

RÉPUBLIQUE ALGÉRIENNE DÉMOCRATIQUE ET POPULAIRE MINISTÈRE  
DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE SCIENTIFIQUE  
UNIVERSITÉ A.MIRA-BEJAIA  
FACULTÉ DES SCIENCES EXACTES  
DÉPARTEMENT INFORMATIQUE



MÉMOIRE DE FIN DE CYCLE

En vue de l'obtention du  
Diplôme de Master professionnel en Informatique  
Option: Administration et sécurité des réseaux

## Thème

---

# Mise en place d'un Serveur d'authentification RADIUS Sous Gns3 Cas : EPB de Bejaia

---

Encadreur : M<sup>me</sup> khaled Hayette

Présenté par :

M<sup>lle</sup> kaddouh Adada

M<sup>r</sup> Belhocine Fayçal

Devant le jury composé de :

Présidente M<sup>me</sup> Ouazine Kahina

Examinatrice M<sup>me</sup> Zidani Ferroudja

Année Universitaire : 2020-2021

# Remerciements

*Avant tout, Il semble approprié d'entamer ce mémoire par des remerciements, d'abord au bon dieu de nous avoir accordé la force et le courage de mener à terme ce modeste travail.*

*Toute notre reconnaissance et toute notre gratitude vont vers Mme khaled hayatte, notre promotrice, qui nous a aidé et accompagné tout au long de cette expérience professionnelle avec beaucoup de patience et d'enthousiasme.*

*Un grand merci pour l'organisme d'accueil EPB, qui nous a accepté comme stagiaires et qui nous a donné une chance pour découvrir le domaine professionnel.*

*Nous remercions également les membres du jury d'avoir accepté d'examiner et de juger notre travail.*

*Que tous ceux qui, de près ou de loin ont contribué, par leurs conseils, leurs encouragements ou leur amitié à l'aboutissement de ce travail, trouvent ici l'expression de notre profonde reconnaissance.*

*Pour leur encouragement, leur soutien moral et la patience qu'ils nous ont manifestée durant toute l'année .*

*Nous remercions fortement tous les membres de nos familles.*

*Enfin remercier nos parents serait se répéter, parfois pour exprimer plus que ce qu'on a envie de dire on a recours au silence.*

## *Dédicaces*

*A l'aide de DIEU tout puissant, qui trace le chemin de ma vie, j'ai pu arriver à réaliser ce modeste travail que je dédie :*

*A 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 .*

*A 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 en très bonne santé .*

*A la mémoire de mes grands parents Saliha et Hocine .*

*A mes tantes et mes oncles .*

*A ma sœur Souhila a qui je souhaite tout le bonheur dans sa vie .*

*A tous mes cousins et cousines .*

*A ma meilleure amie "A.Ryma" pour son soutien durant toutes ces années .*

*A mes enseignants pour leurs patience, leurs soutien, leurs encouragements et à mes amis pour leur témoigner une amitié et fidélité indéfinies.*

*A ma binôme Adada , je lui souhaite une réussite dans sa vie .*

*A tous les étudiants en 2eme master informatique de l'université de Béjaia .*

*Fayçal*

## *Dédicaces*

*A l'aide de DIEU tout puissant, qui trace le chemin de ma vie, j'ai pu arriver à réaliser ce modeste travail que je dédie :*

*A L'homme de ma vie, mon exemple étendu, mon soutien moral et ma source de joie et de bonheur. A celui qui s'est toujours sacrifier pour me voir réussir, qui éclair mon chemin et m'illumine de douceur et de l'amour, que dieu te garde pour nous papa.*

*A ma plus belle Etoile qui puisse exister dans l'univers ma très chère maman en signe d'amour, de reconnaissance et de gratitude pour tout le soutien et les sacrifices dont elle a fait preuve à mon égard.*

*A mes chères frères « Mohammed » et « Aissa » et ma petite sœur « Hassina ».*

*A mes grand-mères que dieu les protèges.*

*A mon soutien moral et source de joie et de bonheur, mon chère amour « Hamza » pour l'encouragement qu'il m'a toujours accordé.*

*A tous les membres de ma famille : tante, oncle, cousin maternelle et paternelle.*

*A ceux que j'aime beaucoup ,qui m'ont toujours soutenus et étaient toujours à mes côté ,mes chères amis spécialement :Nassima ,Ouissam ,Nadjet ,Wissam ,Sara ,Mila ,Lila ,Lynda ,Kahina ,Léa , Ryma, Amel ,Rania ,Thiziri et Tinhinane .*

*Je termine avec la personne qui a partagé tous le travail, mon binôme « Fayçal » et sa famille.*

*Et à tous ceux qui ont contribué de près ou de loin pour que ce projet soit possible, je vous dis merci.*

