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

Mémoire de fin de cycle

En vue d'Obtention du Diplôme de Master Professionnel en Informatique
Option : Administration et Sécurité des Réseaux

Mise en place d'une Politique AAA pour le réseau sans fil de l'Université de Béjaia

Réalisé par :
HAMDAD Sabrina.
KHELFAOUI Katia.

Sous la direction de :
Dr. A. SIDER

Président :	M^{r} SEBAA	Abderrezak,	Université de A.Mira, Bejaia.
Examinateur :	D^{r} OMAR	Mawloud,	Université de A.Mira, Bejaia.
Examinateur :	M^{me} BENSAID	Samia,	Université de A.Mira, Bejaia.

Année Universitaire 2012/2013

Remerciements

NOUS rendons grâce à notre Dieu, le tout puissant et miséricordieux, pour nous avoir donné le courage et la patience pour mener à bout ce modeste travail.

Nos plus sincères remerciements s'adressent à notre encadreur M^r SIDER Abderrahmane maître de conférences à l'université de Béjaia, pour nous avoir proposé ce sujet intéressant et pour ses précieux conseils et encouragements.

Nos remerciements s'adressent également aux membres de jury, en l'occurrence M^r SEEBA Abderrezak, M^r OMAR Mawloud et M^{me} BENSAID Samia d'avoir accepté d'évaluer notre travail et pour l'intérêt qu'ils y portent.

Nous tenons à remercier tous les enseignants, qui ont assuré notre formation durant notre cycle universitaire.

Enfin un grand merci à nos familles, pour leur soutien permanent et indéfectible qui nous ont permis de chercher au plus profond fond de nous même la force, la volonté et la persévérance à même d'arriver à cet instant des plus important de notre vie et à nos amis et tous ceux qui ont contribué de près ou de loin à la concrétisation de cette oeuvre.

Dédicaces

Je dédie ce modeste travail :

À mes très chèr parent qui n'ont pas cessé de m'encourager et de se sacrifier pour que je puisse franchir tout obstacle durant toutes mes années d'étude que dieu me les garde en très bonne santé ;
À mes frères Miloud et Khellaf et à ma sœur Sihem ;
À la mémoire de mes grands parents ;
À mes oncles, à mes tantes, à toutes mes cousines et cousins
À toute ma famille de prés et de loin , À Dahia, Katia, Asma, Kahina, Jojo, Et je pense tous particulièrement ;
À mes deux meilleures amis : Amine & Souhila, ainsi à leurs familles.
Sabrina

Que la paix d'Allah soit avec tous

Je dédie ce modeste travail *:*

À ma plus belle étoile qui puisse exister dans l'univers,
ma très chère mère celle a qui je souhaite une longue vie et
bonne santé ;
À mon père qui n'a pas cessé de m'encourager et de se sacrifier
pour que je puisse franchir tout obstacle durant toutes mes années
d'étude que le dieu me le garde entrès bonne santé ;
À mes chères frères Mendoh, Dida et Boukrou et à mes chéres soeurs Siham,
Mina et Biha ;
À mon chère âme soeur Fayssal pour ton soutien, tes conseils et tes
encouragements qui m'ont appris à ne pas me sous-estimer et m'ont permis de
réussir mes études ;
À la mémoire de mes grands-mères Djida et Menana ;
À chaque cousins et cousines surtout Nouara, Karima, Djamila, Hafit, Lamia, Nabila,
Jaja, Cyline, Lili, Sara et aux petites adorables Malek et Nadine ;
À ma très chère binôme et amie Sabrina, malgré les obstacles et les difficultés qui
se sont interposées, nous avons pu les surmontés. En témoignage de l'amitié qui nous uni
et des souvenirs de tous les moments que nous avons passé ensemble, je te dédie ce travail
et je te souhaite une vie pleine de santé et de bonheur ;
À tous mes chères amies spécialement : Asma, kahina$\times 3$, $widad$, $sabah$, $Doria\ et\ Dalila$;
À tous ceux qui m'ont aidé sourtout Fafo, Khaled et à tous ceux qui m'aiment et qui me
cannaient de proche ou de loin.
katia

Que la paix d'Allah soit avec tous

Table des matières

Table des matières i

Liste des Abréviations iv

Liste des figures x

Liste des tableaux xii

Introduction Générale 1

1 Etat de l'art sur la sécurité comprenant les politiques AAA 3
- 1.1 Introduction . . . 3
- 1.2 Les réseaux informatiques . . . 3
- 1.3 Menaces courantes de sécurité . . . 4
  - 1.3.1 Vulnérabilité . . . 4
  - 1.3.2 Les menaces . . . 5
  - 1.3.3 Les attaques . . . 6
- 1.4 La sécurité informatique . . . 8
  - 1.4.1 Objectif de la sécurité informatique . . . 8
  - 1.4.2 Les éléments à protéger . . . 8
  - 1.4.3 Mise en oeuvre de la sécurité informatique . . . 9
- 1.5 Les politiques AAA . . . 14
  - 1.5.1 Définition de AAA . . . 14
  - 1.5.2 Architecture AAA . . . 15
  - 1.5.3 Protocole AAA . . . 15
- 1.6 Conclusion . . . 17

2 Etude des architectures de sécurité des réseaux sans fil notamment les différentes techniques EAP et leurs implications 18
- 2.1 Introduction . . . 18
- 2.2 Les réseaux sans fil . . . 19
  - 2.2.1 Les différents types de réseaux sans fil . . . 19
  - 2.2.2 Les contraintes liées aux réseaux sans fil . . . 21
- 2.3 Présentation du WiFi . . . 22

2.3.1 Utilisation du WiFi . . . 22
2.3.2 Les modes de fonctionnement du WiFi . . . 22
2.3.3 Les avantages du WiFi . . . 24
2.4 Sécurité du 802.11 . . . 25
2.4.1 Limiter les débordements . . . 25
2.4.2 Masquer le SSID . . . 25
2.4.3 Filtrage par adresse MAC . . . 25
2.4.4 Les VLAN . . . 26
2.4.5 Le cryptage WEP . . . 26
2.5 Les nouvelles solutions de sécurité . . . 28
2.5.1 Les VPN . . . 28
2.5.2 Le WPA . . . 29
2.5.3 Le WPA2 . . . 30
2.5.4 Le 802.1x . . . 30
2.6 L'EAP . . . 32
2.6.1 Le protocole PPP . . . 32
2.6.2 Le fonctionnement d'EAP . . . 34
2.6.3 Mécanismes d'authentification EAP . . . 35
2.7 Conclusion . . . 37

3 Proposition d'une solution AAA open source basée sur RADIUS/OpenLDAP/OpenSSL 38
3.1 Introduction . . . 38
3.2 Objectif du travail . . . 38
3.3 Démarche adoptée . . . 39
3.4 La politique de sécurité . . . 40
3.5 Type d'authentification choisie . . . 40
3.6 Le portail captif . . . 42
3.6.1 Définition d'un portail captif . . . 42
3.6.2 Les principaux portails captifs . . . 42
3.6.3 PfSense . . . 43
3.7 RADIUS . . . 43
3.7.1 Principe de fonctionnement . . . 43
3.7.2 Les différents types de paquets . . . 44
3.7.3 Les différents implémentation de RADIUS . . . 46
3.7.4 FreeRADIUS . . . 47
3.8 Annuaire LDAP . . . 48
3.8.1 Définition d'un annuaire . . . 48
3.8.2 Définition d'un annuaire LDAP . . . 48
3.8.3 Les avantages des annuaire LDAP . . . 49
3.8.4 OpenLDAP . . . 49
3.8.5 LDAP et la sécurité . . . 50

3.9 SSL . . . 50
3.9.1 Le protocole SSL . . . 50
3.9.2 Le fonctionnement de SSL . . . 51
3.9.3 Openssl . . . 51
3.10 Conclusion . . . 52

4 Implémentation de la solution et tests **53**
4.1 Introduction . . . 53
4.2 Pré-requis . . . 53
4.3 Mise en place du serveur LDAP . . . 54
4.3.1 L'installation de OpenLDAP . . . 54
4.3.2 Configuration d'OpenLDAP . . . 55
4.3.3 Ajout des entrées dans la base LDAP . . . 58
4.3.4 Outils d'administration de l'annuaire . . . 59
4.4 Installation de OpenSSL . . . 61
4.4.1 Génération du certificat pour le serveur LDAP . . . 61
4.4.2 Modification de la configuration du serveur LDAP . . . 62
4.5 Mise en place du serveur FreeRADIUS . . . 63
4.5.1 Installation de FreeRADIUS . . . 63
4.5.2 Modification sur le serveur LDAP . . . 64
4.5.3 Configuration du FreeRADIUS . . . 65
4.6 Configuration de MySQL . . . 72
4.6.1 Pré-requis . . . 72
4.6.2 Création de la base de données . . . 72
4.6.3 Inclusion des schémas dans la base de données . . . 72
4.7 L'interface web d'administration du serveur RADIUS . . . 73
4.7.1 Installation de Daloradius . . . 73
4.7.2 Installation de PfSense . . . 75
4.7.3 Configuration de PfSense . . . 77
4.7.4 Configuration du portail captif . . . 78
4.8 Test de fonctionnement . . . 79
4.8.1 Test de l'authentification et l'authorisation . . . 79
4.8.2 Test de la comptabilité . . . 80
4.9 Conclusion . . . 81

Conclusion Générale **82**

Bibliographie **91**

Liste des Abréviations

C

CA : Certification Authority.

CCM : Counter with CBC-MAC.

CCMP : Counter with CBC MAC Protocol.

CERT : Computer Emergency Response Team.

CHAP : Challenge Handshake Authentication Protocol.

CRC : Control Redundancy Check.

D

DES : Data Encryption Standard.

DHCP : Dynamic Host Configuration Protocol.

DN : Distinguished Name.

DNS : Domain Name Server.

DoS : Denial of Service.

DS : Distribution System.

DSA : Digital Signature Algorithm.

DVB-S : Digital Video Broadcasting-Satellite.

E

EAP : Extensible Authentification Protocol.

EAP-MD5 : EAP-Message Digest 5.

EAP-SIM : EAP - Subsciber Identity Module.

EAP-TLS : EAP-Transport Layer Security.

EAP-TTLS : EAP-Tunneled Transport Layer Security.

EAPOL : Extensible Authentification Protocol Over Lan.

ESS : Extended Service Set.

ETSI : European Telecommunications Standards Institute.

F

FAI : Fournisseur d'Accès à Internet.

FHSS : Frequency Hopping Spread Spectrum.

FTP : File Transfer Protocol.

G

GPRS : General Packet Radio Service.

GSM : Global System for Mobile Communications.

GTC : Generic Token Card.

H

HDLC : High Data Level Control.

HiperLAN2 : High Performance Radio LAN 2.0.

HTTP : Hypertext Transfer Protocol.

I

IBSS : Independent Basic Service Set.

ICMP : Internet Control Message Protocol.

IDEA : International Data Encryptions Algorithm.

IEEE : Institute of Electrical and Electronics Engineer.

IETF : Internet Engineering Task Force.

IP : Internet Protocol.

IPX : Internetwork Packet eXchange.

IR : Infrarouges.

ISO : International Organization for Standardization.

IV : Vecteur d'initialisation.

L

LAN : Local Area Network.

LCP : Link Control Protocol.

LDAP : Lightweight Directory Access Protocol.

LEAP : Lightweight Extensible Authentification Protocol.

M

MAC : Medium Access Control.

MAN : Metropolitan Area Network.

MANET : Mobile Ad-Hoc NETworks.

MD5 : Message Digest 5.

MS-CHAP 2 : Microsoft Challenge Handshake Authentication Protocol version 2.

MySQL : My Structured Query Language.

N

NAS : Network Access Server.

NCP : Network Control Protocol.

NETBEUI : NETBIOS Extended User Interface.

NSLOOKUP : Name Server Lookup.

O

OCB : Offset Code Book.

OSI : Open Source Inder.

OTP : One Time Password.

P

PAP : Password Authentication Protocol.

PDA : Personal Digital Assistant.

PEAP : Protected EAP.

PGSQL : PostgreSQL.

PPP : Point to Point Protocol.

PSK : Pré-Shared Key.

R

RADIUS : Remote Authentification Dial In User Service.

RC2 : Rivest Cipher 2.

RC4 : Rivest Cipher 4

RFC : Request For Comment.

RIPEMD160 : RACE Integrity Primitives Evaluation Message Digest.

S

SCTP : Stream Control Transmission Protocol.

SHA : Super High Aperture.

SI : Système d'Information.

S/MIME : Secure/Multiplepurpose Internet Mail Extension.

SIM : Subscriber Identity Module.

SSID : Service Set Identifier.

SSL : Secure Socket Layer.

T

TACACS+ : Terminal Access Controller Access Control System Plus.

TCP : Transmission Control Protocol.

TGS : Ticket Granting Server.

TKIP : Temporal Key Integrity Protocol.

TLS : Transport Layer Security.

TTLS : Tunneled TLS.

U

UDP : User Datagram Protocol.

UIT : Union internationale des télécommunications.

UMTS : UMTSUniversal Mobile Telecommunications System.

USB : Universal Serial Bus.

V

VLAN : Virtual Local Area Network.

VPN : Virtual Private Network.

W

WAN : Wide Area Network.

WECA : Wireless Ethernet Compatibility Alliance.

WEP : Wired Equivalent Privacy.

WiFi : Wireless Fidelity.

Wi-Max : Worldwide Interoperability for Microwave Access.

WLAN : Wireless Local Area Networks.

WMAN : Wireless Metropolitan Area Network.

WPA2 : Wi-Fi Protected Access version 2.

WPAN : Wireless Personal Area Network.

WPA : Personal Wi-Fi Protected Access Personal.

WRAP : Wireless Robust Authenticated Protocol.

WWAN : Wireless Wide Area Network.

X

XOR : OU exclusive.

LISTE DES FIGURES

1.1 Architecture AAA simple 15

2.1 Les types de réseaux sans fil [2]. 21
2.2 Le mode infrastructure 23
2.3 Le mode Ah Hoc 24
2.4 Filtrage par adresse MAC. 26
2.5 Opération de chiffrement et déchiffrement. 27
2.6 Architecture d'authentification 802.1X. 31
2.7 L'identification avec le protocole PAP. 33
2.8 L'identification avec le protocole CHAP. 34

3.1 Schématisation de la solution. 39
3.2 L'authentification PEAP. 41
3.3 L'architecture RADIUS. 44
3.4 Un scénario de communication RADIUS. 45

4.1 Reconfiguration de debconf. 54
4.2 La translation du niveau élevé à basse. 54
4.3 La configuration principale d'OpenLDAP. 56
4.4 L'ajout du schéma core.ldif. 57
4.5 Le fichier LDIF pour l'insertion de données dans la base. 58
4.6 Insertion de l'arborescence. 59
4.7 L'interface graphique de PHPLDAPADMIN. 60
4.8 Visualisation de l'annuaire à travers PHPLDAPADMIN. 60
4.9 Génération du certificat du serveur LDAP. 61
4.10 Modification du fichier /etc/default/slapd. 63
4.11 Test de présence du serveur freeradius. 64
4.12 Une entrée adaptée a radius. 64
4.13 Importation du schéma freeradius.ldif dans OpenLDAP. 65
4.14 Les principaux fichiers de configuration. 66
4.15 Modification de la partie log du fichier radiusd.conf 67
4.16 Modification de la partie #$INCLUDE sql.conf. 68
4.17 Le fichier de configuration Clients.conf 68
4.18 Le fichier de configuration ldap. 69

4.19 La partie authenticate du fichier default. 70
4.20 La partie authorize du fichier default. 70
4.21 L'activation de PEAP dans le fichier eap.conf. 71
4.22 Le fichier de configuration sql.conf. 72
4.23 Le fichier de configuration daloradius.conf.php. 74
4.24 L'interface de connexion de Daloradius. 74
4.25 L'interface principale de Daloradius. 75
4.26 Le menu de démarrage de pfsense. 75
4.27 Détection des cartes réseaux. 76
4.28 Le menu d'installation. 76
4.29 La configuration de l'interface LAN de PfSense. 77
4.30 La configuration du portail captif. 78
4.31 Le portail captif de PfSense. 79
4.32 Test de fonctionnement avec l'invité de commande. 80
4.33 Ajout d'un client NAS sur daloradius. 80
4.34 La liste des clients NAS sur daloradius. 81
4.35 La comptabilité des utilisateurs. 81
4.36 Le fichier cn={0}freeradius.ldif avant modification. 84
4.37 Le fichier cn={0}freeradius.ldif après modification. 85
4.38 Les lignes à supprimer du fichier cn={0}freeradius.ldif. 85
4.39 propriétés du réseau sans fil. 86
4.40 Changement du type de sécurité a WPA2-Entreprise. 87
4.41 Propriétés EAP protégées. 88
4.42 Propriétés EAP MSCHAPv2. 89

LISTE DES TABLEAUX

1.1 Les principaux avantages et inconvénients des techniques d'authentification [50]. . . 13

3.1 Les principaux portails captifs [49]. 42
3.2 Les différentes méthodes d'authentification supportées par le service RADIUS. . . . 46
3.3 Les différents connecteurs supportés par le service RADIUS. 46
3.4 Les services proxy et accouting supportés par RADIUS. 47

INTRODUCTION GÉNÉRALE

L'évolution des technologies de l'information et l'utilisation d'Internet a permit à beaucoup d'entreprises d'ouvrir leurs systèmes d'information à leurs partenaires ou leurs fournisseurs, sur ce, il s'avère donc essentiel de connaître les ressources de l'entreprise à protéger et ainsi maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information.

Dans les réseaux locaux, les réseaux sans fil viennent naturellement compléter les réseaux existants, ils sont plus souvent considérés comme une extension à un réseau filaire et non comme un potentiel remplaçant.

Depuis quelques années, les réseaux sans fil ne cessent de se développer. Ils rencontrent aujourd'hui un succès important car ils permettent de déployer des moyens de transmission sans contrainte d'immobilité liée aux câblages et aux prises. La promotion actuelle de ce type de solution est uniquement axée sur les avantages qu'elle procure : facilité et rapidité d'installation, coût inférieur à un système filaire, mobilité, accès partagé à des services de haut débit.

Bien que cette technologie semble aux premiers abords parfaite et sans soucis, la réalité est plus dure, due surtout au problème de la protection de ces réseaux sans fil. La nature de signal transmis (ondes électro magnétiques) rend difficile, voir impossible la maitrise complète de la propagation. En conséquent, il est assez facile d'écouter les messages et même de s'introduire sur de tels réseaux.

Notre objectif se cantonne à garantir les droits d'accès aux données et ressources de notre système en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des ressources possèdent uniquement les droits qui leurs ont été octroyés.

De ce fait, le travail que nous présentons dans le cadre du projet de fin d'étude consiste à la « Conception et Réalisation d'une Politique AAA pour le réseau sans fil de l'Université de Béjaia ». Notre travail va consister donc à exposer en détail le déploiement d'une solution de sécurité de réseau sans fil pour notre université.

Afin d'atteindre cet objectif, avec un niveau de protection satisfaisant, il convient de définir une politique de sécurité correspondante aux besoins, on a à notre disposition toute une palette de protocoles d'authentification qu'on doit associer selon une formule optimale tel, les protocoles AAA (Authentication, Authorization, Accounting) qui permettent d'authentifier des utilisateurs, de leur autoriser certains services et de collecter des informations sur l'utilisation des ressources.

Pour présenter ce projet, nous avons jugé judicieux de partager notre mémoire en quatre chapitres traitant chacun un problème particulier comme suit :

- Le premier chapitre, présente les aspects élémentaires des réseaux locaux sans fil, ainsi quelques notions fondamentales de la sécurité plus particulièrement la politique AAA.
- Le second chapitre, est consacré à l'étude des architectures de sécurité sans fil, de plus, il traite la présentation de diverses méthodes EAP avec leurs implications.
- Le troisième chapitre, constitue le noyau de notre projet, il présente la solution choisie qui est basée sur le 802.1x avec un serveur d'authentification radius qui sera complété par un annuaire LDAP. Pour cela le serveur d'authentification radius est chargé d'autoriser la connexion à un utilisateur possédant un compte valide dans l'annuaire LDAP de l'université.
- Le quatrième chapitre, concerne la mise en pratique de ces concepts et détaille l'implémentation des mécanismes et protocoles qu'on a choisis dans le chapitre précédent. Puis, nous terminons avec quelques testes afin de garantir le bon fonctionnement de notre solution.

Enfin notre mémoire s'achèvera par une conclusion générale résumant les points principaux qui ont été de grands apports et nous clôturerons avec quelques perspectives.

CHAPITRE 1

ETAT DE L'ART SUR LA SÉCURITÉ COMPRENANT LES POLITIQUES AAA

1.1 Introduction

La problématique de sécurité est omniprésente lorsque l'on évoque les systèmes d'informations et elle devient fondamentale lorsque l'on parle des réseaux. Comme tous les êtres humains, les usagers d'un réseau ressentent le besoin de sécurité et cela est dû à la grande place qu'occupe le réseau dans leurs vies. Les données transmises se rapportant à des biens personnels et professionnels nécessitent la confidentialité des échanges, l'authentification des sources, la garantie de leurs intégrité, etc. Ces apports ne peuvent, par ailleurs, être fournis sans la garantie de la disponibilité du réseau et des services associés. On ne peut en effet concevoir la sécurité sans la sûreté de fonctionnement.

1.2 Les réseaux informatiques

Les réseaux ont pour fonction de transporter des données d'une machine terminale à une autre. Une série d'équipements matériels et de processus logiciels sont mis en oeuvre pour assurer ce transport, depuis les câbles terrestres (coaxial, fibre optique) ou les ondes radio (Wimax, WiFi, Bluetooth, infrarouge) dans lesquels circulent les données jusqu'aux protocoles et règles permettant de les traiter [1].

En fonction de la localisation, la distance et le débit, les réseaux sont classés en trois types :

- LAN (*Local Area Network*) : réseau local, intra entreprise permettant l'échange de données et le partage de ressources.
- MAN (*Metropolitan Area Network*) : réseau metropolitain qui permet la connexion de plusieurs sites à l'échelle d'une ville.

– WAN (*Wide Area Network*) : réseau à l'échelle d'un pays, généralement celui des opérateurs. Le plus connu des WAN est Internet.

1.3 Menaces courantes de sécurité

Lorsqu'il est question de sécurité des réseaux, les trois notions qui interviennent habituellement dans la discussion sont la vulnérabilité, les menaces et les attaques [20] [17].

1.3.1 Vulnérabilité

La vulnérabilité est le degré de faiblesse inhérent à tout réseau ou périphérique. Les vulnérabilités ou faiblesses principales sont au nombre de trois :

1.5.1.1 Faiblesses technologiques

On peut citer trois principales qui sont :

– **Vulnérabilité du protocole TCP/IP :**
Par exemple les protocoles HTTP (*Hypertext Transfer Protocol*), FTP (*File Transfer Protocol*) et ICMP (*Internet Control Message Protocol*) sont non sécurisés.
– **Vulnérabilité des systèmes d'exploitation :**
Tous les systèmes d'exploitation présentent des problèmes de sécurité qui doivent être résolus. Ces problèmes sont documentés dans les archives du CERT (*Computer Emergency Response Team*).
– **Vulnérabilité des équipements réseau :**
Différents types d'équipements réseau ont des faiblesses de sécurité qui doivent faire l'objet d'une détection et d'une protection. Ces faiblesses concernent la protection des mots de passe, le manque d'authentification, les protocoles de routage et les ouvertures dans les pare-feu.

1.5.1.2 Faiblesses de configuration

Un des premiers problèmes de sécurité vient de la faiblesse des configurations appliquées aux différents matériaux. Les administrateurs réseaux préfèrent souvent une configuration qui fonctionne

bien et qui est faite rapidement. Par exemple, il n'est pas rare de voir des bornes qui utilisent des clés WEP, plutôt que des clés WPA.

1.5.1.3 Faiblesses dans la stratégie de sécurité

Une stratégie de sécurité peut être trop permissive ou au contraire trop restrictive. Dans le premier cas, elle risque de présenter une faiblesse de sécurité par son coté laxiste. Dans le second, elle peut devenir inapplicable du fait de règles trop strictes. Comme dans de nombreux domaines, seule l'expérience guide l'écriture d'une politique de sécurité ainsi que ces règles. Dans tous les cas, plus les ressources sont critiques, plus les règles doivent être strictes. Il existe des risques de sécurité pour le réseau, si par exemple les utilisateurs ne respectent pas la stratégie de sécurité.

1.3.2 Les menaces

Une menace est un événement, d'origine accidentelle ou délibérée, capable s'il se réalise de causer un dommage au sujet étudié, en d'autre terme c'est l'ensemble des actions de l'environnement d'un système pouvant nuire à la sécurité. Les menaces sont de plusieurs types, on peut citer la malveillance, l'erreur et l'accident, elles peuvent être subdivisées en deux types :

1.5.2.1 Les menaces non intentionnelles

Elles peuvent être causées par des pannes du système informatique (disfonctionnement matériel ou logiciel), des erreurs de manipulation de système, erreurs de manipulation d'informations, ou erreurs de conception d'application.

1.5.2.2 Les menaces intentionnelles

C'est l'ensemble des actions malveillantes qui constituent la plus grosse partie du risque. Elles font l'objet principal des mesures de protection.

1.3.3 Les attaques

Ces menaces sont mises en oeuvre à l'aide d'une variété d'outils et de programmes permettant de lancer des attaques contre des réseaux et leurs périphériques. Il existe quatre catégories principales d'attaques.

1.5.3.1 Reconnaissance

La reconnaissance est la découverte non autorisée des systèmes, de leurs adresses et de leurs services, ou encore la découverte de leurs vulnérabilités. Il s'agit d'une collecte d'informations qui, dans la plupart des cas, précède un autre type d'attaque.

Les attaques de reconnaissance peuvent avoir les formes suivantes :

- **Demandes d'informations Internet :** Des assaillants externes peuvent utiliser des outils Internet, comme les utilitaires nslookup et whois, pour découvrir facilement les adresses IP.
- **Balayages ping :** Une fois ces adresses IP connues, l'assaillant peut lancer des requêtes ping vers les adresses publiquement accessibles pour déterminer celles qui sont actives.
- **Balayages de ports :** Lorsque les adresses IP actives sont identifiées, l'intrus se sert d'un outil de balayage des ports pour détecter les services réseau ou les ports ouverts sur chaque adresse IP active.

