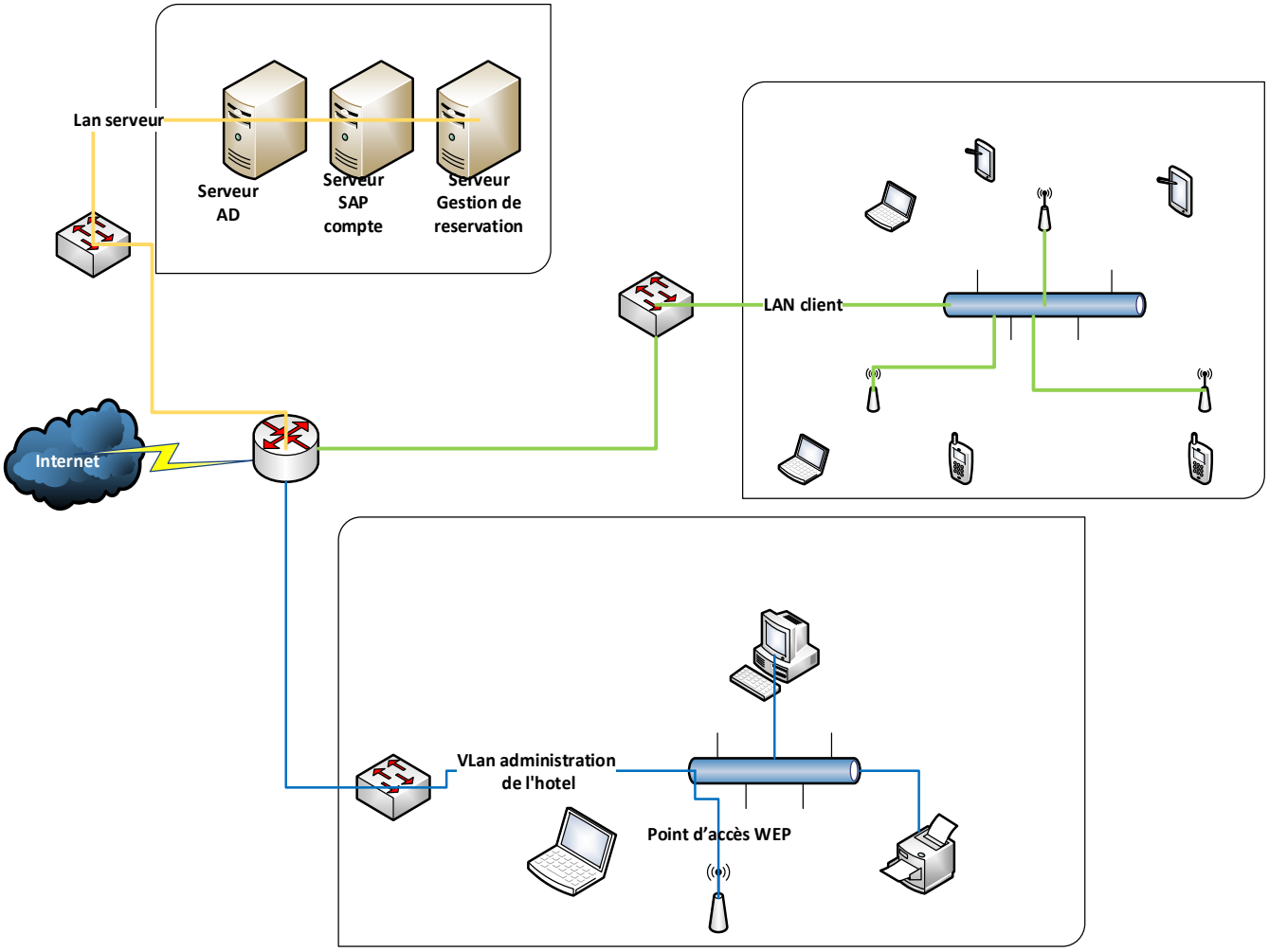

Figure 3.3 : Architecture d'un hôtel

Fonctionnement

Ce schéma est le réseau d'un hôtel qui utilise le réseau sans fil Wifi. Les employés de l'hôtel se connectent aux points d'accès après une authentification par le protocole WEP; sur

le même réseau filaire, ils sont connectés d'autres équipements comme des PC fixes, des imprimantes, des caméras de surveillances…pour les visiteurs et sur un autre réseau LAN, ils ont un accès au Wifi sans authentification.les serveurs sont mis dans un Lan séparé et protégé par des droits d'accès.

Avantages :

- Isolation des serveurs des autres réseaux LAN.
- Création des Vlans différents : Vlan client, Vlan employé, Vlan Serveur.

Inconvénients :

- Les points d'accès met à la disposition des clients ne sont pas sécurisés par les protocoles d'authentifications.
- Utilise le mode d'authentification WEP pour les points d'accès qui se trouvent dans le LAN employé.
- Possibilité d'accès aux réseaux LAN des employés par un malveillant et donc aux données stockées sur les équipements connectés.
- N'utilise pas une authentification via serveur Radius.
- N'utilise pas le filtrage MAC.
- Accès à l'interface de configuration des points d'accès.

2. Expression du besoin :

Après l'étape de l'étude d'existant, c'est l'étape d'expression du besoin, pour arriver à réaliser le but du projet convenablement à ce que le client attend. Elle permet de définir le résultat recherché non plus en termes techniques décrivant la solution, mais en termes d'exigences à satisfaire.

L'architecture qu'on va mettre devra s'assurer de répondre aux besoins suivants :

- Les interfaces des commutateurs existants permettent un débit de 1000Mbps.
- Segmenter le réseau en créant des VLANs et mettre en place une sécurité qui permettra à tous les VLANs de ne pas communiquer.
- Proposer des points d'accès compatibles avec les normes Wifi a/b/g/n/ac.

- Définition des règles applicatives à mettre en œuvre sur le réseau de communication radio.
- Définition des règles de sécurité à mettre en place : authentification via serveur IAS, authentification forte, Multi SSID, cryptage des connexions.
- Centraliser l'administration pour une meilleure gestion.
- Accessibilité à l'administration depuis des postes définis.
- Sécuriser l'accès physique des points d'accès (... pirate qui remet paramètres par défaut).
- Journalisation des accès.
- Pouvoir détecter les anomalies de configuration automatiquement (par des outils d'analyse automatique des vulnérabilités du système).
- La confidentialité, consistante à assurer que les seuls utilisateurs autorisés aient accès aux ressources qu'ils échangent.
- La disponibilité, permettant de maintenir le bon fonctionnement du système d'information pour assurer un accès permanent.
- Journalisation des actions afin de s'assurer de la non-répudiation des données.
- Un mécanisme de sécurité pour isoler logiquement le trafic lorsqu'une personne malveillante parvient à accéder physiquement au réseau interne d'une entreprise.
- Vérifier si les employés n'installent pas des AP sans autorisation.
- Assurer la mobilité des utilisateurs.

On doit aussi savoir que le besoin diffère d'une entreprise à une autre selon la taille de l'endroit où on va déployer le réseau sans fil.

Petite entreprise :

Dans l'architecture d'une petite entreprise, afin de déployer le Wifi pour faire communiquer les utilisateurs on va se contenter d'utiliser des points d'accès, tout en le configurant convenablement afin d'assurer la sécurité des données.

