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

Mémoire de fin de cycle

En vue d'obtention du diplôme de Master en Informatique.
Spécialité : Adminstration et Sécurité des Réseaux.

Thème

Mise en place d'un réseau Wi-Fi avec authentification basée sur des certificats PEAP/TLS

Réalisé par :

Mlle. TIGUERT Melissa et Mlle. SAADI Fatima .

Evalué le 02/07/2023 devant le jury composé de :

Le(a) président(e)	**Dr. KHALED Hayette**	**U. A/Mira Béjaïa.**
Examinateur 1	**Dr.BOUADEM Nassima**	**U. A/Mira Béjaïa.**
Encadrant	**Dr.GHANEM Souhila**	**U. A/Mira Béjaïa.**

Année universitaire 2022/2023

Remerciements

À travers ce modeste travail, nous tenons à remercier notre encadrant pour ses conseils, son orientation et son aide tout au long de notre projet de fin d'étude.

Nos remerciements s'adressent également au président et aux membres du jury pour avoir accepté d'examiner et d'évaluer notre travail.

Nous tenons également à exprimer notre gratitude envers le Dr TOUAZI Djoudi et monsieur DJEBBARI YASSINE pour avoir fourni le matériel nécessaire à la réalisation de notre travail, ainsi qu'à tous ceux qui ont réalisé de près ou de loin à sa réalisation.

Nous remercions également le personnel de l'entreprise SONATRCK pour leur accueil lors de notre stage pratique.

Et enfin, que nos chers parents et familles, trouvent ici l'expression de nos remerciements les plus sincères et les plus profonds en reconnaissance de leurs sacrifices, aides, soutien et encouragement afin de nous assurer cette formation dans les meilleures conditions.

Table des matières

Table des figures

Liste des tableaux

Liste des abréviations

AP	Access Point
BSS	Basic Set Service
CHAP	Challenge Handshake Authentication Protocol)
CCMP	Counter Mode with CBC MAC Protocol
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DNS	Domain Name System
DCF	Domain Name System
DIFS	DCF IF
DSSS	Direct-sequence spread spectrum
EAP	Extensible Authentication Protocol
FTP	File Transfer Protocol
FHSS	Frequency Hopping Spread Spectrum
IP	Internet Protocol
IR	infrarouge
ISO	International Organization for Standardization
IFS	Inter-Frame Space
LAN	Local Area Network
LEAP	Lightweight EAP
MAC	Media Access Control
NAV	Network Allocation Vector
OSI	Open Systems Interconnection
OFDM	Orthogonal frequency-division multiplexing
PLCP	Physical Layer Convergence Protocol
PMD	Physical Medium Dependent
PAP	Password Authentication Protocol
PEAP	Protected Extensible Authentication Protocol
PIFS	PCF IFS
PPP	The Point-to-Point Protocol
RTC	Request to Send
RTP	Real-time Transport Protocol
SIFS	Short IFS
TLS	Transport Layer Security
TTL	Time To Live
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VTP	VLAN Trunking Protocol
VCS	Virtual Carrier Sense
WRAP	Wireless Robust Authenticated Protocol
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPAN	Wireless Personnel Area Network
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network)
WWAN	Wireless Wide Area Network)

Introduction générale

Dans le monde interconnecté d'aujourd'hui, le besoin d'une communication sans fil transparente et sécurisée est devenu de plus en plus vital. L'avènement des réseaux sans fil a révolutionné la façon dont nous accédons et partageons les informations, offrant flexibilité, mobilité et commodité dans divers environnements. Un aspect important des réseaux sans fil est la mise en œuvre de mécanismes d'authentification robustes pour garantir un accès sécurisé à ces réseaux.

Au niveau des réseaux locaux, de nombreuses technologies ont émergé, offrant toujours de nouvelles fonctionnalités et une meilleure qualité de service. Parmi elles, la norme IEEE 802.11, plus connue sous le nom de Wi-Fi, s'impose comme une référence et a été largement adoptée par les fabricants de matériel informatique.

Cependant, malgré les apparences, cette technologie n'est pas sans failles. La nature des signaux électromagnétiques rend difficile, voire impossible, le contrôle de leur propagation. Par conséquent, un réseau Wi-Fi mal sécurisé peut être facilement intercepté ou même altéré, exposant les informations échangées. Face à ces risques, les entreprises ont initialement été réticentes à adopter ces technologies au sein de leurs locaux. Face à ce genre de risques, les entreprises étaient, dans un premier temps, très réticentes à l'adoption de ce genre de technologies au sein de leurs locaux.

Heureusement, l'évolution du Wi-Fi ne s'est pas limitée aux critères de débit et de portée du signal. Ces dernières années, des efforts considérables ont été déployés pour sécuriser ces réseaux, chaque nouvelle norme apportant des améliorations visant à garantir la confidentialité et l'intégrité des données.

Aujourd'hui, chaque entreprise dispose d'un réseau informatique qui permet une optimisa-

tion des ressources (temps, budget, etc.) et offre une plus grande facilité aux employés dans l'exécution de leurs tâches quotidiennes.

Dans la plupart des organisations informatisées, la possibilité de partager des données directement entre machines est une préoccupation majeure. Il est donc essentiel de renforcer les mesures de sécurité afin de préserver la confidentialité, l'intégrité et le contrôle d'accès au réseau, ainsi que les risques d'attaques. Pour ce faire, il est crucial de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information.

Après une analyse approfondie des caractéristiques et des besoins de l'entreprise SONATRACH de Béjaïa, nous avons constaté que leur réseau sans fil n'est pas déployé en raison de problèmes de sécurité. Notre objectif principal est donc de concevoir une architecture sans fil sécurisé basée sur la norme 802.11 et de proposer une solution d'authentification utilisant des certificats PEAP/TLS. Cette solution permettra de renforcer la sécurité et de compléter leur réseau existant, en traitant les différentes vulnérabilités qui y sont présentes.

Afin de réaliser cet objectif, nous avons retenu plusieurs solutions d'authentification parmi lesquelles nous avons choisi le protocole 802.1x. Son objectif principal est de permettre l'accès physique à un réseau local après une phase d'authentification. Ce protocole utilise l'encapsulation PEAP (Protected Extensible Authentication Protocol) pour établir une connexion entre le serveur d'authentification RADIUS (Remote Access Dial In User Services) et le système à authentifier.

Notre mémoire est organisé en quatre chapitres comme suit :
Le premier chapitre s'intitule "Généralités sur les réseaux sans fil et le standard 802.11". Il va traiter des réseaux sans fil en général, les différentes catégories existantes, ainsi que leurs avantages et inconvénients

Le second chapitre nommé "Organisme d'accueil" aura pour but de mieux comprendre l'entreprise ou nous avons effectué notre stage, sa structure hiérarchique, son réseau informatique ainsi que les différentes technologies utilisées. Nous évoquerons les différentes problématiques posée de son réseau

Dans le troisième chapitre, nous nous consacrons à une analyse approfondie de la solution proposée et à sa mise en œuvre concrète. Cette solution repose sur l'utilisation du protocole 802.1x en conjonction avec un serveur d'authentification RADIUS qui utilise des certificats PEAP/TLS pour assurer la sécurité du réseau de SONATRACH de Bejaia. Ce chapitre met en évidence les différents moyens et outils qui ont été déployés pour la mise en place réussie de cette solution.

Le quatrième et dernier chapitre sera intitulé "Implimentation de la splution et configuration". Dans ce chapitre, nous nous concentrons sur la configuration et la mise en œuvre des différentes solutions retenues. Nous décrivons en détail les étapes et les processus impliqués dans la concrétisation de ces solutions.De plus, des tests ont été effectués pour garantir le bon fonctionnement de notre solution et vérifier son efficacité.

En conclusion, nous récapitulerons les principaux points forts de notre projet et aborderons quelques perspectives futures. Cette introduction générale met en évidence les réalisations et les résultats obtenus, tout en présentant les avantages et les bénéfices apportés par notre solution.

Chapitre 1

Reseaux sans fil et le standard IEEE 802.11

1.1 Introduction

Un réseau sans fil permet la communication entre deux patients ou plus sans avoir besoin de liaisons physiques. Ces réseaux permettent la possibilité aux utilisateurs de rester connectés tout en se déplaçant dans une zone de données géographiques, ce qui est souvent associé à la notion de mobilité. Les réseaux sans fil se caractérisent par leur déploiement rapide et facile, permettant non seulement la transmission de données, mais également d'autres applications telles que la voix, la vidéo et l'accès à Internet.
La norme IEEE 802.11, également connue sous le nom de Wi-Fi, est devenue la norme de facto pour les réseaux locaux sans fil. Elle offre des avantages tels que la portée, la connectivité simultan ee de plusieurs appareils et des vitesse de transfert de donn ees elevées. Cependant, pour garantir la sécurité et la fiabilité des réseaux sans fil, des régles et des normes strictes doivent etre mises en place. Ces régles concernent notamment l'identification et l'authentification des utilisateurs.

1.2 Définition des réseaux sans fil

Un réseau sans fils (en anglais wireless network), est un système de communication qui permet au moins deux terminaux de communiquer sans liaison filaire, en utilisant des ondes radio électriques ou infrarouges, plutot que des cables. Les réseaux sans fil permettent la possibilité de rester connecté tout en se déplacant dans une zone géographique plus ou moins etendue, ce qui est souvent appelé "mobilité". Ils permettent de relier facilement des équipements distants d'une dizaine de métres à quelques kilométres sans nécessiter de lourds aménagements d'infrastructures. Cependant, les réseaux sans fil sont réglementés et peuvent etre vulnérables aux attaques de pirates informatiques, nécessitant la mise en place de dispositions pour assurer la confidentialité des données circulant sur le réseau[1].

1.3 Classification des réseaux sans fil

Les réseaux sans fil sont classifiés selon leur étendue et domaine d'application en quatre (4) catégories :

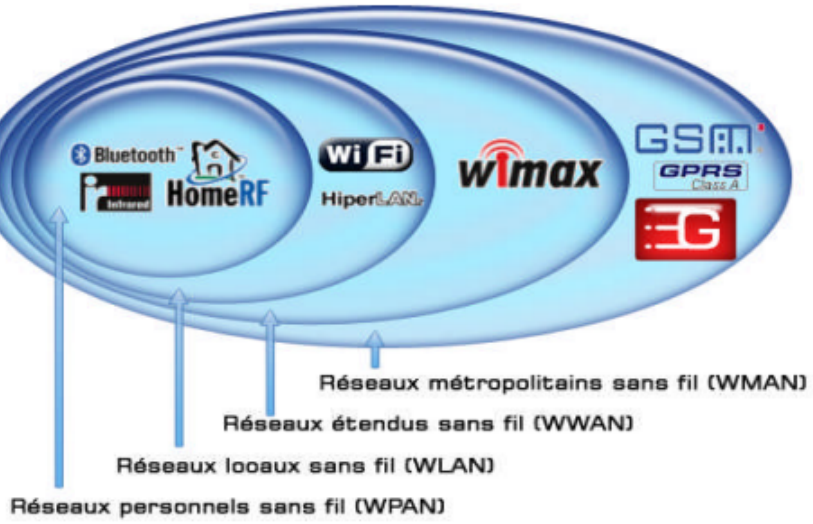

FIGURE 1.1 – classification des réseaux sans fi

1 **Les réseaux personnels sans fil (WPAN, Wireless Personnel Area Network) :** Concernent les réseaux sans fil d'une faible portée de l'ordre de quelques dizaines de mètres. Ce type de réseau sert généralement à relier des périphériques (imprimante, téléphone portable, ...) sans liaison filaire ou bien à permettre la liaison sans fil entre deux machines très peu distantes. Parmi les technologies de WPAN on trouve : Le Bluetooth, UWB (Ultra-Wide Band) et le ZigBee.

2 **Les réseaux locaux sans fil (WLAN, Wireless Local Area Network) :** Prolongent ou remplacent un réseau local traditionnel. Ces réseaux autorisent des débits dans les versions courantes qui peuvent aller jusqu'à 6 Gbit/s. Le wifi est considéré comme la principale technologie de communication connue dans les réseaux locaux sans fil.

3 **Les réseaux métropolitains sans fil (WMAN, Wireless Metropolitan Area Network) :** Il s'agit d'un réseau sans fil qui a une zone de couverture pouvant aller jusqu'à 50 km (une ville), le WiMax (worldwide Interopability for Microwave Access) s'agit d'un exemple de

technologie de communication de WMAN.

4 **Les réseaux étendus sans fil (WWAN, Wireless Wide Area Network) :** Est la catégorie des réseaux cellulaires mobiles dont la zone de couverture est très large (échelles mondiale). Pour cette catégorie,nous pouvons citer le réseau GSM et ces extensions (GPRS (General Radio Service), EDGE (Enhenced Data Rates for Gsm), l'UMTS (Univesal Mobile Telecommunication System), 3ème génération (3G).

1.4 Mode de communication

a) Mode ad hoc : La norme 802.11 définit une première architecture qui permet la communication en mode ad hoc ou sans infrastructure. Dans ce mode, les stations clientes sans fil peuvent établir une communication directe les unes avec les autres, formant ainsi un réseau point à point sans nécessiter un point d'accès central. Chaque station a la capacité de recevoir et d'émettre des données.

Ce regroupement de différentes stations est appelé un ensemble de services de base indépendants (Independent Basic Service Set ou IBSS). Dans ce mode, les stations clientes sont autonomes et peuvent se connecter ou se déconnecter du réseau ad hoc en fonction de leur proximité les unes avec les autres. Cela permet une grande flexibilité du réseau, mais peut également entraîner une fiabilité moindre en raison de la mobilité des stations clientes[2].

b) Mode infrastructure : C'est un mode de communication sans fil dans lequel les stations de type client se connectent à un point d'accès (AP) via une liaison sans fil. Le point d'accès est un composant d'infrastructure qui permet la communication entre les stations et d'autres réseaux. Les ensembles formés par le point d'accès et les stations placés dans sa zone de couverture sont appelés Basic Service Area (BSA) et constituant un Basic Service Set (BSS). Dans ce mode de communication, les stations peuvent se déplacer et sortir de la zone de couverture de leur BSA, ce qui peut affecter la qualité de la communication. Pour cela, plusieurs points d'accès peuvent être déployés pour l'ancien ensemble de services étendu (ESS) qui couvre naturellement un éspace appelé zone de service étendue (ESA), composé de plusieurs cellules [3] [4] .

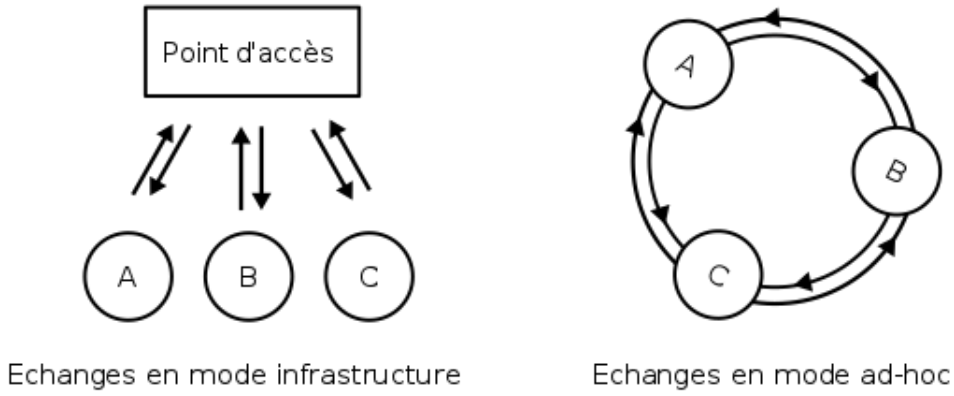

FIGURE 1.2 – Les deux modes de commnications

1.5 Types de liaison

Dans les réseaux sans fil, les informations sont transmises par liaison infrarouge ou par onde radioélectrique (onde radio ou onde hertzienne) remplaçant ainsi les câbles traditionnels utilisés dans les réseaux câblés[5].

1. **Liaison de type onde radio :** On appelle liaison radio toute interconnexion entre des dispositifs de télécomm-unication réalisée par ondes électromagnétiques. Les liaisons radio permettent la transmision des informations entre différents points ou zones dans

lesquels il n'est généralement pas possible de réaliser une infrastructure avec câble en cuivre ni fibre optique[6]. donc la liaion de type onde radio est caractérisé par :

- Les ondes radio sont émises d'une manière omnidirectionnelle.
- Possibilité de connecter plusieurs appareils entre eux, en même temps.
- Les ondes hertziennes sont difficiles à confiner dans un espace restreint ce qui les rend idéales pour les communications longues distances (plusieurs Km).
- Un mode de communication modèle pour les liaisons avec les objets mobiles,piétons, automobiles, bateaux, trains, avions, fusées, satellites.
- Les perturbations extérieures peuvent affecter la communication par l'utilisation de la même fréquence par exemple[6].

2. **Liaison de type infrarouge :** Les infrarouges correspondent à des rayonnements dont la longueur d'onde est comprise entre 800 nm et 1 mm, mais la spectroscopie IR ne fait en général appel qu'à ceux compris approximativement entre 2,5 m et 25 m ce qui correspond à un intervalle de nombre d'onde compris entre 400 et 4000 cm-1, appelés infrarouge.[6] donc la liaion de type infrarouge est caractérisé par :
   - Possibilité de mettre en place des réseaux sans fil de quelques dizaines de mètres.
   - Des débits de quelques mégabits par seconde.
   - Visibilité des appareils, aucun obstacle ne doit cacher l'émetteur du récepteur car la transmission est unidirectionnelle.
   - Utilisation d'onde lumineuse pour la transmission de données car la nature non dissipative de ces ondes permet un degré de sécurité plus élevé.
   - Exemple d'utilisation : Télécommande de télévision, de jouet, de voiture..., etc [7].

1.6 les composants de l'infrastructure

a) Le controleur :

Un contrôleur Wi-Fi est un dispositif matériel ou logiciel qui gère et contrôle les points d'accès Wi-Fi dans un réseau. Le contrôleur Wi-Fi fournit un point central de gestion pour les

réseaux sans fil, permettant à l'administrateur réseau de configurer, surveiller et gérer les points d'accès sans fil à partir d'un emplacement central. Le contrôleur Wi-Fi est responsable de la gestion du trafic sans fil, de l'allocation de la bande passante, de la mise en place des politiques de sécurité, du provisionnement des points d'accès et de la gestion des mises à jour logicielles. Il offre également une vue d'ensemble du réseau Wi-Fi et fournit des statistiques sur les performances du réseau sans fil.

b) Le point d'acces :

est un dispositif qui permet de créer un réseau local sans fil .un point d'accès se connecte à un routeur filaire, commutateur par un câble Ethernet et donne un signal wifi à une zone dédié [3].

c) Interface client (Carte reseaux sans fil) :

permet de se connecter à internet et au réseau local, et il est obligatoire pour connecté un ordinateur à un réseau sans fil [3]. L'interface client, également connue sous le nom de carte réseau sans fil (WNIC), est un composant matériel qui se trouve sur un ordinateur ou un périphérique réseau et qui permet à l'utilisateur de se connecter à un réseau sans fil. L'interface client se connecte au point d'accès sans fil (AP) pour établir une liaison sans fil. Elle est responsable de la transmission et de la réception de données sur le réseau sans fil. L'interface client utilise des protocoles de communication sans fil, tels que le Wi-Fi, pour communiquer avec le point d'accès sans fil. l'interface client (carte réseau sans fil) est un composant clé pour établir une connexion sans fil entre un ordinateur ou un périphérique réseau et un réseau sans fil.

1.7 La technologie Wi-Fi

Comme il a été précisé plus haut dans le rapport,nous désignerons les normes de type IEEE 802.11.

1.7.1 Qu'est-ce que le Wi-Fi ?

Le Wi-Fi est un ensemble de fréquences radio qui élimine les câbles, partage une connexion Internet et permet l'échange de données entre plusieurs postes[8]. La norme internationale IEEE 802.11 définit les caractéristiques d'un réseau local sans fil. À l'origine, le terme Wi-Fi faisait référence à la certification délivrée par la Wi-Fi Alliance, anciennement connue sous le nom de WECA. La mission de la WECA était de garantir l'interopérabilité des produits Wi-Fi (IEEE 802.11) et de promouvoir cette norme comme standard pour les réseaux locaux sans fil dans tous les secteurs du marché.

Le Wi-Fi, ou la norme de réseau 802.11, est un réseau local sans fil proposé par l'organisme de normalisation américain IEEE. Il correspond aux caractéristiques décrites par la norme IEEE 802.11 et permet aux utilisateurs de se connecter à Internet sans avoir besoin de câbles, grâce à la transmission d'ondes radioélectriques.

Grâce au Wi-Fi, il est possible de créer des réseaux locaux sans fil à haut débit, à condition que l'appareil à connecter ne soit pas trop éloigné du point d'accès. En pratique, le Wi-Fi permet de connecter des ordinateurs portables, des ordinateurs de bureau, des tablettes, des smartphones, des imprimantes et divers périphériques à une connexion haut débit sur une distance allant de quelques dizaines de mètres en intérieur (environ 20 à 50 mètres) à plusieurs centaines de mètres en extérieur.

La technologie 802.11 est souvent considérée comme l'équivalent sans fil de la norme 802.3 (Ethernet). De nos jours, le terme IEEE 802.11 est couramment utilisé pour désigner la première norme du Wi-Fi, également connu sous le nom de 802.11 legacy.

L'avantage principal de la connexion Wi-Fi est sa compatibilité avec presque tous les systèmes d'exploitation, les dispositifs de jeu et les imprimantes avancées, ce qui en fait une solution largement adoptée[8].

1.7.2 Les dérivés de la norme IEEE 802.11

IEEE 802.11a : en 1999,la norme 802.11a propose 8 canaux dans la bande de 5 GHz au lieu de 2,4 GHz, modulation radio de type OFDM, débit maximal théorique de 54 Mb/s sur une portée d'environ 20m. La norme IEEE-802.11a possède un avantage dans la mesure ou elle subit moins d'interférence. Cependant, cette fréquence élevée pénètre plus difficilement les murs et réduit la zone de couverture des appareils [9]. Elle permet d'obtenir un débit théorique de 54 Mbps, soit cinq fois plus que le 802.11b, pour une portée d'environ une trentaine de métres seulement. Cette couche physique, compliquée, est basée sur plusieurs techniques de transmission numérique, comme la transmission par multi-porteuse OFDM (Orthogonal Frequency Division Multiplexing) [10].

IEEE 802.11b : Les réseaux locaux sans fil (ou Wi-Fi) IEEE 802.11b connaissent une augmentation remarquable de leur utilisation. L'une des principales raisons du succés du Wi-Fi a été la réduction des couts d'équipement, la simplicité de configuration et les débits de données élevés (jusqu'à 11 Mb/s). Alors que les appareils 802.11b fonctionnent dans les bandes ISM 2,4 GHz [18]. propose une amélioration de la norme initiale en introduisant la modulation CCK pour atteindre ce qu'on appelle le DSSS à haute vitesse ou HR DSSS dans la bande des 2,4 GHz. Deux nouveaux débits sont alors disponibles : 5,5 Mbits/s et 11 Mbits/s sur une portée de quelques dizaines de mètres environ. Ratifiée en septembre 1999, 802.11b est l'amendement de 802.11 qui a donné sa popularité au Wifi. Bien que 802.11b soit encore largement utilisé.

IEEE 802.11g (Wi-Fi 3) : apparue en 2003, constitue une amélioration directe de 802.11b en proposant un débit bande de base de 54 Mbits/s sur la bande des 2,4 GHz. Ce gain en débit est réalisé en reprenant le concept de l'étalement de spectre par OFDM utilisé dans 802.11a. Toutefois, 802.11g garde une compatibilité avec 802.11b, ce qui signifie que des matériels conformes à la norme 802.11g peuvent fonctionner en 802.11b [9].

IEEE 802.11n (Wi-Fi 4) : propose un débit bande de base de 540 Mbits/s sur une portéé de 50 métres environ, grâce à l'utilisation conjointe des techniques MIMO et OFDM. Elle

propose l'utilisation des deux bandes de fréquences 2, 4 GHz (comme 802.11b et 802.11g) et 5 GHz (comme 802.11a). Comme 802.11g, cette norme reste compatible avec 802.11, de plus, elle reprend les concepts de 802.11e pour la gestion de la Qualité de Service, de 802.11i pour la sécurité et de 802.11f pour la gestion des handovers. Cette norme a été ratifiée le 11 septembre 2009 [11].

IEEE 802.11ac (Wi-Fi 5) : appelé également Wi-Fi 5,Cette norme utilise la technologie sans fil à double bande, prenant en charge les connexions simultanées sur les bandes Wi-Fi de 2,4 GHz et 5 GHz. La norme 802.11ac offre une compatibilité ascendante avec la norme 802.11b / g / n et une bande passante allant jusqu'à 1 300 Mbits / s sur la bande 5 GHz, ainsi que jusqu'à 450 Mbits / s sur 2,4 GHz. La plupart des routeurs sans fil à domicile sont conformes à cette norme [12]. les améliorations du Wi-Fi 802.11ac ne concernent que la bande des 5 GHz. Elles se décomposent pour le moment en deux vagues : la première – Wave 1 – a été officialisée en 2013, mais des produits étaient déjà disponibles depuis au moins un an dans le commerce [13].

1.7.3 l'achitecture du IEEE 802.11

La norme 802.11, également connue sous le nom de Wi-Fi, est une norme pour les réseaux sans fil. Elle définit les protocoles de communication pour les réseaux sans fil et comprend plusieurs couches d'architecture. Voici les principales couches d'architecture de 802.11 :

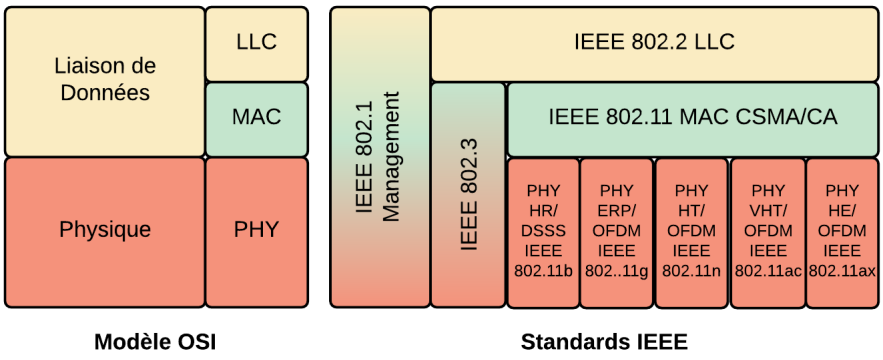

FIGURE 1.3 – Couche Accès IEEE 802.11

— **Couche physique (PHY) :**La couche physique définit les spécifications pour la transmission des données sur le support physique, tel que les ondes radio. Cette couche spécifie les fréquences, les canaux, les débits de données, les modulations, les puissances de transmission et les méthodes de codage pour la transmission des données.

— **Couche de liaison de données (DLL) :** La couche de liaison de données fournit un mécanisme pour transférer des données sur le support physique. Elle divise les données en paquets et ajoute des en-têtes et des pieds de paquets pour fournir un mécanisme de contrôle de l'erreur et de gestion du flux.

— **Couche de contrôle d'accès au support (MAC) :** La couche MAC gère l'accès au support physique pour les stations sans fil et les points d'accès. Elle utilise le protocole CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) pour éviter les collisions de paquets lors de l'accès simultané au support physique.

— **Couche de sécurité :** La couche de sécurité fournit des protocoles pour protéger les transmissions sans fil contre les accès non autorisés. Les protocoles de sécurité les plus courants sont le WEP, le WPA et le WPA2.

1.7.3.1 Couche Physique du standard 802.11

La couche physique définit la modulation des ondes radioélectriques et les caractéristiques de la signalisation pour la transmission de données, elle propose plusieurs types de codage de l'information : DSSS, FHSS, IR, OFDM, toutes ces technologies permettent des débits de 1Mbps et 2Mbps.

— **Spectre étalé a séquence directe (DSSS) :** C'est une méthode de modulation de signale, qui permet un étalement de spectre en séquence directe[33].Fonctionnant dans la bande ISM 2,4 GHz, à des débits de données de 1 Mbps et 2 Mbps. Aux Etats-Unis, la FCC (Federal Communications Commission) n'exige aucune licence pour l'utilisation de cette bande. Le nombre du canaux disponibles dépend de la bande passante allouée par divers organismes nationaux de règlementation[5].

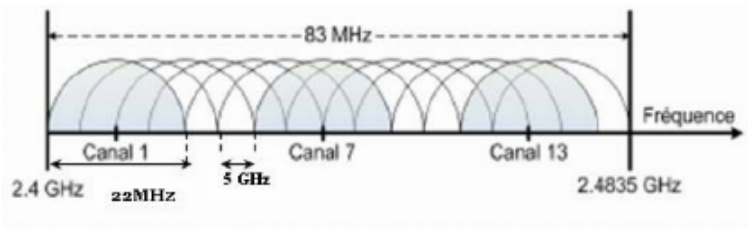

FIGURE 1.4 – Répatitions des 14 cnaux de la technologie DSSS [5]

— **Spectre étalé à sauts de fréquence (FHSS) :** Fonctionnant dans 2,4 GHz dans la bande ISM, à des débits de 1 Mbps et 2 Mbps. Le nombre de chaines disponibles va de 23 au Japon à 70 aux Etats-Unis[4].

— **multiplexage par répartition orthogonale de la fréquence (OFDM) :**Le principe de cette technique consiste à diviser le signal que l'on veut transmettre sur différentes bandes porteuses, comme si l'on combinait ce signal sur un grand nombre d'émetteurs indépendants, fonctionnant sur des fréquences différentes. Un canal est constitué de 52 porteuses de 300 KHz de largeur, 48 porteuses sont dédiées au transport de l'information utile et 4 pour la correction d'erreurs appelées porteuses pilote, Huit canaux de 20 MHz sont définis dans la bande de 5 GHz [14].

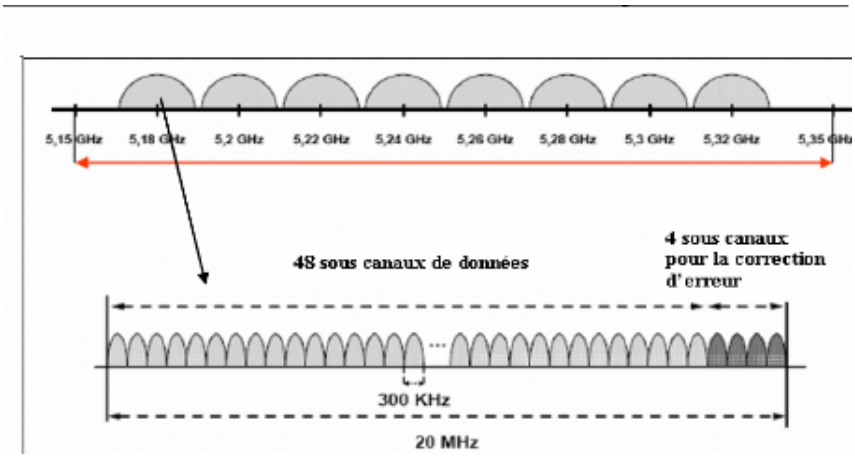

FIGURE 1.5 – Canaux OFDM dans la bande de 5 GHz[14]

1.7.3.2 sous couche physique

La couche Physique définit la modulation des ondes radioélectrique et les caractéristiques de la signalisation pour la transmission de données. Elle est subdivisée en deux sous couches :

La couche PLCP (Physical Layer Convergence Protocol) : Qui s'occupe de l'écoute du support physique et indique à la couche MAC pour la transmission radio si le support est occupé ou non via un signal appelé CCA (Clear Channel Assessement)[15].

La couche PMD (Physical Medium Dependent) : Qui gère la modulation et l'encodage des données à transmettre sur le support[15].