1.5.3.2 Accès

L'accès au système est la possibilité pour un intru d'accéder à un périphérique pour lequel il ne dispose pas d'un compte ou d'un mot de passe. On peut citer :

- **Attaques d'accès :** Les attaques d'accès exploitent des vulnérabilités connues pour accéder à toute information sensible.
- **Attaques de mot de passe :** Les attaques de mot de passe peuvent se faire à l'aide d'un analyseur de paquets pour glaner les comptes et les mots de passe utilisateur transmis en clair. Les attaques de mot de passe se rapportent en général aux tentatives de connexion répétées à une ressource partagée, afin d'identifier un compte utilisateur, un mot de passe ou les deux. Ces tentatives répétées s'appellent attaques par dictionnaire ou attaques en force.

– **Exploitation de la confiance :**
  Une attaque par exploitation de la confiance a pour but de compromettre un hôte de confiance et de l'utiliser ensuite pour lancer des attaques sur d'autres hôtes du réseau.

1.5.3.3 Déni de service

L'attaque par déni de service (DoS) est la forme d'attaque la plus répandue et aussi la plus difficile à éliminer. Elle empêche l'utilisation d'un service par les personnes autorisées en épuisant les ressources du système. Voici quelques exemples des menaces DoS les plus courantes :

– **Ping fatal :** Elle profite des vulnérabilités des anciens systèmes d'exploitation. Le pirate modifiait la partie IP de l'en-tête d'un paquet ping pour indiquer une quantité de données supérieure à la quantité réelle du paquet afin de bloquer un ordinateur cible d'ancienne génération. La plupart des réseaux ne sont actuellement plus vulnérables à ce type d'attaque.
– **Bombes de courriels :** Programmes qui envoient du courriel en masse à des destinataires particuliers, à des listes ou des domaines, monopolisant ainsi les services de messagerie.
– **Applet hostile :** Ces attaques sont des programmes Java, JavaScript ou ActiveX qui détruisent ou immobilisent les ressources d'un ordinateur.

1.5.3.4 Vers, virus et chevaux de Troie

Des logiciels malveillants peuvent être installés sur un ordinateur hôte dans le but d'endommager ou d'altérer un système, de se reproduire ou d'empêcher l'accès à des réseaux, systèmes ou services.

– **Un ver :** Il exécute un code et installe des copies de lui-même dans la mémoire de l'ordinateur infecté, ce qui infecte par la suite d'autres ordinateurs hôtes.
– **Un virus :** C'est un logiciel malveillant intégré à un autre programme afin d'exécuter des fonctions particulières indésirables sur l'ordinateur de l'utilisateur.
– **Un cheval de Troie :**Il se distingue uniquement des vers et des virus par le fait qu'il a été entièrement conçu pour ressembler à une application normale, alors qu'il s'agit d'un instrument d'attaque.

1.4 La sécurité informatique

La sécurité informatique est l'ensemble des moyens mis en oeuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Elle s'occupe de la prévention d'actions non autorisées par les utilisateurs d'un système informatique.

1.4.1 Objectif de la sécurité informatique

La sécurité informatique vise généralement cinq principaux objectifs :

- **La confidentialité :**
  Elle consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs autorisés.
- **L'authentification :**
  Elle consiste à assurer l'identité d'une entité avant de lui donner accès à une ressource.
- **L'intégrité :**
  Vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées (De manière fortuite ou intentionnelle).
- **La non-répudiation :**
  La non-répudiation de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction.
- **La disponibilité :**
  L'objectif de la disponibilité est de garantir l'accès à un service ou à des ressources.

1.4.2 Les éléments à protéger

Les réseaux sont constitués de divers équipements d'une part et de liens filaires ou non filaires qui les relient d'autre part. Toute ou une partie de ces équipements peuvent être gérés par des programmes adaptés et plusieurs sortes de données y sont stockées. Certaines d'entre elles peuvent être l'objet de transferts selon des protocoles appelés protocoles de réseaux [11]. Les éléments principaux à protéger au sein d'un réseau sont :

1.6.3.1 Le matériel

Mis à part les ordinateurs que les réseaux relient, le matériel inclut aussi, les équipements intermédiaires comme les répéteurs, commutateurs, routeurs, serveurs, etc. La limitation de l'accès à ces matériels (enfouissement, salles spécialisées, équipes de gardiennage et de sécurité), participe à la sécurité de l'ensemble.

1.6.3.2 Les programmes

Les programmes incluent les systèmes d'exploitation y compris les pilotes de périphériques ainsi que les logiciels, programmés gérant les différents mécanismes de réseaux. Les services réseau permettent une meilleur gestion, on peut citer DHCP (*Dynamic Host Configuration Protocol*) qui attribue automatiquement des adresses IP aux machines, DNS (*Domain Name Server*) qui facilite la recherche du domaine auquel appartient une page web.

1.6.3.3 Les données

Les données sont essentiellement de deux sortes : celles qui servent au fonctionnement du réseau comme les tables de routage, les fichiers relatifs aux droits d'accès, etc. Et celles qui ne relèvent pas du fonctionnement du réseau comme les documents et les archives, ces derniers organisé de moyens techniques, administratifs, et humains permettant de les gérer s'appelle un système d'information (SI).

1.4.3 Mise en oeuvre de la sécurité informatique

Les principaux dipositifs permettant de sécuriser un réseau sont :

1.6.4.1 Les outils de protection de base

Il est impératif qu'au sein d'une entreprise, chaque poste de travail et/ou le serveur soit protégé par un antivirus et un pare-feu (*firewall*) mis à jour [12].

– **L'antivirus :**

Il s'agit d'un logiciel permettant de protéger son poste informatique ou son système contre les infections informatiques (virus, vers). Ce logiciel surveille et analyse régulièrement l'ensemble des fichiers puis filtre les contenus suspects. Une fois l'anomalie détectée, il en informe l'utilisateur et la détruit.

La plupart des logiciels antivirus intègrent également une protection antispam qui permet d'analyser l'ensemble des messages entrants avant qu'ils ne soient délivrés au destinataire.

– **Le pare-feu :**

Un pare-feu désigne un dispositif capable de bloquer les virus et d'éviter la fuite d'informations vers l'extérieur. Lorsque des données sont transmises entre ordinateurs via Internet, les informations entrent et sortent par des portes virtuelles appelées « ports ».

Ces « entrées »sont autant de possibilités de pénétrer dans le système d'information de l'entreprise. Si bien qu'en l'absence de pare-feu, des pirates informatiques ont tout loisir d'infecter ou de détruire les données d'un ordinateur ou de récupérer des informations.

1.6.4.2 Les outils cryptographique

La cryptographie demeure la technique indispensable pour, d'une part, protéger la confidentialité des informations transmises sur les réseaux ou stockées dans les serveurs de données et pour, d'autre part, assurer l'intégrité d'un document ou pour prouver l'authenticité d'une opération ou d'une transaction. Elle applique des concepts mathématiques et met en place des paradigmes informatiques afin de résister aux attaques potentielles d'assaillants ou de prouver, de manière quasi sûre, qu'une procédure est incorruptible [15] [13] [17].

a. **Algorithme de chiffrement**

Il existe deux grandes familles d'algorithmes de chiffrement, ceux à clès symétriques et asymétriques.

– **Algorithme de chiffrement symétrique**

Le chiffrement symétrique consiste à utiliser la même clé pour le chiffrement que pour le déchiffrement. Il est donc nécessaire que les deux interlocuteurs se soient mis d'accord sur une clé privée, où ils doivent utiliser un canal sécurisé pour l'échanger. Parmi ces algorithmes on trouve DES, AES, RC4, etc.

– **Algorithme de chiffrement asymétrique**

Pour résoudre le problème de l'échange de la clé secrète, un nouveau type de cryptographie a été inventé, c'est la cryptographie asymétrique. Elle désigne une méthode cryp-

tographique faisant intervenir une paire de clés asymétriques : une clé publique et une clé privée. Elle utilise cette paire de clés pour le chiffrement et le déchiffrement. La clé publique est rendue publique est distribué librement, la clé privée n'est jamais distribuée et doit être garder secrète. On peut citer RSA, AL Gamel, etc

Il y a des protections que le chiffrement ne peut pas garantir, par exemple qu'un texte ne soit pas modifié. Pour ce faire on protège l'intégrité des informations grâce à des algorithmes cryptographiques de hachage.

b. **La fonction de hachage**

Une fonction de hachage est une fonction à sens unique qui transforme un message de taille quelconque en un résumé court de taille fixe, appelé le condensé de message, l'empreinte du message, le résumé du message ou encore le message haché. Cependant elle doit en pratique vérifier les conditions suivantes :

- Résistance à la détermination d'une pré-image, ce qui signifie qu'il doit être impossible en pratique, à partir d'un résumé m, de retrouver un message M ayant ce résumé m = h(M).
- Résistance aux collisions, ce qui signifie qu'il est impossible en pratique de construire deux messages M1 et M2 ayant le même résumé : h(M1) = h(M2).

c. **Signature numérique**

La signature numérique consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache, lorsque la signature numérique est crée, l'identité du signataire assurée et l'intégrité de l'acte garantie [21].

En d'autre terme la signature numérique permet de générer un condensé à partir d'un message en clair et le chiffrer en utilisant la clé privée de l'émetteur, ce dernier envoie le message en clair avec la signature numérique. Elle permet donc de reproduire sur Internet l'environnement de confiance des échanges physiques (courriers traditionnels en particulier), puisqu'il devient impossible de répudier un document électronique (un bon de commande, un ordre de paiement, ect).

1.6.4.3 L'authentification

La majorité des systèmes informatiques actuels fournissent aux utilisateurs d'un réseau des services, lesquels doivent pouvoir s'assurer de leurs identité. Ce processus d'identification est appelé « Authentification »est la vérification d'informations relatives à une personne ou à un processus informatique. L'authentification compléte le processus d'idetification dans le sens ou l'authentification permet de prouver une identité déclarée.

L'authentification peut se faire de multiple manières, et notamment par la vérification de [34] :

- **Ce que je sais :** un mot de passe ou nom d'utilisateur ;
- **ce que je sais faire :** une signature manuscrite sur écran tactile ou digitale ;
- **ce que je suis :** une caractéristique physique comme empreinte digitale ;
- **ce que je possède :** une carte à puce, certificat électronique ou clé USB par exemple.

Le choix de telle ou telle technique dépend en grande partie de l'usage que l'on souhaite en faire : Authentification d'un utilisateur qui se connecte à distance, authentification d'un administrateur au système, authentification de l'expéditeur d'un email, etc.

La combinaison de plusieurs de ces facteurs permet de renforcer le processus d'authentification, on parle alors d'authentification forte.

a. **Méthodes courantes d'authentification :**
Pour être authentifié, il faut pouvoir fournir une preuve de son identité, cette preuve peut prendre plusieurs formes mais, elle est basée sur la propriété d'unicité liée à l'utilisateur. pour cela il existe de nombreuses méthodes dont les principales sont décrites ci-dessous [35] :

- **Mot de passe :** Actuellement, tout utilisateur d'une machine en réseau doit gérer un ou plusieurs mots de passe qui sont des secrets partagés entre l'utilisateur et le système auquel il s'authentifie, pris dans leur ensemble sont le moyen d'authentification le plus répondu à ce jour. On distingue deux catégories :
  1. Les mots de passe statiques qui restent identiques pour plusieurs connexions sur un même compte ;
  2. Les mots de passe dynamiques (unique), l'avantage de l'authentification par mot de passe unique est que ce dernier transitant sur le réseau ne fonctionne qu'une fois ce qui rend inutile l'écoute et la récupération

  .
- **Certificats à clés publiques :** La preuve utilisé pour s'assurer qu'une clé appartient à un utilisateur. L'authentification s'appuie sur l'utilisation de techniques cryptographique telles que la fonction de hachage, les algorithmes de cryptographie et la signature numérique.

- **La biométrie :** Cette technique se base sur un trait unique de la morphologie humaine, on trouve l'empreinte digitale, iris de l'oeil, empreinte vocale, etc. Mais ces technologies restent difficiles à déployer.

- **La carte à puce :** Elle a connu un développement très important par sa facilité de fabrication et sa difficulté d'être copiée.

b. **Avantages et inconvénients des différentes techniques d'authentification :**

Le tableau suivant recense les principaux avantages et inconvénients de chacune des techniques d'authentification décrite précédemment :

	Avantages	**Inconvénients**
Mot de passe statique	-Peu couteux -facile à metttre en oeuvre -facile à utiliser	-oublie de mot de passe -peu robuste -vol de mot de passe.
Mot de passe dynamique généré par un logiciel	-Robustesse du mot de passe l'utilisateur	-peu de confort d'utilisation -Protection de l'utilisation de logiciel par une persone non autorisé
Certificat X.509	-Multi-usage -Robustesse de la méthode d'authentification	-Vol ou utilisation frauduleuse
Biométrie	-Pas d'oublie ou de vol possible	-Technologie encore immature -Facilement falsifiable

TABLE 1.1 – Les principaux avantages et inconvénients des techniques d'authentification [50].

La qualité d'une méthode d'authentification ne se mesure pas uniquement par ses avantages et inconvénients généraux ou à sa robustesse théorique face aux attaques mais avant tout à sa capacité à répondre aux besoins de sécurité.

De nombreuses problématiques sécuritaires se posent dans les réseaux modernes, de manière à restreindre au maximum les risques pouvant affecter le système d'information. Une solution globale s'occuperait d'assurer les éléments de base de la sécurité à savoir l'authentification des terminaux, la confidentialité et l'intégrité de leur flux, l'absence de rejeux et la non-répudiation. De tels éléments sont pris en charge par des architectures AAA(*Authentication, Authorization, Accounting*).

1.5 Les politiques AAA

Pour atteindre ces objectifs de sécurité, il est nécessaire de mettre en oeuvre une politique de sécurité, applicable à l'ensemble des entités à l'intérieur d'un domaine géographique ou fonctionnel. La politique exhibe, dans sa rédaction sous forme de règles, des sujets et des objets et précise les activités et opérations autorisées et interdites [17].

Selon la RFC 2196 [14] qui porte le nom « *Site Security Handbook* » : « Une politique de sécurité est une déclaration formelle des règles qui doivent être respectées par des personnes qui ont accès aux ressources technologique et aux données vitales d'une entreprise ».

1.5.1 Définition de AAA

Le terme AAA est apparu au milieu des années 1990 suite à l'effort de standardisation né de la coopération entre l'IEEE et l'IETF, à travers son groupe de travail AAA (*AAA Working Group*), pour développer des applications AAA [18].

Par AAA (*Authentication, Authorization, Accounting*), on désigne un système de mécanismes, protocoles et architectures dont le but est la comptabilité. Mais pour avoir une valeur, la comptabilité doit pouvoir s'appuyer sur des éléments factuels irrécusables, c'est a ce moment qu'intervient l'authentification et l'autorisation. La signification du terme AAA est la suivante :

1.7.2.1 Authentification(Authentication)

L'authentification est le processus par lequel une entité prouve son identité. Ceci est généralement réalisé en utilisant un secret partagé entre l'utilisateur et le serveur tels une combinaison Nom/Mot de passe, une clé, une reconnaissance biométrique, etc.

1.7.2.2 Autorisation(Authorization)

Cela a pour but de déterminer si l'entité authentifiée est autorisée ou non à accèder et/ou utiliser les ressources ou les services demandés.

1.7.2.3 Comptabilité(Accounting)

Pour cette dernière notion, on s'intéresse à ce que fait l'utilisateur des ressources auxquelles il a accès. Le choix de baptiser cette fonction « comptabilité »n'est pas un hasard, les opérateurs de services Internet facturant fréquemment leurs utilisateurs en fonction de ce qu'ils font.

1.5.2 Architecture AAA

Une architecture AAA est généralement une architecture Client-Serveur qui rend réalisable l'ensemble de ces fonctionnalités à travers de multiples technologies de réseaux et de plateformes.

Les serveurs AAA permettent de gérer les utilisateurs et les clients AAA dans des domaines en se basant sur des outils, politiques et données nécessaires à l'authentification et l'autorisation des utilisateurs et à la comptabilisation des ressources consommées. Les clients AAA sont installés sur des routeurs ou des serveurs d'accès au réseau (NAS-*Network Access Server*).

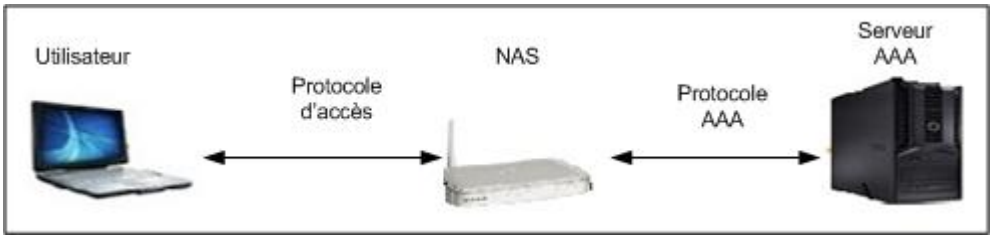

FIGURE 1.1 – Architecture AAA simple

Dans une architecture AAA (figure 1.4), lorsqu'un abonné accède au réseau, il est authentifié et autorisé par le serveur AAA via le NAS. Ce dernier collecte les informations sur les consommations de l'abonné et les envoie au serveur AAA. Les communications entre le NAS et le serveur AAA ont lieu grâce à un protocole AAA, celles entre l'équipement de l'utilisateur et le NAS grâce un protocole d'accès comme PPP (*Point-to-Point Protocol*).

1.5.3 Protocole AAA

Parmi les protocoles AAA connus nous citons :

1.7.4.1 RADIUS

Le protocole RADIUS (*Remote Authentication Dial In User Services*), il fût normalisé par l'IETF sous la forme de RFC 2865 [**?**]. Il s'agit d'un protocole AAA mis au point initialement par Livingston. Il fonctionne selon une architecture de type client/serveur chargé de définir les accès d'utilisateurs distants à un réseau. Il utilise le protocole UDP (*User Datagramme Protocol*) comme protocole de transport, il permet aussi la communication entre un client RADIUS (Client AAA) et un serveur RADIUS(Serveur AAA) qui traite les demandes du client.

1.7.4.2 Diameter

Pendant longtemps le seul protocol standard d'authentification entre un NAS et le serveur était RADIUS. Diameter, normalisé dans la RFC 6733 *Diameter Base Protocol* [20] (qui fait suite à la RFC 3588), visait à le remplacer est bien plus riches en fonctions. Diameter est défini à travers un protocole de base est un ensembles d'applications. Ce protocole utilise une architecture peer to peer pluôt qu'un schéma client/serveur, il transporte les données à l'aide de protocole orienté connexion tels que TCP (*Transport Control Protocol*) et SCTP (*Stream Control Transmission Protocol*).

1.7.4.3 Kerberos

Kerberos est différent de RADIUS et de Diameter dans la mesure où il permet de construire une communication sécurisée avec une application par la mise en place d'une clé de session. Standardisé par l'IETF, Kerberos se décompose en trois sous protocoles :

- **Service d'authentification :** permet d'authentifier les clients ;
- **Le service de délivrement de TGS :** permet de fournir l'authentification auprès des serveurs d'application ;
- **Service d'authentification Client / Serveur :** qui permet d'établir une communication sécurisée entre le client et le serveur d'applications.

L'authentification Kerberos repose sur le principe que chaque client d'un réseau donné doit s'identifier sur un serveur global. Le client doit présenter au serveur un ticket d'authentification que lui a préalablement fourni ce dernier, tout client muni de ce ticket est considéré comme authentifié [24].

1.7.4.4 TACACS+

TACACS+ (*Terminal Access Controller Access Control Plus*) est la dernière version du protocole TACACS développé à l'origine par BBN, puis repris par Cisco. Il utilise TCP pour son transport contrairement à TACACS qui était basé sur l'UDP. Il gère séparément les trois fonctions AAA, contrairement à d'autres protocoles d'authentification [23] [24].

1.6 Conclusion

Les réseaux sans fil présente des intérêts : leurs simplicité de déploiement, mobilité des employés, interopérabilités des équipements, faible coût en comparaison de l'installation et la maintenance d'un réseau câblé. Il faut le considérer a priori comme un réseau ouvert au public mais également comme une bulle de risque, en conséquence toute connexion non autorisée peut remettre en cause la sécurité de l'ensemble du système d'information. Malgré des problèmes de sécurité, les réseaux sans fil continuent et continueront probablement à se développer. Il est donc important de bien connaître les problèmes liés à la mise en place de ce type de réseaux afin d'en limiter les effets néfastes.

CHAPITRE 2

ETUDE DES ARCHITECTURES DE SÉCURITÉ DES RÉSEAUX SANS FIL NOTAMMENT LES DIFFÉRENTES TECHNIQUES EAP ET LEURS IMPLICATIONS

2.1 Introduction

Installer un réseau sans fil sans le sécuriser peut permettre à des personnes non autorisées d'écouter, de modifier et d'accéder à ce réseau. Il est donc indispensable de sécuriser les réseaux sans fil dès leur installation. Il est possible de sécuriser son réseau de façon plus ou moins forte selon les objectifs de sécurité et les ressources que l'on y accorde.

Dans ce chapitre, nous allons présenter d'une part, les réseaux sans fil ainsi que les solutions de bases intégrées à l'origine dans la norme 802.11 comme la délimitation des débordements, le filtrage par adresse MAC et le WEP, etc. Et d'autre part, les nouvelles solutions de sécurité qui se basent sur l'apparition du WPA pour remplacer le WEP après sa chute, WPA étant une norme intermédiaire en attendant la finition et la ratification de la norme IEEE 802.11i donc du WPA2. Enfin nous citons une solution plus robuste qui se base sur la norme IEEE 802.1x qui définit une encapsulation d'EAP, en incluant ces principales techniques d'authentifications.

2.2 Les réseaux sans fil

Un réseau sans fil (en anglais *wireless network*) est, comme son nom l'indique, un réseau dans lequel au moins deux terminaux peuvent communiquer sans liaison filaire. Grâce aux réseaux sans fil, un utilisateur a la possibilité de rester connecté tout en se déplaçant dans un périmètre géographique plus ou moins étendu, c'est la raison pour laquelle on entend parfois parler de « mobilité ».

2.2.1 Les différents types de réseaux sans fil

Comme pour les réseaux filaires basé sur la norme IEEE 802.3 [7](ISO/IEC 8802-3), nous parlerons de différents types de réseaux sans fil selon leur domaine de couverture : les réseaux personnels WPAN (*Wireless Personal Area Networks*), les réseaux locaux WLAN (*Wireless Local Area Networks*), les réseaux métropolitains WMAN (*Wireless Metropolitan Area Networks*) et les réseaux étendus WWAN (*Wireless Wide Area Networks*) [1][2].

1.3.1.1 WPAN

Les réseaux sans fil personnels sont des réseaux sans fil à très faible portée (quelques dizaines de mètres) qui comme leur nom l'indique, sont des réseaux à usage personnel. Ils sont généralement utilisés pour relier des équipements informatiques entre eux : par exemple pour relier une imprimante ou un PDA (*Personal Digital Assistant*) à un ordinateur de bureau. Ils sont déjà présents sous différents noms par exemple le Bluetooth (IEEE 802.15.1 [4]), cette technologie est très peu gourmande en énergie ce qui la rend particulièrement intéressante pour être intégrée dans de petits équipements autonomes sans fil comme les PDA.

1.3.1.2 WLAN

Les réseaux locaux sans fil sont généralement utilisés à l'intérieur d'entreprises, d'universités mais également chez les particuliers. Ces réseaux sont principalement basés sur la technologie IEEE 802.11 [6] (ISO/IEC 8802-11) soutenue par le WECA (*Wireless Ethernet Compatibility Alliance*). Il existe plusieurs technologies concurrentes parmi elles :

– **Le WiFi**

Les réseaux WiFi proviennent de la norme IEEE 802.11 [6] (ISO/IEC 8802-11), qui définit une architecture cellulaire. Un groupe de terminaux munis d'une carte d'interface réseau 802.11 s'associent pour établir des communications directes.

En fait, la norme IEEE 802.11 est la norme initiale à partir de laquelle un certain nombre de normes dérivées ont été créées afin de répondre à des objectifs d'interopérabilité ou de sécurité. Les normes dérivées les plus connues aujourd'hui sont les normes IEEE 802.11a, IEEE 802.11b, IEEE 802.11g, IEEE 802.11i, 802.11n, etc.

– **HiperLAN2 (High Performance Radio LAN 2.0)**

C'est une norme européenne élaborée par l'ETSI (*European Telecommunications Standards Institute*), HiperLan2 s'avère très supérieur au WiFi du fait de sa gestion avancée de la QoS (*Quality of Service*). La technologie intègre en effet une gestion de la qualité de service au niveau radio, ce qui la rend idéale pour des applications comme la diffusion vidéo sans fil.

1.3.1.3 WMAN

Les réseaux métropolitains sans fil également appelés boucle locale radio (BLR) est une technologie sans fil capable de relier les opérateurs à leurs clients grâce aux ondes radio sur des distances de plusieurs kilomètres. Les réseaux basés sur la technologie IEEE 802.16 [5] ont une portée de l'ordre de quelques dizaines de kilomètres plus connue sous le nom commercial « WiMAX ».

1.3.1.4 WWAN

Les réseaux sans fil étendus regroupent notamment les différents réseaux téléphoniques de première et deuxième génération mais également les réseaux satellitaires. Les réseaux cellulaires téléphoniques reposent sur des technologies comme GSM (*Global System for Mobile Communication*), GPRS (*General Packet Radio Service*).