Moyenne entreprise :

Par rapport aux petites entreprises, il y'a un nombre important d'utilisateurs donc on va avoir besoin de plusieurs points d'accès, et afin de gérer la mobilité de chaque utilisateur il faut avoir un contrôleur WLAN.

Grande entreprise

Si l'entreprise à plusieurs sites on va avoir besoin de connecter ces différents sites et on peut recourir au Cloud.

3. Définition des spécifications techniques

Ensuite c'était l'étape de Définition des spécifications, qui consiste à choisir les spécifications du matériel qu'on va utiliser selon le besoin déjà exprimé.

On veut arriver à réaliser une architecture qui est sécurisée avec pas mal d'interactions avec l'extérieur. Selon les besoins exprimés par le client on va avoir besoin d'un serveur LDAP, serveur RADIUS; et comme équipements, on va utiliser des points d'accès et contrôleurs WLAN.

Le protocole RADIUS propose une fonctionnalité d'accounting assurant la journalisation des accès. Le serveur LDAP permet de gérer des annuaires, c.-à-d. d'accéder à des bases d'informations sur les utilisateurs d'un réseau par l'intermédiaire du protocole TCP/IP.

Les points d'accès que nous allons utiliser doivent avoir les caractéristiques suivantes pour répondre aux besoins:

- Standard 802.11ac (2,4 GHz/5 GHz).
- Taux de transfert des données: connexion sans fil à 450 MBits/s (norme IEEE 802.11n), 1300 Mbits/s (norme IEEE 802.11ac).
- Compatible avec les équipements 802.11b/g sans fil existants.
- Compatible réseau filaire.
- Power Over Ethernet (PoE) intégré.
- Sécurité WPA2 avec authentification RADIUS 802.1x de l'utilisateur.
- Configuration et gestion à partir du web.
- Chiffrement : TKIP, AES.

Pour le contrôleur WLAN on va avoir besoin d'un équipement qui a les caractéristiques suivantes :

- Le contrôleur doit être capable de mesurer dans un réseau pendant que le réseau se développe.

- Il doit fournir la transmission en temps réel entre la radio APs et d'autres périphériques pour fournir des stratégies de sécurité centralisées et l'accès invité.
- Il doit avoir le système de prévention des intrusions sans fil (WIPS), la Gestion contexte-avertie (emplacement).
- Il doit assurer la qualité de service (QoS) pour des Services de mobilité tels que la Voix et la vidéo, et le soutien OEAP de la solution de télétravailleur.
- Il doit supporter 5 points d'accès au minimum.
- Il doit offrir la couverture robuste avec le 802.11 a/b/g ou fournit la fiabilité sans précédent utilisant les solutions 802.11n/ac.

Techniquement ce projet qui a pour but de mettre en place une infrastructure Wifi sécurisée doit assurer :

- Le positionnement correct des APs.
- La fréquence utilisée.
- Les AP ne doivent pas être liés aux réseaux de câbles.
- Désactiver la diffusion du SSID dans les AP, et activer le masquage du SSID.
- Désactiver la communication client-client dans l'AP.
- changer les paramètres par défaut des AP (le SSID, les mots de passe, l'adresse IP, etc.).
- Mettre à jour en temps réel du firmware des AP et des cartes sans fil.
- Activer le contrôle d'accès au niveau MAC & IP (activer les deux).
- Activer le chiffrement (minimum de 128 ou de 256-bits).
- Éviter l'utilisation des clés secrètes WEP faciles à deviner.
- Désactiver le protocole DHCP sur les réseaux WLAN, surtout pour étendues des @ IP.
- Observer la création de nouveaux AP, car le pirate peut installer un AP jumeau.
- Installer un faux point d'accès, afin de tromper l'adversaire.
- Déployer un firewall pour protéger le réseau interne.
- Utiliser un mot de passe fort.

II. Mise en Œuvre de la solution

1. Description de la solution

Le but de l'architecture qu'on va mettre en œuvre est :

- Une sécurité assez élevée sans pour autant compromettre l'utilisation du réseau par les utilisateurs (le problème de tout admin …).
- Un coût très faible.
- Une maintenance aisée du réseau (ajout/suppression de postes/utilisateurs)

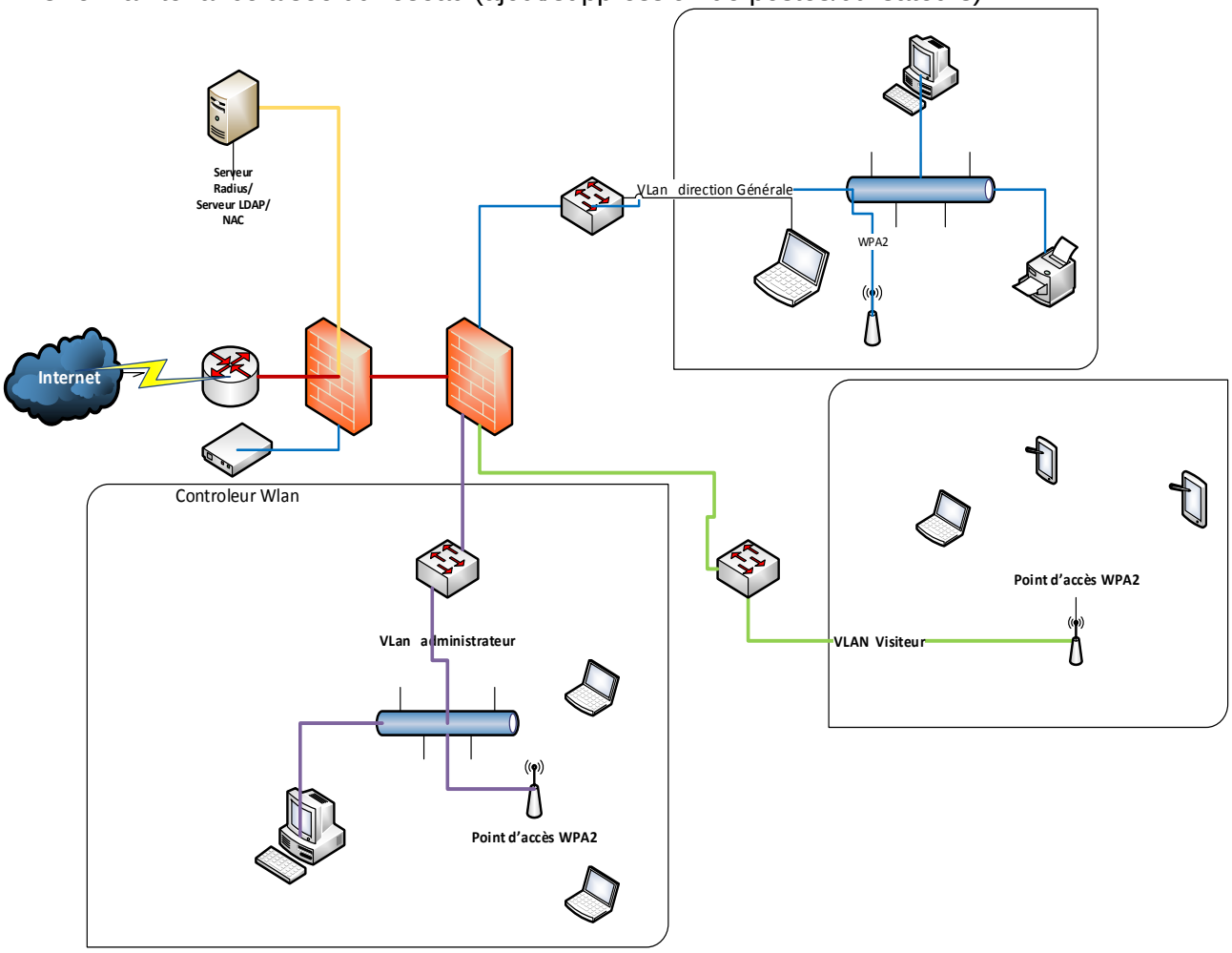

Figure 3.4 : Architecture Wifi sécurisé**e**

L'architecture est constituée de:

- un point d'accès réseau sans fil Aruba 228, matériel conforme à la norme 802.11i et permettant la mise en œuvre de tous les mécanismes de sécurité définis par la norme 802.11i. Ce choix a été fait puisque les points d'accès d'Aruba sont robustes.
- Un switch PoE (Power over Ethernet).
- Routeur

L’intérêt de choisir la technologie PoE dans le matériel qu’on va utiliser est de pouvoir installer les points d’accès dans les endroits qui sont dépourvus d’alimentation électrique (sous plafond par exemple).

L’architecture est alors composée d’un contrôleur ou plusieurs et de points d’accès légers. À chaque démarrage, le contrôleur s’associe avec le point d’accès, et ce dernier récupère sa configuration (paramètre réseau, fréquence utilisée, SSID, etc.) en se connectant au contrôleur. Une connexion sécurisée est établie entre le point d’accès et le contrôleur avec un protocole de contrôle et de gestion d’accès sans fil.

Après l’association au point d’accès du réseau sans fil, l’utilisateur est authentifié à travers une connexion sécurisée pour pouvoir disposer du service Wifi.

Au niveau du serveur RADIUS, la liste des utilisateurs du domaine est restreinte ayant le droit de se connecter au réseau sans fil. L’annuaire des utilisateurs est sous environnement windows server 2012.

Le serveur Radius a été déployé de façon à assurer une connexion par 802.1X, avec un chiffrement WPA2-AES et une gestion de l'authentification par EAP-TLS.

Pour l’authentification choisie, on a pris EAP-TLS vu qu’elle est très sécurisée. Le serveur d’authentification (de type RADIUS) et le client, chacun possède un certificat pour prouver son identité. [19]

Le processus d’accès au réseau est le suivant :

- Une demande par l’utilisateur à l’administrateur réseau est effectuée de manière officielle en faisant parvenir dans la demande l’adresse MAC, ainsi que les informations sur le device, afin que l’administrateur l’ajoute dans la table d’adresses autorisées
- Le point d'accès envoie une requête d'authentification au client. Le client répond avec son identifiant (nom de machine ou login), ce message est relayé par le point d'accès vers le serveur Radius.
- Le serveur RADIUS vérifie les informations d'identité, consulte sa stratégie d'accès et autorise ou refuse l'accès au client.
- S'il est reconnu, le client est autorisé à accéder au réseau et échange les clés de cryptage avec le point d'accès sans fil. En fait, les clés sont générées par le serveur RADIUS et transmises au point d'accès sans fil par un canal sécurisé. Si le client n'est pas reconnu par le serveur, il n'est pas autorisé à accéder au réseau et la communication s'interrompt.

- Le serveur choisit un algorithme de chiffrement parmi ceux qui lui ont été proposés par le client
- Le client vérifie le certificat du serveur et répond avec son propre certificat et sa clé publique.
- Grâce aux clés de cryptage, le client et le point d'accès sans fil établissent une connexion sans fil sécurisée, ce qui permet au client et au réseau interne de communiquer.

Concept de solution basé sur l'authentification EAP-TLS 802.1X

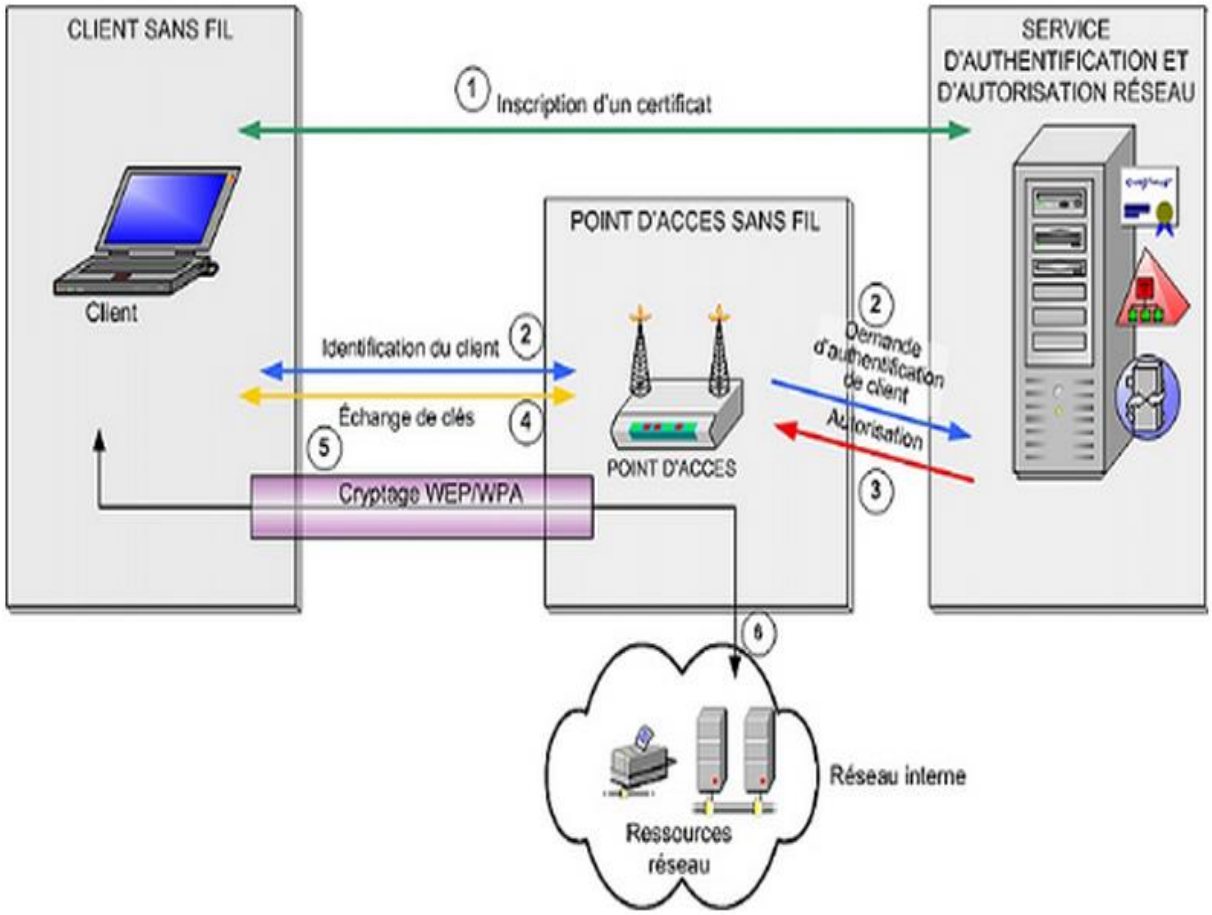

Figure 3.5 : Authentification EAP-TLS 802.1X

2. Démonstration de fonctionnement :

Dans cette partie, on s'intéresse seulement aux utilisateurs du réseau sans fil. La simulation de la solution adoptée est sur packet tracer, afin de s'assurer de sa fiabilité. Le schéma est le suivant :

