République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieure et de la Recherche Scientifique
Université Abderrahmane Mira
Faculté de la Technologie

جامعة بجاية
Tasdawit n Bgayet
Université de Béjaïa

Département d'Automatique, Télécommunication et d'Electronique

Projet de Fin d'Etudes

Pour l'obtention du diplôme de Master

Filière : Télécommunications.
Spécialité :Réseaux et Télécommunications

Thème

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

Préparé par :

- Mlle Belkhichane Ilyssia
- Melle Menzu Massilia

Dirigé par :

M. Diboune Abdelhani

Examiné par :

Mme Mammeri Karima

M. Bellahsene Hocine

Année universitaire : **2022/2023**

Remerciements

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

Nos remerciements s'adressent aussi aux président et membres de jury d'avoir accepté d'examiner et d'évaluer notre travail.

Nous exprimons également notre gratitude à tous les enseignants qui nous ont aidé à réaliser ce travail, sans omettre bien-sûr de remercier profondément tous ceux qui ont contribué de près ou de loin à la réalisation de ce présent travail.

Nous remercions aussi le personnel de l'entreprise Campus NTS, pour leurs accueils en 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

Introduction générale . . . . . .

1 Généralités sur les réseaux sans-fil (WIFI) 2

1.1 Introduction 3

1.2 Architecture d'un réseau sans-fil (BSS, IBSS, ESS) 3

1.3 Mode Ad hoc, infrastructure, équipements 4

1.3.1 Le mode infrastructure 5

1.3.2 Le mode ad-hoc 6

1.3.3 Les équipments 7

1.4 Pile protocolaire d'un réseau sans-fil 8

1.4.1 Couche liaison de données 8

1.4.2 Couche physique 10

1.5 Conclusion 13

2 Sécurité des réseaux sans-fil 14

2.1 Introduction 15

2.2 Les risques 15

2.3 Les attaques 16

2.3.1 Attaque passive 16

2.3.2 Attaques actives 18

2.4 Solutions 20

2.4.1 Intégrité des données 20

2.4.2 Non-répudiation 22

2.4.3 Confidentialité 23

2.4.3.1 Chiffrement 23

2.4.3.2 Certificat 26

2.4.4 Authentification 27

2.4.4.1 DIAMETER 28

2.4.4.2 Kerberos 28

2.4.4.3 TACACS+ 28

2.4.4.4 LDAP 29
2.4.4.5 RADIUS 29
2.4.4.6 Le protocole EAP (Extensible Authentication Protocol) 31
2.4.5 Contrôle d'accès 33
2.4.5.1 Filtrage des adresses mac 34
2.4.5.2 Protocole WPA 35
2.5 conclusion 38

3 Présentation de l'organisme d'accueil 39
3.1 Introduction 40
3.2 Partie 1 : Présentions de l'entreprise « Campus NTS » 40
3.2.1 Création et évolution 40
3.2.2 La localisation de l'entreprise 41
3.2.3 Fiche technique 41
3.2.4Objectifs, Missions et activités de l'Entreprise « N.T.S » 42
3.2.5 Organigramme général de l'organisme d'accueil 43
3.3 Partie 2 : Etude des lieux du client « NGTMEZIANI » 48
3.3.1 Présentation du réseau « NGTMEZIANI» 48
3.3.2 Architecture réseau « NGTMEZIANI» 48
3.3.4 Problématiques 52
3.3.5 Solutions 52
3.4 Conclusion 53

4 Partie Pratique
4.1 Introduction 55
4.2 Environnement de développement 55
4.2.1 Les équipement réseaux 56
4.3 Partie1 : Simulation du réseau sur le simulateur Paquet Tracer 57
4.3.1 Architecture 57
4.3.2 Configuration des VLANs 57
4.3.3 Configuration du contrôleur 63
4.3.4 Configuration de serveur RADUIS et DHCP : 66
4.4 Partie2 : Implémentation sur un réseau réel 69
4.4.1 Présentation d'architecture réseaux 69
4.4.2 Installation et configuration Active directory et DNS 70
4.4.3Installation du DHCP 74
4.4.4 Installation de service de certificats Active Directory 75
4.4.5Configuration du Serveur Radius 76

4.4.6 Création du GPO 78
4.5 Partie Test 83
4.5.1 Test Radius 84
4.5.2 Test AD DS 85
4.5.3 Test DHCP 86
4.5.4 Test certificat 86
4.6 Conclusion 89
Conclusion générale 90
Annexe 93

Table des figures

1.1 Architecture d'un réseau sans fil 3
1.2 Le mode infrastructure [2]. 5
1.3 Architecture d'un réseau ad hoc [2] 6
1.4 Modèle en couches de l'IEEE 802.11 8
1.5 Trame Mac 9

2.1 L'attaque MITM [8] 18
2.2 Les fonctions de hachage [9] 21
2.3 Signature numérique 22
2.4 Etapes de la cryptographie symétrique 23
2.5 Création d'un certificat numérique 27
2.6 Le fonctionnement de Radius 30
2.7 Format des paquets RADIUS 31
2.8 Une connexion Wi-Fi avec un certificat 33
2.9 Filtrage des adresses mac[23] 34
2.10 Authentification par des clés pré-partagées [23] 36
2.11 Le fonctionnement du Wi-Fi avec un serveur d'authentification 37

3.1 Localisation de l'entreprise NTS 41
3.2 Objectifs, Missions et Activités de l'NTS. 42
3.3 L'organigramme de campus NTS 43
3.4 Organigramme de service d'accueil. 45
3.5 Topologie de réseau NGTMEZIANI. 49

4.1 Architecture proposée 57
4.2 Show Vlan brief 61
4.3 Attribution des adresses IP au contrôleur 63
4.4 Partie sécurité 64
4.5 Configuration d'un mot de passe au point d'accès depuis un contrôleur 64
4.6 Les groupes créés 65

4.7 Insertion du mot de passe 66
4.8 Configuration du DHCP selon les vlans 67
4.9 Configuration du serveur radius 68
4.10 Les adresses attribuer aux points d'accées par DHCP 69
4.11 Une vue générale de la solutions 69
4.12 Installation de AD et DNS. 71
4.13 Création d'une Forêt 72
4.14 Création d'un groupe et ordinateur 73
4.15 Ajouter des utilisateurs au groupe 74
4.16 Instalation de certificats AD 76
4.17 Configuration du Bridged physique 77
4.18 Les étapes pour accéder au point d'accès 77
4.19 La stratégie sans fil créer 78
4.20 Activation de l'inscription automatique 79
4.21 Les étapes pour certifier un ordinateur 80
4.22 Création d'une stratégie 81
4.23 Les étapes de la configuration de la règle sans fil 82
4.24 Insertion du nom d'utilisateur et mot de passe 83
4.25 Test Radius 84
4.26 Le message affiché dans le pc client 85
4.27 Le serveur Radius a refusé l'accès pour un ordinateur 85
4.28 Tester la connectivité 85
4.29 Test DHCP 86
4.30 Les Certificats délivrées 86
4.31 Création des stratégies pour chaque vlan 87
4.32 Les étapes de configuration DHCP 89
4.33 VMWare 93
4.34 Windows 10 93
4.35 Installation VMWareworkstation 95
4.36 La clé de VMware 95
4.37 Page d'accueil de VMWareWorkstation 96
4.38 Les étapes d'installation du packettracers 97
4.39 Les étapes d'Installation su serveur Radius 98
4.40 La page du Windows server 2022 99
4.41 La page du serveur RADIUS 99

Liste des tableaux

3.1 Nombre de périphérique par service 50

4.1 Les équipments utilisés 56
4.2 Tableau d'adressage 58
4.3 Commandes de configuration du Switch Core 58
4.4 Commandes de configuration du Switch Core 59
4.5 Commandes de configuration du mode VTP serveur 59
4.6 Commandes de configuration du mode VTP client 59
4.7 Commandes pour nommer les VLANs 60
4.8 Les Vlans associer à chaque switch 61
4.9 Les commandes de configuration du mode access 61
4.10 Tableau d'adressage 62
4.11 Commandes de configuration du routeur 63
4.12 La commande "ip helper-address" 63

Liste des abréviations

AAA Authentication, Authorization, and Accounting
AC Authority certificate
ACK ACKnowledged
AD DS Active Directory Domain Service
AES Advanced Encryption Standard
BSS Base Station Subsystem
CCNA certification Cisco Certified Network Associate
CCNP Cisco Certified Network Professional
CSS Cascading Style Sheets
CTS Clear to send
DIFS Distributed Inter Frame Space
DNS Domain Name System
DHCP Dynamic Host Configuration Protocol
DOS enial of Service
LDAP Lightweight Directory Access Protocol
DS Distribution system
DSSS DIRECT SEQUENCE SPREAD SPECTRUM
ESS Extented Service Set
EAP Extensible Authentication Protocol
FHSS FrequencyHoppingSpread Spectrum
FTP File Transfer Protocol
FTTH Fiber to the Home
FTTX Fiber-to-the-x
GSM Global System for Mobile
GPRS General Packet Radio Service
GPO objet de stratégie de groupe
HTML HyperText MarkupLanguage
IBSS INDEPENDENT Base Station Subsystem
IR INFRAROUGE
IP Internet Protocol
LAN Local Area Network
LLC Logical Link Control
MAN Metropolitan Area Network
MAC Media Access Control
MITM Man-in-the-Middle
NTS New Technology and Solution
OSI Open SystemsInterconnection
PSK PHASE SHIFT KEYING
PLCP Physical Layer Convergence Protocol
PMD Physical Medium Dependent
PPM Pulse Position Modulation
PEAP Protected Extensible Authentication Protocol
PKI Public Key Infrastructure
PHP HypertextPreprocessor

RADIUS	RemoteAuthentication Dial-In User Service
RDP	Remote Desktop Protocol
RTC	Real-Time Clock
SSID	Service Set Identifier
SSH	Secure Shell
SQL	StructuredQueryLanguage
STA	Station
SW	SWITCH
SARL	Société à responsabilité limitée
TACACS+	Terminal Access Controller Access Control System Plus.
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
TKIP	Temporal Key Integrity Protocol
UO	Unité d'Organisation
VNC	Virtual Network Computing
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VTP	VLAN Trunking Protocol
WAN	Wide Area Network
WLAN	Wireless Local Area Network
WiMAX	WorldwideInteroperability for Microwave Access
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access

Introduction générale

L'utilisation croissante des réseaux sans fil locaux (Wi-Fi) dans le cadre des entreprises a transformé la manière dont les communications et la connectivité sont gérées. Ces réseaux offrent une solution pratique et flexible pour connecter les appareils, favorisant ainsi une connectivité sans contrainte des câbles et une mobilité accrue. Les avantages des réseaux sans fil, tels que la collaboration en temps réel, contribuent à améliorer la productivité et l'efficacité des employés.

Cependant, ces réseaux sans fil locaux d'entreprise sont confrontés à des menaces et des attaques qui mettent en jeu la confidentialité, l'intégrité et la disponibilité des données. Des attaques courantes, telles que l'interception de données sensibles, l'injection de codes malveillants et les attaques de déni de service, compromettent la sécurité de ces réseaux.

Dans ce contexte, la méthode traditionnelle d'authentification basée sur un nom d'utilisateur et un mot de passe s'avère de plus en plus insuffisante pour contrer les attaques sophistiquées qui se multiplient. Plusieurs problèmes potentiels peuvent surgir en ce qui concerne la sécurité et la gestion du réseau Wi-Fi au sein d'une entreprise. Tout d'abord, il existe un risque d'accès non autorisé si des mesures de sécurité inadéquates sont mises en place, comme l'utilisation de mots de passe faibles, de clés de cryptage obsolètes ou une mauvaise configuration des points d'accès. Ensuite, l'utilisation excessive de la bande passante peut poser problème lorsque les utilisateurs internes et externes consomment la capacité du réseau Wi-Fi de manière concurente, entraînant ainsi une détérioration des performances pour les utilisateurs légitimes. De plus, le réseau est vulnérable aux attaques qui peuvent paralyser le réseau en saturant la bande passante avec une quantité excessive de trafic, empêchant ainsi les utilisateurs autorisés d'accéder aux ressources du réseau. Les points d'accès mal configurés ou utilisant des mots de passe par défaut représentent également une menace, car ils peuvent être compromis et exposés à des attaques par force brute. Enfin, l'absence de centralisation et de gestion efficace des comptes et des droits d'accès systèmes constitue un autre problème majeur à prendre en compte. Les entreprises réalisent désormais que ces informations sont vulnérables aux techniques de piratage. Pourrenforcer la sécurité de leurs réseaux, elles se tournent vers l'utilisation des certificats, quireprésentent une solution plus solide et sécurisée.

Dans ce mémoire, nous abordons spécifiquement l'authentification basée sur des certificats PEAP/TLS (Protected Extensible Authentication Protocol / Transport Layer Security). LePEAP/TLS est un protocole de sécurité couramment utilisé pour l'authentification des utilisateurs dans les réseaux sans fil. Il permet de sécuriser les échanges d'informations entreles clients et les serveurs en utilisant des certificats numériques.
Ce mémoire est divisé en quatre chapitres

— Dans le premier chapitre, nous présentons les bases des réseaux sans fil, y compris leur architecture et leur pile protocolaire. Nous explorons également les différents modes de fonctionnement des réseaux sans fil, tels que le mode ad hoc et le mode infrastructure.

— Le deuxième chapitre est dédié à la sécurité des réseaux sans fil. Nous examinons les risques et les attaques auxquels ces réseaux sont exposés, notamment les attaques passives et actives. Ensuite, nous proposons des solutions pour renforcer la sécurité des ré-

seaux sans fil, notamment en garantissant l'intégrité des données, la non-répudiation, la confidentialité et l'authentification.

— Dan le troisième chapitre, nous présentons l'organisme d'accueil de ce mémoire, en décrivant son histoire, sa localisation, ses objectifs, ses missions et ses activités. Nous abordons également l'architecture du réseau de son client et les problématiques auxquelles il est confronté.

— Le quatrième chapitre concerne la réalisation et les tests. Nous détaillons l'environnement de développement utilisé, les étapes de simulation du réseau sur un simulateur (Packet Tracer) et d'implémentation sur un réseau réel. Nous présentons également les tests effectués pour vérifier le bon fonctionnement de l'authentification basée sur les certificats PEAP/TLS.

Enfin notre mémoire s'achèvera par une conclusion générale résumant les points principaux qui ont été de grands apports.

Chapitre 1

Généralités sur les réseaux sans-fil (WIFI)

Introduction

La technologie sans fil a connu une adoption croissante et une intégration de plus en plus profonde dans notre vie quotidienne. Les réseaux sans fil offrent une connectivité pratique et flexible, permettant la communication entre différents appareils sans l'utilisation de câbles filaires.

Ce chapitre se concentre sur l'architecture des réseaux sans fil, en mettant l'accent sur la norme IEEE 802.11, qui définit les caractéristiques physiques et les protocoles de communication des réseaux locaux sans fil. Nous examinerons également les différents modes de topologie sans fil, à savoir le mode infrastructure et le mode ad-hoc. Enfin, nous explorerons la pile protocolaire des réseaux sans fil, en détaillant les sous-couches et les méthodes utilisées dans les couches de liaison de données et physiques.

Architecture d'un réseau sans-fil (BSS, IBSS, ESS)

L'architecture 802.11 est un ensemble de normes de communication sans fil qui définissent les caractéristiques physiques et les protocoles de communication des réseaux locaux sans fil. La norme 802.11 a été développée par l'Institute of Electrical and Electronics Engineers (IEEE).

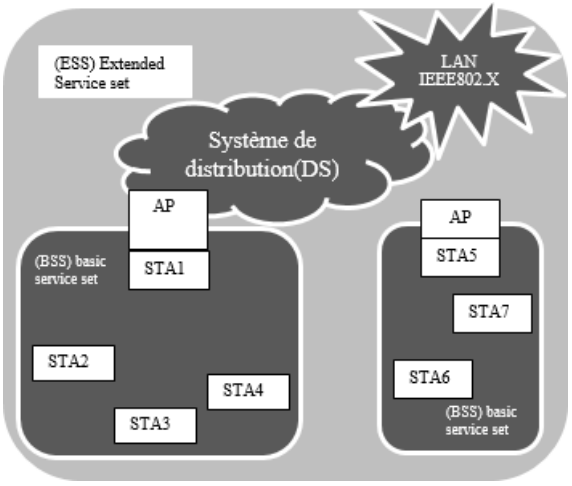


FIGURE 1.1 – Architecture d'un réseau sans fil

L'architecture 802.11 est représentée dans la figure 1.1, montrant la structure du réseau sans fil. Au centre de cette architecture se trouve le BSS (Basic Service Set), qui est l'élément de base contenant un groupe de stations exécutant le même protocole MAC et partageant l'accès à un support sans fil commun. Le BSS peut être soit isolé, soit connecté à un système de distribution (DS).

Dans un Basic Service Set (BSS), les stations clientes ne peuvent pas établir une connexion directe entre elles, mais doivent passer par un point d'accès. Cela signifie qu'une station envoie des trames MAC (Medium Access Control) au point d'accès, qui les transmet ensuite à la station destinataire. De la même manière, lorsqu'une station du BSS émet une trame MAC, celle-ci est relayée par le point d'accès vers le système de distribution (qui peut être un commutateur, un réseau câblé ou un autre réseau sans fil), jusqu'à atteindre la destination souhaitée.

Lorsque tous les BSS sont mobiles et qu'il n'y a pas de connexion avec d'autres BSS, on parle d'IBSS (Independent BSS), qui est une forme de réseau ad hoc. Dans un IBSS, les stations clientes peuvent communiquer directement les unes avec les autres sans passer par un point d'accès.

Un ESS (Extended Service Set) est formé par l'interconnexion de un ou plusieurs BSS via un DS. Il est souvent considéré comme l'épine dorsale du réseau local (LAN).

En résumé, l'architecture 802.11 comprend des BSS qui sont les éléments de base contenant des stations clientes connectées à un point d'accès, un IBSS qui est un réseau ad hoc où les stations clientes se connectent directement, et un ESS qui est formé par l'interconnexion de plusieurs BSS via un DS [5].

Mode Ad hoc, infrastructure, équipements

Les réseaux locaux sans fil peuvent accueillir plusieurs topologies réseau. La norme 802.11 identifie deux principaux modes de topologies sans fil :

Le mode infrastructure

Le mode infrastructure est un réseau sans fil qui possède un point d'accès centralisé au cœur du réseau. En mode infrastructure, chaque ordinateur de station (appelé STA) se connecte à un point d'accès via une connexion sans fil. Cet ensemble formé forme une cellule et est également appelé ensemble de services de base (appelé BSS).

Plusieurs points d'accès (plus précisément, plusieurs BSS) peuvent être interconnectés par des connexions appelées système de distribution (appelé DS dans système de distribution) pour former un ensemble de services améliorés (ESS).

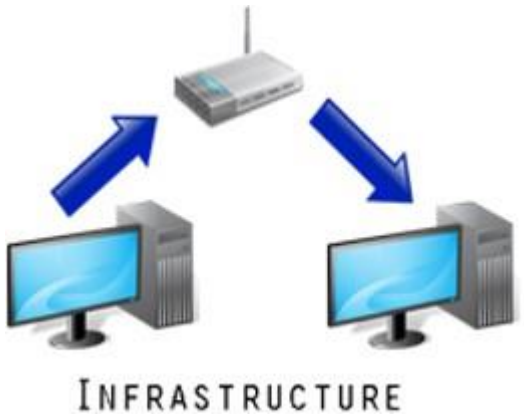


FIGURE 1.2 – Le mode infrastructure [2].

Le mode infrastructure est couramment utilisé pour étendre un réseau câblé, comme Ethernet, en ajoutant une connectivité Wi-Fi à un ordinateur portable ou à un ordinateur, sans nécessiter l'utilisation de câbles. Les réseaux en mode infrastructure offrent des fonctionnalités avancées telles qu'une sécurité renforcée, des vitesses de transfert de données plus rapides et une intégration avec les réseaux câblés. Cela permet aux utilisateurs de bénéficier d'une connectivité sans fil pratique tout en profitant des performances et des fonctionnalités avancées des réseaux câblés.

Le mode ad-hoc

Les réseaux ad hoc permettent à tous les appareils de communiquer directement entre eux. Il n'y a pas de point d'accès central contrôlant la communication entre les appareils. Les périphériques réseau ad hoc ne peuvent communiquer qu'avec d'autres périphériques réseau ad hoc. Il ne peut pas communiquer avec les périphériques du réseau d'infrastructure ou d'autres périphériques connectés à des réseaux câblés. De plus, la sécurité en mode ad-hoc est plus avancée qu'en mode infrastructure [3].

En mode ad-hoc, les machines clientes sans fil se connectent entre elles pour former un réseau point à point (peer-to-peer en anglais). C'est-à-dire un réseau où chaque machine joue simultanément le rôle d'un client et un point d'accès.

IBSS est donc un réseau sans fil composé d'au moins deux stations et n'utilise pas de points d'accès. Dans les réseaux ad hoc, la portée des BSS indépendants est limitée par la portée de chaque station individuelle. Cela signifie que si deux stations se trouvent hors de portée l'une de l'autre, elles ne peuvent pas se "voir" ni communiquer. Contrairement au mode infrastructure, le mode ad hoc ne fournit pas de système distribué permettant l'envoi de trames d'une station à une autre. Par conséquent, par définition, un réseau ad hoc (IBSS) est un réseau sans fil restreint [4].

Ce type de réseau permet qu'à des machines proches de se connecter.

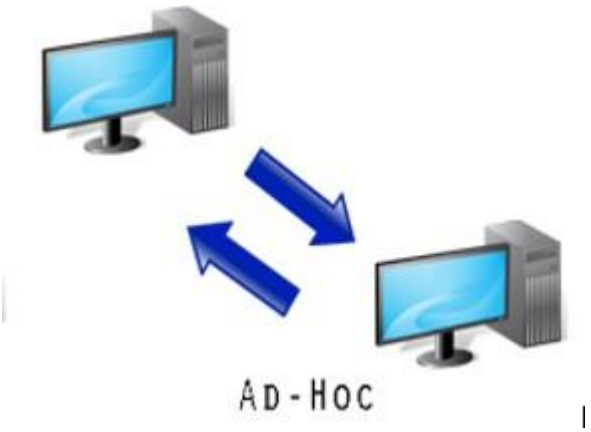


FIGURE 1.3 – Architecture d'un réseau ad hoc [2].

Dans les modes infrastructure et ad hoc, chaque réseau de service est distingué par un identifiant de réseau appelé SSID (Service Set Identifier). Par conséquent, toute station qui souhaite se connecter à un réseau de service spécifique doit être préalablement informée de la valeur du SSID correspondant [2].

Un réseau sans fil est composé de plusieurs éléments qui travaillent ensemble pour fournir une connectivité sans fil. Voici les composants principaux d'un réseau sans fil :

Les équipments

Un réseau sans fil est composé de plusieurs éléments qui travaillent ensemble pour fournir une connectivité sans fil. Voici les composants principaux d'un réseau sans fil :

- **Points d'accès (Access Points) :** Les points d'accès sont des dispositifs qui permettent aux appareils sans fil de se connecter au réseau. Ils agissent comme des relais de communication entre les appareils sans fil et le réseau câblé. Les points d'accès sont généralement connectés à un routeur ou à un commutateur réseau.
- **Routeur :** Le routeur est un dispositif qui relie le réseau sans fil à Internet ou à un autre réseau. Il permet de faire transiter les données entre les appareils du réseau sans fil et les autres réseaux connectés.
- **Cartes réseau :** Les cartes réseau sans fil, également appelées adaptateurs sans fil, sont des composants matériels installés dans les appareils (comme les ordinateurs portables, les smartphones, les tablettes) qui leur permettent de se connecter à un réseau sans fil.
- **Antennes :** Les antennes sont utilisées pour émettre et recevoir les signaux sans fil. Elles sont présentes à la fois sur les points d'accès et sur les appareils clients pour assurer la communication sans fil.

Ces composants travaillent ensemble pour créer un réseau sans fil fonctionnel, permettant aux appareils de communiquer entre eux et d'accéder aux ressources du réseau, qu'il s'agisse d'Internet, de fichiers partagés ou d'autres services réseau.

Pile protocolaire d'un réseau sans-fil

La norme IEEE 802.11, qui régit les réseaux sans fil, est composée de plusieurs couches protocolaires, dont la couche physique et la couche de liaison de données. Voici une explication détaillée des différentes sous-couches et méthodes utilisées dans ces deux couches [2] :

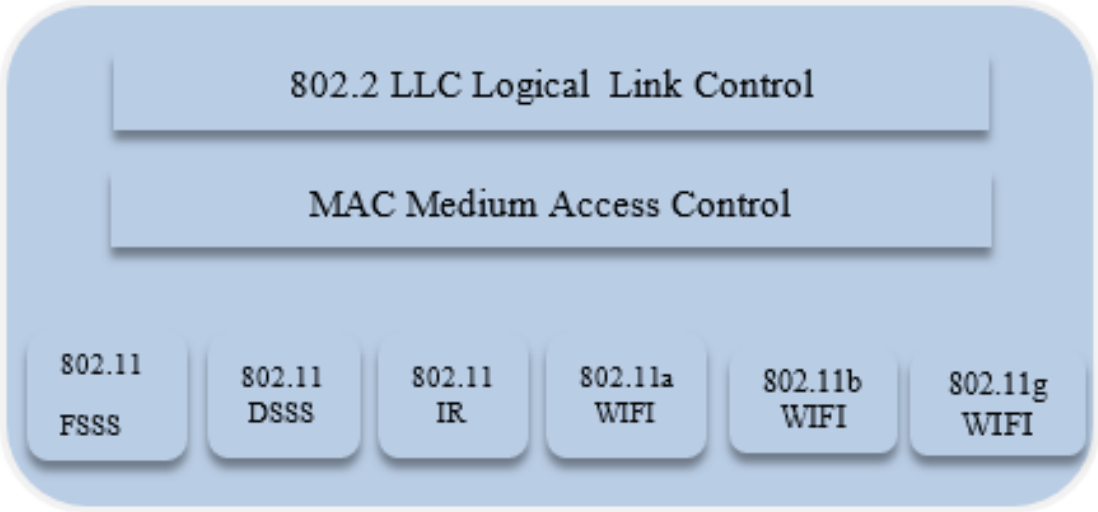


FIGURE 1.4 – Modèle en couches de l'IEEE 802.11

Couche liaison de données

La couche de liaison de données de la norme 802.11 est divisée en deux sous-couches :

- **LLC (Logical Link Control)** : Cette sous-couche est commune à tous les standards du groupe 802. Elle assure la gestion des erreurs et la correction des erreurs de transmission. Elle offre également une connectivité entre la couche réseau et la couche physique pour permettre le transfert de données entre les nœuds du réseau.
- **MAC (Media Access Control) :** La sous-couche MAC est spécifique à la norme IEEE 802.11. Elle gère et contrôle l'accès au support physique du réseau. Elle contrôle la transmission des trames entre les nœuds du réseau, gère les collisions et définit les priorités de transmission.

— **Données MAC (Trame 802.11) :** la figure suivante montre le format général de la trame MAC.

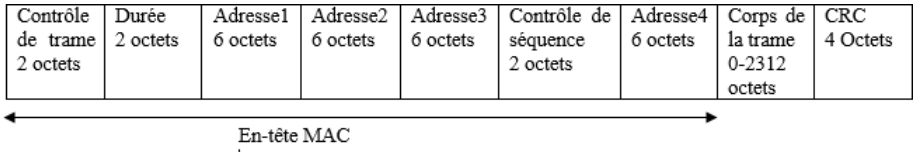


FIGURE 1.5 – Trame Mac

— **Méthode d'accès au canal :** La norme 802.11 utilise la méthode d'accès CSMA/CA pour éviter les collisions et assurer une communication fiable. Avant d'envoyer des données, une station écoute le support pour détecter s'il est occupé. Si le support est occupé, la transmission est différée. Si le support est libre pendant une période spécifique appelée DIFS (Distributed Inter Frame Space), la station est autorisée à transmettre après un délai aléatoire basé sur l'algorithme de "backoff". La station de transmission envoie d'abord une petite trame de contrôle appelée RTS (Request To Send), qui contient des informations sur la source, la destination et la durée de transmission. La station de destination reçoit la trame RTS, vérifie si le canal est libre, puis envoie une trame de confirmation de transmission CTS (Clear To Send) contenant les mêmes informations sur la durée. Lorsque le paquet de données est correctement reçu, la station de réception envoie un accusé de réception (ACK) à l'expéditeur. Si l'ACK n'est pas reçu, l'expéditeur suppose qu'une collision s'est produite et renvoie le paquet de données.

— **L'algorithme de "backoff"** est utilisé pour gérer les collisions de données qui peuvent survenir lors de la transmission. Il est généralement utilisé en conjonction avec la méthode d'accès CSMA/CA dans les réseaux sans fil. Chaque station choisit un délai d'attente aléatoire dans une fenêtre de contention de taille CW (Contention Window), qui représente un certain nombre de slots. La station attend ce nombre de slots avant de transmettre, tout en vérifiant si une autre station a accédé au support avant elle [6].

Couche physique

La couche physique de la norme IEEE 802.11 assure la liaison entre la couche de liaison de données (MAC) et le support de transmission des trames. Elle est subdivisée en deux sous-couches :

— **PLCP (Physical Layer Convergence Protocol) :** Cette sous-couche gère l'encodage des données pour la transmission. Elle se charge de la conversion des données en un format adapté à la transmission sur le support physique.

— **PMD (Physical Medium Dependent) :** Cette sous-couche gère les médias de transmission physiques et fournit des services de signalisation à la couche MAC. Elle informe la couche MAC sur l'état d'occupation du support physique (occupé ou libre) [2].