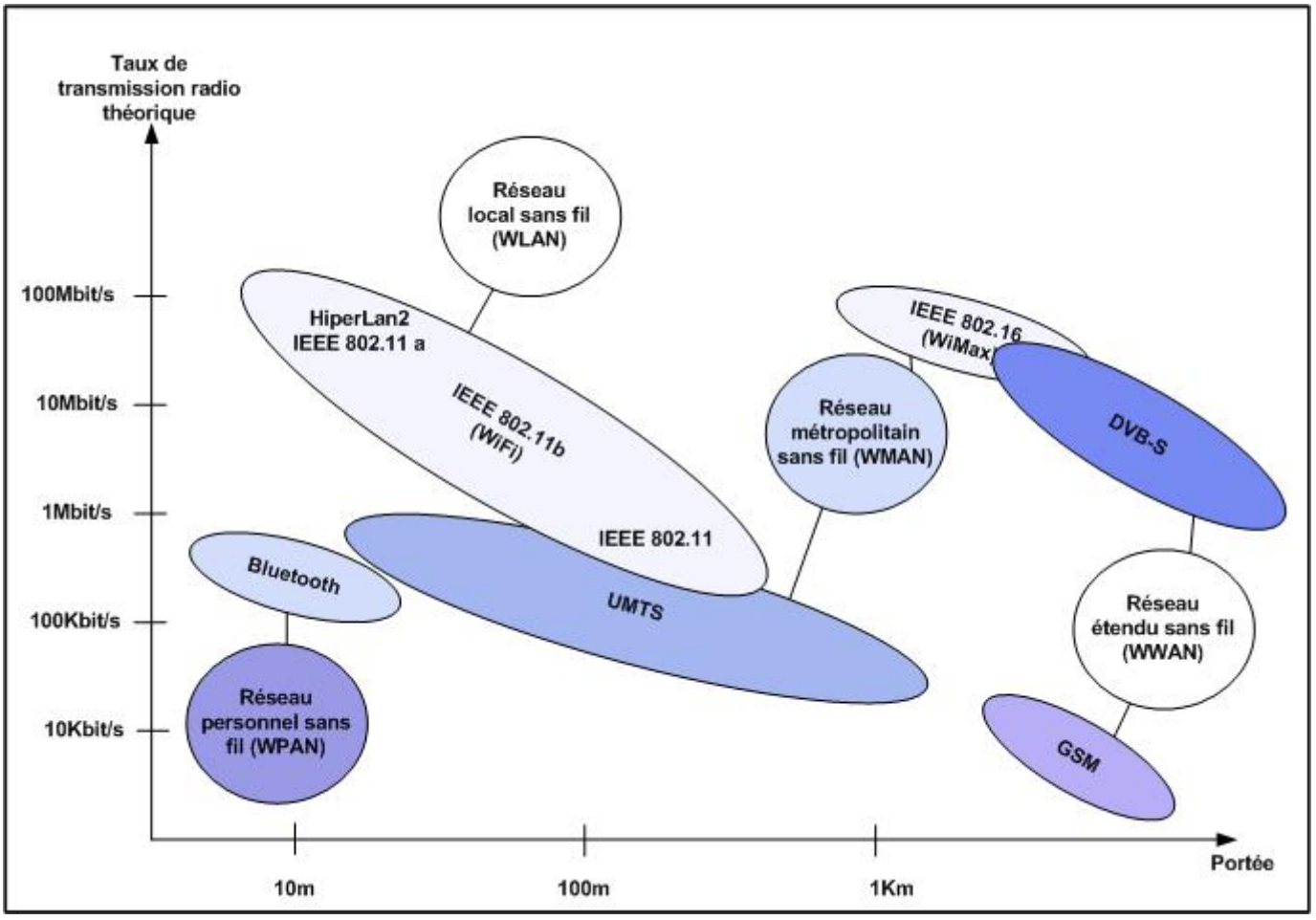

FIGURE 2.1 – Les types de réseaux sans fil [2].

La figure 1.1 présente les différents types des réseaux sans fil. Dans la suite de ce rapport nous nous intéresserons uniquement au réseau local sans fil (WLAN).

2.2.2 Les contraintes liées aux réseaux sans fil

La propagation du signal radio est un élément clé de la qualité d'une transmission mais le nombre de fréquences et de canaux disponibles pour communiquer est limité. Ainsi, lorsque deux noeuds émettent simultanément sur des bandes de fréquences ou des canaux proches, des interférences seront ressenties sur les deux communications [8].

Le fait que le signal s'atténue avec la distance pose un autre problème : le signal émis par un noeud est beaucoup plus fort que n'importe quel signal reçu.

Il est difficile de maîtriser proprement un signal, ou des ondes électromagnétiques. Tous les noeuds peuvent recevoir les paquets émis par leurs voisins même si ceux-ci ne leurs sont pas desti-

nés et ceci de manière beaucoup plus simple que dans un réseau filaire car les communications se déroulent dans l'air, ce qui pose un problème évident de sécurité.

2.3 Présentation du WiFi

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

2.3.1 Utilisation du WiFi

De nos jours les réseaux sans fil se développent très rapidement [10] :

- Pour des réseaux temporaires (salons, conférences, etc) ;
- pour des points d'accès haut débit dans les lieux publics (aéroports, gares, etc) connus sous le nom de hotspot ou des lieux privés accueillant du public (hôtel, restaurant, etc) ;
- dans de nombreux organismes attirés par la souplesse des réseaux sans fil.

2.3.2 Les modes de fonctionnement du WiFi

Le standard 802.11 définit deux modes opératoires le mode infrastructure et Ad Hoc [16].

1.4.2.1 Le mode infrastructure

Les réseaux sans fil avec infrastructure sont également appelés réseaux cellulaires. Ces réseaux se composent de deux types de terminaux : les stations de base ou points d'accès (APs) et les terminaux mobiles.

Comme le montre la figure 1.2, chaque périphérique est relié au réseau via un AP. Un réseau de ce type s'appelle *Basic Service Set* (BSS) et couvre un espace qu'on appelle une cellule ou *Basic Area Network* (BSA). Les terminaux mobiles se déplacent librement mais ne communiquent jamais directement les uns avec les autres. Toutes les communications se font systématiquement vers le point d'accès le plus proche qui se charge ensuite de les relayer à la destination.

Plusieurs APs peuvent être déployés pour atteindre une large couverture WiFi, ils peuvent être reliés par un système de distribution (*Distribution System*). L'ensemble est nommée ESS (Ensemble de Service étendus).

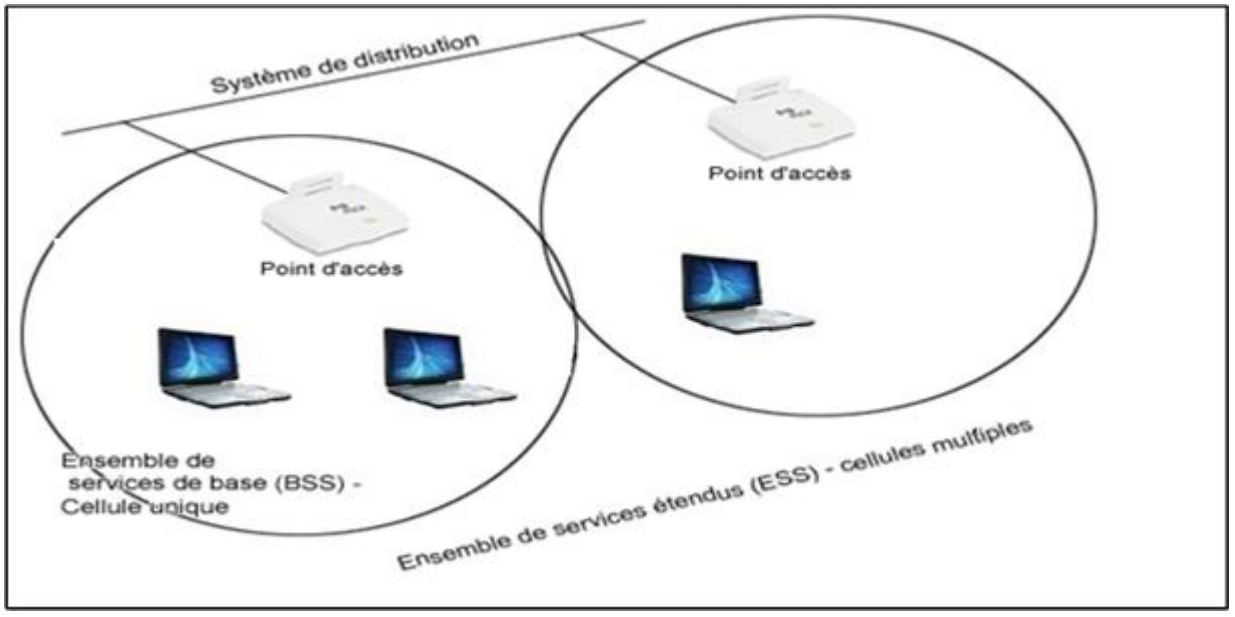

FIGURE 2.2 – Le mode infrastructure

1.4.2.2 Le mode Ad Hoc

Contrairement aux réseaux cellulaires qui sont organisés autour de points d'accès, les réseaux Ad-Hoc sont des réseaux distribués et spontanés se composant uniquement de terminaux mobiles. Dans ce type de réseau, présenté sur la figure 1.3, chaque périphérique communique directement avec les périphériques situés à sa portée, le réseau ainsi constitué s'appelle *Independent Basic Service Set* (IBSS).

Le groupe de travail MANET (*Mobile Ad-Hoc NETworks*) de l'IETF (*Internet Engineering Task Force*) a formalisé l'ensemble de ces caractéristiques dans les RFC(*Request For Comment*) numéro 2501 [9].

Le mode infrastructure est de plus en plus utilisé dans les entreprises et les universités comme dernier bond d'un réseau d'accès à l'Internet ou pour contôler l'accès à leurs réseaux.

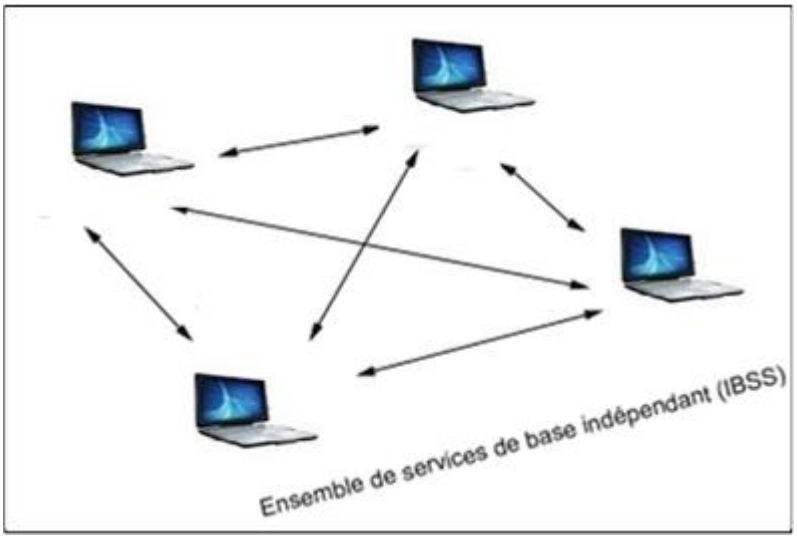

FIGURE 2.3 – Le mode Ah Hoc

2.3.3 Les avantages du WiFi

Comme les autres réseaux sans fils, le WiFi possède plusieurs avantages :

- **Mobilité**
  Les utilisateurs sont généralement satisfaits des libertés offertes par un réseau sans fil.
- **Facilité et souplesse**
  Un réseau sans fil peut être utilisé dans des endroits temporaires, couvrir des zones difficiles d'accès aux câbles, et relier des bâtiments distants.
- **Faible coût**
  Si leur installation est parfois un peu plus couteuse qu'un réseau filaire, les réseaux sans fil ont des coûts de maintenance très réduits, sur le moyen terme, l'investissement est facilement rentabilisé.
- **Evolutivité**
  Les réseaux sans fil peuvent être dimensionnés au plus juste et suivre simplement l'évolution des besoins.

De plus, le WiFi est intéropérable avec les réseaux filaires existants et garantit une grande souplesse sur la topologie du réseau.

2.4 Sécurité du 802.11

La norme 802.11 intégrait à l'origine un ensemble de solutions de sécurité ne sont certes pas parfaites, mais on le mérite d'exister, on peut citer [2] [8] [25] :

2.4.1 Limiter les débordements

Une première mesure de protection contre les attaques du réseau sans fil consiste à s'assurer que les ondes radio ne débordent pas sur l'extérieur de l'entreprise. En positionnant correctement les APs pour que le niveau du signal soit très faible à l'extérieur des locaux ou bien en réglant la puissance d'émission du point d'accès au minimum nécessaire.

2.4.2 Masquer le SSID

Pour s'identifier auprès d'un réseau, les utilisateurs d'un réseau sans fil utilisent un identifiant de réseau (SSID). Le premier niveau de sécurité pour un réseau WiFi consiste simplement à configurer les points d'accès pour qu'ils ne diffusent pas leurs SSID. Si quelqu'un ne connaît pas le SSID du réseau, il ne parviendra pas à s'y associer.

Toutefois, cette sécurité est assez faible car il suffit d'être en possession d'un analyseur de paquets pour sniffer les paquets de sondage envoyés par les stations légitimes du réseau pour pouvoir lire le SSID du réseau.

2.4.3 Filtrage par adresse MAC

Un AP vérifie si l'adresse MAC(*Medium Access Control*) de la station qui cherche à s'authentifier se trouve bien dans une liste d'adresses MAC autorisées, si c'est le cas l'utilisateur est autorisé a accèder au réseau, dans le cas échéant AP lui interdit l'accès (figure 2.1). En effet, l'adresse MAC d'une station est présente dans tous les paquets qu'elle émet, et donc en particulier dans la requête d'authentification.

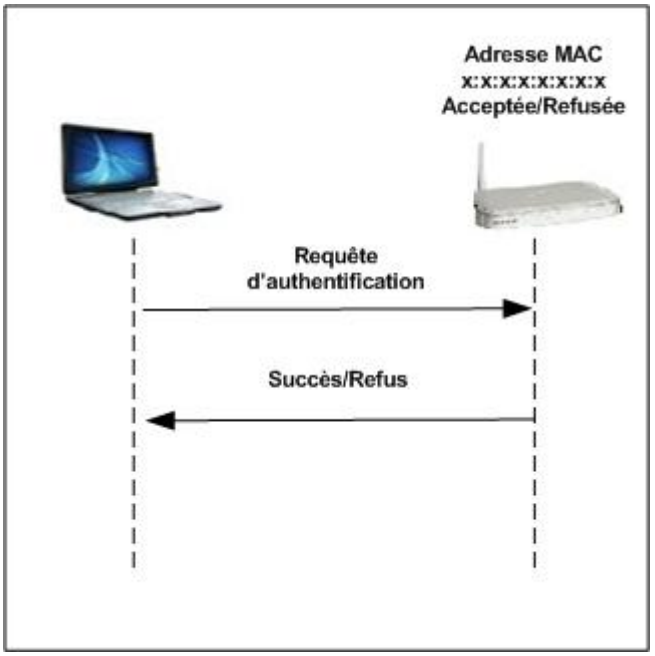

FIGURE 2.4 – Filtrage par adresse MAC.

Malheureusement, il n'est pas très difficile pour un pirate de modifier l'adresse MAC de sa carte WiFi pour se faire passer pour l'un des périphériques.

2.4.4 Les VLAN

Les réseaux locaux virtuels (*Virtual Local Area Network*) permettent la segmentation logique des réseaux dont le but est d'augmenter le niveau de sécurité. Si les APs le permettent, il est bon d'associer le trafic sans fil à un VLAN particulier. Ainsi les groupes contenant des données sensibles sont séparés du reste du réseau, ce qui diminue les risques de violation de confidentialité.

2.4.5 Le cryptage WEP

Le WEP (*Wired Equivalent Privacy*), première solution de sécurité à avoir été intégrée dans le standard 802.11, suit un principe étonnamment simple : chacun doit connaître une même clé WEP, longue de 40 ou 104 bits et cette clé est utilisée par tous pour crypter les communications. Le WEP repose sur un algorithme appelé RC4. Cet algorithme a été conçu par l'un des grands noms de la sécurité informatique : « Ron Rivest ».

2.2.5.1 Principes de fonctionnement du WEP

Le chiffrement en continu RC4 fonctionne comme suit (figure 2.2) : il s'agit de développer une clé secrète et un vecteur d'initialisation (IV) de 24 bits, concaténé à une clé prépartagée, en un flot de clés de longueur arbitraire composé de bits pseudo aléatoires. Le chiffrement s'obtient par l'exécution d'une opération OU exclusive (XOR) entre le flot de clés et le texte en clair, pour produire le cryptogramme. Le déchiffrement se fait par génération du flot de clés identique, basé sur le vecteur d'initialisation et la clé secrète, et par application du OU exclusif sur le cryptogramme, pour récupérer le texte en clair.

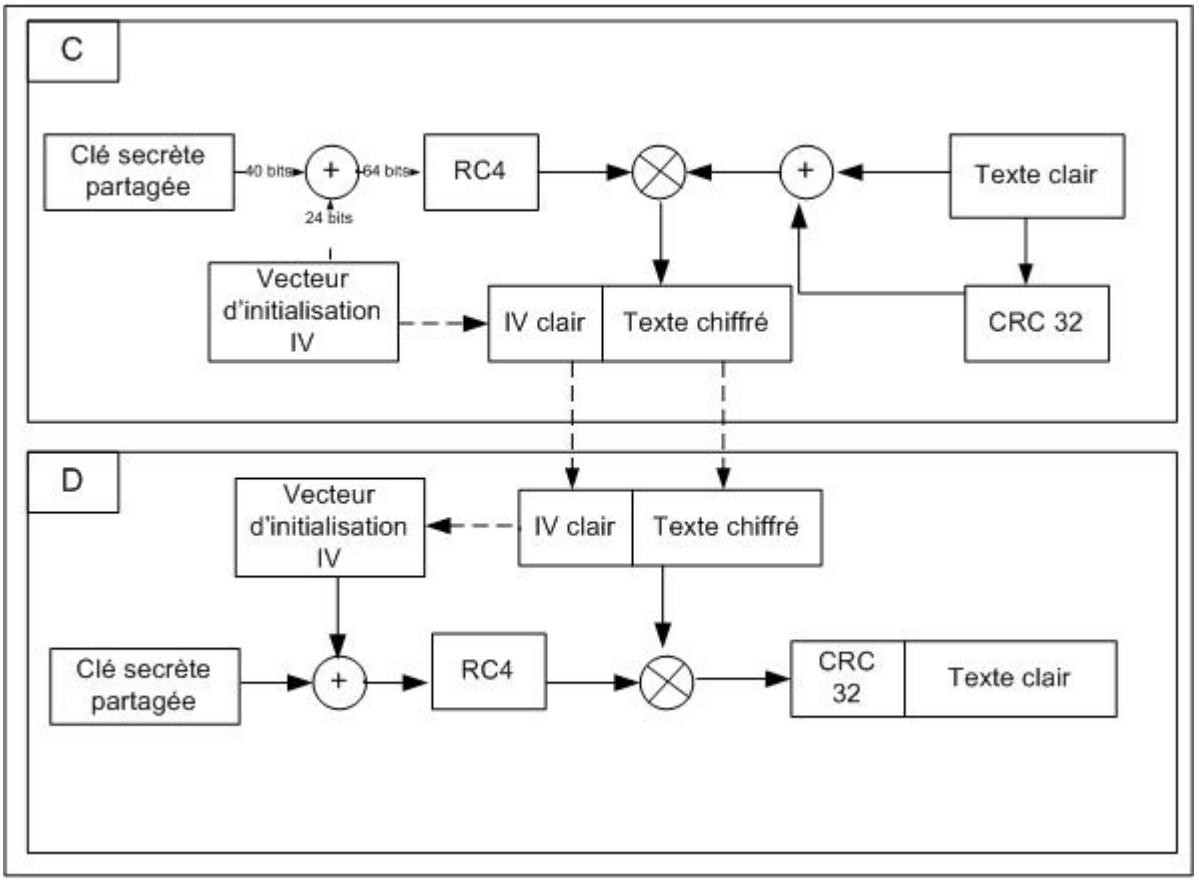

FIGURE 2.5 – Opération de chiffrement et déchiffrement.

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

2.2.5.2 Les faiblesses du WEP

Même au moment de la conception du WEP, l'IEEE savait que cette solution était loin d'être parfaite, mais chacun pensait qu'elle serait suffisante pour satisfaire les besoins des utilisateurs pendant au moins quelques années. Après tout, cette solution reposait sur l'algorithme RC4 qui avait largement fait ses preuves. Ces quelques années devaient être mises à profit pour développer une nouvelle norme de sécurité plus robuste. Malheureusement dès sa publication, le WEP fut décortiqué sous tous les angles par les meilleurs experts en sécurité de la planète, et en moins de trois mois, il fut cassé [2] [12].

Une faille importante du WEP réside dans sa clé. Cette dernière présente deux défauts : elle est constante et le choix des combinaisons est très limité. Les autres faiblesses du WEP sont liées à l'algorithme de chiffrement employé « RC4 ».

Malheureusement, le CRC a été conçu pour lutter contre les erreurs de transmission, mais il ne peut rien contre un pirate : en effet, si un pirate intercepte un paquet et le modifie, il lui suffit de recalculer le CRC avant de laisser ce paquet poursuivre sa route.

2.5 Les nouvelles solutions de sécurité

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

2.5.1 Les VPN

Un VPN (*Virtual Private Network*) est un environnement de communication dans lequel l'accès est contrôlé, afin de permettre des connections entre une communauté d'intérêts seulement. Un VPN est construit avec un partitionnement d'un media de communication commun qui offre des services de façon non exclusive [13] [36]. Les principaux avantages d'un VPN :

- **Sécurité :** Assure des communications sécurisées et chiffrées.
- **Simplicité :** Utilise les circuits de télécommunication classiques.

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

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

– Les solutions VPN du marché peuvent coûter assez cher et sont parfois complexes à mettre en oeuvre ;
– tout le trafic doit passer par un serveur VPN qui ne gère souvent qu'un nombre limité de connexions simultanées ;
– en passant par un tunnel VPN, le débit est parfois réduit et le temps de latence augmenté ;

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

2.5.2 Le WPA

La WiFi Alliance décida alors qu'elle ne voulait pas attendre l'apparution du 802.11i, sa conclusion fut qu'il était nécessaire d'avoir rapidement au moins une version allégée du futur 802.11i. C'est ainsi qu'elle définit la solution *Wireless Protected Access* (WPA) : il s'agit d'une version allégée du standard 802.11i. Il existe deux variantes du WPA : le WPA Personal, également appelé *WPA-PreShared Key* (WPA-PSK) et le WPA Enterprise [10] [26] [**?**].

Le WPA introduit le protocole TKIP (*Temporal Key Integrity Protocol*), qui sera repris par la norme IEEE 802.11i. Ce protocole permet de remédier aux faiblesses du chiffrement WEP en introduisant un chiffrement par paquet ainsi qu'un changement automatique des clés de chiffrement. L'algorithme de chiffrement sous-jacent est toujours le RC4 utilisé avec des clés de 128 bits, mais contrairement au WEP, il est utilisé correctement (au sens cryptographique). Le standard WPA définit deux modes distincts :

2.3.2.1 Le WPA Personal

Le mode « WPA personnel »permet de mettre en oeuvre une infrastructure sécurisée basée sur le WPA sans faire appel à un serveur d'authentification. Le WPA personnel repose sur l'utilisation d'une clé partagée, appelées PSK pour renseignée dans l'AP ainsi que dans les postes clients. Contrairement au WEP, il n'est pas nécessaire de saisir une clé de longueur prédéfinie. En effet, le

WPA permet de saisir une phrase secrète, traduite en PSK par un algorithme de hachage.

Le mode WPA-PSK est vulnérable à des attaques par dictionnaire. Il est donc très important de choisir un secret fort afin de limiter ces risques.

2.3.2.2 Le WPA Enterprise

Le mode entreprise impose l'utilisation d'une infrastructure d'authentification 802.1x basée sur l'utilisation d'un serveur d'authentification, généralement un serveur RADIUS, et d'un contrôleur réseau (le point d'accès). Cette solution est actuellement ce qu'il y a de plus sûr en termes de sécurité d'authentification forte.

2.5.3 Le WPA2

Le WPA2 est la ratification de la norme IEEE 802.11i. Ce standard reprend la grande majorité des principes et protocoles apportés par WPA, avec une différence notoire dans le cas du chiffrement : l'intégration de l'algorithme AES (*Advanced Encryption Standard*). Les protocoles de chiffrement WEP et TKIP sont toujours présents. Deux autres méthodes de chiffrement sont aussi incluses dans IEEE 802.11i en plus [33] :

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

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

2.5.4 Le 802.1x

Le 802.1x est un standard mis en place en juin 2001 par l'IEEE. Ce standard provient du besoin de s'authentifier dès l'accès physique au réseau. Ce besoin s'est particulièrement fait sentir dans le domaine du WiFi, où les clés de cryptage WEP ne sont pas très efficaces, d'où l'idée d'une authentification physique dès les bornes.

Son objectif est de bloquer le flux de données d'un utilisateur non authentifié. C'est-à-dire qu'il permet une authentification lors de l'accès au réseau et donc un contrôle d'accès aux ressources. Le 802.1x s'appuie sur un protocole particulier : l'EAP (*Extensible Authentification Protocol*) décrit par la suite. Le standard s'appuie sur des mécanismes d'authentification existants [27] [28].