*Adada*

# Table de matière

<b>Table des figures</b>	<b>IV</b>
<b>Glossaire</b>	<b>V</b>
<b>Introduction générale</b>	<b>1</b>
<b>1 Généralités sur les réseaux et la sécurité informatique</b>	<b>3</b>
1.1 Introduction . . . . .	4
1.2 Définition d'un réseau informatique . . . . .	4
1.3 Modèle OSI . . . . .	4
1.4 Modèle Client/serveur . . . . .	6
1.4.1 Présentation de l'architecture Client/serveur . . . . .	6
1.4.2 Fonctionnement d'un système Client /serveur . . . . .	6
1.5 Sécurité Informatique . . . . .	6
1.5.1 Critères de la sécurité . . . . .	7
1.6 Outils et systèmes d'authentification . . . . .	7
1.6.1 Quelques définitions . . . . .	8
1.7 Méthodes de protection . . . . .	10
1.7.1 Cryptographie . . . . .	10
1.7.2 Firewall (pare-feu) . . . . .	11
1.8 Certificats . . . . .	11
1.9 Conclusion . . . . .	12
<b>2 Présentation de l'organisme d'accueil</b>	<b>13</b>
2.1 Introduction . . . . .	14
2.2 Présentation de l'organisme d'accueil . . . . .	14
2.3 Organigramme de l'EPB . . . . .	15
2.4 Direction des Systèmes d'Information (DSI) . . . . .	16
2.4.1 Présentation de la DSI . . . . .	16
2.4.2 Missions . . . . .	16
2.4.3 Organisation humaine de la direction des systèmes d'infor- mation . . . . .	16
2.5 Infrastructure informatique . . . . .	17
2.5.1 Réseau local de l'EPB . . . . .	18

2.6	Problématique . . . . .	18
2.7	Solution . . . . .	19
2.8	Conclusion . . . . .	20
<b>3</b>	<b>Serveur d'authentification Radius</b>	<b>21</b>
3.1	Introduction . . . . .	22
3.2	Protocole Radius . . . . .	22
3.2.1	Fonctionnement de Radius . . . . .	22
3.2.2	Format de l'en-tête du paquet Radius . . . . .	24
3.2.3	Rôles de protocole Radius . . . . .	24
3.2.4	Caractéristiques de Radius . . . . .	24
3.2.5	Avantages du Radius . . . . .	25
3.2.6	Protocole Radius et la couche de transport UDP . . . . .	25
3.2.7	Éléments d'authentification Radius . . . . .	26
3.3	Protocole 802.1x . . . . .	28
3.3.1	Composants 802.1x . . . . .	29
3.3.2	Étapes d'authentification 802.1X . . . . .	29
3.3.3	Protocole EAP . . . . .	30
3.4	Conclusion . . . . .	31
<b>4</b>	<b>Mise en œuvre et réalisation</b>	<b>32</b>
4.1	Introduction . . . . .	33
4.2	Composantes utilisées . . . . .	33
4.3	Présentation des outils utilisés . . . . .	33
4.3.1	Logiciel GNS3 . . . . .	33
4.3.2	VM WARE Workstation 15 pro . . . . .	33
4.3.3	Wireshark . . . . .	34
4.3.4	Windows server 2016 . . . . .	34
4.4	Configuration du serveur Radius . . . . .	34
4.4.1	Création du contrôleur de domaine et DNS . . . . .	34
4.4.2	Installation et configuration du service DHCP . . . . .	39
4.4.3	Mise en œuvre de l'autorité de certification Active . . . . .	42
4.4.4	Installation du service "Network Policy and Access Services"(Services de Stratégie Et d'accès réseau) . . . . .	43
4.4.5	Configuration de serveur . . . . .	50
4.4.6	Activè Radius dans pare-feu « Pfsense » . . . . .	51
4.5	Configuration de client d'accès (Windows 10) . . . . .	53
4.6	Présentation de l'architecture réseau . . . . .	55
4.6.1	Configuration de la partie réseau . . . . .	55
4.7	Tests . . . . .	60
4.8	Conclusion . . . . .	66
	<b>Conclusion Générale</b>	<b>67</b>
	<b>Bibliographie</b>	<b>69</b>