La norme originale 802.11 proposait trois couches physiques de base : FHSS, DSSS et IR. Cependant, la norme a été améliorée au fil du temps, et de nouvelles couches physiques ont été ajoutées, telles que celles utilisées dans les normes 802.11b, 802.11a et 802.11g.

Les principales versions de la norme 802.11

— **802.11a :** la norme 802.11a (baptisé WiFi 5) permet d'obtenir un haut débit (54 Mbps théoriques, 30 Mbps réels). La norme 802.11a spécifie 8 canaux radio dans la bande de fréquence des 5 GHz, offre des vitesses de transmission allant jusqu'à 54 Mbit/s et prend en charge jusqu'à 64 utilisateurs.

— **802.11b :** La norme 802.11b est la norme la plus répandue actuellement. Elle propose un débit théorique de 11 Mbps (6 Mbps rééls) avec une portée pouvant aller jusqu'à 300 mètres dans un environnement dégagé. La plage de fréquence utilisée est la bande des 2.4 GHz, avec 3 canaux radio disponibles.

— **802.11c :** La norme 802.11c n'a pas d'intérêt pour le grand public. Il s'agit uniquement d'une modification de la norme 802.1d afin de pouvoir établir un pont avec les trames 802.11.

— **802.11d :** La norme 802.11d est un supplément à la norme 802.11 dont le but est de permettre une utilisation internationale des réseaux locaux 802.11. Elle consiste à permettre aux différents équipements d'échanger des informations sur les plages de fréquence et les puissances autorisées dans le pays d'origine du matériel.

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

— **802.11f :** la norme 802.11f est une recommandation à l'intention des vendeurs de point d'accès pour une meilleure interopérabilité des produits. Elle propose le protocole Inter-Access point roaming protocol permettant à un utilisateur itinérant de changer de point d'accès de façon transparente lors d'un déplacement, quelles que soient les marques des points d'accès présentes dans l'infrastructure réseau. Cette possibilité est appelée itinérance (ou roaming en anglais).

— **802.11g :** publiée en 2003, constitue une amélioration directe de 802.11b en proposant un débit bande de base de 54 Mbits/s utilise une bande de fréquence de 2.4 Ghz ou 5 Ghz, offre une vitesse de transmission sur la bande des 2,4 GHz [5].

— **802.11h :** elle vise à rapprocher la norme 802.11 du standard Européen (HiperLAN 2, doù le h de 802.11h) et être en conformité avec la réglementation européenne en matière de fréquence et d'économie d'énergie.

— **802.11i :** elle a pour but d'améliorer la sécurité des transmissions (gestion et distribution des clés, chiffrement et authentification). Cette norme s'appuie sur l'AES (Advanced Encryption Standard) et propose un chiffrement des communications pour les transmissions utilisant les technologies 802.11a, 802.11b et 802.11g.

— **802.11Ir :** cette norme a été élaborée de telle manière à utiliser des signaux infrarouges. Cette norme est désormais dépassée techniquement.

— **802.11j :** La norme 802.11j est à la réglementation japonaise ce que le 802.11h est à la réglementation européenne.

FHSS

Le standard 802.11 utilise désormais la technique FHSS (Frequency Hopping Spread Spectrum) pour réduire les interférences et les perturbations entre les transmissions des différentes stations d'une cellule. En mode FHSS, les données sont transmises en utilisant une modulation appelée GMSK (Gaussian Minimum Shift Keying). Le débit de transmission varie généralement entre 1 et 2 Mbit/s.

L'un des avantages du FHSS est qu'il permet théoriquement d'exploiter simultanément jusqu'à 26 réseaux 802.11 FHSS dans une même zone. Chaque réseau utilise l'une des séquences prédéfinies, ce qui contribue à minimiser les interférences entre eux.

Cependant, le principal inconvénient du FHSS réside dans sa limitation de débit, qui est plafonné à 2 Mbit/s. Cette limitation est due à la bande passante des canaux utilisée, qui est généralement fixée à 1 MHz.

DSSS

Le DSSS (Direct Sequence Spread Spectrum) est une technique de modulation utilisée dans les réseaux sans fil pour transmettre des données sur une large bande de fréquences. Elle consiste à étaler le signal de données sur une plage de fréquences plus large que nécessaire en utilisant une séquence pseudo-aléatoire appelée code de répétition.

Lors de la transmission, chaque bit de données est étendu à l'aide de cette séquence pseudo-aléatoire, ce qui permet d'augmenter la largeur de bande du signal. Cette extension de la bande passante améliore la résistance aux interférences et la robustesse contre les perturbations.

Infrarouge IR

La norme IEEE 802.11 utilise une technique de transmission infrarouge qui est omnidirectionnelle, ce qui signifie qu'elle émet des signaux dans toutes les directions. Cette technique offre une portée de 20 mètres, ce qui permet aux appareils de communiquer sur une distance relativement courte.

L'utilisation de la technologie infrarouge permet d'atteindre des débits de transmission allant de 1 à 2 Mbit/s. Pour réaliser cette transmission, une modulation appelée PPM (Pulse Position Modulation) est utilisée. La modulation PPM consiste à transmettre des impulsions avec une amplitude constante et à coder l'information en fonction de la position temporelle de ces impulsions. Cela signifie que les données sont codées en modifiant la position relative des impulsions dans le temps[5].

Conclusion

Dans ce chapitre, nous avons abordé les généralités sur les réseaux sans fil, mettant en évidence leur architecture et les options de connectivité offertes par la norme 802.11. Dans le chapitre suivant, nous nous pencherons sur les attaques potentielles auxquelles ces réseaux sont exposés, ainsi que les solutions de sécurité correspondantes.

Chapitre 2

Sécurité des réseaux sans-fil

Introduction

La sécurité des réseaux sans fil est un enjeu crucial dans notre société numérique en constante évolution. Au cours de ce chapitre, nous avons étudié les risques et les différentes attaques auxquels les réseaux sans fil sont exposés.

Pour faire face à ces menaces, nous avons exploré diverses solutions de sécurité. Nous avons présenté des techniques de chiffrement symétrique et asymétrique pour garantir l'intégrité des données.

Nous avons également exploré l'authentification des utilisateurs en présentant des protocoles tels que DIAMETER, Kerberos, TACACS+, LDAP et RADIUS. Ces protocoles offrent des mécanismes robustes pour vérifier l'identité des utilisateurs et contrôler leur accès au réseau.

Enfin, nous avons abordé le contrôle d'accès en examinant des techniques telles que le filtrage des adresses MAC et l'utilisation du protocole WPA (Wi-Fi Protected Access).

Les risques

En sécurité informatique le risque est c'est la probabilité qu'un problème survienne lorsqu'une vulnérabilité est exposée à une population malveillante qui tentera de l'exploiter,Les risques liés à la sécurité des systèmes informatiques peuvent être classés en plusieurs niveaux :

- **Risques physiques :** L'accés non autorisé aux fils d'un réseau informatique comporte plusieurs risques. Les principales menaces incluent l'intreception de données sensibles, la manipulation des câbles pour altérer le trafic. l'injection de données malveillantes.
- **Risques réseau :** Les risques réseau sont liés à la sécurité des réseaux informatiques. Ils peuvent inclure des attaques de type "man-in-the-middle", des attaques par déni de service, des attaques de piratage de réseau, des interceptions non autorisées, etc.

— **Risques système :** Ces risques concernent la sécurité des systèmes d'exploitation et des logiciels qui les accompagnent. Ils incluent les vulnérabilités des logiciels, les erreurs de configuration, les failles de sécurité connues, les faiblesses des mots de passe, etc.

— **Risques d'information :** Les risques d'information se rapportent à la confidentialité et à l'intégrité des données stockées et échangées dans les systèmes informatiques. Ils peuvent inclure l'accès non autorisé aux données sensibles, les fuites d'informations, le vol d'identité, la divulgation d'informations confidentielles, etc.

— **Risques d'application :** Ces risques sont spécifiques aux applications logicielles utilisées dans les systèmes informatiques. Ils incluent les vulnérabilités des applications, les erreurs de programmation, les attaques d'injection de code (comme les attaques par injection SQL), les failles de sécurité dans les interfaces utilisateur, etc.

— **Risques organisationnels :** Les risques organisationnels sont liés à la gestion de la sécurité au sein d'une organisation. Ils incluent les politiques de sécurité inefficaces, les procédures de sauvegarde et de récupération inadéquates, la formation insuffisante du personnel, les erreurs humaines, les politiques de sécurité non respectées, etc.

Les attaques

Les réseaux sans fil présentent des vulnérabilités qui peuvent être exploitées par des attaquants pour mener des activités malveillantes. Ces attaques exploitent les failles de sécurité des réseaux sans fil et peuvent se manifester de différentes façons.

Les attaques sur les réseaux sans fil peuvent être classées en deux catégories principales : les attaques passives et les attaques actives.

Attaque passive

Attaque passive sont les attaques où l'attaquant se met en écoute non autorisée, en surveillant simplement la transmission ou la collecte d'informations. L'oreille indiscrète

n'apporte aucun changement aux données ou au système.

— **Le war-driving :** lors d'une opération de war-driving, les pirates informatiques utilisent souvent des outils tels qu'un ordinateur portable, un PC ou un autre dispositif similaire équipé d'un logiciel de détection de réseau sans fil, d'une carte réseau 802.11, Ces cartes Wi-Fi sont souvent munies d'antennes directives, qui leur permettent d'écouter le trafic radio à distance. En parcourant la zone et en utilisant ces outils, les réseaux sans fil détectés sont affichés à l'écran. Pour plus de précision, un récepteur GPS peut être utilisé pour cartographier de manière très précise tous les points d'accès découverts. Ces pratiques de war-driving mettent en évidence les risques liés à la sécurité des réseaux sans fil, soulignant ainsi l'importance de mettre en place des mesures de sécurité appropriées. Parmi ces mesures, on retrouve l'utilisation de clés de chiffrement robustes, de protocoles de sécurité avancés et de pare-feux pour protéger les réseaux sans fil contre ces attaques passives [7].

— **L'homme du milieu :** cette attaque, connue sous le nom de "Man-in-the-Middle" (MITM) ou interception active, se déroule en disposant un point d'accès non autorisé à proximité des points d'accès légitimes dans un réseau Wi-Fi. Lorsque les utilisateurs tentent de se connecter au réseau, ils fournissent involontairement leurs informations de connexion au point d'accès malveillant. Une station pirate peut alors intercepter le trafic en écoutant les communications et en récupérant les adresses MAC de la station légitime et de son point d'accès. En se positionnant entre les deux, la station pirate agit comme un intermédiaire invisible, permettant d'accéder à toutes les communications échangées sans que les utilisateurs ne se doutent de rien. Ce processus se déroule de manière transparente, la station pirate se comportant comme un proxy, lui permettant ainsi d'obtenir les informations correspondantes [8].

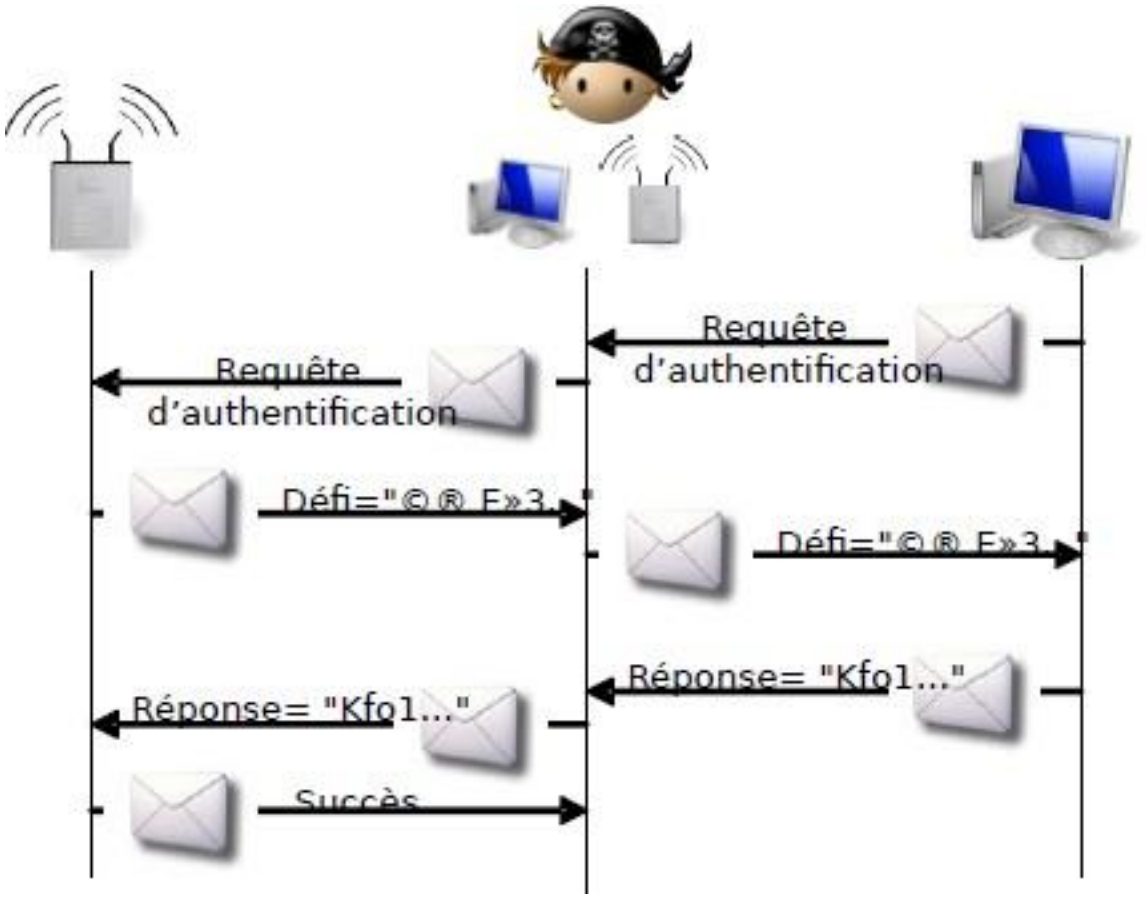


FIGURE 2.1 – L'attaque MITM [8].

Attaques actives

Une attaque active implique une interruption, une modification ou une fabrication d'informations, ce qui entraîne des perturbations dans le fonctionnement normal du réseau sans fil.

— **Spoofing IP :** l'usurpation d'adresse IP, également connue sous le nom de spoofing IP, est une technique qui consiste à envoyer des paquets IP en utilisant une adresse IP source qui ne correspond pas à celle de l'ordinateur émetteur. Cette méthode vise généralement à dissimuler l'identité réelle de l'attaquant lors d'une attaque contre un serveur ou à se faire passer pour un autre équipement du réseau afin de bénéficier de certains privilèges. Parallèlement, le spoofing IP implique une manipulation des pa-

quets émis pour qu'ils donnent l'impression de provenir d'une machine différente. En d'autres termes, le pirate envoie des paquets qui semblent être émis depuis une adresse IP autre que la sienne. Ces deux techniques ont pour objectif de tromper les systèmes de sécurité en compromettant la confiance dans l'origine des paquets IP. En utilisant l'usurpation ou le spoofing IP, les attaquants peuvent contourner les mécanismes de filtrage et d'authentification basés sur l'adresse IP, leur permettant ainsi d'accéder illégalement à des systèmes ou de masquer leur identité réelle. Cela leur permet de sembler provenir d'une source fiable, échappant ainsi à la détection.

— **L'attaque par force brute :** La force brute consiste à essayer toutes les combinaisons possibles. Elle est rapidement efficace sur les petites chaînes (moins de 8 caractères) mais devient rapidement trop longue à exécuter quand la longueur du mot de passe augmente (plus de 16 caractères). L'attaque par force brute est une technique utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Elle consiste à tester méthodiquement toutes les combinaisons possibles de caractères, une à une. Cette approche exhaustive est efficace uniquement lorsque le mot de passe recherché est relativement court.

  Les programmes utilisés dans ce type d'attaque tentent toutes les possibilités de mots de passe dans un ordre aléatoire afin de contourner les logiciels de sécurité qui bloquent les tentatives de mots de passe dans un ordre séquentiel. Bien que cette méthode garantisse la découverte d'un mot de passe, elle peut prendre beaucoup de temps. La meilleure solution est d'utiliser un mot de passe complexe et sécurisé.

— **DOS :** le déni de service réseau est souvent l'alternative à d'autres formes d'attaques car dans beaucoup de cas il est plus simple à mettre en œuvre, nécessite moins de connaissances et est moins facilement traçable qu'une attaque directe visant à entrer dans un système pour en prendre le contrôle. Cette attaque a pour but d'empêcher des utilisateurs légitimes d'accéder à des services en saturant de fausses requêtes ces services. Elle se base généralement sur des " bugs " logiciel. Dans le milieu Wi-Fi, cela consiste notamment à bloquer des points d'accès soit en l'inondant de requête de désassociassions ou des authentification (programme de type Airjack), ou plus simplement

en brouillant les signaux hertziens.

Solutions

Les réseaux sans fil ont connu une expansion considérable ces dernières années, offrant une connectivité pratique et flexible dans de nombreux domaines. Cependant, cette évolution a également posé de nouveaux défis en matière de sécurité des données. Les données transmises via des réseaux sans fil sont plus exposées aux risques de violation de la confidentialité, d'altération et de compromission de l'authenticité. Pour garantir la sécurité des réseaux sans fil, il est essentiel de mettre en place des mesures de protection adéquates. Parmi les principales dimensions de sécurité à prendre en compte, on retrouve l'intégrité des données, la non-répudiation, la confidentialité, le contrôle d'accès et l'authentification [8].

Intégrité des données

Dans un réseau sans fil, les données sont généralement transmises à travers un canal de communication sans fil, ce qui les expose à certains risques tels que les interférences, les erreurs de transmission et les attaques malveillantes. L'intégrité des données vise à détecter et à prévenir ces altérations indésirables afin de garantir que les données restent inchangées et fiables tout au long du processus de transmission sans fil.

Pour assurer l'intégrité des données dans les réseaux sans fil, différentes techniques peuvent être utilisées, telles que :

— **Cryptage** le cryptage des données traduit les données sous une autre forme, ou code, de sorte que seules les personnes ayant accès à une clé secrète (appelée clé de décryptage) ou à un mot de passe peuvent la lire. Les données chiffrées sont communément appelées texte chiffré, tandis que les données non chiffrées sont appelées texte en clair ou donnée en clair. Actuellement, le chiffrement est l'une des méthodes de sécurité des

données les plus populaires et les plus efficaces utilisées par les entreprises. Il existe deux principaux types de cryptage des données

— Le cryptage asymétrique, également appelé cryptage à clé publique.

— Le cryptage symétrique [10].

— **Fonction de hachage :** les fonctions de hachages ont généralement utilisées comme première étape pour vérifier l'intégrité d'un message ou pour générer une signature numérique. Supposons que voussouhaitiez envoyer un fichier par e-mail, mais que ce fichier soit volumineux et que vous vouliez rassurer le destinataire sur l'origine de ce fichier et sur ce qu'il contient. Au lieu de chiffrer le fichier directement avec votre clé privée, hachez le fichier et chiffrez le résumé résultant avec votre clé privée. Envoyez ensuite le fichier originale le résumé signé (signature)au destinataire.

A réception, ce dernier vérifie l'exactitude de la signature en vérifiant la signature du haché et la validité des données.

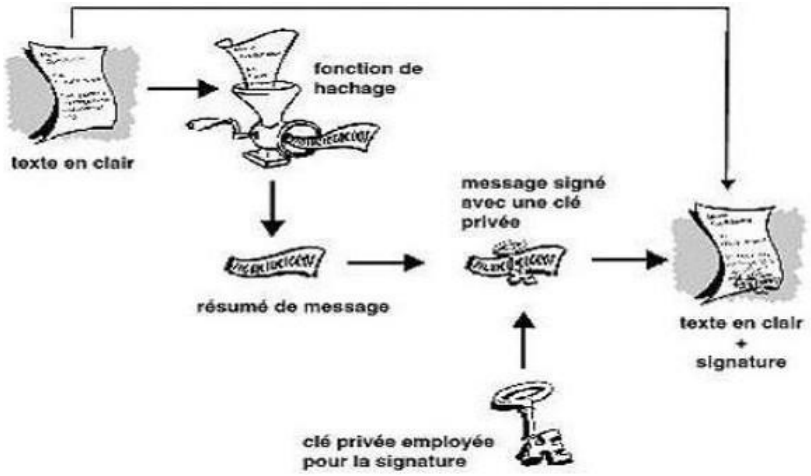


FIGURE 2.2 – Les fonctions de hachage [9] .

Le but principal d'une fonction de hachage dans les réseaux sans fil est d'assurer l'intégrité des données, c'est-à-dire de garantir que les données transmises ou stockées n'ont pas été modifiées de manière non autorisée ou accidentelle [9].

— **Signature numérique :** la signature numérique est un mécanisme cryptographique utilisé pour garantir l'intégrité, l'authenticité des données dans les réseaux sans fil. Elle

permet de vérifier l'origine des données et de s'assurer qu'elles n'ont pas été altérées pendant leur transmission [11].

La signature numérique utilise une paire de clés cryptographiques pour créer une empreinte numérique unique des données, qui est ensuite chiffrée avec la clé privée de l'expéditeur pour former la signature numérique. Le destinataire peut vérifier l'intégrité des données en utilisant la clé publiquecorrespondante pour déchiffrer la signature et comparer l'empreinte numérique déchiffrée avec l'empreinte numérique calculée à partir des données reçues.

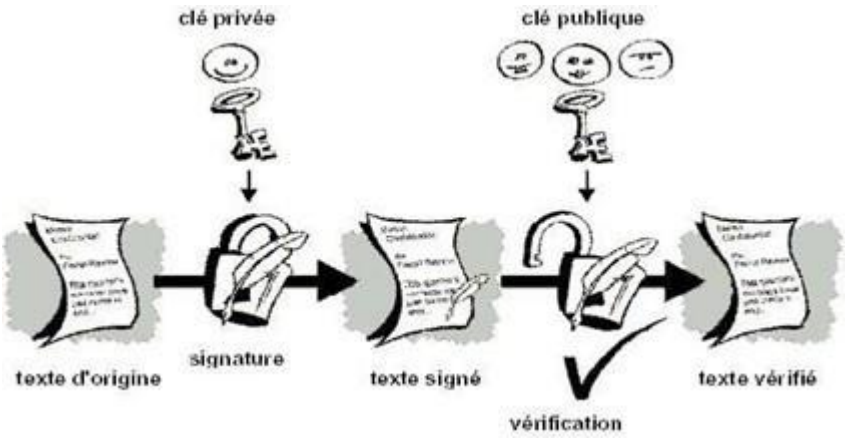


FIGURE 2.3 – Signature numérique

Non-répudiation

La non-répudiation est un principe de sécurité dans les réseaux sans fil qui garantit qu'une partie ne peut pas nier l'origine ou l'envoi d'un message ou d'une action. Cela signifie qu'une fois qu'une partie a envoyé un message ou effectué une action, elle ne peut pas le contester ou le nier ultérieurement. La non-répudiation est un principe de sécurité dans les réseaux sans fil qui garantit qu'une partie ne peut pas nier l'origine ou l'envoi d'un message ou d'une action. Cela signifie qu'une fois qu'une partie a envoyé un message ou effectué une action, elle ne peut pas le contester ou le nier ultérieurement. Elle est utilisée pour assurer la confiance et la responsabilité dans les échanges d'informations.

Confidentialité

La confidentialité est la propriété qui assure que l'information est rendu inintelligible aux individus, entités, et processus non autorisés.

Chiffrement

1. **Chiffrement symétrique :** la cryptographie symétrique (ou le cryptage des clés symétriques) est une classe d'algorithmes de cryptographie qui utilisent les mêmes clés cryptographiques pour le cryptage du texte clair et le décryptage du texte chiffré.

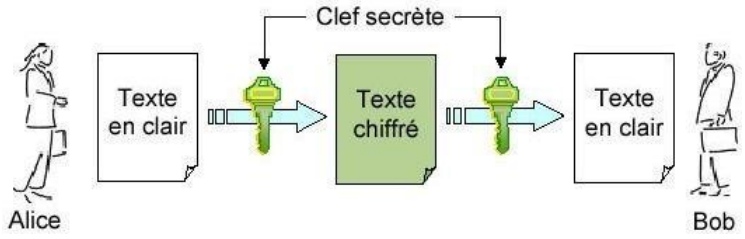


FIGURE 2.4 – Etapes de la cryptographie symétrique.

— **Algorithme DES (Data encryption standard) :** le DES (Data Encryption Standard) est un algorithme de chiffrement symétrique qui opère sur des blocs de 64 bits, transformant ainsi un bloc en un autre bloc de 64 bits. Il utilise des clés individuelles de 56 bits, représentées par 64 bits où un bit de chaque octet est réservé au contrôle de parité.

Le DES est basé sur le schéma de Feistel, du nom de Horst Feistel qui a également conçu le chiffrement Lucifer. Il suit les principes fondamentaux des fonctions cryptographiques, tels que la substitution (confusion) et la transposition (diffusion), ainsi que des opérations comme le décalage et le swap Ping. L'algorithme est composé de 16 tours, chacun utilisant une clé ronde unique. Les clés sont générées à partir d'un générateur de clés rondes, produisant des clés de 48 bits pour chaque tour.

Il est important de souligner que le DES était largement utilisé par le passé, mais il est maintenant considéré comme obsolète en raison de la longueur relativement

courte de sa clé et de ses vulnérabilités face aux attaques par force brute. Pour garantir une sécurité adéquate des données, il est recommandé d'utiliser des algorithmes de chiffrement plus robustes, tels que l'AES (Advanced Encryption Standard).[12]

— **IDEA (International Data Encryption Algorithm) :** l'algorithme IDEA (International Data Encryption Algorithm) est un algorithme de chiffrement symétrique. Il fonctionne sur des blocs de texte en clair de 64 bits et utilise une clé de chiffrement de 128 bits (qui doit être générée de manière aléatoire) pour chiffrer les données. Pour déchiffrer les données, la même clé secrète est nécessaire. Le processus de chiffrement se décompose en huit étapes identiques appelées "rondes", suivies d'une transformation du bloc de sortie [13].

— **L'algorithme AES (cipher bloc Advenced Encryption Standard) :** l'AES (Advanced Encryption Standard), également connu sous le nom de Rinjdaël, est le standard actuel utilisé pour les chiffrements symétriques. Contrairement au DES, il n'utilise pas de réseau de Feistel. Il opère sur des blocs de taille fixe de 16 octets (128 bits) et prend en charge trois variantes de taille de clé : 128, 192 et 256 bits. L'AES a été publié en 2001 à la suite d'un appel du NIST (Institut National des Standards et de la Technologie) qui a donné lieu à une compétition de cinq ans (FIPS-PUB 197) entre plusieurs algorithmes tels que MARS, RC6, Rinjdaël, Serpent et Twofish.

  En ce qui concerne les performances, l'AES128 est environ 2,7 fois plus rapide que le 3DES (Triple DES) et presque aussi rapide que le DES lui-même [14].

— **RC :** RC est une famille de chiffrement développée par les laboratoires de la RSA et nommée d'après son auteur, Ron Rivest. Les niveaux actuels sont RC4, RC5 et RC6. RC5 utilise une taille de clé allant jusqu'à 2048 bits; il est considéré comme un système fort. RC4 est très utilisé pour le chiffrement sans fil et WEP/WPA. Il s'agit d'un chiffrement en continu qui fonctionne avec des tailles de clé comprises entre 40 et 2048 bits, et il est utilisé pour le SSL et le TLS. Il est également prisé de certains utilitaires, qui l'utilisent pour télécharger des fichiers torrents. De nombreux four-

nisseurs limitent le téléchargement de ces fichiers, mais l'utilisation de RC4 pour brouiller l'en-tête et le flux fait qu'il est plus difficile pour le fournisseur de services de se rendre compte que les fichiers déplacés sont de type torrent.

2. Chiffrement asymétrique

La cryptographie asymétrique (ou algorithmes à clé publique) est un peu plus compliquée. Il contient deux clés, une pour le chiffrement et une pour le déchiffrement. Il s'agit d'une paire de clés publique/privée. Une clé privée est la propriété exclusive de son propriétaire et reste avec lui. Ainsi, l'expéditeur et le destinataire ont chacun quelque chose de très différent. Les clés publiques, en revanche, peuvent être connues de n'importe qui. Du fait des algorithmes utilisés, un message chiffré avec la clé privée ne peut être déchiffré qu'avec la clé publique et inversement (même si les deux clés sont mathématiquement liées, on ne peut pas le deviner). Crypté avec la clé publique du serveur, vous êtes certain que seul ce serveur avec la clé privée correspondante pourra décrypter le message

— **RSA :** RSA est un algorithme de chiffrement appartenant à la catégorie des systèmes cryptographiques asymétriques ou à clé publique. Son nom est dérivé des premières lettres des noms de ses trois inventeurs, Rivest, Shamir et Adleman. Il est largement reconnu comme l'un des algorithmes de chiffrement asymétriques les plus connus et utilisés.

L'algorithme RSA repose sur le choix d'un couple de deux nombres premiers, généralement appelés p et q, qui doivent être gardés secrets. Ces nombres premiers sont sélectionnés pour être aussi grands que possible afin de rendre la tâche de toute personne cherchant à attaquer le système extrêmement difficile. Ce couple de nombres va générer d'autres nombres qui constitueront la clé du procédé. Ainsi, le RSA fonctionne à partir de deux nombres premiers distincts.