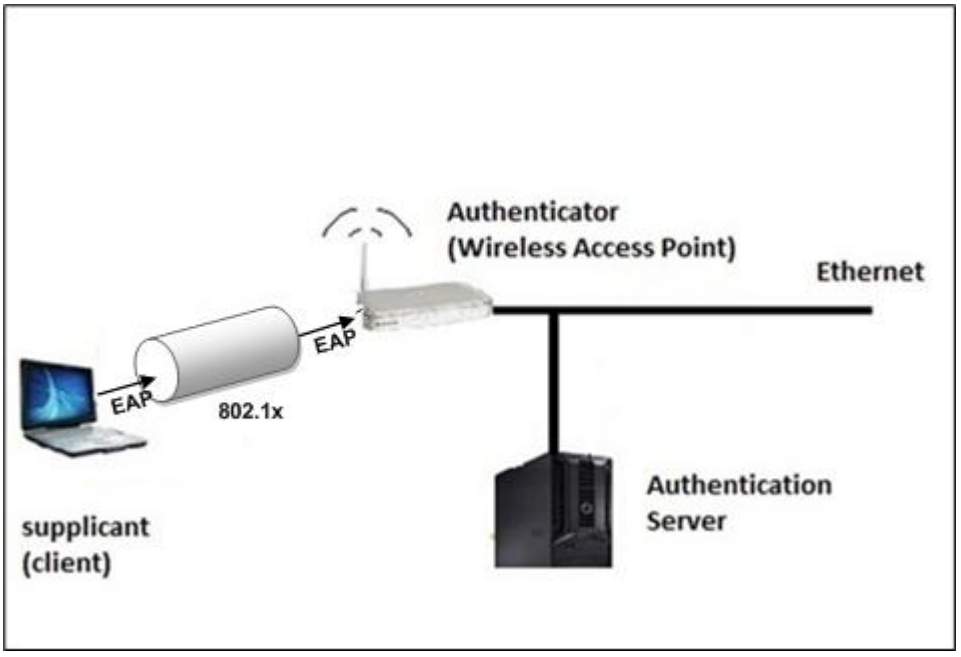

FIGURE 2.6 – Architecture d'authentification 802.1X.

Le 802.1x utilise un modèle qui s'appuie sur trois entités fonctionnelles (figure2.3) :

- **Le système à authentifier (supplicant) :** c'est un poste de travail (terminal informatique) demandant un accès au réseau.
- **Le système authentificateur (authenticator) :** c'est l'unité qui contrôle et fournit la connexion au réseau dans la plupart du temps c'est un AP. Un port contrôlé par cette unité peut avoir deux états : non autorisé ou autorisé. Lorsque le client n'est pas authentifié, le port est dans l'état non autorisé et seulement le trafic nécessité par l'authentification est permis.
- **Le serveur d'authentification (Authentication Server) :** il réalise la procédure d'authentification avec le système d'authentification et valide la demande d'accès. Si la requête d'accès est validée par le serveur, le port est commuté dans l'état autorisé et le client est autorisé à avoir un accès complet au réseau.

2.6 L'EAP

Il est donc temps d'aborder le protocole EAP, il est à la base du 802.1x, sur lequel reposent à leur tour les nouvelles solutions de sécurité du WiFi, le WPA Enterprise et le WPA2 Enterprise. Le protocole d'authentification EAP a été défini par l'IETF.

Le 802.1x est une pyramide de protocoles dont la base est l'EAP. Pour comprendre le 802.1x, il faut donc comprendre l'EAP. Et pour bien comprendre l'EAP, il faut revenir à son origine qui est le Protocole de Point à Point, décrit dans la RFC 1661 [29] « The Point-to-Point Protocol (PPP) »et quelques RFC associées.

2.6.1 Le protocole PPP

2.4.1.1 Présentation du protocole PPP

PPP est un protocole de couche 2 du modèle OSI, il fournit une méthode standard pour transporter les datagrammes multi protocole (Ip, Ipx et Netbeui) sur des liens point à point synchrones ou asynchrones. Il est employé pour créer une connexion à la demande entre un client et un serveur d'accès réseau. Le protocole PPP permet aussi d'authentifier des connexions en utilisant le protocole d'authentification du mot de passe (*Password Authentication Protocol*, PAP) ou le protocole d'authentification à échanges confirmés (*Challenge Handshake Authentication Protocol*, CHAP), ce dernier étant plus efficace. L'utilisation du protocole PPP présente de nombreux avantages, notamment le fait qu'il n'est pas propriétaire [20] [2].

Le protocole PPP s'appuie sur trois composants :

- L'encapsulation des datagrammes grâce à HDLC (*High-Level Data Link Control*).
- Le contrôle de la liaison avec LCP (*Link Control Protocol*).
- Le contrôle de la couche réseau avec NCP (*Network Control Protocol*).

2.4.1.2 L'authentification avec PPP

Le protocole PPP prend en charge deux principales méthodes d'authentification par mot de passe[20] :

– **PAP :** Le PAP est défini dans la RFC 1334 « PPP Authentication Protocols »[30]. Il procure une méthode simple permettant à un noeud distant d'établir son identité à l'aide d'un échange en deux étapes. PAP n'est pas interactif. Il ne présente pas de chiffrement : les nom d'utilisateur et mot de passe sont envoyés en texte clair. S'ils sont acceptés, la connexion est autorisée.

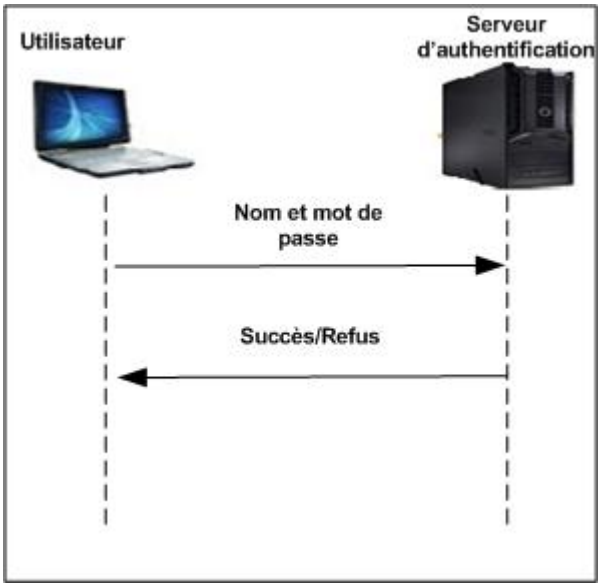

FIGURE 2.7 – L'identification avec le protocole PAP.

Le protocole PAP n'est pas un protocole d'authentification très fort. En effet, les mots de passe sont transmis en clair sur la liaison et PAP n'offre aucune protection contre la lecture répétée des informations ou les attaques répétées par essais et erreurs.

– **CHAP :** Le CHAP est défini dans la RFC 1994 et RFC 2153 qui porte le nom « PPP Challenge Handshake Authentication Protocol (CHAP) »[31]. Le serveur commence par envoyer un « défi » au client, ainsi qu'un compteur qu'il incrémente à chaque fois qu'il lance un défi. Le client doit alors passer le compteur, son mot de passe et le défi au travers d'un algorithme de hachage, habituellement l'algorithme MD5. S'ils sont acceptés, la connexion est autorisée.

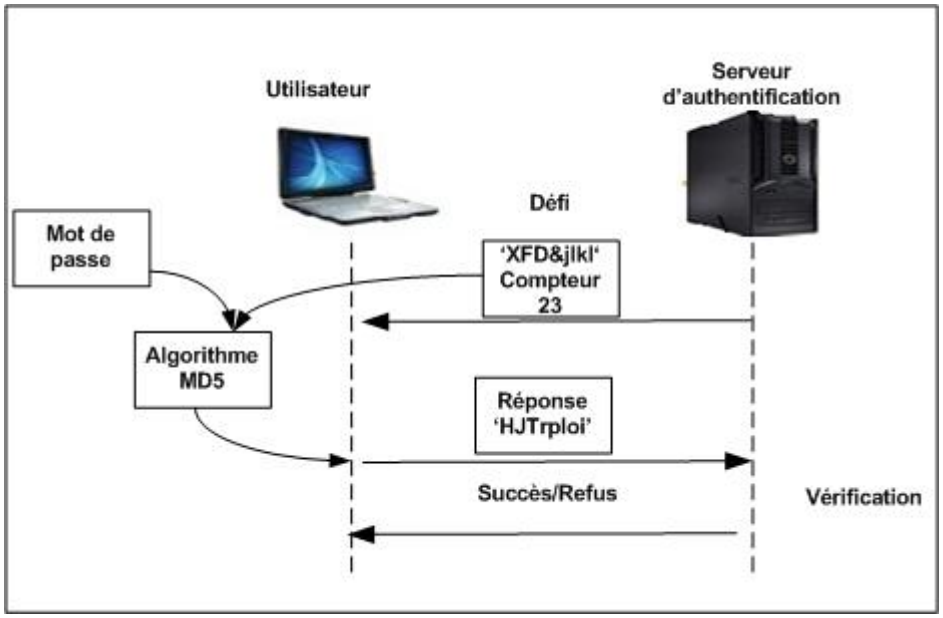

FIGURE 2.8 – L'identification avec le protocole CHAP.

2.4.1.3 Les limites de ces méthodes

Malheureusement, la méthode PAP n'est pas sécurisée et la méthode CHAP est vulnérable face à des attaques hors-ligne de type dictionnaire, il suffit qu'un seul utilisateur légitime ait un mot de passe faible pour que le pirate puisse entrer sur le réseau.

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

2.6.2 Le fonctionnement d'EAP

Le principe d'EAP est très simple, si un utilisateur cherche à accéder au réseau, un contrôleur d'accès lui barrera le chemin jusqu'à ce qu'il s'identifie auprès du serveur d'authentification. Le contrôleur d'accès sert d'intermédiaire pour la communication entre l'utilisateur et le serveur d'authentification. Dans le cadre du WiFi, lorsque le 802.1x est utilisé, chaque AP est un contrôleur d'accès [34].

Le fait que le contrôleur d'accès ne soit qu'un intermédiaire entre l'utilisateur et le serveur est l'un des grands intérêts de l'EAP : en effet, si une nouvelle méthode d'authentification est inventée,

il ne sera pas nécessaire de changer les contrôleurs d'accès, car seuls les utilisateurs et le serveur d'authentification devront être mis à jour [2].

2.6.3 Mécanismes d'authentification EAP

Le protocole 802.1x ne propose pas une seule méthode d'authentification mais un canevas sur lequel sont basés une douzaine de différents scénarios d'authentification, basés sur plusieurs éléments d'identification (login / mot de passe, certificat électronique, puce SIM) qui peuvent, selon les scénarios, être combinés. Nous allons présenter brièvement les principales procédures d'authentification couramment utilisées via EAP [33] [2] [27] :

2.4.3.1 EAP-MD5

Cette méthode d'authentification est définie dans la RFC 3748. Elle repose tout simplement sur le protocole CHAP étudié plus haut, avec le hash MD5. Simpliste mais la moins sécurisée, ne propose pas d'authentification mutuelle, il s'appuie uniquement sur l'utilisation d'un couple login/mot de passe. EAP-MD5 est d'ailleurs beaucoup utilisé pour des réseaux filaires où la contrainte liée au chiffrage des échanges est moins forte que pour les réseaux Wifi.

2.4.3.2 EAP/OTP

Le système *One Time Password* (OTP) est défini dans la RFC 2289. L'utilisation des OTP avec EAP est définie dans la RFC 3748. Un OTP est un mot de passe conçu pour n'être utilisé qu'une seule fois. Ceci permet de l'échanger non crypté, sans craindre qu'il soit réutilisé par un pirate.

2.4.3.3 EAP-TLS

L'EAP-TLS (*Transport Layer Security*) utilise deux certificats pour la création d'un tunnel sécurisé qui permettra ensuite l'identification : un côté serveur et un côté client. Cela signifie que même si le mot de passe est découvert, il ne sera d'aucune utilité sans le certificat client. Bien qu'EAP-TLS fournisse une excellente sécurité, l'obligation de disposer d'autant de certificats peut dissuader de nombreux administrateur.

En effet lorsque l'on dispose d'un grand nombre de machines, il peut s'avérer difficile et coûteux

de gérer un certificat par machine. C'est pour se passer du certificat client que les protocoles PEAP et EAP-TTLS ont été créés.

2.4.3.4 EAP-TTLS

EAP-Tunneled Transport Layer Security fournit un tunnel sécurisé entre le client et le serveur d'authentification. Il offre un très bon niveau de sécurité. Il utilise des certificats X-509 uniquement sur le serveur d'identification. Le certificat est optionnel du côté client.

Le défaut de EAP-TTLS par rapport à PEAP est de ne pas être présent nativement sur les systèmes Microsoft et Cisco. En revanche, il est légèrement plus sécurisé que PEAP car il ne diffuse pas le nom de l'utilisateur en clair.

2.4.3.5 PEAP

Il permet d'ajouter une couche TLS sur EAP (comme EAP-TTLS), permet d'authentifier le serveur au client mais pas l'inverse, c'est la méthode protégée par PEAP qui doit authentifier le client. Offre les services d'authentification (impossible de falsifier ou insérer des messages EAP), de chiffrement, d'échange de clé (WEP dynamique ou TKIP), fragmentation et réassemblage, reconnexion rapide.

Puisque PEAP n'impose pas de déployer un certificat sur le poste de chaque client, il peut être assez simple à mettre en oeuvre, tout en offrant un niveau de sécurité très important.

2.4.3.6 LEAP

Lightweight Extensible Authentication Protocol est une implémentation propriétaire de EAP conçue par Cisco Systems. Des produits compatibles existent, mais ils ne sont pas présents nativement sous Windows.

Il consiste à calculer une empreinte MD4 issue du mot de passe, concaténée à 5 octets nuls. Nous optiendrons 21 octets que nous interprètons sous la forme d'un 3DES. Nous chiffrons par la suite, un nombre aléatoire que nous le combinons à la clé 3DES, le tout est utilisé pour une double authentification de type CHAP entre le supplicant et le serveur d'authentification, puis entre le serveur d'authentification et le point d'accès. Cette méthode est fragile face à des attaques par dictionnaire sur mots de passe faibles.

2.4.3.7 EAP/GTC

La RFC 3748 prévoit un type d'identification appelé *Generic Token Card* (carte à jeton générique). Cette méthode est très simple : le serveur envoie un défi au client et celui-ci doit y répondre en tapant sa réponse, qui est renvoyée en clair. Le serveur vérifie la validité de la réponse. Cette méthode très simple laisse une grande marge de manoeuvre pour mettre en place des mécanismes très variés.

2.4.3.8 EAP/SIM

Cette méthode d'authentification est définie dans la RFC 4186. Son but est de permettre à un utilisateur de s'identifier grâce la carte SIM de son téléphone portable GSM. Celle-ci peut être connectée à l'ordinateur via une clé USB, par exemple, ou directement intégrée dans l'adaptateur WiFi. Pour que l'identification puisse fonctionner, le serveur d'authentification doit être relié à l'opérateur mobile de l'utilisateur : il ne sert alors que d'intermédiaire entre le client et le serveur d'authentification de l'opérateur mobile.

Cette solution a sans doute peu d'intérêt pour la plupart des entreprises dans le contexte d'un réseau WiFi, mais il s'agit encore d'une nouvelle preuve de la convergence entre la téléphonie et les technologies de l'information.

2.7 Conclusion

De nombreuses évolutions protocolaires ont rythmé la sécurité des réseaux sans fil afin d'assurer les objectifs de la sécurité informatique. Il est donc indispensable de mettre en place une politique d'authentification. Il est déconseiller d'utiliser une authentification qui s'appuie sur une clé partagée ou sur un filtrage des adresses MAC, une solution plus robuste est apportée par le protocole 802.1x. Pour augmenter encore le niveau de sécurité des informations circulant dans le réseau, nous avons aussi la possibilité d'utiliser des réseaux privés virtuels, WPA et WPA2 qui assurent la confidentialité et l'intégrité des données.

CHAPITRE 3

PROPOSITION D'UNE SOLUTION AAA OPEN SOURCE BASÉE SUR RADIUS/OPENLDAP/OPENSSL

3.1 Introduction

L'objet de notre étude porte sur les moyens utilisés pour sécuriser l'accès au réseau sans fil au sein de notre université. Dans ce qui suit nous allons présenter une architecture de sécurité. Le service d'authentification est basé sur la norme 802.1x qui assure une connexion sécurisée au niveau physique du réseau et un serveur d'authentification RADIUS est chargé d'autoriser la connexion à un utilisateur possédant un compte valide dans un annuaire LDAP, et lui autoriser l'accès à telle ou telle ressource et de comptabiliser des informations le concernant.

3.2 Objectif du travail

L'Université de Bejaia compte environ 50 000 étudiants, 2000 enseignants et autant d'agents administratifs et techniques. La difficulté de gérer de multiples référentiels utilisateurs nous a amené à sécuriser l'accès au réseau sans fil. La sécurité d'un réseau sans fil repose en particulier sur le contrôle d'accès des utilisateurs et la gestion de journaux d'utilisation afin de réprimer les abus et de ne permettre qu'aux utilisateurs légitimes d'accéder et d'utiliser le réseau sans fil.

3.3 Démarche adoptée

Il s'agit donc ici de proposer une méthode efficace et sûre qui sera basé sur les concepts étudiés pour sécuriser le réseau sans fil, tout en limitant les coûts et les manoeuvres de déploiement. Parmi les solutions citées dans le chapitre précédent, nous optons pour une authentification basée sur 802.1x associée à une infrastructure RADIUS.

Afin de mettre en place ce projet nous utiliserons donc :

- Un annuaire LDAP ;
- un serveur RADIUS qui communiquera avec l'annuaire LDAP pour authentifier un utilisateur ;
- un contrôleur d'accès qui sert d'intermédiaire entre l'utilisateur final et le serveur Radius.

Voici une représentation schématisée de cette solution :

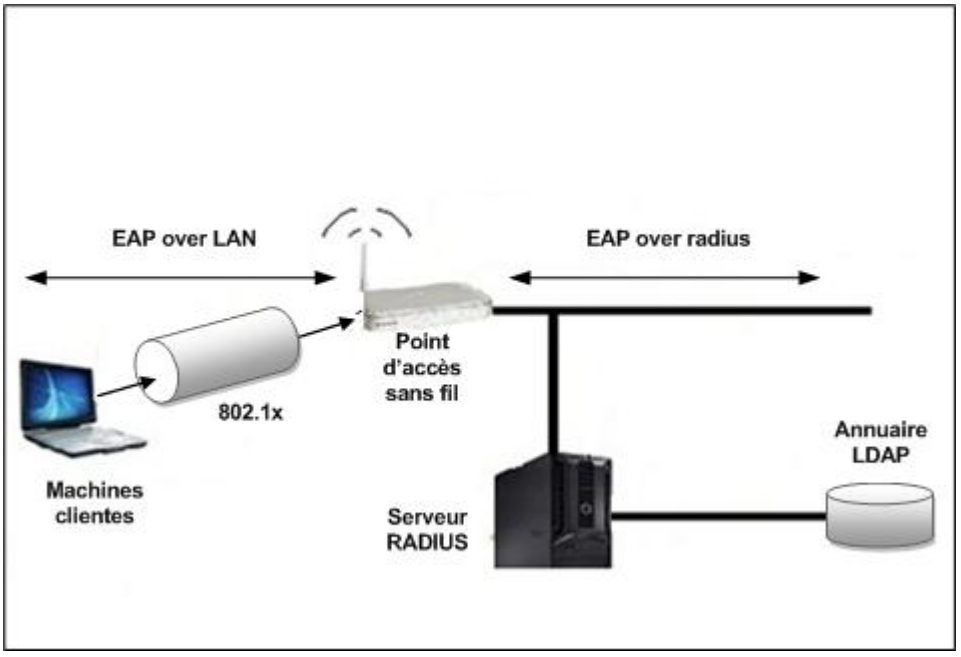

FIGURE 3.1 – Schématisation de la solution.

Le 802.1x et RADIUS étant conçus pour la même architecture et étant finalement assez complémentaires. Le protocole 802.1x suggère fortement l'utilisation d'un serveur RADIUS comme serveur d'authentification.

Voici comment les deux protocoles fonctionnent ensemble :

- L'utilisateur et le contrôleur d'accès dialoguent avec le protocole 802.1x, c'est-à-dire en utilisant le protocole EAPoL ;
- les paquets EAP que le contrôleur d'accès doit échanger avec le serveur sont véhiculés au sein

de paquets RADIUS.

En reposant sur les protocoles EAPoL et RADIUS pour le transport des paquets, l'utilisateur et le serveur dialoguent selon le protocole EAP.

3.4 La politique de sécurité

Avec un réseau sans fil, on doit tenir compte de la politique de sécurité qui va protéger nos ressources des personnes non autorisées. C'est pour cela, pour bien mener notre projet, il est nécéssaire de déterminer au premier lieu la politique de sécurité a prendre en charge qu'est comme suit :

- Le service d'accès libre sans fil est un service réservé aux utilisateurs reconnus de l'Université . Seuls les étudiants, professeurs ou membres du personnel de l'Université de Bejaia inscrits à l'Intranet de l'Université, ont accès à ce service.
- Les autres utilisateurs, conférenciers, professeurs invités, etc. qui n'ont pas de code d'utilisateur à l'Université de Bejaia et qui seraient sur place pour une période prolongée devront se faire parrainer par un responsable administratif ou un professeur afin d'obtenir un code d'accès d'invité.
- Facilité l'accés au réseau pour les utilisateurs qu'ils que soient leurs divers plate-formes :WINDOWS,LINUX, etc.
- Sécuriser les échanges d'authentification, de maniere à ce que la capture d'un paquet n'en permette pas le vol de session ou l'usurpation d'identité.
- Ne pas diffuser le SSID.
- Réduire la propagation des ondes radio vers l'extérieur de l'établissement
- Centraliser l'authentification car, elle permet non seulement de simplifier la gestion des comptes utilisateurs mais surtout de limiter les risque potentiels liés aux authentification multiples.

3.5 Type d'authentification choisie

Le choix d'un EAP est important car il va influencer sur le travail a faire et le niveau de sécurité du WiFi. La mise en place de certificats étant assez lourde à gérer par les clients, c'est pour cela que dans notre projet, nous avons choisit d'utilisé EAP-PEAP car il n'impose pas de déployer de certificat sur les postes des clients. Cette technique, associée à un cryptage WPA, est couramment utilisée pour garantir une installation facilement déployable tout en offrant un niveau de sécurité très important.

Une authentification PEAP se décompose suivant le modèle à quatre étapes d'EAP :

- Identité externe ;
- négociation de protocole ;
- protocole transporté ;
- clés de chiffrement.

Ce schéma décrit l'ensemble du processus avec la méthode PEAP en utilisant un annuaire LDAP pour la validation des comptes utilisateur.

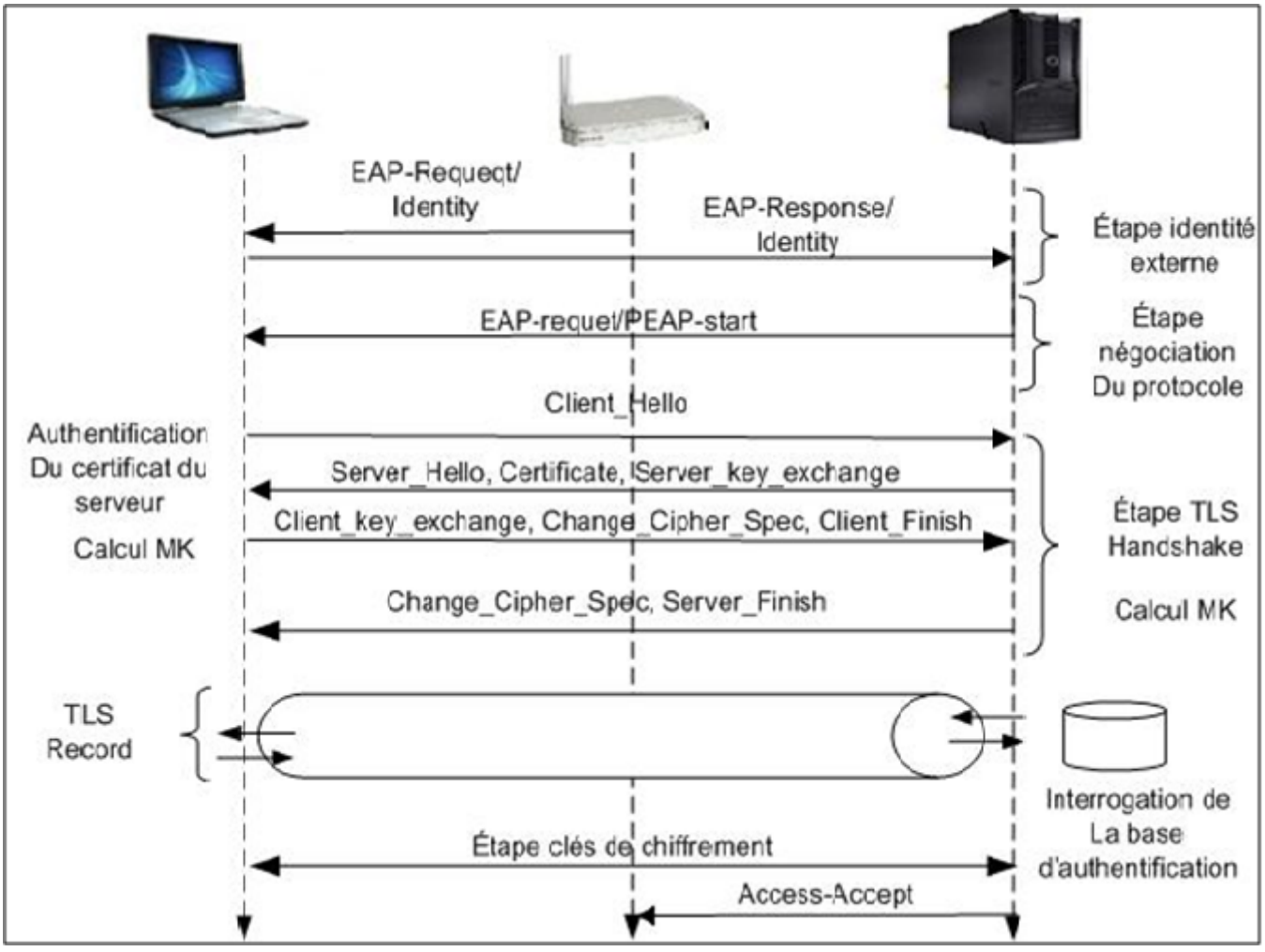

FIGURE 3.2 – L'authentification PEAP.