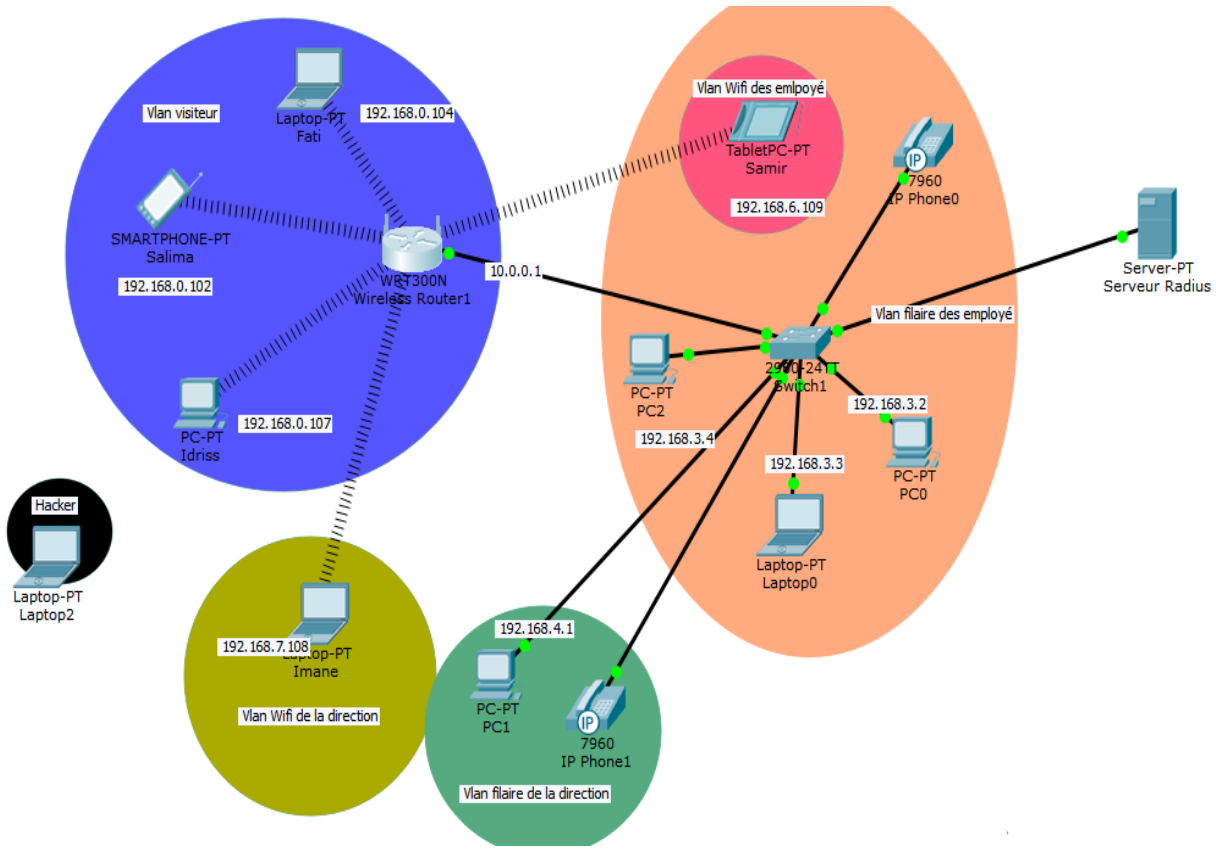

Figure 3.6 : Simulation de l'architecture sur packet tracer

Dans ce qui va suivre, on va configurer les équipements et on va faire un test pour montrer la crédibilité de la solution en termes de sécurité.

2.1 Outils de démonstration de fonctionnement :

Packet Tracer est un simulateur de matériel réseau Cisco (routeurs, commutateurs). Cet outil est créé par Cisco Systems qui le fournit gratuitement aux centres de formation, étudiants et diplômés participant, ou ayant participé au programme de formation Cisco (Cisco Networking Academy). Le but de Packet Tracer est d'offrir aux élèves et aux professeurs un outil permettant d'apprendre les principes du réseau, tout en acquérant des compétences aux technologies spécifiques de Cisco. Il peut être utilisé pour s'entraîner, se former, préparer les examens de certification Cisco, mais également pour de la simulation réseau.

2.2 Configuration du serveur Radius

On configure le DHCP pour qu'il donne les adresses IP aux équipements connectés sur le réseau, pour ainsi faciliter l'affectation des adresses IP pendant la configuration. (Figure 3.8)

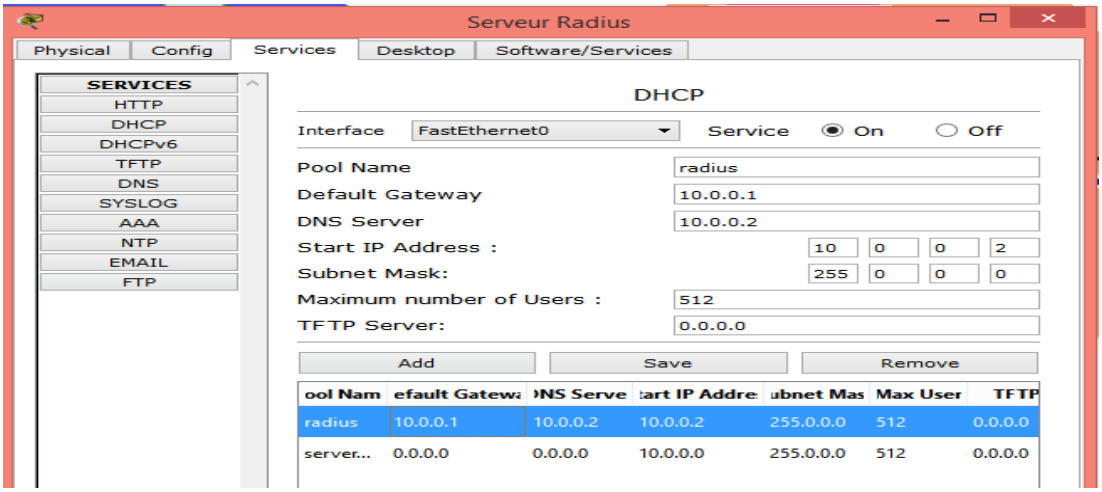

Figure 3.7 : Interface de configuration de DHCP sur Radius

Ensuite on configure le serveur Radius, en ajoutant les utilisateurs qui ont le droit d'accéder au réseau sans fil. On ajoute le login et mot de passe qui doit être unique.(Figure 3.9)