# Table des figures

1.1	Les couches du modèle OSI . . . . .	5
1.2	Modèle client /serveur . . . . .	6
1.3	Critères de la sécurité . . . . .	7
1.4	Cryptage Symétrique . . . . .	10
1.5	Cryptage Asymétrique . . . . .	11
1.6	Le principe de fonctionnement d'un par feu . . . . .	11
2.1	Organigramme générale de l'EPB. . . . .	15
2.2	Missions du système d'information de l'EPB. . . . .	16
2.3	Organigramme de la Direction des Systèmes d'Information. . . . .	17
2.4	Réseau fibre optique de l'EPB. . . . .	17
2.5	L'architecture du réseau LAN de l'entreprise EPB. . . . .	18
2.6	Comparaison entre Radius , Diameter et Tacacs+ . . . . .	19
3.1	Architecture Radius . . . . .	23
3.2	En-tête du paquet Radius. . . . .	24
3.3	principes de l'authentification Radius-MAC . . . . .	26
3.4	principe d'authentification 802.1X . . . . .	27
3.5	État du port avant la phase d'authentification . . . . .	28
3.6	État du port après une authentification réussie . . . . .	28
3.7	Composants 802.1x. . . . .	29
3.8	Processus d'authentification. . . . .	30
4.1	La fenêtre principale du VMware. . . . .	34
4.2	Ajout du service AD DS et serveur. . . . .	35
4.3	Promouvoir le serveur en contrôleur de domaine. . . . .	35
4.4	Création du domaine« EPB.local ». . . . .	36
4.5	Niveau fonctionnel de la forêt et du domaine. . . . .	36
4.6	Nom NetBIOS de domaine. . . . .	37
4.7	l'emplacement des fichiers Active Directory. . . . .	37
4.8	Ouverture de la session Administrateur. . . . .	38
4.9	Création de groupe G-Radius. . . . .	38
4.10	Création d'un utilisateur. . . . .	38
4.11	Introduction de mot de passe d'utilisateur. . . . .	39
4.12	Membres du groupe-Radius. . . . .	39
4.13	Ajout du serveur DHCP. . . . .	40

---

TABLE DES FIGURES

---

4.14	Installation du serveur DHCP. . . . .	40
4.15	Autorisation du serveur DHCP dans les services AD DS. . . . .	41
4.16	Plage d'adresse allouée aux machines clientes. . . . .	41
4.17	Ajout d'exclusion DHCP. . . . .	41
4.18	Ajout de l'adresse IP du pare-feu. . . . .	42
4.19	Ajout du nom de domaine serveur DNS. . . . .	42
4.20	Ajout des services de certificats Active Directory. . . . .	43
4.21	Configuration d'une PKI. . . . .	43
4.22	Ajout des services de stratégie et d'accès réseau. . . . .	44
4.23	Inscription du serveur NPS dans le domaine. . . . .	45
4.24	Création du client Radius. . . . .	45
4.25	Sélection d'un scénario de configuration. . . . .	46
4.26	Type de connexion 802.1X. . . . .	46
4.27	Ajout de client Radius. . . . .	47
4.28	Type de protocole pour cette stratégie. . . . .	47
4.29	Spécification de groupe d'utilisateurs pour la connexion 802.1x câblée. . . . .	47
4.30	Configuration des conditions de cette stratégie réseau. . . . .	48
4.31	Choix des méthodes d'authentification. . . . .	48
4.32	Ajout d'attributs Radius. . . . .	49
4.33	Configuration des conditions de cette stratégie réseau. . . . .	49
4.34	Choix des méthodes d'authentification. . . . .	50
4.35	Ajout d'attributs Radius. . . . .	50
4.36	Attribution d'une adresse statique au serveur. . . . .	51
4.37	Configuration l'authentification du serveur Radius. . . . .	51
4.38	Configuration autorisation active du groupe d'annuaires. . . . .	52
4.39	Activer l'authentification du répertoire. . . . .	52
4.40	Démarrage de service " Configuration automatique de réseau câblé". . . . .	53
4.41	Activation de l'authentification 802.1x. . . . .	54
4.42	Sélection de méthode d'authentification " EAP-MSCHAP v2 ". . . . .	54
4.43	Ajout de la machine au domaine. . . . .	55
4.44	Architecture du réseau proposé. . . . .	55
4.45	Tableau d'adressage . . . . .	56
4.46	console du pare-feu après insertion de nos adresses. . . . .	56
4.47	Ajout de la carte réseau coté serveur sur pare-feu. . . . .	57
4.48	Configuration de l'interface vlan 1. . . . .	57
4.49	Activer le modèle AAA. . . . .	57
4.50	Authentification. . . . .	58
4.51	Autorisation d'accès au réseau. . . . .	58
4.52	Activation du protocole 802.1x sur Client Radius. . . . .	58
4.53	Configuration de l'adresse IP de serveur Radius. . . . .	59
4.54	Activation du protocole 802.1x sur le port de l'utilisateur. . . . .	59
4.55	Authentification Radius. . . . .	59
4.56	Activer le protocole SSH. . . . .	60
4.57	Wireshark sous GNS3. . . . .	60
4.58	Analyse de la conversation entre switch et serveur. . . . .	61
4.59	Test d'authentification d'un utilisateur. . . . .	62
4.60	Traçabilité de l'utilisateur connecté au serveur Radius. . . . .	62



---

## TABLE DES FIGURES

---

4.61	Vérification d'adresse IP de la machine Windows 10. . . . .	63
4.62	L'accès au switch avec un client SSH. . . . .	63
4.63	L'accès au switch avec mot de passe . . . . .	64
4.64	L'accès au switch avec un client SSH. . . . .	64
4.65	L'accès au switch avec password. . . . .	65
4.66	Succès de L'authentification du serveur PFSense Radius sur Active Directory. . . . .	65