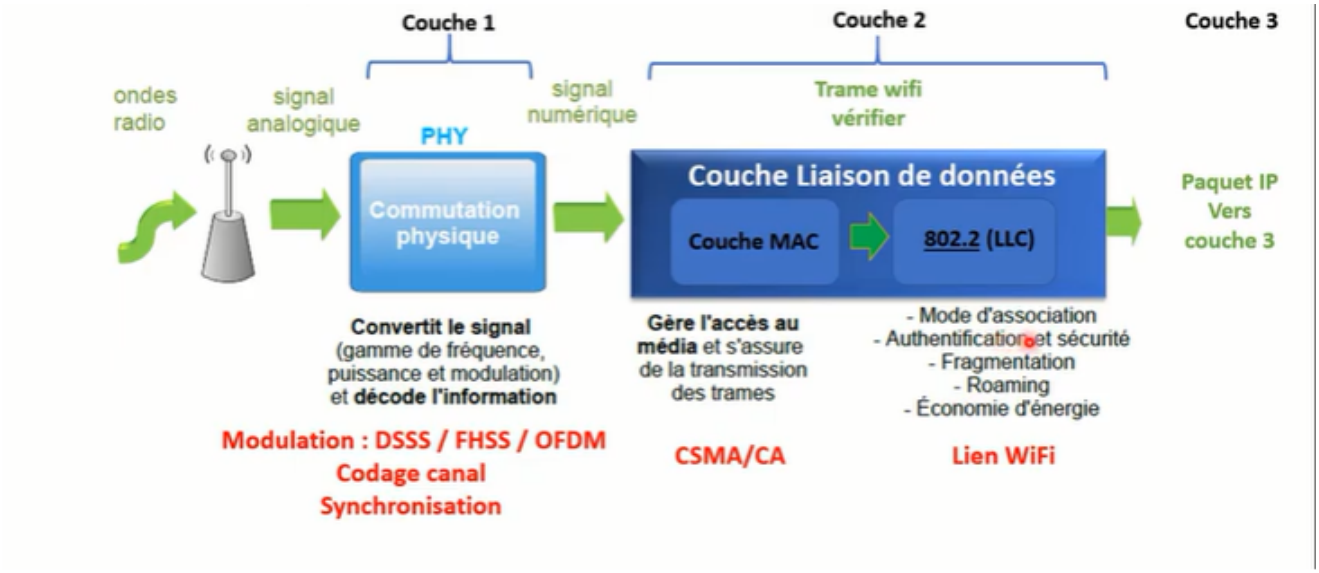

FIGURE 1.6 – Le principe des couches du IEEE 802.11

1.7.4 Les techniques d'accès au support radio

La technique DCF pour l 'accès au support de transmission constitue la technique d'accès par défaut. Elle permet la transmission de données en mode asynchrone et best-effort, sans aucune exigence de priorité. La technique DCF s'appuie sur le protocole CSMA/CA , qui est la variante sans fil du traditionnel CSMA/CD du monde Ethernet. Dans ce qui suit, nous donnons les caractéristiques principales du protocole CSMA/CA, ainsi que le mécanisme

de réservation du support hertzien.

1.7.4.1 La méthode d'accès (CSMA/CA)

Dans un réseau local Ethernet classique, on utilise le CSMA/CD. Chaque machine envoyant un message vérifie qu'aucun autre message n'a été envoyé en même temps par une autre machine sur le canal de transmission. Si en effet il y a des informations qui transite sur le canal, les deux machines patientent un temps aléatoire avant de retenter l'émission [16].
La première caractéristique de la couche MAC de 802.11 est donc d'utiliser des acquittements pour détecter ces collisions et permettre la retransmission des paquets qui ont été perdus et en l'absence d'acquittement, l'émetteur sait qu'il doit retransmettre [17]. écouter avant d'émettre .

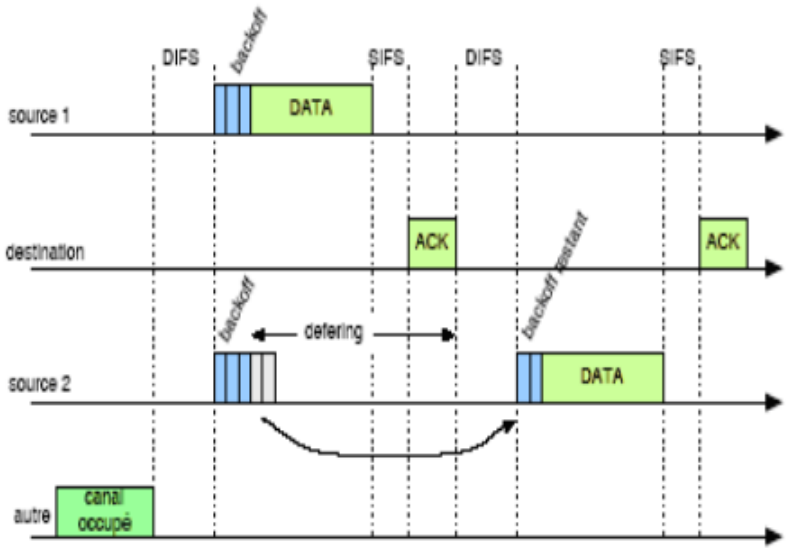

FIGURE 1.7 – Carrier Sense Multiple Access/Collision Avoidance

- Si le canal libre : transmettre la trame
- Si le canal occupé : différer la transmission.
- CSMA/CA : est une méthode qui permet de réduire le nombre de conflits
- CSMA/CA retardent l'émission lorsque le canal est détecté occupé.
- Les stations attendent un temps aléatoire après une collision avant d'écouter une autre

fois sur le canal [18].

Le protocole CSMA/CA doit donc éviter les collisions, à défaut de pouvoir les détecter. CSMA/CA se base principalement sur les espaces inter trames ou encore IFS pour l'évitement de collisions ; ces IFS sont les intervalles de temps séparant la transmission de trames consécutives et qui correspondent à des périodes d'inactivité sur le support de transmission. Le standard défini trois types d'IFS différents [19] :

1 SIFS (Short IFS) : SIFS est utilisé pour séparer les transmissions de trames consécutives au sein d' une même transmission (envoi de données, ACK, etc.). Durant cet intervalle, il n'y a qu'une seule station pouvant transmettre.

2 PIFS (PCF IFS) : PIFS est utilisé par le point d'accès pour accéder avec priorité au support.

3 DIFS (DCF IFS) : DIFS est utilisé lorsqu'une station veut commencer une nouvelle transmission, ainsi, lors de l'envoi d'une trame par la station source, les autres stations entendent cette transmission et pour éviter une collision, il incrémente la valeur d'un compteur, appelé NAV (Network Allocation Vector), qui sert à retarder toutes les transmissions prévues de toutes les stations. La valeur d'incrémentation du NAV est calculée par rapport au champ durée de vie, ou TIL, contenu dans les trames qui passent sur le support. Ensuite, le compteur NAV est décrémenté jusqu'à atteindre la valeur 0, instant signalant à la station l'autorisation de transmettre ses données, après un intervalle DIFS [20].

a) Variantes de CSMA/CA :

Il existe deux variantes de CSMA/CA :

1 CSMA/CA persistante :

- Tant que le canal est occupé continuer l'écoute.
- Dés que le canal est libre alors envoyer les données.

2 CSMA/CA non persistante :

- Une station peut ne pas rester tout le temps à l'écoute de la porteuse.
- Si le canal est occupé alors attendre une durée aléatoire avant d'écouter une autre fois[18] .

1.7.4.2 Mécanisme de réservation du support RTS/CTS

Les normalisateurs ont inclus dans le standard IEEE 802.11 un mécanisme permettant de réserver le support pour une transmission particulière. Ce mécanisme n'est pas actif par défaut dans le standard, mais il est activé optionnellement par la station souhaitant réserver le support exclusivement pour sa transmission. Ce mécanisme n'est autre que VCS localisé au niveau de la couche MAC. VCS se base sur l'émission de trames RTS/CTS entre une station source et une station destination, précédant toute transmission de données.

Ainsi, une station source voulant transmettre des données émet une trame RTS . Toutes les stations de la cellule BSS détectant le RTS lisent son champ TTL et mettent à jour leur valeur de NAV. La station destination ayant reçu le RTS réplique par un CTS, en temporisant sa transmission pendant un SIFS. Les autres stations détectent le CTS, lisent le champ TTL de celui-ci et mettent à nouveau à jour leur NAV [21] .

Après réception du CTS, la station source est assurée que le support est stable et réservé exclusivement pour sa transmission de données. De cette manière, la station source peut transmettre ses données ainsi que recevoir l' ACK sans collision. Ce mécanisme de réservation est surtout utilisé pour l'envoi de grosses trames pour lesquelles une retransmission serait trop coûteuse en bande passante [21]. afin de remédier aux problèmes du nœud caché

et/ou du nœud exposé 802.11 propose le mécanisme RTS/CTS donc :

— Un mobile qui veut émettre ne va plus directement envoyer son gros paquet de données, mais plutôt un petit paquet RTS pour lequel les chances de collision sont plus faibles.

— A ce paquet RTS, le destinataire va répondre par un petit paquet CTS qu'il diffuse à tout son voisinage.

— Au niveau des mobiles, la réservation du canal est implémentée grâce au Network Allocation Vector (NAV).

— Dans chaque nœud, le NAV indique pour combien de temps le canal est utilisé par un autre nœud.

— Les paquets RTS et CTS contiennent des informations qui permettent de réserver le canal pour la durée de transmission des données qui vont suivre.

— Un mobile qui reçoit un CTS alors qu'il n'a pas envoyé (ni même détecté de RTS) sait que quelqu'un d'autre va émettre et doit donc attendre.

— Le mobile qui a envoyé le RTS sait, quand il reçoit le CTS correspondant, que le canal a été réservé pour lui et qu'il peut émettre [22].

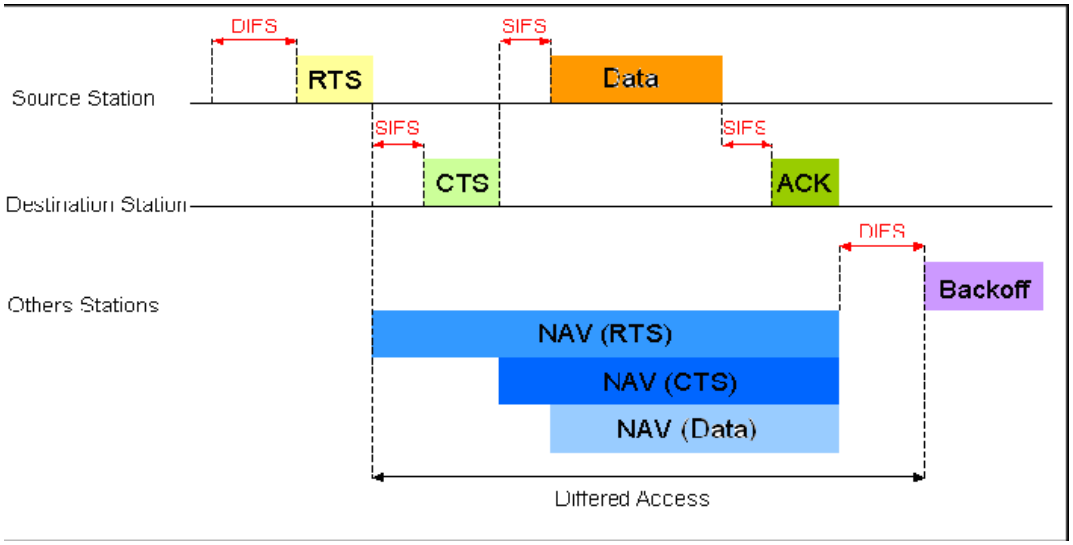

FIGURE 1.8 – Transmission avec le mécanisme de réservation (RTS/CTS) [22]

1.7.4.3 L'algorithme de Backoff

- Lorsque le canal devient libre, avant toute chose, il faut qu'il le reste pour une période DIFS.
- Si le canal est resté libre durant toute cette période, alors les mobiles qui veulent émettre choisissent un backoff aléatoire exprimé en un nombre de time slots d'une durée fixe de 20 micro secondes.
- Le backoff est choisi au hasard dans un intervalle appelé Contention Window (CW).
- Une fois ce tirage effectué, tant que le canal reste libre, les mobiles décrémentent leur backoff.
- Dès que l'un d'eux a terminé, il émet.
- L'autre mobile, dès qu'il détecte le regain d'activité sur le canal stope la décrémentation de son backoff et entre en période de defering.
- Il faut noter que le temps de pause qui sépare un paquet de données de son acquittement est appelé SIFS (Short Inter-Frame Space).
- le SIFS qu'il est plus court que DIFS[22].

1.7.5 Les bandes de fréquences et le debit

1.7.5.1 Les bandes de fréquences du standard IEEE 802.11

Les différents modules radios des standards IEEE 802.11a/b/g utilisent des fréquences situées dans des bandes dites sans licence. Ce sont des bandes à accès libre. La configuration de ces bandes dépend du milieu de l'application intérieur ou extérieur (indoor/outdoor). Les deux bandes sans licence utilisées par L'IEEE 802.11 sont :

- La bande ISM (Industrial, Scientific and Medical)
- La bande U-NII (Unlicenced-National Information Infrastructure)[16].

1.7.5.2 Le debit

C'est le nombre de bits qui transitent dans le canal de transmission chaque seconde et il dépend de la largeur de ce canal, on peut le calculer avec la formule suivante :

$$C = H \times \log_2(1 + \frac{Ps}{Pb})$$

C : la capacité maximale du canal de communication en bits par seconde.

H : est la largeur de la bande de fréquences utilisées, en hertz.

Log2 (Ps/Pb) = log(Ps/Pb) / log (2).

Ps : c'est la puissance du signal exprimée en Watt.

Pb : c'est la puissance du bruit exprimée aussi en Watt.

Le débit maximal des réseaux sans fil dépend de la largeur de bande de fréquences utilisées. Plus les fréquences sont élevées, plus il est possible d'exploiter des bandes de fréquences larges, ce qui permet d'atteindre un débit plus important. Cependant, dans le cas du Wi-Fi, les canaux de communication définis pour les fréquences de 2,4 GHz sur une largeur de 22 MHz, tandis que les canaux de 5 GHz sur une largeur de 20 MHz. Malgré cela, le débit maximal théorique est plus ou moins identique dans les deux cas, ce qui explique pourquoi le 802.11a et le 802.11g permettent à tous les deux le même débit maximal, même si le 802.11a utilise des fréquences plus élevées que le 802.11g . Cependant, dans la bande des 5 GHz, il y a plus de canaux pour communiquer qu'avec les 2,4 GHz. Pour obtenir un bon débit, il est également important d' avoir un bon rapport signal-bruit. Plus on s'éloigne de l'émetteur, plus le RSB diminue, ce qui entraîne une diminution du débit. Par exemple, avec un émetteur 802.11g à 15 dBm et un bon récepteur, on peut théoriquement obtenir un débit de 11 Mbps jusqu'à 100 mètres, mais au-delà, le débit tombera à 5,5 Mbps, puis à 2 Mbps et enfin à 1 Mbps jusqu'à plus de 300 mètres [23].

1.8 Avantages et inconvenients des réseaux sans-fil

L'utilisation des réseaux sans fil procure plusieurs avantages, notamment :

- La mobilité.
- L'usage facile dans les endroits à câblage difficile.
- La réduction du temps de déploiement et d'installation.
- L'augmentation de la connectivité (évolutivité) .

D'autres part les réseaux sans fil soufrent de problèmes tel que :

- La sécurité.
- Les interférences des ondes électromagnétiques.
- Débit et portée faibles.
- détection des collisions [24].

1.9 Conclusion

Dans ce chapitre, nous avons examiné en détail la norme 802.11, qui forme la base d'un réseau WiFi. Cette norme couvre les deux premières couches du modèle OSI : la couche physique et la couche liaison de données (MAC), qui joue un rôle crucial dans la définition de fonctionnalités avancées telles que la sécurité des communications, l'économie d'énergie, le contrôle d'erreur et la garantie d'une qualité de service optimale.
Bien que le WiFi utilise les ondes radio comme support de transmission, il offre plusieurs avantages par rapport aux réseaux locaux filaires, notamment la simplicité d'installation et la mobilité. Cependant, il est confronté à plusieurs problèmes de sécurité, qui seront évoqués dans les chapitres suivants. Dans le prochain chapitre, nous allons présenter l'organisme d'accueil.

Chapitre 2

Présentation de l’organisme d’accueil

2.1 Introduction

Dans ce chapitre, nous allons examiner l'étude de l'organisme d'accueil qui revêt une importance capitale puisqu'elle permet de cerner les contraintes et les enjeux inhérents à notre projet. Ainsi, nous allons présenter l'entreprise SONATRACH et les différents départements qui la composent, tout en fournissant des informations clés pour notre travail. Nous poserons également la problématique centrale autour de laquelle s'articulera notre mémoire.

2.2 Présentation général de l'organisme d'accueil

2.2.1 Présentation de SONATRACH

SONATRACH est un Groupe pétrolier et gazier intégré sur toute la chaine des hydrocarbures. Il détient en to- talité ou en majorité absolue, plus de vingt entreprises importantes sur tous les métiers connexes à l'industrie pétroliére tel que le forage, le raffinage... Il posséde aussi des participations significatives dans prés de 50 en- treprises implantées tant en Algérie qu'à l'étranger.

Le logo de l'entreprise est sur la FIGURE 2.1 :

FIGURE 2.1 – Logo de sonatrach

2.2.2 Historique ,Missions et activités de l'Entreprise

Sonatrach, avant d'avoir ce nom, était la société pétrolière de gérance (SOPEG) fondée le 12 mars 1956 par la compagnie française des pétroles Algérie (C F P A) et la société nationale de recherche et exploitation des pétroles en Algérie (S N R E P AL). Après l'indépendance, et grâce au décret n 36/491 de la nationalisation des hydrocarbures, la SOPEG est devenue sonatrach.

L'entreprise SONATRACH a été créé le 31 décembre 1963 par le décret n°63/491, les statuts ont été modifiés par le décret n°66/292 du 22 septembre 1966, et SONATRACH devient "Société nationale pour la recherche, la production, le transport, la transformation et la commercialisation des hydrocarbures», cela a conduit à une restructuration de l'entreprise dans le cadre d'un schéma directeur approuvé au début de l'année 1981 pour une meilleure efficacité organisationnelle et économique, de ces principes SONATRACH a donné naissance à 17 entreprises : (NAFTAL, ENIP, ENAC,..., etc.).

Les activités de base de SONATRACH furent fixées en 1992, afin d'atteindre ses objectifs en :

— L'exploitation et la recherche.

— L'exploitation des gisements d'hydrocarbures.

— La liquéfaction et la transformation du gaz.

— Le transport par canalisation.

— La commercialisation.

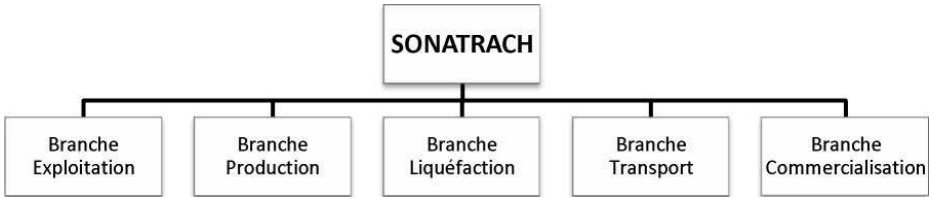

FIGURE 2.2 – Branches de Sonatrach.

2.2.3 Les directions régionales de transport de Sonatrach

La SONATRACH possède cinq directions régionales de transport des hydrocarbures :

— La direction régionale Est (Skikda),

— La direction régionale Centre (Béjaïa),

— La direction régionale Ouest (Arzew),

— La direction régionale de Haoud-EL-Hamra,

— La direction régionale d'Ain Amenas.

2.2.4 Présentation de la RTC (Région Transport Centre)

La direction régionale de transport de Béjaïa, est l'une des cinq directions régionales de transport des hydrocarbures de la SONATRACH (TRC). Elle a pour mission de transporter, stocker et livrer les hydrocarbures liquides et gazeux. Elle est chargée de l'exploitation de deux oléoducs, d'un gazoduc et d'un port pétrolier.

2.2.5 Activité de la branche transport par canalisation (TRC)

L'activité de transport par canalisation (TRC) est en charge de l'acheminement des hydrocarbures pétroles brut, gaz et condensat vers les ports pétroliers, les zones de stockages et les pays d'exploitation.

Les missions affectées à la branche transport par canalisation sont :

— La gestion et l'exploitation des ouvrages et canalisations de transport d'hydrocarbures ;

— La coordination et le contrôle de l'exécution des programmes de transport arrêtés en fonction des impératifs de production et de commercialisation ;

— La maintenance, l'entretien et la protection des ouvrages et canalisation ;

— L'exécution des révisions générales, des machines tournantes et équipements ;

— Les installations de pompage et de stockage pour répondre aux besoins de SONATRACH dans les meilleures conditions d'économie, de qualité, de sécurité et de respect de l'environnement ;

— Gère l'interface transport des projets internationaux du groupe ou en partenariat.

2.2.6 Structure de la RTC

La direction régionale de Béjaïa comporte plusieurs constituants illustrés dans l'organigramme ci-dessous :

FIGURE 2.3 – Organigramme général de Organisation de la direction régionale de Béjaïa

2.2.7 Description de chaque service

— **Direction régionale :** elle est dirigée par un directeur régional aidé par des assistants et un secrétariat.

— **Assistant de sécurité interne :** sa mission est de protéger et de sauvegarder le patrimoine humain et matériel de la DRGB.

— **Centre informatique :** il regroupe les moyens d'exploitation et de développement des applications informatiques pour l'ensemble des structures de la DRGB, ainsi que la gestion du réseau informatique interne.

— **Sous-direction technique :** elle a pour mission d'assurer la maintenance et la protection des ouvrages. Elle est organisée en quatre départements : département

maintenance, département protection des ouvrages, département approvisionnement et transport et département des travaux neufs.

— **Sous-direction exploitation :** elle est chargée de l'exploitation des installations de la région, et de maintenir le fonctionnement des trois ouvrages en effectuant des réparations en cas de fuite, de Sabotage ou de panne pour les stations de pompage. Elle est composée de deux départements : le département exploitation liquide et le département exploitation gaz

— **Sous direction Finances et juridique :** Elle a pour missions d'effectuer la gestion financière, le budget et le contrôle de gestion et de prendre en charge les affaires juridiques de la DRGB. Elle est organisée en trois départements : département finances, département juridique, département budget et contrôle de gestion.

— **Sous direction Administration :** Elle a pour mission la gestion des ressources humaines et les moyens généraux. Elle est organisée en trois départements : département administration et social, département ressources humaines et communication, département moyens généraux.

2.2.8 Présentation du centre informatique

Le centre informatique est chargé du développement et de l'exploitation des applications informatiques de gestion pour le compte de la direction régionale de Béjaïa (DRGB) et des autres régions.

2.2.8.1 Organigramme du centre informatique

L'organisation du centre ne cesse de subir des changements et l'évolution rapide de l'informatique pousse le centre à adopter des actions nouvelles à chaque fois afin de subvenir aux nouveaux besoins de l'entreprise.

Le centre informatique se constitue de 3 services gérés par un chef de centre. Ces derniers sont illustrés dans le diagramme suivant :

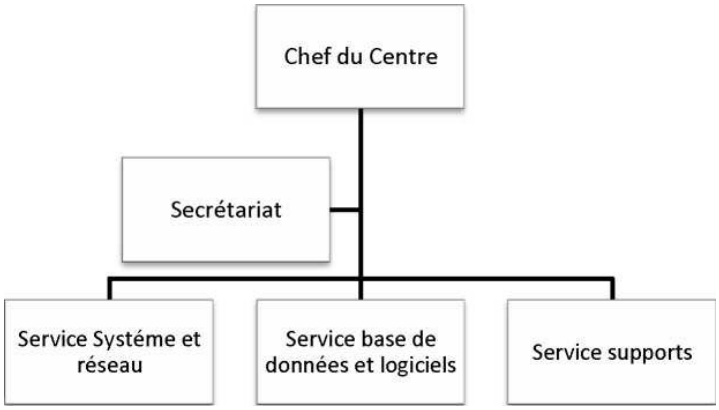

FIGURE 2.4 – Éléments de service technique

2.2.8.2 Rôle de chaque service

Chaque service a sa propre fonction, nous allons définir et citer les différentes tâches de chacun ci-dessous :

Service système et réseau : Ce service est divisé en deux sections :

A . **Service système et réseaux :**

Système :

• Choix des équipements informatique et logiciel de base.

• Mise en œuvre les solutions matériels et logiciels retenues.

• Installation et configuration des systèmes.

• Orientation des travaux de l'équipe de développement par une bonne utilisation des ressources de l'ordinateur.

• Mise en œuvre des nouvelles versions de logiciels.

Réseaux :

• Assurer le bon fonctionnement, la fiabilité des communications, l'administration du réseau et organiser l'évolution de sa structure.

• Conduite de l'étude pour le choix de l'architecture du réseau à installer.

• Participer à la mise en place des réseaux.

• Définir les droits d'accès à l'utilisation du réseau.

- Assurer la surveillance permanente pour détecter et prévenir les pannes.
- Traitement des dysfonctionnements et incidents survenant sur le réseau.

B . **Service base de données et logiciels :**

Base de données :

- Conçoit les bases de données et assure l'optimisation et le suivi de la gestion des données informatiques.
- Installe, configure et exploite le SGBD et ses bases.
- Met en ouvre et gère les procédures de sécurité (accès, intégrité).
- Gère la sauvegarde, la restauration et la migration des données.
- Assure la cohérence et la qualité des données introduites par les utilisateurs.

Logiciels :

- Etude et conception des systèmes d'information.
- Développement et maintenance de l'application informatique pour TRC.
- Déploiement des applications et formation des utilisateurs.

C . **Service supports :**

- Assistance aux utilisateurs en cas de problèmes software et hardware.
- Installation des logiciels, technique et bureautique.
- Formation aux nouveaux produits installés.

2.3 Etude des lieux (réseau de l'entreprise)

L'architecture physique du réseau LAN est structur ee suivant le modéle hiérarchique en 3 couches : une couche cœur (core layer), une couche distribution (distibution layer), et une couche d'accés (access layer).

2.3.1 Modéle Hierarchique

Le modéle hierarchique est composé de trois couches présentées ci-dessous :

— **La couche cœur de réseau (Core layer) :** est la couche superieure dont le rôle consiste à relier entre eux les différents segments d'un rérseau à savoir : les sites distants, les réseaux locaux (LANs) ou les étages de l'immeuble d'une société. Cette couche est aussi appelée Backbone [25].

— **La couche distribution (Distribution layer) :** Le rôle de cette couche a pour rôle de filtrer, de router, d'autoriser ou non les paquets. Cette couche se trouve entre la couche cœur et la couche d'accés c'est-à-dire entre la partie (liaison] et la partie (utilisateur). La segmentation du reseau commence ici en ajou-tant plusieurs switches de niveau 3 qui sont relies à la fois à la couche cœur et d'accées[25] .

— **La couche d'accés (Access layer) :** Cette couche qui est la dernire du modéle hierarchique permet de connecter les peripheriques des utilisateurs finaux au réseau. A ce niveau, on utilise des switches de niveau 2 car la configuration de ce type de switches pose moins de contraintes : le besoin en performance n'est plus vraiment une nécessité car chaque switch aura un nombre d'utilisateur egal à son nombre de ports (moins 1 ou 2 pour le trunk entre la couche d'Access et de Distribution). Les traitements restent basiques et ne demandent peu de ressources[25].

2.4 L'architecture réseau de l'entreprise

2.4.1 L'architecture physique du réseau

L'entreprise SONATRACH RTC de Béjaïa utilise principalement des équipements de marque CISCO. Ils sont réputés pour leurs fiabilités et leurs performances ainsi que la disponibilité de la main-d'œuvre qualifiée, ceci permet d'éviter des formations coûteuses pour l'entreprise. Ses équipements sont répartis sur les deux infrastructures.
Le LAN de la RTC se divise en effet en deux réseaux interconnectés :

— **Le réseau de l'ancien bâtiment :** il a une topologie hybride imposée par l'architecture de l'immeuble.

— **Le réseau du nouveau bâtiment :** il a une topologie en étoile.

Ancien bâtiment : La commutation est articulée autour de deux niveaux :

— Un niveau accès et distribution. À ce niveau-là, les équipements utilisés sont : des Switchs simples Catalyst 2950/2960 ainsi que des Switchs multicouches Catalyst 3550.

— Un niveau nommé Core (ou noyau), avec deux Switchs fédérateur multicouches Catalyst 6509 plus performants que les 3550, pour amortir la charge liée aux différentes sollicitations des serveurs (messagerie, antivirus, DHCP, DNS..., etc.).

La redondance est assurée grâce au protocole HSRP.

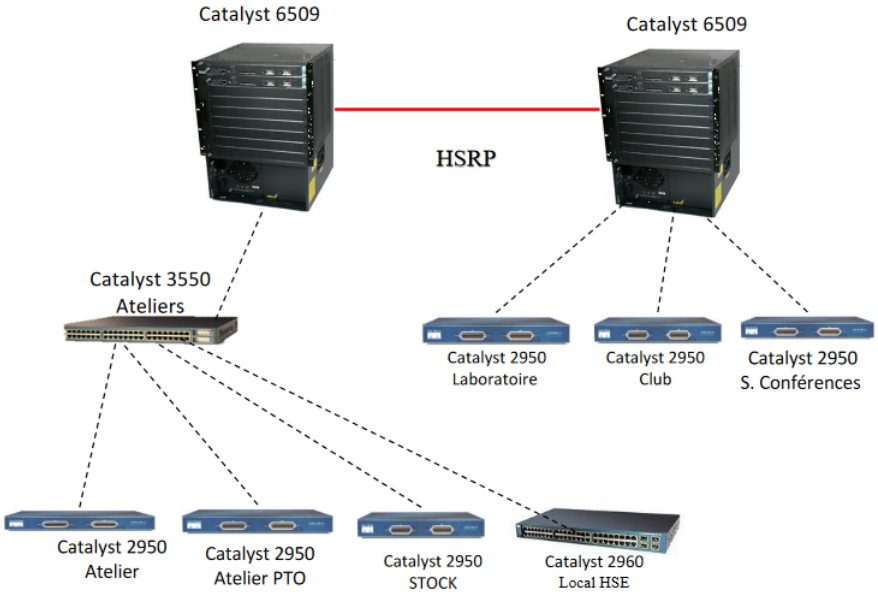

FIGURE 2.5 – La hiérarchie réseau de l'ancien bâtiment

Nouveau bâtiment : La commutation est articulée autour de deux niveaux :

— Un niveau accès et distribution. À ce niveau-là, les équipements utilisés sont des Switch multicouches 3750 (moins performants que les 6509).

— Un niveau Core, avec deux switchs fédérateurs multicouches Catalyst 6509.

Les deux switchs fédérateurs sont configurés pour une redondance par câble contrairement à ceux de l'ancien bâtiment.

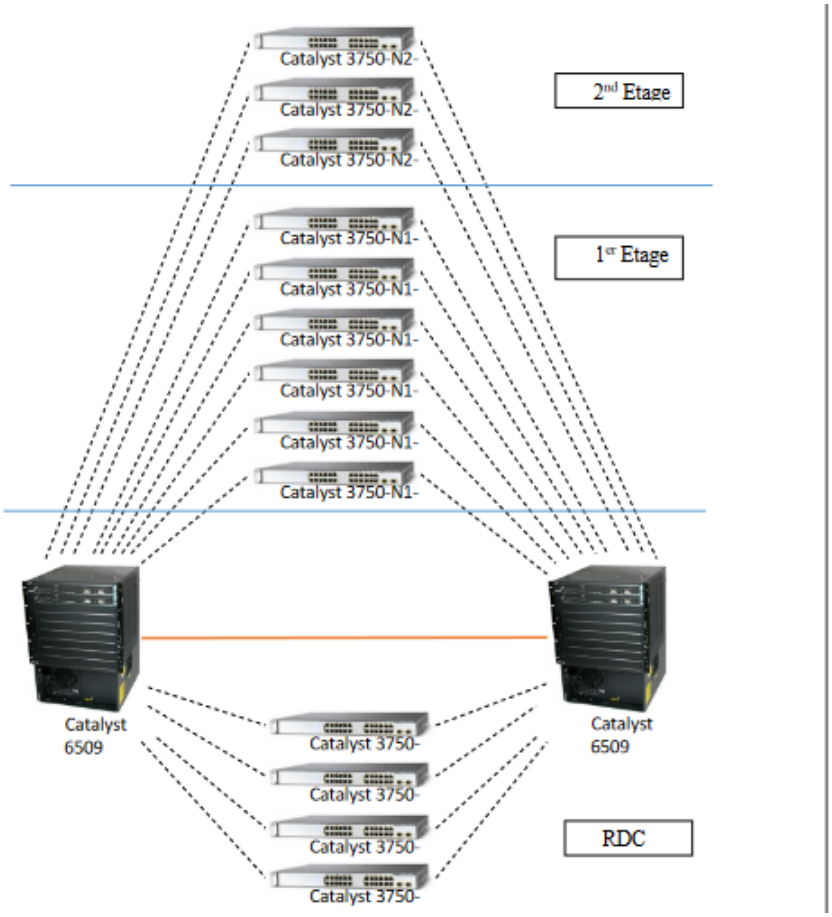

FIGURE 2.6 – La hiérarchie réseau du nouveau bâtiment

Les switchs fédérateurs de l'ancien et du nouveau bâtiment sont reliés entre eux via une fibre optique, pour former l'intranet de l'entreprise

2.5 La définition des équipements utilisés dans le réseau de la RTC

2.5.1 Commutateurs utilisés dans le réseau de la RTC

Le réseau de la RTC utilise les commutateurs suivant :

— **Catalyst Cisco 6509 :** La gamme Catalyst 6509 offre des moyens pour soutenir la capacité de la bande passante du syst'eme et des capacités amélior ees de gestion des

câbles. Elle fournit egalement des flux d'air d'avant en arriére qui est optimisé pour les conceptions allée chaude et froide dans le centre de données co-localisées et les déploiements de services. En outre elle offre une protection exceptionnelle des investissements en soutenant plusieurs générations de produits sur le même chassis, réduisant ainsi les coûts totaux de propriété. Le cadre Cisco Catalyst 6509 supporte à la fois la gamme Cisco Catalyst 6500 Supervisor Engine 32 et Cisco Catalyst 6500 Series Supervisor Engine 720 familles, avec LAN associés, WAN, et des modules de services [26].