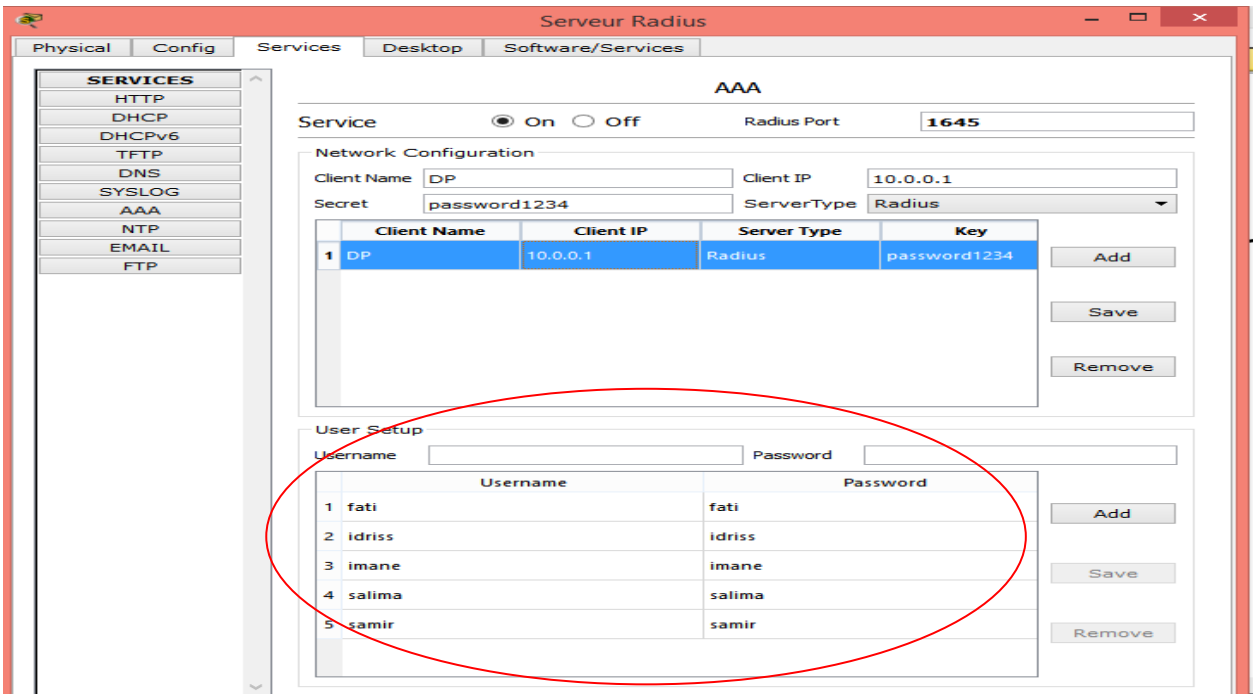

Figure 3.8 : Interface d'ajout des utilisateurs sur Radius

2.3 Configuration du routeur sans fil

On nomme le réseau sans fil, dans cette démonstration on a pris « dp », ensuite on active la diffusion du nom du réseau sans fil « SSID » pour faciliter l'authentification. (Figure 3.10)

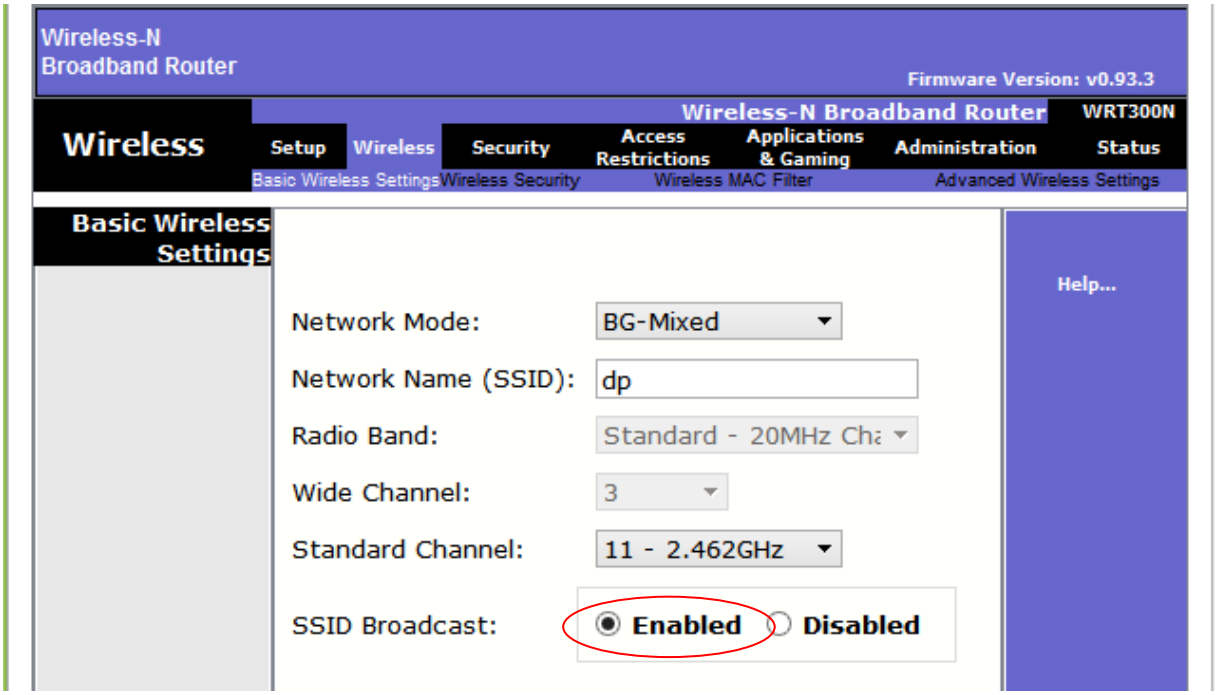

Figure 3.9 : Interface de configuration du réseau sans fil sur le routeur

Sur le routeur, on lui assigne son adresse IP et on active le protocole DHCP. (Figure 3.11)