# Glossaire

## A

---

**AAA** : Authentication Authorization Accounting.

**AD** : Active Directory.

## C

---

**CA** : Certification Authority.

**CHAP** : Challenge Handshake Authentication Protocol.

**CNAN** : Compagnie Nationale Algérienne de Navigation.

## D

---

**DHCP** : Dynamic Host Configuration Protocol.

**DNS** : Domain Name Server.

**Dos** : Denial of Service .

**DSI** : Direction des Systèmes d'Information.

**E**

---

**EAP** : Extensible Authentication Protocol.

**EAP-FAST** : Extensible Authentication Protocol- Flexible Authentication via Secure Tunneling.

**EAP-MD5** : Extensible Authentication Protocol Message Digest 5.

**EAPOL** : Extensible Authentication Protocol Over Lan.

**EAPOR** : Extensible Authentication Protocol over RADIUS .

**EAP-TLS** : Extensible Authentication Protocol- Transport Layer Security.

**EAP-TTLS** : Extensible Authentication Protocol -Tunneled Transport Layer.

**EPB** : l'Entreprise Portuaire de Bejaïa.

**G**

---

**GNS3** : Graphical Network System 3.

**I**

---

**ID** : Identifiant.

**IETF** : Internet Engineering Task Force.

**IOS** : Internetwork Operating System.

**IP** : Internet Protocol.

**L**

---

**LAN** : Local Area Network.

---

**LDAP** : lightweight Directory Access Protocol.

**M**

---

**MAC** : Media Access Control.

**MS-CHAP** : Microsoft Challenge Handshake Authentication Protocol.

**MS-CHAPv2** : Microsoft Challenge Handshake Authentication Protocol Version 2.

**N**

---

**NAS** : Network Access Server.

**NPS** : Network Policy Server.

**NetBIOS** : Network Basic Input Output System.

**O**

---

**ONP** : Office National des Ports .

**OSI** : Open Systems Interconnexion.

**P**

---

**PAP** : Password Authentication Protocol.

**PEAP** : Protected Extensible Authentication Protocol.

**PKI** : Public Key Infrastructure.

**PPP** : Point to Point Protocol.

**R**

---

**RADIUS** : Remote Access Dial In User Service.

**RFC** : Request For Comment.

**S**

---

**SI** : Système d'information.

**SO.NA.MA** : Société Nationale de Manutention.

**SSH** : Secure shell.

**SYSVOL** : Système Volume.

**T**

---

**TCP** : Transmission Control Protocol.

**TTLS** : Tunneled Transport Layer Security.

**U**

---

**UDP** : User Datagram Protocol.

**V**

---

**VLAN** : Virtual Local Area Network.

**VM** : Virtuelles Machines.

**VPN** : Virtuel Private Network.

**W**

---

**WAN** : Wide Area Network.

**WiFi** : Wireless Fidelity.

**WPA** : Wi-Fi Protected Access.

# Introduction générale

Les réseaux informatiques sont un ensemble d'équipements reliés entre eux pour échanger des informations. Ils ont fait irruption dans le quotidien des entreprises permettant ainsi une amélioration des services qui y sont offerts. Entre autres : le partage de ressources, la gestion centralisée de ces ressources ainsi qu'une meilleure circulation des informations au sein de l'entreprise.

Les réseaux informatiques sont à l'origine de la révolution de la communication et à l'émergence d'une société multimédia. Ils sont la conséquence d'un partage équitable des ressources technologiques.

L'information recherchée sur les réseaux de communication doit être localisée très rapidement et dans son intégralité. Ainsi pour bénéficier des grands avantages que l'interconnexion des réseaux apporte, de plus en plus d'entreprises ouvrent leurs systèmes d'informations à leurs partenaires ou leurs fournisseurs afin de satisfaire leurs besoins en matière d'échange d'information et faire face aux insuffisances de l'utilisation des réseaux locaux en termes de communication.

Dans ce cas, lorsque la sécurité d'un réseau est compromise, de très graves conséquences peuvent en résulter, comme l'atteinte à la vie privée, le vol d'informations et même l'engagement de la responsabilité civile.

Pour rendre cette situation encore plus difficile, les types de menaces potentielles sont en évolution constante. De plus, la difficulté que représente la sécurité dans son ensemble est de trouver un compromis entre deux besoins essentiels : le besoin d'ouvrir des réseaux pour profiter de nouvelles opportunités commerciales et le besoin de protéger des informations privées ou publiques et des informations stratégiques.

Pour cela la sécurité se place actuellement au premier plan de la mise en œuvre et de l'administration réseau. L'application d'une stratégie de sécurité efficace est l'étape la plus importante qu'une entreprise doit franchir pour protéger son réseau. Faisant partie de cette stratégie de sécurisation, le contrôle de l'accès physique au réseau s'avère une opération efficace pour limiter les possibilités d'accès au réseau des entités non désirées. L'un des moyens pour réaliser ce contrôle est l'authentification des utilisateurs et l'application de droits utilisateurs.