FIGURE 2.7 – Commutateur Catalyst Cisco 6509

— **Catalyst Cisco 3750 :** La gamme Cisco Catalyst 3750 est une ligne de commutateurs innovants qui améliorent l'efficacité de l'exploitation des réseaux locaux grâce à leur simplicité d'utilisation et leur résilience la plus elevée disponibles pour des commutateurs empilables. Cette gamme de produits dispose de la technologie Cisco StackWiseTM, interconnectant les commutateurs au sein d'une même pile à 32 Gbps qui permet de construire un système unique de commutation à haute disponibilité, vu comme un simple commutateur virtuel [27].

FIGURE 2.8 – Commutateur Catalyst Cisco 3750

— **Catalyst Cisco 3550 :** Le commutateur Ethernet intelligent de la gamme Cisco Catalyst 3550 est une gamme de commutateurs multicouches empilables qui offrent une haute disponibilité, une qualit e de service (QoS) et une sécurité pour améliorer les op

erations r eseau. Avec une gamme de configurations Fast Ethernet et Gigabit Ethernet, la gamme Cisco Catalyst 3550 est une option puissante pour les applications d'accés d'entreprise et métropolitaine [28].

FIGURE 2.9 – Commutateur Catalyst Cisco 3550

— **Catalyst Cisco 2950 :** Série Catalyst 2950 commutateur Cisco configuration fixe, empilables, qui fournit à vitesse filaire Fast Ethernet et Gigabit Ethernet. Ce commutateur offre deux différents ensembles de fonctionnalités logicielles et une large gamme de configurations afin de permettre aux petites et moyennes entreprises et/ou les branches de l'entreprise dans des environnements industriels, pour obtenir la bonne combinaison pour l'environnement réseau[29].

FIGURE 2.10 – Commutateur Catalyst Cisco 2950

2.5.2 Les serveurs

— **Serveur de fichier :** Un serveur de fichiers permet de partager des données à travers un réseau. Le terme désigne souvent l'ordinateur (serveur) hébergeant le service applicatif. Il possède généralement une grande quantité d'espace disque où sont déposés des fichiers. Les utilisateurs peuvent ensuite les récupérer au moyen d'un protocole de partage de fichiers. On utilise généralement l'un des quatre protocoles suivant :

  - **FTP** (File Transfer Protocol)
  - **CIFS** (Common Internet File System) anciennement nommé SMB (Server Message Block)
  - **NFS** (Network File System)
  - **NCP** (Netware Core Protocol).

- **Serveur de bases de données :** Un serveur de base de données répond à des demandes de manipulation de données stockées dans une ou plusieurs bases de données. Il s'agit typiquement de demandes de recherche, de tri, d'ajout, de modification ou de suppression de données. Le serveur de base de données fait partie d'un système de gestion de base de données - logiciel qui manipule une base de données - qui comporte un logiciel client et un logiciel serveur. Les demandes de manipulation de données sont souvent créées par un logiciel de gestion sous forme de requêtes en langage SQL, puis le client les transmet au serveur en utilisant un protocole propre au SGBD.
- **Serveur LMS :** Serveur LAN Management Solution (LMS) offre un ensemble robuste d'applications dédiées à l'administration, la surveillance et le dépannage des environnements LAN commutés Cisco. Complément majeur des architectures matérielles de réseau Cisco AVVID (Architecture for Voice, Video and Integrated Data) ce produit a été conçu dans l'objectif de maximiser la disponibilité de service du réseau en four- nissant aux équipes techniques un puissant outil d'administration de bout en bout, capable de démultiplier l'efficacité de chaque action d'administration.

2.6 Problématique

Durant le stage effectué au niveau de département réseau et sécurité informatique de sonatrach, nous avons pu constater que le réseau de sonatrach possèdent de nombreux postes informatiques reliés entre eux par un réseau local filaire et sans fils. Ce réseau permet d'échanger des données entre les divers collaborateurs internes à l'entreprise et aussi de se connecter à l'internet. L'une des principales préoccupations liées aux réseaux sans fil est la question de la sécurité. Les entreprises craignent souvent que l'utilisation d'un réseau sans fil augmente les risques de piratage, d'accès non autorisé et de fuites de données sensibles. Par conséquent, elles peuvent hésiter à activer ou à réussir un réseau sans fil tant que des

mesures de sécurité adéquates ne sont pas en place. Afin de garantir un niveau élevé de sécurité, il est essentiel de mettre en œuvre des protocoles de chiffrement robustes, de limiter l'accès au réseau aux utilisateurs autorisés et de mettre en place des mécanismes de surveillance.

Outre les problèmes de sécurité, la gestion des utilisateurs constitue également un défi majeur dans les réseaux sans fil. La gestion des droits d'accès, des identifiants et des référentiels utilisateurs peut devenir complexe, en particulier lorsque l'entreprise dispose de multiples systèmes et applications. Une gestion d'accès inefficace peut entraîner des problèmes tels que des autorisations incorrectes, des non autorisées ou une difficulté à révoquer les droits d'accès en cas de départ d'un utilisateur. Il est donc crucial de mettre en place des solutions de gestion des utilisateurs centralisées et cohérentes, permettant un contrôle précis des droits d'accès et une administration simplifiée.

Parallèlement, les problèmes de configuration et d'authentification peuvent également se poser dans les réseaux sans fil. Une configuration incorrecte des points d'accès, des protocoles de sécurité ou des paramètres réseau peut entraîner des vulnérabilités et des dysfonctionnements. De plus, une authentification faible ou inefficace peut permettre à des utilisateurs non autorisés d'accéder au réseau ou de compromettre la sécurité des données échangées. Il est donc nécessaire de mettre en place des processus de configuration rigoureux, des mécanismes d'authentification solides et des protocoles de gestion des clés pour assurer l'intégrité et la confidentialité des communications dans le réseau sans fil. donc comment résoudre les problèmes de sécurité, de gestion des utilisateurs, de configuration et d'authentification dans un réseau sans fil ?

2.6.1 Solution

L'objectif principal de notre étude est de mettre en œuvre une solution d'administration et d'authentification pour améliorer la gestion et la sécurité de l'accès aux services réseau de Sonatrach. Nous avons choisi plusieurs solutions pour atteindre cet objectif, en collaboration avec Sonatrach qui nous a proposé cette démarche. Notre approche repose sur l'utilisation des contrôleurs d'accès sans fil (AC) pour centraliser et gérer les points d'accès du réseau sans fil, permettant ainsi une gestion simplifiée et efficace. Pour l'authentification et la gestion des autorisations d'accès, nous avons mis en place le protocole RADIUS,

qui centralise les informations d'identification des clients, facilitant ainsi leur gestion. De plus, nous avons intégré le protocole 802. 1x et la méthode PEAP-TLS pour sécuriser l'accès distant aux réseaux, en utilisant des certificats pour une authentification robuste et un transport sécurisé des données d'authentification. Pour renforcer la sécurité du réseau sans fil, nous avons opté pour le protocole WPA2, qui offre une protection avancée. Grâce à ces solutions, notre objectif est d'améliorer la gestion des utilisateurs, de renforcer la sécurité de l'accès aux services réseau et de fournir un environnement Wi-Fi sécurisé au sein de l'entreprise Sonatrach.

2.7 Conclusion

Dans ce chapitre, nous avons abordé brièvement le fonctionnement du réseau de la RTC de Béjaïa, Cependant, nous avons également identifié un problème qui a motivé notre recherche et notre mise en place d'une nouvelle conception de réseau sécurisé. Dans le prochain chapitre, nous nous concentrerons sur l'implémentation de la solution proposée et son application concrète.

Chapitre 3

La sécurité d’un réseaux wifi

3.1 Introduction

Un réseau sans fil non sécurisé peut être vulnérable à des attaques, permettant ainsi aux personnes non autorisées d'intercepter, de modifier ou d'accéder à des informations confidentielles.
Il est donc crucial de sécuriser les réseaux sans fil dès leur installation. Il existe différents niveaux de sécurité en fonction des objectifs et des ressources disponibles. Dans ce chapitre, nous examinerons les types d'attaques susceptibles de viser un réseau Wi-Fi, ainsi que les techniques de base intégrées dans la norme 802.11, telles que la délimitation des débordements, le filtrage par adresse MAC ,les Vlans et le WEP. Nous aborderons également les nouvelles solutions de sécurité, telles que le WPA et le WPA2, ainsi que des techniques plus avancées basées sur la norme IEEE 802.1x, qui permettent une authentification plus robuste à l'aide d'une encapsulation EAP.

3.2 La définition de la sécurité

La sécurité informatique comprend un ensemble de techniques et de technologies utilisées pour minimiser les risques de fuites d'informations, de modifications de données ou de détérioration des services dans un environnement informatique. Elle implique l'utilisation de diverses méthodes, technologies et architectures pour atteindre un niveau de protection optimal contre les menaces informatiques[30].

3.2.1 Les services de base de la sécurité

Classiquement la sécurité s'appuie sur cinq services de base : l'authentification, la confidentialité, l'intégrité des données, La disponibilité et la non-répudiation. Si chaque point est assuré, on peut dire que le système est sécurisé.

• **Authentification :** Cette opération consiste à faire la preuve de son identité. Par exemple

on peut utiliser un mot de passe, ou une méthode de défi basée sur une fonction cryptographique et un secret partagé[31].

• **Confidentialité :** C'est la garantie que les données échangées ne soient compréhensibles que pour les deux entités qui partagent un même secret. Cette propriété implique la mise en oeuvre de mécanismes et des méthodes de chiffrement [31].

• **Intégrité :**L'intégrité des données consiste à prouver que les données n'ont pas été altérées ou modifiées durant la communication, elles peuvent être copiées, mais aucun bit ne doit avoir été changé [31].

•**La disponibilité :** C'est un service qui permet de garantir ou assurer que l'information soit toujours accessible lorsque l'utilisateur autorisé en a besoin peu importe le moment choisi[32].

• **Non répudiation :** Les services de non-répudiation consistent à empêcher le démenti qu'un message a été reçu par une station qui l'a réclamé, ou empêcher le démenti par une station qui a émis un message de prétendre ne jamais l'avoir fait. La fonction de non-répudiation peut s'effectuer à l'aide d'une signature à clé privée ou publique ou par un tiers de confiance qui peut certifier que la communication a bien eu lieu [33] [34].

3.2.2 Les mécanismes cryptographiques

La cryptographie est l'étude des méthodes permettant de transmettre des données de manière confidentielle. Afin de protéger un message, on lui applique une transformation qui le rend incompréhensible ; c'est ce qu'on appelle le chiffrement, qui apartir d'un texte en clair, donne un texte chiffré ou cryptogramme. Inversement, le déchiffrement est l'action qui permet de reconstruire le texte en clair à partir de texte chiffré [35].

Chiffrement symétrique ou à clé secrète : Dans ce type de chiffrement, les clés de chiffrement et de déchiffrement sont identiques : c'est la clé secrète, qui doit être connue des tiers communicants et d'eux seuls. Ce procédé de chiffrement est dit symétrique [35] [36].
Les exemples d'algorithmes de chiffrement symétrique les plus couramment utilisés sont :

• AES (Advanced Encryption Standard) ,

• DES (Data Encryption Standard),

• RC4 (Rivest Cipher 4) .

Chiffrement asymétrique ou à clé publique : Avec ce système de chiffrement, les clés de chiffrement et de déchiffrement sont distinctes et ne peuvent pas se déduire l'une de l'autre, l'une est publique qui doit être connue de tous, c'est pourquoi on parle de chiffrement à clé publique. Pour envoyer un message confidentiel à un destinataire, l'émetteur le chiffre avec la clé publique du destinataire. A sa réception, ce dernier le déchiffrera avec sa clé privée qu'il est le seul à connaitre . Par ailleurs, le chiffrement asymétrique permet également de chiffrer en utilisant la clé secrète, cela permet donc la signature de messages[35][36].
Les exemples d'algorithmes de chiffrement asymétrique les plus couramment utilisés sont :

• RSA (Rivest-Shamir-Adleman) ,

• ECC (Elliptic Curve Cryptography) .

Signature numérique : La signature numérique, également connue sous le nom de signature électronique, est un processus permettant à un destinataire de vérifier l'origine et l'intégrité d'un message reçu. Cette technique garantit que seul l'expéditeur a la capacité de générer la signature, ce qui assure la non-répudiation du message signé. En d'autres termes, la signature numérique est une méthode de vérification de l'authenticité et de l'intégrité d'un message électronique, assurant ainsi que le destinataire peut avoir confiance dans le fait que le message a été envoyé par l'expéditeur prévu et qu'il n'a pas été modifié pendant la transmission [35][37].

Certificat numérique : Un certificat numérique, également connu sous le nom de certificat électronique, est un document électronique qui joue le rôle d'une carte d'identité numérique pour une entité spécifique. Il contient des informations importantes sur cette entité, telles que sa clé publique, et il est signé par une autorité de certification après vérification de l'exactitude des informations qu'il contient [35][36].

Fonction de hachage : Une fonction de hachage est une opération mathématique qui transforme un message long en une empreinte ou un résumé de taille fixe. Cette empreinte, éga-

lement appelée condensé ou haché, est générée de manière à ce qu'il soit extrêmement difficile, voire impossible en pratique, de trouver deux messages différents produisant le même haché. En d'autres termes, la fonction de hachage doit être résistante aux collisions.
De plus, une fonction de hachage doit être à sens unique, ce qui signifie qu'il est pratiquement impossible de reconstituer le message d'origine à partir de son haché. Cela garantit que l'empreinte ne peut pas être inversée pour obtenir le message original[37][38].

3.2.3 Les attaques d'un réseau Wi-Fi

Les réseaux Wi-Fi peuvent être attaqués de plusieurs façons, et à différents niveaux. Pour pouvoir faire face à ces attaques, nous devons préalablement les définir et connaître qu'elles sont les composantes matérielles et logicielles qu'elles visent.

3.2.3.1 Les attaques passives

Les attaques passives sont des attaques dans lesquelles un pirate écoute de manière non autorisée les transmissions sur le réseau sans modifier les données ni le fonctionnement du réseau. Bien que ces attaques soient souvent indétectables, elles peuvent être prévenues. La dangerosité de ces attaques réside dans le fait qu'elles permettent à l'attaquant de recueillir des informations sensibles sans être repéré, ce qui peut compromettre la sécurité du réseau.Parmi les principales attaques passives [39].

— **Le sniffing (espionnage)** : L'attaque la plus utilisée car cela consiste à écouter les transmissions des différents utilisateurs du réseau sans fil, et de récupérer n'importe qu'elles données transitant sur le réseau si celles-ci ne sont pas cryptées efficacement. Il s'agit d'une attaque sur la confidentialité. Il suffit pour cela de disposer d'un adaptateur Wi-Fi capable de lire toutes les trames qui circulent, et pas uniquement celles qui lui sont adressées (le mode monitor). Ensuite, il faut utiliser un logiciel d'analyse du réseau comme « wireshark » ou « Kismet » afin de capturer et afficher les paquets. L'espionnage conduit à la divulgation d'informations confidentielles (Mots de passe, documents secrets, numéros de cartes bancaires. . ., etc.) ou bien prépare une attaque active de plus

grande envergure. La Figure suivante illustre le schéma classique d'une attaque de type sniffing[40][41].

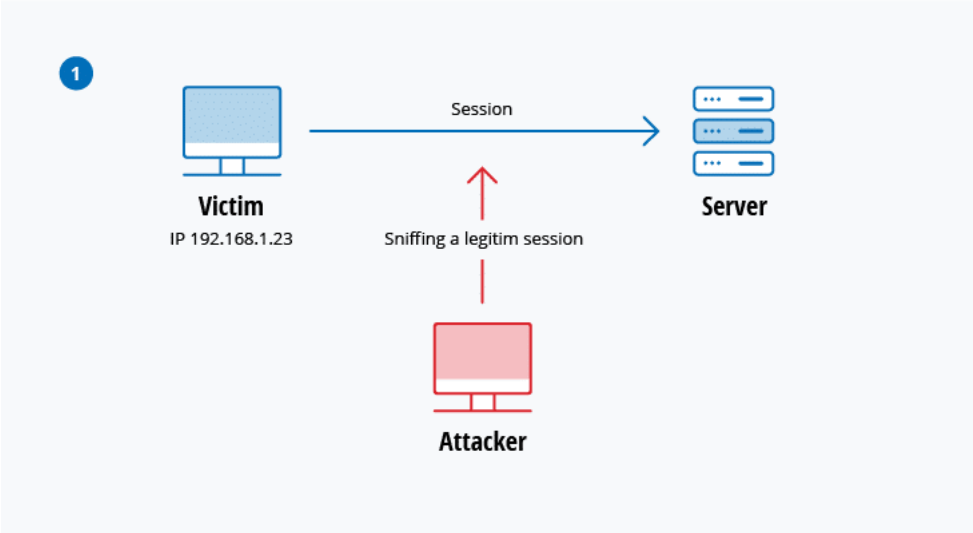

FIGURE 3.1 – L'attaque d'écoute passive sur un réseau sans fil non sécurisé.

3.2.3.2 Les attaques actives

Les attaques actives sont les attaques où le pirate modifie des données, s'introduit dans des équipements du réseau ou perturbe le bon fonctionnement de ce dernier. Elles se basent généralement sur des vulnérabilités aux niveaux physique et protocolaire. Parmi les principales attaques actives [39].

— **Spooffing (usurpation) :** Le spooffing consiste à usurper soit l'adresse MAC, soit l'adresse IP (après l'intrusion) d'une autre machine. En modifiant l'adresse source dans l'entête du paquet, le récepteur croira avoir reçu un paquet de cette machine. Si le serveur considérait cette machine comme une machine de confiance, beaucoup de données sensibles pourront être consultées, modifiées, voir même supprimées[40].

— **DOS (Déni de service) :** Une attaque par déni de service est une attaque informatique ayant pour but de rendre indisponible un service, et empêcher les utilisateurs légitimes d'un service de l'utiliser. Elle est souvent utilisée sur Internet afin de rendre inutilisable un site web, et peut parfois s'accompagner d'une demande de rançon pour cesser l'attaque. Sur les réseaux Wi-Fi, ce type d'attaque peut s'opérer de différentes manières au

niveau des couches 1 et 2 du modèle OSI. Le facteur commun étant leur efficacité et la facilité de leur mise en œuvre.

Attaque par brouillage radio sur la couche physique : Les ondes radio sont très sensibles aux interférences, la bande ISM 2,4 GHz implémentée dans la majorité des périphériques Wi-Fi a aussi d'autres usages (Four à micro-onde, Bluetooth…, etc.), ce qui peut occasionner des conflits accidentels tels que des déconnexions ou des baisses de débit. Cependant, un pirate peut exploiter cette faille afin de brouiller toutes les communications d'un réseau Wi-Fi en utilisant un puissant émetteur radio sur la fréquence de celui-ci. La dangerosité de cette attaque réside dans le fait qu'elle est quasiment imparable, bien qu'il existe des équipements radio qui permettent de localiser l'emplacement de l'émetteur du signal parasite .

Attaque de désauthentification au niveau de la couche MAC : Cette faille vient du fait que rien n'est prévu dans le standard 802.11 pour sécuriser les trames de management. Un pirate peut alors usurper l'identité d'un AP et utiliser des trames de désauthentification pour déconnecter un utilisateur précis du réseau, ou alors envoyer un flux continu de ces trames à toutes les stations connectées au point d'accès pour empêcher l'utilisation de ce dernier. Le but de cette attaque peut être la capture de mot de passe lors de la réauthentification, ou la redirection des clients vers un point d'accès pirate (Attaque evil twin, MitM…, etc.) [40][41].

— **Man in the middle (Homme au milieu) :** Le principe de cette attaque est d'intercepter les communications entre deux entités du réseau en se mettant au milieu. Dans les réseaux Wi-Fi, le pirate joue le rôle de relais entre la victime et le point d'accès légitime. Tout le trafic passe ainsi par sa machine avant d'être redirigé vers le réseau, ce qui lui laisse le loisir d'espionner les échanges ainsi que de pouvoir modifier le contenu de ces derniers (voir Figure 3-2 : L'attaque MitM sur Wi-Fi)[41].

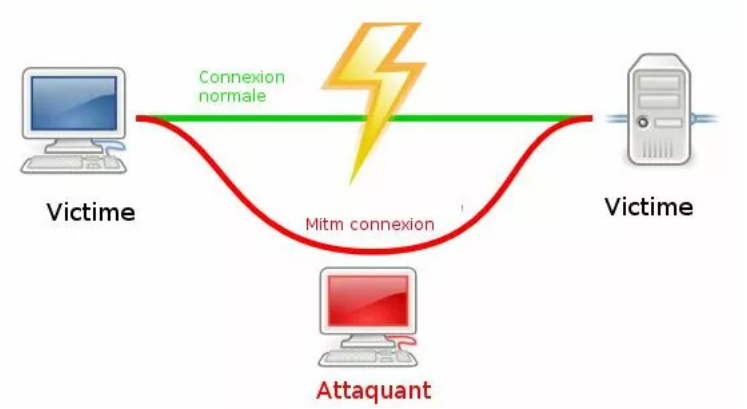

FIGURE 3.2 – L'attaque MitM sur Wi-F

— **Wiphisher Evil Twin (Jumeau maléfique) :** C'est une attaque qui allie la technique de spoofing d'adresse MAC, l'attaque par déni de service, et le social engineering. Dans un premier temps, le pirate effectue une écoute afin de récolter les informations de L'AP cible. Il crée un point d'accès pirate identique (en usurpant son adresse MAC BSSID et le nom du réseau Wi-Fi SSID) mais non sécurisé. Après ça, il utilise une attaque DOS (Généralement un flux de désauthentification) sur l'AP légitime afin de forcer la déconnexion des clients et les pousser vers l'AP frauduleux. Une fois le client connecté, le pirate redirigera ses requêtes web vers un portail fictif préalablement configuré qui demandera à l'utilisateur des informations sensibles (tel que le mot de passe du Wi-Fi légitime) qui seront directement communiquées au pirate. La figure suivante illustre un exemple de portail fictif pouvant être utilisé par un pirate pour le vol d'identifiants [40].

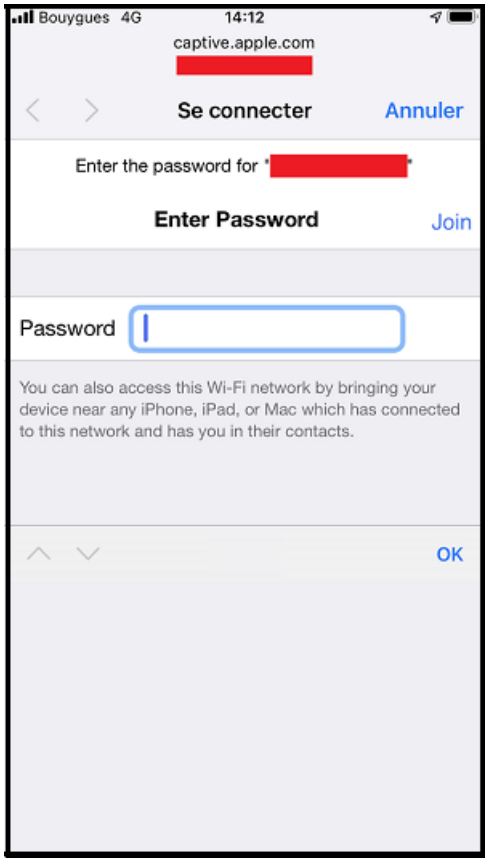

FIGURE 3.3 – Exemple de portail captif utilisé dans l'attaque Evil Twin.

— **Attaque par dictionnaire et force brute :** Ce sont des attaques qui visent les mots de passe gérer par les différents protocoles sans fil. L'attaque par force brute est une attaque qui théoriquement fonctionne à tous les coups. Elle consiste à essayer toutes les clés possibles, une à une, jusqu'à ce qu'on retrouve la clé utilisée pour le chiffrement.

Une autre attaque semblable est l'attaque par dictionnaire, Cette attaque est souvent utilisée en parallèle avec l'attaque par force brute, et consiste à essayer de retrouver un mot de passe en essayant tous les mots d'une liste contenant des mots souvent utilisés en tant que mot de passe . Ces types d'attaque sont fréquemment mener contre les réseaux sans fils[42].

3.2.4 La sécurité obsolète du IEEE 802.11

La norme 802.11 intégrait à l'origine un ensemble de solutions de sécurité ne sont certes pas parfaites, mais méritent d'exister, on peut citer :

3.2.4.1 Limiter les débordements

Pour limiter les risques d'attaques sur le réseau sans fil, il est essentiel de prendre des mesures pour éviter que les ondes radio ne se propagent à l'extérieur de l'entreprise. Cela peut être réalisé en plaçant stratégiquement les points d'accès de manière à ce que le niveau du signal soit maintenu à un niveau très faible à l'extérieur des locaux. Une autre approche consiste à ajuster la puissance d'émission des points d'accès au minimum nécessaire, afin de limiter la portée du signal sans compromettre la couverture à l'intérieur de l'entreprise. En prenant ces précautions, on réduit les possibilités pour les attaquants de capter le signal et d'interférer avec le réseau[43].

3.2.4.2 Masquer le SSID

Afin d'assurer une sécurité supplémentaire pour un réseau sans fil, il est recommandé de masquer le SSID, qui est l'identifiant de réseau utilisé par les utilisateurs pour se connecter. En configurant les points d'accès de manière à ne pas diffuser activement le SSID, on rend plus difficile pour les utilisateurs non autorisés de découvrir le réseau. Cependant, il est important de noter que cette mesure de sécurité est relativement faible, car il est possible pour un individu possédant un analyseur de paquets d'intercepter les paquets de sondage émis par les stations légitimes du réseau, ce qui lui permettrait de lire le SSID du réseau[43].

3.2.4.3 Filtrage par adresse MAC

Le filtrage par adresse MAC est une méthode de sécurité dans laquelle un point d'accès (AP) vérifie si l'adresse MAC (Medium Access Control) de la station qui tente de s'authentifier se trouve dans une liste d'adresses MAC autorisées. Si c'est le cas, l'utilisateur est autorisé à

accéder au réseau. Dans le cas contraire, l'AP lui refuse l'accès. Il est important de noter que l'adresse MAC d'une station est présente dans tous les paquets qu'elle émet, y compris la requête d'authentification.

Cependant, il est regrettable que la modification de l'adresse MAC d'une carte WiFi par un pirate ne soit pas très difficile. Ainsi, un pirate peut se faire passer pour l'un des périphériques autorisés en modifiant son adresse MAC. Par conséquent, bien que le filtrage par adresse MAC puisse fournir une certaine couche de sécurité, il ne doit pas être considéré comme une mesure de sécurité absolue[44].

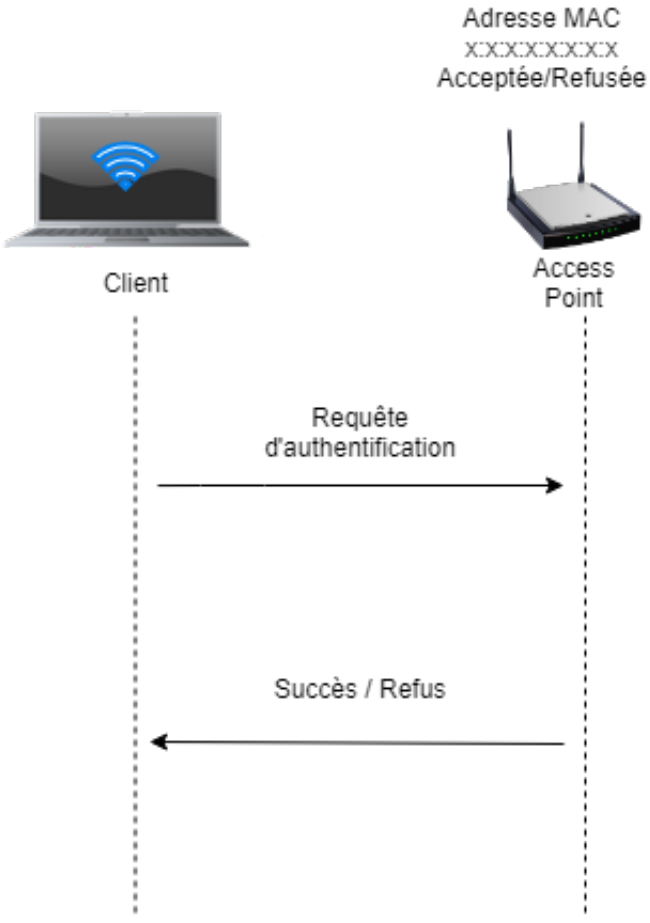

FIGURE 3.4 – Filtrage par adresse MAC

3.2.4.4 Les VLAN

Les VLAN (Virtual Local Area Network), ou réseaux locaux virtuels, offrent une segmentation logique des réseaux dans le but d'améliorer le niveau de sécurité. Lorsque les points d'ac-

cès le permettent, il est recommandé d'associer le trafic sans fil à un VLAN spécifique. Cela permet de séparer les groupes de données sensibles du reste du réseau, réduisant ainsi les risques de violation de la confidentialité. En attribuant des VLAN spécifiques au trafic sans fil, on crée une isolation et une protection supplémentaires pour les données sensibles, renforçant ainsi la sécurité globale du réseau[45].

3.2.4.5 Le cryptage WEP

Le WEP (Wired Equivalent Privacy), qui était la première solution de sécurité intégrée dans la norme 802.11, repose sur un principe simple. Chaque utilisateur doit connaître une même clé WEP, qui peut avoir une longueur de 40 ou 104 bits, et cette clé est utilisée par tous pour chiffrer les communications. Le WEP utilise l'algorithme RC4, conçu par l'éminent spécialiste de la sécurité informatique, Ron Rivest[44].

1. **Le principes de fonctionnement du WEP :** Le chiffrement en continu RC4 fonctionne comme suit voi la FIGURE 3.5 : il s'agit de développer une clé secrète et un vecteur d'initialisation (IV) de 24 bits, concaténé à une clé prépartagée, en un flot de clés de longueur arbitraire composé de bits pseudo aléatoires. Le chiffrement s'obtient par l'exécution d'une opération OU exclusive (XOR) entre le flot de clés et le texte en clair, pour produire le cryptogramme. Le déchiffrement se fait par génération du flot de clés identique, basé sur le vecteur d'initialisation et la clé secrète, et par application du OU exclusif sur le cryptogramme, pour récupérer le texte en clair.

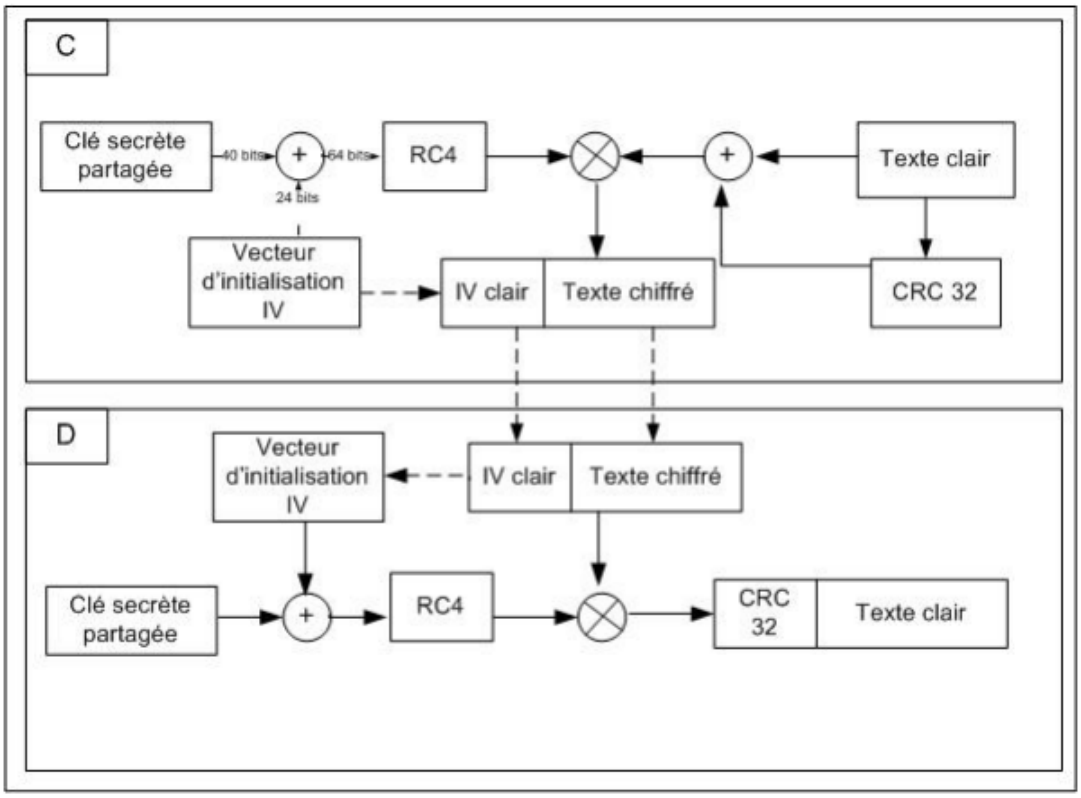

FIGURE 3.5 – Opération de chiffrement et déchiffrement

Le dernier volet de la sécurité WEP est le contrôle de l'intégrité des paquets échangés. Cela est réalisé en calculant le code de redondance cyclique (CRC) de 32 bits était rajouté à la fin de chaque paquet WiFi. Ce code est calculé en fonction du contenu du paquet et en constitue une sorte de résumé[43].