Le produit de p et q est noté n, ce qui est appelé le module de chiffrement : n = p × q. De plus, on calcule l'indicatrice d'Euler de n, notée $\varphi(n) = (p-1) \times (q-1)$. Ensuite, un entier e est choisi, qui est premier avec $\varphi(n)$ et est appelé exposant de

chiffrement. il existe un entier d tel que $e \,.\, d = 1[\varphi(n)]$. Cet entier d est l'exposant de déchiffrement et explique le choix de la lettre d pour "decryption".

Enfin, après toutes ces étapes, nous obtenons deux couples de clés : la clé publique (n, e) et la clé privée (n, d). La clé publique est utilisée pour chiffrer les données, tandis que la clé privée est utilisée pour les déchiffrer. [14]

Certificat

Le problème de la clé publique est, par exemple, qu'un pirate réussit à remplacer la clé publique de l'utilisateur x par la sienne sur un répertoire. Et toutes les personnes croyant encrypter pour l'utilisateur x encrypterons pour le pirate. Par conséquent, les systèmes à clé publique ne garantissent pas que la clé appartienne réellement à l'utilisateur qui devrait la posséder.

Pour éviter les tentatives d'usurpation d'identité, vous devez configurer un dispositif d'authentification pour vérifier que la clé publique est bien associée à son propriétaire légitime et pour authentifier le gestionnaire des clés. Un certificat est un document délivré par une autorité reconnue qui prouve qu'un communicant possède une clé publique.Il doit être infalsifiable, sûr à obtenir et utilisable uniquement par le destinataire légitime.[15]

Un certificat contient généralement les éléments suivants : un numéro de série, une clé publique, un identifiant pour le propriétaire de la clé publique, des dates de validité (les dates de débutet de fin de validité),un identifiant pour l'AC délivrant le certificat et un certificat signé utilisant la clé privée de l'AC.

Toutes ces informations sont signées et délivrées par autorité de certification (souvent notée CA pour Certification Authority). Les clés publiques sont largement diffusées pour permettre aux utilisateurs de vérifier les signatures à l'aide de la clé publique de l'autorité de certification. [16]

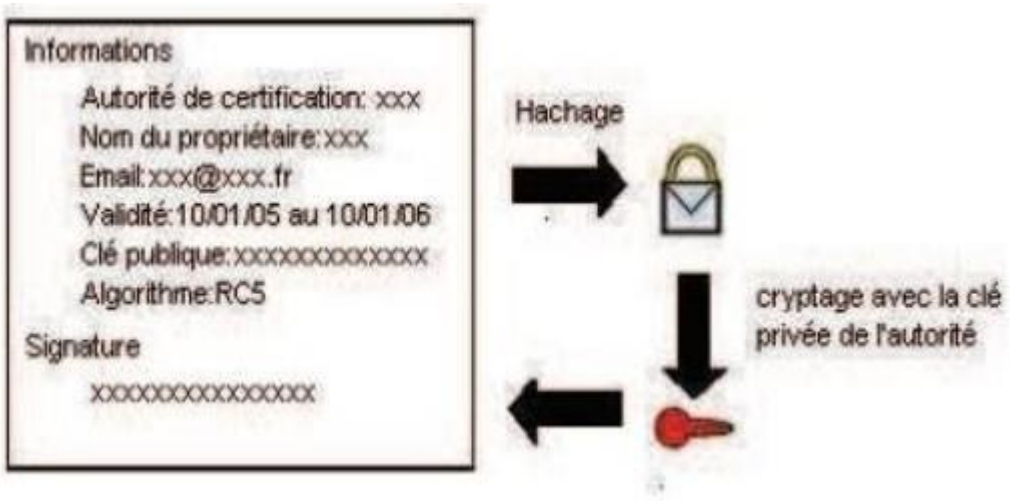


FIGURE 2.5 – Création d'un certificat numérique

Authentification

L'authentification dans un système informatique est un processus par lequel le système vérifie la légitimité d'une demande d'accès formulée par une entité, qu'il s'agisse d'un être humain ou d'un autre système. Ce processus permet à cette entité d'accéder aux ressources du système en respectant les paramètres de contrôle d'accès defines [17].

— Le modéle AAA : le terme AAA est une abréviation pour "Authentication, Authorization, and Accounting" (Authentification, Autorisation et Comptabilité en français). Il s'agit d'un modèle de sécurité couramment utilisé dans les réseaux informatiques pour contrôler l'accès aux ressources et assurer la traçabilité des activités des utilisateurs.

  Le modèle AAA est généralement mis en œuvre à l'aide de protocoles de réseau tels que RADIUS (RemoteAuthentication Dial-In User Service) et TACACS+ (Terminal Access Controller Access-Control System Plus). Ces protocoles permettent la communication entre les clients, les serveurs d'authentification et les serveurs d'autorisation, facilitant ainsi la gestion centralisée des utilisateurs et des autorisations d'accès.

— **Les protocoles AAA :** les deux principaux protocoles pour la communication entre un client et un serveur triple-A sont RADIUS et TACACS+. Toutefois nous pouvons mentionner d'autres, notamment DIAMETER et TACACS.

DIAMETER

Pendant longtemps, le seul protocole standard d'authentification entre un NAS (Network Access Server) et le serveur était RADIUS. Cependant, Diameter a été développé pour remplacer RADIUS en offrant des fonctionnalités plus riches. Diameter est normalisé dans la RFC 6733 Diameter Base Protocol, qui succède à la RFC 3588.

Ce protocole permet aux opérateurs d'authentifier des utilisateurs, de leur accorder l'autorisation d'accéder à certains services et de collecter des informations sur l'utilisation des ressources. Il a été conçu pour répondre aux nouveaux besoins suscités par la mobilité dans les réseaux. Le protocole de base de Diameter définit le format des messages, leur mode de transport, les messages d'erreur ainsi que les services de sécurité que toutes les implémentations doivent prendre en charge. En plus du protocole de base, il existe des applications spécifiques telles que Mobile IP, NAS et CMS [18].

Kerberos

Kerberos est un système d'authentification développé par le MIT. La version 5 du protocole a été normalisée par l'IETF dans la RFC 1510 (septembre 1993) et RFC 1964 (juin 1996). Le nom "Kerberos" provient de la mythologie grecque. Kerberos utilise des tickets pour permettre à un utilisateur de ne pas avoir à s'authentifier constamment auprès des différents serveurs auxquels il se connecte. Un système Kerberos est composé d'un serveur d'authentification (SA), d'un serveur de tickets (TGS), de clients et de serveurs de services.

L'authentification Kerberos repose sur le principe selon lequel chaque client d'un réseau donné doit s'identifier auprès d'un serveur global. Le client présente un ticket d'authentification préalablement fourni par ce dernier, et tout client muni de ce ticket est considéré comme authentifié [19].

TACACS+

TACACS+ (Terminal Access Controller Access Control Plus) est la version la plus récente du protocole TACACS, qui a été initialement développé par BBN(Le Bureau Burundais de Nor-

malisation) puis repris par Cisco. Contrairement à TACACS qui utilisait l'UDP (User Datagram Protocol) pour son transport, TACACS+ utilise TCP (Transmission Control Protocol). Une des caractéristiques distinctives de TACACS+ est sa gestion séparée des trois fonctions AAA (Authentification, Autorisation et Accounting), ce qui le différencie d'autres protocoles d'authentification [20].

LDAP

Le LDAP (Lightweight Directory Access Protocol), apparu en 1993, est un protocole qui permet d'interroger et de modifier des annuaires. Il offre la possibilité de rechercher et de modifier des informations dans ces annuaires. En plus de gérer l'authentification des utilisateurs, il permet également de gérer leurs habilitations dans un système informatique.

Aujourd'hui, le LDAP est devenu un standard incontournable en raison de sa capacité à s'adapter à de nombreux cas d'utilisation. Outre l'authentification, un annuaire LDAP est devenu essentiel au cœur d'un système informatique en raison de sa polyvalence [19].

RADIUS

RADIUS (RemoteAuthentication Dial-In User Service) est un protocole d'authentification client/serveur largement utilisé pour l'accès distant. Il est défini par la RFC 2865 et permet de sécuriser les réseaux contre les accès à distance non autorisés. Le protocole RADIUS est conçu pour fonctionner indépendamment du type de support utilisé.

Dans le protocole RADIUS, un serveur RADIUS est connecté à une base d'identification telle qu'un fichier local, une base de données ou un annuaire LDAP. Un client RADIUS, appelé NAS (Network Access Server), agit en tant qu'intermédiaire entre l'utilisateur final et le serveur. Pour authentifier les transactions entre le client RADIUS et le serveur, le mot de passe est chiffré et authentifié à l'aide d'un secret partagé.

Il convient de mentionner que le serveur RADIUS peut également fonctionner en tant que proxy, c'est-à-dire qu'il peut transmettre les requêtes du client à d'autres serveurs RADIUS.

Cela permet d'étendre la portée de l'authentification et de l'autorisation à travers des serveurs RADIUS interconnectés.

— **Fonctionnement**

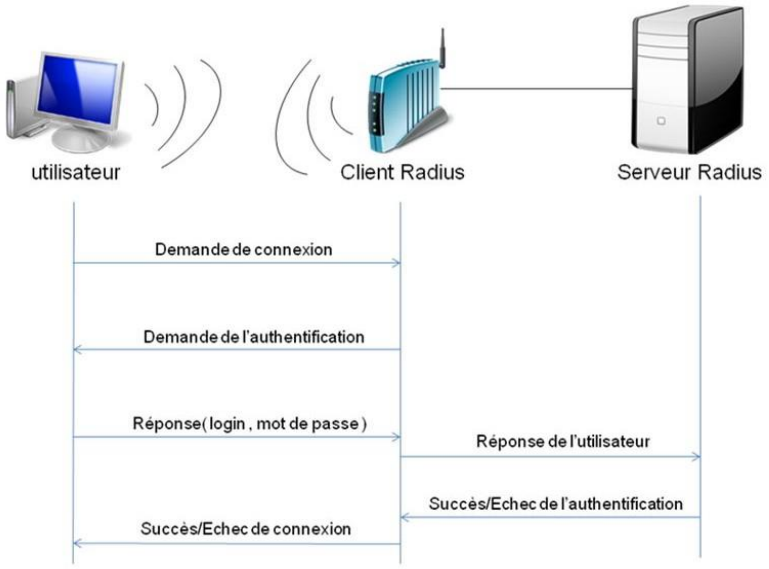


FIGURE 2.6 – Le fonctionnement de Radius.

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

1. Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance.
2. Le NAS achemine la demande au serveur Radius.
3. Le serveur Radius consulte la base de données d'identification afin de connaître le type des scénarios d'identification demandé pour l'utilisateur. Si le scénario actuel est approprié, il est utilisé. Sinon, une autre méthode d'authentification est demandée à l'utilisateur.

Le serveur Radius retourne ainsi une des quatre réponses suivantes :

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

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

— **CHALLENGE :** le serveur RADIUS souhaite collecter des informations supplémentaires de la part de l'utilisateur et propose un « défi » (en anglais « challenge »).

— **CHANGE PASSWORD :** le serveur Radius demande à l'utilisateur un nouveau mot de passe. Suite à cette phase d'authentification débute une phase d'autorisation ou le serveur retourne les autorisations aux utilisateurs [21] .

— **Format d'un paquet RADIUS**

L'en-tête du paquet Radius comporte 5 champs 5 :

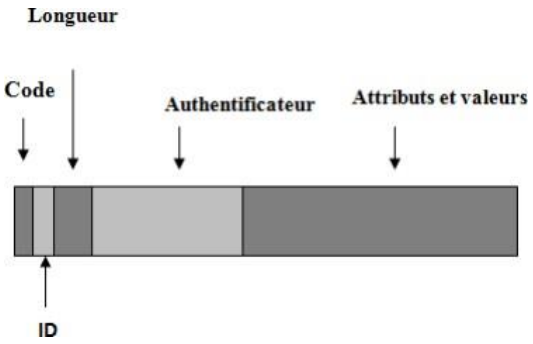


FIGURE 2.7 – Format des paquets RADIUS

[7].

— **Code :** Définit le type de trame (acceptation, rejet, challenges, requête).

— **Identifier :** Associe les réponses reçues aux requêtes envoyées.

— **Length :** Champ longueur.

— **Authentificator :** champ d'authentification comprenant les éléments nécessaire.

— **Attribuées :** Ensemble de couples (attribut, valeur) [17].

Le protocole EAP (Extensible Authentication Protocol)

Le protocole EAP (Extensible Authentication Protocol) est un protocole d'authentification utilisé dans les réseaux informatiques pour vérifier l'identité des utilisateurs et leur accorder l'accès aux ressources réseau. Il est conçu pour être extensible, ce qui signifie qu'il peut prendre en charge différentes méthodes d'authentification.

Le fonctionnement d'EAP repose sur un échange de messages entre le client et le serveur d'authentification. Le client envoie une demande d'authentification au serveur, qui répond en proposant une méthode d'authentification prise en charge par les deux parties. Le client et le serveur échangent ensuite des messages pour effectuer l'authentification selon la méthode choisie.

EAP est couramment utilisé dans les réseaux sans fil sécurisés, où il permet d'établir une authentification robuste entre les clients et les points d'accès. L'objectif de l'authentification basée sur EAP dans un réseau non ouvert est de vérifier l'identité d'un utilisateur avant de lui accorder l'accès au réseau. Dans ce type de réseau, seuls les échanges EAP sont autorisés initialement afin de permettre l'authentification. Une méthode d'authentification EAP utilise différents éléments tels que des couples "login/mot de passe", des certificats électroniques, des cartes à puce (SIM), etc.

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

EAP-TLS est une méthode d'authentification mutuelle où le client et le serveur se prouvent respectivement leur identité. Lors de l'échange EAP-TLS, le client d'accès à distance envoie son certificat utilisateur et le serveur d'accès à distance envoie son certificat d'ordinateur. Si l'un des certificats n'est pas envoyé ou n'est pas valide, la connexion est interrompue. EAP-TLS utilise le protocole de sécurité TLS, version normalisée de SSL (Secure Socket Layer), qui offre un transport sécurisé incluant le chiffrement, l'authentification mutuelle et le contrôle d'intégrité.

Dans ce contexte, la méthode EAP-TLS est privilégiée en raison de sa sécurité accrue. L'authentification du client d'accès peut se faire de différentes façons avec EAP-TLS :

— En utilisant un certificat associé à la machine, l'authentification a lieu au démarrage de la machine.

— En utilisant un certificat associé à l'utilisateur, l'authentification a lieu après la connexion de l'utilisateur.

Le schéma représente une connexion Wi-Fi utilisant un serveur d'authentification EAP avec un certificat. Le processus débute lorsque le serveur envoie une requête d'authen-

tification au client. Le client peut répondre en utilisant un mot de passe, une carte à jeton ou un certificat.

Dans ce cas précis, le client ne possédant pas de carte à jeton, il propose une alternative d'authentification au serveur, qui choisit alors le certificat.

Après vérification par le serveur, le client envoie une requête pour s'associer au point d'accès. Si le serveur accepte la demande, le client est alors connecté au réseau.

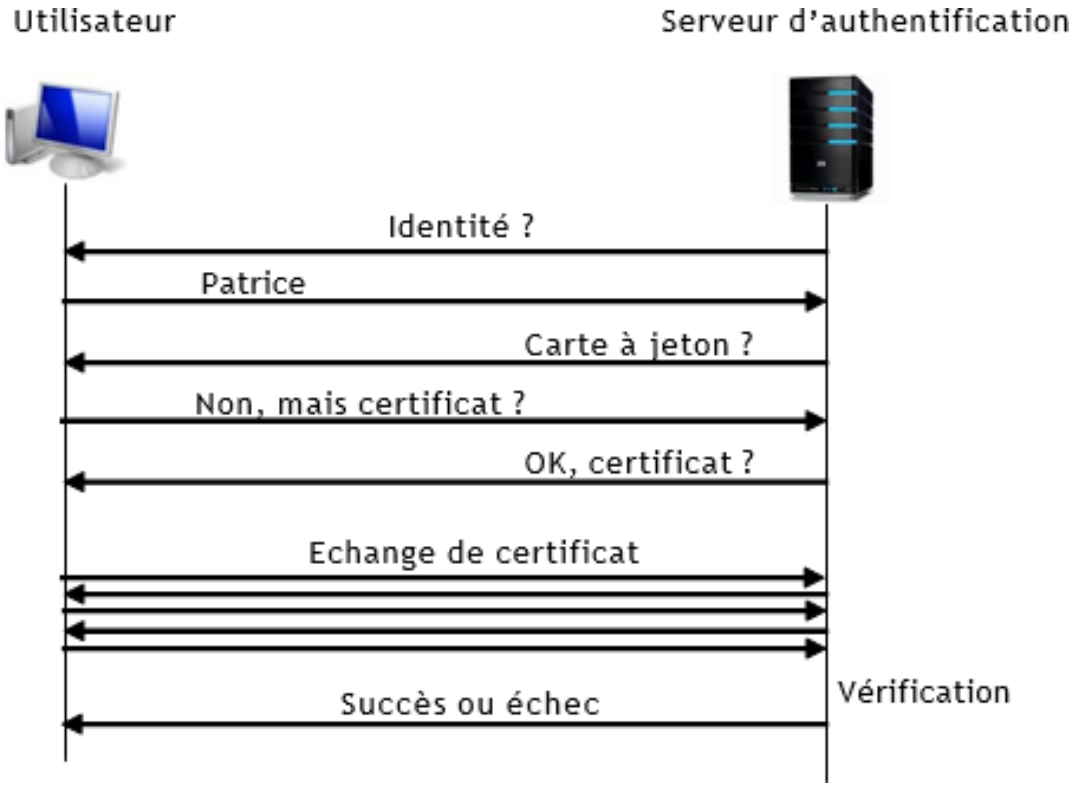


FIGURE 2.8 – Une connexion Wi-Fi avec un certificat.

Contrôle d'accès

Le contrôle d'accès est un élément incontournable de la sécurité et détermine qui est autorisé à accéder à certaines données dans quelles circonstances.

Filtrage des adresses mac

Le filtrage par adresses MAC est une méthode utilisée pour empêcher les accès non autorisés aux réseaux locaux sans fil. Elle repose sur l'utilisation des adresses MAC (Media Access Control) des utilisateurs mobiles. Chaque carte réseau possède une adresse MAC unique qui permet de l'identifier de manière distincte. Dans cette méthode, un point d'accès peut stocker une liste de contrôle d'accès contenant les adresses MAC des utilisateurs autorisés à se connecter au réseau sans fil via ce point d'accès. Ainsi, tout utilisateur mobile ayant une adresse MAC qui ne figure pas dans la liste de contrôle se verra automatiquement refuser l'accès.

Cependant, la mise en place de cette technique requiert un travail conséquent de la part de l'administrateur réseau, qui doit programmer tous les points d'accès avec les bonnes adresses MAC et les maintenir à jour. De plus, cela limite la mobilité des utilisateurs aux points d'accès préalablement enregistrés avec leurs adresses MAC. En outre, il est important de noter que dans certains cas, des individus malveillants peuvent modifier l'adresse MAC des cartes réseau sans fil à l'aide d'outils de modification du firmware, contournant ainsi le filtrage par adresses MAC.

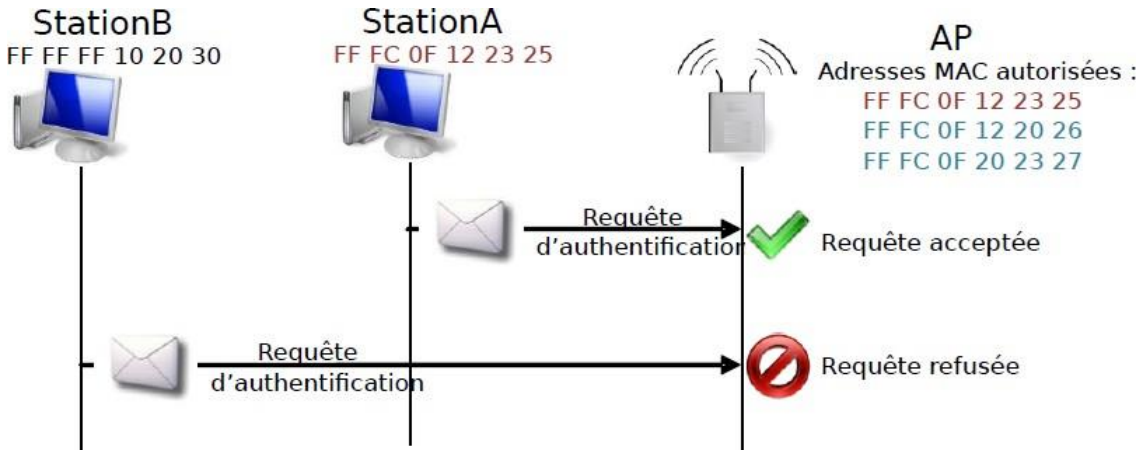


FIGURE 2.9 – Filtrage des adresses mac[23]

Protocole WPA

Le Wireless Protected Access (WPA) est une version simplifiée du standard 802.11i. Il comprend deux variantes : le WPA Personal, également connu sous le nom de WPA-PreShared Key (WPA-PSK), et le WPA Enterprise. Le WPA-PSK nécessite la configuration d'une clé partagée dans tous les points d'accès (AP) et les appareils connectés au réseau. Le WPA Enterprise repose sur le protocole 802.1x et un serveur d'authentification RADIUS (RemoteAuthentication Dial In User Service) [22].

Fonctionnement

Il existe 2 types de WPA, la version personal la plus utilisée, mais aussi la version enterprise utilisant un serveur d'authentification.

— **Authentification par des clés pré-partagées**

Le mode personnel du WPA permet de créer une infrastructure sécurisée basée sur le WPA sans nécessiter l'utilisation d'un serveur d'authentification. Il repose sur l'utilisation d'une clé partagée appelée PSK (Pre-Shared Key), qui est configurée à la fois dans le point d'accès et dans les postes clients. Cette clé est générée à partir d'une phrase secrète (passphrase) en utilisant un algorithme de hachage.

Lors d'une connexion Wi-Fi de base, le processus d'authentification débute lorsque le client envoie une requête au point d'accès. Le point d'accès répond à cette requête, et si l'authentification réussit, le client envoie une requête pour s'associer au point d'accès. Si le point d'accès accepte, le client est alors connecté au point d'accès [23] .

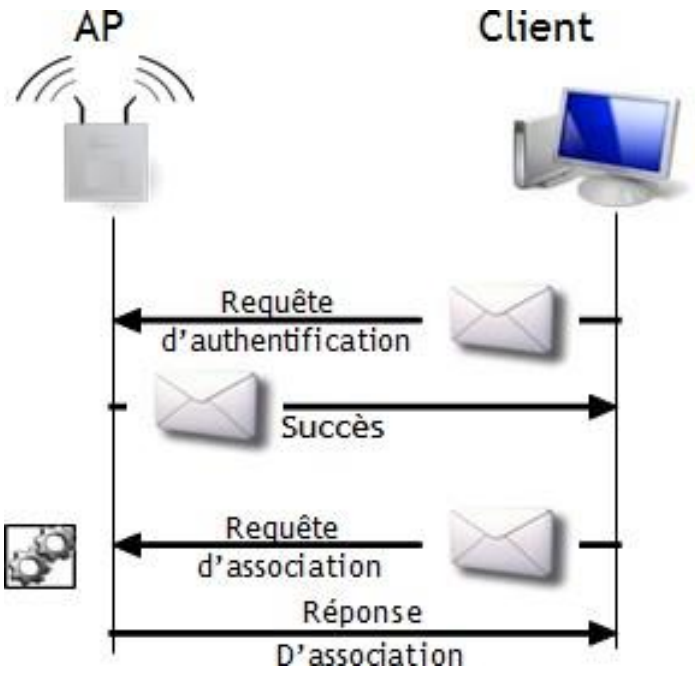


FIGURE 2.10 – Authentification par des clés pré-partagées [23]

— **WPA enterprise : architecture 802.1x (RADIUS avec EAP)**

Le mode Enterprise du WPA requiert l'utilisation d'une infrastructure d'authentification 802.1x, qui repose sur un serveur d'authentification tel qu'un serveur RADIUS (RemoteAuthentication Dial-in User Service) et un contrôleur réseau, généralement le point d'accès lui-même.

Dans ce mode, le protocole EAP (Extensible Authentication Protocol) est utilisé pour identifier les utilisateurs avant de leur permettre d'accéder au réseau. Plusieurs méthodes d'authentification peuvent être utilisées, telles que les mots de passe, les cartes à puce, les certificats électroniques, etc.

Voici le schéma illustrant le fonctionnement de la connexion Wi-Fi avec un serveur d'authentification dans la version WPA Enterprise. Les clients sont connectés au point d'accès, mais pour accéder au réseau, ils doivent s'authentifier auprès du serveur d'authentification.

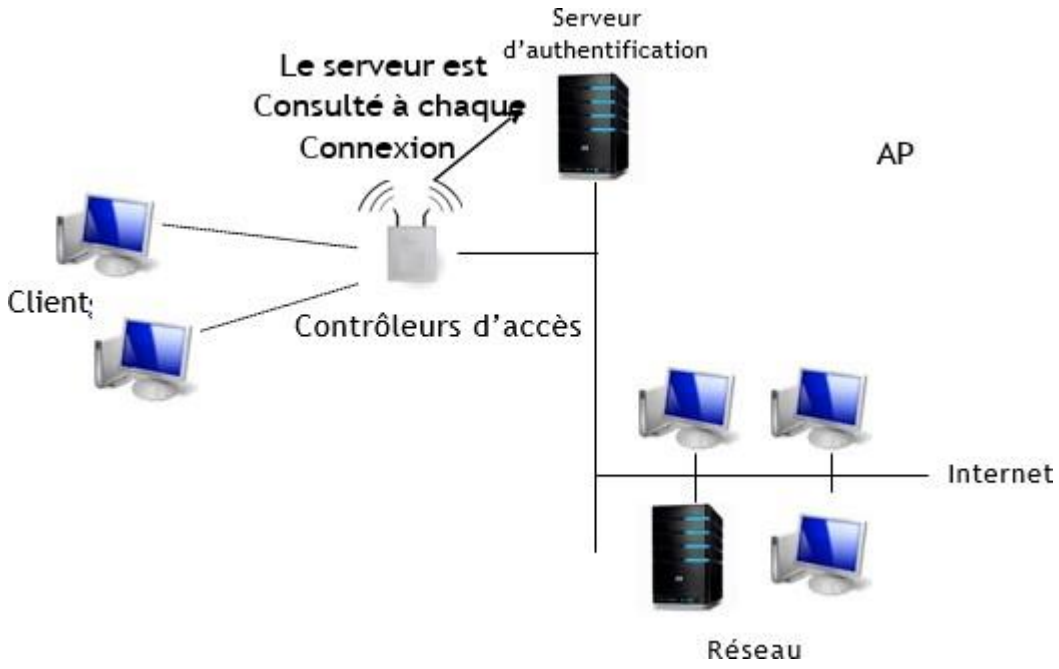


FIGURE 2.11 – Le fonctionnement du Wi-Fi avec un serveur d'authentification

Le protocole WPA (Wi-Fi Protected Access) est utilisé pour sécuriser les réseaux sans fil. Il fonctionne en utilisant des clés WPA dynamiques spécifiques à chaque utilisateur, renforçant ainsi la sécurité globale du réseau. Ces clés sont générées une fois qu'un utilisateur est authentifié avec succès et sont utilisées pour chiffrer les données en transit sur le réseau sans fil, assurant ainsi leur confidentialité.

Pour détecter toute altération ou manipulation des données en transit, le protocole WPA utilise un code de vérification d'intégrité (MIC - Message Integrity Code). Lorsqu'un appareil envoie des données à travers le réseau sans fil, il génère un code de vérification d'intégrité unique en utilisant un algorithme de hachage spécifique. Ce code est ensuite comparé par le destinataire avec celui envoyé par l'émetteur pour garantir l'authenticité et l'intégrité des données.

TKIP (Temporal Key Integrity Protocol) est utilisé dans les réseaux WiFi pour assurer la sécurité et l'authentification des données en transit. Le protocole WPA utilise TKIP, qui utilise l'algorithme de chiffrement RC4 avec une clé de 128 bits, pour chiffrer les données lors de leur transmission entre les appareils du réseau.

Pour prévenir les attaques basées sur l'analyse de la clé, le protocole WPA recommande de changer périodiquement la clé TKIP utilisée pour le chiffrement des données. Cela rend plus difficile pour un attaquant de décrypter les données en cas de compromission d'une clé.

Dans le processus de calcul du code de vérification d'intégrité, l'adresse MAC (Media Access Control) de l'appareil émetteur est incluse. Cela ajoute une couche de sécurité supplémentaire, car l'adresse MAC est également utilisée dans le calcul du code MIC. Ainsi, falsifier ou modifier le code MIC nécessiterait également de falsifier l'adresse MAC, rendant la tâche plus difficile pour un attaquant.

En utilisant ces mécanismes d'authentification, de chiffrement, de changement de clé périodique et de vérification d'intégrité, le protocole WPA offre une sécurité améliorée pour les réseaux sans fil. Il garantit la confidentialité et l'intégrité des données en transit, assurant ainsi la protection des informations échangées sur le réseau.

2.5 conclusion

En conclusion, la sécurité des réseaux sans fil est un domaine complexe et en constante évolution. Il est essentiel de prendre des mesures adéquates pour protéger les réseaux Wi-Fi et les données qu'ils véhiculent. En utilisant des solutions telles que le chiffrement, les certificats et les protocoles d'authentification robustes, il est possible de renforcer la sécurité des réseaux sans fil et de prévenir les attaques potentielles

Chapitre 3

Présentation de l'organisme d'accueil

Introduction

Ce chapitre sera réservé à la présentation du campus NTS (New Technology § Solutions) où nous effectuons notre stage. Dans un premier temps, nous aborderons un bref aperçu de l'entreprise pour mieux comprendre sa structure et ses objectifs. Nous étudierons ensuite l'architecteur réseau de son client « ngtmeziani » et ses composantesafin de pouvoir suggérer d'éventuelles améliorations.