Notre objectif dans ce projet est de mettre en place une solution d'authentification permettant de sécuriser l'accès des utilisateurs au réseau de l'Entreprise EBP de Bejaia.

Notre mémoire est organisé en quatre chapitres : Le premier consiste à définir les notions de bases des réseaux informatiques. Le deuxième porte sur la présentation d'organisme d'accueil EBP avec la problématique posée de son réseau ainsi que la solution proposée pour la résoudre. Le troisième chapitre a pour but d'étudier la solution proposée pour l'entreprise en se basant sur la présentation de protocole d'authentification Radius, ses principes son fonctionnement, ainsi que les protocoles sur lesquels il est épaulé, tel que la norme 802.1X et le standard EAP. Le quatrième chapitre est consacré à la mise en œuvre de service d'authentification Radius pour le réseau d'EPB de Bejaia. On présente les différents moyens et outils déployés pour l'implémentation de cette solution (Windows server 2016, l'annuaire Active Directory, le simulateur GNS3,...), ainsi les étapes de configuration mises en place pour pouvoir tester l'authentification des utilisateurs par le mécanisme de sécurité retenu.

Nous terminerons par une conclusion générale en décrivant les éléments essentiels qui ont été développés dans ce mémoire, et quelques perspectives pour ce projet.



Chapitre **1**

# Généralités sur les réseaux et la sécurité informatique

## 1.1 Introduction

De nos jours, Le monde connaît des avancées très significatives dans le domaine informatique, les besoins en matière de sécurité sont un peu plus impérieux, et la prédisposition n'est forcément pas à la baisse. Depuis quelques années, on participe à un changement constant des techniques, qu'il s'agisse des techniques visant à sécuriser l'échange des données ou des techniques de mise au point pour contourner les systèmes sécurisés. D'où, la sécurité des données tend à s'améliorer. Et comme prône ce proverbe chinois : « l'art de la guerre est basé sur la tromperie », de même par analogie, la sécurité informatique doit représenter une stratégie qui éradique cette tromperie.

Le besoin de communication et de partage a poussé les entreprises à s'orienter vers les réseaux informatiques et travailler d'avantage pour les améliorer et pour les sécuriser.

La sécurité consiste à assurer que les ressources matérielles ou logicielles d'une organisation soient uniquement utilisées dans le cadre prévu.

Ce chapitre a pour objectif de comprendre les notions de base sur les réseaux informatiques . Nous allons montrer les moyens et les dispositifs de sécurité utilisés pour l'assurer afin de bien maîtriser notre sujet.

## 1.2 Définition d'un réseau informatique

Un réseau informatique est un ensemble d'équipement informatiques (ordinateur et périphériques) reliés entre eux grâce à des supports de communication (câble : réseau câblé, ou onde : réseau sans fil..) permettant la communication (transfert des informations électroniques) et le partage de ressources (matérielles et logicielles).

## 1.3 Modèle OSI

Le modèle OSI est un modèle conceptuel créé par l'Organisation internationale de normalisation qui permet à divers systèmes de communication de communiquer à l'aide de protocoles standard .En clair, l'OSI fournit une norme pour que différents systèmes informatiques communiquent entre eux.

Le modèle OSI peut être considéré comme un langage universel pour les réseaux informatiques .Il est basé sur un concept consistant à diviser un système de communication en sept couches abstraites, empilées les unes sur les autres [1]. (voir la figure 1.1)

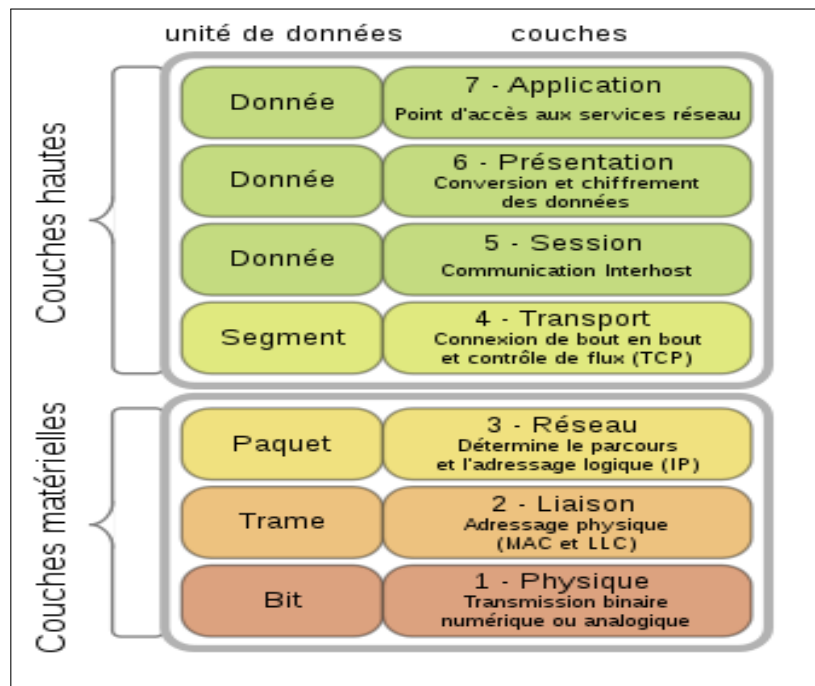


FIGURE 1.1 – Les couches du modèle OSI [1].