2. **Les faiblesses du WEP :** Même lors de la conception du WEP, l'IEEE était conscient que cette solution était loin d'être parfaite, mais suffisante pour répondre aux besoins des utilisateurs pendant quelques années. Après tout, le WEP reposait sur l'algorithme éprouvé RC4.Malheureusement, dès sa publication, le WEP a été minutieusement analysé par les meilleurs experts en sécurité du monde, et en moins de trois mois, il a été compromis.

   Une des principales failles du WEP réside dans sa clé. Celle-ci présente deux défauts majeurs : elle est constante et les combinaisons possibles sont très limitées. Les autres vulnérabilités du WEP sont liées à l'algorithme de chiffrement utilisé, le RC4.

Malheureusement, le CRC (Cyclic Redundancy Check) a été conçu pour détecter les erreurs de transmission, mais il est impuissant contre un pirate. En effet, si un pirate intercepte un paquet et le modifie, il lui suffit de recalculer le CRC avant de laisser le paquet continuer son chemin[43][46].

3.3 Les nouvelles solutions de sécurité d'un réseaux Wifi

Plusieurs techniques de sécurité ont été développées jusqu'à nos jours pour tenter d'offrir une sécurité poussée aux réseaux sans fil. Ils s'utilisent ainsi avec les normes qui ont été ratifiées par l'IEEE, la WiFi Alliance, etc. Initialement, la sécurité du Wi-Fi était assurée par le WEP. Cependant, il se pose le problème de la gestion des clés qui n'est pas traité par le WEP. Pour pallier à cette lacune plusieurs solutions de sécurité restent envisageables nous citons :

3.3.1 Les VPN

Un VPN (Virtual Private Network) est un environnement de communication dans lequel l'accès est contrôlé, afin de permettre des connections entre une communauté d'intérêts seulement. Un VPN est construit avec un partitionnement d'un media de communication commun qui offre des services de façon non exclusive . Les principaux avantages d'un VPN :

. **La Sécurité :** Assure des communications sécurisées et chiffrées.

. **La simplicité :** Utilise les circuits de télécommunication classiques.

. **L'économie :** Utilise Internet en tant que media principal de transport, ce qui évite les coûts lies à une ligne dédie.

Toutefois, isoler le réseau sans fil et obliger les utilisateurs à passer par des tunnels VPN pose quelques problèmes :

— Les solutions VPN du marché peuvent coûter assez cher et sont parfois complexes à mettre en oeuvre ;

— tout le trafic doit passer par un serveur VPN qui ne gère souvent qu'un nombre limité de connexions simultanées ;

Malgré ces défauts, la solution VPN était la seule à réellement offrir un niveau important de protection avant l'arrivée du WPA et du WPA2 [47][48].

3.3.2 Le WPA

La WiFi Alliance décida alors qu'elle ne voulait pas attendre l'apparution du 802.11i, sa conclusion fut qu'il était nécessaire d'avoir rapidement au moins une version allégée du futur 802.11i. C'est ainsi qu'elle définit la solution Wireless Protected Access (WPA) : il s'agit d'une version allégée du standard 802.11i. Il existe deux variantes du WPA : le WPA Personal, également appelé WPA-PreShared Key (WPA-PSK) et le WPA Enterprise .
Le WPA introduit le protocole TKIP (Temporal Key Integrity Protocol), qui sera repris par la norme IEEE 802.11i. Ce protocole permet de remédier aux faiblesses du chiffrement WEP en introduisant un chiffrement par paquet ainsi qu'un changement automatique des clés de chiffrement.
L'algorithme de chiffrement sous-jacent est toujours le RC4 utilisé avec des clés de 128 bits, mais contrairement au WEP, il est utilisé correctement (au sens cryptographique). Le standard WPA définit deux modes distincts [49] :

1. **Le WPA Personal :** Le mode « WPA personnel »permet de mettre en oeuvre une infrastructure sécurisée basée sur le WPA sans faire appel à un serveur d'authentification. Le WPA personnel repose sur l'utilisation d'une clé partagée, appelées PSK pour renseignée dans l'AP ainsi que dans les postes clients, contrairement au WEP, il n'est pas nécessaire de saisir une clé de longueur prédéfinie.
   En effet, le WPA permet de saisir une phrase secrète, traduite en PSK par un algorithme de hachage. Le mode WPA-PSK est vulnérable à des attaques par dictionnaire. Il est donc très important de choisir un secret fort afin de limiter ces risques[49,50].
2. **Le WPA Enterprise :** Le mode entreprise impose l'utilisation d'une infrastructure d'authentification 802.1x basée sur l'utilisation d'un serveur d'authentification, générale-

ment un serveur RADIUS, et d'un contrôleur réseau (le point d'accès). Cette solution est actuellement ce qu'il y a de plus sûr en termes de sécurité d'authentification forte[49][50].

3.3.3 Le WPA2

Le WPA2 est la ratification de la norme IEEE 802.11i. Ce standard reprend la grande majorité des principes et protocoles apportés par WPA, avec une différence notoire dans le cas du chiffrement : l'intégration de l'algorithme AES (Advanced Encryption Standard). Les protocoles de chiffrement WEP et TKIP sont toujours présents. Deux autres méthodes de chiffrement sont aussi incluses dans IEEE 802.11i :

- **WRAP (Wireless Robust Authenticated Protocol) :** s'appuyant sur le mode opératoire OCB (Offset Codebook) de AES ;
- **CCMP (Counter Mode with CBC MAC Protocol) :** s'appuyant sur le mode opératoire CCM (Counter with CBC-MAC) de AES.

Le chiffrement CCMP est le chiffrement recommandé dans le cadre de la norme IEEE 802.11i. Ce chiffrement, s'appuyant sur AES, utilise des clés de 128 bits avec un vecteur d'initialisation de 48 bits [51].

3.4 Authentification 802.1x

Le 802.1x est un standard mis en place en juin 2001 par l'IEEE. Ce standard provient du besoin de s'authentifier dès l'accès physique au réseau. Ce besoin s'est particulièrement fait sentir dans le domaine du WiFi, où les clés de cryptage WEP ne sont pas très efficaces, d'où l'idée d'une authentification physique dès les bornes.
Son objectif est de bloquer le flux de données d'un utilisateur non authentifié. C'est-à-dire qu'il permet une authentification lors de l'accès au réseau et donc un contrôle d'accès aux ressources.
Le 802.1x s'appuie sur un protocole particulier : **l'EAP (Extensible Authentification Protocol)** décrit par la suite. Le standard s'appuie sur des mécanismes d'authentification existants

.

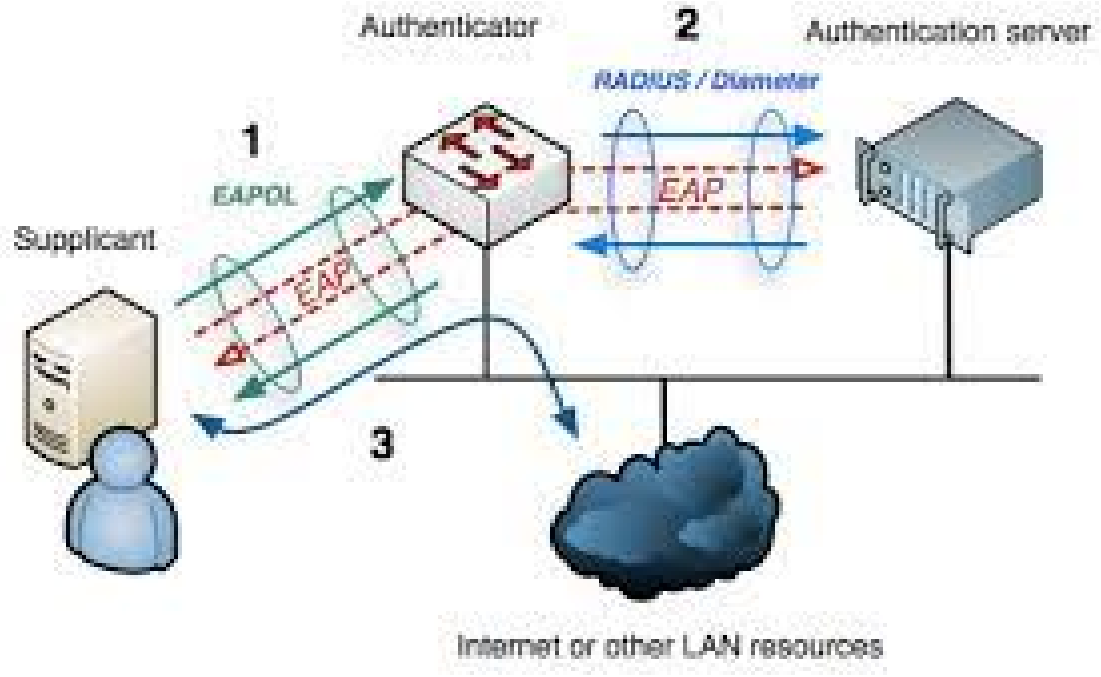

FIGURE 3.6 – Architecture d'authentification 802.1X.

Le 802.1x utilise un modèle qui s'appuie sur trois entités fonctionnelles

- **Le système à authentifier (supplicant) :** c'est un poste de travail (terminal informatique) demandant un accès au réseau.

- **Le système authentificateur (authenticator) :** c'est l'unité qui contrôle et fournit la connexion au réseau dans la plupart du temps c'est un AP. Un port contrôlé par cette unité peut avoir deux états : non autorisé ou autorisé. Lorsque le client n'est pas authentifié, le port est dans l'état non autorisé et seulement le trafic nécessité par l'authentification est permis.

-**Le serveur d'authentification (Authentication Server) :** il réalise la procédure d'authentification avec le système d'authentification et valide la demande d'accès. Si la requête d'accès est validée par le serveur, le port est commuté dans l'état autorisé et le client est autorisé à avoir un accès complet au réseau [52][53].

3.5 EAP (Extensible Authentication Protocol)

La communication entre l'équipement réseau (authenticator) et le serveur d'authentification est assurée par le protocole EAP (Extensible Authentication Protocol) qui assure le transport des informations d'authentification et permet d'utiliser différentes méthodes d'authentification d'où le terme '' Extensible". Le domaine d'application de ce protocole correspond donc à tous les modes de connexion pouvant être considérés comme des connexions dites point à point telles que : connexion réseau sans fil entre un poste utilisateur et une borne d'accès Wifi.
protocole EAP, il est à la base du 802.1x, sur lequel reposent à leur tour les nouvelles solutions de sécurité du WiFi, le WPA Enterprise et le WPA2 Enterprise. Le protocole d'authentification EAP a été défini par l'IETF.
Le 802.1x est une pyramide de protocoles dont la base est l'EAP. Pour comprendre le 802.1x, il faut donc comprendre l'EAP, et pour bien comprendre l'EAP, il faut revenir à son origine qui est le Protocole de Point à Point , « The Point-to-Point Protocol (PPP) »[54].

3.5.1 Le protocole PPP

3.5.1.1 Présentation du protocole PPP

PPP est un protocole de couche 2 du modèle OSI, il fournit une méthode standard pour transporter les datagrammes multi protocole (Ip, Ipx et Netbeui) sur des liens point à point synchrones ou asynchrones. Il est employé pour créer une connexion à la demande entre un client et un serveur d'accès réseau. Le protocole PPP permet aussi d'authentifier des connexions en utilisant le protocole d'authentification du mot de passe (Password Authentication Protocol, PAP) ou le protocole d'authentification à échanges confirmés (Challenge Handshake Authentication Protocol, CHAP), ce dernier étant plus efficace. L'utilisation du protocole PPP présente de nombreux avantages, notamment le fait qu'il n'est pas propriétair[55].
Le protocole PPP s'appuie sur trois composants :

— L'encapsulation des datagrammes grâce à HDLC (High-Level Data Link Control).

— Le contrôle de la liaison avec LCP (Link Control Protocol).

— Le contrôle de la couche réseau avec NCP (Network Control Protocol).

3.5.1.2 L'authentification avec PPP

Le protocole PPP prend en charge deux principales méthodes d'authentification par mot de passe :

1. **PAP (Password Authentication Protocol) :**PAP est l'une des méthodes d'authentification les plus simples et les moins sécurisées disponibles dans le protocole PPP.
   Lors de l'authentification PAP, le client envoie son nom d'utilisateur (username) et son mot de passe (password) en clair au serveur d'authentification.
   Le serveur d'authentification vérifie les informations d'identification reçues et accepte ou refuse l'accès en fonction de la correspondance du nom d'utilisateur et du mot de passe fournis [56].

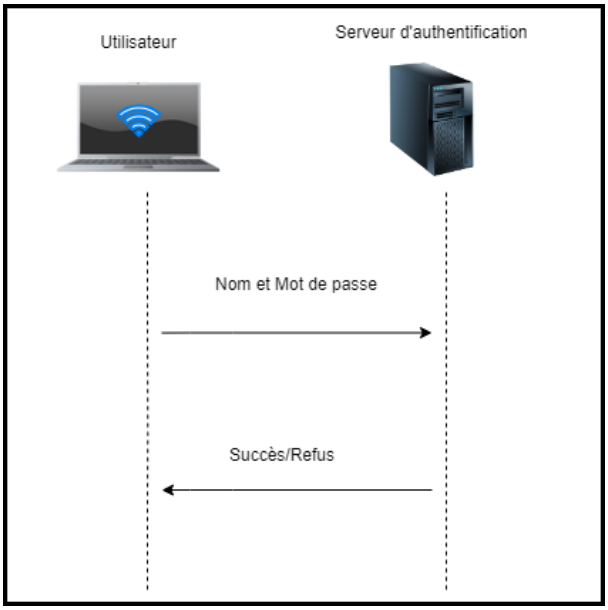

FIGURE 3.7 – L'identification avec le protocole PAP

2. **CHAP (Challenge Handshake Authentication Protocol) :** CHAP est une méthode d'authentification plus sécurisée que PAP, utilisant des défis (challenges) et des réponses

(responses) pour vérifier l'identité du client. Lors de l'authentification CHAP, le serveur d'authentification envoie un défi (challenge) au client. Le client utilise un algorithme de hachage (hash) , habituellement l'algorithme MD5. pour combiner le défi avec son mot de passe et envoie la réponse (response) au serveur. Le serveur d'authentification effectue également le même calcul en utilisant le mot de passe stocké pour le client. Si la réponse du client correspond à celle calculée par le serveur, l'authentification est réussie[57].

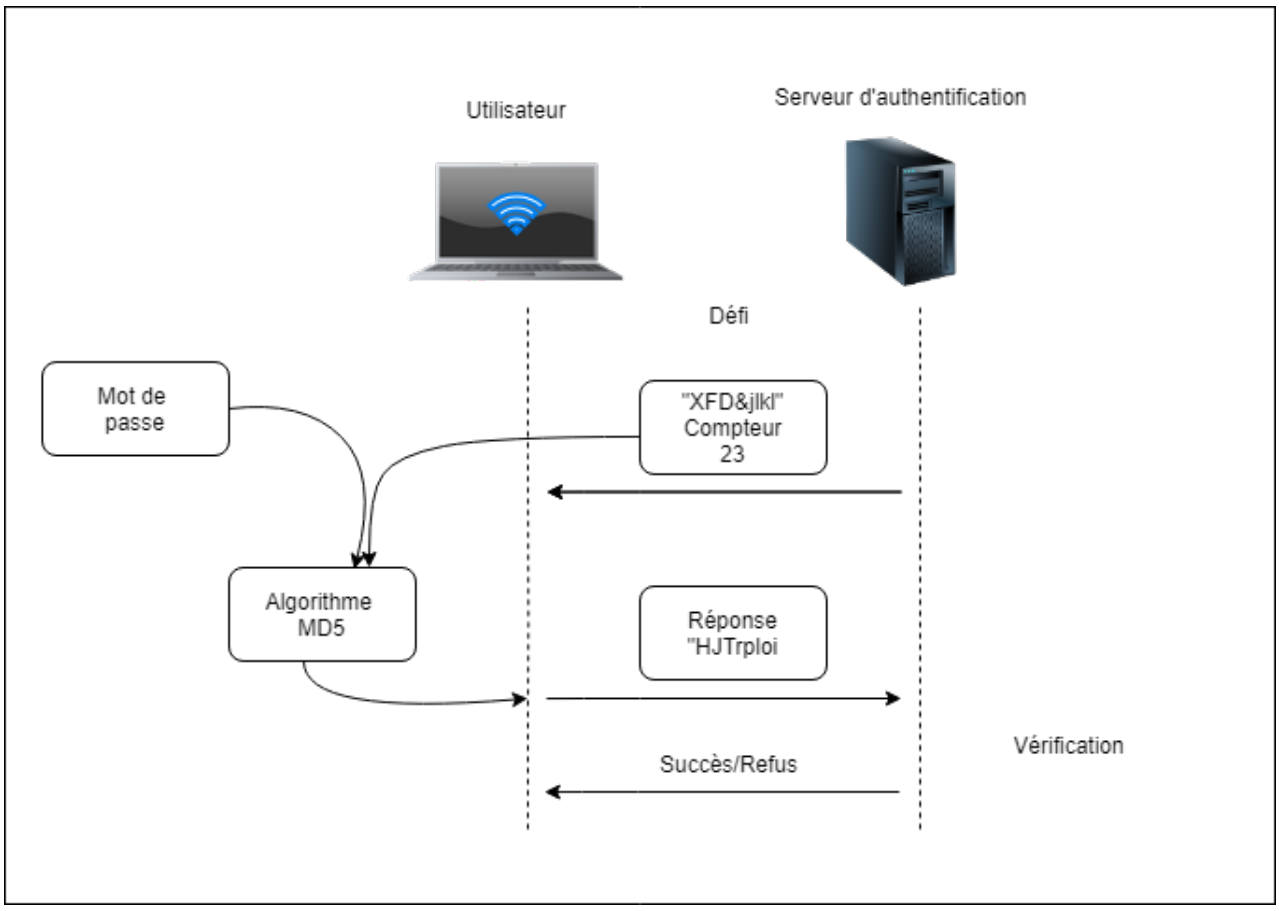

FIGURE 3.8 – L'identification avec le protocole CHAP

3.5.1.3 Les limites de ces méthodes

Malheureusement, la méthode PAP n'est pas sécurisée et la méthode CHAP est vulnérable face à des attaques hors-ligne de type dictionnaire, il suffit qu'un seul utilisateur légitime ait

un mot de passe faible pour que le pirate puisse entrer sur le réseau.

En outre, certains FAI (Fournisseur d'Accès Internet) ont estimé qu'il était dommage qu'on ne puisse identifier les utilisateurs que sur la base d'un simple mot de passe. Certains voulaient pouvoir identifier les utilisateurs avec une carte à puce, d'autres voulaient utiliser des certificats électroniques, etc. C'est de ce besoin qu'est né l'EAP [56][57] .

3.5.2 Le fonctionnement d'EAP

Le principe d'EAP est très simple, si un utilisateur cherche à accéder au réseau, un contrôleur d'accès lui barrera le chemin jusqu'à ce qu'il s'identifie auprès du serveur d'authentification. Le contrôleur d'accès sert d'intermédiaire pour la communication entre l'utilisateur et le serveur d'authentification. Dans le cadre du WiFi, lorsque le 802.1x est utilisé, chaque AP est un contrôleur d'accès [58]. Le fait que le contrôleur d'accès ne soit qu'un intermédiaire entre l'utilisateur et le serveur est l'un des grands intérêts de l'EAP : en effet, si une nouvelle méthode d'authentification est inventée, il ne sera pas nécessaire de changer les contrôleurs d'accès, car seuls les utilisateurs et le serveur d'authentification devront être mis à jour [59].

3.5.3 Méthode d'authentification associée à EAP

Le protocole 802.1x ne propose pas une seule méthode d'authentification mais un canevas sur lequel sont basés une douzaine de différents scénarios d'authentification, basés sur plusieurs éléments d'identification (login / mot de passe, certificat électronique, puce SIM) qui peuvent, selon les scénarios, être combinés. Nous allons présenter brièvement les principales procédures d'authentification couramment utilisées via EAP [60][52].

a) Méthodes basées sur les mots de passes :

1. **EAP-MD5 :** est l'une des méthodes d'authentification les plus simples d'EAP, elle est très simple à mettre en place et son mécanisme d'authentification est semblable à

la méthode CHAP . Chaque utilisateur possède un mot de passe associé à un nom d'utilisateur qu'il utilise pour s'authentifié auprès d'un serveur d'authentification avec le mécanisme de défi/réponse. Comme l'illustre la figure 3.9 , l'authentification avec EAP/MD5 se déroule comme suit :

Le serveur d'authentification envoi un défi (Challenge) au client et celui-ci le chiffre via l'algorithme de hachage MD5 et le renvoi au serveur. À la réception de la réponse du défi, le serveur récupère dans sa base de donnees, le mot de passe correspondant au nom d'utilisateur du message reçu, et l'utilise pour faire le même calcul fait par le client, et si les résultats sont identiques, alors le serveur lui renverra un message EAP success indiquant la réussite de l'authentification au client, sinon il renverra un message EAP faillure indiquant l'échec de l'authentification .

Le problème majeur de cette méthode réside dans le fait que les échanges ne sont pas chiffrés. En outre, EAP-MD5 ne gère pas la distribution dynamique des clés WEP.

Le seul avantage de cette méthode est la simplicité : il est relativement facile de mettre en place une structure d'authentification basée sur cette méthode. Celle-ci est d'ailleurs beaucoup utilisé pour des réseaux filaires où la contrainte lié au chiffrage des échanges est moins forte que pour les réseaux Wifi [60].

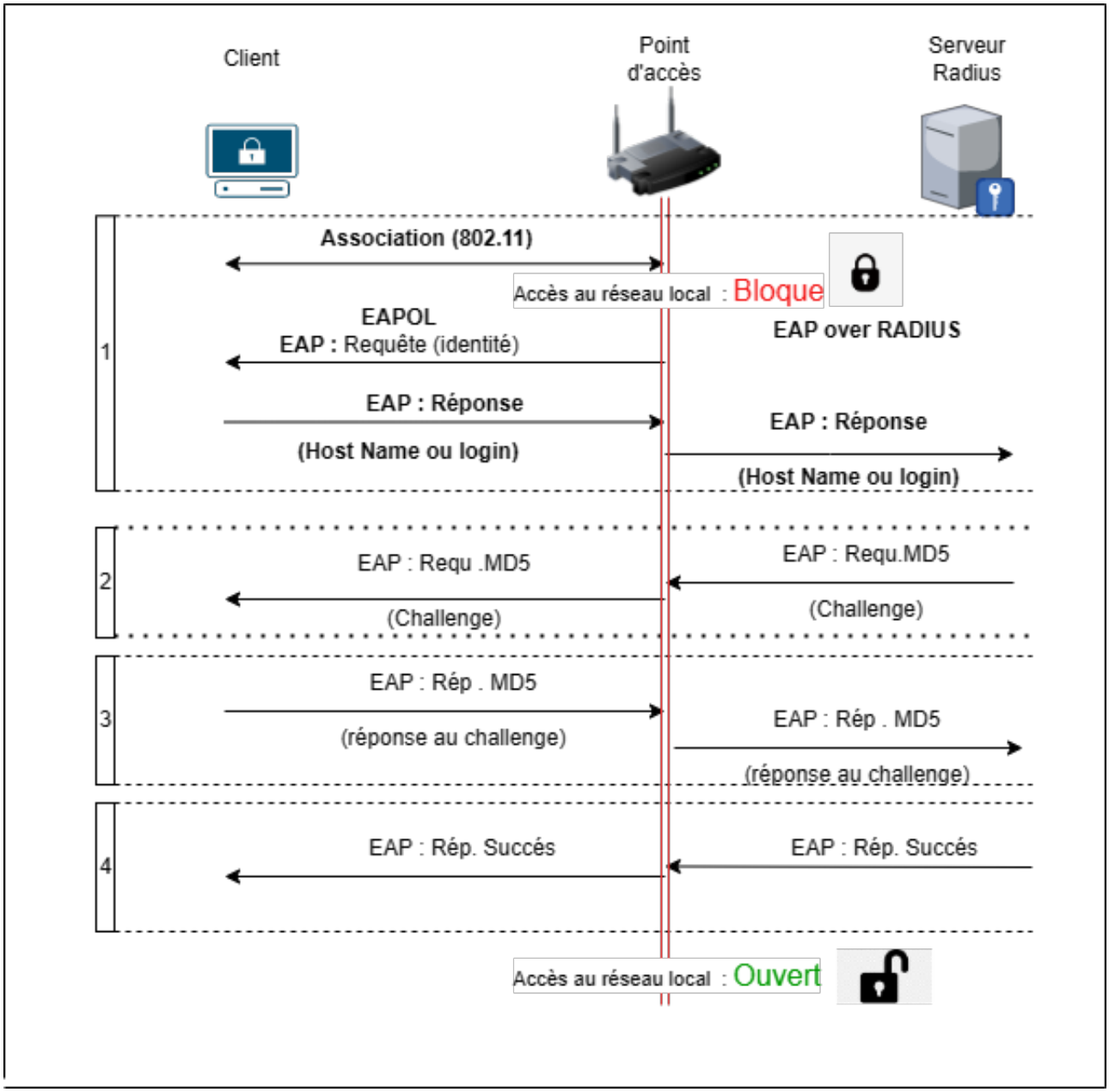

FIGURE 3.9 – Diagramme d'échanges EAP-MD5

2. **LEAP ((Lightweight EAP) :** Est une implementation propriétaire d'EAP conçu par Cisco systems assurant une authentification simple par mot de passe via une encapsulation s´ecurisée, ce protocole est vulnérable aux attaques (cryptage MD5) sauf si l'utilisateur utilise des mots de passe complexes [52].

b) Méthodes basées sur les Certificats :

1. **EAP-TLS :** L'EAP-TLS (Transport Layer Security) utilise deux certificats pour la création d'un tunnel sécurisé qui permettra ensuite l'identification : un côté serveur et un côté client. Cela signifie que même si le mot de passe est découvert, il ne sera d'aucune utilité sans le certificat client. Bien qu'EAP-TLS fournisse une excellente sécurité, l'obligation de disposer d'autant de certificats peut dissuader de nombreux administrateur. En effet lorsque l'on dispose d'un grand nombre de machines, il peut s'avérer difficile et coûteux de gérer un certificat par machine. C'est pour se passer du certificat client que les protocoles PEAP et EAP-TTLS ont été créés [52].

3.5.4 Protocole Radius

3.5.4.1 Présentation

RADIUS (Remote Authentification Dial In User Service) est un protocole d'authentification client/serveur habituellement utilisé pour l'accès à distance, défini par la RFC 2865. Ce protocole permet de sécuriser les réseaux contre des accès à distance non autorisés. Ce protocole est indépendant du type de support utilisé le protocole Radius repose principalement sur un serveur (serveur Radius), relié à une base d'identification (fichier local, base de données, annuaire LDAP, etc.)et un client Radius, Appelé NAS (Network Access Server), faisant office d'intermédiaire entre l'utilisateur final et le serveur. Le mot de passe servant à authentifier les transactions entre le client Radius et le serveur Radius est chiffré et authentifier grâce à un secret partagé[61].

3.5.4.2 Principe de fonctionnement

Le fonctionnement de Radius est basé sur un scénario proche de celui-ci :

- 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.

Le serveur Radius retourne ainsi une des quatre réponses suivantes :

— **ACCEPT :**l'identification a réussi.

— **REJECT :**l'identification a échoué.

— **CHALLANGE :** le serveur RADIUS souhaite des informations supplémentaires de la part de l'utilisateur et propose un «défi».

— **CHANGE PASSWORD :**le serveur Radius demande à l'utilisateur un nouveau mot de passe.Suite à cette phase d'authentification débute une phase d'autorisation ou le serveur retourne les autorisations aux utilisateurs[61].

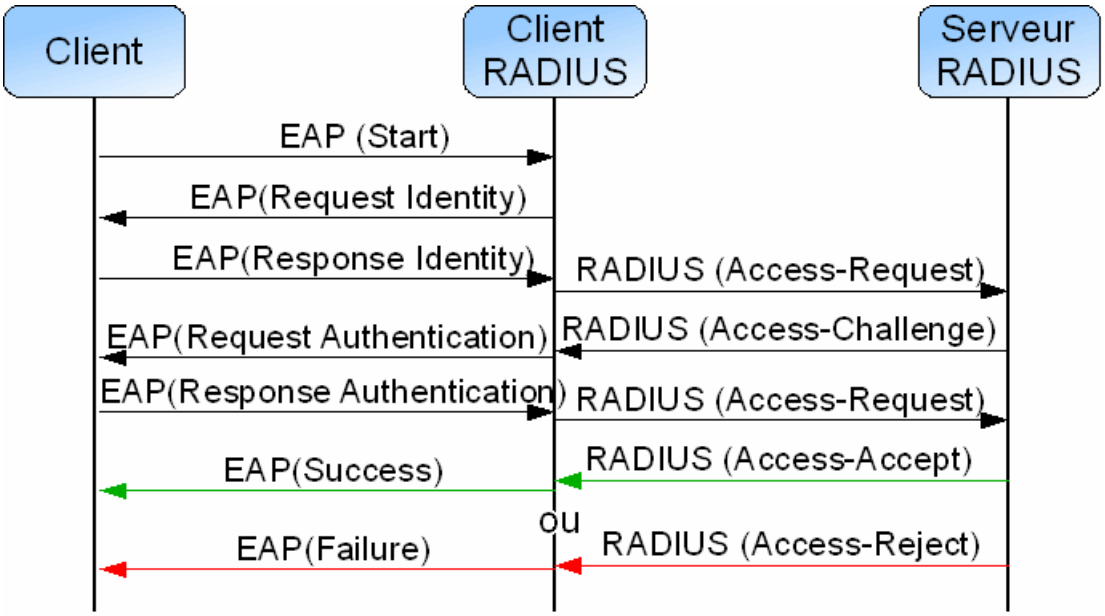

FIGURE 3.10 – L'identification avec le protocole RADIUS

3.6 La solution proposé

L'objectif principal de notre étude mise en œuvre d'une solution d'administration et d'authentification pour améliorer la gestion et la sécurité de l'accès aux services réseau de Sonatrach.

Dans le cadre de notre étude, nous avons choisi plusieurs solutions pour atteindre notre objectif.

Tout d'abord, nous avons opté pour l'utilisation de contrôleurs d'accès sans fil (AC)

afin de contrôler et gérer de manière centralisée les multiples points d'accès. Ainsi, le point d'accès sans fil n'agit plus comme un dispositif intelligent indépendant, mais le contrôleur d'accès sans fil devient le "cerveau" du réseau sans fil.

Pour assurer l'authentification et la gestion des autorisations d'accès, nous avons mis en place le protocole RADIUS. En plus de l'authentification, RADIUS permet de gérer les mots de passe et les identifiants des clients, centralisant ainsi les informations d'identification et simplifiant leur gestion.

Dans le cadre de la sécurisation de l'accès à distance aux réseaux, nous utilisons le protocole RADIUS conjointement avec la norme 802.1x et la méthode PEAP-TLS. Le protocole 802.1x assure l'authentification des clients en utilisant des certificats, tandis que le protocole PEAP permet le transport sécurisé des données d'authentification, y compris les anciens protocoles basés sur les mots de passe, sur les réseaux Wi-Fi 802.11.

En outre, nous utilisons WPA2 (Wi-Fi Protected Access 2) pour renforcer la sécurité du réseau sans fil. Cependant, il est important de noter que WPA2 nécessite des équipements capables de traiter les opérations de chiffrement AES.