3.6 Le portail captif

3.6.1 Définition d'un portail captif

Un portail captif est une structure permettant un accès rapide et sécurisé à Internet. Lorsqu'un utilisateur cherche à accéder à Internet pour la première fois, le portail capte sa demande de connexion grâce à un routage interne et lui propose de s'identifier afin de pouvoir recevoir son accès. Cette demande d'authentification se fait via une page web stockée localement sur le portail captif [49].

3.6.2 Les principaux portails captifs

Nous avons récupéré une liste des principaux portails captifs libres et comparer ces derniers.

	Avantages	Inconvénients
NoCatSplash	S'intègre bien comme solution rapide.	Les utilisateurs s'enregistrent eux-mêmes.
Talweg	Simple, efficace.	Seul le port 80 passe.
Wifidog	Supporte tous les protocoles, sécurité des authentifications.	Difficile à mettre en place, trafic non sécurisé.
Chillispot	Spécialement conçu pour le WiFi	Trafic non sécurisé.
Pfsense	Administration autonome en local, multi-fonctionnalités.	Disponible qu'en anglais.

TABLE 3.1 – Les principaux portails captifs [49].

Au vu de ce comparatif PfSense apparaît comme le meilleur compromis entre portail captif.

En effet c'est cette solution qui répond le mieux aux critères de IUT[48] :

- Disponibilité (Base FreeBSD, etc).
- Confidentialité (HTTPS Web GUI, HTTPS authentification, IPSEC, PPTP, etc).
- Auditabilité.
- Mise à jour.
- Simplicité d'administration, d'installation.
- Autonomie complète.

3.6.3 PfSense

PfSense est un firewall/routeur basé sur FreeBSD, gratuit et open-source taillé pour une utilisation firewall ou routeur. En plus de sa puissance et flexibilité, la distribution inclut une longue liste de fonctionnalités et un système de paquets permettant sont extensibilité sans les vulnérabilité et les instabilités[49].

Pfsense peut être dédié à divers usage :
- Firewall ;
- LAN/WAN routeur ;
- point d'accès wireless (avec portail captif) ;
- Sniffer ;
- VPN (Ipsec,L2TP,OpenVPN ou PPTP) ;
- proxy (avec Squid) et inverse proxy ;
- serveur DHCP, DNS (TinyDNS) ;
- serveur de VOIP.

Pfsense dans notre cas va être principalement utilisé comme firewall, routeur et serveur DHCP pour notre interface LAN et point d'accès wireless avec portail captif.

3.7 RADIUS

Radius est un protocole client-serveur permettant de centraliser des données d'authentification. Ce protocole permet de sécuriser les réseaux contre des accès à distance non autorisés. Il est indépendant du type de support utilisé.

Le protocole Radius repose principalement sur un serveur (serveur Radius), relié a un annuaire LDAP et un client Radius, appelé NAS, faisant office d'intermédiaire entre l'utilisateur final et le serveur. Il est à noter que le serveur Radius peut faire office de proxy, c'est-à-dire transmettre les requêtes du client a d'autres serveurs Radius [37].

3.7.1 Principe de fonctionnement

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 de scénario d'identification demandé pour l'utilisateur pour autoriser ou non l'accès au réseau.

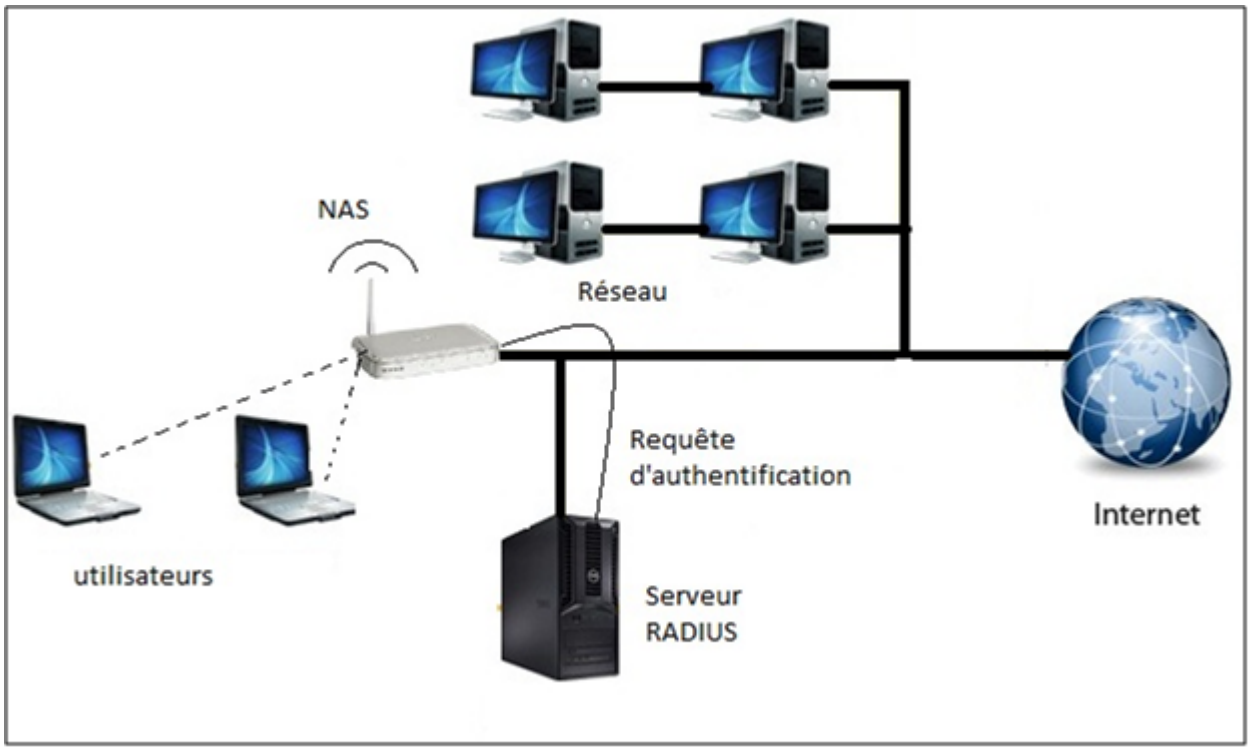

FIGURE 3.3 – L'architecture RADIUS.

Suite à cette phase d'authentification débute une phase d'autorisation ou le serveur retourne les autorisations aux utilisateurs.

3.7.2 Les différents types de paquets

Le protocole RADIUS sert aux échanges entre le NAS et le serveur RADIUS. Il spécifie six types principaux de paquets :

- **Le paquet Access-Request :** est envoyé par le NAS lorsqu'un client doit être authentifié pour accéder au réseau. Ce paquet contient entre autres l'identifiant de l'utilisateur ainsi que la preuve de son identité.
- **Un paquet Access-Challenge :** contenant un défi, peut être renvoyé par le serveur en réponse à un paquet Access-Request. Ceci est utile si la méthode d'authentification de l'utilisateur fait intervenir un défi.
- **Le paquet Access-Accept :** est renvoyé au NAS par le serveur, pour indiquer que l'utilisateur est autorisé à accéder au réseau.
- **Le paquet Access-Reject :** est bien sûr envoyé au NAS si l'utilisateur n'est pas autorisé à accéder au réseau.

- **Le paquet Accounting-Request :** est envoyé par le NAS pour indiquer au serveur le début ou la fin d'une session.
- **Le paquet Accounting-Response :** est renvoyé par le serveur pour indiquer qu'il a bien reçu le paquet Account-Request.

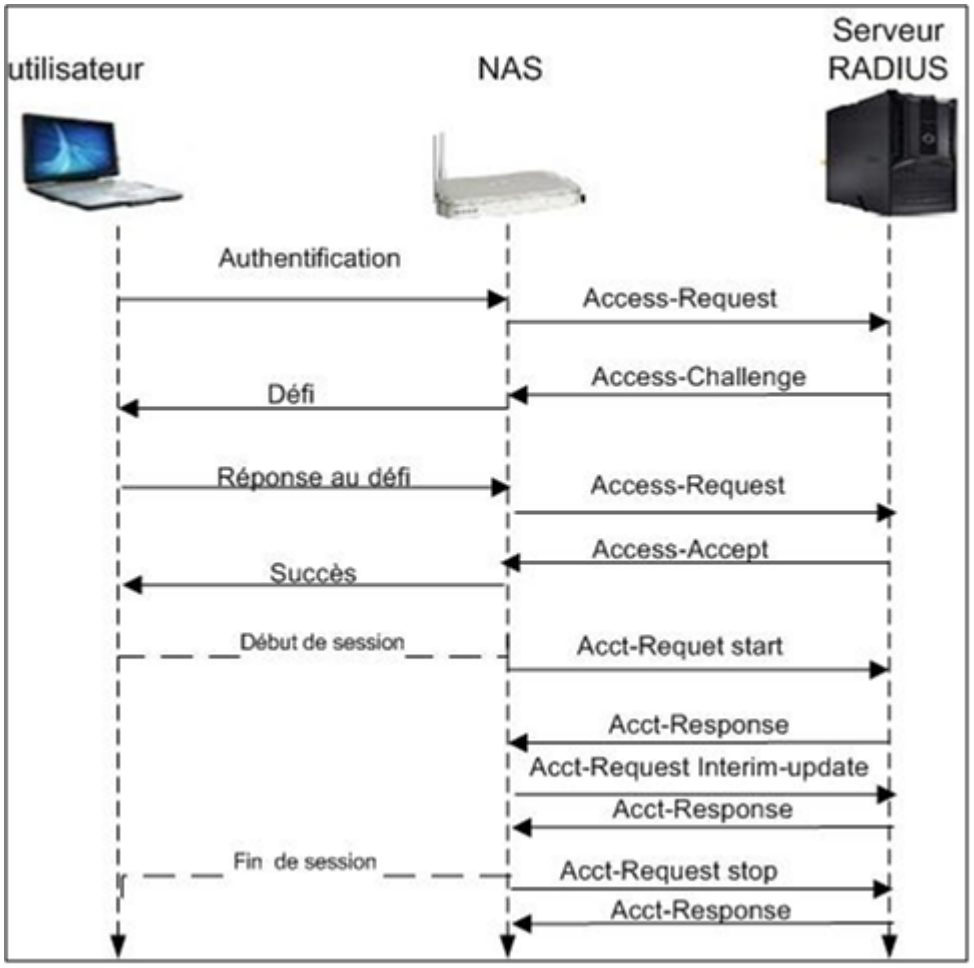

FIGURE 3.4 – Un scénario de communication RADIUS.

3.7.3 Les différents implémentation de RADIUS

Le choix du serveur est évidemment très important, il faut évaluer attentivement son coût, les méthodes EAP qu'il gère, sa stabilité, les systèmes d'exploitation sur lesquels il peut être installé, son ouverture et le support fourni.

Ce premier tableau est un comparatif des différentes méthodes d'authentification supportées par le service RADIUS :

Méthodes	**FreeRADIUS**	**CistronRADIUS**	**OpenRADIUS**	**GNU-Radius**
EAP/TLS	X			
EAP/TTLS	X			
EAP/MD5	X			
CHAP	X			X
PAP	X			X
PEAP	X			
Cisco-LEAP	X			
Couple login/pass	X	X	X	X

TABLE 3.2 – Les différentes méthodes d'authentification supportées par le service RADIUS.

Le second critère de comparaison se fait sur les types d'authentifications supportés pour authentifier les utilisateurs.

Support d'authentification	**FreeRADIUS**	**CistronRADIUS**	**OpenRADIUS**	**GNU-Radius**
PAM	X	X	X	X
Unix	X	X	X	X
MySQL	X		X	X
PostgreSQL	X		X	X
Oracle	X			
LDAP	X		X	

TABLE 3.3 – Les différents connecteurs supportés par le service RADIUS.

Enfin, dans le tableau suivant nous verrons la possibilité de liaison d'un proxy et de pouvoir garder un historique de passage des utilisateurs.

Fonctionnalités	**FreeRADIUS**	**CistronRADIUS**	**OpenRADIUS**	**GNU-Radius**
Proxy	X	X		
Accouting	X	X		

TABLE 3.4 – Les services proxy et accouting supportés par RADIUS.

C'est cette première implémentation « FreeRADIUS »que nous utiliserons et que nous détaillerons ci dessous. Elle présente l'avantage d'être très stable, de bénéficier d'une communauté très active au travers d'un site web et de listes de diffusion. Il est apte à s'intégrer dans des environnements très variés grâce à sa compatibilité avec les standards les plus courants. De plus, elle est gratuite.

3.7.4 FreeRADIUS

Freeradius est un serveur AAA basé sur le protocole RADIUS. Ce protocole effectue une authentification à distance du client et lui donne certains droits d'accès aux ressources réseaux [47].

FreeRadius est une implémentation de Radius élaborée, à la suite du projet Cistron, par un groupe de développeurs. C'est un logiciel gratuit et libre, il supporte de nombreux EAP, souvent plus que certains produits concurrents payants. Il permet d'authentifier les utilisateurs selon plusieurs moyens : mots de passe UNIX, fichier texte, base de données SQL (MySQL, PostgreSQL...) et, pour notre projet, via un annuaire LDAP.

Freeradius fonctionne par un échange de messages entre les points d'accès et le serveur. Le serveur utilise les ports UDP, le 1812 pour l'authentificationet et 1813 pour la gestion de comptes (accounting). Il y a une authentification mutuelle entre le serveur et les points d'accès grâce à un mot de passe partagé qui n'est jamais envoyé sur le réseau. Ce mot de passe commun sert à crypter les échanges entre le serveur Freeradius et les points d'accès.

3.8 Annuaire LDAP

3.8.1 Définition d'un annuaire

Un annuaire est un type de base de données spécifique, c'est-à-dire qu'il s'agit d'une sorte de base de données ayant des caractéristiques particulières [39] :

- Un annuaire est prévu pour être plus sollicité en lecture qu'en écriture. Cela signifie qu'un annuaire est conçu pour être plus souvent consulté que mis à jour ;
- les données sont stockées de manière hiérarchique dans l'annuaire, tandis que les bases de données dites relationnelles stockent les enregistrements de façon tabulaire ;
- les annuaires doivent pouvoir être répartis. Cela signifie qu'un serveur d'annuaire doit comporter des mécanismes permettant de coopérer, c'est-à-dire d'étendre la recherche sur des serveurs tiers si jamais aucun enregistrement n'est trouvé ;
- Un annuaire doit être capable de gérer l'authentification des utilisateurs ainsi que les droits de ceux-ci pour la consultation ou la modification de données.

3.8.2 Définition d'un annuaire LDAP

Depuis quelques années [40] [41], les annuaires LDAP (*Lightweight Directory Access Protocol*) se sont imposés comme étant l'outil d'échange universel des paramètres utilisateurs. LDAP est à l'origine un protocole reposant sur TCP/IP qui permet d'interroger et modifier des services d'annuaire. Un service d'annuaire est une sorte de base de données électronique permettant de définir des utilisateurs, des groupes, des applications, des ressources, etc. Mais contrairement à une base de données, l'organisation des données n'est pas relationnelle mais hiérarchique, c'est à dire telle une arborescence.

Il a cependant évolué pour représenter une norme pour les systèmes d'annuaires incluant :

- un modèle de données ;
- un modèle de nommage ;
- un modèle fonctionnel basé sur le protocole LDAP ;
- un modèle de sécurité ;
- un modèle de réplication.

Ainsi, grâce à son annuaire, LDAP sera capable de gérer de manière souple un grand nombre

de données le rendant bien adapté pour le monde d'Entreprise. Mais surtout, ce qui fait sa force, est qu'il offre un support d'authentification qui centralise tous les utilisateurs pour un grand nombre de services.

3.8.3 Les avantages des annuaire LDAP

La popularité actuale de LDAP est due à un certain nombre de facteurs que nous pouvons résumer ici [46] :

- Le meilleur argument en faveur de LDAP est sans dote le fait qu'il soit, un standard ouvert. Presque toutes les nouvelles applications seront capables de rechercher des informations dans la base LDAP et pouront accéder à l'annuair d'à peu prés n'importe quelle plate-forme.
- Centraliser toutes les informations dans un endroit donné offre des avantages considérables : un seul point d'administration, moins de risques d'erreurs, moins de données redondantes dans tous les coins et le souci de les sauvegarder.
- La plupart des serveurs LDAP sont simples à instaler, facile à maintenir et à optimiser.
- LDAP permet d'affecter efficacement des droits de lecture et de modification suivant des besoins spécifiques, en utilisant des ACL (Access Control List).

3.8.4 OpenLDAP

OpenLDAP est l'implémentation la plus répandue de LDAP développé par The OpenLDAP Project. Par définition l'installation et l'utilisation de ce serveur sont gratuites. Ce serveur peut être installé sur tout type de plate-forme, y compris Windows et les principaux Unix, dont Linux. Son code source est accessible et il est tout à fait possible de faire évoluer le serveur d'annuaire en fonction des besoins de l'université. Ceci nous permet de trouver des extensions qui permettent d'intégrer Radius comme dans notre projet.

Enfin, il est possible d'utiliser une interface web pour gérer l'annuaire LDAP grâce à Phpldapadmin qui facilite donc l'édition des données de l'annuaire OpenLDAP[43].

3.8.5 LDAP et la sécurité

LDAP est un protocole réseau disposant d'une implémentation sur la couche sécurisée SSL(*Secure Socket Layer*). Les possibilités de chiffrer stématiquement tout le trafic réseau entre serveur et client, ainsi que d'authentifier le serveur, limitent la sensibilité à l'écoute frauduleuse et le risque d'utiliser les services d'un serveur pirate.

3.9 SSL

Convaincus de la nécessité de déployer des solutions à base de chiffrement pour renforcer le système informatique de l'université, on décide de mettre en oeuvre le protocole SSL quand cela s'avérait possible et utile.

3.9.1 Le protocole SSL

SSL est un protocole cryptographique, défini en 1994 par Netscape, en collaboration avec Mastercard, Bank of America, MCI et Silicon Graphics. appliqué à la communication sécurisée point à point entre deux entités d'un réseau. C'est un protocole de sécurisation des échanges électroniques, qui est intégré dans tous les butineurs des terminaux connectables à Internet. C'est le protocole de sécurité, le plus déployé, pour sécuriser le canal de transmission d'informations entre deux ordinateurs. Son application la plus répandue est la connexion sécurisée sur un serveur pour éviter les abus et les fraudes, pendant les transactions sur le réseau [44] [45].

SSL sécurise toutes les applications qui fonctionnent nativement sur le protocole TCP. Il utilise les fonctionnalités du protocole TCP/IP pour permettre aux applications d'accéder à un mode sécurisé pour la transmission sécurisée de documents ou l'exécution de transactions sécurisées. SSL n'implique aucune modification au niveau des applications pourvu qu'il soit incorporé dans le navigateur, ce qui a concouru à faciliter son déploiement.

SSL permet donc d'assurer la confidentialité et l'intégrité des données échangées. Toutes les données sont chiffrées afin d'empêcher leur lecture par des tiers, si bien que rien ne transite en clair. SSL permet d'assurer l'authentification du serveur et, optionnellement, l'ordinateur du client. En d'autres termes, le client peut être sûr de s'adresser au bon serveur sur Internet lors d'une transaction sur Internet. SSL offre enfin le service de sécurité de non-rejeu.

3.9.2 Le fonctionnement de SSL

SSL est un protocole qui vient s'intercaler entre la couche réseau TCP et les couches applicatives de haut niveau. Il fonctionne sous un mode client/serveur, est en fait composé de quatre protocoles : Handshake, Record, Alert et Change Cipher Spec. Il fonctionne en deux étapes : la première phase est assurée par le protocole Handshake, durant laquelle les deux protagonistes négocient les algorithmes de chiffrement, la création et le partage des secrets, ainsi que l'authentification des parties.

Dans la deuxième phase, le protocole Change Cipher Spec active les paramètres négociés entre les parties, le protocole Record assure les services de sécurité du protocole SSL. Enfin, le protocole Alert gère les erreurs et les dysfonctionnements.

SSL offre des fonctions fondamentales nécessaires à la communication sécurisé sur Internet et sur tout réseau TCP/IP :

- L'authentification SSL du serveur permet de garantir son identité à chacun des clients utilisant ses services. Cet authentification s'appuit en particulier sur des techniques de chiffrement à clé publique.
- L'authentification SSL du client permet au serveur de valider l'identité du client.
- Une connexion SSL permet de chiffrer l'ensemble des données échangées entre un client et un serveur, ce qui apporte un haut niveau de confidentialité. La confidentialité est importante pour les deux parties dans la plupart des transactions privées. En complément de ce chiffrement, des mécanismes de vérification d'intégrité détectent automatiquement l'altération des données lors du transfert.

3.9.3 Openssl

OpenSSL fournit une couche de transport des données chiffrée par-dessus la couche de communication, lui permettant ainsi d'être liée à de nombreux services et applications réseau. OpenSSL est une boîte à outils de chiffrement comportant deux bibliothèques (une de cryptographie générale et une implémentant le protocole SSL et TLS), ainsi qu'une commande en ligne[38] :

1. Une bibliothèque de programmation en C permettant de réaliser des applications client/serveur sécurisées s'appuyant sur SSL/TLS.
2. Une commande en ligne (openssl) permettant :
   - La création de clés RSA, DSA (signature) ;

- la création de certificats X509 ;
- le calcul d'empreintes (MD5, SHA, RIPEMD160, etc) ;
- le chiffrement et le déchiffrement (DES, IDEA, RC2, RC4, etc).

3.10 Conclusion

A l'issue de ce chapitre, on décide de mettre en place un réseau WiFi sécurisé par WPA2 avec une authentification centralisé et sécurisé grâce au 802.1x, comme serveur d'authentification un serveur RADIUS avec l'utilisation de compte stocké sur l'annuaire LDAP, pour la vérification des mots de passe. Notre serveur communique en EAP/PEAP et permet de garder une traçabilité des utilisateurs en stockant un historique de leur passage sur le réseau.

CHAPITRE 4

IMPLÉMENTATION DE LA SOLUTION ET TESTS

4.1 Introduction

Après avoir présenté dans le chapitre précédent la démarche à adopter pour sécuriser le réseau sans fil de notre université. Ce chapitre nous permettra d'expliquer l'ensemble des étapes nécessaires à la mise en oeuvre de cette dernière. Pour la réalisation nous avons fait appel au VMware où on a installé le serveur RADIUS et LDAP, ainsi que pfsense.

4.2 Pré-requis

Le niveau de priorité de Debconf sur Ubuntu est à « Élevé ». Ce qui réduit sensiblement le nombre de questions qui nous sont posées lors de l'installation d'un paquet. nous avons donc changer le niveau à « basse »pour contrôler un maximum.

Pour cela nous saisissons en root la commande :

```
# dpkg-reconfigure debconf
```

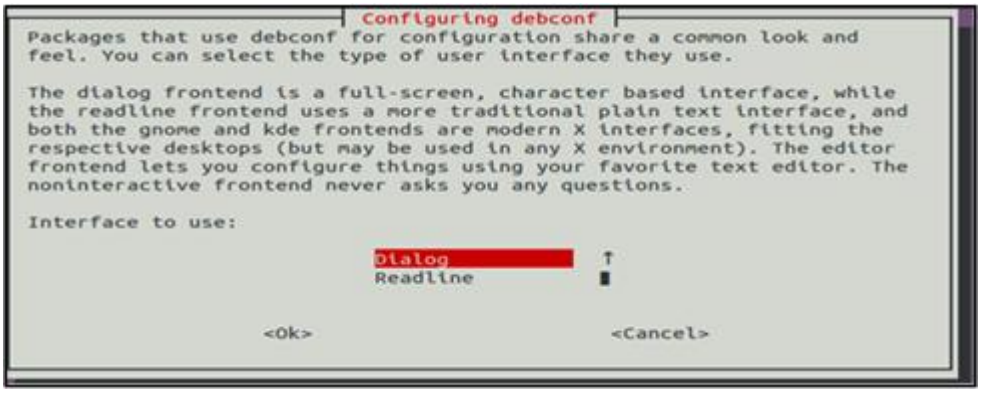

FIGURE 4.1 – Reconfiguration de debconf.

Le niveau passe de « Elevé »à « Basse ».

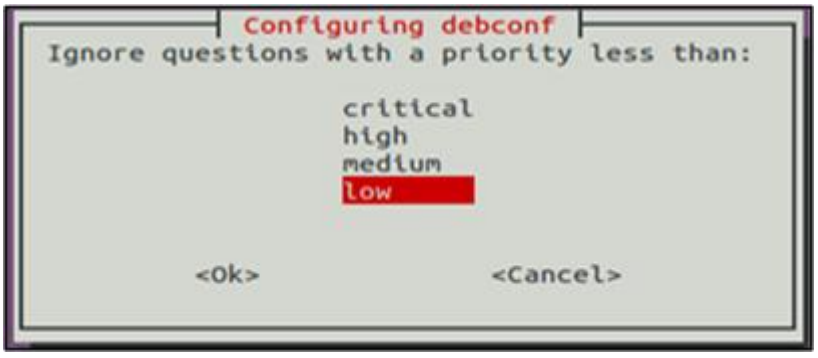

FIGURE 4.2 – La translation du niveau élevé à basse.

4.3 Mise en place du serveur LDAP

4.3.1 L'installation de OpenLDAP

Comme pour tout logiciel, il est possible d'installer OpenLDAP par le biais de paquets binaires fournis par une distribution, ou bien en compilant les sources. L'installation par paquets est souvent conseillée car elle facilite la maintenance du logiciel par la suite.

Le paquet slapd contient la partie serveur d'OpenLDAP

```
# apt-get install slapd ldap-utils
```

Lors de cette installation un certain nombre de question nous sont posées :

- **Voulez vous omettre la configuration d'openLDAP ?** : on répond NON, cela permet de générer un fichier de configuration rempli correctement en répondant aux questions qui suivent ;
- **Nom de domaine :** nous avons choisi pour le projet « univ-bejaia.dz » ;
- **Nom de votre organisation :** nous avons choisi pour l'exemple « Université de Bejaia » ;
- **Mot de passe de l'administrateur :** il s'agit d'un mot de passe pour l'administrateur de la base LDAP, dans notre cas nous avons choisi « ldap » ;
- **Module de base de données à utiliser ? :** on choisi le module HDB ;
- **Fau- il supprimer la base données à la purge de paquet ?** : on répond NON. Ainsi, si on désinstalle le paquet slapd, on ne supprime pas sa base d'utilisateurs. Cela évite la suppression malencontreuse des données ;
- **Faut-il déplacer l'ancienne base de données ? :** on répond NON ;
- **Faut-il autoriser le protocole LDAPv2 ? :** on répond NON, nous utiliserons uniquement le protocole v3.