#### Les 7 couches du modèle OSI :

1. **La couche « physique »** : est chargée de la transmission effective des signaux entre les interlocuteurs.
2. **La couche « liaison de données »** : gère les communications entre deux machines directement connectées entre elles, ou connectées à un équipement qui émule une connexion directe (commutateur).
3. **La couche « réseau »** : gère les communications de proche en proche, généralement entre machines : routage et adressage des paquets.
4. **La couche « transport »** : gère les communications de bout en bout entre processus (programmes en cours d'exécution) .Cette fonction est réalisée par les protocoles TCP (Transmission Control Protocol) et UDP (User Datagram Protocol) de la famille des protocoles TCP/IP.
5. **La couche « session »** : gère la synchronisation des échanges et les « transactions », permet l'ouverture et la fermeture de session.
6. **La couche « présentation »** : est chargée du codage des données applicatives, précisément de la conversion entre données manipulées au niveau applicatif et chaînes d'octets effectivement transmises.
7. **La couche « application »** : est le point d'accès aux services réseaux, elle n'a pas de service propre spécifique et entrant dans la portée de la norme [1].

## 1.4 Modèle Client/serveur

Le modèle client-serveur s'articule autour d'un réseau auquel sont connectés deux types d'ordinateurs : le serveur et le client. Le client et le serveur communiquent via des protocoles. Les applications et les données sont réparties entre le client et le serveur de manière à réduire les coûts. Le client-serveur représente un dialogue entre deux processus informatiques par l'intermédiaire d'un échange de messages. Le processus client soustrait au processus serveur des services à réaliser [2].

### 1.4.1 Présentation de l'architecture Client/serveur

L'architecture client/serveur désigne un modèle de communication entre plusieurs ordinateurs d'un réseau . Il distingue plusieurs postes clients qui contactent un serveur (une machine généralement très puissante en termes de capacités d'entrée/sortie) pour leur fournir des services. Ces services sont des programmes fournissant des données telles que l'heure, des fichiers, une connexion... Les services sont exploités par des programmes, appelés programmes clients, s'exécutant sur les machines clientes [2].

### 1.4.2 Fonctionnement d'un système Client /serveur

Un système client/serveur (figure 1.2) fonctionne selon le schéma suivant : Le client émet une requête vers le serveur grâce à son adresse IP et le port, qui désigne un service particulier du serveur. Le serveur reçoit la demande et répond à l'aide de l'adresse de la machine cliente et son port [2].

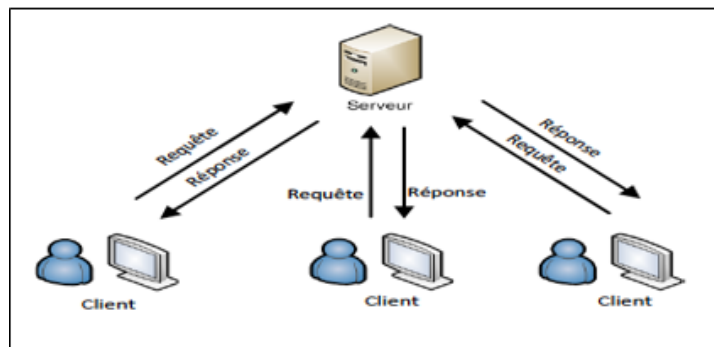


FIGURE 1.2 – Modèle client /serveur  
[2].

## 1.5 Sécurité Informatique

La sécurité informatique est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique. Elles caractérisent ce à quoi s'attendent les utilisateurs de systèmes informatiques en regard de la sécurité [3].

### 1.5.1 Critères de la sécurité

La figure 1.3 montre les différents critères de la sécurité :

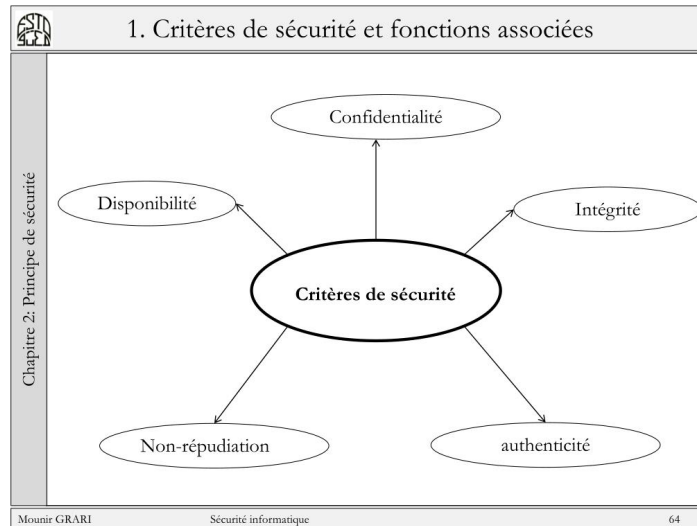


FIGURE 1.3 – Critères de la sécurité [4].