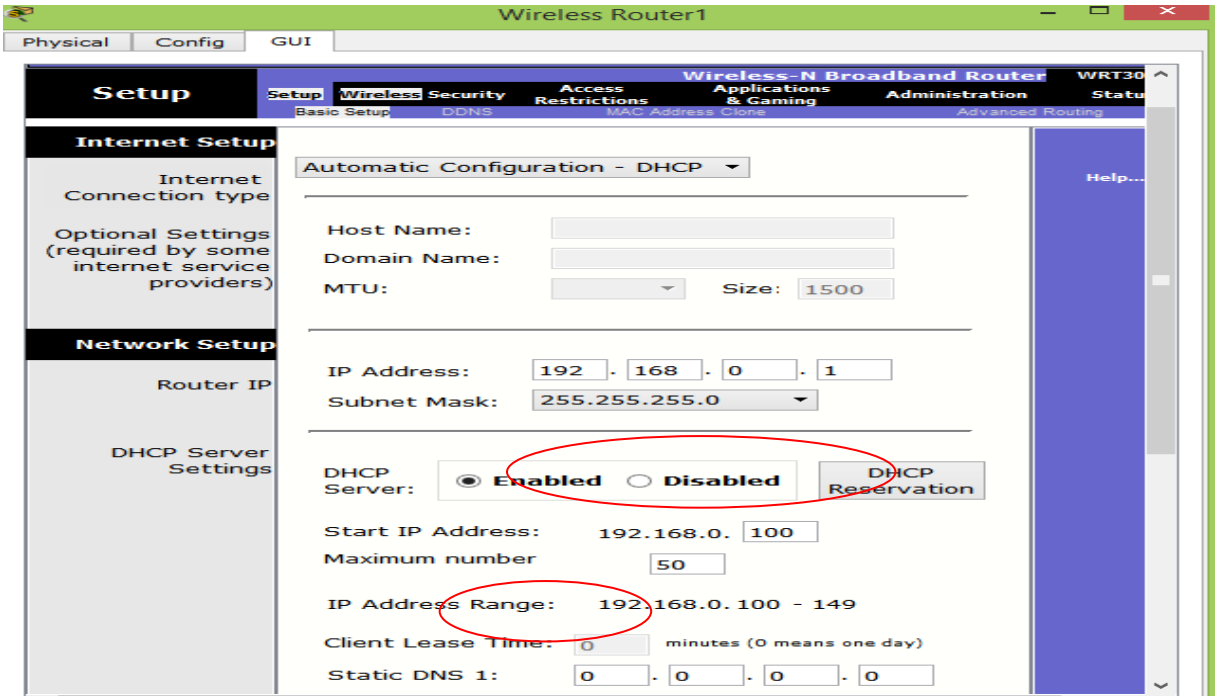

Figure 3.10 : Interface de configuration du DHCP sur le routeur sans fil

Le droit d'accès au paramètre du routeur est limité à l'administrateur du réseau par un identifiant. (Figure 3.12)

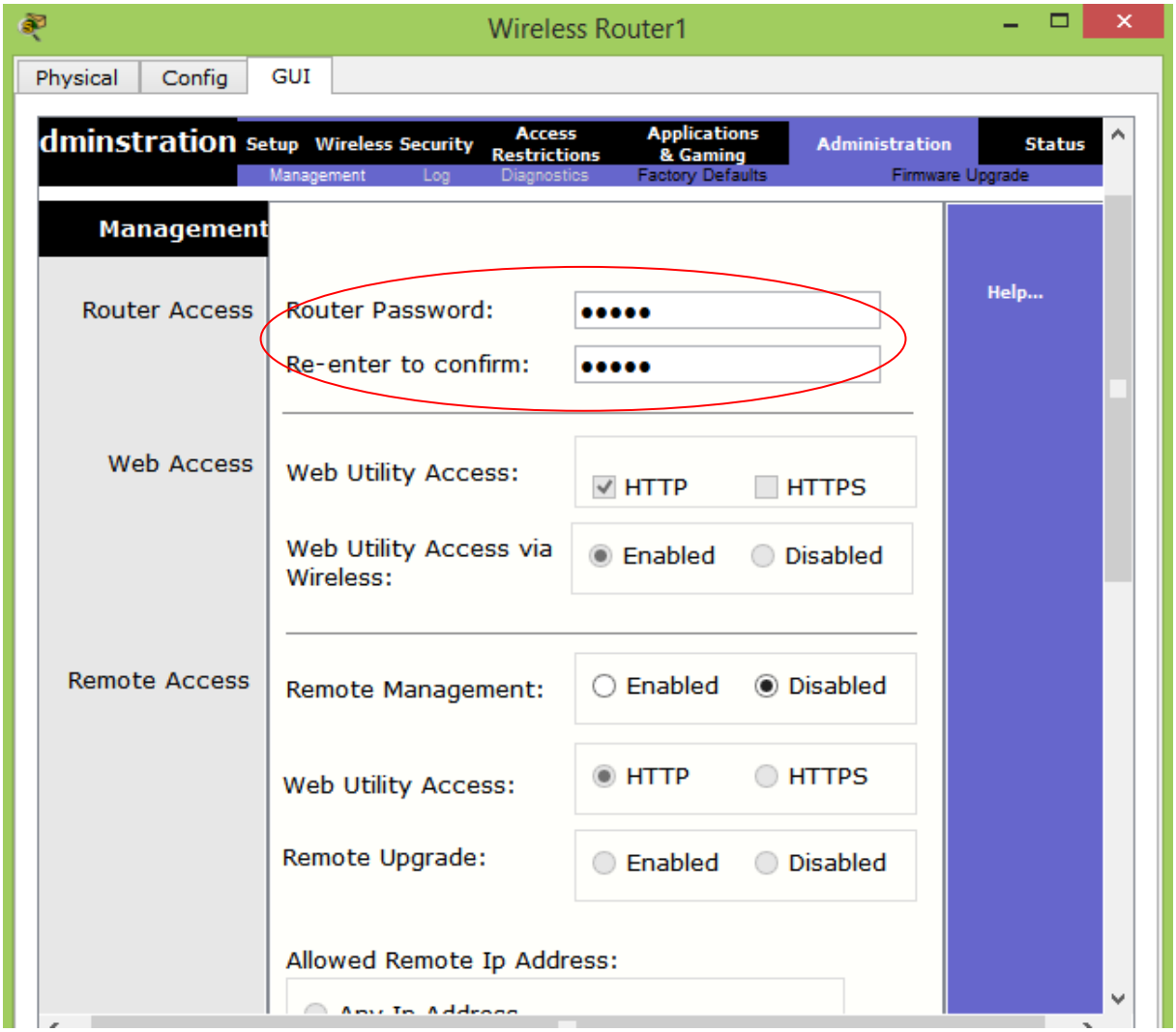

Figure 3.11 : Interface de configuration des droits d'accès du routeur

2.4 Configuration des Vlan

Le réseau est séparé en cinq Vlans comme illustré dans le tableau ci-dessous:

Vlan	Adresse IP	Passerelle
Vlan employé	192.168.3.0/24	10.0.0.1
Vlan employé-wifi	192.168.6.0/24	10.0.0.1
Vlan direction	192.168.4.0/24	10.0.0.1
Vlan direction-wifi	192.168.7.0/24	10.0.0.1
Vlan visiteur	192.168.7.0/24	10.0.0.1

Tableau 3. 1 : Configuration des Vlans du réseau

2.5 Configuration des équipements

Les adresses IP des équipements sont configurées par le serveur DHCP. Les utilisateurs s'authentifient par le login et le mot de passe entrés dans le serveur radius. (Figure 3.13)