Grâce à ces solutions mises en place, nous visons à améliorer la gestion des utilisateurs, à renforcer la sécurité de l'accès aux services réseau et à fournir un environnement Wi-Fi sécurisé au sein de l'entreprise Sonatrach.

3.6.1 Le fonctionnement de notre solution

3.6.1.1 PEAP-TLS (Protected Extensible Authentication Protocol/Transport Layer Security)

a) Processus d'authentification : Lorsqu'un client souhaite se connecter à un réseau Wi-Fi sécurisé utilisant PEAP/TLS, il envoie une demande de connexion au point d'accès (AP) ou au contrôleur Wi-Fi. Le point d'accès ou le contrôleur Wi-Fi redirige ensuite le client vers un serveur d'authentification, généralement un serveur RADIUS (Remote Authentication Dial-In User Service). Le serveur RADIUS et le client entament une session sécurisée en utilisant le protocole TLS (Transport Layer Security). Pendant la

phase d'établissement de la session TLS, le serveur RADIUS présente son certificat numérique au client pour prouver son identité. Le client vérifie l'authenticité du certificat en utilisant une autorité de certification (AC) de confiance. Une fois que la confiance mutuelle est établie, le client présente son propre certificat numérique au serveur RADIUS pour prouver son identité. Le serveur RADIUS vérifie l'authenticité du certificat du client en utilisant l'AC de confiance. Si l'authentification réussit des deux côtés, une session sécurisée est établie entre le client et le serveur RADIUS, permettant au client d'accéder au réseau Wi-Fi[52].

b) Avantages de PEAP/TLS dans la sécurisation des réseaux Wi-Fi :

- Authentification robuste :L'utilisation de certificats numériques renforce l'authentification en garantissant l'identité des clients et des serveurs. Cela empêche les attaques de type "man-in-the-middle" où un attaquant tente de se faire passer pour le serveur ou le client.
- Confidentialité des données : Le protocole TLS chiffre les données échangées pendant le processus d'authentification, assurant ainsi la confidentialité des informations sensibles, telles que les identifiants d'utilisateur, qui sont protégés contre les interceptions et les écoutes.
- Intégration avec les infrastructures existantes : PEAP/TLS s'intègre facilement avec les infrastructures existantes utilisant le protocole RADIUS, ce qui facilite son adoption dans les réseaux Wi-Fi existants.
- Gestion centralisée des certificats : Les certificats numériques utilisés dans PEAP/TLS peuvent être gérés de manière centralisée à partir d'une autorité de certification interne ; cela facilite l'émission, le renouvellement et la révocation des certificats pour les utilisateurs et les appareils connectés [62].

3.7 Conclusion

Dans ce chapitre, nous avons examiné en détail les différents niveaux de sécurité ainsi que les différentes attaques auxquelles les réseaux sans fil peuvent être confrontés. À partir de

là, nous avons présenté notre solution, qui repose sur l'authentification basée sur des certificats PEAP/TLS, en expliquant en détail son fonctionnement et ses avantages en termes de sécurité.

Dans le prochain chapitre, nous allons nous concentrer sur la mise en place concrète de notre solution. Nous aborderons les différentes configurations nécessaires pour assurer un déploiement efficace et sécurisé. Nous explorerons également des exemples de captures réelles afin d'illustrer les bénéfices de notre solution dans des scénarios pratiques.

Chapitre 4

Implimentation de la solution et configuration

4.1 Introduction

Dans ce chapitre, nous mettrons en œuvre notre projet en utilisant les solutions précédemment proposées. Nous détaillerons les diverses configurations requises pour le réseau intranet de l'entreprise , en utilisant les simulateurs Cisco Packet Tracer et GNS3.
Afin de présenter les configurations que nous avons effectuées, nous illustrerons les différentes étapes à l'aide de captures d'écran. Ces captures d'écran permettront de visualiser concrètement les étapes de configuration réalisées.

4.2 Présentation des outils

4.2.1 VMware Workstation 17

Application de virtualisation des postes de travail rationalisée, VMware Workstation Player permet d'exécuter un ou plusieurs systèmes d'exploitation sur un même ordinateur sans redémarrage. Simplicité de l'interface utilisateur, prise en charge et portabilité inégalées des systèmes d'exploitation [63].

4.2.1.1 Installation de VMware Workstation 17

On pourrait toutefois télécharger une version d'évaluation de VMware Workstation 17 Pro via deux façons :

— Le premier moyen consiste à se connecter sur son compte « my vmware » à l'adresse www.vmware.com. Si on ne dispose pas de compte, on pourrait le créer gratuitement sur le site web de VMware. Une fois connectée à son compte, se rendre à la section « VMware Workstation 17Pro for Windows » choisir la version du produit à télécharger via un menu déroulant à la version et cliquer sur le bouton « Télécharger maintenant » pour démarrer le téléchargement du produit.

— Le deuxième moyen de télécharger la VMware Workstation 17 Pro sans disposer de compte VMware, est de se rendre sur le lien ci-dessous : https ://goo.gl/5SyGWT. Une

fois sur la page « Try VMware Workstation Pro », cliquez juste sur le lien « Télécharger maintenant »[63].

FIGURE 4.1 – installation de VMware Workstation 17

4.2.2 Présentation de GNS3 (Graphical Network Simulator)

Est une solution open-source qui permet d'émuler des équipements informatiques (routeur, switch, PC. .) et qui permet de simuler leurs fonctionnements. Cet outil est très utile pour maquetter avant une mise en production [64].

4.2.2.1 Installation de GNS3 sous windows

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

1. Téléchargez l'installeur Windows depuis le lien fourni (www.GNS3.com) et lancer l'exécution de linstallateur.
2. Lorsque la fenêtre de bienvenue s'affiche, appuyez sur « next » et Acceptez les termes de la licence.

3. Ne modifiez pas le répertoire du menu démarrer au travers duquel GNS3 est accessible, laissez la liste des composants à installer inchangée.
4. A l'apparition de l'écran de bienvenue de Wireshark, appuyez sur « next ».
5. Acceptez les termes de la licence.
6. Laissez la liste des composants à installer inchangée et validez.
7. Laissez la liste des taches additionnelles inchangée et validez.
8. Ne modifiez pas le répertoire dans lequel Wireshark sera installé et validez.
9. l'apparition de l'écran de bienvenue de Winpcap, appuyez sur « OK ».
10. Acceptez les termes de la licence.
11. Autorisez le module winpcap à s'exécute au démarrage.
12. Lorsque l'installation se termine, cliquez sur « Finish ».
13. Après l'installation de GNS3, cliquez sur « Next ».
14. A la demande d'inscription à la mailing-list de GNS3„ cliquez sur « next » puis sur « No » à la fenêtre demandant de confirmer.
15. Décochez « Start GNS3 » et cliquez sur « Finish »,l'installation est terminée [64].

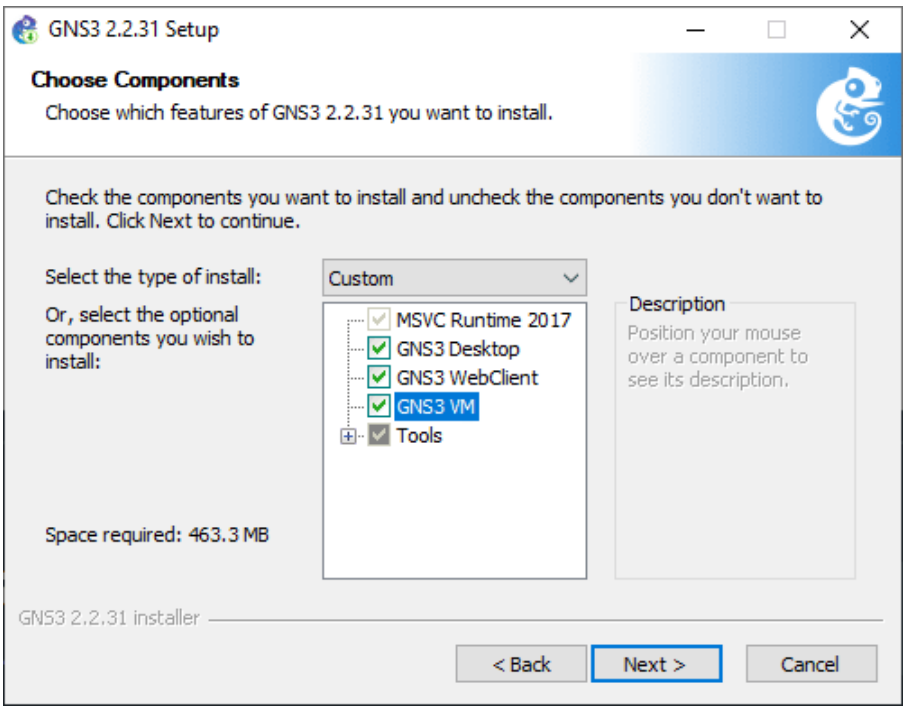

FIGURE 4.2 – installation GNS3

4.2.3 Présentation du simulateur Cisco Packet Tracer 7.2.1

Packet Tracer est un puissant simulateur de réseau développé par Cisco Systems, conçu pour créer des plans d'infrastructure de réseau en temps réel. Il offre la possibilité de créer, visualiser et simuler des réseaux informatiques [65].

4.3 L'architecture proposée

Topologie de notre solution implémentée sous GNS3 voire la FIGURE 4.3 :

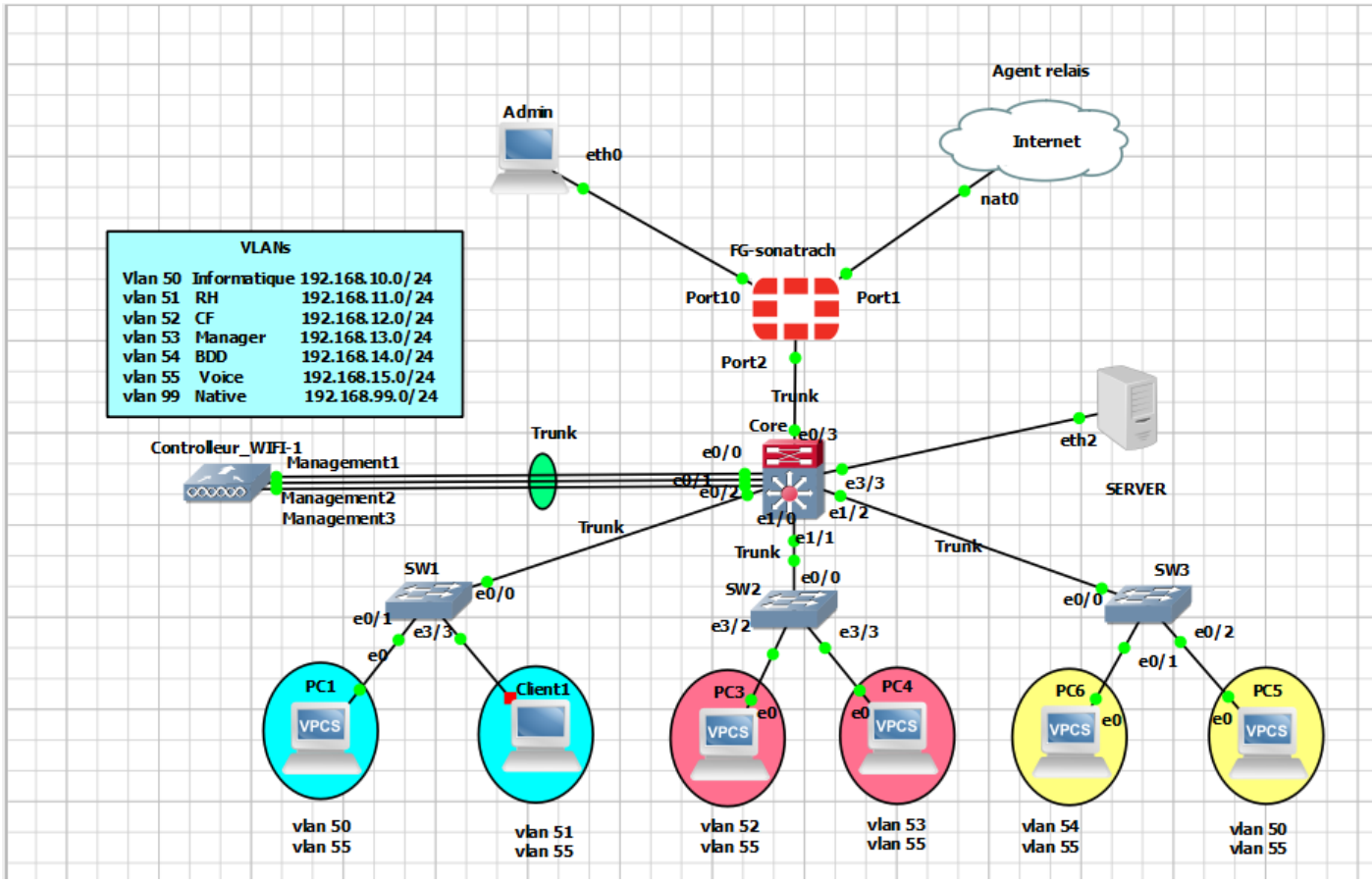

FIGURE 4.3 – Architecture Réseaux

4.4 Configuration de base

4.4.1 Plan d'adressage IPv4

L'adresse du réseau est **192.168.10.0/24**, ce qui signifie que son masque de sous-réseau est **255.255.255.0**.

En utilisant ce masque, chaque sous-réseau peut accueillir jusqu'à 254 adresses IP utilisables.

Dans le cadre de la mise en place des VLAN, les machines associées à un même VLAN partageront des adresses IP provenant d'un même sous-réseau. La TABLE 4.1 présente la liste des VLANs à mettre en œuvre, ainsi que leurs paramètres IP correspondants.

Nom du vlan	Id du vlan	Adress ip	masque	passerelle
Informatique	50	192.168.10.0	255.255.255.0	192.168.10.254
RH	51	192.168.11.0	255.255.255.0	192.168.11.254
CF	52	192.168.12.0	255.255.255.0	192.168.12.254
Manager	53	192.168.13.0	255.255.255.0	192.168.13.254
BDD	54	192.168.14.0	255.255.255.0	192.168.14.254
Voice	55	192.168.15.0	255.255.255.0	192.168.15.254
Native	99	192.168.99.0	255.255.255.0	192.168.99.254

TABLE 4.1 – Plan d'adressage IPv4

4.4.2 Configuration VTP (Serveur/Client)

Pour faciliter la configuration des VLAN sur plusieurs switchs, il faut configurer le protocole VTP (Virtual LAN Trunk Protocol) : protocoles de niveau 2 permis d'ajouter un ou plusieurs vlans sur le seul switch de distribution.

1.Pour configurer Switch Cœur en tant que serveur VTP :

Le commutateur CORE Switch sera configuré en tant que serveur VTP, ce qui lui permettra de prendre en charge l'administration de tous les VLANs.

La configuration du serveur VTP sur le switch core est illustrée dans la FIGURE 4.3

```
Core#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Core(config)#vtp mode server
Device mode already VTP Server for VLANS.
Core(config)#vtp domain sontrach.vtp
Changing VTP domain name from NULL to sontrach.vtp
Core(config)#vtp password sonatrach123
Setting device VTP password to sonatrach123
Core(config)#vtp version 2
Core(config)#vtp pruning
Pruning switched on
```

FIGURE 4.4 – La configuration du VTP serveur

2.Les switchs switch Access 1,switch Access 2, switch Access 3 :

sont configuré de la même manière mais en mode client.

La configuration VTP-client des autres commutateurs est représentée dans la FIGURE 4.4

```
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#vtp mode client
Setting device to VTP Client mode for VLANS.
SW1(config)#vtp domain sontrach.vtp
Changing VTP domain name from NULL to sontrach.vtp
SW1(config)#vtp password sonatrach123
Setting device VTP password to sonatrach123
SW1(config)#vtp version 2
Cannot modify version in VTP client mode unless the system is in VTP version 3
SW1(config)#
SW1(config)#end
```

FIGURE 4.5 – La configuration du VTP client

4.4.3 Interface en mode trunk

1.Configuration des ports “trunk” :

dans le le switch Core est illustrée dans la FIGURE 4.5

```
Core#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Core(config)#interface range ethernet 1/0-2
Core(config-if-range)#switchport trunk encapsulation dot1q
Core(config-if-range)#switchport mode trunk
Core(config-if-range)#switchport trunk native vlan 99
Core(config-if-range)#switchport trunk allowed vlan 50-55,99
Core(config-if-range)#end
Core#
*Jun 11 09:41:13.551: %SYS-5-CONFIG_I: Configured from console by console
Core#
```

FIGURE 4.6 – La configuration en mode trunk

4.4.4 Création des vlan

La création des vlan se fait pour renforcer la sécurite du réseaux,donc la création des réseaux locaux virtuels (VLAN) sera effectuée sur le CORE Switch, et cette configuration sera ensuite automatiquement propagée aux autres commutateurs grâce au protocole VTP. Les commandes de base pour la création des VLANs sont présentées dans la FIGURE 4.6

```
Core(config)#vlan 50
Core(config-vlan)#name informatique
Core(config-vlan)#vlan 51
Core(config-vlan)#name RH
Core(config-vlan)#vlan 52
Core(config-vlan)#name CF
Core(config-vlan)#vlan 53
Core(config-vlan)#name Manager
Core(config-vlan)#vlan 54
Core(config-vlan)#name voice
Core(config-vlan)#vlan 55
Core(config-vlan)#name native
```

FIGURE 4.7 – création des VLANs

4.4.5 Affectation des port au vlans

Le mode access est utilisé pour connecter des périphériques finaux à un VLAN spécifique.

• switch Access 1 :

On va affecter les ports aux vlan

Le port 0/1 de ce switch sont configurés en mode Access pour le VLAN 50

Le port 3/3 de ce switch sont configurés en mode Access pour le VLAN 51

Les commandes nécessaires sont illustrées dans la FIGURE 4.7

```
SW1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
SW1(config)#interface ethernet 0/1
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 50
SW1(config-if)#switchport voice  vlan 55
SW1(config-if)#exit
SW1(config)#interface ethernet 3/3
SW1(config-if)#switchport mode access
SW1(config-if)#switchport access vlan 51
SW1(config-if)#switchport voice  vlan 55
SW1(config-if)#end
```

FIGURE 4.8 – Configuration des interfaces sur le switch Access 1

On va appliquer la même méthode pour les autres switches.

4.4.6 Interfaces VLANs et Routage inter-VLAN

En créant des interfaces VLAN sur le switch central et en leur assignant des adresses IP, il devient possible de les utiliser comme passerelles par défaut pour chaque VLAN du réseau. Une fois cela réalisé, nous pouvons activer le routage inter-VLAN en utilisant la commande "IP routing".

La configuration requise pour cette mise en place est présentée dans la FIGURE 4.8 , qui illustre les commandes nécessaires.

```
Core#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Core(config)#interface vlan 50
Core(config-if)#ip address 192.168.10.253 255.255.255.0
Core(config-if)#NO sh
Core(config-if)#interface vlan 51
Core(config-if)#ip address 192.168.11.253 255.255.255.0
Core(config-if)#NO sh
Core(config-if)#interface vlan 52
Core(config-if)#ip address 192.168.12.253 255.255.255.0
Core(config-if)#NO sh
Core(config-if)#interface vlan 53
Core(config-if)#ip address 192.168.13.253 255.255.255.0
Core(config-if)#NO sh
Core(config-if)#interface vlan 54
Core(config-if)#ip address 192.168.14.253 255.255.255.0
Core(config-if)#NO sh
Core(config-if)#interface vlan 55
Core(config-if)#ip address 192.168.15.253 255.255.255.0
Core(config-if)#NO sh
```

FIGURE 4.9 – Configuration des interfaces VLANs et routage inter-VLAN

4.4.7 Architecture de mise en œuvre

Pour configurer le nouveau réseau local de SONATRACH, nous avons utilisé une simulation sur Cisco Packet Tracer. Nous nous sommes concentrés uniquement sur la partie liée au réseau sans fil, car le reste du réseau filaire ne serait pas affecté.

FIGURE 4.9 montre la topologie sans fil du réseau local de SONATRACH

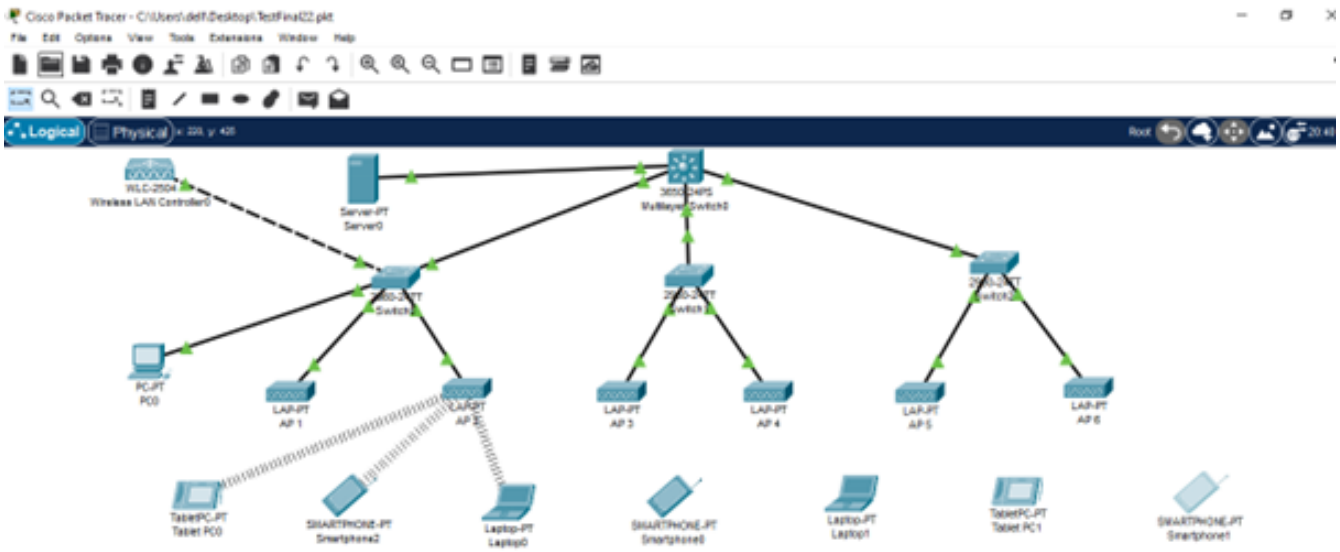

FIGURE 4.10 – Topologie simulée du réseau

a) Configuration du WLC Le contrôleur WiFi permet la gestion centralisée des points

d'accès sans fil dans le réseau. Il peut configurer, surveiller et mettre à jour les AP de manière centralisée, plutôt que de devoir le faire individuellement pour chaque AP.

— **Management :** La configuration complète du contrôleur WiFi (WLC) se fera via son interface graphique, accessible via un navigateur en utilisant l'adresse IP de l'interface de gestion. Avant cela, deux éléments doivent être configurés préalablement :

1. Les paramètres IP du PC MANAGER :

Dans l'onglet **"DESKTOP > IP configuration"**, nous activons le DHCP.

2. L'interface de gestion du WLC :

Dans l'onglet **"CONFIG > Management"** , nous définissons les paramètres IP statiques. voir la FIGURE 4.10

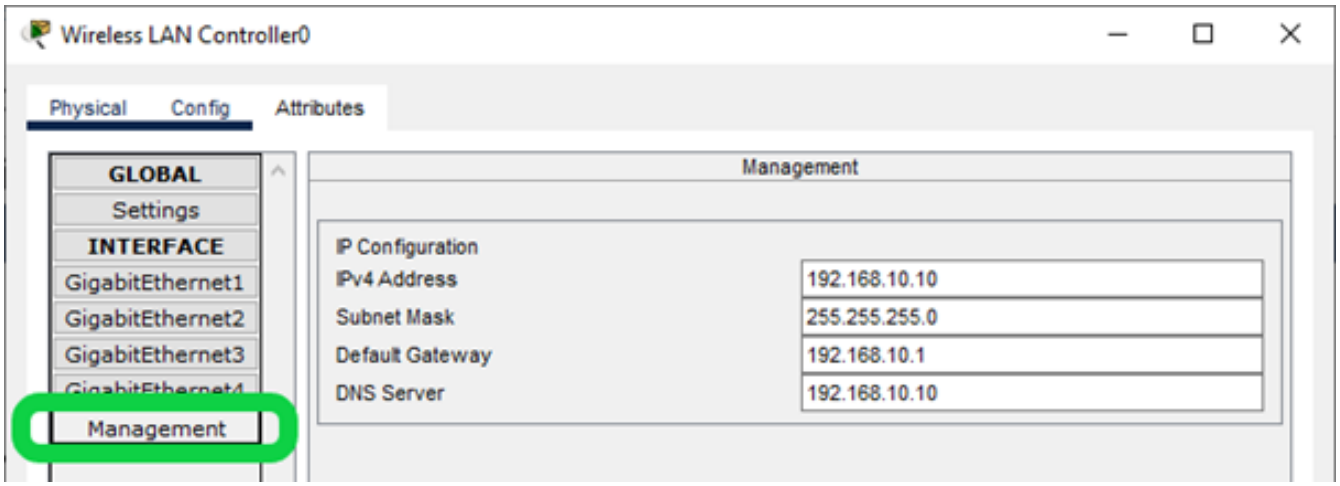

FIGURE 4.11 – Configuration de l'interface Management du WLC

— **Création d'un compte Administrateur :** Une fois que vous avez saisi l'adresse IP du contrôleur WiFi (WLC) dans le navigateur Web du PC MANAGER, l'interface graphique s'affiche, vous invitant à créer un nom d'utilisateur et un mot de passe (complexe) pour l'administrateur. FIGURE 4.11

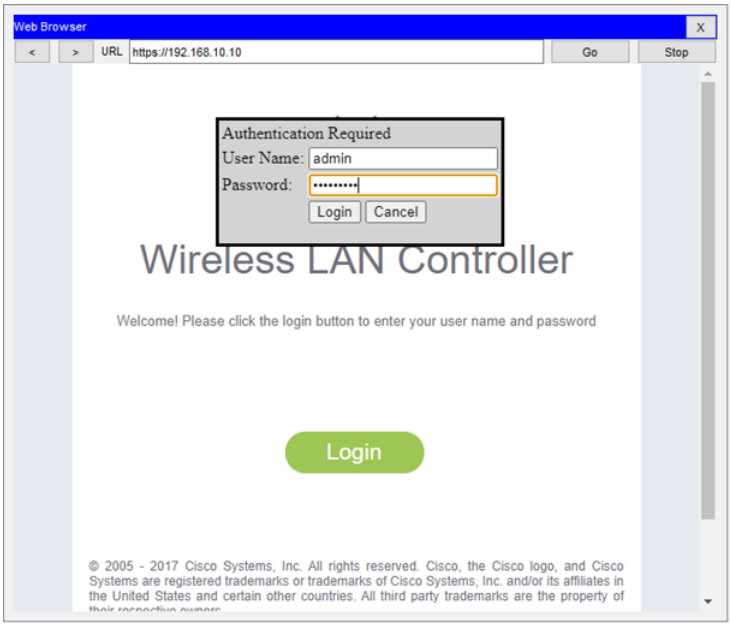

FIGURE 4.12 – Création d'un administrateur sur le WLC

Ensuite, nous saisissons attentivement les informations requises telles que mentionnées précédemment, puis nous les appliquons.

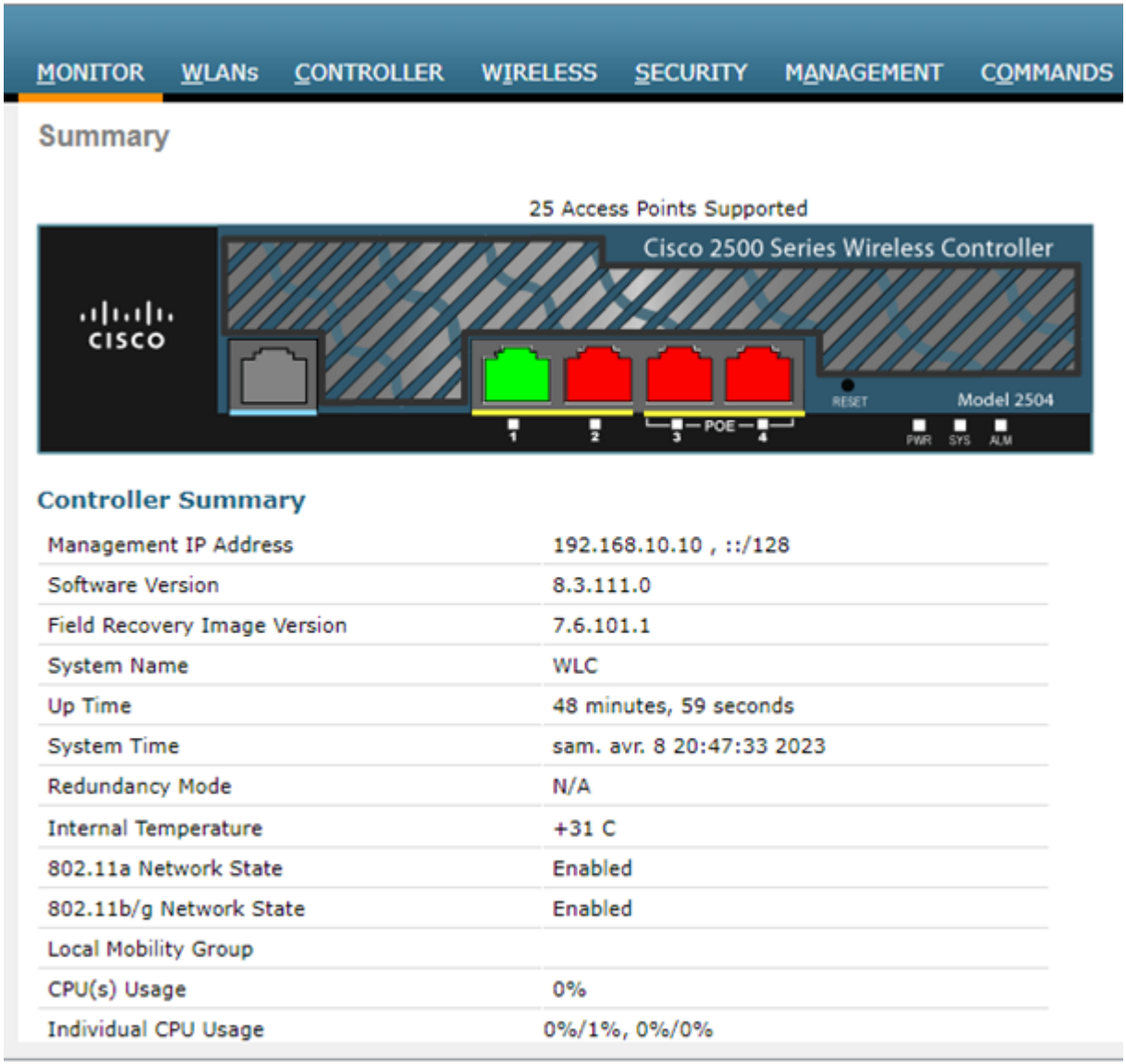

FIGURE 4.13 – l'interface graphique de contrôleur wifi

— **Centralisation des points d'accès :** Voici les étapes essentielles pour centraliser tous les points d'accès sur un contrôleur :

1. On va assurer que le contrôleur WiFi et tous les points d'accès sont connectés et fonctionnent correctement.
2. On accède à l'interface de gestion du contrôleur WiFi via un navigateur Web en utilisant son adresse IP (@IP 192.168.10.10) de gestion.
3. Ensuit on connecte à l'interface de gestion en utilisant les informations d'iden-

tification de l'administrateur (Nom d'utilisateur et le Mot de passe).

4. Apres on recherche un onglet dédié à la gestion des points d'accès.
5. On sélectionne l'option d'ajout ou de recherche des points d'accès disponibles.
6. Le contrôleur WiFi détectera et affichera la liste des points d'accès disponibles sur le réseau.
7. On sélectionne les points d'accès qu'on vous souhaite centraliser sur le contrôleur.
8. Confirme et enregistre les modifications.

Après avoir suivi ces étapes essentielles, les points d'accès sélectionnés seront centralisés et gérés par le contrôleur WiFi.