4.3.2 Configuration d'OpenLDAP

Depuis la version 2.4.23-3 la configuration de OpenLDAP a été modifié, le fichier /etc/ldap /slapd.conf n'existe plus, toute la configuration se trouve désormais dans le répertoire /etc /ldap /slapd.d/cn=config sous forme de fichier LDIF. Avec le nouveau style de configuration, il est possible de modifier les valeurs à la volée sans avoir à redémarrer slapd.

Pour vérifier que la configuration a bien été crée nous saisissons en root :

```
# ldapsearch -Y EXTERNAL -H ldapi:/// -b 'cn=config'
```

On aura comme résultat :

```
# {1}hdb, config
dn: olcDatabase={1}hdb,cn=config
objectClass: olcDatabaseConfig
objectClass: olcHdbConfig
olcDatabase: {1}hdb
olcDbDirectory: /var/lib/ldap
olcSuffix: dc=univ-bejaia,dc=dz
olcAccess: {0}to attrs=userPassword,shadowLastChange by self write by anonymou
 s auth by dn="cn=admin,dc=univ-bejaia,dc=dz" write by * none
olcAccess: {1}to dn.base="" by * read
olcAccess: {2}to * by self write by dn="cn=admin,dc=univ-bejaia,dc=dz" write b
 y * read
olcLastMod: TRUE
olcRootDN: cn=admin,dc=univ-bejaia,dc=dz
olcRootPW: {SSHA}FWfKWRSP2pduvBSlYtpp+dKVlV75cFt6
olcDbCheckpoint: 512 30
olcDbConfig: {0}set_cachesize 0 2097152 0
olcDbConfig: {1}set_lk_max_objects 1500
olcDbConfig: {2}set_lk_max_locks 1500
olcDbConfig: {3}set_lk_max_lockers 1500
olcDbIndex: objectClass eq
```

FIGURE 4.3 – La configuration principale d'OpenLDAP.

1.3.2.1 La racine de l'arbre

L'IETF préconise d'utiliser l'attribut ***Domain Component*** (dc) car elle permettra en utilisant le service d'enregistrement du DNS de déterminer automatiquement le serveur LDAP à contacter à partir du '**DN**' utiliser dans la requête.

Elle est spécifiée par la directive :

```
olcSuffix : dc=univ-bejaia,dc=dz
```

1.3.2.2 L'accès administrateur

On déclare un compte qui ne sera sujet à aucune limitation. Il sera purement virtuel si aucun **DN** n'est effectivement stocké dans l'annuaire. Ce compte particulier n'est pas soumis aux restrictions imposées par les **ACLs**.

le compte administrateur de notre arborescence et son mot de passe sont déclarés par la directive :

```
olcRootDN: cn=admin,dc=univ-bejaia,dc=dz
olcRootPW: {SSHA} FWfKWRSP2pduvBSlYtpp+dKVlV75cFt6
```

Le mot de passe peut être soit en clair, soit un hash généré par la commande slappasswd.

1.3.2.3 L'inclusion schéma

Le modèle de données LDAP impose une approche objet Un annuaire LDAP. A travers ces schémas, il est possible de définir de nouveaux attributs et de nouveaux objectClass. Cette souplesse permet de définir très finement ce qui sera stocké dans notre annuaire.

Il s'agit d'un fichier qui décrit un à un les attributs disponibles (leur nom, leur type, etc...), ainsi que les objectClass qui y font appel. Au démarrage du serveur LDAP, le ou les fichiers de schéma spécifiés dans sa configuration seront chargés.

L'inclusion des schémas est effectuée par la directive :

```
# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/core.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/cosine.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/nis.ldif
# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/ldap/schema/inetorgpers
  on.ldif
```

Un exemple d'ajout de schéma, quand cela fonctionne le système écrira pour les quatres schémas : *adding new entry* .

FIGURE 4.4 – L'ajout du schéma core.ldif.

Plusieurs schémas sont fournis par défaut, on les trouve dans le répertoire : /etc/ldap/schema.

4.3.3 Ajout des entrées dans la base LDAP

C'est l'outil **ldapadd** qui va nous permettre d'effectuer cette opération. Il suffit de fournir à **ldapadd** un fichier LDIF contenant plusieurs entrées qui seront ajoutées dans le même ordre avec lequel elles apparaissent dans le fichier.

Fichier LDIF à insérer (ajout.ldif) :

FIGURE 4.5 – Le fichier LDIF pour l'insertion de données dans la base.

Le **DN** de chaque entrée le référence de manière unique dans l'arbre, formé de la suite des noms d'entrées, en partant de l'entrée et en remontant vers la racine. On utilise alors l'attribut '**uid**'qui permet d'identifier chaque personne de manière unique et pour les groupe c'est '**cn**'.

L'insertion de cette arborescence s'effectue comme suit :

FIGURE 4.6 – Insertion de l'arborescence.

Afin de visualiser notre nouveau LDAP, on installe « phpldapadmin »qui nous permettra de visualiser plus simplement notre annuaire.

4.3.4 Outils d'administration de l'annuaire

C'est une sorte d'équivalent à PHPMYADMIN (Pour gérer son serveur Mysql). PHPLDAPADMIN nous permet de manipuler et de visualiser facilement les éléments de votre annuaire LDAP.

Le paquet phpldapadmin est donc installé avec la commande :

```
# apt-get install phpldapadmin
```

Lors de l'installation un certain nombre de question seront posées :
- **Adresse du serveur LDAP :** 127.0.0.1.
- **Faut-il gérer le protocole LDAPS :** Non.
- **Nom distinctif de la base de recherche :** « dc=univ-bejaia,dc=dz ».
- **Type d'authentification :** session.
- **Identifiant dn de connexion au serveur LDAP :** « cn=admin,dc=univ-bejaia,dc=dz ».
- **Serveur web à reconfigurer automatiquement :** apache2.
- **Faut-il redémarrer le serveur web :** Oui

Nous ouvrons un navigateur internet et on insert l'URL suivante « http ://127.0.0.1/phpldapadmin »avec comme login : cn=admin,dc=univ-bejaia,dc=dz et le mot de passe de l'annuaire :

FIGURE 4.7 – L'interface graphique de PHPLDAPADMIN.

Après l'authentification, nous visualisons notre arboressence.

FIGURE 4.8 – Visualisation de l'annuaire à travers PHPLDAPADMIN.

Nous ajoutons la couche de chiffrement SSL au protocole LDAP pour être totalement compatible avec LDAPv3.

4.4 Installation de OpenSSL

Il peut être plus qu'intéressant de sécuriser les échanges entre les clients LDAP et le serveur à l'aide du protocole SSL. Nous allons mettre en place le SSL sur OpenLDAP en utilisant OpenSSL.

Pour installer OpenSSL, il suffit de taper cette commande en mode root :

```
# apt-get install openssl
```

4.4.1 Génération du certificat pour le serveur LDAP

Nous devons générer un certificat comme suit :

```
# openssl req -newkey rsa:1024 -x509 -nodes -out server.pem -keyout
 server.pem -days 7300
```

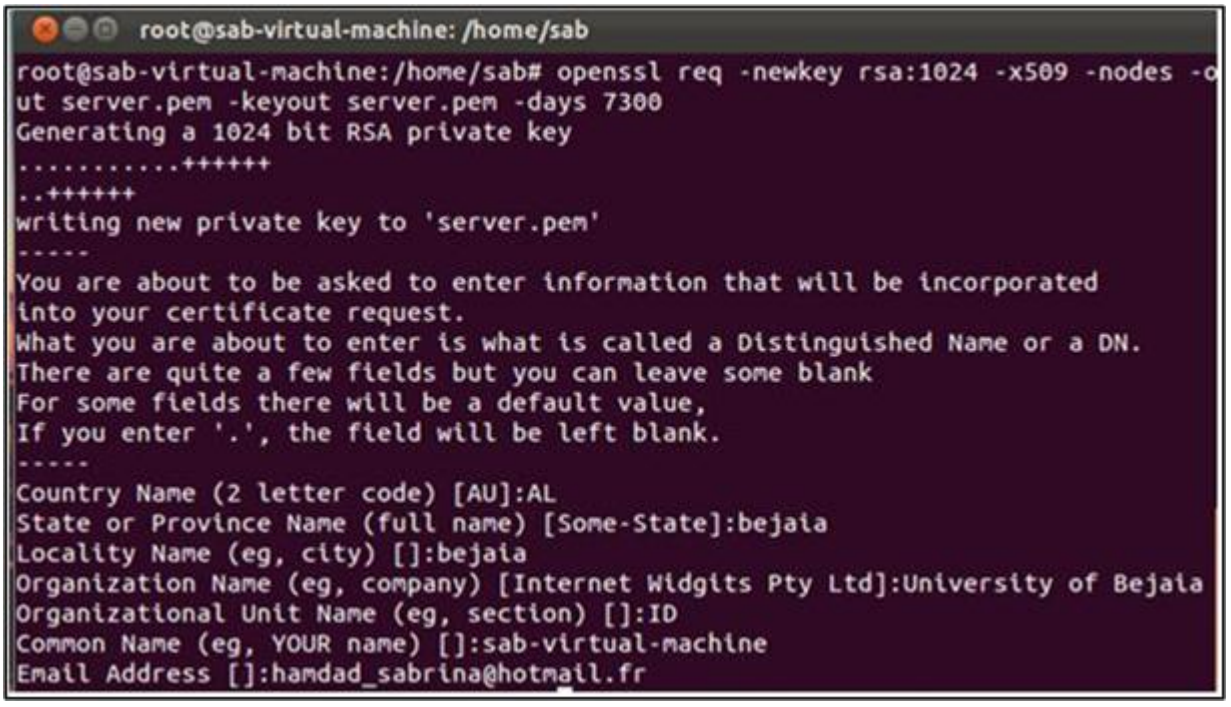

FIGURE 4.9 – Génération du certificat du serveur LDAP.

La validité du certificat est de 20 ans, il est conseillé de mettre le FQDN (*Fully Qualified Domain Name*) du serveur dans le « *Common Name* » : ici « univ-bejaia.dz ».

On déplace le certificat crée server.pem dans un répertoire dédié à cet effet :

```
# mv server.pem /etc/ldap/ssl/server.pem
```

4.4.2 Modification de la configuration du serveur LDAP

On crée un fichier tls_ldap.ldif contenant les références aux certificats :

```
dn: cn=config
add: olcTLSCACertificateFile
olcTLSCACertificateFile: /etc/ldap/ssl/server.pem
-
add: olcTLSCertificateFile
olcTLSCertificateFile: /etc/ldap/ssl/server.pem
-
add: olcTLSCertificateKeyFile
olcTLSCertificateKeyFile: /etc/ldap/ssl/server.pem
```

On ajoute la configuration au serveur LDAP :

```
#ldapmodify -Y EXTERNAL -H ldapi:/// -f /home/sab/Bureau tls_l
 dif.ldap
```

Après on modifie le fichier /etc/default/slapd pour n'autoriser que le ldaps, et ldap qu'en local :

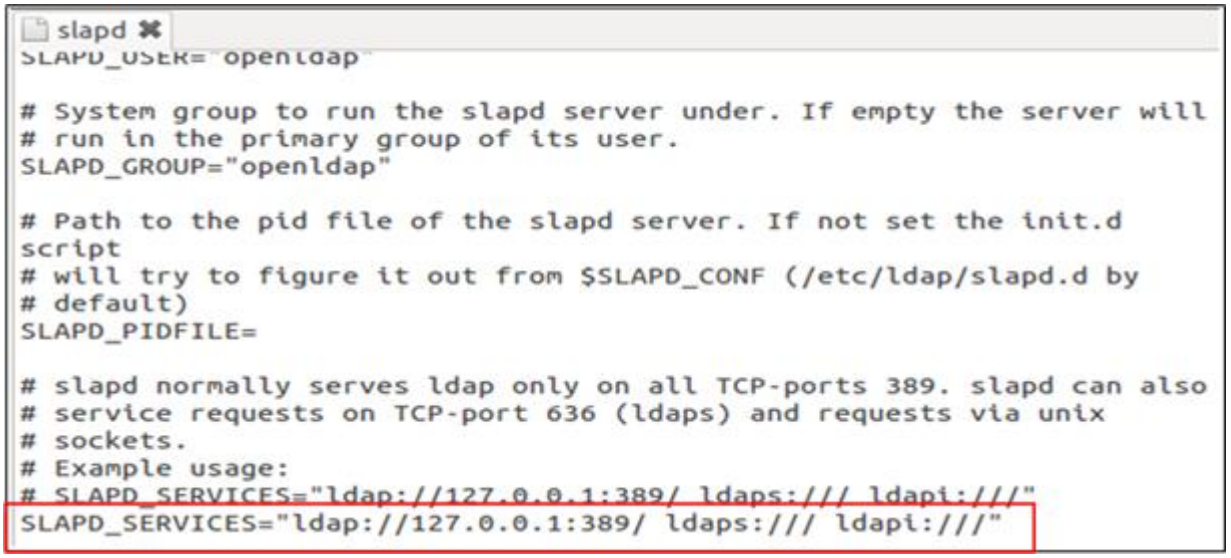

FIGURE 4.10 – Modification du fichier /etc/default/slapd.

On redémarre le serveur avec la commande :

```
#/etc/init.d/slapd restart
```

4.5 Mise en place du serveur FreeRADIUS

4.5.1 Installation de FreeRADIUS

Pour installer Freeradius sous Ubuntu, on tape la commande suivante :

```
#apt-get install freeradius freeradius-utils freeradius-ldap
 freeradius-mysql
```

On test la présence du serveur freeradius avec la ligne de commande suivante :

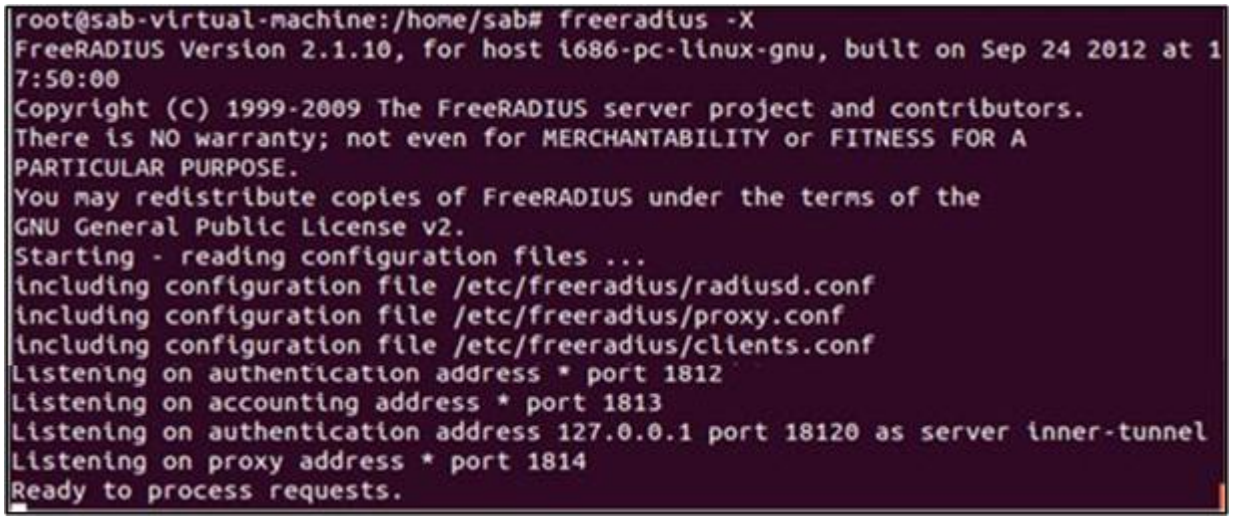

FIGURE 4.11 – Test de présence du serveur freeradius.

Le serveur écoute et attend, on peut l'arrêter avec CTRL+C. Il permet d'obtenir énormément d'informations quant au déroulement des opérations.

4.5.2 Modification sur le serveur LDAP

Il est très important de remarquer que le serveur RADIUS nécessite une classe d'objet spécifique pour qu'il puisse authentifier une personne. Par conséquent chaque entrée correspondant à une personne souhaitant être authentifié par un serveur radius doit être définit comme suit :

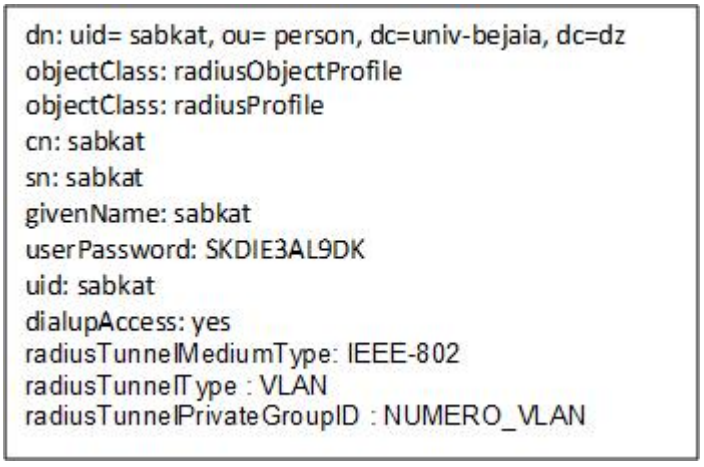

FIGURE 4.12 – Une entrée adaptée a radius.

Nous avons besoins de trois « Objetclass »pour que les utilisateurs soient reconnus par le schéma.

- RadiusObjectProfile
- Top
- Radiusprofile

Enfin, pour que l'annuaire LDAP puisse trouver cette classe d'objet et ne pas causer d'erreurs lors de l'ajout de cette entrée, il faut ajouter le schéma radius. Ce schéma se trouve dans /usr/share/doc/freeradius/examples/openldap.schema. On renomme ce schéma en freeradius.schema, et on le transfert vers /etc/ldap/schema.

```
#cp /usr/share/doc/freeradius/examples/openldap.schema /etc/ldap/schema
    /freeradius.schema
```

On doit rajouter le schema freeradius, pour cela on doit transformer freeradius.schema en freeradius.ldif (Voir annexe). Après la transformation, on importe le schéma freeradius.ldif dans OpenLDAP.

FIGURE 4.13 – Importation du schéma freeradius.ldif dans OpenLDAP.

4.5.3 Configuration du FreeRADIUS

Dans le répertoire « /etc/freeradius/ »on trouve l'ensemble des fichiers de configuration. La configuration est répartie en dossiers de manières à simplifier l'administration.

Voici un aperçu des fichiers de configuration :

FIGURE 4.14 – Les principaux fichiers de configuration.

Freeradius est conçu de façon extrêmement modulaire, ce qui permet de l'interfacer facilement avec tout autre type de matériel ou service. Quelques exemples de modules :

- **radiusd.conf :** La configuration principale est lue à partir du fichier radiusd.conf, contenant la définition et les liens de modules, etc ;
- **clients.conf :** Fichier des points d'accès reconnus par RADIUS (même mot de passe partagé) ;
- **eap.conf :** activer et configurer le tls et le peap pour établir le tunnel peap, et activer mschap- pour activer le MS-CHAP-v2 à l'intérieur du tunnel ;
- **users :** Fichier des utilisateurs locaux.
- **modules/ldap :** configurer les paramètres d'accès à l'annuaire, et les paramètres de recherche des entrées des utilisateurs ;
- **sites-available/default :** activer preprocess et eap dans la phase authorize, et eap uniquement dans la phase authenticate ;
- **sites-available/inner-tunnel :** activer preprocess, eap et ldap dans la phase authorize, et mschap uniquement dans la phase authenticate
- **ldap.attrmap :** Correspondance entre les attributs LDAP et attributs RADIUS.
- **sql.conf :** Fichier de configuration pour MySQL.

1.5.3.1 Le fichier de configuration principale radiusd.conf

Il est divisé en sections (Security, proxy, thread pool,modules, authorize, authenticate et accounting) :

- **La section security** permet de protéger le serveur contre quelques attaques DoS notamment.
- **La section proxy** permet de configurer les paramètres relatifs à la communication avec d'autres serveurs RADIUS.
- **La section thread pool** permet de configurer le nombre de serveurs qui traitent les requêtes et le nombre de processus lancés.
- **La section modules** permet d'activer et de configurer les méthodes d'authentification.
- **La section log** qui représente la partie journaux.

Nous allons modifier la partie journaux.

```
#
log {
        #
        #  Destination for log messages.  This can be one of:
        #
        stripped_names = yes

        #  Log authentication requests to the log file.
        #
        #  allowed values: {no, yes}
        #
        auth = yes

        #  Log passwords with the authentication requests.
        #  auth_badpass  - logs password if it's rejected
        #  auth_goodpass - logs password if it's correct
        #
        #  allowed values: {no, yes}
        #
        auth_badpass = yes
        auth_goodpass = yes

}
```

FIGURE 4.15 – Modification de la partie log du fichier radiusd.conf

Et décommenter #$INCLUDE sql.conf.

```
#  Include another file that has the SQL-related configuration.
#  This is another file only because it tends to be big.
#
$INCLUDE sql.conf
```

FIGURE 4.16 – Modification de la partie #$INCLUDE sql.conf.

1.5.3.2 Le fichier de configuration clients.conf

Il nous faut ensuite les informations concernant le client radius. Celles-ci sont stockées dans le fichier /etc/freeradius/clients.conf. Ce fichier sert à la définition des NAS ou les éléments du réseau autorisé à émettre des requêtes valide vers le serveur. C'est ici que l'on va définir le secret partagé entre un client spécifique et le serveur. Un client peut être une borne wifi mais il peut être aussi un autre serveur radius d'une autre Université.

clients.conf

```
#  format is still accepted.
#
client localhost {
        #  Allowed values are:
        #       dotted quad (1.2.3.4)
        #       hostname    (radius.example.com)
        ipaddr = 127.0.0.1

        secret          = testing123

        #  allowed values: yes, no
        require_message_authenticator = no

        #
        shortname       = localhost

        #
        nastype     = other     # localhost isn't usually a NAS...

}
```

FIGURE 4.17 – Le fichier de configuration Clients.conf

1.5.3.3 Connexion entre LDAP et freeradius

Il nous faut donc les informations permettant d'accéder à l'annuaire LDAP. Ces informations que nécessite le serveur Radius sont stockées dans le fichier /etc/freeradius/modules/ldap.

Voici un aperçu de ce fichier :

ldap

```
#
ldap {
        #
        #  Note that this needs to match the name in the LDAP
        #  server certificate, if you're using ldaps.
        server = "127.0.0.1"
        identity = "cn=admin,dc=univ-bejaia,dc=dz"
        password = ldap
        basedn = "dc=univ-bejaia,dc=dz"
        filter = "(&(uid=%{%{Stripped-User-Name}:-%{User-Name}}) (dialupAccess=yes))"
        base_filter = "(objectclass=radiusprofile)"

        #  How many connections to keep open to the LDAP server.
        #  This saves time over opening a new LDAP socket for
        #  every authentication request.
        ldap_connections_number = 5

        # seconds to wait for LDAP query to finish. default: 20
        timeout = 4

        #  seconds LDAP server has to process the query (server-side
        #  time limit). default: 20
        #
        #  LDAP_OPT_TIMELIMIT is set to this value.
        timelimit = 3

         # default_profile = "cn=radprofile,ou=dialup,o=My Org,c=UA"
         # profile_attribute = "radiusProfileDn"
         access_attr = "dialupAccess"

        password_attribute = userPassword
}
```

FIGURE 4.18 – Le fichier de configuration ldap.

- Le champ server = 127.0.0.1 correspond à l'adresse IP de l'annuaire LDAP.
- Le champ identity= cn=admin,dc=univ-bejaia,dc=dz au chemin dans l'arbre jusqu'à l'admin.
- Le champ password= ldap au mot de passe admin du LDAP.
- Le champ basedn= cn=admin,dc=univ-bejaia,dc=dz à la base de l'arbre LDAP.
- Le champ filter=(&(uid=%Stripped-User-Name :-%User-Name)(dialupAccess=yes)) permet de localiser un utilisateur utilisant les paramètres fournis par le client.
- Le champ base_filter= (objectclass=radiusprofile) permet de filtrer la recherche à l'utilisateur de cette classe.
- Le champ access_attr permet de donner l'accès au utilisateur possédant l'attribut dialupAccess = yes.

Maintenant que le module LDAP est bien configuré, il faut dire au serveur Radius d'utiliser ce module LDAP pour cela il faut décommenter les lignes correspondantes à LDAP dans les fichiers site-enabled/default et sites-enabled/inner-tunnel

1.5.3.6 Le fichier site-enabled/default

Nous modifions la partie « authorize »et « authenticate ». Le module LDAP effectue des tâches différentes selon les sections où on l'active :

FIGURE 4.19 – La partie authenticate du fichier default.