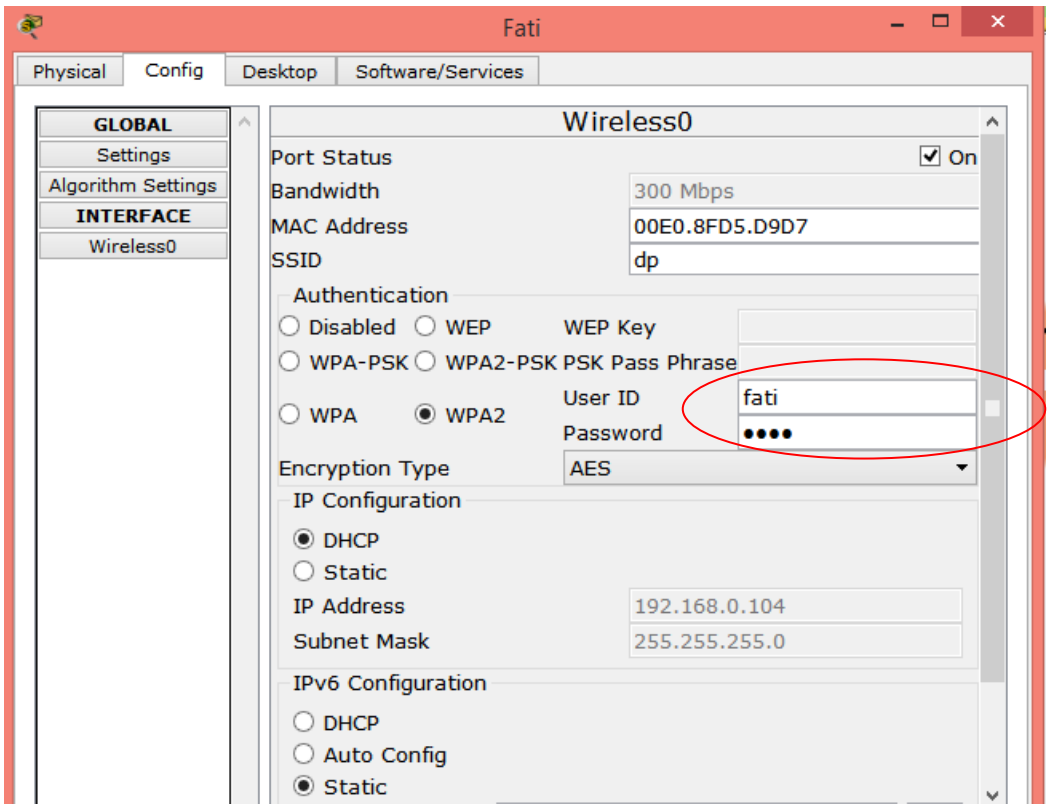

Figure 3.12 : Interface de configuration des adresses IP des équipements

Le serveur Radius vérifie les identifiants des utilisateurs puis il leurs donne ou non l'accès au réseau sans fil de l'entreprise. Dans l'interface ci-dessous l'utilisateur est connecté. (Figure 3.14)

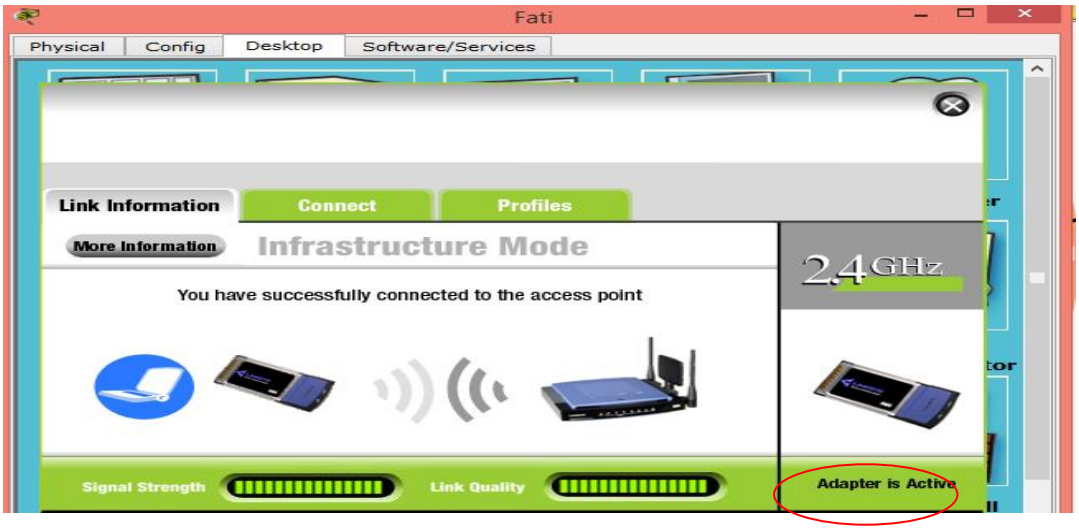

Figure 3.13 : interface d'établissement de la connexion Wifi

Interprétation : l'utilisateur autorisé sur le serveur Radius est connecté.

2.6 Test de sécurité :

Dans cette partie on va voir le cas d'un utilisateur non autorisé, qui veut se connecter au réseau sans fil.

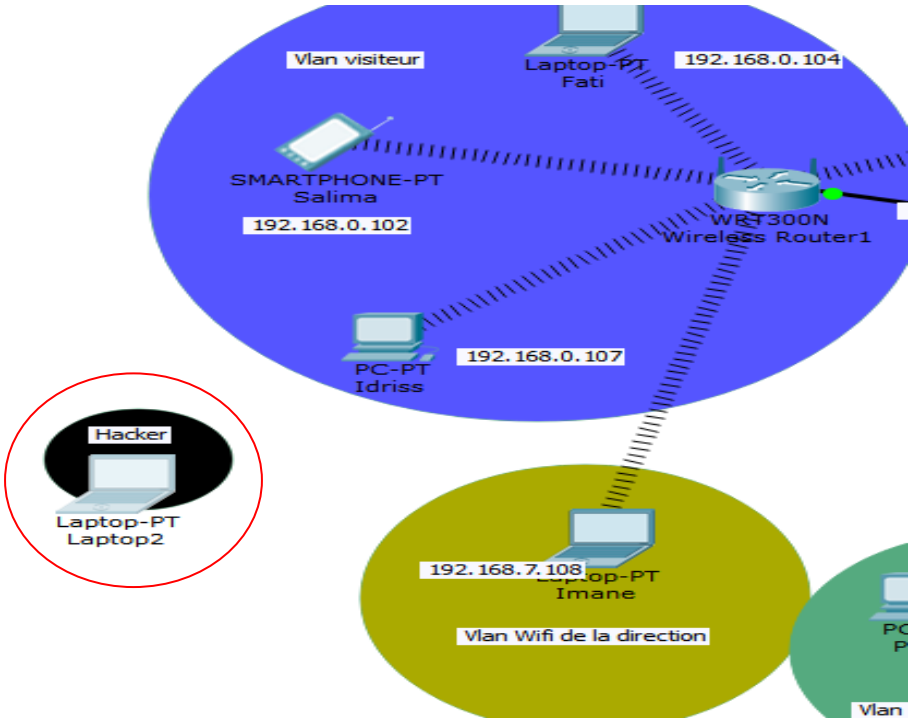

Figure 3.14 : utilisateurs non identifiés sur le réseau

Figure 3.15 : Interface de rejet des utilisateurs non autorisés

Interprétation : l'utilisateur ne peut pas accéder au réseau sans fil parce qu'il n'existe pas dans la base de données du serveur Radius.

Conclusion : On remarque donc que malgré les faiblesses existantes des protocoles de sécurités (WPA, WPA2) le serveur Radius et l'isolation des équipements, ajoutent une protection supplémentaire aux données circulantes sur le réseau.

CONCLUSION

On a présenté dans ce rapport le projet de fin d'études effectué au sein de DATAPROTECT. Ce travail consiste à l'élaboration d'un document pour la mise en place d'une infrastructure Wifi sécurisée. Les objectifs fonctionnels de ce projet devraient permettre de : avoir une connexion haut débit, protéger les données de l'entreprise, journalisation des accès, limitation d'accès au réseau sans fil par des identifiants.