- **Intégrité** : le critère d'intégrité des ressources physiques et logiques (équipements, données, traitements, transactions et services) est relatif au fait qu'elles n'ont pas été détruites (altération totale) ou modifiées (altération partielle) à l'insu de leurs propriétaires tant de manière intentionnelle ou accidentelle [4].
- **Confidentialité** : la confidentialité des données peut être définie comme la protection des données contre une divulgation non autorisée [4].
- **Disponibilité** : le bon fonctionnement des services, systèmes et données doivent être accessibles aux ayants droits en continu sans interruption, sans retard, ni dégradation [4].
- **Non-répudiation** : c'est le fait de ne pas pouvoir nier qu'un événement (actions, transactions) a eu lieu [4].
- **Authentification** : doit permettre de vérifier l'identité d'une entité pour pouvoir assurer son authentification, ainsi seules les personnes autorisées auront accès aux ressources [4].

## 1.6 Outils et systèmes d'authentification

L'authentification pour un système informatique est un processus permettant au système de s'assurer de la légitimité de la demande d'accès faite par une entité (être humain ou un autre système) cela permet à cette entité d'accéder à des ressources du système conformément au paramétrage du contrôle d'accès.

### 1.6.1 Quelques définitions

Quelques définitions des éléments qu'on a utilisés :

#### A. Les annuaires

Un annuaire est une bibliothèque mise à jour régulièrement qui regroupe des informations (nom, adresse, coordonnées) sur les membres d'une association, d'une entreprise ou d'un organisme professionnel [5].

#### B. Active Directory

Active Directory est un annuaire système hiérarchique. Il permet de localiser, rechercher et gérer des ressources représentées par des objets de l'annuaire. Il offre des mécanismes de sécurité pour protéger ses informations. Il permet de gérer des ressources liées à la gestion du réseau (domaines, comptes utilisateurs, stratégies de sécurité etc. . . ). La base de données d'AD est distribuée, ce qui lui permet d'améliorer la tolérance aux pannes. Certains produits Microsoft sont installés par défaut (ou fortement conseillés lors de l'installation) comme : DNS serveur web. Active Directory centralise l'authentification. Le contrôle d'accès peut être défini à la fois sur chaque objet de l'annuaire [6].

#### C. Définition d'un domaine Windows

Un domaine est l'ensemble d'objets : ordinateurs, utilisateurs et groupes définis par un administrateur réseau. Ces objets partagent une base de données d'annuaire et des stratégies de sécurité [7].

#### D. Les protocoles d'authentification

Un protocole d'authentification est un moyen de contrôle d'accès.

##### 1. Protocole PAP « Password Authentication Protocol »

Le protocole PAP, comme son nom l'indique, est un protocole d'authentification par mot de passe. Il a été originellement utilisé dans le cadre du protocole PPP.

Son principe consiste à envoyer l'identifiant et le mot de passe en clair à travers le réseau. Si le mot de passe correspond, alors l'accès est autorisé [8].

##### 2. Protocole CHAP « Challenge Handshake Authentication Protocol »

Le protocole CHAP est un protocole d'authentification basé sur la résolution d'un défi, c'est-à-dire une séquence à chiffrer avec une clé et la comparaison de la séquence chiffrée ainsi envoyée. Les étapes du défi sont les suivantes :

- Un nombre aléatoire de 16 bits est envoyé au client par le serveur d'authentification, ainsi qu'un compteur incrémenté à chaque envoi.
- La machine distante hache ce nombre et le compteur ainsi que sa clé secrète (le mot de passe) avec l'algorithme de hachage MD5 et le renvoie sur le réseau.
- Le serveur d'authentification compare le résultat transmis par la machine distante avec le calcul effectué localement avec la clé secrète associée à l'utilisateur.

- Si les deux résultats sont égaux, alors l'identification réussit, sinon elle échoue [9].

3. **Protocole MS-CHAP « Microsoft Challenge Handshake Authentication Protocol »**

Microsoft a mis au point une version spécifique de CHAP, baptisée MS-CHAP version 1 «noté parfois MS-CHAP-v1», améliorant globalement la sécurité.

En effet, le protocole CHAP implique que l'ensemble des mots de passe des utilisateurs soient stockés en clair sur le serveur, ce qui constitue une vulnérabilité potentielle. Ainsi MS-CHAP propose une fonction de hachage propriétaire permettant de stocker un hash intermédiaire du mot de passe sur le serveur. Lorsque la machine distante répond au défi, elle doit ainsi hacher le mot de passe à l'aide de l'algorithme propriétaire. Le protocole MS-CHAP-v1 souffre malheureusement de failles de sécurité liées à des faiblesses de la fonction de hachage propriétaire [9].