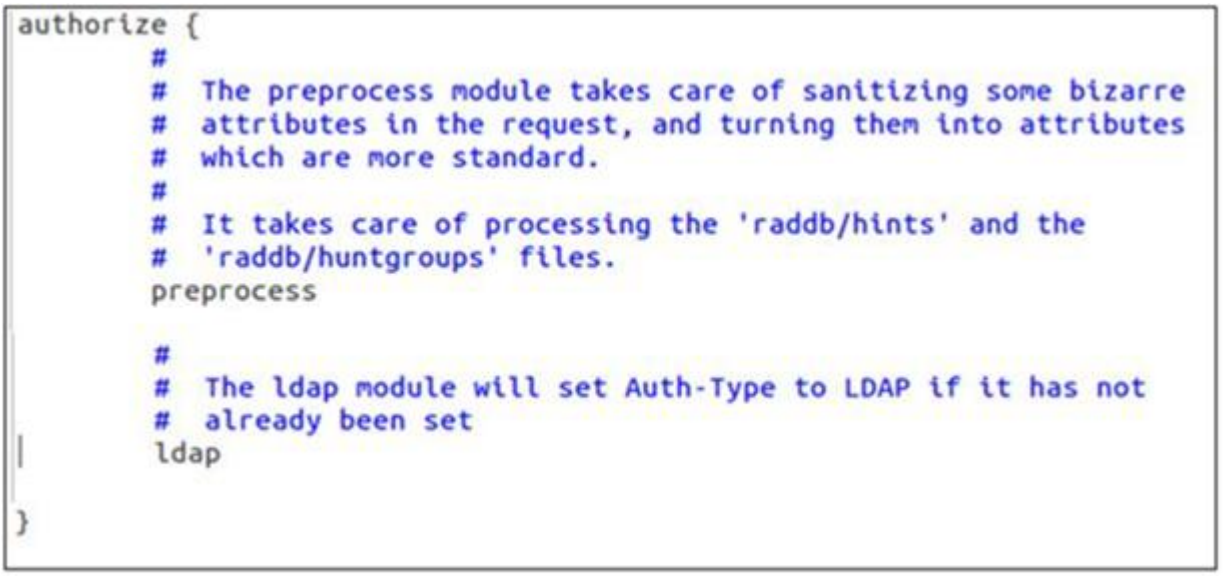

FIGURE 4.20 – La partie authorize du fichier default.

1.5.3.5 Le fichier eap.conf

Nous activons et configurons le tls et le peap pour établir le tunnel peap, et mschap pour activer le MS-CHAP-v2 à l'intérieur du tunnel.

```
eap {
        default_eap_type = peap
        timer_expire = 60
        ignore_unknown_eap_types = no
        cisco_accounting_username_bug = no
        max_sessions = 4096
        tls {
        certdir = ${confdir}/certs
        cadir = ${confdir}/certs
        private_key_file = ${certdir}/server.key
        certificate_file = ${certdir}/server.pem
        dh_file = ${certdir}/dh
        random_file = ${certdir}/random
        cipher_list = "DEFAULT"
        cache {
        enable = no
        lifetime = 24
        max_entries = 255
        }
}
peap {
        default_eap_type = mschapv2
        copy_request_to_tunnel = yes
        use_tunneled_reply = no
        virtual_server = "inner-tunnel"
        }
mschapv2 {
}
```

FIGURE 4.21 – L'activation de PEAP dans le fichier eap.conf.

1.5.3.4 Le fichier sql.conf

Nous modifions le fichier /etc/freeradius/sql.conf.

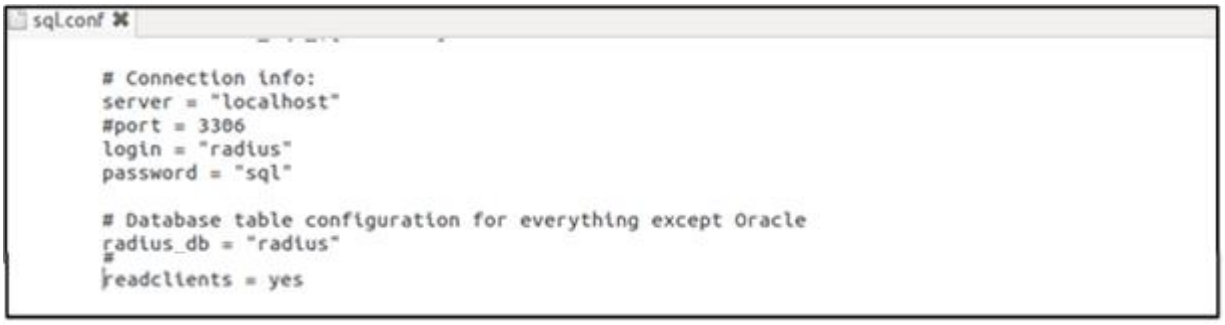

FIGURE 4.22 – Le fichier de configuration sql.conf.

4.6 Configuration de MySQL

4.6.1 Pré-requis

Apache2, MySQL, Php et PhpMyAdmin (pour gérer vos bases de données) doivent être impérativement installé au préalable.

4.6.2 Création de la base de données

On prépare la BDD et on lui attribue un nom d'utilisateur et mot de passe.

```
# mysql -u root -p

mysql> create database radius;
mysql> grant all on radius.* to radius@localhost identified by "sql";
```

4.6.3 Inclusion des schémas dans la base de données

L'étape suivante consiste à insérer le schema dans la base de données.

```
# mysql -u root -p radius < /etc/freeradius/sql/mysql/schema.sql
Enter password:
# mysql -u root -p radius < /etc/freeradius/sql/mysql/nas.sql
Enter password:
```

4.7 L'interface web d'administration du serveur RADIUS

Il existe plusieurs applications web avancées de gestion qui sont open source et gratuites. Parmi eux on trouve « Daloradius », il comporte la gestion des utilisateurs, des NAS, des rapports graphiques, de la comptabilité, de facturation et s'intègre avec le moteur Google Maps pour géolocaliser.

4.7.1 Installation de Daloradius

Un certain nombre de bibliothèques doivent être installé pour que Daloradius fonctionne correctement.

```
# apt-get install php5-gd php-pear php-db
```

Se rendre sur le site pour télécharger l'archive http ://sourceforge.net/projects/daloradius/. Après on extrait daloradius.tar.gz dans /var/www

Nous plaçons le dossier du serveur web

```
#tar -zxvf daloradius-0.9-9.tar.gz
#cp daloradius-0.9-9/ /var/www -R
```

Ensuite, nous avons besoin de configurer la base de données. Vu que nous avons déjà configuré le freeradius utilisant MySQL, donc nous n'avons pas besoin d'une nouvelle base de données. Tout ce que nous devons faire est d'importer le schéma de daloradius dans notre base de données 'radius' existante grâce à la commande :

```
# cd /var/www/daloradius0.9-9/contrib/db
# mysql -u root -p radius < mysql-daloradius.sql
```

Nous modifions le fichier de configuration daloradius.conf.php, en insérant le mot de passe de la base de données « radius ».

```
$configValues['DALORADIUS_VERSION'] = '0.9-9';
$configValues['FREERADIUS_VERSION'] = '2';
$configValues['CONFIG_DB_ENGINE'] = 'mysql';
$configValues['CONFIG_DB_HOST'] = 'localhost';
$configValues['CONFIG_DB_PORT'] = '3306';
$configValues['CONFIG_DB_USER'] = 'root';
$configValues['CONFIG_DB_PASS'] = 'sql';
$configValues['CONFIG_DB_NAME'] = 'radius';
$configValues['CONFIG_DB_TBL_RADCHECK'] = 'radcheck';
$configValues['CONFIG_DB_TBL_RADREPLY'] = 'radreply';
$configValues['CONFIG_DB_TBL_RADGROUPREPLY'] = 'radgroupreply';
$configValues['CONFIG_DB_TBL_RADGROUPCHECK'] = 'radgroupcheck';
$configValues['CONFIG_DB_TBL_RADUSERGROUP'] = 'radusergroup';
$configValues['CONFIG_DB_TBL_RADNAS'] = 'nas';
```

FIGURE 4.23 – Le fichier de configuration daloradius.conf.php.

Après, l'installation on accède à l'interface de Daloradius en tapant dans le navigateur l'URL suivante : http ://127.0.0.1/daloradius.

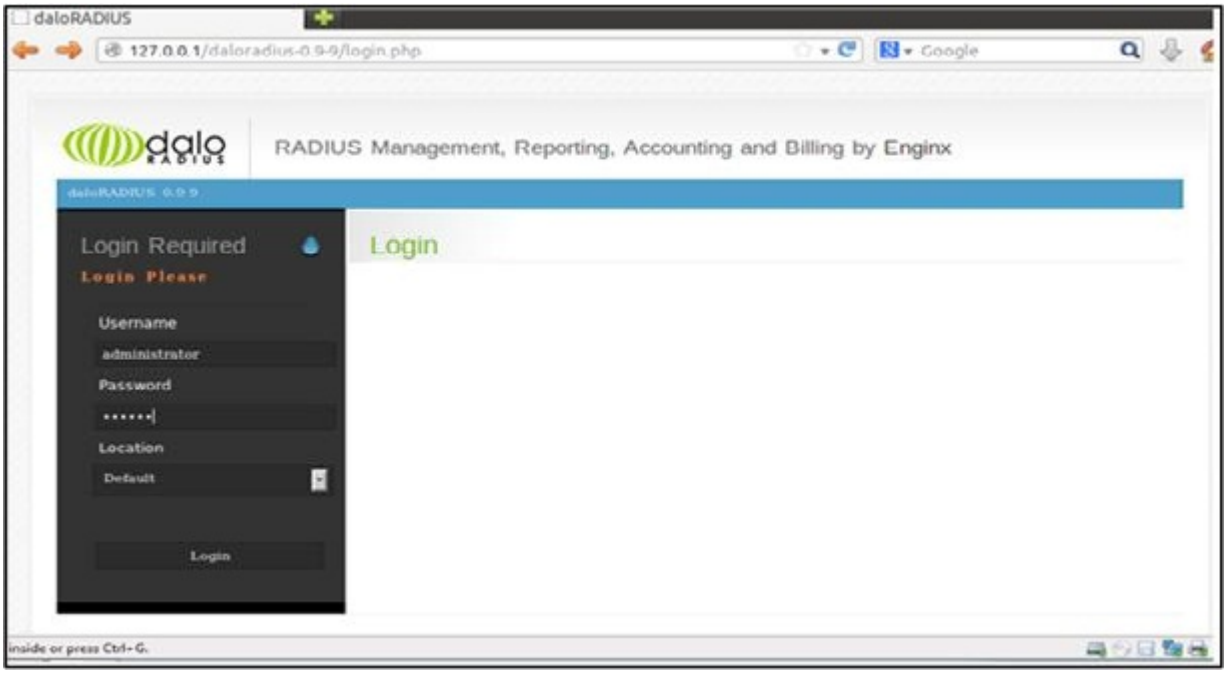

FIGURE 4.24 – L'interface de connexion de Daloradius.

Après l'authentification de l'administrateur avec comme, login=administrator et mot de passe=radius. Nous accèdons à la page principale de Daloradius, qui permet la gestion, la maintenance du serveur RADIUS.

FIGURE 4.25 – L'interface principale de Daloradius.

4.7.2 Installation de PfSense

Au démarrage, nous arrivons sur le menu suivant, que nous validerons avec le choix n°1.

FIGURE 4.26 – Le menu de démarrage de pfsense.

Une fois le premier écran validé, les cartes réseaux sont affichées, avec comme identificateur : em0 et em1.

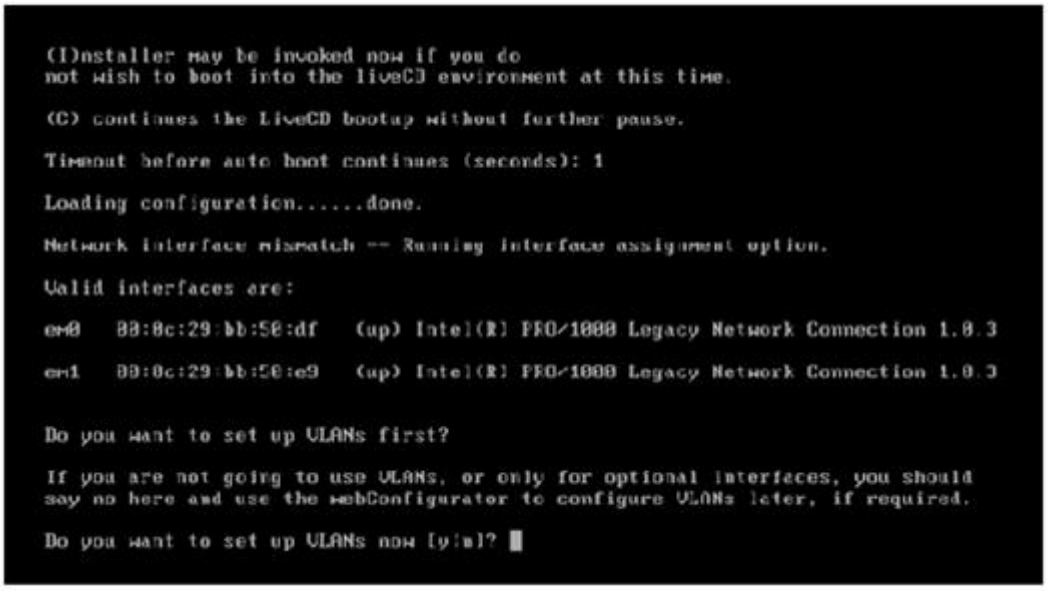

FIGURE 4.27 – Détection des cartes réseaux.

La première question concerne les Vlans. Nous refuserons de les configurer maintenant (cela se fera par l'interface graphique). Nous avons franchi une étape et le système en sait assez pour s'installer, choisissons l'option 99.

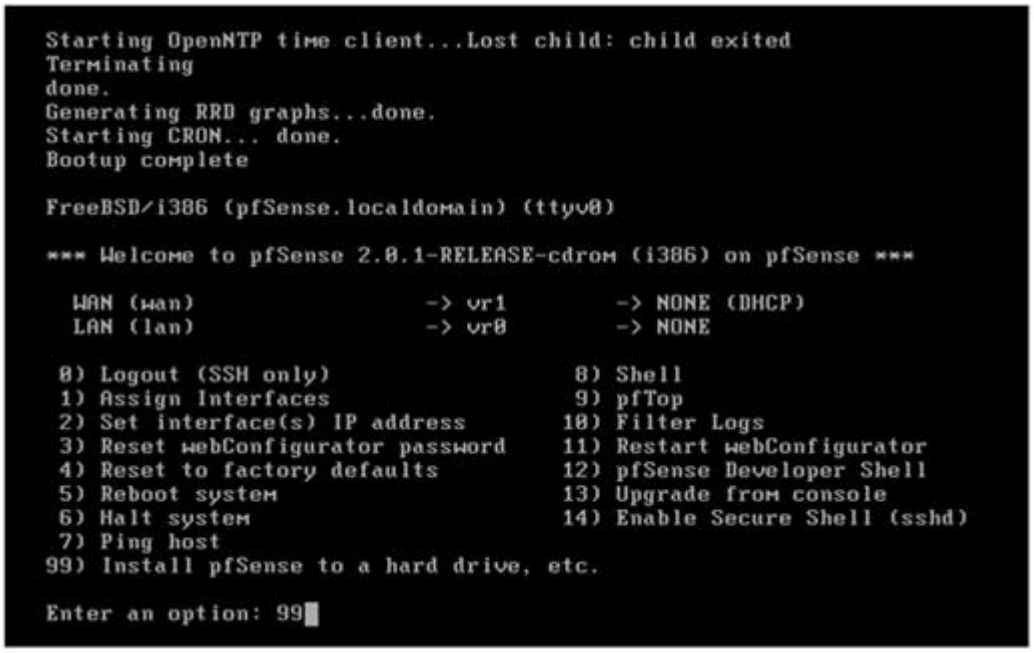

FIGURE 4.28 – Le menu d'installation.

4.7.3 Configuration de PfSense

Nous allons maintenant configurer PfSense. Avant tout, nous changeons l'IP sur la machine de PfSense directement, pour plus de simplicité par la suite. Pour cela, dans le menu de PfSense, nous saisissons le choix 2 Set LAN IP address. Puis nous inserons l'adresse IP correspondant à votre LAN.

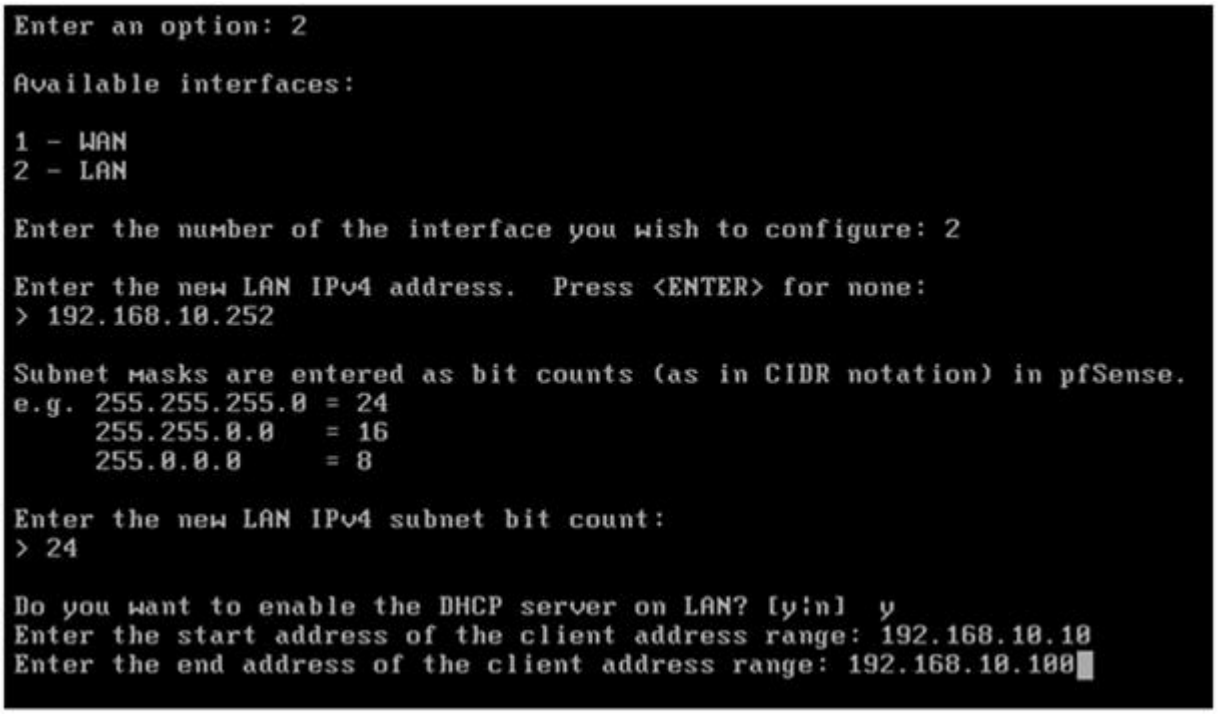

FIGURE 4.29 – La configuration de l'interface LAN de PfSense.

PfSense est maintenant accessible depuis l'internet à l'adresse IP https ://192.168.1.252

4.7.4 Configuration du portail captif

Nous allons désormais mettre en place le portail captif. Pour cela, dans la section Captive portail nous cochons la case Enable captive portail, puis choisissons l'interface sur laquelle le portail captif va écouter (LAN dans notre cas).

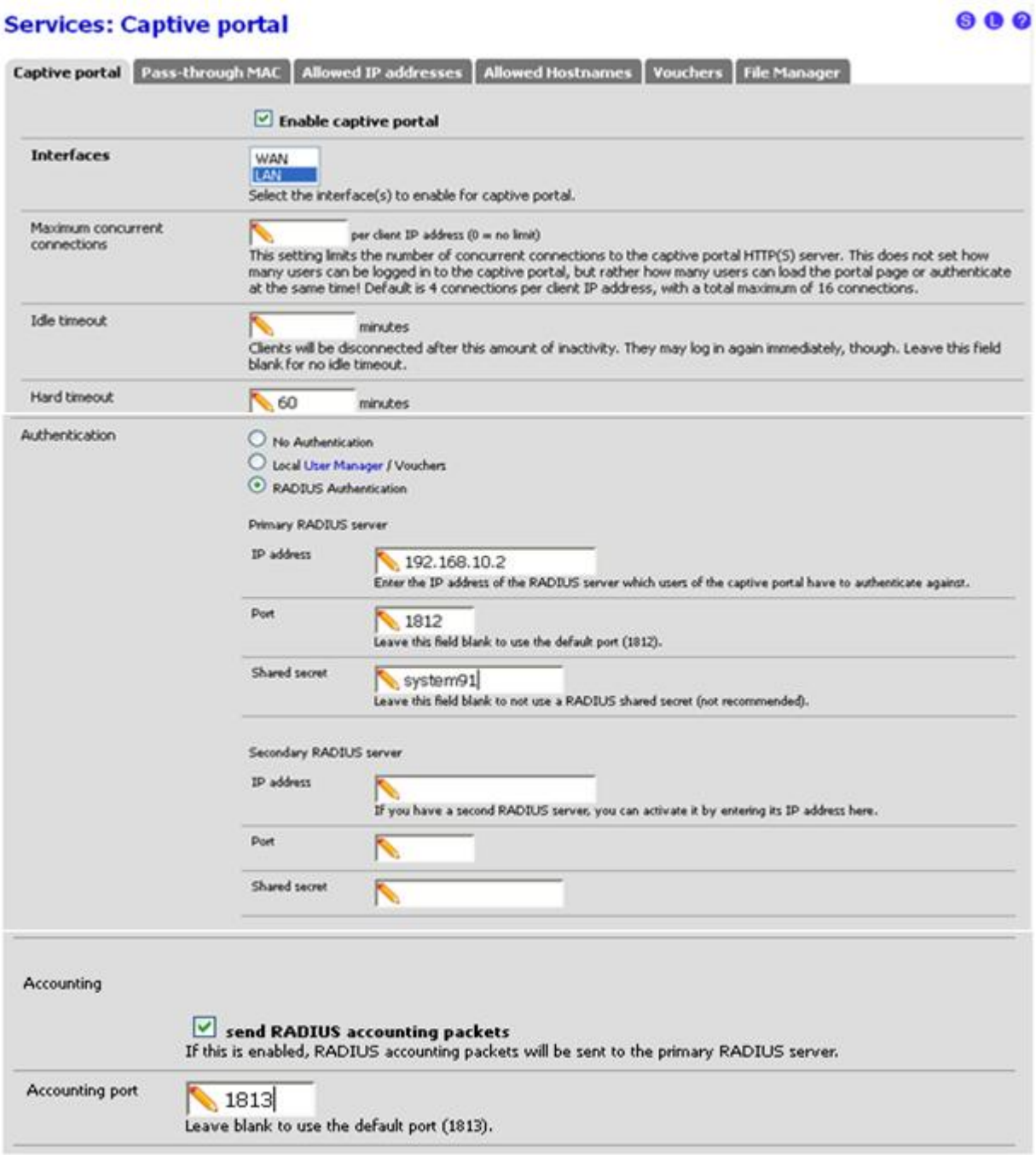

FIGURE 4.30 – La configuration du portail captif.

4.8 Test de fonctionnement

Si un utilisateur cherche à accéder au réseau sans fil le parefeu PfSense lui barrera le chemin jusqu'à ce qu'il s'identifie auprès du serveur RADIUS à travers un Login et mot de passe. Le Parefeu sert d'intermédiaire pour la communication entre l'utilisateur et le serveur RADIUS.

4.8.1 Test de l'authentification et l'authorisation

L'utilisateur devra saisir ces informations sur cette interface.

FIGURE 4.31 – Le portail captif de PfSense.

Après l'authenfication et l'authorisation de la part du serveur RADIUS, l'utilisateur aurra accès au réseau sans fil.

A l'aide de l'invité de commande, nous avons pu voir que PfSense à interdit l'accès tant que l'utilisateur ne s'est pas authentifier.

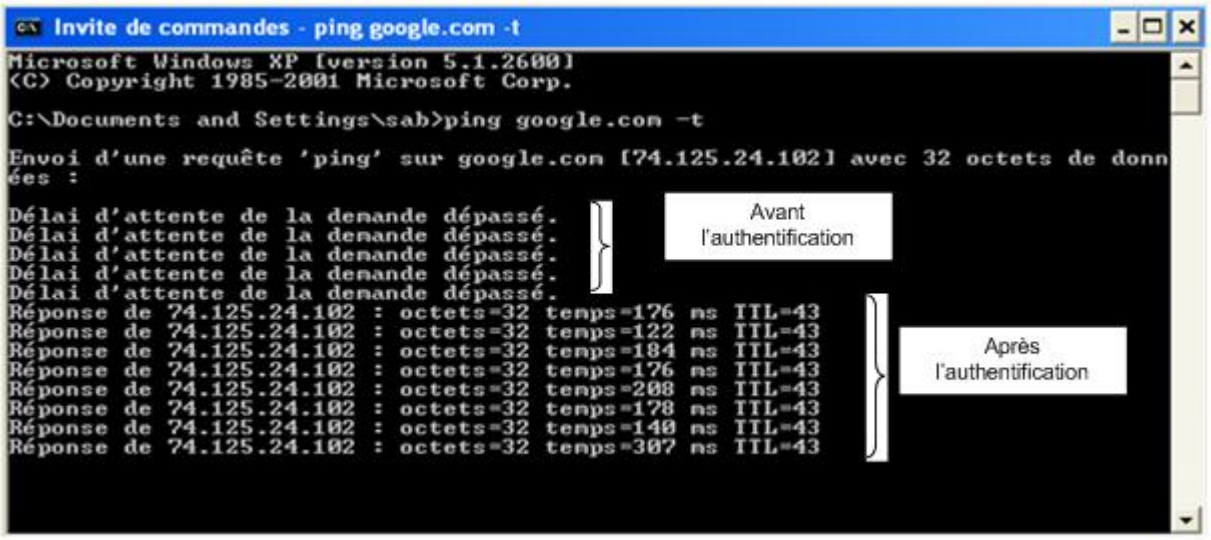

FIGURE 4.32 – Test de fonctionnement avec l'invité de commande.