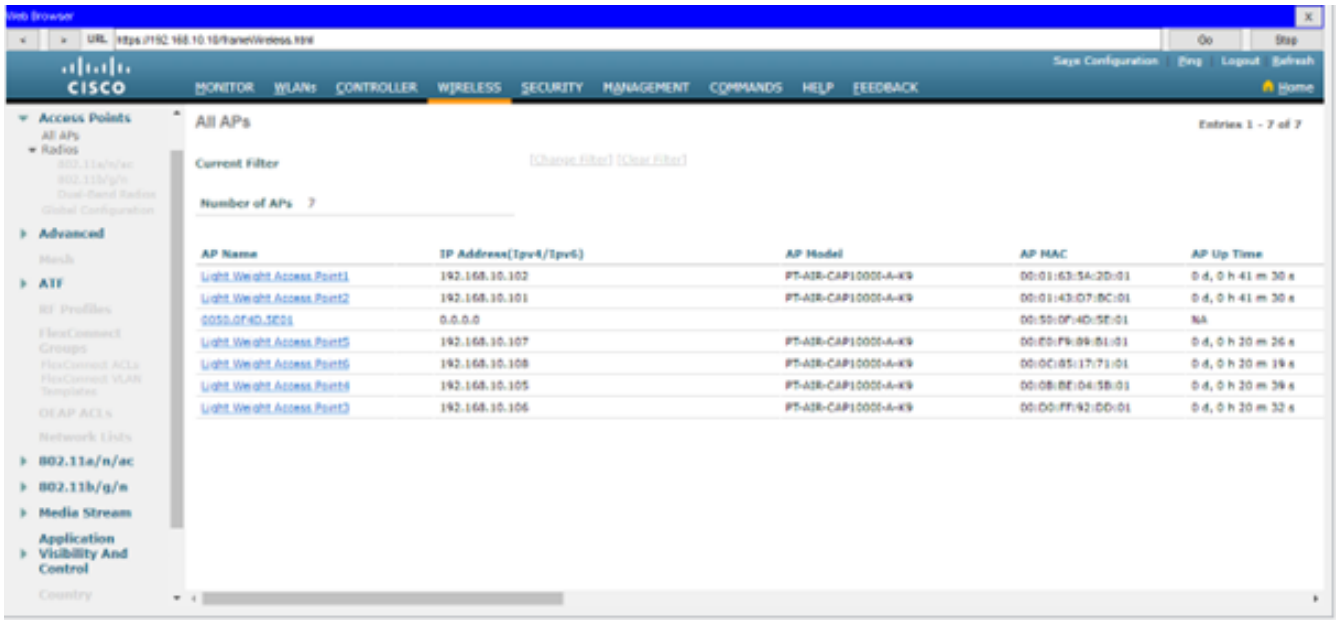

FIGURE 4.14 – Centraliser les points d'accès

4.5 Configuration des serveurs

4.5.1 Configuration d'active directory

a) Installation du rôle Active Directory : L'installation du rôle Active Directory dans un environnement de sécurité des réseaux Wi-Fi permet une gestion centralisée des utilisateurs, une authentification sécurisée, un contrôle d'accès basé sur les rôles et la gestion des certificats,cela contribue à renforcer la sécurité du réseau et à assurer une gestion efficace des utilisateurs et de leurs droits d'accès.

1. Sur un serveur Windows Server on va ouvrez le Gestionnaire de serveur.
2. On Clique sur "Ajouter des rôles et fonctionnalités".
3. On va Sélectionnez le serveur sur lequel on vous installer Active Directory
4. On Coche la case "Services de domaine Active Directory".
5. Suivez les étapes de l'assistant d'installation pour terminer l'installation du rôle.
6. Les rôles installer sont :Services AD DS , Serveur DNS , Serveur DHCP , Services de certificats Active Directory , Services de stratégie et d'accès réseaux , accès à distance .

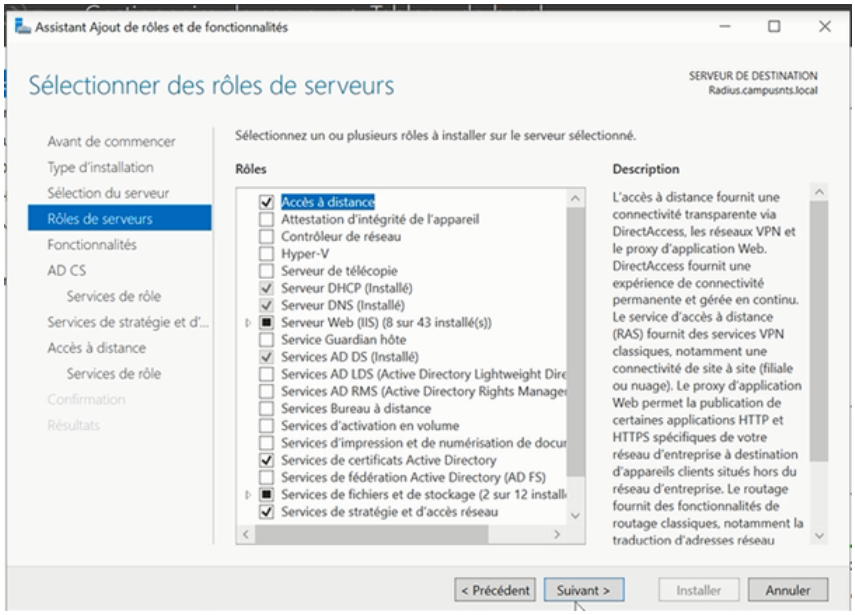

FIGURE 4.15 – Installation des rôles AD

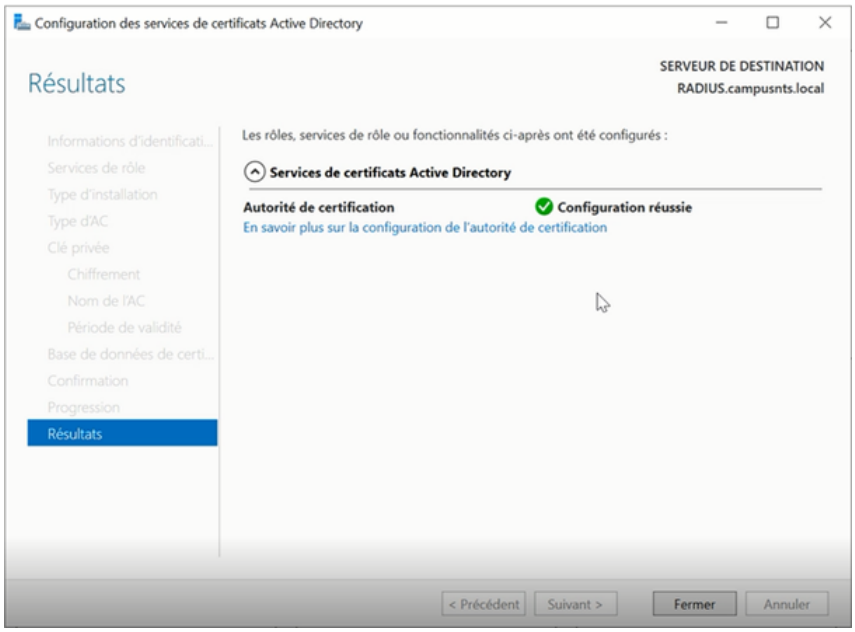

FIGURE 4.16 – Installation réussite

Une fois les rôles Active Directory sont bien installés on va passer à la Configuration.

4.5.1.1 Configuration du serveur DHCP

Lors de la configuration du serveur DHCP, il est nécessaire de spécifier un nom et un intervalle d'adresses, comme illustré dans la figure ci-dessous. FIGURE 4.16 FIGURE 4.17

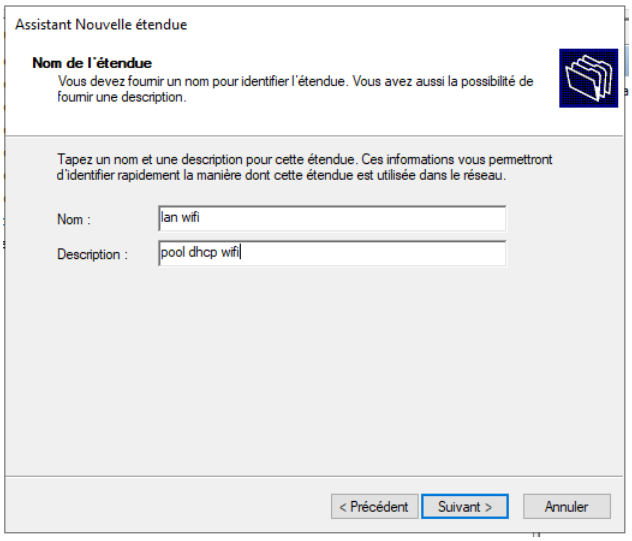

FIGURE 4.17 – Nom de l'étendue

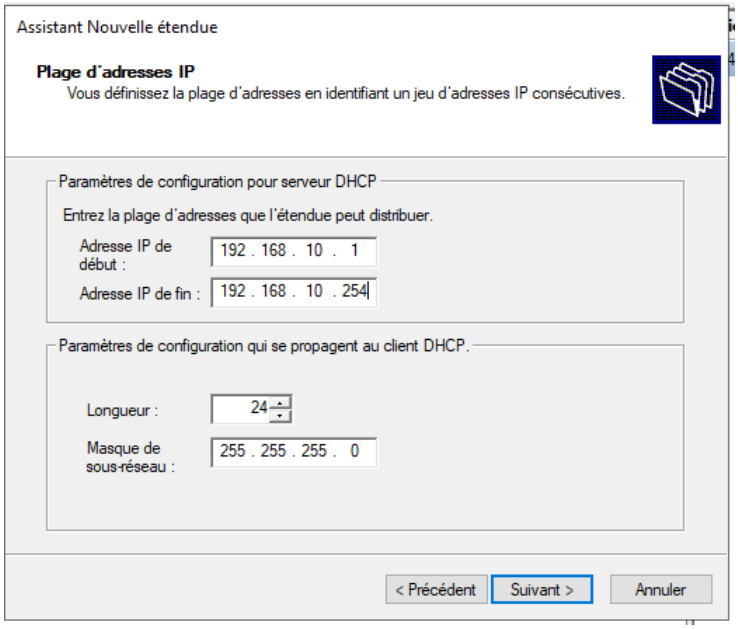

FIGURE 4.18 – Configuration d'une plage d'adresse du serveur DHCP

L'étape suivante consiste à exclure une plage d'adresses. Nous avons réservé l'intervalle d'adresses 192.168.10.1 à 192.168.10.50. Tous les PC appartenant au VLAN 10 se voient attribuer une adresse IP dans l'intervalle 192.168.10.51 à 192.168.10.254, comme indiqué dans les deux figures ci-dessus. FIGURE 4.18 FIGURE 4.19

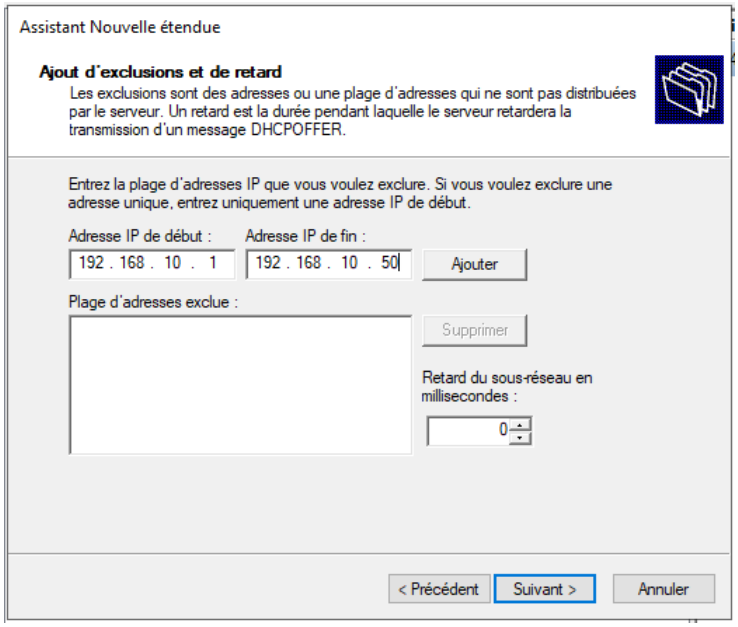

FIGURE 4.19 – Exclusion d'adresse

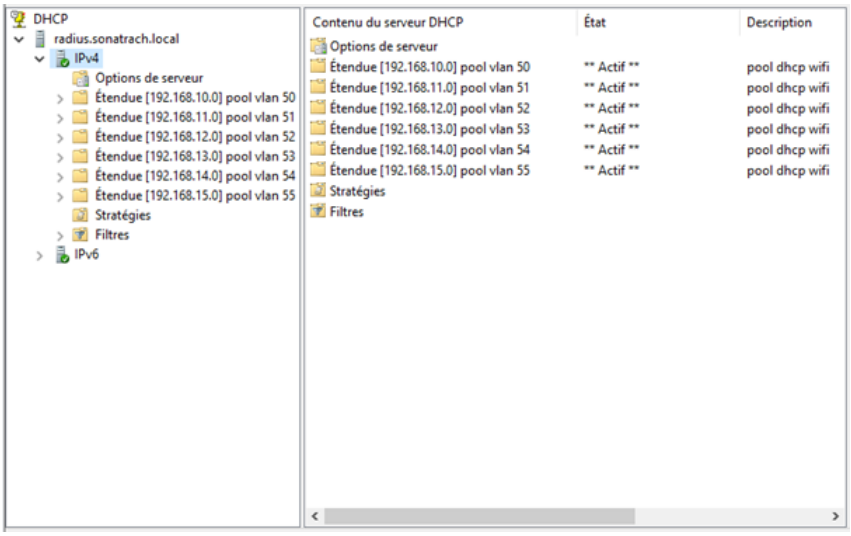

FIGURE 4.20 – Ensemble des plages d'adressage

4.5.1.2 Utilisateur et ordinateur Active Directory

A. **Création de l'unité d'organisation dans Active Directory :** Afin d'assurer la flexibilité, nous avons choisi de mettre en place des unités d'organisation. Nous avons créé une unité d'organisation centrale appelée "Sonatrach Central Alger". À l'intérieur de "Sonatrach Central Alger", nous avons créé une unité d'organisation spécifique nommée "Sonatrach Bejaïa : Ordinateur-Wifi-Sonatrach", qui contient deux autres unités d'organisation, à savoir "Ordinateurs" et "Utilisateurs".

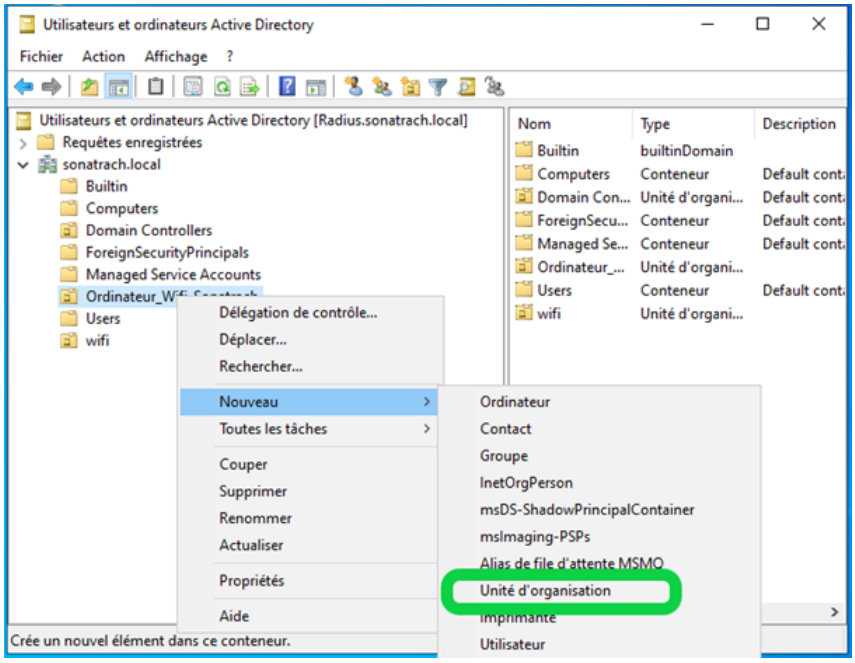

FIGURE 4.21 – Création d'une unité d'organisation dans Active Directory

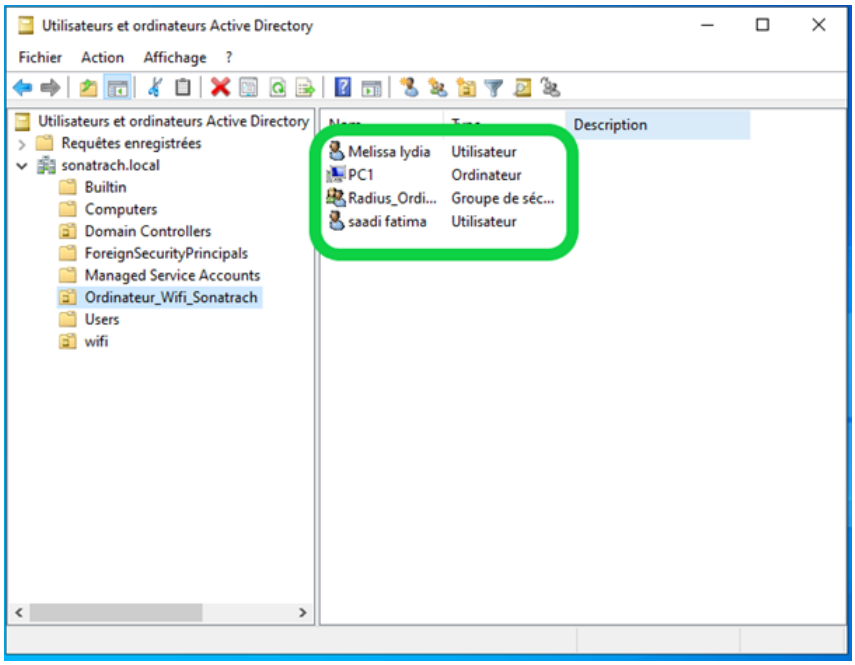

FIGURE 4.22 – Les unités d'organisations créer

B. **Création des groupes Radius :** Une fois l'unité d'organisation "Utilisateur" créée, nous allons procéder à la création de groupes et d'utilisateurs à l'intérieur de celle-ci.

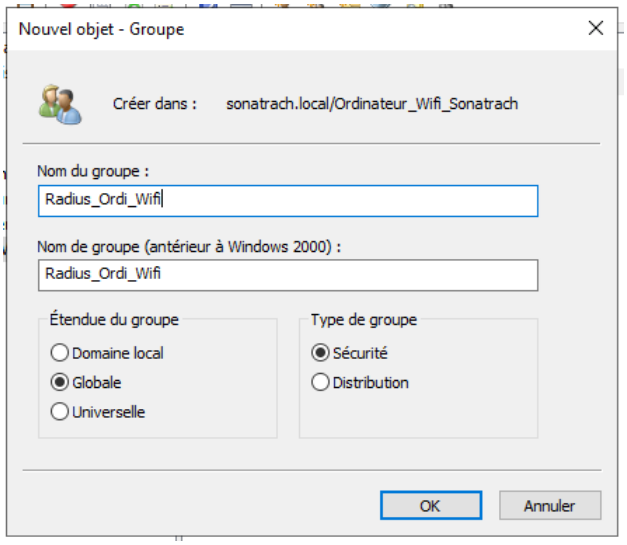

FIGURE 4.23 – Création d'un groupe dans Active Directory

C. **Création d'utilisateur dans Active Directory :** Pour créer un utilisateur dans Active Directory, il vous suffit de faire un clic droit sur l'unité d'organisation "Utilisateur", puis de sélectionner "Nouveau" et "Utilisateur".

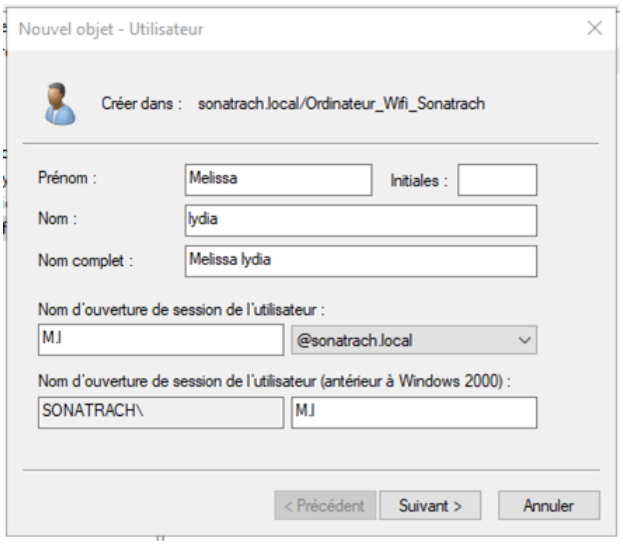

FIGURE 4.24 – Création d'un utilisateur dans Active Directory

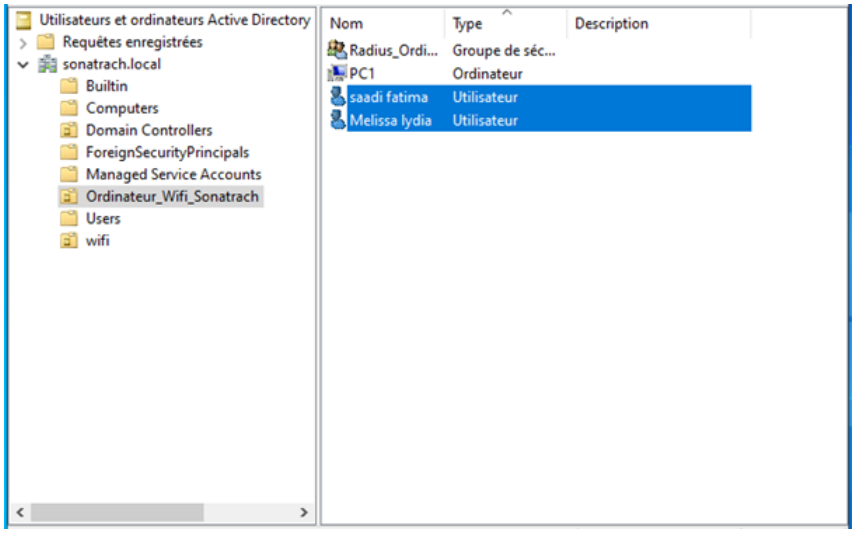

FIGURE 4.25 – les utilisateurs crées

4.5.1.3 Gestion des stratégies de groupe ‘’GPO”

A. **Créations d’une stratégie de groupe d’objet (GPO) :** Dans cette étape, nous allons créer une stratégie de groupe (GPO) appelée "Régles-Radius" et l’appliquer à l’unité d’organisation "Ordinateur".

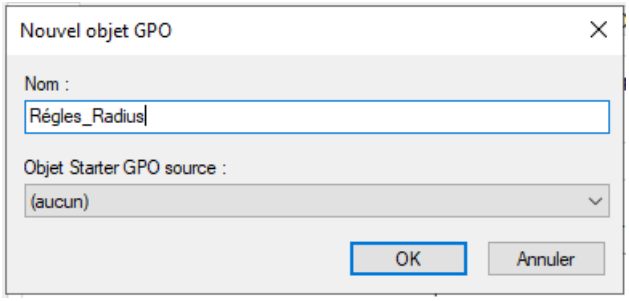

FIGURE 4.26 – Création d’une nouvelle GPO

Dans la FIGURE 4.27 on voit bien que la GPO a été créé dans l’unité d’organisation Ordinateur.

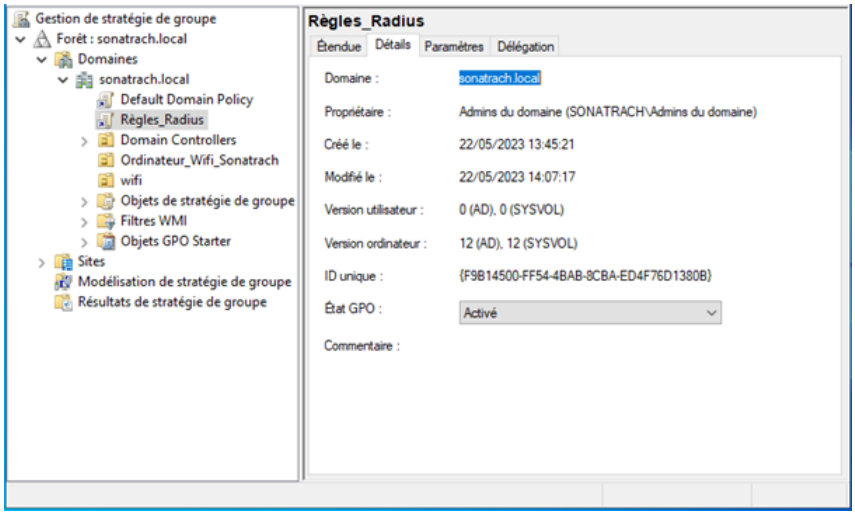

FIGURE 4.27 – GPO Régles-Radius

4.5.1.4 Serveur NPS (Network Policy Server)

Dans notre travail, le serveur NPS (Network Policy Server) est utilisé comme serveur RADIUS. Lorsque le serveur NPS est configuré en tant que serveur RADIUS, il prend en charge les fonctions d'authentification, d'autorisation et de gestion des demandes de connexion pour le domaine. Ainsi, le serveur NPS joue un rôle clé dans le processus global de gestion des connexions. Les étapes sont la suivante :

1. **Inscrire NPS dans active directory :** Afin que le serveur NPS puisse accéder aux informations d'identification des utilisateurs finaux stockées dans Active Directory, il est nécessaire d'enregistrer le serveur NPS dans Active Directory. Ce processus d'enregistrement établit la connexion entre le serveur NPS et Active Directory, permettant ainsi au serveur NPS d'avoir accès aux informations d'identification nécessaires pour l'authentification et l'autorisation des utilisateurs.

FIGURE 4.28 – Inscrire NPS dans AD

2. **Création des clients radius :**Les clients RADIUS jouent un rôle d'intermédiaire entre le serveur RADIUS et les clients (utilisateurs). Ils agissent en tant que passerelle qui transmet les demandes d'authentification et d'autorisation des clients au serveur RADIUS, et renvoient les réponses correspondantes du serveur RADIUS aux clients.

   Pour créer des clients RADIUS, il vous suffit de cliquer avec le bouton droit sur "Client RADIUS" et de sélectionner l'option "Ajouter". Ensuite, on va saisir un nom, une adresse IP et une clé partagée pour le client RADIUS.

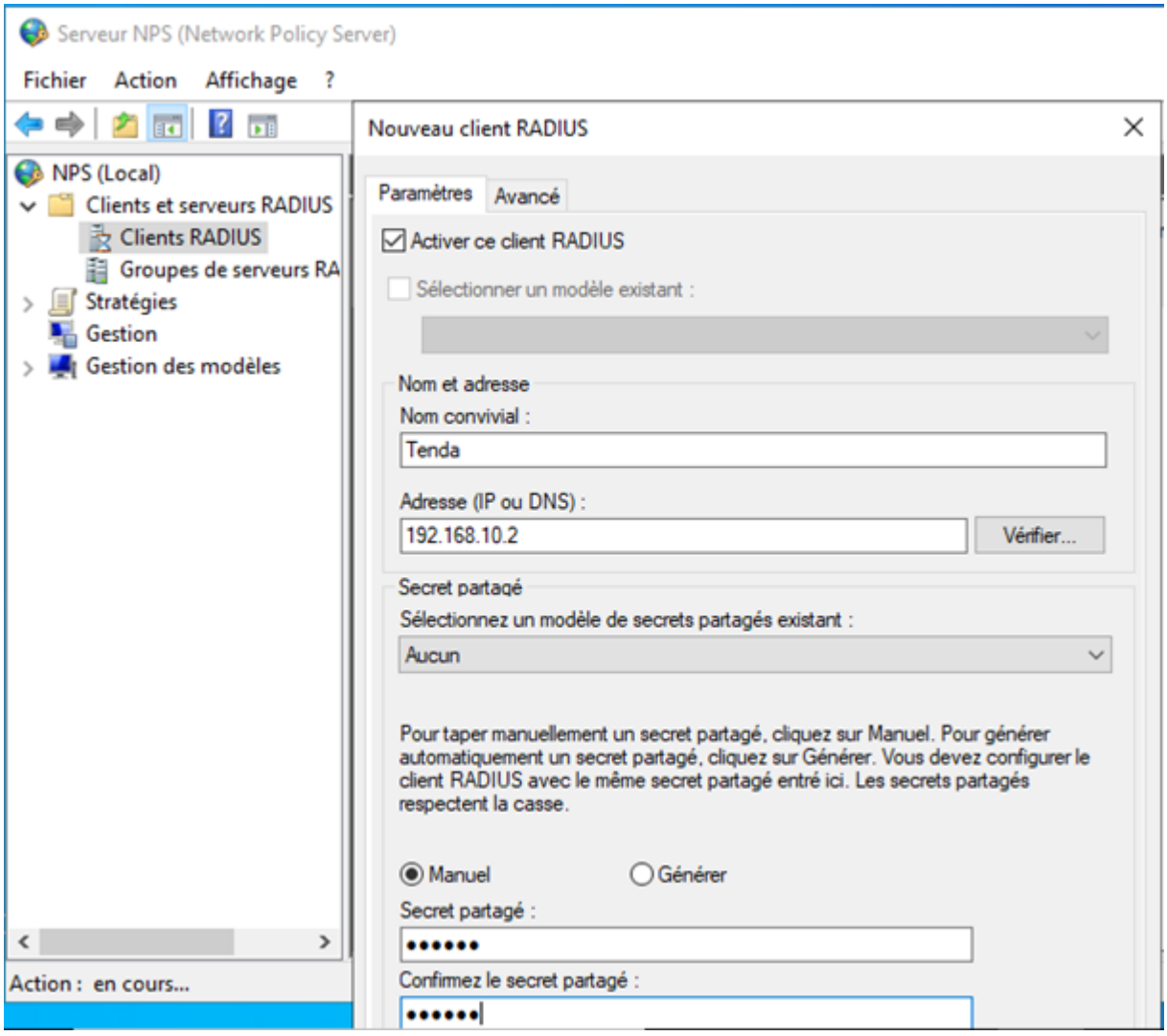

FIGURE 4.29 – Création d'un client radius

3. **Configuration de la 802.1x :** Pour configurer la norme 802.1X, vous pouvez suivre ces étapes :

   a. Cliquez sur NPS (Network Policy Server) pour accéder à la console de configuration.

   b. Choisissez le scénario de configuration correspondant à vos besoins : "Serveur RADIUS pour la connexion câblée ou sans fil 802.1X".

   c. Cliquez sur "Configurer 802.1X" pour accéder aux paramètres de configuration de la norme 802.1X.

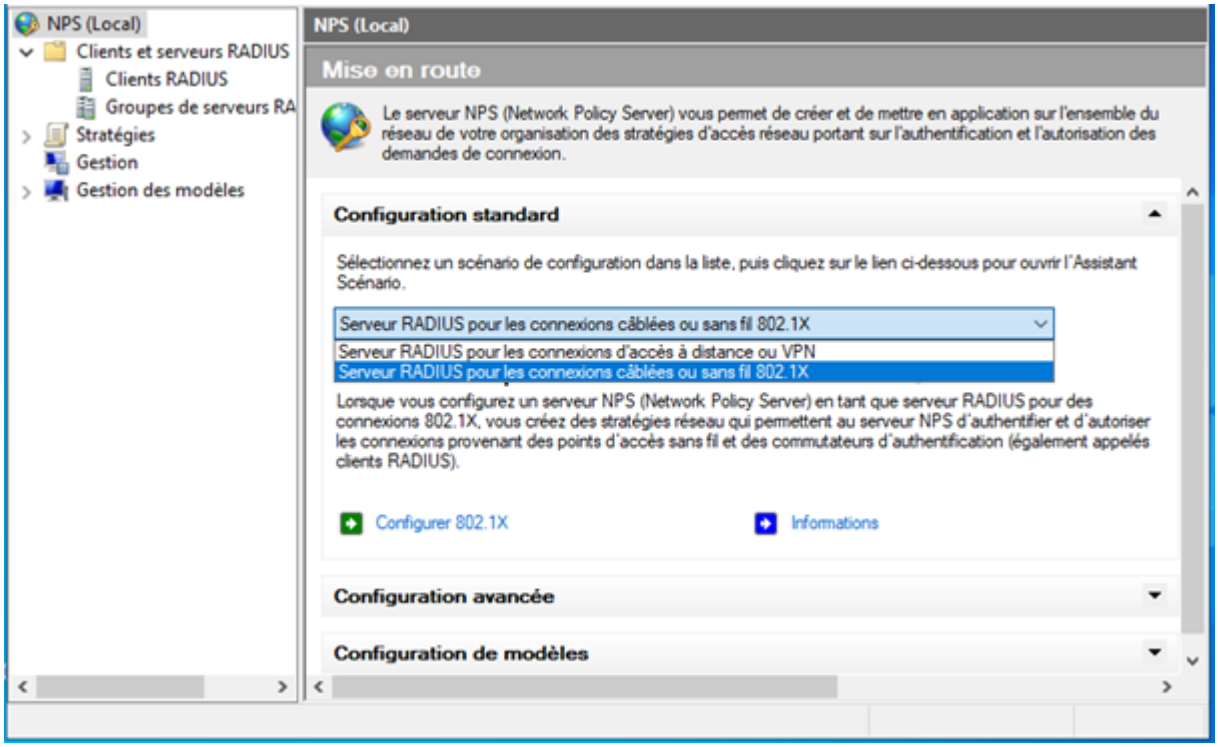

FIGURE 4.30 – Choix de la configuration réseaux

Le type d'authentification utilisé est PEAP, comme indiqué dans la figure affichée.