Partie 1 : Présentions de l'entreprise « Campus NTS »

Création et évolution

NTS est une jeune entreprise axée sur la recherche, la conception et la mise en œuvre de solutions, d'intégration de systèmes de sécurité, d'importation et de la distribution d'équipements et de matériels de sécurité des réseaux et des télécommunications, de la formation et le conseil. Elle a été créeen 2020à Bejaia par Yassine djebbari, qui a de nombreuses d'années d'expérience et a réalisé d'importants projets dans différents secteurs et régions du pays, comme référence :

- Air Algérie.
- Retelem Alger.
- Poste d'Algérie.
- Adèle.
- RATP ALJAZAIR.
- La technologie.
- Géant de l'électronique BBR.
- Morsi.
- Université de Bejaïa.
- Cité universitaire à Bejaïa (targaouzamour, 17 octobre, etc.).

— SARL Alphas Bejaïa.

— ProvidentiaBéjaïa.

La localisation de l'entreprise

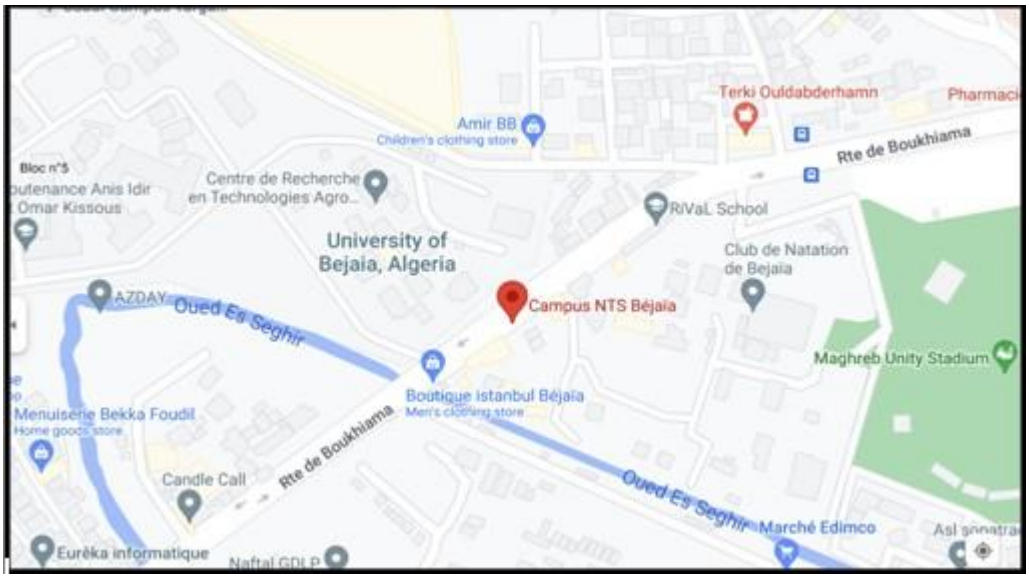


FIGURE 3.1 – Localisation de l'entreprise NTS.

Fiche technique

Le tableau 1 ci-dessous représente quelques informations relatives à l'entreprise dans laquelle nous avons effectué notre stage de projet de fin d'étude.

Dénomination	Campus NTS
Logo	
Siège	Bâtiment A les beaux quartiers TargaOuzemour, Béjaïa 06000
Secteurs d'activités	Informatique et telecommunication
Numéros de FAX	044 204 400
Numéros de Téléphone	0770446101
Email	contact@campus-nts.com
Site Internet	http://www.campus-nts.com/

Objectifs, Missions et activités de l'Entreprise « N.T.S »

Les objectifs, les missions et les activités sont représentées dans la figure 2 :

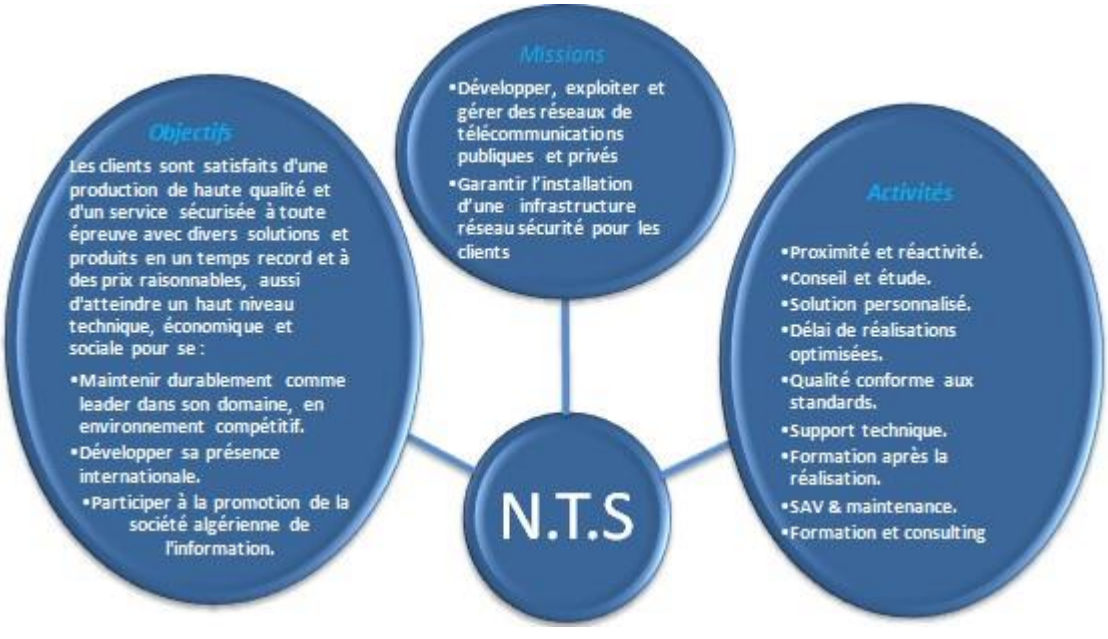


FIGURE 3.2 – Objectifs, Missions et Activités de l'NTS..

Organigramme général de l'organisme d'accueil

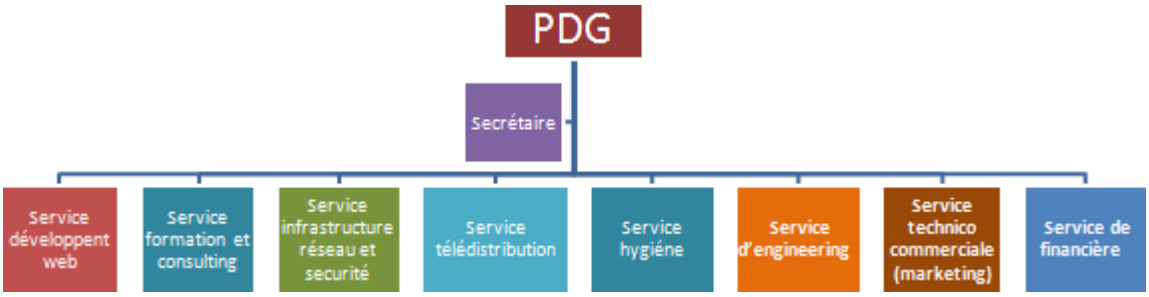


FIGURE 3.3 – L'organigramme de campus NTS.

Nous allons nous contenter de présenter ci- dessous la description de l'organigramme du campus NTS (voir la figure 3) dans lequel cet apprentissage termine le stage :

1. **Service développement web**

   Il est responsable de la création des sites web, des applications pour internet, applications mobiles ou des solutions logicielles adaptées aux besoins des clients utilisant des langages de programmation informatique tels que : HTML5, CSS, JavaScript ou PHP. En général, il représente les tâches liées au développement du site Web en améliorant son positionnement sur les moteurs de recherche qui seront hébergés sur Internet.

2. **Service formation et consulting** Ce secteur a été créé par le campus NTS pour offrir des stages et des formations professionnelles dans les domaines suivants :

   — Installation et configuration des réseaux informatiques.

   — Administration et sécurité des réseaux et système.

   — Installation et configuration des firewalls (pfsense, Sophos, fortigate, palo alto…).

   — Installation et configuration des réseaux sans fil professionnel.

   — Installation et configuration des caméras de surveillance analogique et numérique.

— Fibre optique les réseaux d'accès FTTH/FTTX.

— Création des sites web.

— Programmation (C, C++, C, Java, Python…etc.).

— Electricités Bâtiments et industriels.

— Formation Cisco CCNA, CCNP SR.

— Virtualisation.

— Microsoft server, SQL

— Cyber sécurité.

Ces stages s'adressent aux étudiants, ouvriers, entreprises en fin de projet et à tous ceux qui apprécient le terrain pour développer leurs compétences en sécurité, acquérir des qualifications supérieures et leur expérience en entreprise. NTSrepose sur la capacité des ressources et desstructures à délivrer à ses clients et à ses partenaires (Alhua, Hikvision, Cisco, Legend, Mikrotik, Zkteco, Commax, D-link, Alcatel-Lucent, Synology, Microsoft, Apollo, Panasonic, Huawei).

3. Service d'accueil

Présentation de service infrastructure réseau et sécurité

L'infrastructure réseau est au cœur des opérations commerciales dans la plupart des industries. Il peut être considéré comme le centre sensible de toute l'organisation informatique car il centralise les données, simplifie les échanges de données et facilite la communication entre les employés. A ce titre, il est un outil important pour le fonctionnement normal de l'entreprise et nécessite une attention constante en matière de sécurité. Ceci afin d'empêcher le nombre croissant et l'affectation des attaques externes et internes.

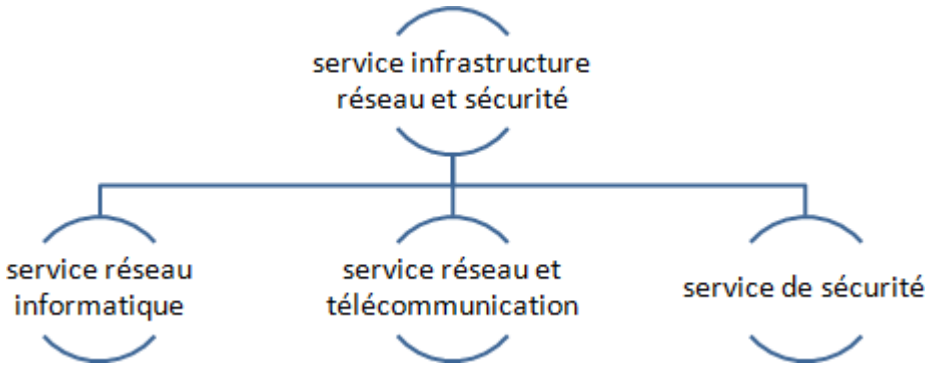


FIGURE 3.4 – Organigramme de service d'accueil.

4. Service réseau informatique

Ce service représente tous les appareils et périphériques au sein d'une entreprise qui sont physiquement ou virtuellement connectés les uns aux autres à partir d'un wifi professionnel ou d'autre méthodes afin de partager des ressources ou des informations. En fait, l'infrastructure réseau offre un large éventail de fonctionnalités pour les clients de services et les producteurs de services, telles que : Limitation de débit, analyse, vérification, surveillance et enregistrement et sécurisation du réseau de cette entreprise.

5. Service réseau et Télécommunication

Les services de télécommunications sont conçus pour transmettre des informations en un temps réel (synchronisation des informations) sous forme analogique ou numérique à l'exception de la radio et de la télévision. La plupart de ces services peuvent aider les clients à identifier leurs besoins en matière d'infrastructure de télécommunications. Voici des exemples de services d'infrastructure de télécommunications :

— pose de fibre optique.

— Emplacement du site de la tour cellulaire

— Test d'antenne radio. **I**nstallation d'équipements téléphoniques standards et réseau de données.

— Téléphonie standard.

6. **Service de sécurité** Cette entreprise NTS accomplit à la fois le gardiennage et l'installation des systèmes de sécurité électroniques. Aussi elle fournit aux clients des solutions complètes et fiables pour protéger leurs ressources. Les services qu'elle réalise sont les suivants :

   — Caméras de surveillance.

   — Alarme anti- intrusion.

   — Détection incendie .

   — Pointeuse et Contrôles d'accès.

   — Vidéophonie.

7. **Service télédistribution** Ce service est spécialisé dans la transmission de données par câble (fibre optique, paire torsadée et onde horizontale) ou autres systèmes de distribution (paraboles collectif, télévision numériques terrestre et audiovisuelle). Son objectif principal est de garantir l'installation de ces supports de transmission à haut débit. Enfin, les services de télédistribution ont été appelés à jouer un rôle majeur dans l'émergence des nouveaux médias tel que :

   — Rediffusion de programmation par satellite.

   — Transmission de chaînes de télévision par abonnement.

   — Services interactifs.

   — Programmation locale.

8. **Service d'engineering** Il est constitué d'une équipe multidisciplinaire d'experts dont la mission est de rechercher et d'analyser les besoins des clients pour trouver la meilleure solution spécifique à leur projet. L'équipe de campus NTS n'hésite pas à se circuler sur le terrain pour consulter l'état d'avancement du projet afin de faire face à d'éventuelles difficultés qui auraient pu survenir auparavant. Cette équipe est composée :

   — D'ingénieurs en télécommunications.

— D'informaticiens en gestion et sécurité des réseaux

— D'administrateurs de systèmes d'information.

— D'informaticiens en programmation.

— De techniciens fibre.

— De techniciens supérieurs en informatique.

Leurs propositions sont en recherche informatique et sécurité et leurs cotations est dans la recherche sur les réseaux et les systèmes de télécommunication.

9. **Service technico commerciale (marketing)**

Leurs offres ne se limitent pas à de simples fournitures standards. Ils disposent d'une équipe qui s'assure de répondre aux besoins et au confort de ses précieux clients dans le but de développer les services de cette entreprise. Par ailleurs, ce service commercialise aussi les services proposés par campus NTS.

10. **Service de financière**

Le service financier situé au cœur del'entreprise, représente l'ensemble des personnes chargées de la fonction comptable. Il intervient pour faire de bons investissements en prévenant d'éventuels risques de perte. Ce service contient un ensemble de tâches et rôles au sein de la société NTS :

Les tâches principales du Service des finances :

— Assurer une saine gestion des ressources financières de l'entreprise par la planification.

— La coordination et le contrôle de toutes les politiques et procédures requises pour la protection des actifs.

— La production des informations financières exactes et pertinentes afin que le gestionnaire puisse prendre la décision éclairée.

Le rôle du service financier :

— La préparation et du suivi des budgets de fonctionnement et d'investissement.

— La préparation des états financiers.

- La gestion de la trésorerie et de des encaissements.
- La rémunération des employés, des comptes à payer.
- De l'acquisition des biens et services pour l'ensemble de l'entreprise, des projets de recherche.
- La réception des marchandises et du courrier.

11. **Service hygiène** La sécurité et la santé occupent une place prépondérante dans les conditions de travail. L'employeur est en effet responsable de la santé et de la sécurité de ses salariés. Il coordonne ses différentes équipes et attribue les moyens nécessaires tel que :
    - Des actions de prévention des risques professionnels et de la pénibilité au travail.
    - La mise en place d'une organisation et de moyens adaptés.

Partie 2 : Etude des lieux du client « NGTMEZIANI »

Présentation du réseau « NGTMEZIANI»

Afin de bien comprendre les domaines dans lesquels un service informatique souhaite amé- liorer ses capacités et les besoins et contraintes d'information à respecter, nous examinerons un ensemble de spécifications pour l'infrastructure informatique et technique dont le service a besoin. Cette section contient tous les détails sur l'infrastructure réseau et matérielle.

Architecture réseau « NGTMEZIANI»

Le service informatique ngtmeziani a mis en place son réseau en choisissant une topologie en étoile pour relier ses différents équipements et ces sites distant comme le montre la figure suivante :

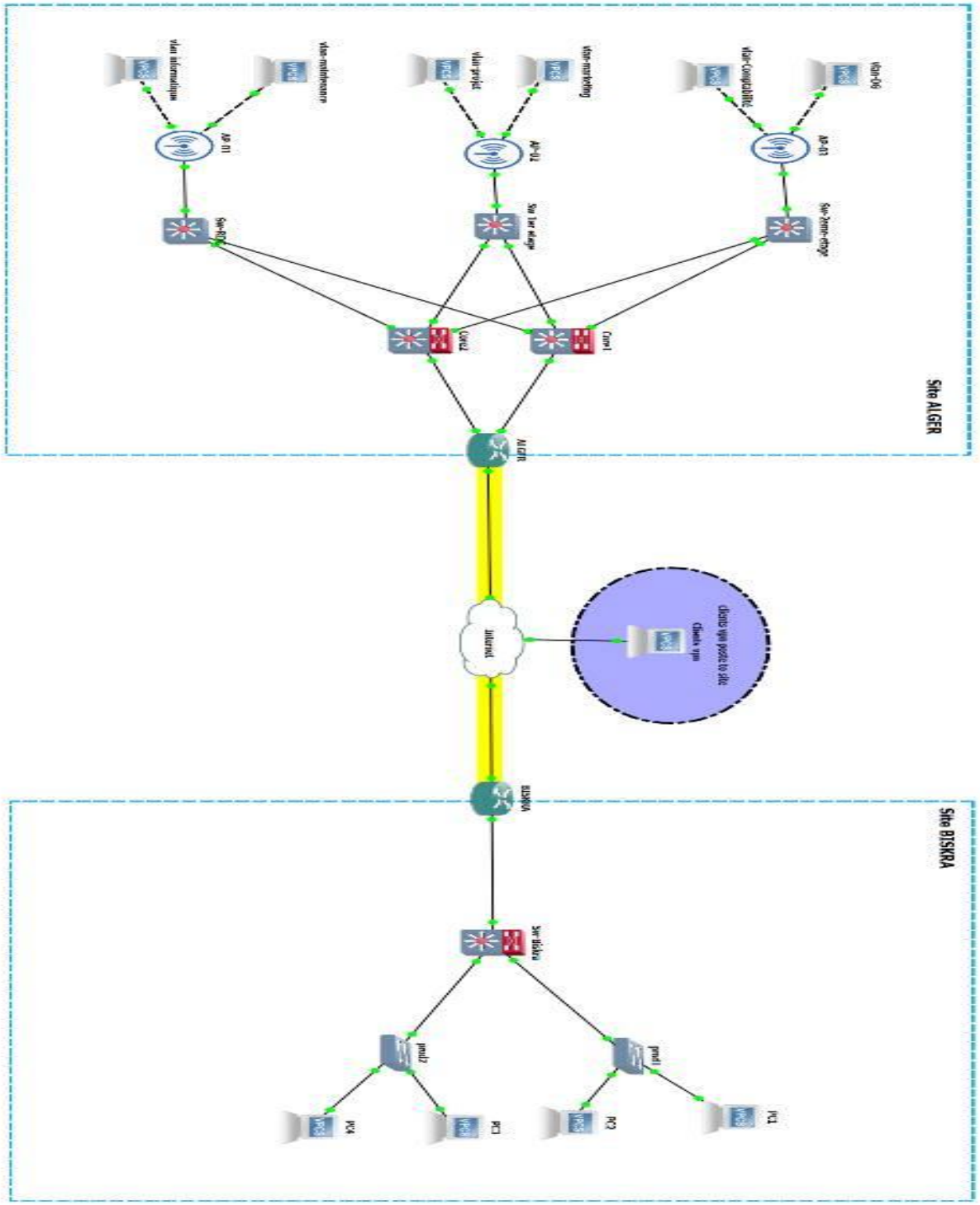


FIGURE 3.5 – Topologie de réseau NGTMEZIANI.

— **Analyse du parc informatique** Les périphériques connectés dans sont : les ordinateurs, téléphones et les imprimantes Le tableau suivant contient les statistiques des périphériques par service :

Services	Nombre d'hôtes	Type de connexion
Informatique	25	RJ45 ET WIFI
Maintenance ET SAV	08	RJ45 ET WIFI
Projets	10	RJ 45 ET WIFI
Marketing	18	RJ45 ET WIFI
Comptabilité	12	RJ45 ET WIFI
Direction Générale	04	WIFI

TABLE 3.1 – Nombre de périphérique par service

— **Matériel utilisé :** Le matériel utilisé dans le réseau sont :

- Firewall
- Switches Multicouche
- Switches d'accès
- Les Points d'accès
- Les ordinateurs et imprimantes
- Serveurs
- Prises RJ45
- Câbles à paire torsadée
- Câble à fibre optique pour les armoires

Nom de l'équipement	Le hardware (hard)	Software (soft)
Firewall 	FortiGate 1800F Series	FortiOS ortinet *Operating System)*
Switches Multicouche 	Cisco MDS 9000	IOS (*Internetwork Operating System)*
Switches d'accès **ackable (Empilable)** 	Catalyst 9200 multi gigabit 48 ports	IOS (*Internetwork Operating System)*
ordinateurs 	DELL PC Bureau : Optiplex 7080 MT PC portable : DELL LATITUDE 5300	Windows 10 et 11
Serveurs 	Serveur HPE ProLiant DL380 Gen10	ESXi Server Windows Server 2021 Linux server
Point d'accès 	Tenda	Tenda web

Partie 3 : Problématiques et Solutions proposées

Problématiques

Durant le stage effectué au niveau de service projet réseau et sécurité informatique pour le client « NGTMEZIANI », nous avons pu constater que ce client « NGTMEZIANI » possèdent de nombreux postes informatiques reliés entre eux par un réseau local filaire et sans fils, Nous avons pu mettre en évidence des failles de sécurité de ce réseau telles que :

- La possibilité d'accès non autorisé au réseau wifi peut se produire si les mures de sécurité telles que les mots de passes faibles, les clés de cryptage obsolètes ou la mauvaise configuration des points d'accès permettent à des personnes non autorisées de se connecter.
- Des utilisateurs interne et externe peuvent consommer de manière successive la bande passante du réseau wifi de l'entreprise ce qui peut entrainer une dégradation des performances pour les utilisateurs légitimes.
- Le réseau peut subir des attaques citons l'attaque par déni de service (DOS) qui peut paralysée le réseau wifi de l'entreprise en surchargent le réseau avec une quantité excessive de trafique empêchant ainsi les utilisateurs autorisé d'accéder au ressources réseaux.
- Les points d'accès non configurer correctement ou utilise des mots de passe par défaut est susceptibles d'être compromis et exposer a des attaques par force brute.
- Absence de point de centralisation et de gestion des comptes et droit des accès systèmes.
- Absence d'un contrôleur dans l'architecture du réseau de l'entreprise .

Solutions

L'objectif principal de notre étude est la mise en œuvre d'une solution d'administration et d'authentification qui nous permet de mieux gérer et sécuriser l'accès aux services

réseaux de « NGTMEZIANI », pour cela nous avons opté pour les solutions suivant à savoir :

1. L'utilisation d'un contrôleur wifi peut s'avérer très utile pour la sécurité du réseau sans fil de l'entreprise.
2. La certification des ordinateurs de l'entreprise.
3. Pour la certification, nous devons implépenter un serveur d'authentification et dans notre cas c'est le serveur **RADIUS.**
   - Radius offre plus que de l'authentification, il fournit également une gestion des autorisations d'accès et une journalisation des échanges. Cette solution permet de centraliser les identifiants, de gérer les mots de passe et les processus d'authentification pour les clients. De plus, Radius permet de définir les accès des utilisateurs distants à un réseau et de sécuriser l'accès à distance en utilisant des certificats.
4. Utilisation de la norme 802.1x qui, associé aux fonctions PEAP-TLS,

Conclusion

Dans ce chapitre, nous avons donné un aperçu général de l'entreprise du campus NTS et son Client NGTMEZIANI, puis nous avons découvert un problème qui nous a amenés à rechercher de mettre en œuvre une architecture qui puisse améliorer la sécurité des réseaux sans fil. Enfin, l'application de la solution proposée fera l'objet du chapitre suivant.

Chapitre 4

Partie Pratique

Introduction

Ce chapitre pratique se focalise sur la mise en place d'un réseau sans fil sécurisé en utilisant des technologies avancées telles que RADIUS (RemoteAuthentication Dial-In User Service) et les certificats PEAP/TLS (Protected Extensible Authentication Protocol/Transport Layer Security). Pour ce faire, nous avons utilisé deux environnements de simulation distincts, à savoir Cisco Packet Tracer et VMware, afin de modéliser et de tester notre solution de réseau sans fil.

Dans les prochaines sections de ce chapitre, nous examinerons en détail les différentes étapes de déploiement du certificat PEAP/TLS. Nous mettrons en évidence les configurations spécifiques effectuées et les manipulations réalisées pour assurer une mise en œuvre efficace. De plus, nous présenterons les résultats obtenus lors de nos expérimentations.

Environnement de développement

Dans le domaine des réseaux informatiques et de la virtualisation, nous avons utilisé deux outils sont Packet Tracer version 8.2.0 et VMware. Ces outils offrent des fonctionnalités puissantes pour la simulation de réseaux et la création de machines virtuelles, respectivement.

— Packet Tracer version 8.2.0 est un logiciel de simulation réseau développé par Cisco Système. Il est utilisé dans les environnements éducatifs et professionnels pour concevoir, configurer et tester des topologies réseau virtuelles. Grâce à Packet Tracer, les utilisateurs peuvent simuler le comportement des périphériques réseau tels que des routeurs, des commutateurs et des hôtes, et expérimenter différentes configurations et scénarios réseau.

— VMware, quant à lui, est une plateforme de virtualisation largement utilisée pour créer et gérer des machines virtuelles sur un ordinateur hôte. VMware propose

divers produits, dont VMware Workstation, qui permet aux utilisateurs de créer et d'exécuter plusieurs systèmes d'exploitation simultanément sur une seule machine physique. Cela offre un environnement isolé et sécurisé pour tester des logiciels, des configurations réseau et d'autres applications sans avoir besoin de matériel dédié.

Maintenant, une fois le VMware est installé sur l'ordinateur, nous allons procéder à l'installation de la machine virtuelle qui servira de serveur RADIUS. Cette machine virtuelle sera utilisée pour gérer l'authentification et l'autorisation des utilisateurs se connectant au réseau. Pour commencer, allumez la machine virtuelle dans VMware. Une fois la machine virtuelle allumée, on pourra procéder à l'installation du système d'exploitation nécessaire pour le serveur RADIUS.

Après avoir installé le système d'exploitation, nous allons définir un mot de passe pour le serveur afin d'assurer sa sécurité. Il faut assurer d'utiliser un mot de passe fort et de le conserver en lieu sûr .Ensuite, pour améliorer l'expérience utilisateur, nous procéderons à l'installation des pilotes VMware Tools sur la machine virtuelle. Les VMware Tools sont un ensemble de pilotes et de services qui améliorent la performance et la fonctionnalité des machines virtuelles. Ils permettent notamment l'affichage en plein écran, le partage de fichiers et la gestion des périphériques virtuels.

4.2.1 Les équipement réseaux

Equipments	Marque	Système
Serveur	Asus 5 émé géreration	windows serveur 2022
point d'accès	Tenda	
Switch	CISCO	System IOS Cisco
PC1(client)	HP	windows 10

TABLE 4.1 – Les équipments utilisés

Partie1 : Simulation du réseau sur le simulateur Pa-quet Tracer

Architecture

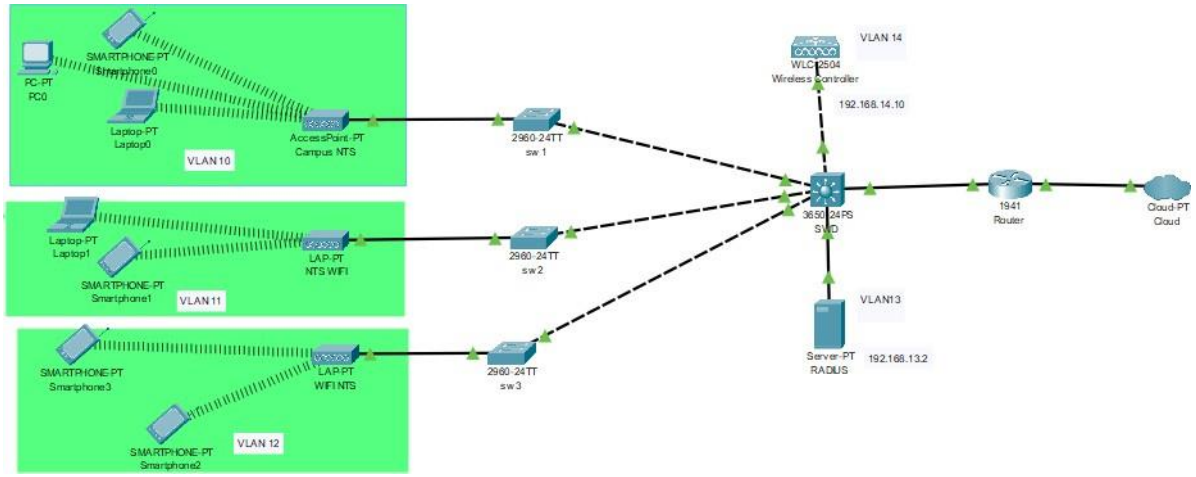


FIGURE 4.1 – Topologie proposée

Configuration des VLANs

— Tableau d'adressage des VLANs

Equipment	Interfaces	L'adresse IP
Serveur	Fa 0	192.168.13.2/24
Contrôleur	Gig 1	192.168.14.10/24
Point d'accès 1	Gig 0	192.168.11.104/24
Point d'accès 2	Gig 0	192.168.12.100/24
Routeur	Gig 0/0.10	192.168.10.1/24
	Gig 0/0.11	192.168.11.1/24
	Gig 0/0.12	192.168.12.1/24
	Gig 0/0.13	192.168.13.1/24
	Gig 0/0.14	192.168.14/24

TABLE 4.2 – Tableau d'adressage

— Configurations des VLANS

Nous devons accéder au commutateur central (switch core) et exécuter les commandes suivantes :

Tout d'abord, nous allons configurer le mode trunk pour les interfaces Gigabit 1/0/1-3. Pour chaque interface, nous allons attribuer les VLANs correspondant à l'aide de la commande "switchport trunk allowed vlan10-14,99".Lorsque cette commande est exécutée, elle spécifie les VLAN qui sont autorisés à passer à travers le lien trunk. Dans cet exemple, les VLAN 10, 11, 12, 13, 14 et 99 sont autorisés.