4.8.2 Test de la comptabilité

Dans l'onglet management->Nas, nous ajoutons le client Nas, puis nous inserons les informations de notre parefeu PfSense comme ci-dessous :

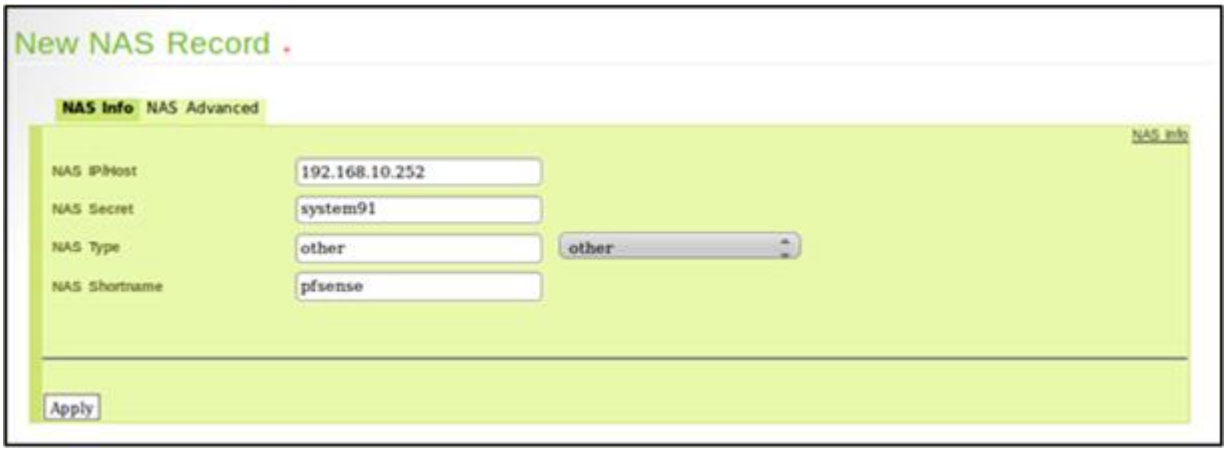

FIGURE 4.33 – Ajout d'un client NAS sur daloradius.

Après enregistrement nous verifions l'existance dans la liste ListNas.

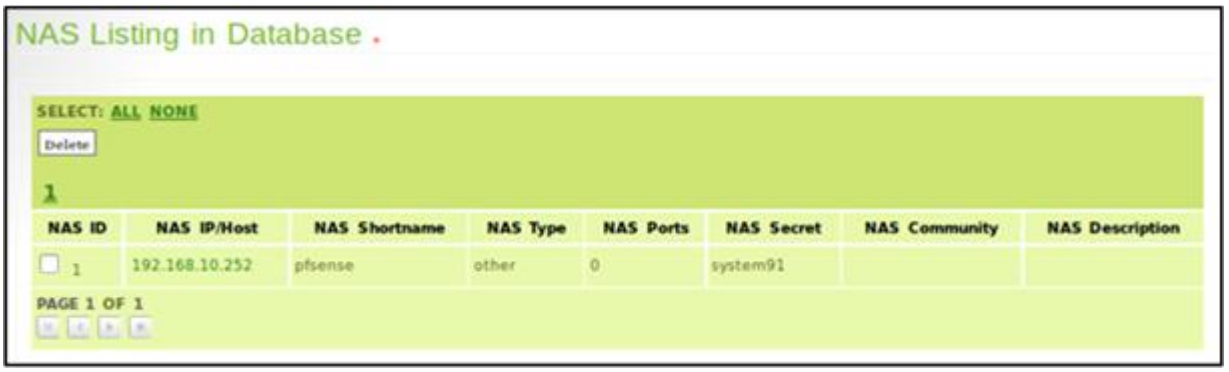

FIGURE 4.34 – La liste des clients NAS sur daloradius.

Pour vérifier la comptabilité, dans l'onglet Accounting-> All record, nous trouvons toutes les informations concernant les utilisateurs authenfiés.

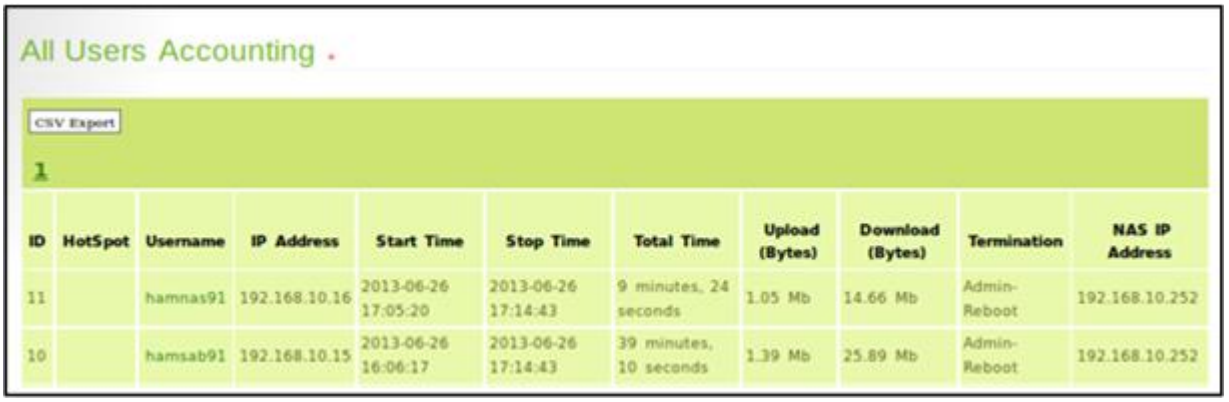

FIGURE 4.35 – La comptabilité des utilisateurs.

4.9 Conclusion

Dans ce chapitre, nous avons configuré et mis en place une solution robuste pour contrôler l'accès au réseau sans fil de notre université. Nous avons expliqué la configuration faite pour chacun des éléments pour la réalisation de ce projet. Néanmoins, cette structure a ses limites et doit coexister avec d'autres méthodes complémentaires (notamment pour la gestion des droits) afin de proposer une solution véritablement intégrée.

Ce travail nous a amené à acquérir diverses compétences. L'informatique est un monde en constante évolution et ce travail est pour nous la meilleure preuve que l'informaticien est en quelque sorte « un éternel étudiant ».

CONCLUSION GÉNÉRALE

Les réseaux sans fil sont quasi-indispensable de nos jours, ils présentent divers avantages parmi : leurs simplicité de déploiement, mobilité, faible coût en comparaison de l'installation et la maintenance d'un réseau câblé. Il faut le considérer a priori comme un réseau ouvert au public mais également comme une bulle de risque à cause principalement d'absence de support physique qui augmente le niveau d'écoute indésirer.

Afin de proposer un bon mécanisme de sécurité d'un réseau sans fil « le WiFi », comme solution contre les points faibles dont il souffre, l'AAA permet de palier à l'un des plus gros défauts de ce type d'accès qui est la sécurité. Nous avons tout au long de ce travail mis en place un système sécurisé en restant compatible avec les différentes technologies existantes, tout en tenant compte de la durabilité, l'évolution et la fiabilité de cette solution, assez bien en termes techniques que économiques.

Pour cela, nous avons opté pour une solution qui sera facile a géré coté administrateur, ne complique pas l'accés au réseau coté utilisateur et qui repond parfaitement a notre objectif qui est l'implimentation d'une solution d'authentification forte, mutuelle et centralisée. Les acteurs principaux de cette solution sont la norme 802.1x, le serveur RADIUS avec l'utilisation de compte stocké sur un annuaire LDAP. Notre serveur communique en EAP/PEAP et permet de garder un historique de leur passage sur le réseau.

Nous avons rencontré plusieurs difficultés pour maîtriser ce projet, mais y avoir recherché et travaillé pendant trois mois, nous a donné l'occasion de bien évoluer et approfondir nos connaissances et capacités dans le domaine des sécurités réseau.

Pour conclure, comme perspectives dans notre maquette un seul serveur Radius suffit mais comme il sera très vite un maillon vital de l'architecture, il faudra prévoir de le doubler par une machine secondaire apte à prendre le relais en cas de panne du serveur principal. Mais aussi de rem-

placer Radius par Diameter qui est son successeur, et est bien plus riche en fonctions. Il utilise une architecture peer to peer plutôt qu'un schéma client/server et le protocole TCP au lieu UDP et mieux adapté au roaming. Pour finir il faut prévoir un mécanisme de réplication au niveau de l'annuaire LDAP, qui offrira la possibilité de répliquer l'annuaire dit « maître »pour répartir la charge de travail.

Annexes

Annexe A : Conversion du fichier freeradius.schema pour l'importation dans openldap

On commence par copier le schéma « openldap »qui se trouve dans /usr/share/doc/freeradius/examples/ vers /etc/freeradius/. On renomme ce schéma en freeradius.schema.

Ensuite, on crée un fichier « convert-schema.conf »et un réptertoire « res », le ficher va contenir :

```
# include /etc/freeradius/freeradius.schema
```

Puis, on convertit le fichier grâce à la commande :

```
# slaptest -f convert-schema.conf -F /schema/res
```

Quand cela fonctionne le système écrira, **config file testing succeded**.

On ouvre le fichier « /schema/res/cn=config/cn=schema/cn=0freeradius.ldif »et on remplace :

FIGURE 4.36 – Le fichier cn={0}freeradius.ldif avant modification.

par :

FIGURE 4.37 – Le fichier cn={0}freeradius.ldif après modification.

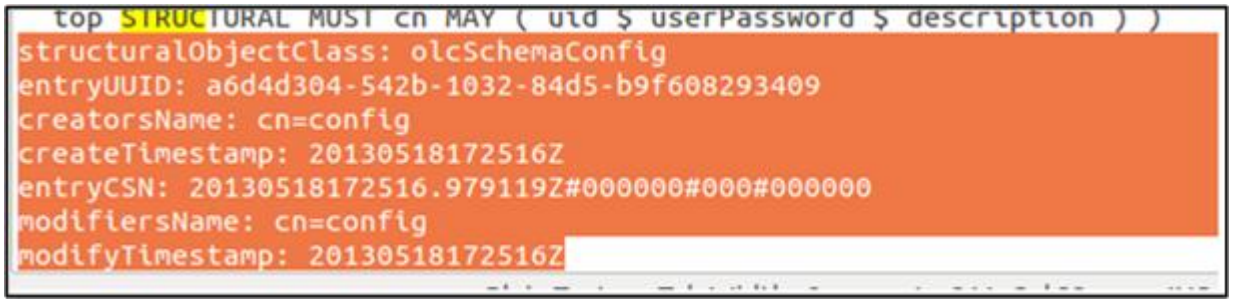

FIGURE 4.38 – Les lignes à supprimer du fichier cn={0}freeradius.ldif.

Puis on supprime les lignes suivantes à la fin du fichier :

Enfin, on importe le fichier freeradius.ldif dans OpenLDAP grâce à la commande :

```
# ldapadd -Y EXTERNAL -H ldapi:/// -f /schema/res/cn=config/cn=schema
  /cn=\{\0\}freeradius.ldif
```

Annexe B : Configuration d'un poste client cas Windows

Pour chaque utilisateur voulant se connecter à notre réseau sécurisé 802.11, la configuration de leur connexion réseau et/ou installer un client 802.1x sont nécessaires.

Sélectionner le réseau puis cliquez sur propriétés, s'il n'existe pas dans la liste ajouter-le, ensuite continuer la configuration en cliquant sur propriétés.

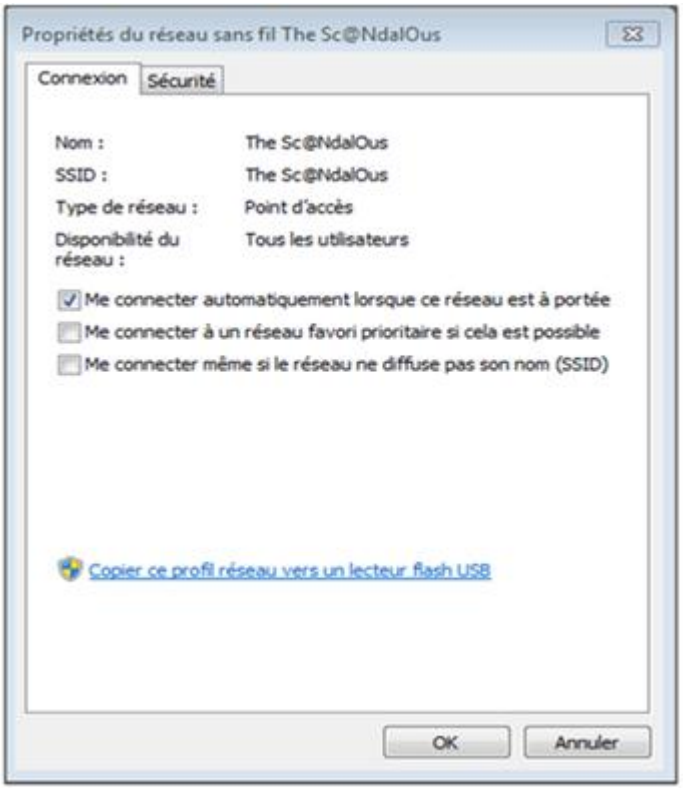

FIGURE 4.39 – propriétés du réseau sans fil.

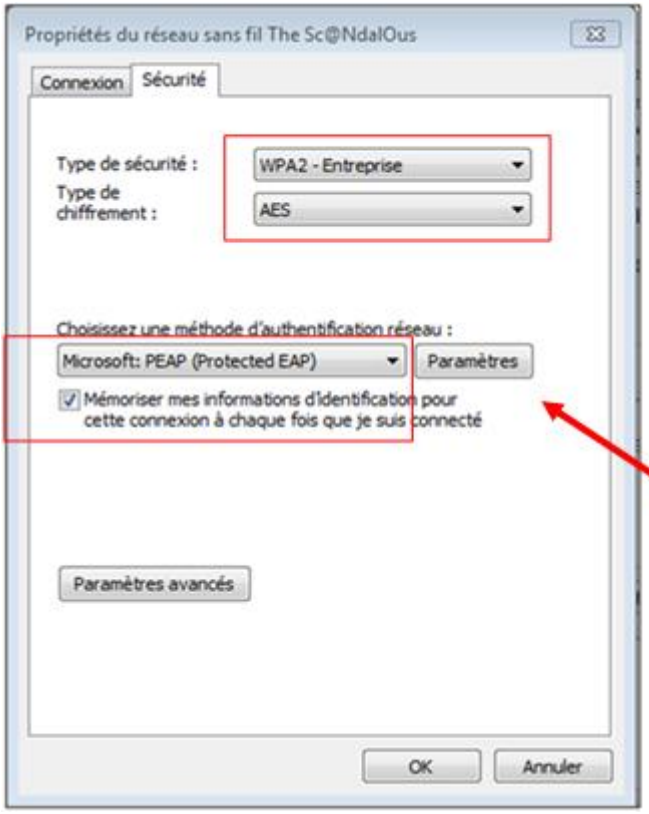

FIGURE 4.40 – Changement du type de sécurité a WPA2-Entreprise.

Dans l'onglet sécurité, on change le type de sécurité en WPA2-Entreprise avec la type de chiffrement AES. On sélectionne PEAP comme type d'EAP et on édite ses propriétés.

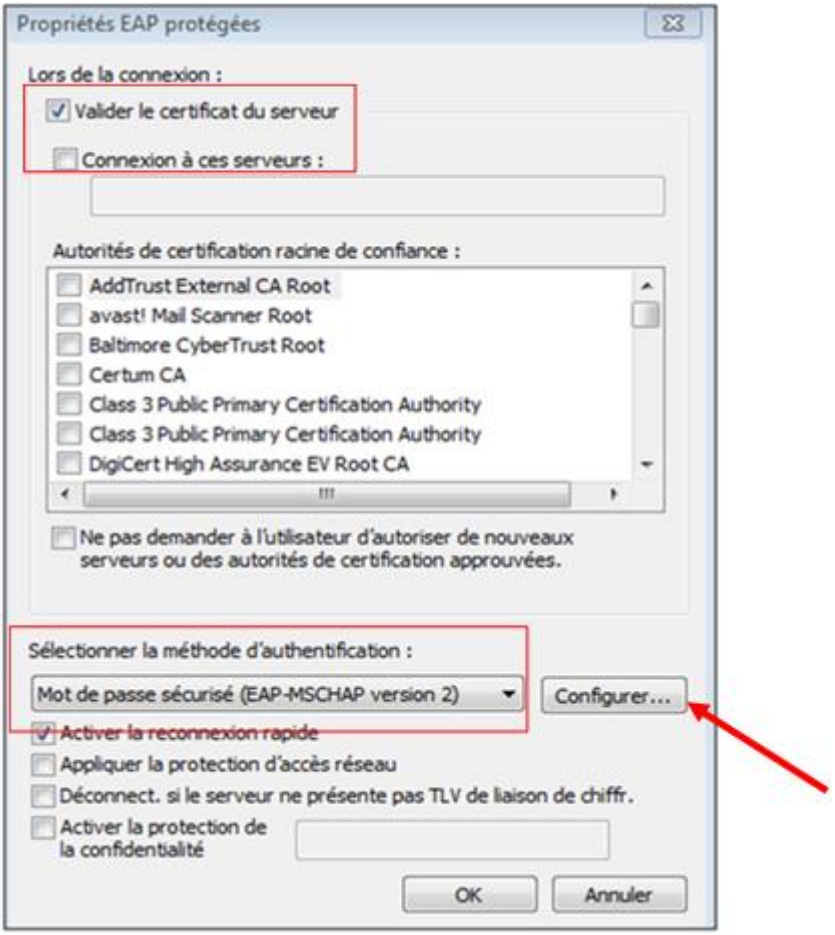

FIGURE 4.41 – Propriétés EAP protégées.

En décochant cette case, une fenêtre d'authentification s'ouvrira lors de la connexion. Etape importante pour spécifier un nom d'utilisateur différent que celui de windows.

FIGURE 4.42 – Propriétés EAP MSCHAPv2.

On sélectionne la méthode d'authentification « EAP-MSCHAP v2 »et on édite sa configuration.

Annexe C : Configuration d'un poste client Linux

Sous les systèmes d'exploitation GNU/linux, il faut utiliser un client d'authentification 802.1x tel que le client « Xsupplicant »qui est un outil open source, téléchargeable depuis son lien suivant : http ://open1x.sourceforge.net/. Ce client supporte tous les types d'authentification EAP actuellement existants (EAP-PEAP inclus).

Après une installation classique, le fichier exécutable Xsupplicant se trouve dans« /usr/local/sbin », le fichier de configuration xsupplicant.conf dans « /etc/ ». C'est dans ce fichier de configuration qu'il faut indiquer le répertoire contenant les certificats (ceux de l'utilisateur et de l'autorité), indiquer son nom d'utilisateur et son mot de passe en fonction de la méthode EAP choisie.

Bibliographie

[1] G.Pujolle, Les réseaux 2008, 6 Edition EYROLLES

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

[4] IEEE 802.15.1, Standard for Information technology-Telecommunications and information exchange bet-ween systems- Local and metropolitan area networks-Specific requirements Part 15.1 : Wireless medium access control (MAC) and physical layer (PHY) specifications for wireless personal area networks (WPANs). New York, 2002, http ://grouper.ieee.org/groups/802/15/.

[5] IEEE 802.16, SIEEE Standard 802.16-2004 : IEEE Standard for Local and Metropolitan Area Networks - Part 16 : Air Interface for Fixed Broadband Wireless Access Systems. New York, 2004, http ://grouper.ieee.org/groups/802/16/.

[6] 802.11 Draft Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specication. New York, 1997.

[7] ETHERNET WORKING GROUP, IEEE 802.3, http ://ieee802.org/3/.

[8] Sécurité informatique, Wi-Fi, http ://www.securite-informatique.gouv.fr/gp_article88.html, 2007.

[9] S. Corson and J. Macker, Mobile Ad hoc Networking (MANET) : Routing Protocol Performance Issues and Evaluation Considerations. Internet Request for Comments RFC 2501 Internet Engineering Task Force(IETF), 1999.

[10] CERTA, Sécurité des réseaux sans fil (Wi-Fi), 2008, http ://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-002/index.html.

[11] Mme Claire, Sondès LARAFA, Services AAA dans les réseaux ad hoc mobiles, 2012, Thèse de doctorat de Télécom SudParis.

[12] Espace Numérique Entreprises - Direccte Rhône-Alpes, Sécurité des Systèmes d'Information, 2010, http ://www.lamelee.com/les-ressources/securite-de-linformation/securite-des-systemes-dinformation/details.html.

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

[14] B.Fraser, Site Security Handbook Request For Comment 2196, 1997.

[15] Bruce schneier, Cryptographie appliquée, algorithmes, protocoles et codes sources en C, Vuibert, 1997.

[16] Bruno DUPORT, Les réseaux sans fil (WiFi), Edition Techni.Cités, 2004.

[17] Michel Riguidel, La sécurité des réseaux et des systèmes, ENST Paris, 2007.

[18] AAA-WG, Authentication, Authorization and Accounting, 2011, http ://datatracker.ietf.org/wg/aaa/charter.

[19] C.Rigney, S. Willens, A. Rubenset W.Simpson, Remote Authen-tication Dial In User Service (RADIUS) RFC 2865, IETF, 2000.

[20] CISCO Systems, CCNA Accès au réseau étendu, 2008.

[21] Jean Viale, Les services basés sur la signature électronique. LETTRE, 2002.

[22] Refik Molva, Yves Roudier, Authentification, EURECOM.

[23] Cisco System, TACACS+ and RADIUS Comparison, 2008, http ://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.html.

[24] Tarik BOUDJEMAA, Sadek YAHIAOUI, Sécurisation des systèmes, 2008.

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

[26] CERTA, Vulnérabilités dans certaines mises en oeuvre de WPA, 2008, http ://www.certa.ssi.gouv.fr/site/CERTA-2008-ACT-045/.

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

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

[29] W. Simpson, The Point-to-Point Protocol (PPP), http ://www.ietf.org/rfc/rfc1661.txt, 1994.

[30] B. Lloyd, W. Simpson, PPP Authentication Protocols, http ://www.ietf.org/rfc/rfc1334.txt, 1992.

[31] W. Simpson, PPP Challenge Handshake Authentication Protocol (CHAP), http ://www.ietf.org/rfc/rfc1994.txt, 1996.

[32] L. Blunk, J. Vollbrecht, PPP Extensible Authentication Protocol (EAP), http ://www.ietf.org/rfc/rfc2284.txt, 1998.

[33] La sécurité réseau, www.tri.on.ma.

[34] Authentification, régles et recomendation concernant les mécanismes d'authentification, 2010, Agence nationale de la sécurité des systèmes d'information.

[35] David ROUMANET, Nomadisme et sécurité sur les réseaux informatiques, Memoire d'ingénieur C.N.A.M. en informatique, 2005

[36] DEBAILLE Sébastien, VEROT Aubin, Réseaux privés virtuels, Travail d'étude et de recherche, 2005.

[37] Serge Bordères, Authentification réseau Radius, 3 Edition EYROLLES, 2006.

[38] M.Petitot, OpenSSL, 2012.

[39] Philippe Latu, Introduction aux annuaires LDAP, http ://www.inetdoc.net.

[40] Denoun Jérémy, De Daniloff Cyril,Bettan Michael, Authentification Centralisée LDAP / Radius, 2009.

[41] Laboratoires technique-info (IEPSCF-UCCLE), Serveur OpenLdap pour authentification de client Windows, 2011.

[42] Laboratoires technique-info (IEPSCF-UCCLE), Authentification forte auprés d'un serveur LDAP par la méthode SASL kerberos, 2004.

[43] CLEMENÇON Maxime, JUANEDA Matthieu, KERGADALLAN Guillaume, Authentification nomade, 2010.

[44] Amyn Bennamane, Le protocole SSL, 2009.

[45] D.Folio, Introduction aux annuaires LDAP avec OpenLDAP, http ://dfolio.free.fr/wiki/Crypto/OpenSSL, 2013.

[46] Marcel Rizcallah, LDAP, 2007, 2 Edition EYROLLES.

[47] Aurélien Géron, freeradius, 2011.

[48] Georges Charpenay, PfSense, 2009, http ://www.info.lesbarques.fr/spip.php ?article123.

[49] Anthony COSTANZO, Damien GRILLAT, Lylian LEFRANCOIS, Etude des principaux services fournis par PfSense, 2009, http ://www.pfSense.org.

[50] Richard E.smith, Authentification, 2001, http :// www.cryptosmith.com/doc/authento1.pdf.

Résumé

Le réseau Wifi constitue de plus en plus la technologie qui s'est imposée par excellence ces dernières années, permettant aux utilisateurs un accès à Internet ou au réseau local sans contrainte d'immobilité liée aux câblages. Bien que cette technologie semble aux premiers abords parfaite et sans soucis, la réalité est plus dure, due à l'absence de support physique de transmission, ce qui pose un problème évident de sécurité. Malgré ces défauts, le Wifi continu et continuera à se développer, sur ce, il s'avère donc essentiel de connaître les ressources à protéger et ainsi maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information.

Le but de notre projet de fin d'études consiste justement à étudier et analyser les solutions pour en choisir et déployer la plus efficace pour sécuriser le réseau sans fil de l'Université de Béjaia. Dans cette optique, nous avons donc étudié le réseau Wi-Fi standardisé, avec son fonctionnement ainsi que ses mécanismes de sécurité. Nous avons ensuite opté pour l'utilisation d'un serveur RADIUS utilisant le protocole 801.1x pour l'authentification des utilisateurs avec comme méthode d'authentification PEAP. Cette dernière, associée à un cryptage WPA2. L'authentification des utilisateurs se fait à travers un portail captif inclus dans un serveur pfsense qui joue le rôle d'un authentificateur. Le travail mis en place un système sécurisé en restant compatible avec les différentes technologies existantes, tout en tenant compte de la durabilité, l'évolution et la fiabilité de cette solution, assez bien en termes techniques qu'économiques. **Mot clés :** WiFi, AAA, Sécurité, 802.1x, RADIUS.

Abstract

The wireless network becomes the technology of choice, that is more and more used these last years, allowing users to have access to Internet or local network without stress of immobility related to wiring. Although this technology seems perfect and carefree, reality is different, due to the lack of physical transmission means, which poses an obvious security problem. Despite these defects, Wi-Fi continues and will continue to expand, so it is essential to know the resources to protect and thus manage access control and the rights of users of the information system.

The aim of our project graduation is precisely to study and analyze the solutions in order to select and deploy the most effective way to secure the wireless network at the University of Bejaia. In this context, we studied the standardized Wi-Fi network with its operation and security mechanisms. Then, we decided to use a RADIUS server using 801.1x protocol for user authentication with PEAP as the authentication method. The latter, combined with WPA2 encryption. User authentication is done through a captive portal included in pfsense server that acts as an authenticator. The work established a secure system, which still compatible with the various existing technologies and taking into account sustainability, development and reliability of this solution on the technical and economic terms. **Key words :** WiFi, AAA, Security, 802.1x, RADIUS.