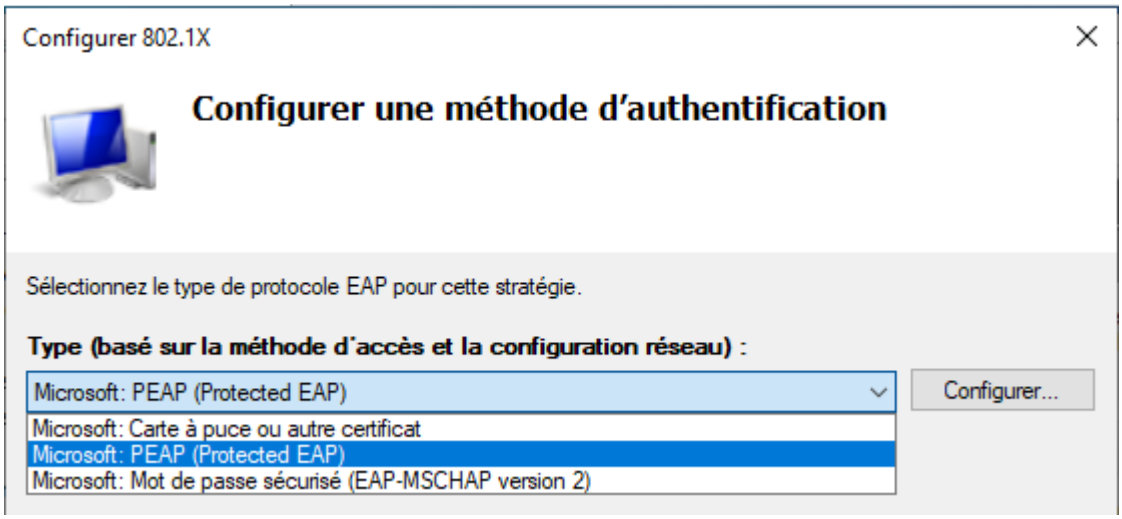

FIGURE 4.31 – type d'authentification

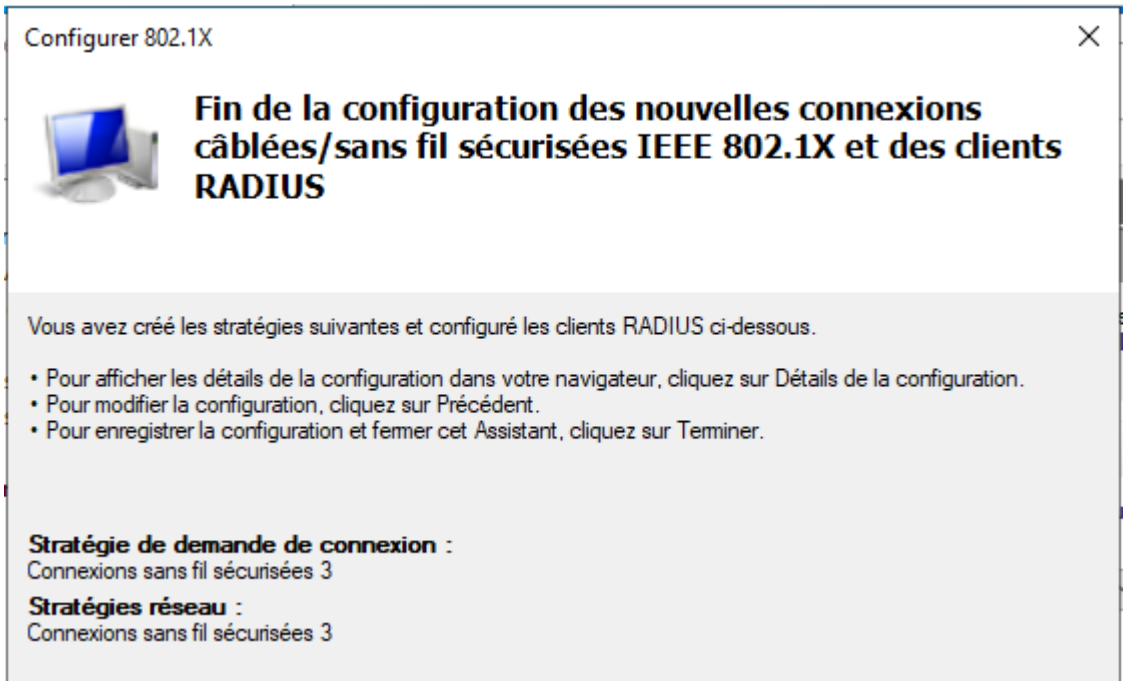

FIGURE 4.32 – la stratégie crée

4. **Propriétés de la connexion sans fil sécurisées :** Après avoir créé la stratégie (Connexions Sans fil sécurisé), on va vérifier la Stratégie réseaux :

   — **état de la stratégie :**Si la stratégie est activée, le serveur NPS l'évalue lors de l'autorisation. En revanche, si elle est désactivée, le serveur NPS ne procède pas à son évaluation.

   — **Autorisation d'accès :** Lorsque la demande de connexion satisfait aux conditions et contraintes de la stratégie réseau, celle-ci a la possibilité d'accorder ou de refuser l'accès.

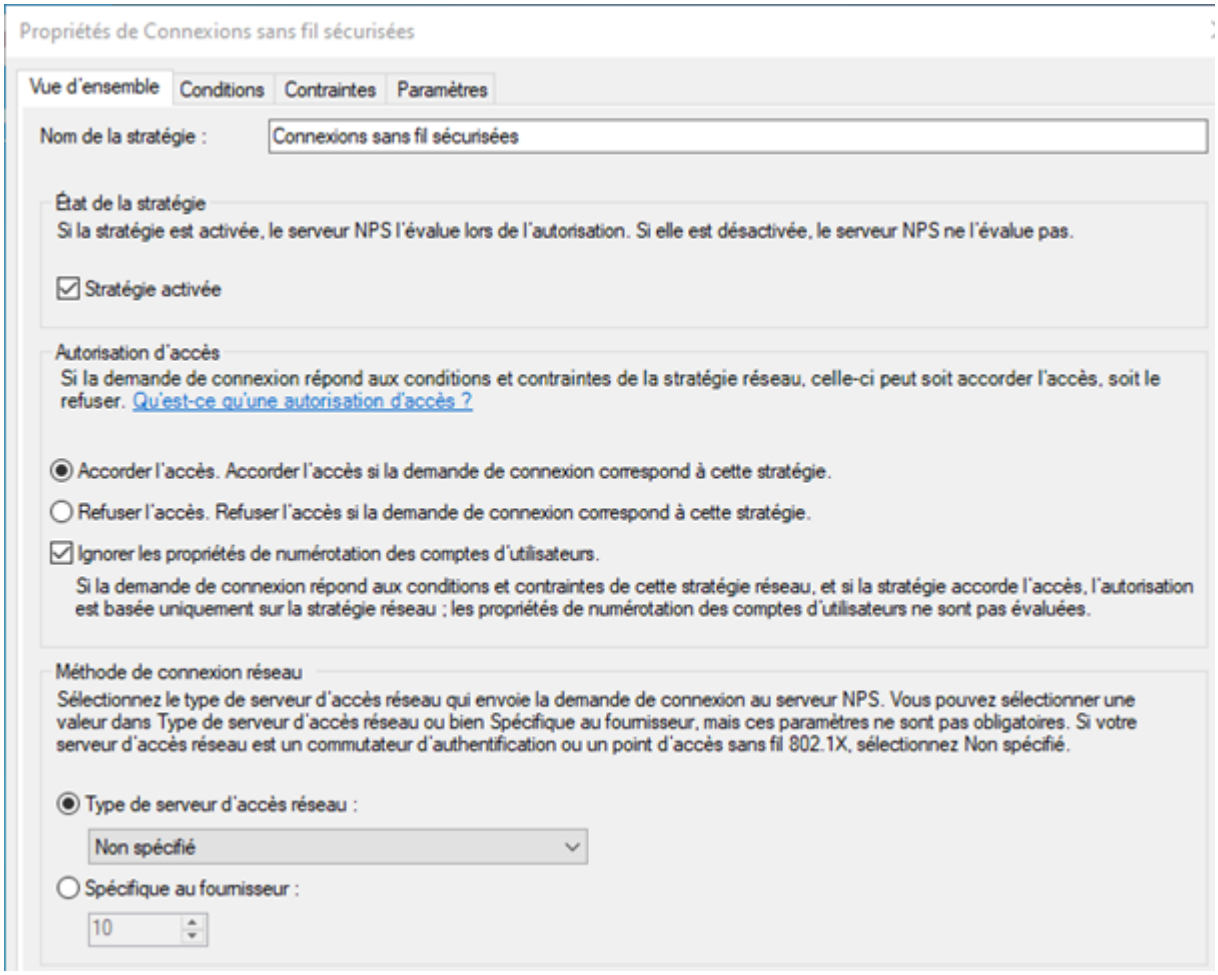

FIGURE 4.33 – Vue globale de la stratégie

Et pour les Contraintes on a choisi le PEAP (Protocole EAP) comme méthode d'authentification FIGURE 4.34 .

Seuls les clients utilisant les méthodes spécifiées pour s'authentifier auront accès autorisé.

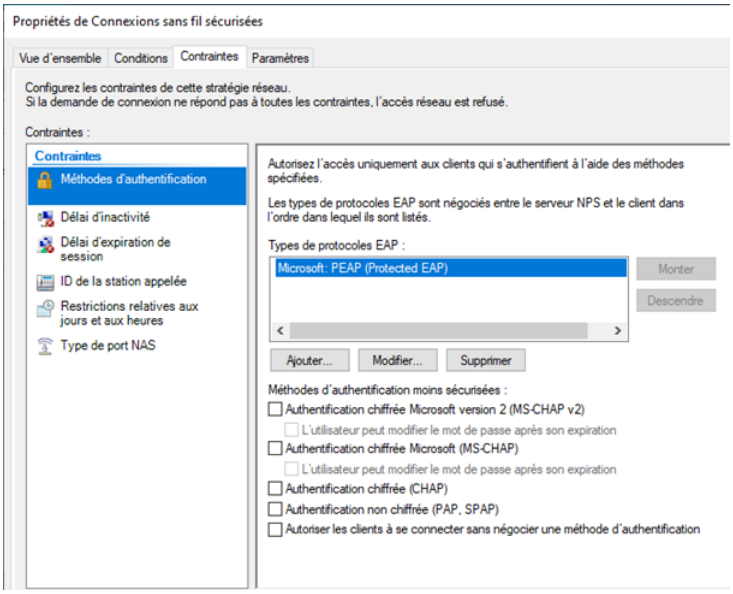

FIGURE 4.34 – Condition de la stratégie

4.5.1.5 Autorité de certification

A. **Création des groupes Certificats :**Dans le cadre de notre travail, nous allons mettre en place deux groupes de certificats distincts : un groupe de certificats pour le serveur et un autre groupe de certificats pour les ordinateurs. FIGURE 4.35

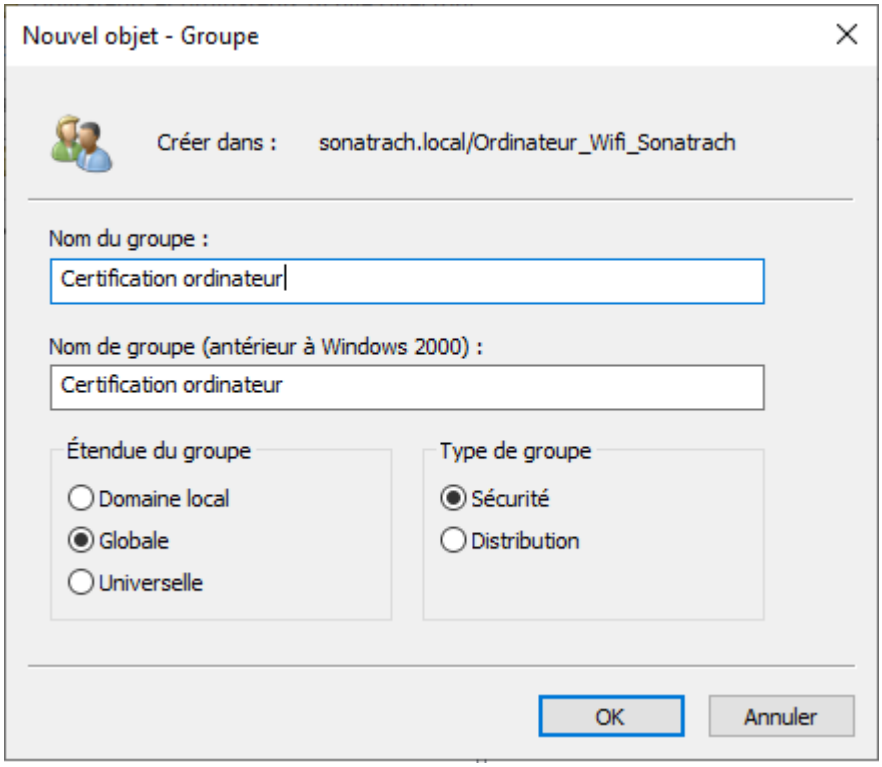

FIGURE 4.35 – Création du groupe certificat ordinateur

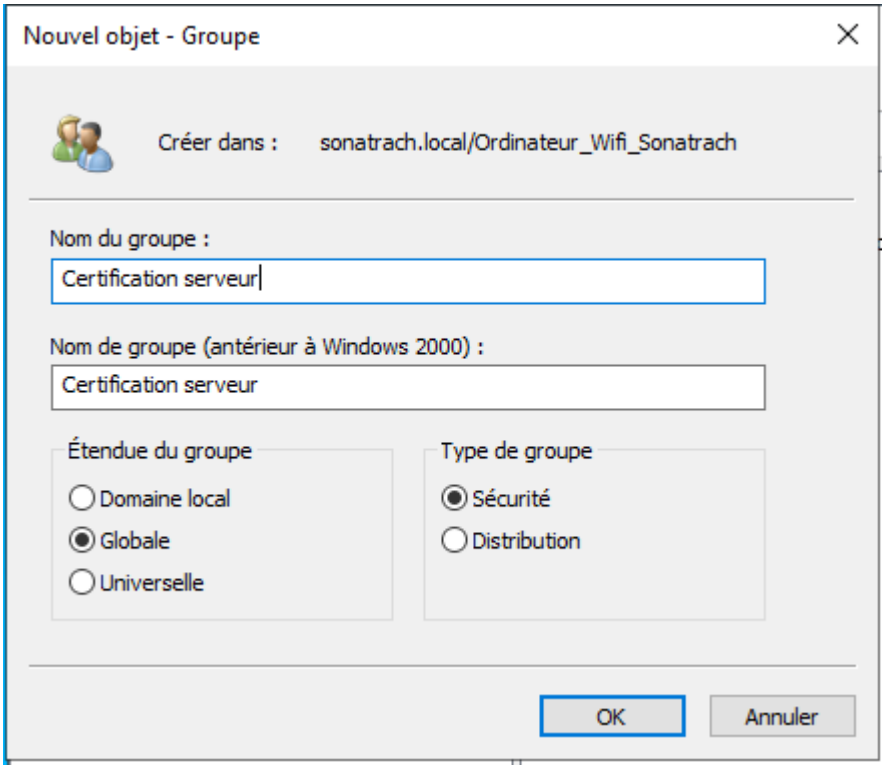

FIGURE 4.36 – Création du groupe certificat server

B. **Certificat serveur :**Dans le dossier modèle de certificat, nous avons effectué une duplication du serveur RAS (Remote Access Server) et IAS (Internet Authentication Service), que nous avons ensuite renommé "Certificate Server".

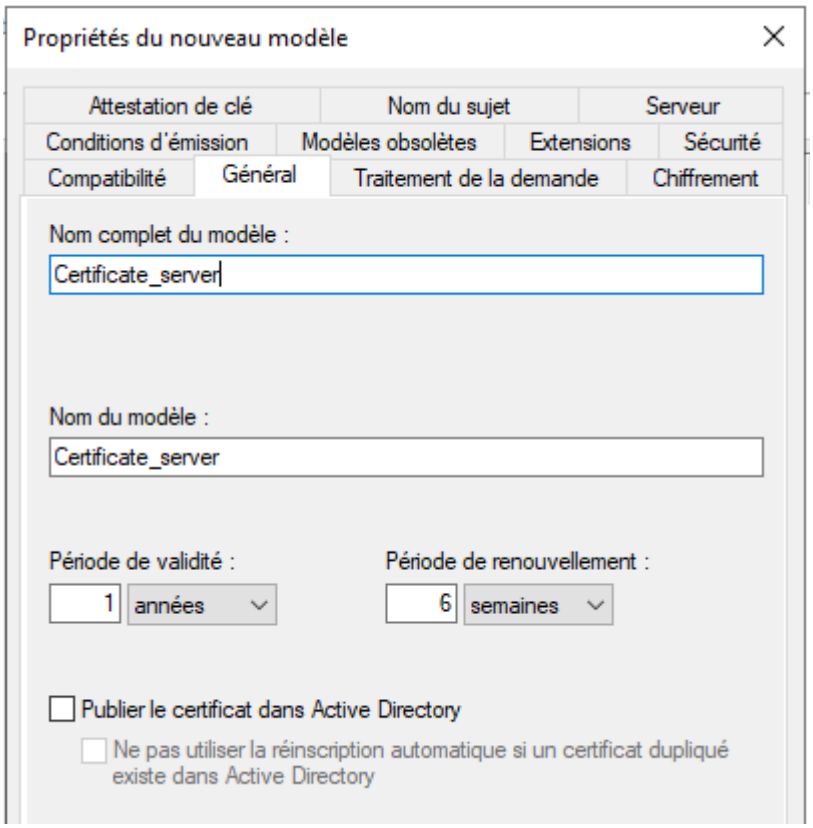

FIGURE 4.37 – Vue générale de certificat server

C. **Certificat Pc (Station de travail) :** Pendant cette étape, nous avons réalisé une duplication du modèle "Authentification de station de travail" que nous avons ensuite renommé "Certificate ordinateurs".

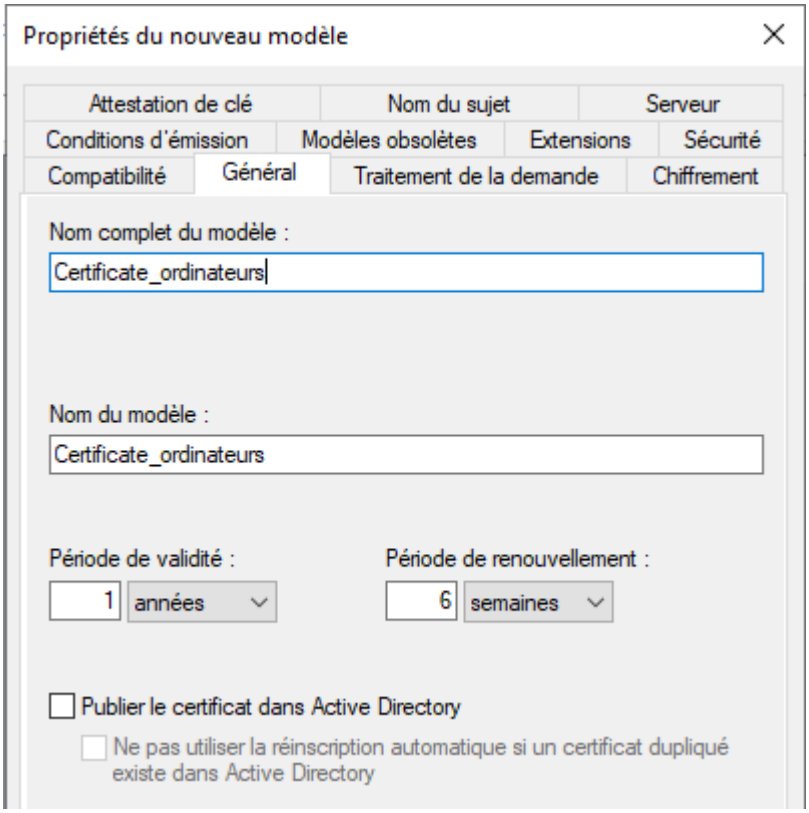

FIGURE 4.38 – Vue général du modèle certificat pour les stations de travaille

D. **Activer la distribution du certificat automatiquement :** Nous allons procéder à l'activation de la distribution automatique des certificats, de sorte qu'une certification soit automatiquement délivrée pour chaque ordinateur. FIGURE 4.39

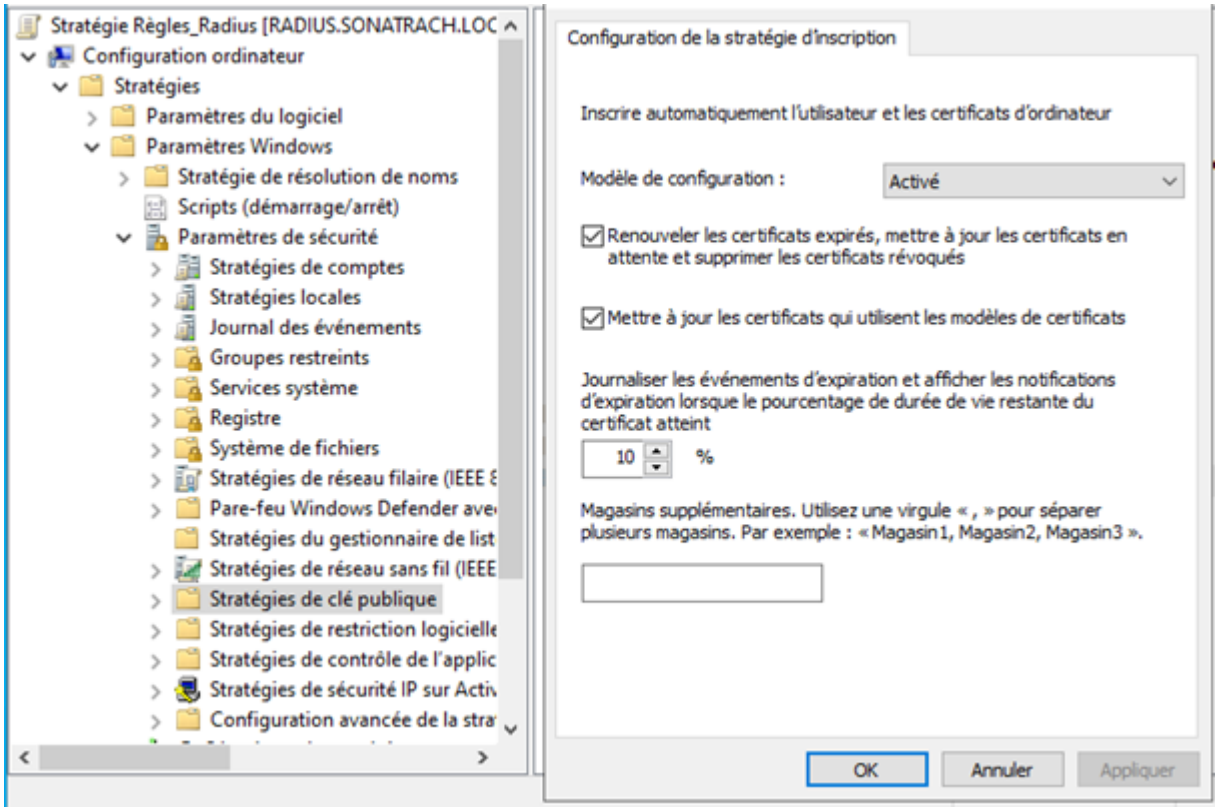

FIGURE 4.39 – Activation automatique des certificats

4.6 Configuration de base sur firwall

4.6.1 Configurations des interfaces

On va attribut port 1 pour internet, port 10 pour managment , port 2 pour les intervlan.

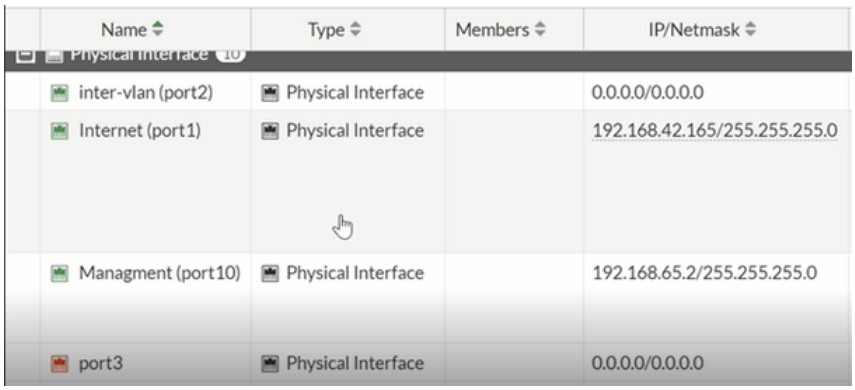

FIGURE 4.40 – configuration des interfaces

4.6.2 Creation des vlan

Sur interfaces, on clique sur Create New puis interface

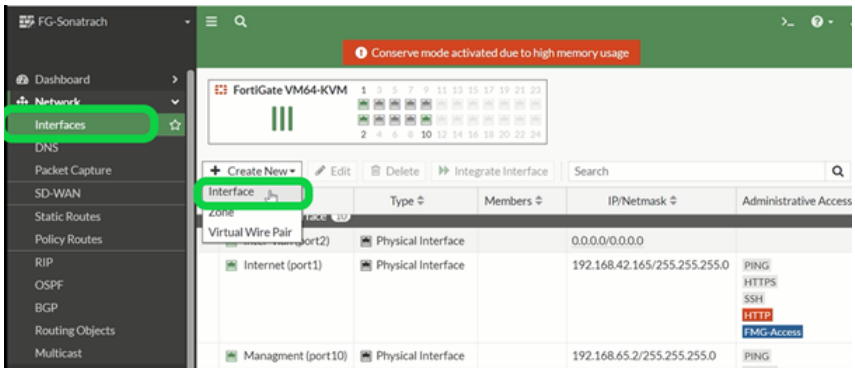

FIGURE 4.41 – Création des interfaces

Dans la configuration du VLAN, vous devrez spécifier un identifiant unique pour le VLAN (ID VLAN), ainsi qu'un nom ou une description pour le VLAN.
Vous pouvez également définir les paramètres spécifiques pour le VLAN, tels que la plage d'adresses IP, le masque de sous-réseau, les paramètres de routage, etc ...

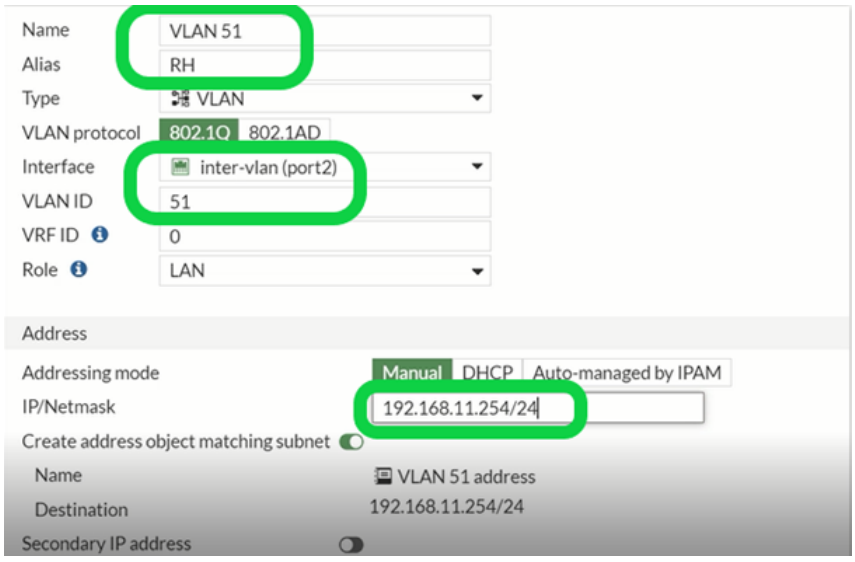

FIGURE 4.42 – configuration de vlan RH

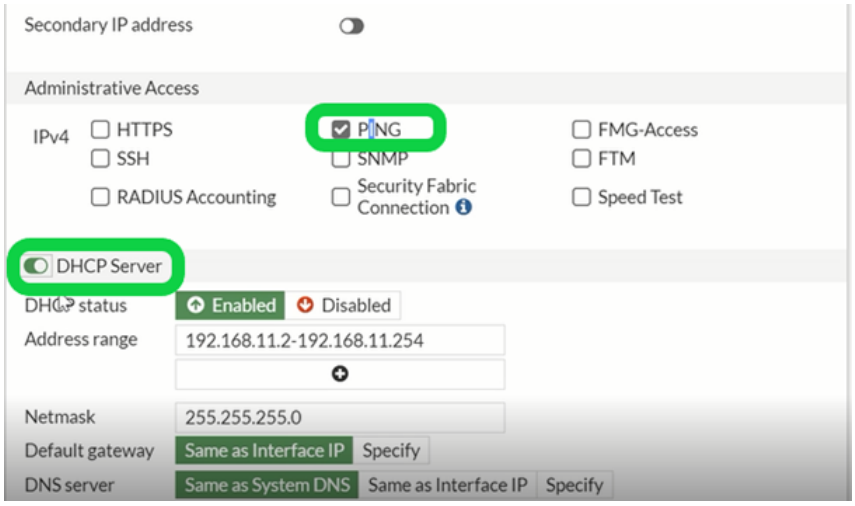

FIGURE 4.43 – attribution des droit administatif au vlan RH

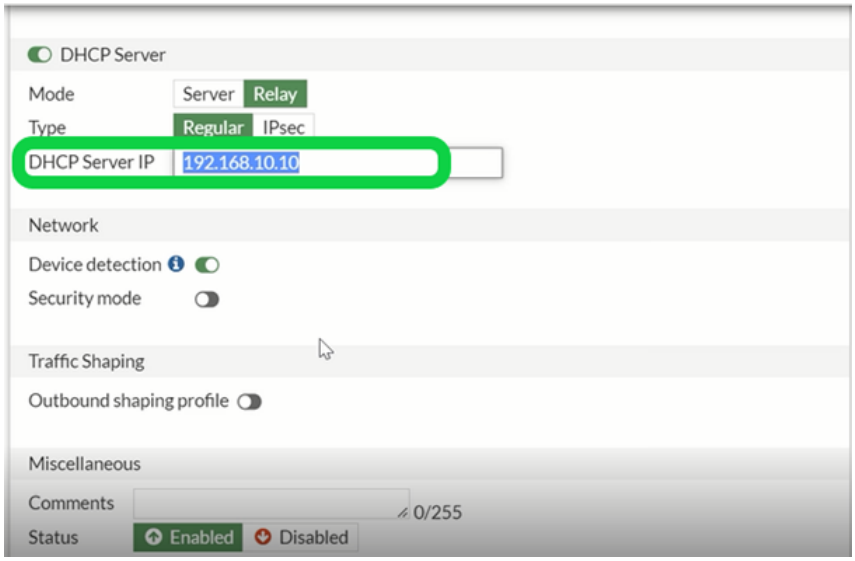

FIGURE 4.44 – attribution de l'adresse server au vilan RH

On va suivre les étapes précédentes pour créer d'autres VLAN.

Voila la FIGURE 4.45 montre les vlans déja céer.

FIGURE 4.45 – les Vlans crée

4.6.3 Configuration du routage

A. **La création de la zone du routage :** Sur interfaces, on clique sur Create New puis Zone.

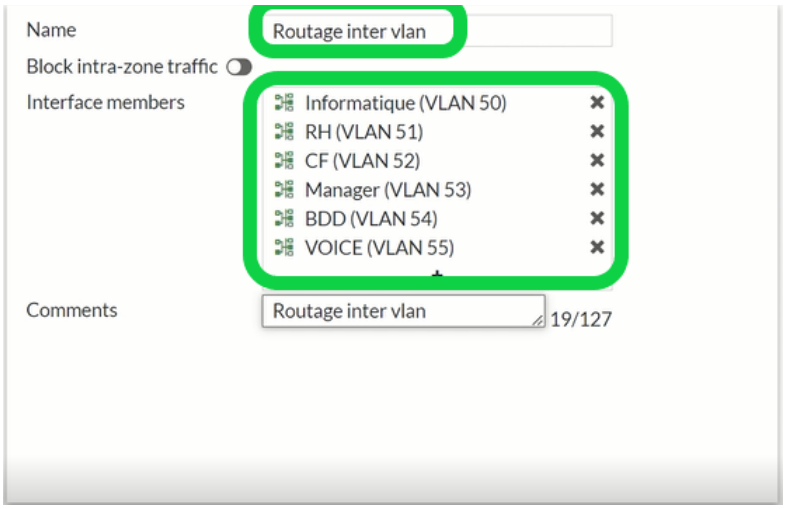

FIGURE 4.46 – la creation de la zone

Maintenant les vlan peuvent se communiquer entre eux.