Cela signifie que le switch core permettra le trafic des périphériques et des utilisateurs situés dans ces VLAN à travers le lien trunk .Pour faire cela il faudrait suivre les commandes du tableau 4.3.

```
SWD # configure terminal
SWD (config)# interface range gigabitEthernet 1/0/1-3
SWD (config-if-range)#switchport mode trunk
SWD (config-if-range)#switchport trunk allowed vlan 10-14,99
SWD (config-if-range)#switchport trunk native vlan 99
SWD (config-if-range)#end
```

TABLE 4.3 – Commandes de configuration du Switch Core

Pour attribuer les VLANS correspondant pour chaque switch il fallait exécuter ces commandes du tableau 4.4.

```
SWD # configure terminal
SWD (config)# interface fastEhernet 0/2
SWD (config-if-range)#switchport trunk allowed vlan 10-14,99
SWD (config-if-range)#end
```

TABLE 4.4 – Commandes de configuration du Switch Core

— Configuration VTP

Ensuite, nous allons configurer le mode VTP (VLAN Trunking Protocol) en tant que serveur sur le commutateur central (switch core). Cela permettra la création des VLAN sur l'ensemble des commutateurs.en utilisant les commandes du tableau 4.5

```
SWD(config)#vtp mode server
SWD(config)#vtp dommain campusnts.vtp
SWD(config)#vtp password campus nts123
SWD(config)#vtp version 2
SWD(config)#end
```

TABLE 4.5 – Commandes de configuration du mode VTP serveur

Ensuite,sur les commutateurs, nous allons configurer le mode VTP (VLAN Trunking Protocol)en tant que client . On suivant les commandes du tableau 4.6 .

```
SW1 (config)#vtp mode client
SW1 (config)#vtp dommain campusnts.vtp
SW1 (config)#vtp password campusnts123
SW1 (config)#vtp version 2
SW1 (config)#end
```

TABLE 4.6 – Commandes de configuration du mode VTP client

Et nous répéterons la même procédure pour le switch 2 et 3.

Une fois que le mode VTP est configuré sur tous les commutateurs, nous nous

rendrons sur le commutateur central (switch core) pour attribuer des noms aux VLANS comme le montre le tableau 4.7 :

```
SWD#config t
SWD(config)#VLAN 10
SWD(config-vlan)#name telecom
SWD(config-vlan)#VLAN 11
SWD(config-vlan)#name RT
SWD(config-vlan)#VLAN 12
SWD(config-vlan)#name ST
SWD(config-vlan)#vlan 13
SWD(config-vlan)#name raduis
SWD(config-vlan)#VLAN 14
SWD(config-vlan)#name controleur
```

TABLE 4.7 – Commandes pour nommer les VLANs

Nous configurons le mode trunk pour les interfaces 1/0/5,qui est connectée au contrôleur,et l'interface 1/0/6,qui est reliée au routeur dans le switch core.

Enfin,nous configurons le mode access pour l'interface 1/0/5, qui est connectée au serveur Radius par les commandes suivante « switchport mode access», une fois cette commande est faites on exécute cette commande « switchport access vlan 13 »

Pour vérifier que tous les VLANs sont attribués et configurés correctement, nous exécutons la commande "show vlan brief ".Cela nous fournira un aperçu des VLANs avec leurs paramètres.

```
SWD>en
SWD#show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Gig1/0/7, Gig1/0/8, Gig1/0/9, Gig1/0/10
                                                Gig1/0/11, Gig1/0/12, Gig1/0/13,
Gig1/0/14
                                                Gig1/0/15, Gig1/0/16, Gig1/0/17,
Gig1/0/18
                                                Gig1/0/19, Gig1/0/20, Gig1/0/21,
Gig1/0/22
                                                Gig1/0/23, Gig1/0/24, Gig1/1/1, Gig1/1/2
                                                Gig1/1/3, Gig1/1/4
10   telecommunication                active
11   RT                               active
12   ST                               active
13   radius                           active    Gig1/0/4
14   controlleurs                     active    Gig1/0/5
99   native                           active
1002 fddi-default                     active
1003 token-ring-default               active
1004 fddinet-default                  active
1005 trnet-default                    active
SWD#
```

FIGURE 4.2 – Show Vlan brief

— Création des VLANS

Nous configurons le « mode access » pour l'interface 0/1 de chaque commutateur par son vlan correspond comme le tableau montre

Switchs	Switch 1	Switch 2	Switch 3
Vlans	Vlan 10	Vlan 11	Vlan 12

TABLE 4.8 – Les Vlans associer à chaque switch

Nous allons configurer le mode access au niveau de chaque commutateur en suivants les commandes du tableau 4.9.

```
Sw(config)#int fa0/1
Sw(config-if)#switchport mode access
Sw(config-if)#switchport access vlan x
Sw(config-if)#end
```

TABLE 4.9 – Les commandes de configuration du mode access

Chaque VLAN fonctionne comme un réseau indépendant avec ses propres adresses IP

et sous-réseaux.Par défaut,les VLANs sont isolés les uns des autres,ce qui signifie que les hôtes d'un VLAN ne peuvent pas communiquer directement avec ceux d'un autre VLAN.

C'est là qu'intervient le routage IP. En configurant le routage IP entre les VLANs, vous permettez aux hôtes des VLANs différents de communiquer entre eux.

Après avoir configuré les interfaces VLAN, nous activons le routage IP (IP routing) sur le routeur ou le commutateur multicouche. Cette fonctionnalité permet au routeur de diriger les paquets IP entre les VLANs en configurant des entrées de routage dans ses tables de routage. Cela permet au routeur de déterminer les chemins appropriés vers les sous-réseaux des autres VLANs et de savoir comment acheminer les paquets entre eux.

Une fois le routage IP mis en place,les hôtes des différents VLANs peuvent communiquer entre eux en utilisant leurs adresses IP. Lorsqu'un paquet provient d'un VLAN, il est envoyé au routeur,qui examine l'adresse IP de destination. En fonction de cette adresse,le routeur achemine le paquet vers le VLAN approprié, permettant ainsi la communication entre les hôtes des VLANs différents. Le routage IP dans les VLANs permet donc d'établir des communications inter-VLANs, ce qui est essentiel pour des environnements réseau plus complexes où la segmentation et la séparation des flux de données sont nécessaires pour des raisons de sécurité,de performances ou d'organisation.

interface gigabitethernt0/0.10	192.168.10.1/24
interface gigabitethernt0/0.11	192.168.11.1/24
interface gigabitethernt0/0.12	192.168.12.1/24
interface gigabitethernt0/0.13	192.168.13.1/24
interface gigabitethernt0/0.14	192.168.14.1/24

TABLE 4.10 – Tableau d'adressage

```
R(config)#interface gigabiethernet 0/0
R(config)#no shutdown
R(config)#interface gigabitethernt0/0.x
R(config)#encapsulation dot1q
R(config)#ip add 192.168.x.1 255.255.255.0
R(config)#exit
```

TABLE 4.11 – Commandes de configuration du routeur

La commande "ip helper-address" est utilisée sur un routeur pour permettre la transmission de messages DHCP à travers des interfaces de réseau différentes.

```
R(config)#interface gigabiethernet 0/0.x
R(config)#ip helper-address 192.168.13.2
R(config)#exit
```

TABLE 4.12 – La commande "ip helper-address"

Configuration du contrôleur

Nous allons ajuster l'adresse IP du contrôleur en fonction du VLAN au quel il est associé,plus précisément VLAN 14.

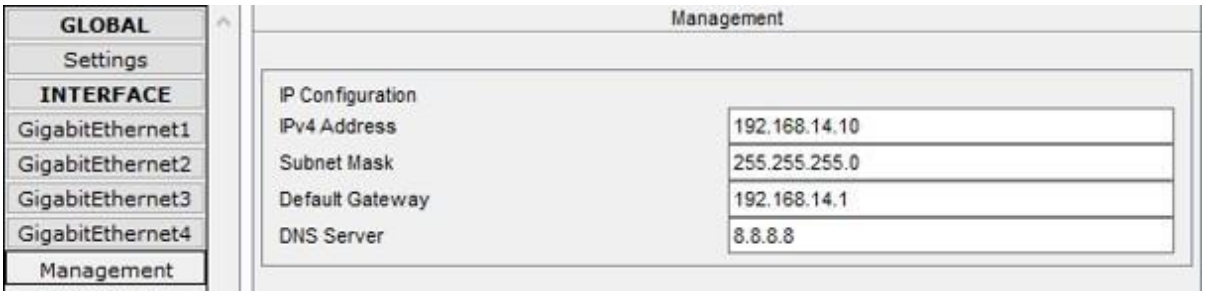


FIGURE 4.3 – Attribution des adresses IP au contrôleur

Nous allons procéder à l'attribution des adresses IP aux ordinateurs et aux téléphones. Pour cela, nous allons effectuer la configuration initiale du contrôleur à partir d'un PC. Une fois que le contrôleur est configuré, nous pourrons y accéder depuis un PC en

utilisant le nom d'utilisateur et le mot de passe appropriés. Après avoir fourni ces informations, nous pourrons ajouter les points d'accès au contrôleur.

Pour ajouter les points d'accès, il vous suffit de cliquer sur le bouton "Go" et d'entrer leurs noms et SSID dans les champs correspondants. Ensuite, cliquez sur "Apply" pour finaliser la configuration

En activant le protocole WPA2 et le chiffrement AES pour chaque point d'accès, comme représenté dans la figure suivante

FIGURE 4.4 – Partie sécurité

Ensuite, nous saisissons le mot de passe 'ilissia123' pour le point d'accès "NTS WIFI" et le mot de passe 'massilia123'pour le deuxième point d'accès "WifiNTS",comme indiqué dans la figure suivante :

FIGURE 4.5 – configuration d'un mot de passe au point d'accès depuis un contrôleur

Maintenant,nous allons former deux groupes. Un groupe sera destiné aux utilisateurs souhaitant accéder aux points d'accès NTS WIFI, tandis que l'autre groupe sera réservé aux utilisateurs désirant accéder au point d'accès WIFINTS.

Pour créer un groupe d'employés, il suffit de cliquer sur "Ajouter un nouveau groupe AP "et pour l'ajouter, il vous suffit de cliquer sur le bouton "Ajouter". La même procédure s'applique pour créer et ajouter un groupe de clients.

Afin de gérer les groupes et ajouter le nom du réseau sans fil (WLAN), il vous suffit de cliquer sur l'option WLAN, puis sélectionner 'Add New 'pour choisir le nom souhaité. De plus, pour choisir le point d'accès approprié, vous pouvez cliquer sur l'option APS

Nous suivrons également les mêmes étapes pour créer le groupe de clients

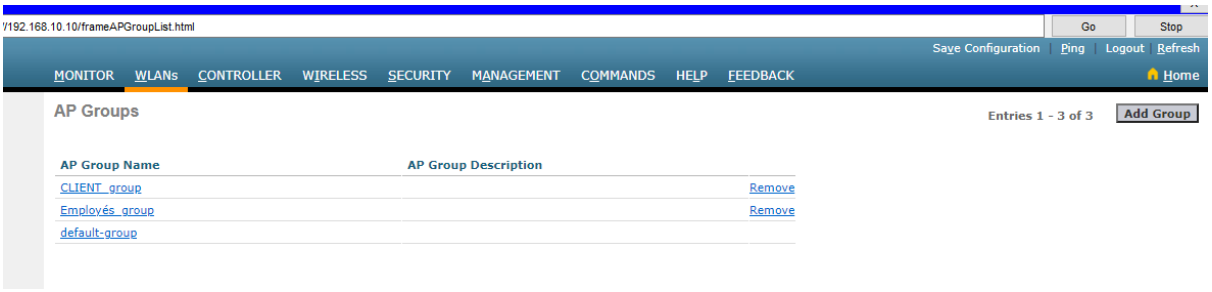


FIGURE 4.6 – Les groupes créés

Pour connecter les utilisateurs à leurs points d'accès respectifs, par exemple ceux qui souhaitent se connecter au point d'accès "WIFI NTS",ils doivent accéder aux paramètres de leur ordinateur, smartphone ou autre appareil. Ensuite, ils doivent sélectionner l'option "Sansfil"(ou"Wireless")et modifier le SSID en remplaçant par le nom de leur point d'accès.

Ensuite, ils devront ajouter leur mot de passe comme indiqué dans l'exemple ci-dessous :

FIGURE 4.7 – Insertion du mot de passe

Configuration de serveur RADUIS et DHCP :

Nous allons configurer le serveur DHCP pour chaque VLAN.

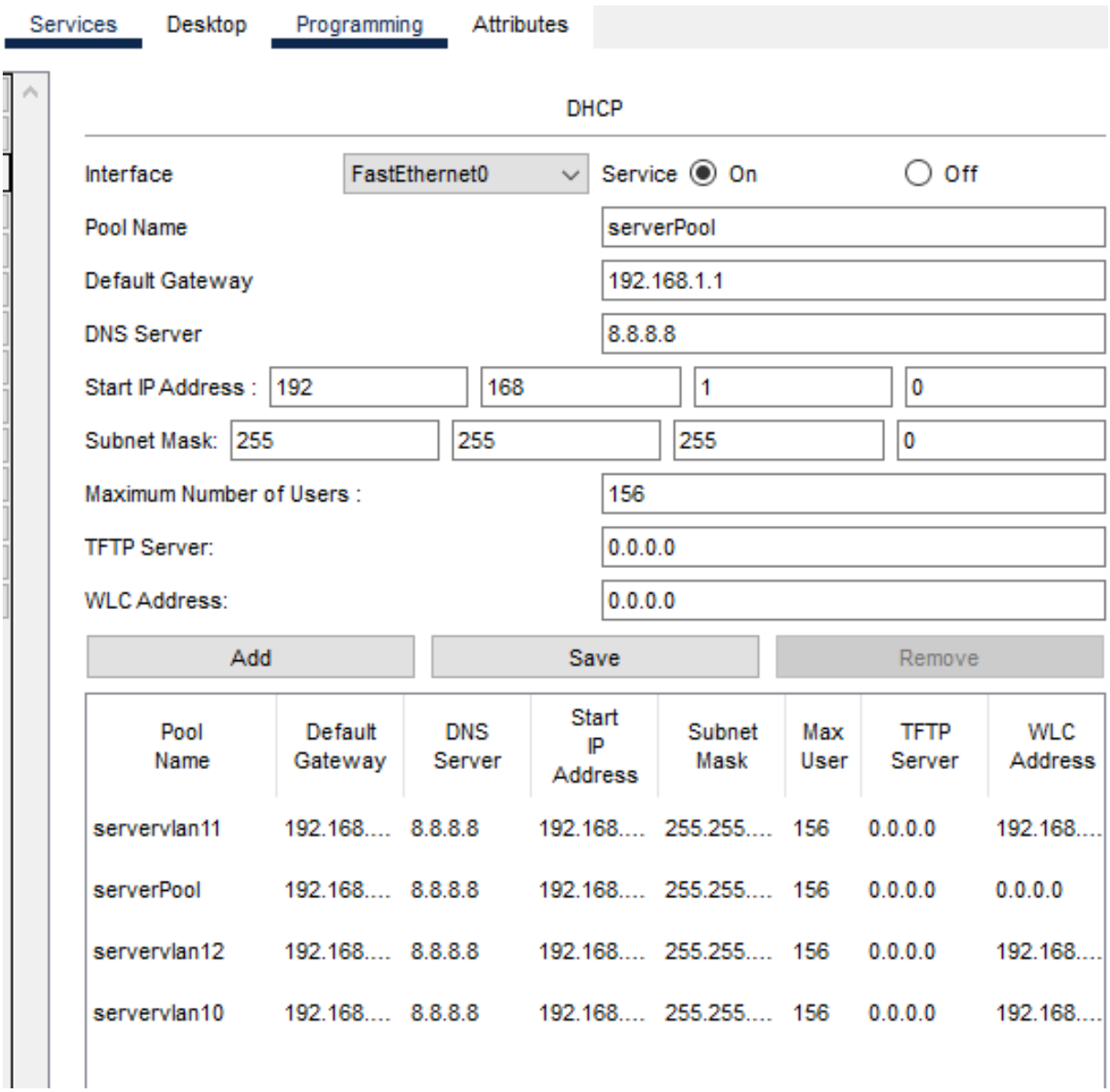


FIGURE 4.8 – Configuration du DHCP selon les vlans

Nous avons procédé à l'ajout des clients Wi-Fi au serveur Radius AAA. À chacun de ces clients, nous avons attribué des adresses IP pour permettre leur identification et leur communication au sein du réseau. Ensuite, afin de renforcer la sécurité du réseau, nous avons configuré des mots de passes pour limiter l'accès aux utilisateurs autorisés. De plus, nous avons créé des utilisateurs avec des identifiants uniques, permettant ainsi une authentification sécurisée lors de leur connexion au réseau.

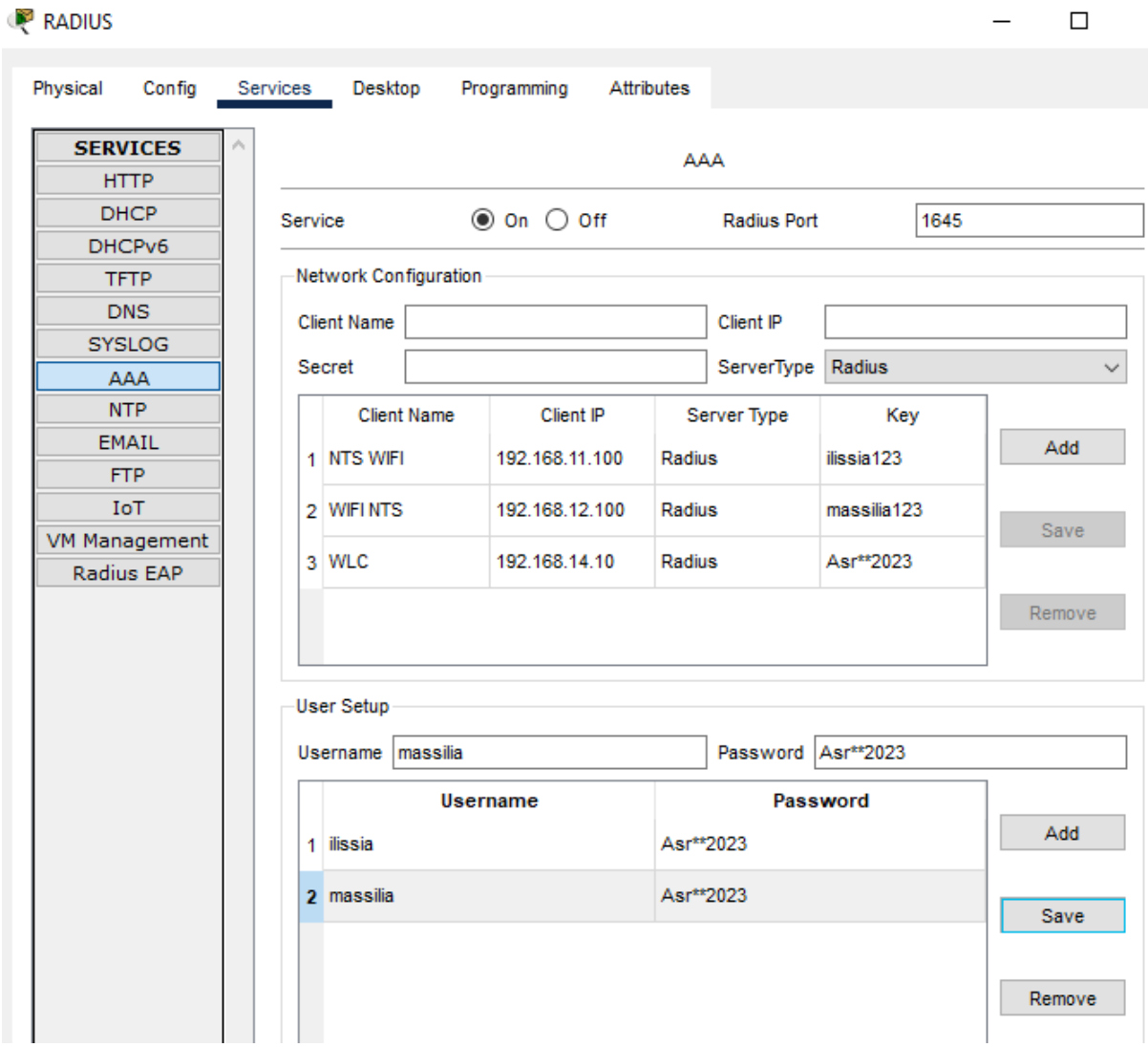


FIGURE 4.9 – Configuration du serveur radius

Finalement, notre serveur DHCP a été configuré pour attribuer des adresses IP aux points d'accès.

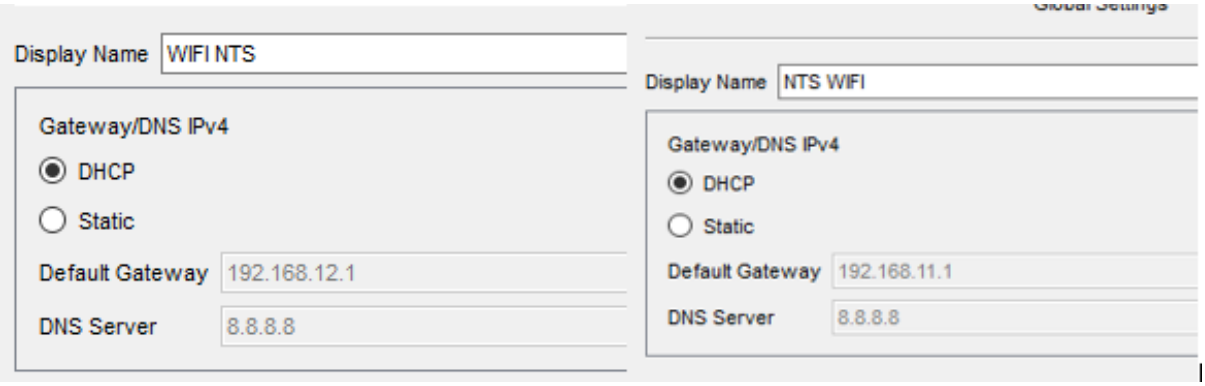


FIGURE 4.10 – Les adresses attribuer aux points d'accées par DHCP

Partie2 : Implémentation sur un réseau réel

Présentation d'architecture réseaux

Méthodologie :

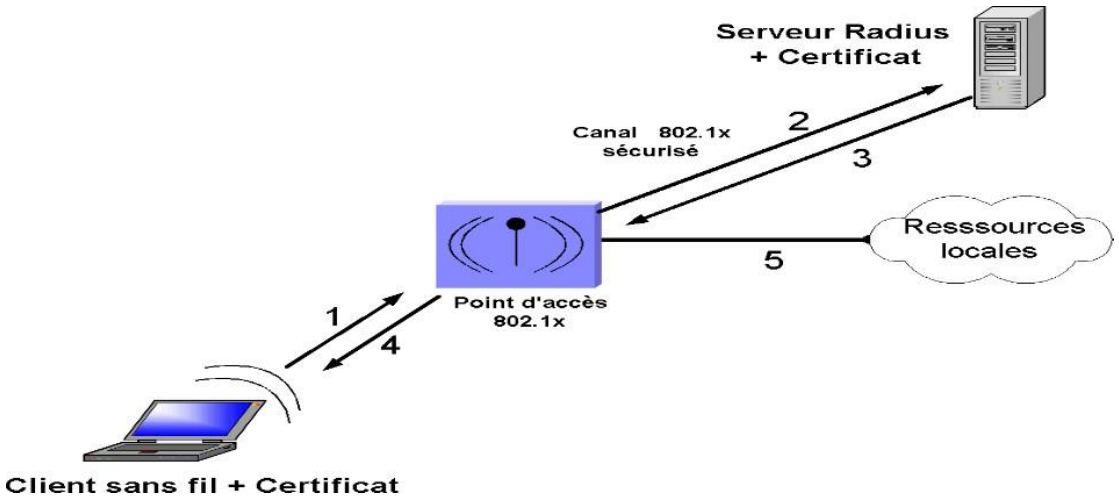


FIGURE 4.11 – Une vue générale de la solution

Description des étapes du processus

1. Lorsque le client demande à accéder au réseau après avoir obtenu du serveur

DHCP une adresse IP, il transmet ses informations d'identité au point d'accès sans fil. Pendant cette phase, le client ne peut avoir accès aux ressources locales.

2. Le point d'accès sans fil renvoie ces informations au serveur Radius. Le serveur Radius vérifie les informations d'identité, consulte sa stratégie d'accès et autorise ou refuse l'accès au client.
3. S'il est reconnu, le client est autorisé à accéder au réseau et échange les clés de cryptage avec le point d'accès sans fil. En fait, les clés sont générées par le serveur Radius et transmises au point d'accès sans fil via le canal sécurisé (802.1x). Si le client n'est pas reconnu par le serveur Radius, il n'est pas autorisé à accéder au réseau et la communication s'interrompt .
4. Grâce aux clés de cryptage, le client et le point d'accès sans fil établissent une connexion sans fil sécurisée, ce qui permet au client et au réseau interne de communiquer.
5. Le client commence à communiquer avec des périphériques du réseau interne. Cette architecture implique une authentification du point d'accès au niveau du serveur,l'utilisation de certificat aussi bien par le client sans fil que par le serveur Radius. Ces certificats peuvent être générés par une Autorité de certification ou par un équipement du réseau configuré pour ce fait. Nous avons préféré que ce soit le serveur Radius qui se charge de cette tâche.

Installation et configuration Active directory et DNS

Active Directory permet de facilite l'authentification et l'autorisation des utilisateurs dans les réseaux sans fil. Il permet de vérifier les informations d'identification des utilisateurs dans la base de données d'Active Directory, de déterminer leurs autorisations et de fournir les paramètres appropriés pour l'accès au réseau sans fil. Cela garantit une gestion centralisée des utilisateurs et des politiques de sécurité, renforçant ainsi la sécurité et la gestion des réseaux sans fil.

Voici les étapes générales pour installer Active Directory et DNS dans VMware :

1. Nous accédons au "Gestionnaire de serveur" dans WindowsServer.
2. Nous allons sélectionné "Ajouter des rôles et fonctionnalités "dans le Gestionnaire de serveur.
3. Nous suivons les instructions pour installer le rôle "Services de domaine Active Directory" et le rôle" Serveur DNS".

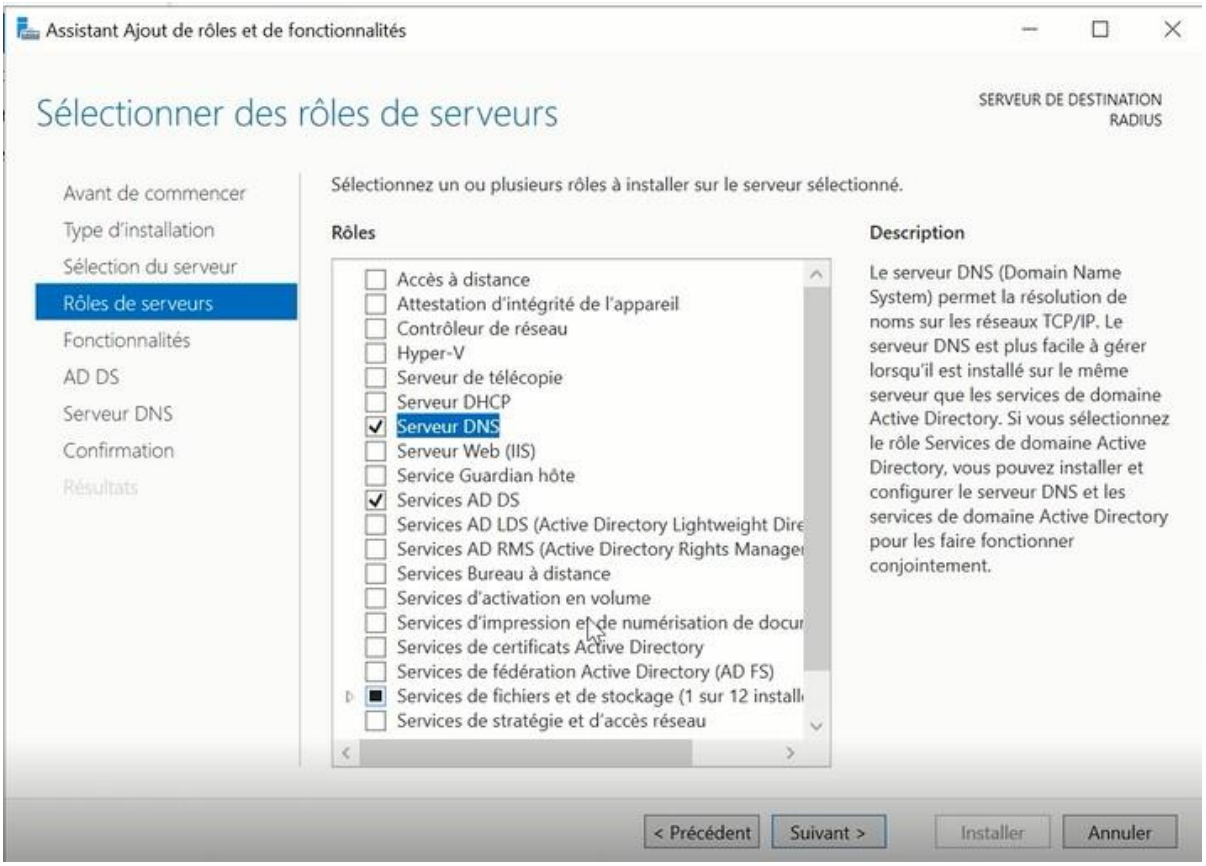


FIGURE 4.12 – Installation de AD et DNS.