Durant le projet, on a fait une étude sur les normes supportant le Wifi, les paramétrages et les règles de sécurité à utiliser pour sécuriser le réseau sans fil. Le but de cette étude est de proposer une architecture sécurisée destinée aux clients de Dataprotect qui veulent déployer le Wifi tout en assurant la sécurité de leurs données.

L'architecture adopte des protocoles de sécurité qui permettent de garantir un niveau de fiabilité. Ce document intègre les équipements à introduire et les configurations à choisir afin d'assurer la souplesse et la sécurité aux utilisateurs pendant la connexion au réseau sans fil.

Notre solution a satisfait les objectifs fonctionnels ainsi que techniques attendus vu la sécurité et la qualité de service qu'elle permet aux propriétaires de l'entreprise, par l'isolation des réseaux et les méthodes et protocoles d'authentification utilisés ainsi que le débit qu'elle procure à ses clients.

Étant donné la période limitée du stage ainsi que l'étendu de ce sujet, notre travail nous a permis d'établir le fonctionnement de l'architecture sécurisée et la mise en place des paramétrages associés, en attendant la disponibilité des équipements pour accomplir ce projet et avoir un document plus crédible.

BIBLIOGRAPHIE ET WEBOGRAPHIE

Ouvrage numérique :

[1] : La Sécurité des Réseaux Wi-Fi,Aspects Cryptographiques],[Julien Cathalo],[2012]

[2] : [Solution d'authentification sécurisée pour le futur réseau sans fil de l'Université LouisPasteur], [Christophe Saillard]

[3] : [Recommandations de sécurité relatives aux réseaux WiFi],[ANSSI],[2013]

[4] : [Technologies de l'information — Techniques de sécurité — Code de bonne pratique pour le management de la sécurité de l'information], [NM ISO/IEC 27002] ,[2013]

[5] : [Normes en matière de sécurité des données], [Payment Card Industry (PCI)], [2006]

[6] : [Guidelines for Securing Wireless Local Area Networks], [NIST Computer Security Division], [2012]

Site web :

[7] : http://portail-des-pme.fr/internet-referencement/1717-le-role-des-technologies-dans-lentreprise

[8] : https://fr.wikipedia.org/wiki/Wi-Fi

[9] : http://www.commentcamarche.net/contents/91-radius

[10] : http://www.panoptinet.com/cybersecurite-pratique/securite-wi-fi-les-recommandations-de-lanssi/

[11] : http://www.iso.org/iso/fr/catalogue_detail?csnumber=54533

[12] : http://www.bee-ware.net/fr/solutions/conformit%C3%A9-pci-dss

[13] : https://fr.wikipedia.org/wiki/National_Institute_of_Standards_and_Technology

[14] : http://www.fortinet.com/products/fortiap/indoor-ap.html

[15] : https://meraki.cisco.com/

[16] : http://www.arubanetworks.com/products/networking/access-points/

[17] : http://fr.ruckuswireless.com/products

[18] : http://www.aerohive.com/80211ac

[19] : http://www.memoefix.com/?p=260

ANNEXE : **Glossaire des principaux sigles et acronymes utilisés**

Terme	Définition
Adresse MAC (@ Media Access Control)	L'adresse MAC est un identifiant physique unique pour toutes les cartes réseau dans le monde. Elle est inscrite en usine de manière définitive dans la ROM.
AES (Advanced Encryption Standard)	un mécanisme de chiffrement qui est plus fort que TKIP et qui est utilisé par WPA2
AP (Access point)	Un point d'accès permet de relier sans fil des stations clientes Wifi et de se connecter en 2,4 GHz ou en 5 GHz à un réseau haut débit.
Attaque MiM (Attaque man in the middle)	une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis
BSSID (Basic Service Set Identifier)	Identificateur unique à chaque client sans fil d'un réseau sans fil. Le BSSID est l'adresse MAC Ethernet de chaque carte du réseau.
CERTIFICAT	Il permet d'associer une clé publique à une entité pour empêcher qu'un pirate la clé publique originale.
CLOUD	Un modèle qui permet un accès omniprésent, pratique et à la demande à un réseau partagé et à un ensemble de ressources informatiques configurables (par exemple : des réseaux, des serveurs, du stockage, des applications et des services) qui peuvent être provisionnées et libérées avec un minimum d'administration.
DHCP (Dynamic Host Configuration Protocol)	Un protocole réseau chargé de la configuration automatique des adresses IP d'un réseau informatique.
DNS	Le DNS est un protocole qui permet d'associer un nom de domaine à une adresse IP
FIREWALL (pare-feu)	Il a pour but de vérifier tous les ports ouverts et de bloquer toute émission ou réception de données par ceux-ci sans l'autorisation de l'utilisateur.

IEEE (Institute of Electrical and Electronics Engineers)	Une organisation qui a pour but de promouvoir la connaissance dans le domaine de l'ingénierie électrique.
LAN (Local Area Network)	Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation, et reliés entre eux dans une petite aire géographique par un réseau, souvent à l'aide d'une même technologie
LDAP (Lightweight Directory Access Protocol)	Le Protocole d'accès aux annuaires léger est un protocole standard permettant de gérer des annuaires, c'est-à-dire d'accéder à des bases d'informations sur les utilisateurs d'un réseau par l'intermédiaire de protocoles TCP/IP.
MIMO (Multiple Inputs Multiple Outputs)	Une Technologie permettant d'accélérer le débit et d'élargir la portée d'un réseau Wifi, en employant plusieurs antennes radio pour l'émission et la réception (Entrée multiple sortie multiple).
NAC (Network Access Control)	il permet de soumettre l'accès au réseau d'entreprise à un protocole d'identification de l'utilisateur et au respect des restrictions d'usages définies pour ce réseau.
POE (Power over Ethernet)	Technologie permettant à un câble réseau Ethernet de fournir des données et l'alimentation électrique.
RADIUS (Remote Authentication Dial-In User Service)	Un protocole d'authentification standard
"Rogue" AP:	Un point d'accès non autorisé sur un réseau. Son but est de contourner les vérifications de sécurité pour accéder à un réseau interne.
SSID (Service Set Identifier)	Nom de réseau sans fil
TKIP (Temporal Key Integrity Protocol)	Une clé de 128 bits est utilisée pour chaque paquet. On génère une nouvelle clé pour chaque paquet. TKIP est utilisé par WPA.
VLAN (Virtual Locan Area Network)	Réseau virtuel au sein d'un réseau global permettant d'isoler certaines machines entre elles du réseau global.
VPN (Virtual Private Network)	La mise en place d'un réseau privé virtuel permet de connecter de façon sécurisée des ordinateurs distants au travers d'une liaison non fiable (Internet), comme s'ils étaient sur le même réseau local.

WEP (Wired Equivalent Privacy)	Méthode de chiffrement utilisée pour les liaisons d'un réseau local sans fil 802.11. Ce protocole de sécurisation n'est pas fiable.
WIFI (Wireless Fidelity)	Une technologie permettant de créer des réseaux informatiques sans fil. Il s'agit d'une norme de l'IEEE baptisée 802.11.
WIPS (wireless intrusion prevention system)	Système de prévention des intrusions sans fil
WLAN (wireless Local Area Network)	Réseau local sans fil
WPA (Wi-Fi Protected Access)	Une norme de protection des données, amenée à remplacer la clef WEP.