B. **La création de la route statique vers internet :** Nous allons mettre en place une route statique via la passerelle (@ 192.168.42.2) pour accéder à Internet.

Sur interfaces, on clique sur Static Routes puis Create New

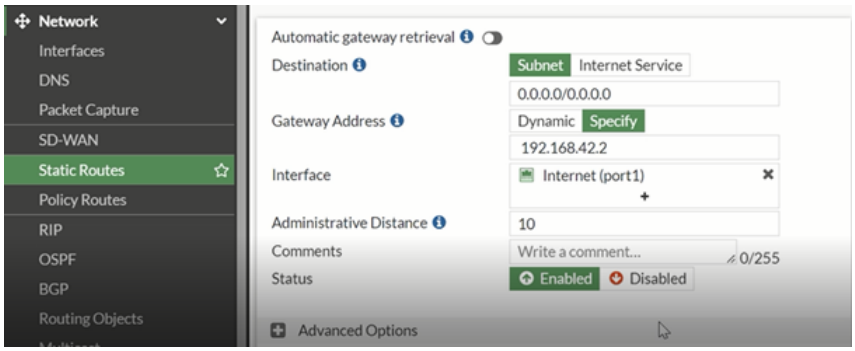

FIGURE 4.47 – La création de la route statique

Ensuit en va autoriser le trafic : **sur Policy et Objects, on clique sur Firwall Policy puis New Policy.**

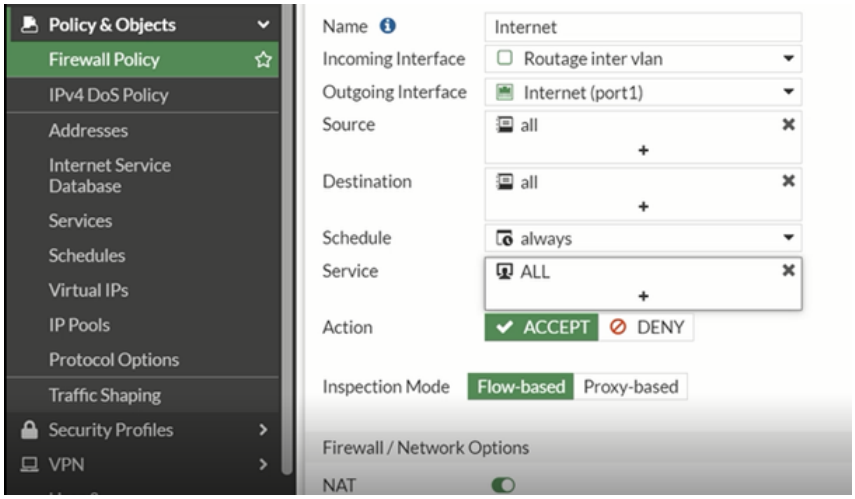

FIGURE 4.48 – Autorisation de trafic

Maintenant, ils peuvent se communiquer à internet.

4.7 Configuration du point d'accès

Premièrement on va désactiver le server DHCP.

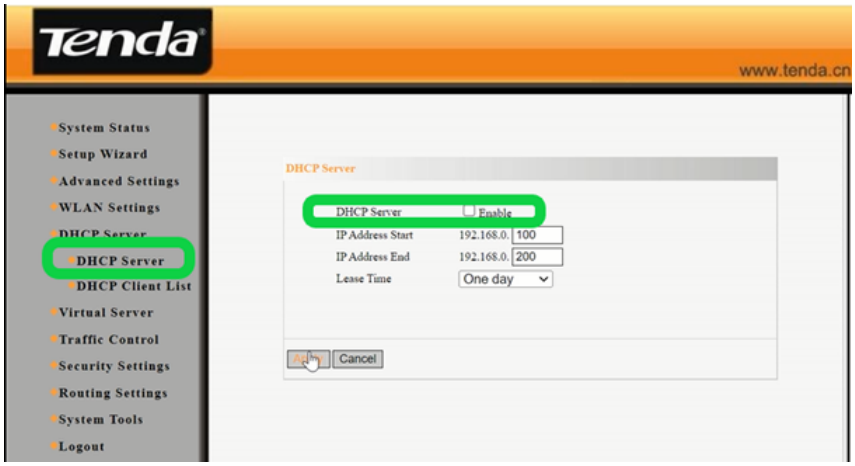

FIGURE 4.49 – La désactivation du DHCP server

En suit on va changer l'adresse de point d'accès : sur Advanced Setting on clique sur LAN Setting

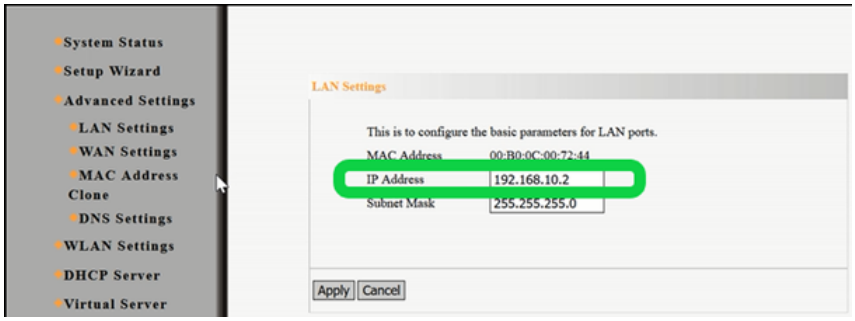

FIGURE 4.50 – L'atribution de l'adresse ip au AP

Apres on passe à la partie de sécurité : on active le mode de sécurité **WPA2-Entreprise** avec l'algorithme de chiffrement **AES**.

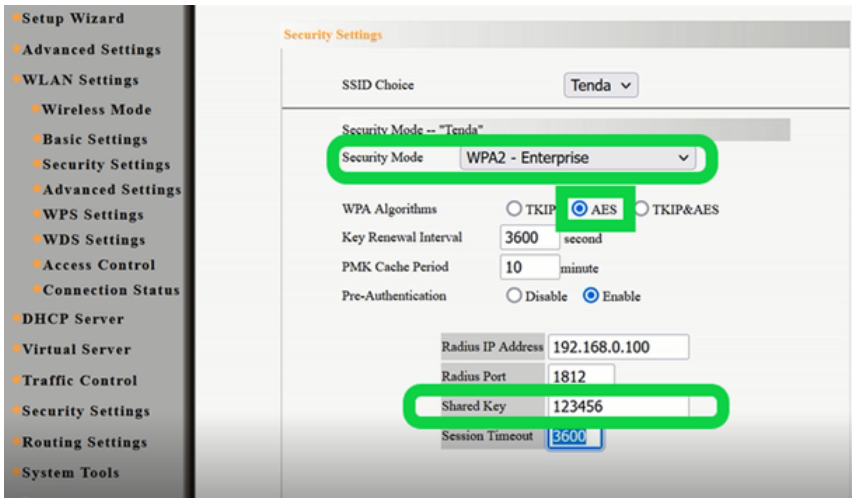

FIGURE 4.51 – L'activation du mode sécurité au AP

4.8 Les tests

4.8.1 Vérification de la création des VLANs

On utilise la commande « show vlan brief » sur chaque commutateur afin de vérifier que la configuration des VLANs a bien été distribuée par le serveur VTP voir la FIGURE 4.52.

```
Core#show  vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------------------
1    default                           active    Et1/3, Et2/0, Et2/1, Et2/2
                                                 Et2/3, Et3/0, Et3/1, Et3/2
50   informatique                      active
51   RH                                active
52   CF                                active
53   Manager                           active
54   bdd                               active
55   voicea                            active    Et3/3
99   native                            active
1002 fddi-default                      act/unsup
1003 trcrf-default                     act/unsup
1004 fddinet-default                   act/unsup
1005 trbrf-default                     act/unsup
```

FIGURE 4.52 – Vérification de la création des VLANs sur le client VTP.

4.8.2 Test DHCP

On utilise la commande « ip dhcp » sur chaque PC afin de vérifier que la configuration des addresses ip a bien été distribuée par le serveur RADIUS on affichant le resultat "DORA" voir la FIGURE 4.53

```
PC5> ip dhcp
DDD
Can't find dhcp server

PC5> ip dhcp
DORA IP 192.168.10.12/24 GW 192.168.10.1

PC5>
```

FIGURE 4.53 – Test DHCP

4.8.3 Test de connectivité

Nous allons tester la connectivité entre le serveur RADIUS et le Client RADIUS (FIGURE 4.54), et entre le serveur RADIUS et le Firewall (FIGURE 4.55) enfin entre le serveur RADIUS et le point d'acces (FIGURE 4.56) Pour cela nous allons sur l'invite commande (cmd) du serveur avec la commande (Ping adresse IP).

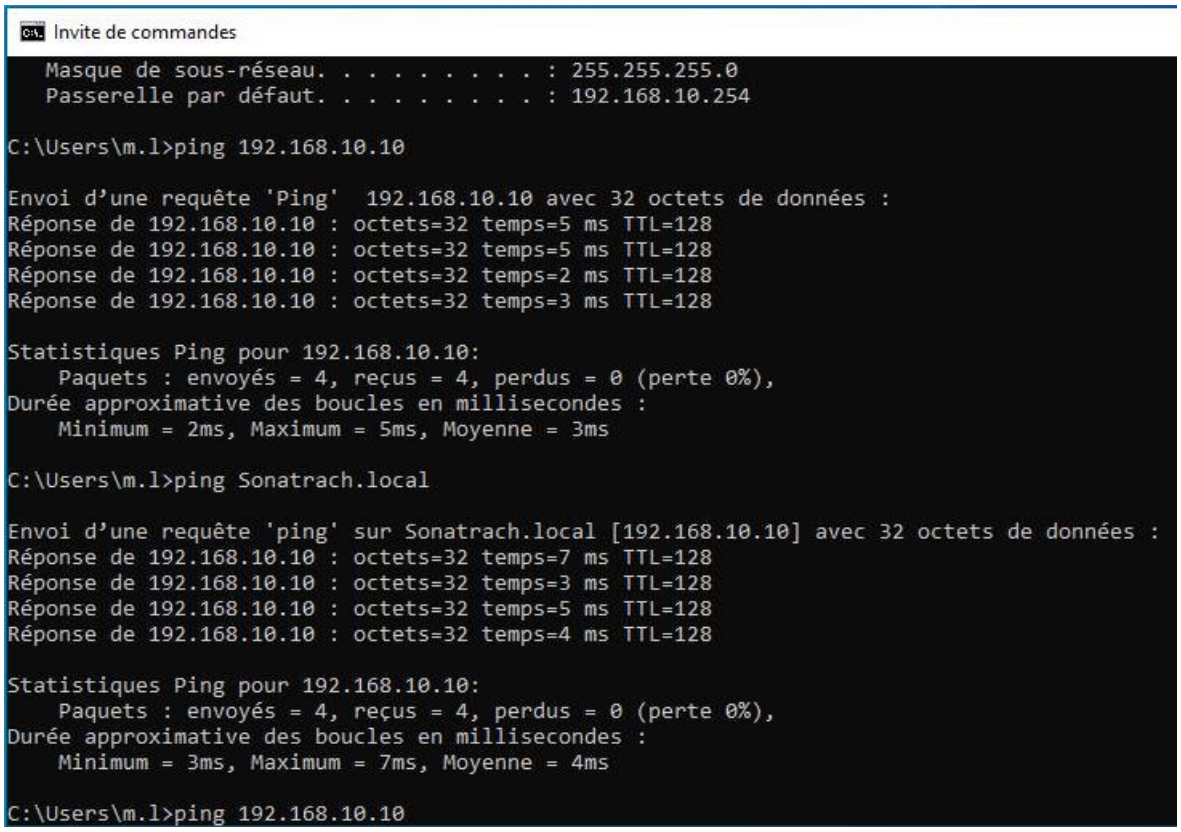

FIGURE 4.54 – Test entre le serveur et le switch client

```
FG-Sonatrack # execute ping 192.168.10.10
PING 192.168.10.10 (192.168.10.10): 56 data bytes
64 bytes from 192.168.10.10: icmp_seq=0 ttl=128 time=3.1 ms
64 bytes from 192.168.10.10: icmp_seq=1 ttl=128 time=2.1 ms
64 bytes from 192.168.10.10: icmp_seq=2 ttl=128 time=2.2 ms
64 bytes from 192.168.10.10: icmp_seq=3 ttl=128 time=2.5 ms
64 bytes from 192.168.10.10: icmp_seq=4 ttl=128 time=3.0 ms

--- 192.168.10.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.1/2.5/3.1 ms

FG-Sonatrack #
```

FIGURE 4.55 – Test entre le serveur et le Firewall

```
Invite de commandes
Microsoft Windows [version 10.0.19045.3086]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\acer>ping 192.168.10.2

Envoi d'une requête 'Ping'  192.168.10.2 avec 32 octets de données :
Réponse de 192.168.10.2 : octets=32 temps<1ms TTL=64
Réponse de 192.168.10.2 : octets=32 temps<1ms TTL=64
Réponse de 192.168.10.2 : octets=32 temps<1ms TTL=64
Réponse de 192.168.10.2 : octets=32 temps<1ms TTL=64

Statistiques Ping pour 192.168.10.2:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\acer>
```

FIGURE 4.56 – Test entre le serveur et le point d'acces

4.8.4 Test de l'authentification RADIUS

Pour l'authentification RADIUS nous avons deux cas :

L'authentification réussie : Nous allons capturer le trafic radius sur Wireshark voir la FIGURE 4.57, nous verrons que l'authentification est faite avec succés

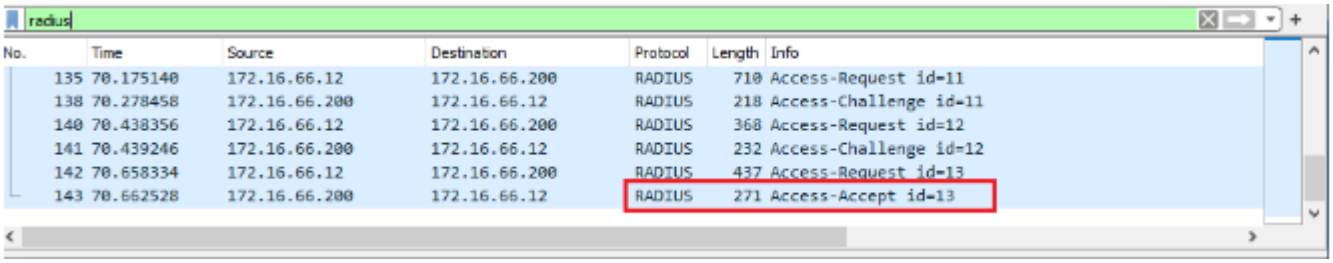

FIGURE 4.57 – Authentification réussie sur Wireshark

Et au niveau du journal d'évènement qui se trouve dans le serveur, nous allons voir que le l'authentification du PC5 est faite avec succés.

FIGURE 4.58 – Journal d'évènement.

Les certificats delivrés : on as deux modeles de certificats delivré qui sont authentification client et authentification server voir la FIGURE 4.59

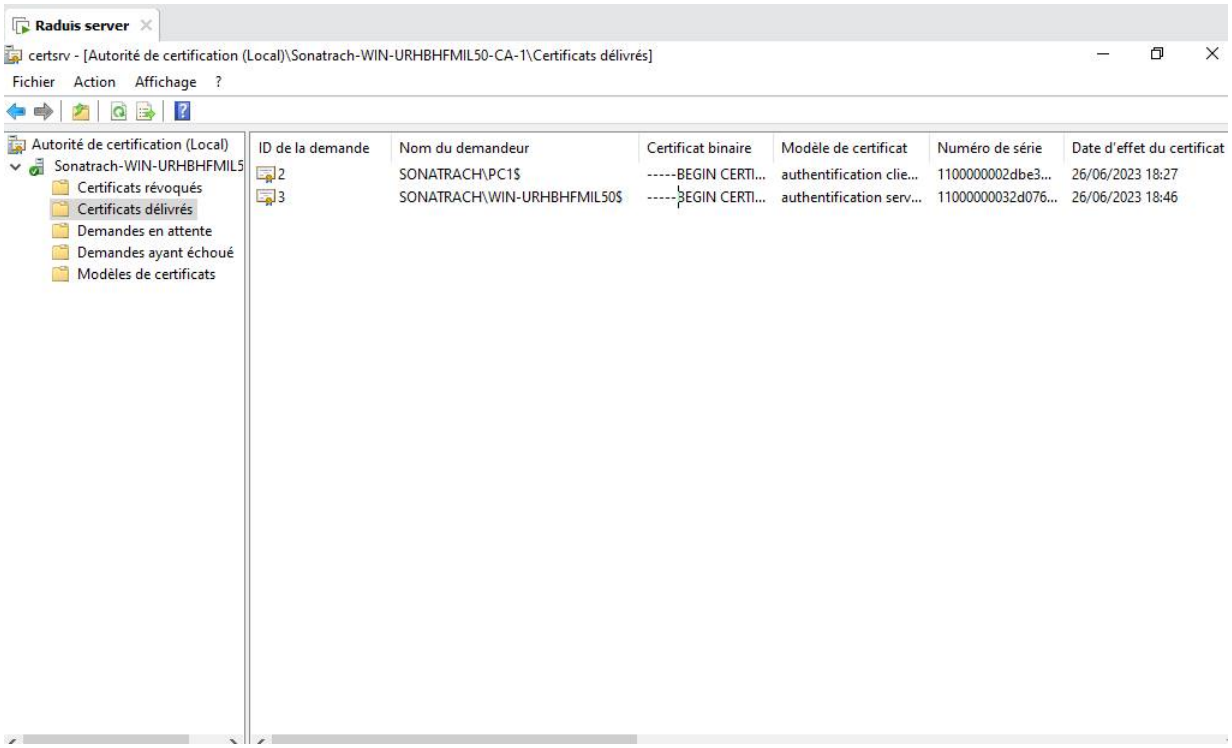

FIGURE 4.59 – Certificats délivrés

-L'authentification échouée : Dans le cas ou l'authentification a échoué, nous ob- servons dans la machine client qu'il y a un échec d'authentification comme le représente la FIGURE 4.59

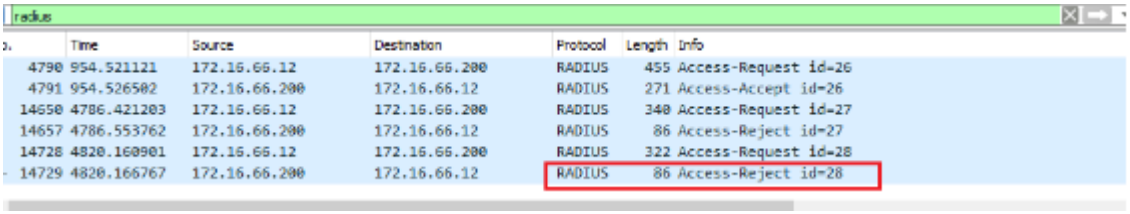

FIGURE 4.60 – Authentification rejeté sur Wireshark

4.9 Conclusion

Ce chapitre a couvert la planification et la réalisation de notre projet de sécurisation d'un réseau Wi-Fi en utilisant des certificats PEAP/TLS. Nous avons soigneusement évalué les besoins de sécurité spécifiques au réseau, mis en place les serveurs d'authentification et de certificats appropriés, et déployé avec succès les certificats PEAP/TLS sur les points d'accès

et les clients.

La gestion efficace des certificats a également été soulignée comme une étape cruciale pour maintenir la sécurité du réseau,cette phase de planification et de réalisation nous a permis de mettre en place une infrastructure fiable pour assurer la sécurité du réseau Wi-Fi.

Conclusion générale

En conclusion, la mise en place d'un réseau Wi-Fi avec une authentification basée sur des certificats PEAP/TLS offre plusieurs avantages significatifs en termes de sécurité et de gestion des accès. dans notre projet on a réussi à créer un environnement réseau sécurisé en renforçant l'authentification des utilisateurs et en protégeant les données échangées sur le réseau.

Les principaux points forts de notre projet incluent l'utilisation du protocole 802.1x avec un serveur d'authentification RADIUS et des certificats PEAP/TLS, garantissant une authentification solide et un chiffrement des communications. Cela a permis de limiter les accès non autorisés, de protéger les informations sensibles et de prévenir les attaques potentielles.

De plus, notre solution offre une gestion centralisée des utilisateurs et des droits d'accès, facilitant la gestion des autorisations et facilitant la productivité. La possibilité d'étendre la portée et la capacité du réseau Wi-Fi, ainsi que l'intégration de fonctionnalités avancées, sont des perspectives intéressantes pour l'avenir du projet.

Il sera également important de rester à jour avec les évolutions technologiques et les normes de sécurité pour maintenir la protection continue du réseau Wi-Fi. L'implémentation de cartes à puce constitue une perspective prometteuse pour renforcer encore la sécurité de l'authentification en ajoutant une couche supplémentaire de protection basée sur des éléments physiques et cryptographiques.

Bibliographie

[1] G.Frédéric.“ WiFi L’essentiel qu’il faut savoir ”. Dunod. Paris. 2003

[2] P.ATELIN. Réseaux sans fil 802.11 : Technologie - Déploiement – Sécurisation 2eme edition)

[3] https ://web.maths.unsw.edu.au/ lafaye/CCM/wifi/wifimodes.htm consulte le 05/01/2023

[4] W.Sttalings, Wireless Communications And Networks, Second Edition, 2004.

[5] R.KUMAR, « A Comparative Study of MAC Layer Protocols for Mobile Ad-Hoc Networks ». Bhagwan Parshuram Institute of Technology Rohini, New Delhi, India. 2014.

[6] CCNA | WIFI RADIO FRÉQUENCE Par Damien Soulages février 13, 2020

[7] R.KUMAR, « A Comparative Study of MAC Layer Protocols for Mobile Ad-Hoc Networks ». Bhagwan Parshuram Institute of Technology Rohini, New Delhi, India. 2014.

[8] DI GALLO Frédéric-WiFi L’essentiel qu’il faut savoir...- 802.11-WEP -SSID-2003

[9] A.Geron,Wifi-professionnel-La-norme-802-11-le-deploiement-la-securite-3e édition A, DUNOD, 2009.

[10] H. Gilbert , Qualité de service et qualité de contole d’un système discret control´e en réseaux sans fil : proposition d’une approche de co-conception appliqu´ee au standard IEEE 802.11, Thése de doctorat en Informatique, Universit´e de Lorraine, 2010

[11] IEEE 802.11nD5.00, Approved Draft Standard for Information Technology Telecommunications and information exchange between systems–Local and metropolitan area networks– Specific requirements– Part 11 : Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications : Amendment 4 : Enhancements for Higher Throughput, IEEE, Fevrier 2012

[12] M. terré, Couche physique et couche MAC Le standard 802.11, Conservatoir National des Arts et Métiers, Version 1.1, 2007

[13] L.Fedoua . « Qualité de Service dans les réseaux locaux sans fil de type IEEE 802.11 », Thèse doctorat. Université Abou Bekr Belkaid.2010.

[14] Les technologies sans fil Le Wi-Fi et la Sécurité-Informatique et Télécommunications-par Nadia ADRAR Université Abderrahmane Mira - BàJAia- Licence Académique en Informatique LMD 2009

[15] Couche physique Standard pour réseaux sans fil : IEEE 802.11 Auteur(s) : Daniel TREZENTOS Date de publication : 10 mai 2002

[16] K.Dridi,Spécification du protocole MAC pour les réseaux IEEE 802.11e à différentiation de services sous contrainte de mobilité. Thèse de doctorat. Université Paris-Est, 2011

[17] Cours réseaux master 1 : MAC IEEE 802.11 Kamal Mehaoued Département d'informatique, Université de Béjaia 2022/2023

[18] Réseaux | 21 - Le Protocole CSMA (1-persistant amp ; non persistant) Mohamed Herak youtub)

[19] G.Pujolle, O.Salvatori et J. Nozick. « Les Réseaux, Édition 2005 ». Paris : Édition Eyro ll es, 2004, 1094p.

[20] UNIVERSITÉ DU QUÉBEC À MONTRÉAL SÉCURITÉ DANS LES RÉSEAUX WI-FI : ÉTUDE DÉTAILLÉE DES ATTAQUES ET PROPOSITION D39 ;UNE ARCHITECTURE WI-FI SÉCURISÉE MÉMOIRE PRÉSENTÉ COMME EXIGENCE PARTIELLE DE LA MAÎTRISE EN INFORMA TIQUE PAR MAHERGAHA MARS 2007

[21] G.Pujolle, O.Salvatori et J. Nozick. « Les Réseaux, Édition 2005 ». Paris : Édition Eyro ll es, 2004,1094p.

[22] Les réseaux mobiles Master 2 informatique ASR Kamal Mehaoued Université de Béjaia – Faculté des sciences exactes 2018/2019

[23] R.KUMAR, « A Comparative Study of MAC Layer Protocols for Mobile Ad-Hoc Networks ». Bhagwan Parshuram Institute of Technology Rohini, New Delhi, India. 2014.

[24] A.Geron,wifi déploiement et securité-la Qos et WPA- 2 e édition

[25] Topologie-reseau. http ://bits-genius.com/topologie-reseau/ consulté le 02/5/2023.

[26] Switch 6509. https ://www.cisco.com/c/en/us/products/switches/catalyst-6509- neb-a-switch/index.html consulté le 29/06/2023.

[27] Switch 3750. https ://www.cisco.com/c/dam/global/frfr/assets/documents/pdfs/datasheet/switchin consulté le 29/06/2023.

[28] Switch 3550. https ://www.cisco.com/web/ANZ/cpp/refguide/hview/switch/3550.html consulté le 29/06/2023

[29] Swicht 2950. https ://www.mercadoit.com/fr/5-switch-cisco consulté le 29/06/2023.

[30] https ://www.redhat.com/fr/topics/security consulté le 13/06/2023

[31] G.Pujolle. Sécurité Wi-Fi. EYROLLES, Paris, 2004

[32] A.SAIDANE, " Conception et réalisation d'une architecture tolérant les intrusions pour des serveurs Internet ", thèse doctorat, Institut National des Sciences Appliquées de Toulouse, janvier 2005.

[33] G.Pujolle. Les Réseaux. EYROLLES, Paris, 2008.

[34] A.Géron. WI-FI Professionnel : La norme 802.11, le déploiement, la sécurité. Dunod 3eme Edition, Paris, 2009.

[35]] Gh. Labouret. Introduction à la cryptographie. http ://www.labouret.net/crypto/233, Consulté le 20 Mai 2012.

[36] S.Ghernaouti-Hélie. Sécurité Informatique et Réseaux : Cours avec plus de 100 exercices corrigés. Dunod 3e Edition, Paris, 2011.

[37] F.Pillion and J. P.Bay. Tout sur la Sécurité Informatique. Dunod 2e Edition, Paris, 2009.

[38] R.Rolland P.Barthelemy. Cryptographie : Principes et mises en oeuvre. Lavoisier, Cachan, 2005

[39] G.Aurélien, « WIFI PROFESSIONNEL. La norme, le déploiement, la sécurité. 3ème édition » ; éditeur : Dunod en Malakof, France ; paru le 23/09/2009 ; Collection InfoPro - Réseaux et télécoms.

[40] K.Hamza, « Formation Hacking et Sécurité, Expert : Réseaux sans Fil », publié dans le site alphorm.com le 14/03/2016.

[41]] « Différence entre attaque active et attaque passive », publié dans le site waytolearnx.com le 28/07/2018

[42] Q.Stiévenart. La cryptologie : Peut-on réellement cacher des informations? Athénée Royal de Waterloo, 2009.

[43] A.Géron, WIFI Professionnel La norme 802.11, le déploiement, la sécurité, 2009, 3 Edition EYROLLES.

[44] Centre de la sécurité des télécommunications Canada, Évaluation de la vulnérabilité des réseaux locaux sans fil (WLAN) 802.11, 2008.

[45] Espace Numérique Entreprises - Direccte Rhône-Alpes, Sécurité des Systèmes d'Information, 2010, http ://www.lamelee.com/les-ressources/securite-de-linformation/securite-des-systemesdinformation/details.html consulté le 09/06/2023

[46] D.Renaud, Introduction à la cryptographie et à la sécurité informatique, 2007, www.montefoire.ulq.ac.be/ dumont/pdf/crypto.pdf.

[47] D.Sébastien, V.Aubin, Réseaux privés virtuels, Travail d'étude et de recherche, 2005.

[48] CERTA,Sécurité des réseaux sans fil (Wi-Fi), 2008, http ://www.certa.ssi.gouv.fr/site/CERTA2002-REC-002/index.html consulté le 29/05/2023

[49] CERTA, Vulnérabilités dans certaines mises en oeuvre de WPA, 2008, http ://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-045/ consulté le 20/06/2023.

[50] La sécurité réseau, www.tri.on.ma consulté le 02/06/2023

[51] C.Saillard, 802.1X : Solution d'authentification sécurisée pour le futur réseau sans fil de l'Université Louis Pasteur, Centre Réseau Communication, Université Louis Pasteur, Strasbourg.

[52] M.Badra, Le transport et la sécurisation des échanges sur les réseaux sans fil, Thèse de doctorat l'Ecole Nationale Supérieure des Télécommunications.

[53] W. Simpson, The Point-to-Point Protocol (PPP), http ://www.ietf.org/rfc/rfc1661.txt, 1994 consulté le 02/06/2023.

[54] PPP. http ://www.labouret.net/ppp/ consulte le 10/04/2023

[55] PAP. http ://www.coursnet.com/2014/11/configuration-des-protocoles-reseau-papet-chap.html consulte le 10/04/2023

[56] CHAP. http ://www.coursnet.com/2014/11/configuration-des-protocoles-reseaupap-et-chap.html consulte le 10/04/2023.

[57] Authentification, règles et recommandation concernant les mécanismes d'authentification, 2010, Agence nationale de la sécurité des systèmes d'information.

[58] A.Géron, WIFI Professionnel La norme 802.11, le déploiement, la sécurité, 2009, 3 Edition EYROLLES.

[59] Cheikhrouhou O., Laurent-Maknavicius M., Ben Jemaa M., « Nouvelle méthode d'authentification EAP-EHash », 12ème Colloque Francophone sur l'Ingénierie des Protocoles CFIP'2006, Tozeur, Tunisie, Octobre 2006.

[60] https ://web.maths.unsw.edu.au/ lafaye/CCM/authentification/radius.htm consulté le 27/06/2023

[61] https ://learn.microsoft.com/fr-fr/security-updates/security/20141645 consulté le 27/06/2023

[62] https ://www.vmware.com/fr/products/workstation-pro.html consulté le 09/06/2023

[63] https ://openclassrooms.com/fr/courses/2581701-simulez-des-architectures-reseaux-avec-gns3/4823151-maitrisez-les-fonctionnalites-de-base-de-gns3 consulté le 27/06/2023

[64] https ://www.netacad.com/fr/courses/packet-tracer consulté le 20/06/2023

Résumé

Le projet aborde la mise en place d'un réseau Wi-Fi sécurisé pour l'entreprise SONATRACH, avec une authentification basée sur des certificats PEAP/TLS. Un laboratoire réel a été utilisé, avec un point d'accès Tenda et un serveur Windows Server 2022. L'utilisation de l'outil GNS3 a permis de recréer l'architecture intranet de SONATRACH et d'illustrer l'utilisation des VLAN pour la segmentation du réseau et l'amélioration de la sécurité et des performances. Le logiciel Packet Tracer a été utilisé pour assurer la gestion centralisée des points d'accès et la supervision du réseau Wi-Fi. L'ensemble de ces démonstrations met en évidence les avantages de la solution proposée, tels que l'amélioration de la sécurité, la gestion centralisée des utilisateurs et des droits d'accès, et l'optimisation des performances du réseau Wi-Fi. Ce projet a permis une mise en pratique concrète et souligne les perspectives d'amélioration pour SONATRACH

Mots clés : Cisco Packet Tracer, GNS3, Windows Server 2022, VMware workstation, RADIUS,certificats PEAP/TLS.

Abstract

The project focuses on implementing a secure Wi-Fi network for SONATRACH, with authentication based on PEAP/TLS certificates. A real laboratory environment was used, including a Tenda access point and a Windows Server 2022. GNS3 was utilized to recreate SONATRACH's intranet architecture and demonstrate the use of VLANs for network segmentation, enhancing security and performance. Packet Tracer software was employed to showcase centralized access point management and Wi-Fi network supervision. These demonstrations highlight the benefits of the proposed solution, such as improved security, centralized user and access rights management, and optimized Wi-Fi network performance. This project enabled practical implementation and underscores potential areas for improvement at SONATRACH.

Keywords : Cisco Packet Tracer, GNS3, Windows Server 2022, VMware Workstation, RADIUS, PEAP/TLS certificates.