4. Une fois les rôles installés, nous lancons l'Assistant Configuration des services de domaine Active Directory.
5. Nous suivons les étapes de l'assistant pour configurer un nouvel environnement de domaine 'une nouvelle forêt'.
6. Pour notre installation spécifique, nous avons nommé la forêt "campusnts.local".

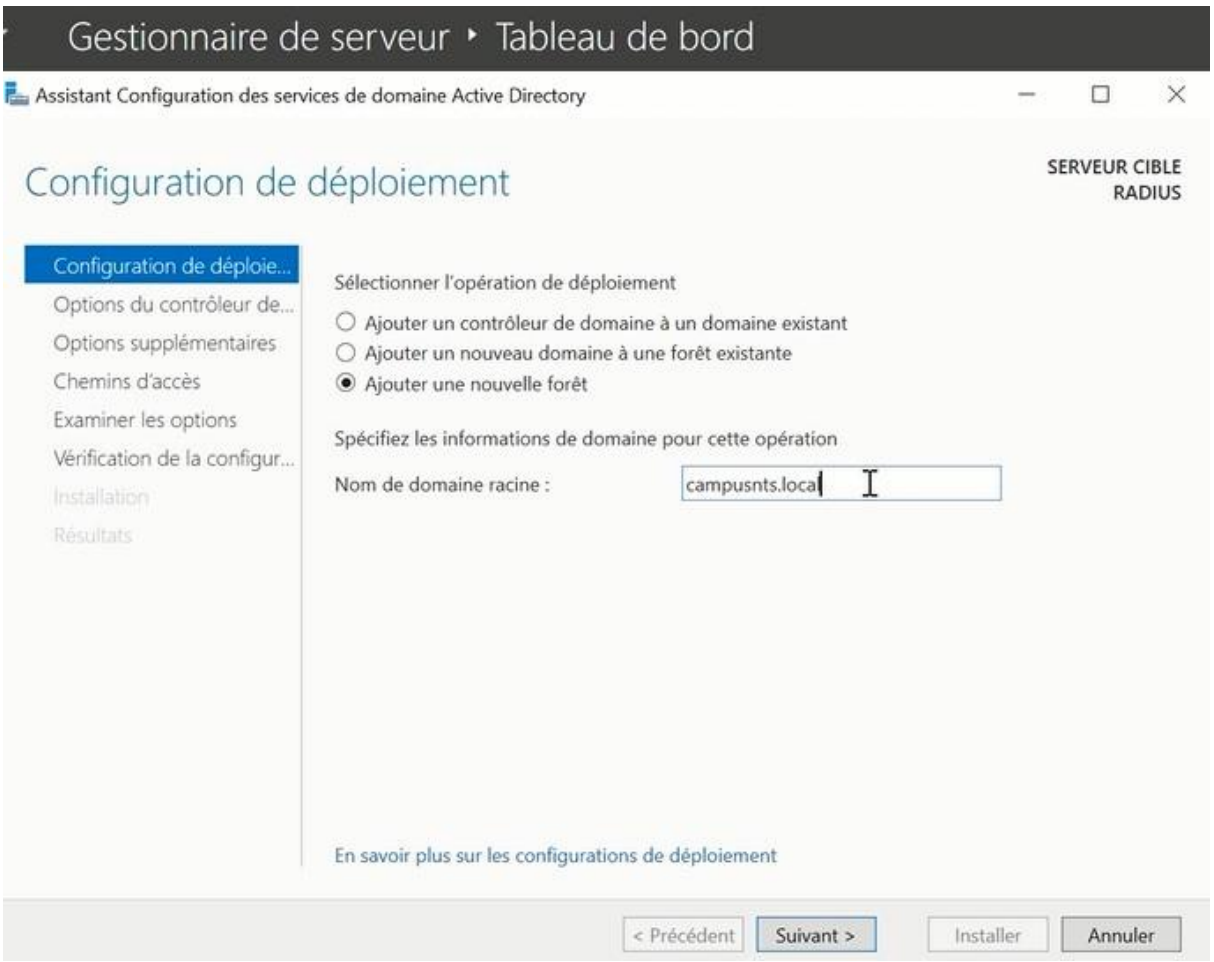


FIGURE 4.13 – Création d'une Forêt

La création de la forêt dans Active Directory a été réalisée dans le but de fournir une structure d'organisation et de gestion des ressources informatiques au sein d'un réseau d'entreprise

Une fois qu'Active Directory est installé, nous pouvons suivre les étapes suivantes :

1. Nous accédons à "Ordinateurs et Utilisateurs Active Directory" pour gérer la structure de notre domaine.
2. Nous créons une nouvelle unité d'organisation (OU) que nous nommons "ordinateurs-wifi-campusnts". Cela nous permettra d'organiser les ordinateurs et les utilisateurs liés au WiFi.

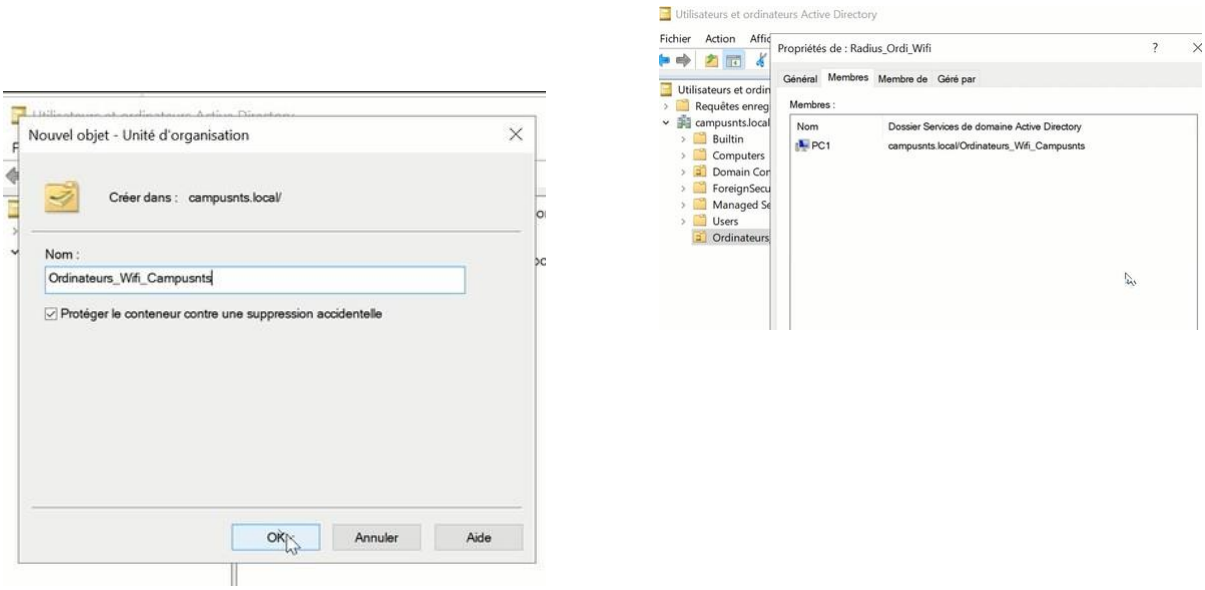


FIGURE 4.14 – Création d'un groupe et ordinateur

3. À l'intérieur de l'OU "ordinateurs-wifi-campusnts", créons de nouveaux objets d'ordinateur pour chaque nouvel ordinateur que nous souhaitons ajouter. Nous pouvons spécifier des noms uniques pour chaque ordinateur.
4. Créons également de nouveaux objets d'utilisateurs pour les utilisateurs qui auront accès au WiFi. Nous pouvons spécifier leurs noms, attribuer des mots de passe et configurer d'autres paramètres nécessaires.
5. Pour gérer les autorisations pour les utilisateurs et les ordinateurs WiFi, créons un groupe nommé "Radius-ordi-wifi". Nous pouvons ensuite ajouter les utilisateurs et les ordinateurs appropriés à ce groupe pour leur permettre de se connecter au domaine via le WiFi.

Nous avons créé deux utilisateurs « ilyssia.belkhichane» et « massilia.menzou »munis d'un mot de passe « Asr**2023 »pour permettre l'accès à partir d'un ordinateur certifié sur le domaine campusnts.local.

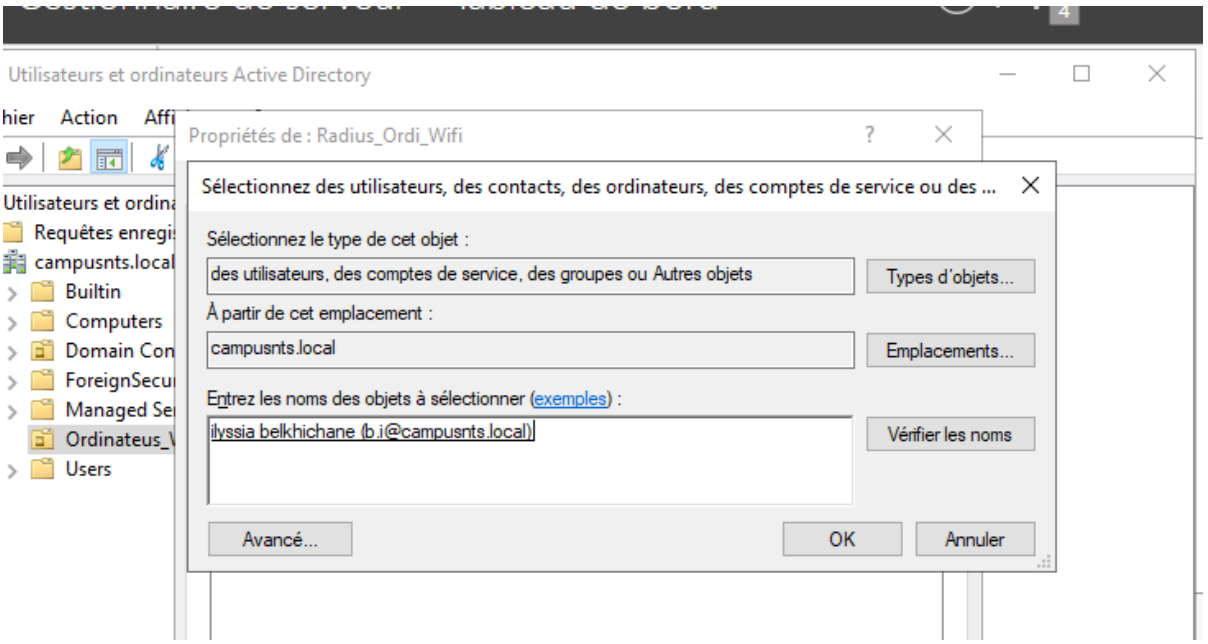


FIGURE 4.15 – Ajouter des utilisateurs au groupe

Installation du DHCP

L'installation du service DHCP dans un environnement VMware simplifie la gestion des adresses IP en automatisant leur attribution et en centralisant leur configuration. Cela réduit les erreurs de configuration, améliore l'efficacité de gestion du réseau, offre une flexibilité.

Pour installer le service DHCP (Dynamic Host Configuration Protocol) dans un environnement VMware, nous pouvons suivre les étapes suivantes :

1. Dans le gestionnaire de serveur, sélectionnons "Ajouter des rôles et fonctionnalités" pour lancer l'assistant d'installation.
2. Suivons les étapes de l'assistant d'installation en sélectionnant "Serveur DHCP" comme rôle à ajouter. Acceptons les options par défaut ou les configurons selon nos besoins. Pour créer une nouvelle étendue sur DHCP nommée "Lan wifi" et définir la plage d'adresses qu'elle peut distribuer, ainsi qu'une plage exclue, suivez les étapes suivantes :
3. Nous accédons à la console de gestion DHCP.

4. Nous faisons un clic droit sur "Étendues" et choisissez "Nouvelle étendue" pour créer une nouvelle étendue.
5. Suivons les instructions pour configurer l'étendue en spécifiant un nom, une plage d'adresses IP et d'autres paramètres requis.
6. Définissons la plage d'adresses que l'étendue "Lan wifi" peut distribuer en spécifiant l'adresse de début et l'adresse de fin.
7. Déterminons la plage d'adresses à exclure en spécifiant les adresses spécifiques qui ne doivent pas être attribuées par l'étendue DHCP. [192.168.10.1 – 192.168.10.50]
8. Nous ajoutons une passerelle par défaut d'un router192.168.10.254
9. Nous Ajoutons le nom d'un domaine « campusnts.local » pour les ordinateurs clients.
10. Pour configurer les clients d'étendue pour qu'ils utilisent le serveur DNS sur le réseau on ajoute une adresse IP de serveur 192.168.10.10.
11. Ajoutons l'adresse IP 192.168.10.10 aux serveurs WINS pour convertir les noms NetBIOS d'ordinateur en adresse IP
12. Une fois l'adress est ajouter on active d'étudue.

Installation de service de certificats Active Directory

Pour installer le rôle de service de certificats Active Directory (AD DS) dans une machine nous avons suivi les étapes suivantes:

1. Dans le gestionnaire de serveur,nous cliquons sur "Ajouter des rôles et des fonctionnalités".
2. Nous suivons l'assistant d'installation en sélectionnant les options par défaut jusqu'à atteindre la page"Sélectionner les rôles du serveur".
3. Nous cochons la case "Services de certificats Active Directory".

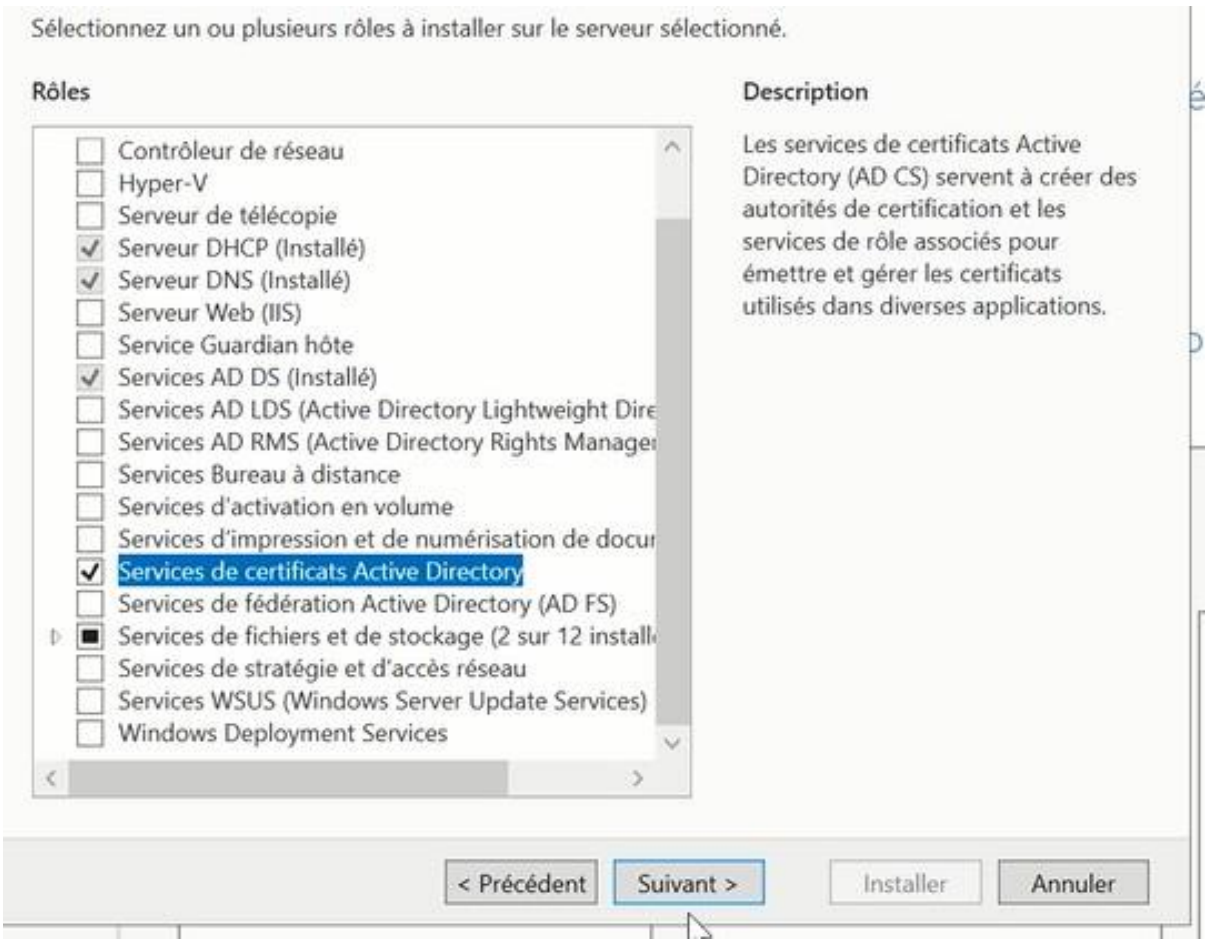


FIGURE 4.16 – Instalation de certificats AD

4. Nous continuons à suivre l'assistant en sélectionnant les options appropriées jusqu'à ce que l'installation soit terminée.

Configuration du Serveur Radius

La première chose que on doit faire c'est de relier le serveur Radius a active directory . Premièrement pour connecter à notre Switch nous allons effectuer l'étape suivante

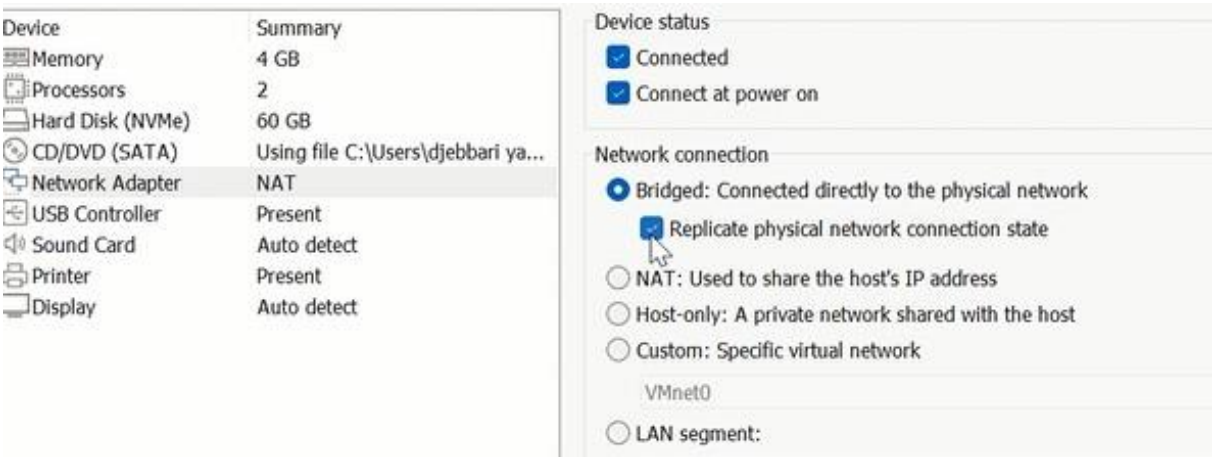


FIGURE 4.17 – Configuration du Bridged physique

Nous débutons en attribuant un nom au serveur, puis en nommant la carte réseau après on ajoute une adresse IP 192.168.10.99 et sa passerelle par défaut 192.168.10.254 .

Nous accédons à l'interface de configuration du point d'accès en utilisant un navigateur Web et l'adresse IP du point d'accès et à l'interface de configuration en saison le nom d'utilisateur et le mot de passe approprie.

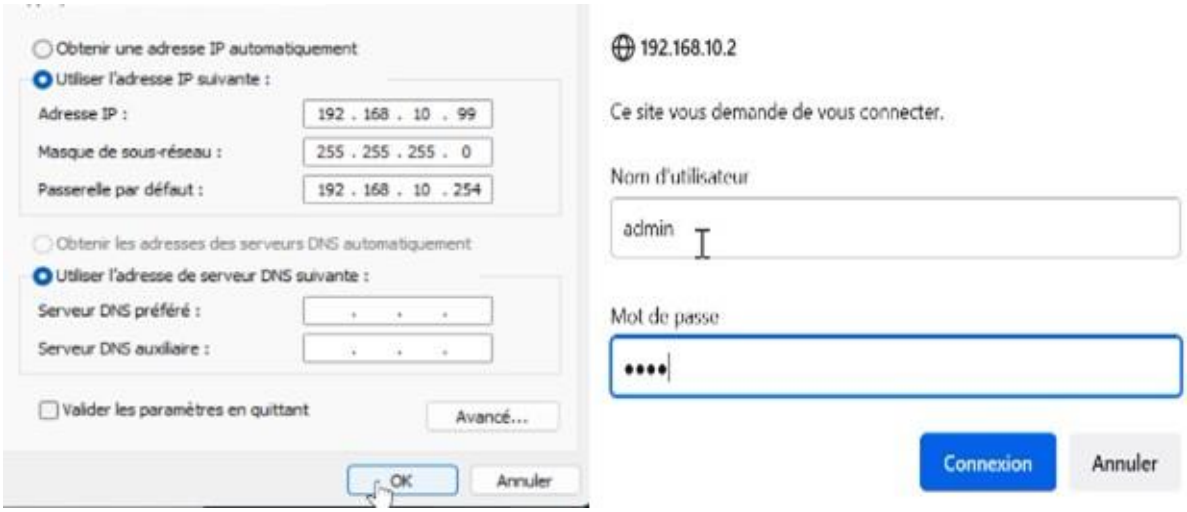


FIGURE 4.18 – Les étapes pour accéder au point d'accès

1. Une fois le mot de passe est saisi,nous procédons à la désactivation du DHCP et

SSID à la sécurisation du réseau en définissant un mot de passe,puis nous enregistrons les modifications en effectuant une sauvegarde.

2. Lorsqu'un utilisateur souhaites connecter au point d'accès ,il sera invité à saisir un mot de passe pour accéder au réseau.

   Créer un nouveau client RADIUS et une nouvelle stratégie :

3. Nous accédons à l'interface de gestion du client RADIUS.
4. Nous sélectionnons l'option pour créer un nouveau client RADIUS.
5. Nous fournissonsles informations requises, telles que le nom du client 'tenda' l'adresse IP 192.168.10.2 et le mot de passe '123456'
6. Nous définissons les conditions de la stratégie, telles que le type d'authentification,l'adresse IP source,les groupes d'utilisateurs.
7. En assurant de désactiver les autres stratégies existantes si on souhaite qu'elles ne soient,plus utilisées.

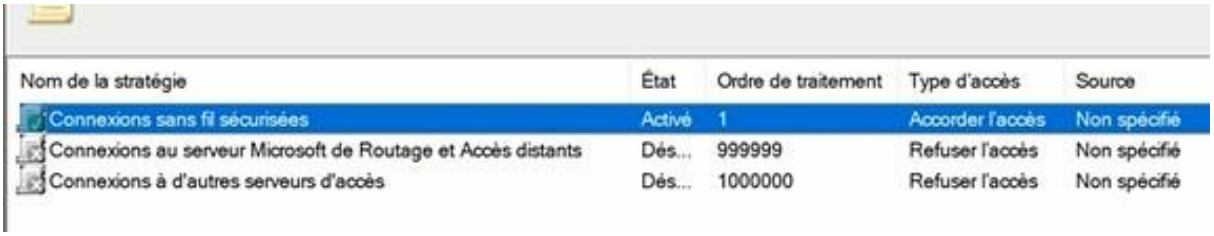


FIGURE 4.19 – La stratégie sans fil créer

Création du GPO

Nous allons procéder comme suite pour créer un nouvel objet GPO et ajouter le groupe" Radius-ordi-wifi"en supprimant le groupe "Utilisateurs authentifiés "existant :

1. Nous accédons à la console de gestion des stratégies de groupe.
2. Nous créons un nouvel objet de stratégie de groupe (GPO).
3. Nous sélectionnons le nouvel objet GPO.
4. Nous ajoutons le groupe "Radius-ordi-wifi" à cet objet GPO.

5. Nous supprimons le groupe existant "Utilisateurs authentifiés"de l'objet GPO.

Créer une GPO pour distribuée les certificats automatiquement Pour activer la fonctionnalité d'inscription automatique dans les Règles Radius,veuillez suivre ces étapes :

1. Nous accédons à la "Gestion des stratégies de groupe".
2. Nous sélectionnons "Règles Radius".
3. Nous faisons un clic droit et choisissez "Modifier"pour ouvrir la fenêtre de modification des règles.
4. Nous cliquons sur "Stratégie",puis "Paramètre Windows".
5. Sélectionnons "Paramètre de sécurité"et ensuite "Stratégies de clé publique".
6. Nous trouvons l'option "Inscription automatique"et activez-la.

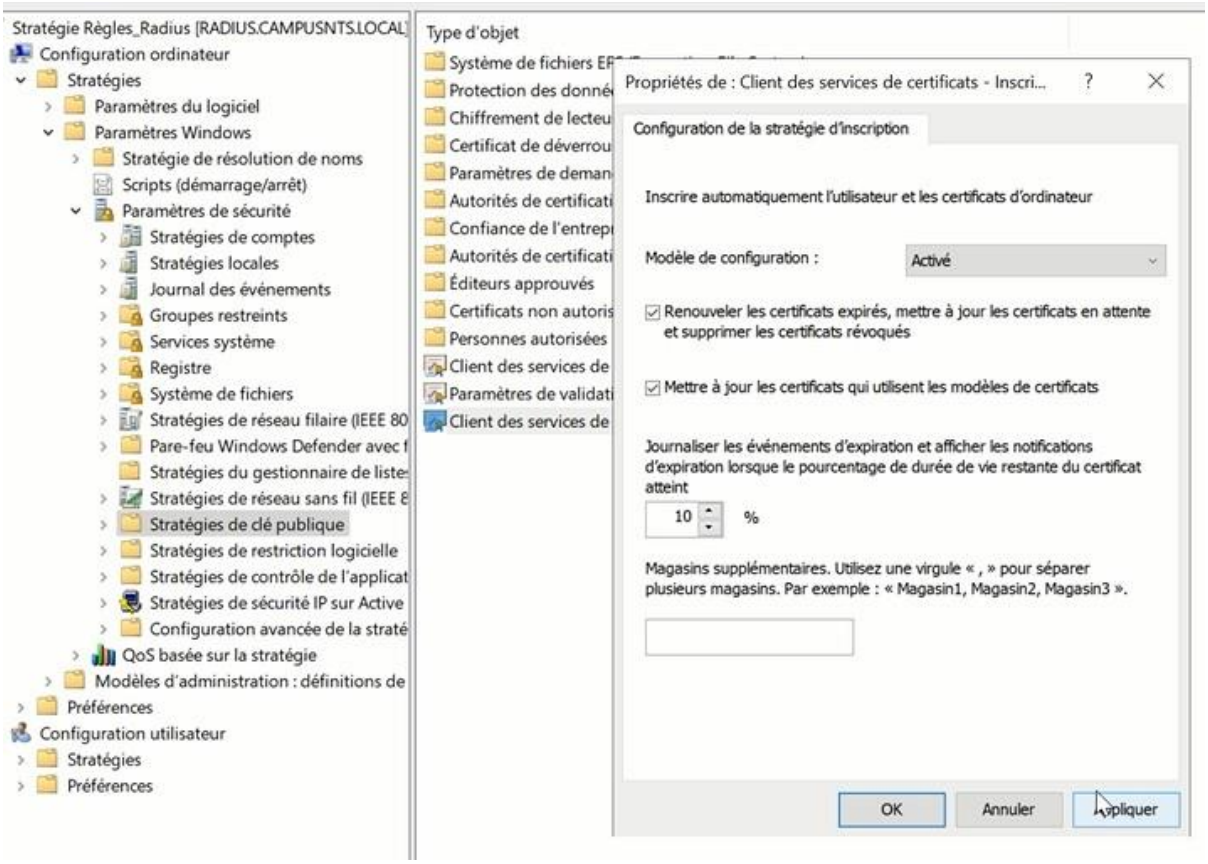


FIGURE 4.20 – Activation de l'inscription automatique

Une fois cette opération effectuée, les clients concernés qui se connectent à Active Directory recevront automatiquement le certificat.

Pour préciser que vous souhaitez certifier les ordinateurs, vous pouvez suivre les étapes suivantes:

1. Nous accédons aux "Paramètres de demande automatique de certificat".
2. Nous effectuons un clic droit et sélectionnez "Nouveau"puis"Demande automatique de certificat".
3. Nous choisissons"Les ordinateurs"comme agent d'inscription.

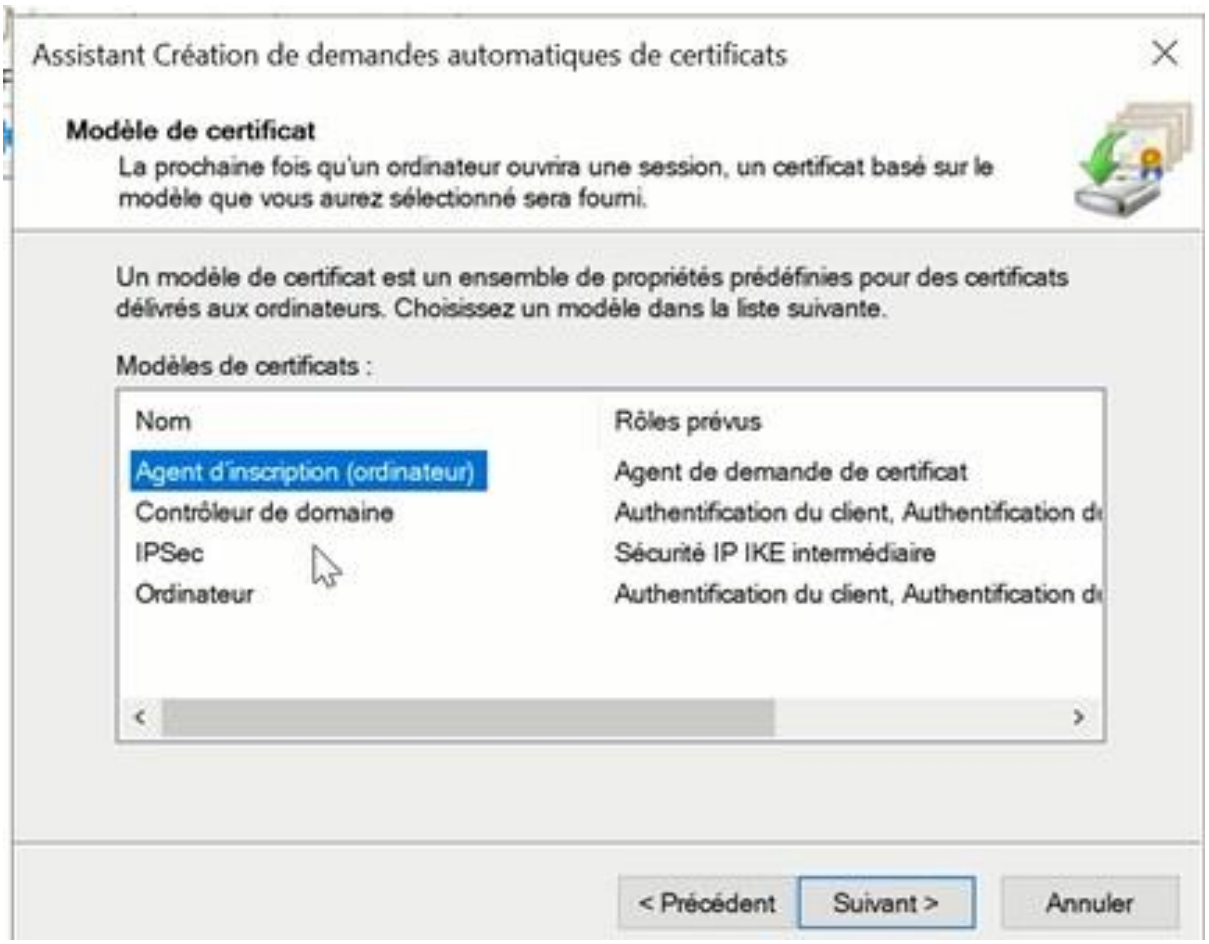


FIGURE 4.21 – Les étapes pour certifier un ordinateur

Nous créons une nouvelle stratégie dans les "Stratégies de réseau sans fil IEEE 802.11"et nous la nommons"Règles sans fil".

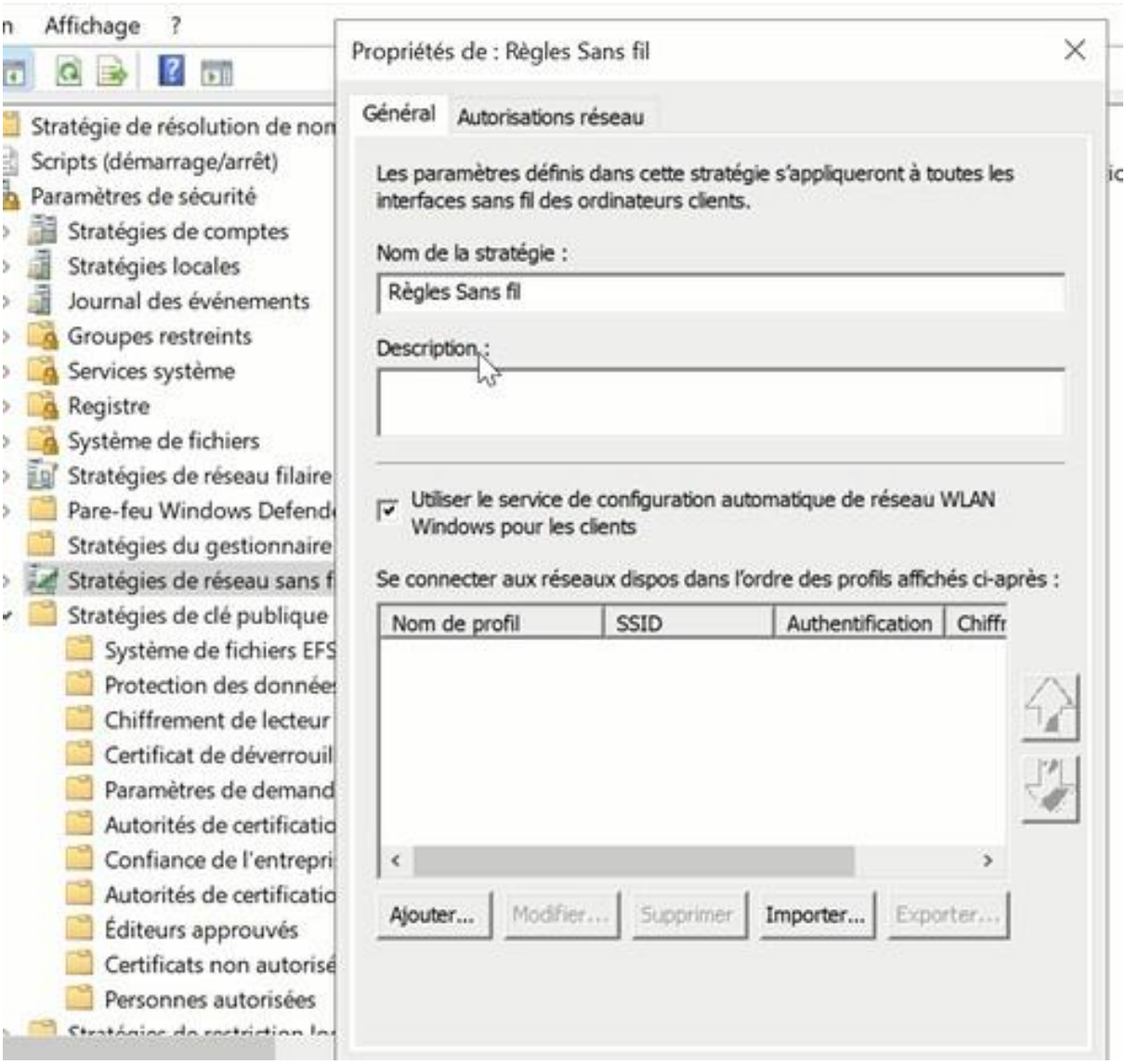


FIGURE 4.22 – Création d'une stratégie

Pour nommer le profil Wifi,nous effectuons un double-clique sur la stratégie" Règles sans fil". Ensuite,nous mentionnons le nom du réseau Tenda. Après cela, nous cliquons sur l'ongle "Sécurité"et sélectionnons la méthode d'authentification WPA2-Entreprise et le chiffrement AES. Nous choisissons le mode d'authentification de l'ordinateur et une méthode d'authentification réseau PEAP. Enfin, nous suivons les étapes suivantes pour entrer le nomdu Serveur Raduis.

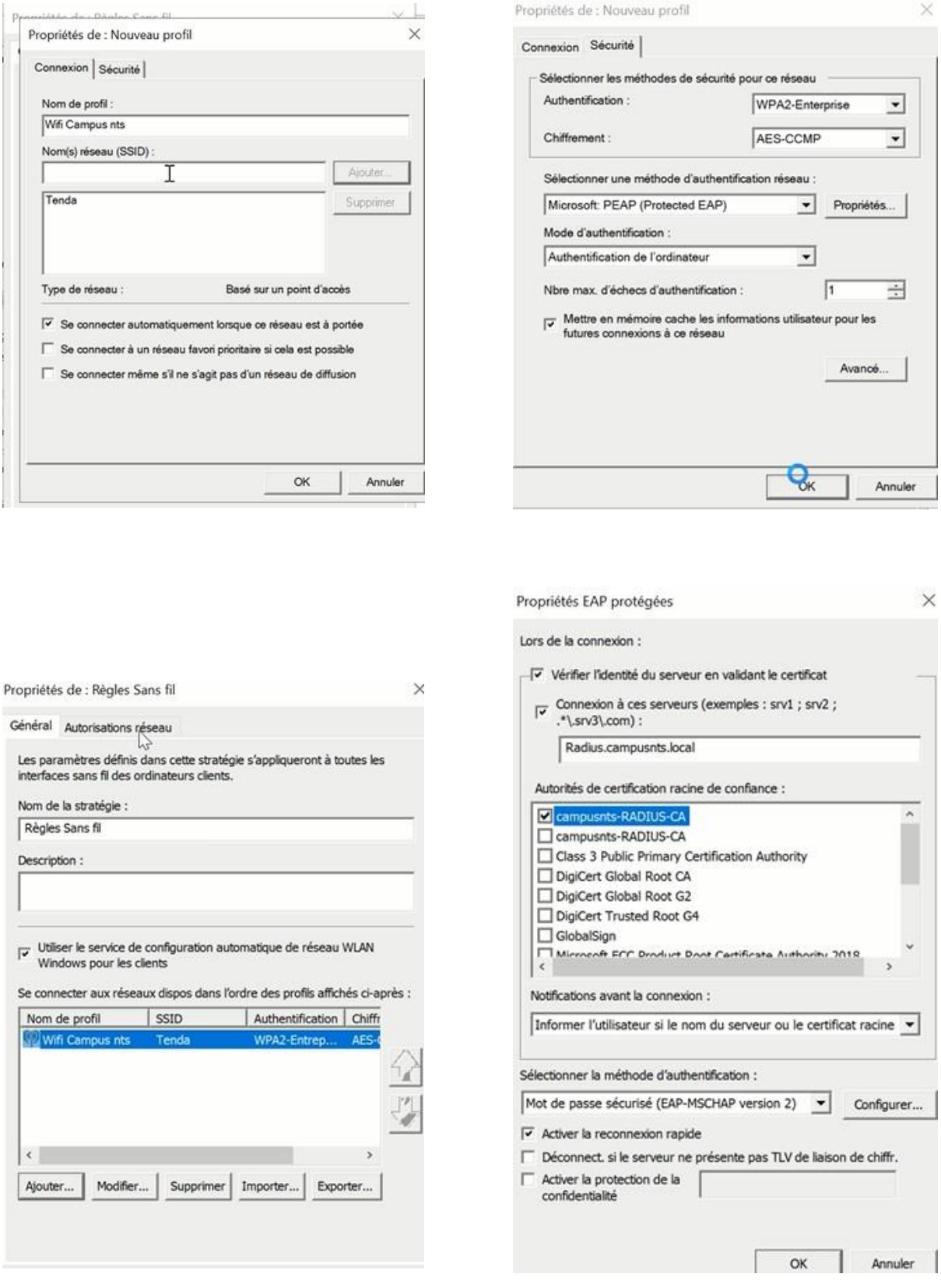


FIGURE 4.24 – Les étapes de la configuration de la règle sans fil

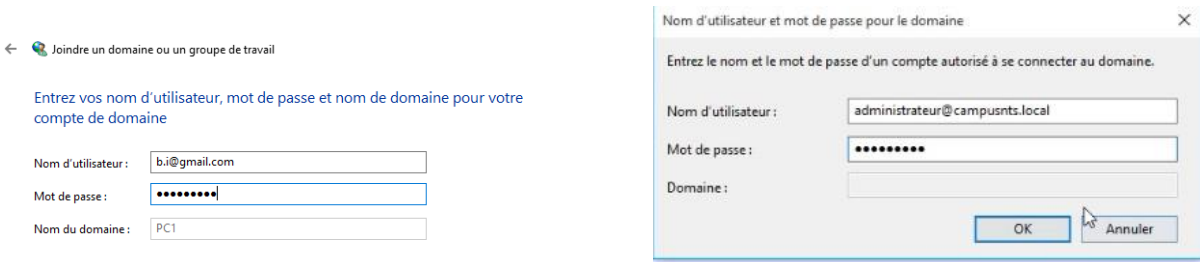


FIGURE 4.25 – Insertion du nom d'utilisateur et mot de passe

Partie Test

Nous allons maintenant nous rendre sur un autre ordinateur, qui sera le client nommé "PC1". Ce PC est déjà configuré dans Active Directory,et nous allons modifier ses paramètres afin qu'il puisse accéder au domaine "campusnts.local".Suivez les étapes illustrées dans la figure suivante :

1. commencons par ouvrir les paramètres de PC1 après on clique sur le boutton droit et en sélectionnant l'option "propriétés".
2. Dans les propriétés système, nous accédons aux paramètres système avancés. Et choisit l'option « modifier des paramètres »
3. Nous Cliquons sur "Identité du réseau"pour accéder au domaine.Pour modifies la description de ordinateur
4. Pour entrer ces informations,nous avons besoin du nom d'utilisateur et du mot de passe du compte du domaine, ainsi que du nom d'utilisateur et du mot de passe du domaine.
5. Nous avons également choisir le type de compte dans le domaine administrateur.
6. Enfin,il sera demandéder de redémarrer l'ordinateur pour finaliser le proces-sus.

Après le redémarrage, l'ordinateur sera intégré au domaine et certifié.

Test Radius

Nous avons examiné les journaux et l'observateur d'événements du serveur pour évaluer les autorisations d'accès accordées à un PC spécifique.

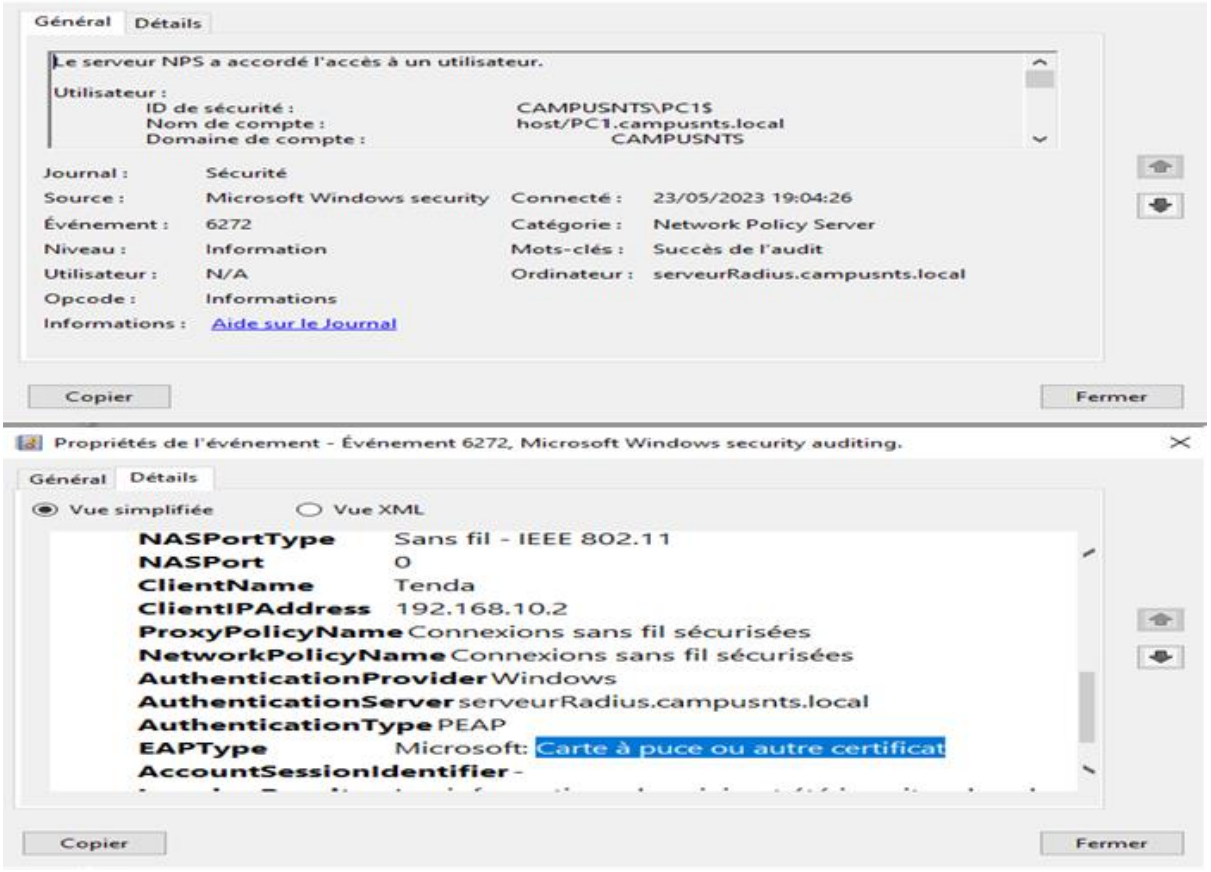


FIGURE 4.26 – Test Radius

SI on retire le PC 1 du groupe on ne pourra pas accéder au domaine

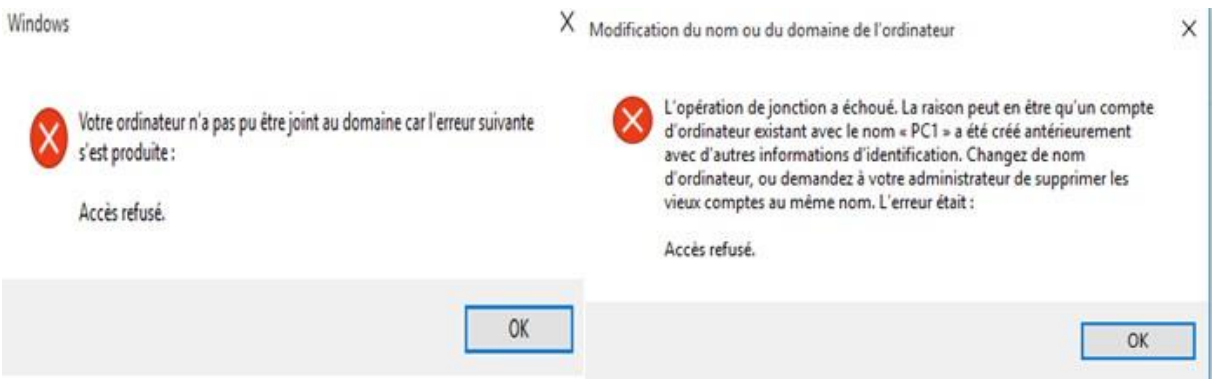


FIGURE 4.27 – Le message affiché dans le pc client

Et dans le serveur radius on remarque que le serveur NPS a refusé l'accès

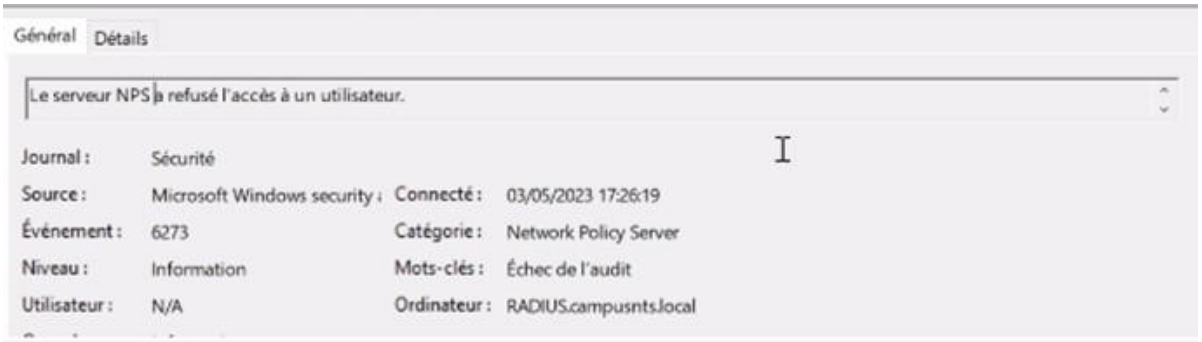


FIGURE 4.28 – le serveur Radius a refusé l'accès pour un ordinateur

Test AD DS

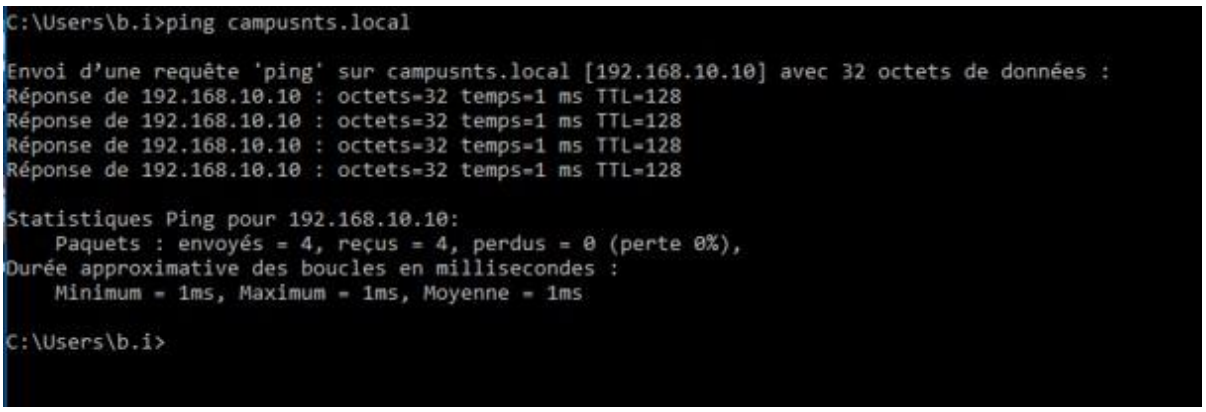
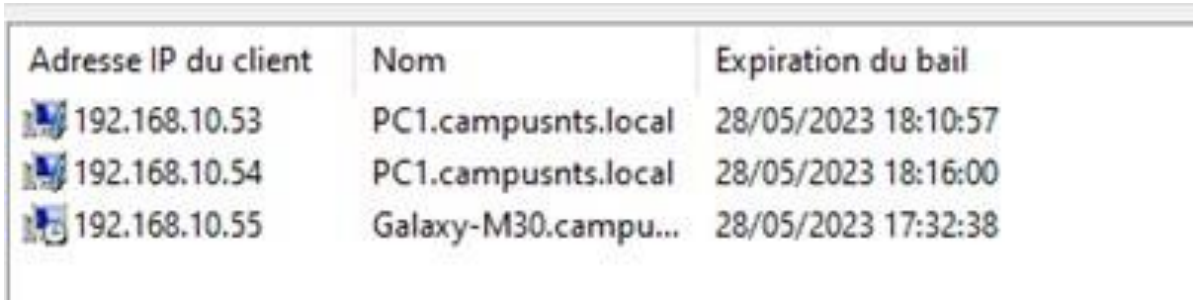


FIGURE 4.29 – Tester la connectivité

Test DHCP



Adresse IP du client	Nom	Expiration du bail
192.168.10.53	PC1.campusnts.local	28/05/2023 18:10:57
192.168.10.54	PC1.campusnts.local	28/05/2023 18:16:00
192.168.10.55	Galaxy-M30.campu...	28/05/2023 17:32:38

FIGURE 4.30 – Test DHCP

Test certificat

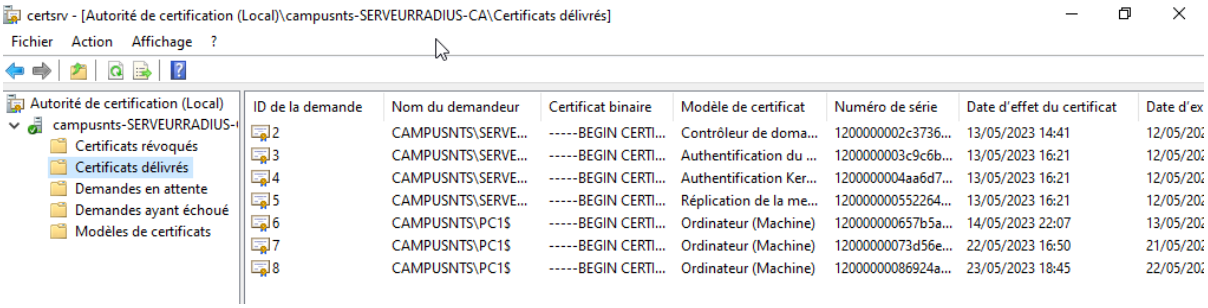


FIGURE 4.31 – Les Certificats délivrées

Pour mettre en œuvre notre solution, nous avons d'abord effectué une simulation sur un réseau local (LAN). Toutefois, nous avons également la possibilité de le faire fonctionner sur des réseaux virtuels en utilisant un commutateur de niveau 3 ou un routeur. Voici les étapes nécessaires pour le faire sur notre serveur :

Configuration des VLANS :

Nous accédons à l'outil "Utilisateurs et ordinateurs Active Directory" où nous créons trois groupes pour chaque VLAN.

— Groupe Télécom pour Vlan 10

— Groupe RT pour Vlan 11

— Groupe ST pour Vlan 12

Puis, nous ajoutons les ordinateurs respectifs à ces groupes.

Ensuite, nous procédons à l'ajout des ordinateurs et des utilisateurs à chaque groupe, en suivant les étapes décrites dans une figure précédente. Nous cliquons sur le groupe souhaité, puis sur "Membres", suivi de "Ajouter" et sélectionnons les ordinateurs ou utilisateurs que nous voulons ajouter. Nous vérifions les noms des ordinateurs, puis cliquons sur "Appliquer" pour les ajouter au groupe. Après cela, nous nous rendons sur le serveur Radius et accédons aux stratégies pour ajouter trois nouvelles stratégies. Nous nommons ces stratégies en fonction du numéro de VLAN Correspondant.

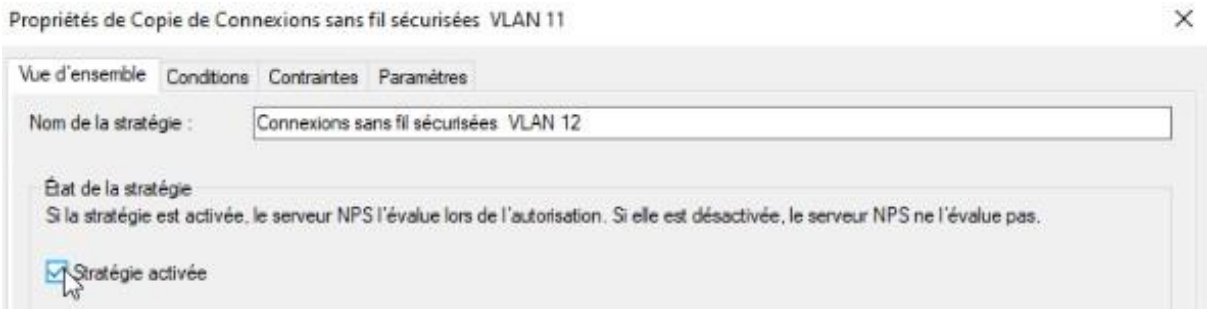


FIGURE 4.32 – Création des stratégies pour chaque vlan

Pour chaque stratégie, nous commençons par supprimer le groupe par défaut, puis nous ajoutons les groupes correspondants à chaque VLAN. Par exemple, pour la stratégie liée au VLAN 10, nous ajoutons le groupe "Télécommunication". Pour la stratégie du VLAN 11, nous ajoutons le groupe "RT" et pour le VLAN 12, nous ajoutons le groupe "ST"etnous ajoutons le type authentification PEAP.

Le tunnel-tag permet d'identifier le trafic encapsulé dans un tunnel, le tunnel-medium spécifie le support utilisé pour acheminer le trafic et le tunnel-type définit le type de tunnel utilisé pour encapsuler le trafic. Ces concepts sont essentiels pour la mise en place et la configuration de tunnels de communication dans les réseaux.

— Nous avons choisit le type de tunnel « tunnel-pvt-group-ID » pour connecter un groupe spécifique d'utilisateurs ou de périphériques distants. Il est souvent utilisé dans les réseaux d'entreprise pour permettre l'accès sécurisé à distance à des

ressources réseau spécifiques.

— On ajoute les vlan 10,11et 12. Et on choisit la connexion 802.1x cette connexion 802.1x permet la sécurité et de la gestion de l'accès aux réseaux.

— On ajoute les stratégie dans NPS pour chaque vlan 10,11et 12.

— Configuration du serveur DHCP

Nous allons créer des nouvelles étendu pour chaque vlan 10,11 et 12. On suivant les étapes pour vlan 11 mêmes étapes pour vlan 12 et 10

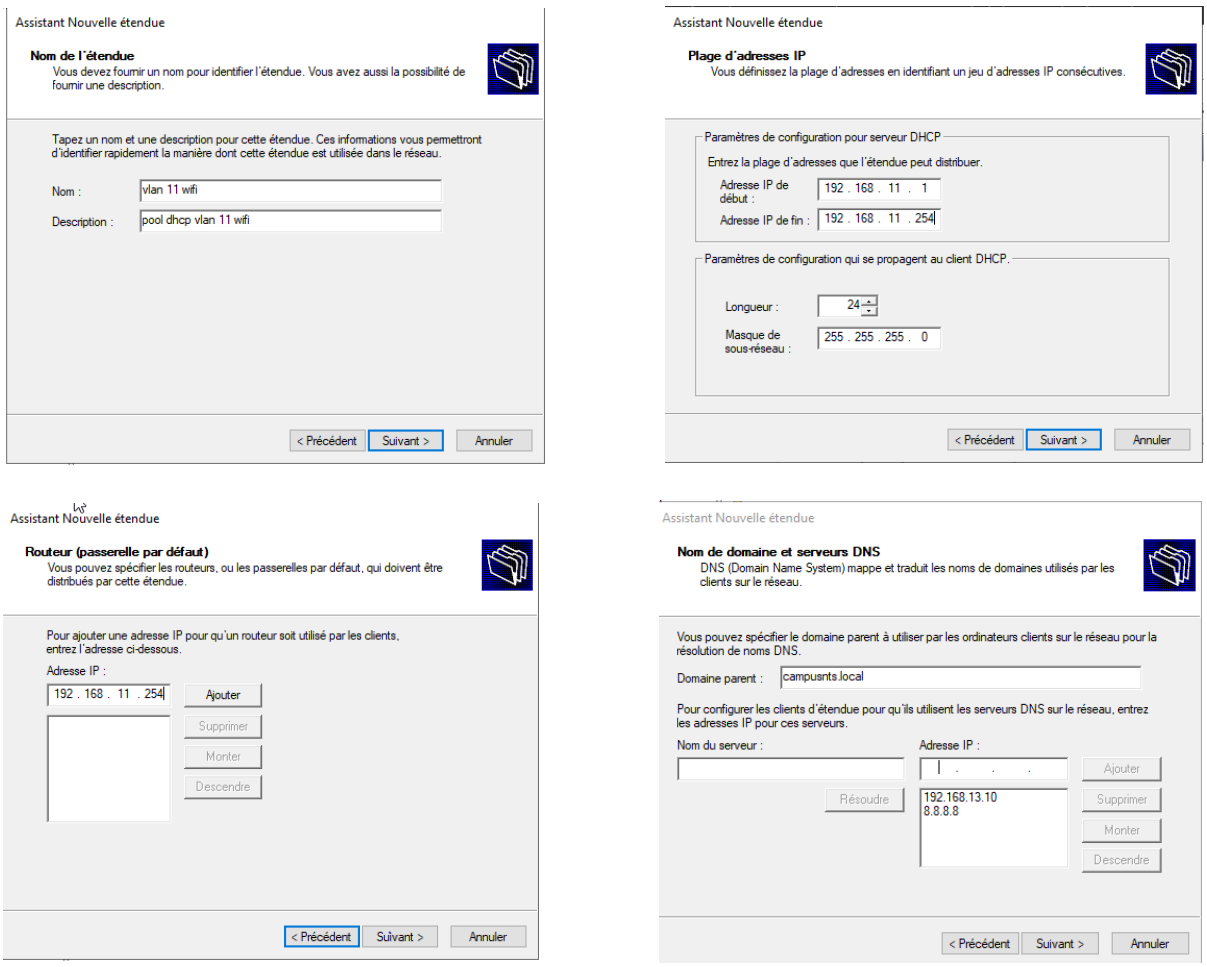


FIGURE 4.33 – Les étapes de configuration DHCP

Conclusion

En conclusion, ce chapitre pratique constitue une étape essentielle dans notre démarche visant à sécuriser un réseau sans fil en utilisant le certificat PEAP/TLS. En nous basant sur des outils de simulation tels que Packet Tracer et VMware, nous avons pu explorer concrètement les solutions de sécurisation et évaluer leur efficacité. Les connaissances acquises grâce à cette étude contribuer ont à renforcer la résilience des réseaux fil aires et garantir un environnement de communication sur et fiable.

Conclusion générale

En conclusion, ce mémoire de fin d'études a mis en évidence l'importance croissante de la sécurité des réseaux sans fil, en particulier des réseaux Wi-Fi, dans notre société actuelle. Avec la prolifération des dispositifs connectés et la dépendance croissante à l'égard des communications sans fil, il est essentiel de mettre en place des mesures de sécurité adéquates pour protéger l'intégrité des données, garantir la confidentialité des informations, contrôler l'accès au réseau et authentifier les utilisateurs.

Le mémoire a examiné en détail les différentes dimensions de la sécurité des réseaux sans fil, en mettant l'accent sur l'authentification basée sur des certificats PEAP/TLS. Il a exploré les risques et les attaques potentiels auxquels les réseaux Wi-Fi sont exposés, tout en proposant des solutions et des techniques de sécurité pour contrer ces menaces.

De plus, ce mémoire a présenté une étude de cas sur l'entreprise "N.T.S" et son client "ngtmeziani", mettant en évidence les problématiques de sécurité auxquelles elle est confrontée. Des solutions spécifiques ont été proposées pour améliorer la sécurité de ce réseau, en mettant en œuvre une authentification basée sur des certificats PEAP/TLS.

En mettant en pratique ces solutions, ce mémoire a démontré la faisabilité et l'efficacité de l'authentification basée sur des certificats pour garantir la sécurité des réseaux Wi-Fi. Il a souligné l'importance de comprendre les fondamentaux des réseaux sans fil et de la sécurité informatique pour concevoir et mettre en œuvre des réseaux sécurisés.

En conclusion, ce mémoire a contribué à approfondir nos connaissances sur la sécurité des réseaux sans fil . Il a souligné l'importance de rester à jour avec les avancées technologiques et les meilleures pratiques de sécurité pour faire face aux défis continus liés à la protection des réseaux sans fil dans un monde de plus en plus connecté.

Bibliographie

[1] https ://fr.farnell.com/ wireless-technology

[2] AMINI Hocine, GUERMAH Nabila, Etude sur les mécanismes de sécurité d'un réseau Wi-Fi , UNIVERSITE MOULOUD MAMMERI TIZI-OUZOU, Promotion 2012-2013

[3] https ://web.maths.unsw.edu.au/lafaye/CCM/wifi/wifimodes.htm

[4] Réseaux et communication sans fil (2eme édition), l'auteur sttaling

[5] Terre, M. (2007). Wifi, le Standard 802.11, couche physique et couche MAC (Version 1.1). Technical report, Mars.

[6] Rabehi Sidi, Mohamed El Amine , Mise en place d'un serveur radius sous linux pour la sécurisation d'un réseau 802.11, Universite abou baker belkaid , Année universitaire : 2010 - 2011

[7] MIHOUBI MOHAMED, MEDJANI NACER, Sécurisation d'une infrastructure LAN/WANA base d'équipement Cisco, UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU, année 2015

[8] Ouziane mohamed, Sécurité d'agrégation de données dans les réseaux de capteur sans fils , Université Mouloud Mammeri de Tizi-Ouzou, Année universitaire : 2012-2013

[9] https :actualite informatique.fr-wp-content-uploads-2019-11-Data-Encryption.webp

[10] Houda HAFI, Protocole pour la sécurité des réseaux sans fil peer to peer, Université Kasdi Merbah – Ouargla.

[11] Belarbi abd elkader,Benaida Ahmed,Étude comparative de systèmes cryptographiques, UNIVERSITE Dr. TAHAR MOULAY SAIDA, Année Universitaire 2020-2021

[12] Allou Said, Allouane Kahina, Cryptographie et sécurité des Réseaux Implémentation de l'AES sous MATLAB, Année 2008

[13] MIROUD Amina, NOUADRI Mouna , Cryptanalyse de RSA : Etude comparative de deux approches, UNIVERSITE LARBI BEN M'HIDI OUM EL BOUAGHI,Année universitaire 2016

[14] Alexandre Berzati, Analyse cryptographique des altérations d'algorithmes , Université de Versailles-Saint Quentin en Yvelines, Année 2011.

[15] http ://www.microsoft.com/whdc/hwdev/tech/network/802x/accesspts.mspx

[16] kaddouh Adada, Belhocine Faycal, Mise en place d'un Serveur d'authentification RADIUS Sous Gns3 Cas : EPB de Bejaia, Universite A.MIRA-BEJAIA, Année Universitaire : 2020-2021

[17] BOUAZIZ Sihem, FAREZ Nouara, Sécuriser un réseau Wifi en implémentant le protocole d'authentification 802.1x sur le serveur RADIUS, UNIVERSITE MOULOUD MAMMERI, TIZI-OUZOU, Année Universitaire : 2012/2013

[18] ADJAOUD Yougourthen, KEHOUL Tarek, Authentification unique avec CAS et LDAP, Université A/Mira de Béjaïa, Année Universitaire : 2011 - 2012

[19] HAMDAD Sabrina, KHELFAOUI Katia, Mise en place d'une Politique AAA pour le réseau sans fil, Université A. Mira de Béjaia, Année Universitaire 2012/2013

[20] MESSOUS Massinissa,Mise en place d'un système de sécurité basé sur l'authentification dans un réseau IP, UNIVERSITE MOULOUD MAMMERI DE TIZI-OUZOU,Année Universitaire : 2014/2015

[21] YBOUGHANI Rafik,YAHIA CHERIF Fawzi, ÉTUDE, ANALYSE ET PROPOSITION D'UNE SOLUTION D'AUTHENTIFICATION ET DE GESTION DE CLÉS DU STANDARD 802.11i,Université A/Mira de Béjaia, Année Universitaire 2011/2012

[22] Monnier, marie, 10807915, wpa 2008 2009

[23] Exposé, sécurité réseaux sans fil, standard wifi, promotion 2010/2011

Annexe

Installation de VMware Workstation version 17 Définition

VMware Workstation est un logiciel de virtualisation développé par VMware qui permet de créer et de gérer des machines virtuelles sur un ordinateur hôte. Il offre la possibilité d'exécuter plusieurs systèmes d'exploitation simultanément sur une seule machine physique, permettant ainsi aux utilisateurs de tester des logiciels, de développer des applications multiplateformes et d'effectuer des configurations complexes sans avoir besoin de plusieurs ordinateurs physiques.

FIGURE 4.34 – VMWare

1. **Installation de la VMware Workstation**

   Il est important de noter que VMware Workstation est une application qui permet d'exécuter des machines virtuelles sur un système d'exploitation existant, tel que Windows 10. Nous devons donc avoir Windows 10 installé et fonctionnel sur l ordinateur avant de pouvoir installer et utiliser VMware Workstation.

FIGURE 4.35 – Windows 10

Pour commencer l'installation de VMware Workstation, nous devons tout d'abord té-

lécharger le programme d'installation à partir du site officiel de VMware. Une fois le programme d'installation téléchargé, nous pourrons le lancer en effectuant un double-clique dessus pour démarrer le processus d'installation en suivant les étapes de la figure

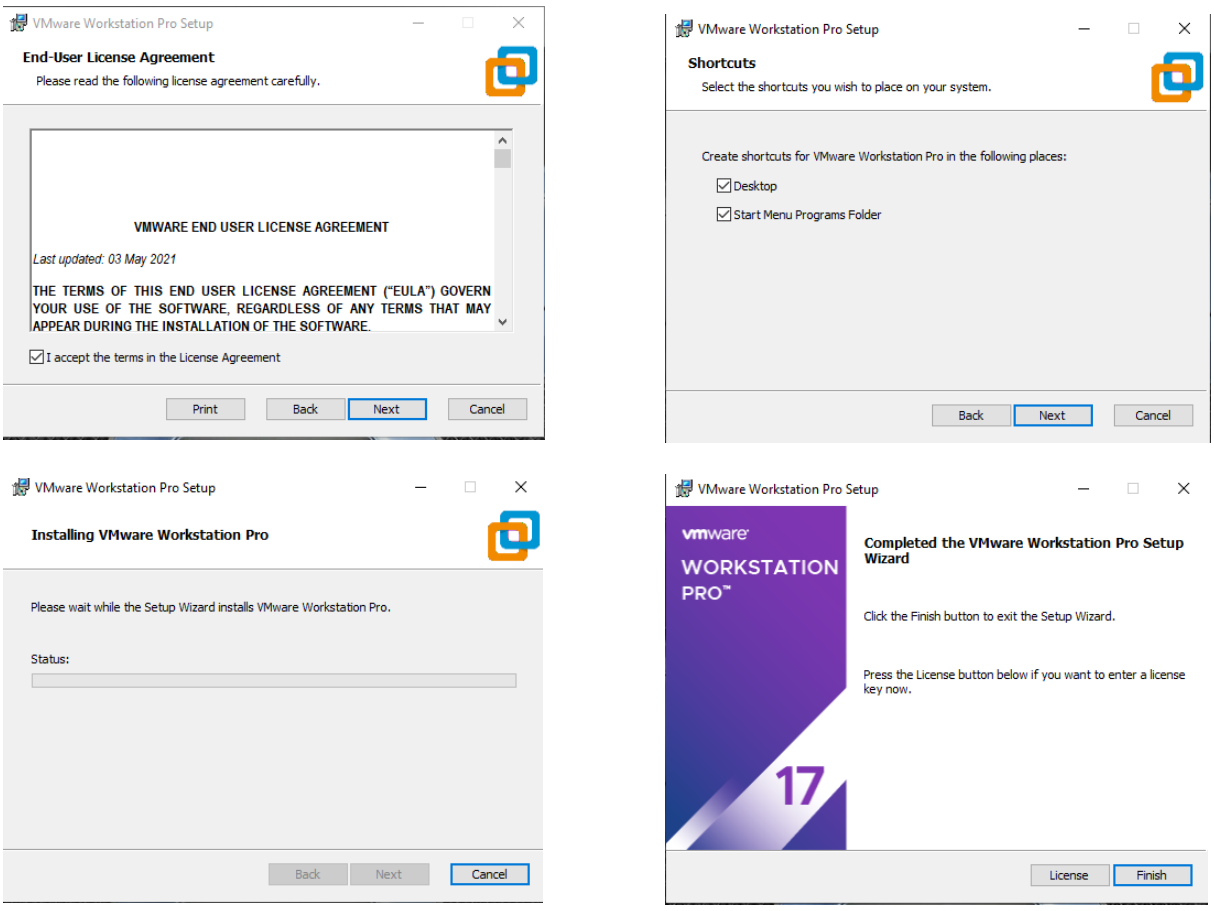


FIGURE 4.36 – Installation VMWareworkstation

Une fois que l installation est fini nous devons insérer une clé pour accéder

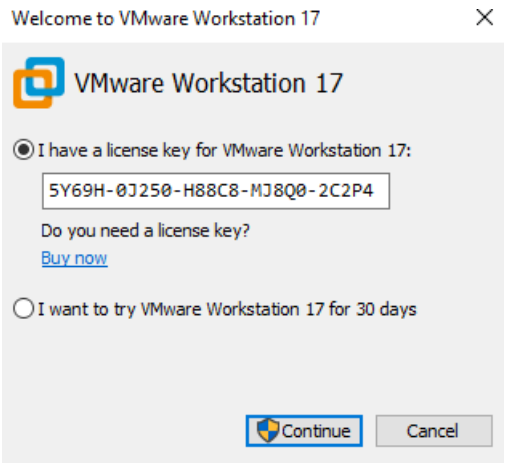


FIGURE 4.37 – La clé de VMware

Après l'installation de VMware une page d'accueil apparaitra

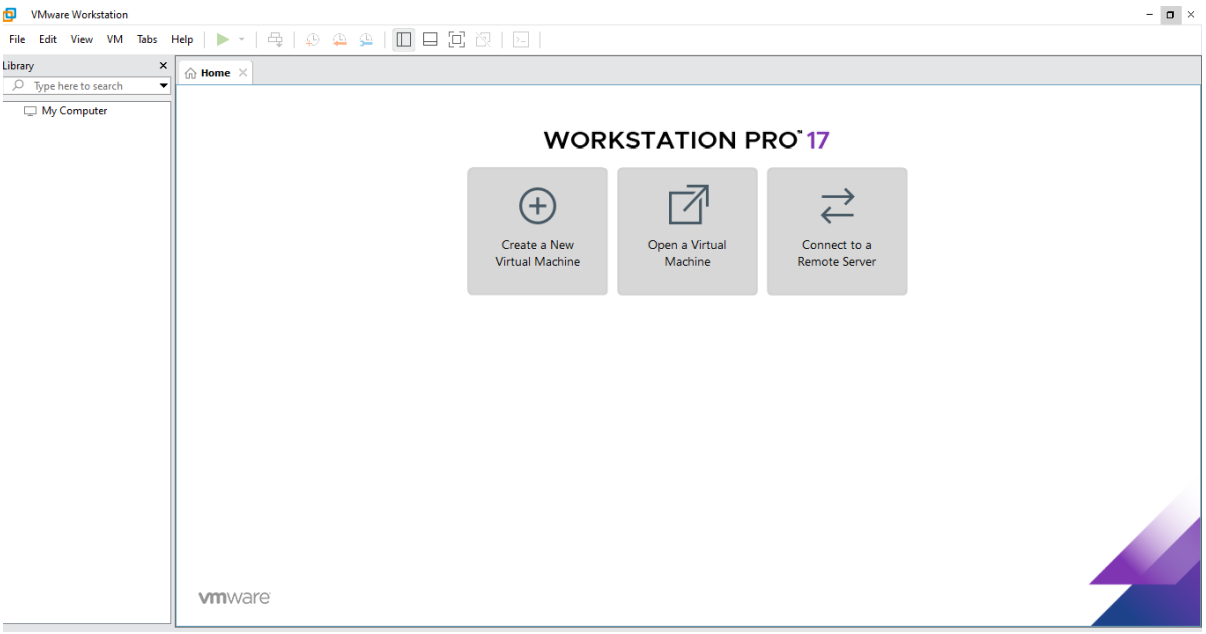


FIGURE 4.38 – Page d'accueil de VMWareWorkstation

2. Installation du packettracer

Pour installer Cisco packet tracer nous téléchargeons sur le site officiel et cliquer deux fois en suivant les étapes suivantes

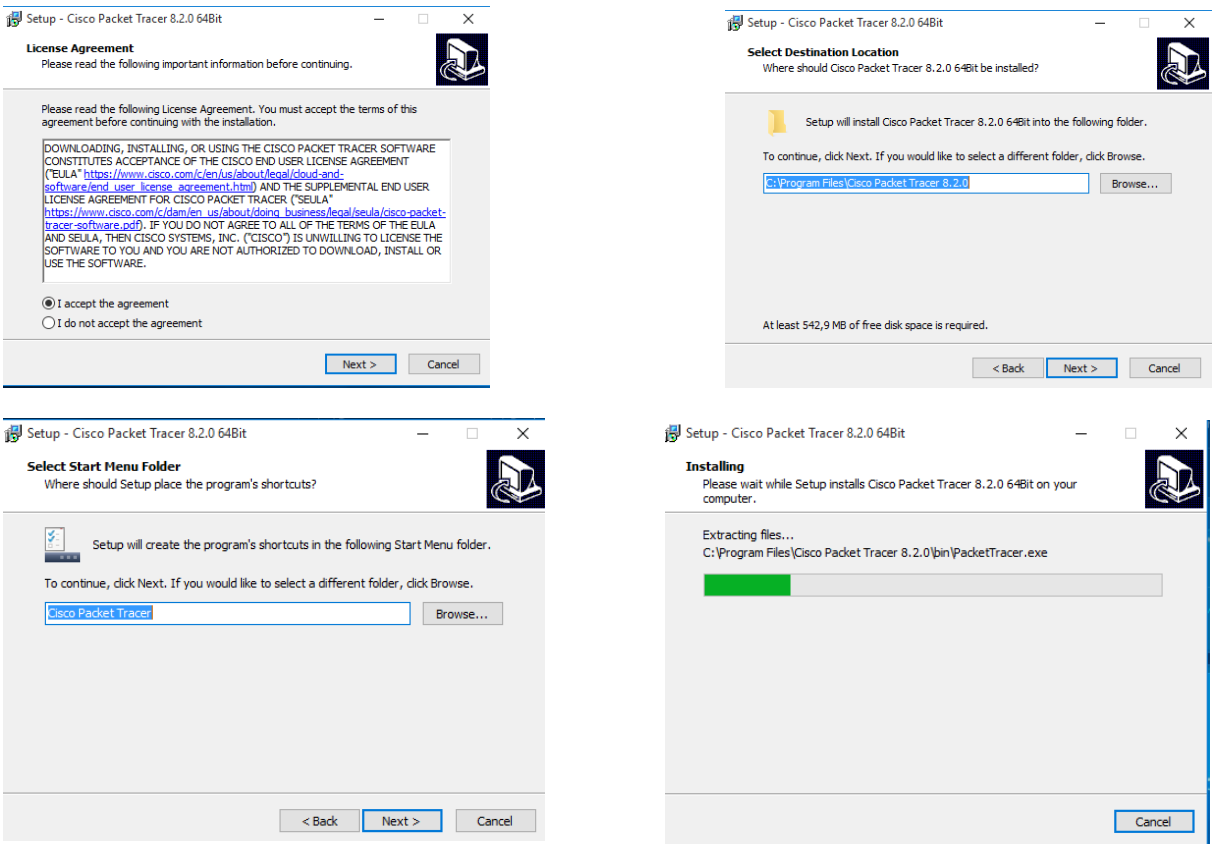


FIGURE 4.39 – Les étapes d'installation du packettracers

Installation du Serveur Radius

Une fois VMware installé, nous procéderons à l'installation de la machine virtuelle qui servira de serveur Radius en suivant les étapes illustrées dans les figures

Ensuite nous allumons le serveur pour continuer l'installation puis lui insérer un mot de passe :

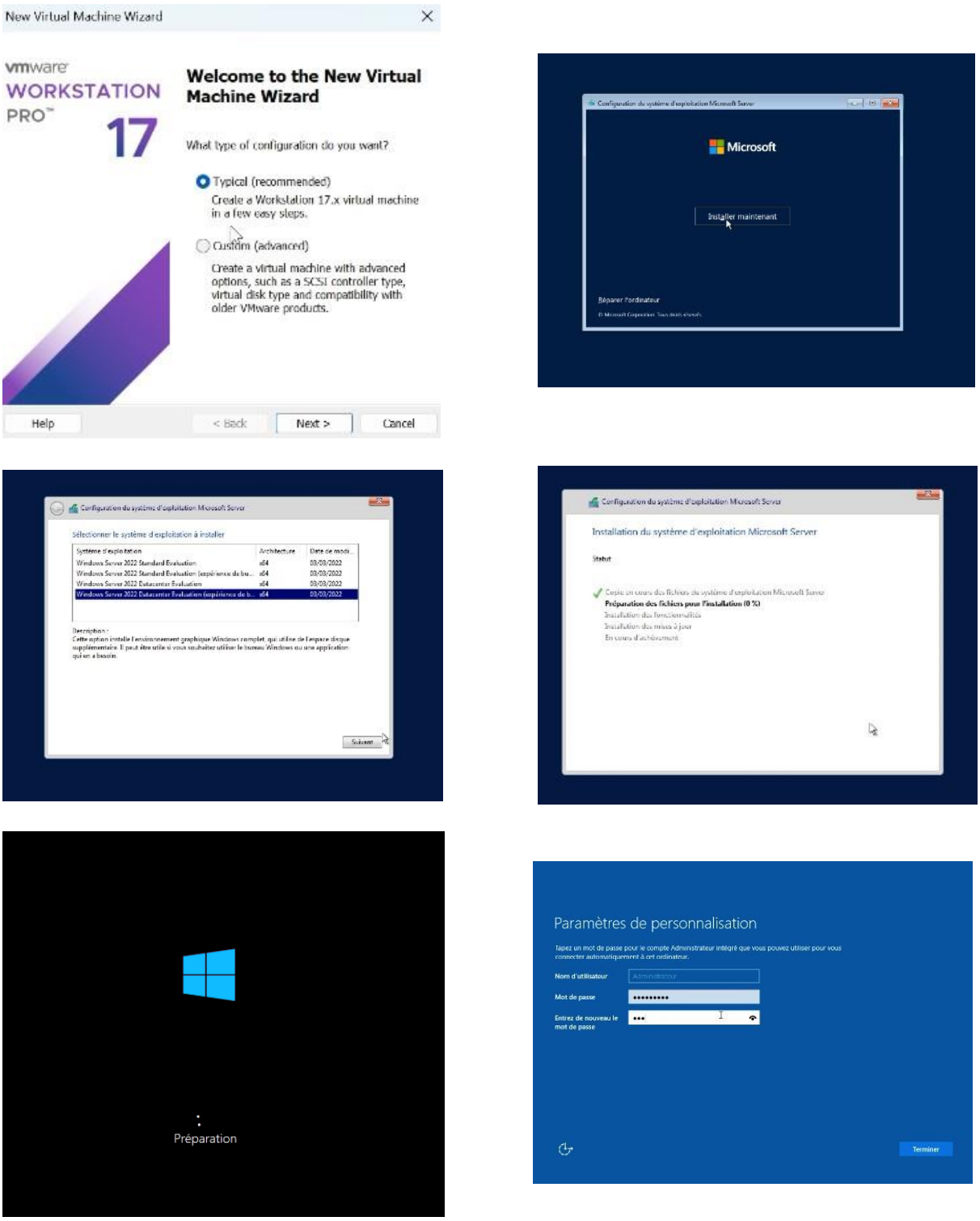


FIGURE 4.40 – Les étapes d'Installation su serveur Radius

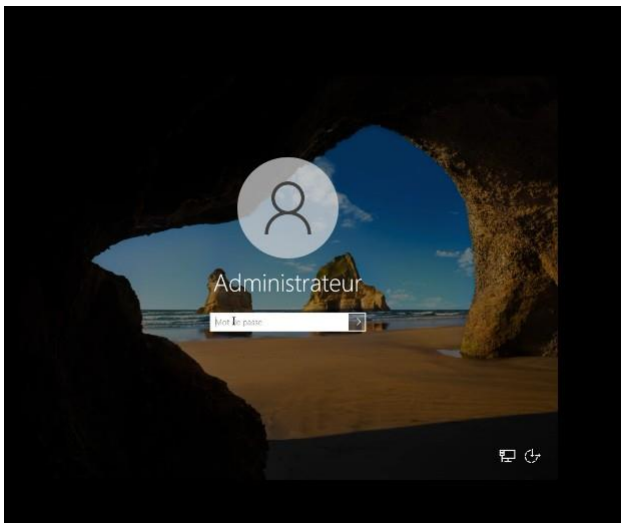


FIGURE 4.41 – La page du Windows server 2022

La figure ci-dessus montre la page d'accueil du serveur Radius:

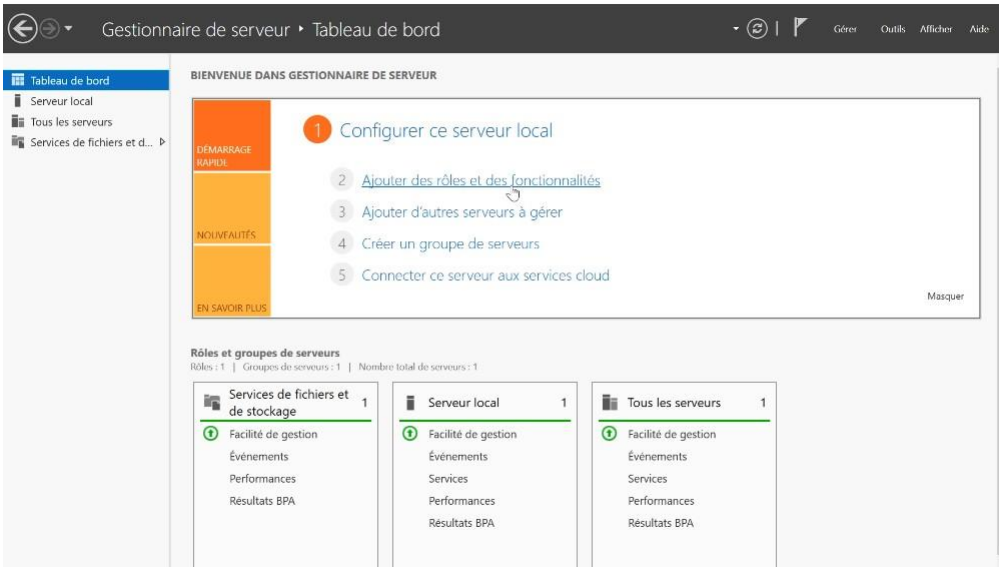


FIGURE 4.42 – la page du serveur RADIUS

Résumé

Dans notre société contemporaine, les réseaux sans fil représentent une source de commodité et de connectivité permanente. Toutefois, cette facilité d'utilisation comporte également des risques potentiels. Les réseaux sans fil sont souvent accessibles à distance, ce qui expose nos données sensibles à d'éventuelles tentatives d'accès non autorisées et comproettent la sécurité de nos appareils.

Dans le cadre de notre projet, nous avons mis en place une solution sécurisée en utilisant un serveur Radius. Cette solution est spécifiquement conçue pour répondre aux besoins de l'utilisation professionnelle, permettant ainsi de mettre en place un réseau sans fil sécurisé en utilisant la certification des ordinateurs basée sur PEAP/TLS. Cette approche garantit une authentification solide et une communication sécurisée entre les appareils connectés, renforçant ainsi la confidentialité des données et la protection du réseau.
L'implémentation de cette architecture a été faite avec des outils VMware Workstation et un serveur Radius.

Mots clés: Réseaux sans fil, Serveur Radius, PEAP/TLS, Authentification

Abstact

In today's society, wireless networks represent a source of commodity and constant connectivity. However, this ease of use also entails potential risks. Wireless networks can often be accessed remotely, exposing our sensitive data to unauthorised access and compromising the security of our devices.

As part of our project, we implemented a secure solution using a Radius server. This solution is specifically designed to meet the needs of business use, enabling a secure wireless network to be set up using PEAP/TLS-based computer certification. This approach ensures strong authentication and secure communication between connected devices, reinforcing data confidentiality and network protection.

This architecture was implemented using VMware Workstation tools and a Radius server.

Key word: wireless networks, Radius server, PEAP/TLS, authentication