4. **Protocole MS-CHAPv2 « Microsoft Challenge Handshake Authentication Protocol version 2 »**

La version 2 du protocole MS-CHAP Cette nouvelle version du protocole définit une méthode dite " authentication mutuelle ", permettant au serveur d'authentification et à la machine distante de vérifier leurs identités respectives [9].

5. **Protocole Radius (Remote Authentication Dial-In User Service)**

Le protocole Radius , mis au point initialement par Livingston, est un protocole d'authentification standard, défini par un certain nombre de RFC [14].

6. **Ethernet**

Ethernet désigne un protocole de réseau local (LAN). Celui-ci se base sur des commutations de paquets et sur des câbles en paires torsadées pour permettre de relier plusieurs machines entre elles [9].

E. **Serveur dhcp (Dynamic Host Configuration Protocol)**

Le serveur DHCP permet la gestion et la distribution des adresses IP dynamiquement à un ordinateur qui se connecte sur un réseau, son but principal étant la simplification de l'administration d'un réseau [25].

F. **Le serveur dns (Domain Name System)**

Le service DNS permet de faciliter et de standardiser le processus d'identification des ressources connectées aux réseaux informatiques, et il associe un nom à une adresse IP à chaque machine connectée au réseau [25].

G. **Politique de sécurité**

Une politique de sécurité informatique est une stratégie visant à maximiser la sécurité informatique d'une entreprise. Elle est matérialisée dans un document qui reprend l'ensemble des enjeux, objectifs, analyses, actions et procédures faisant parti de cette stratégie[24].

## 1.7 Méthodes de protection

Des messages se basent sur l'idée de brouiller le message de manière à le rendre incompréhensible et inintelligible pour l'attaquant.

### 1.7.1 Cryptographie

Les données qui peuvent être lues et comprises sans mesures spéciales sont appelées texte clair. Le procédé qui consiste à dissimuler du texte clair de façon à cacher sa substance est appelé cryptographie ou chiffrement. Le chiffrement des données fut inventé pour assurer la confidentialité des données. Il est assuré par un système de clé (algorithme) appliqué sur le message. Ce dernier est décryptable par une clé unique correspondant au cryptage [10].

#### A. Cryptage symétrique

La cryptographie symétrique (figure 1.4), également dite à clé secrète. Est la plus ancienne forme de chiffrement. Elle permet à la fois de chiffrer et de déchiffrer des messages à l'aide d'un même mot clé [10].

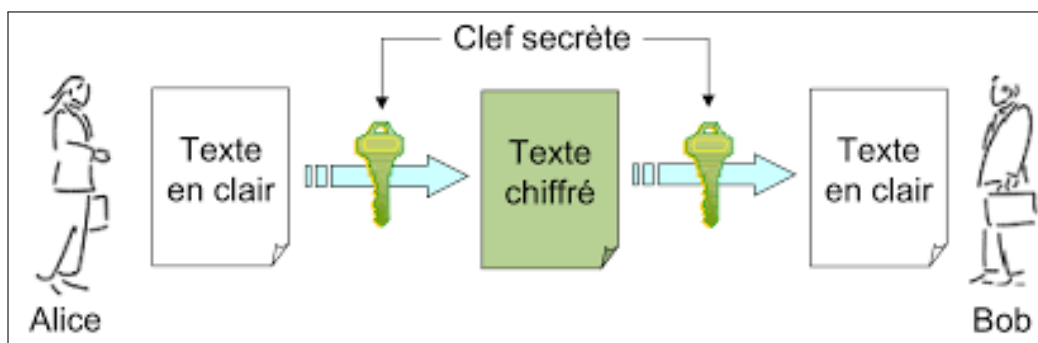


FIGURE 1.4 – Cryptage Symétrique [10].

#### B. Cryptage asymétrique

La cryptographie asymétrique (figure 1.5) est utilisée pour protéger des fichiers, des registres et des disques entiers contre les accès non autorisés ainsi que pour échanger des messages secrets. Pour cela, on utilise des clés, pour le chiffrement et le déchiffrement des données.

Ce système de cryptage utilise deux clés différentes pour chaque utilisateur, une privée et n'est connue que de l'utilisateur, l'autre publique et donc accessible par tout le monde [10].

- Une première clé, visible, appelée clé publique est utilisée pour chiffrer un texte en clair.
- Une deuxième clé, secrète, appelée clé privée est connue seulement par le destinataire, qui est utilisé pour déchiffrer un texte.





FIGURE 1.5 – Cryptage Asymétrique [10].

### 1.7.2 Firewall (pare-feu)

C'est un ensemble de différents composants matériels (physique) et logiciels (logique) qui contrôlent le trafic intérieur/extérieur selon une politique de sécurité. Un système pare-feu (figure 1.6) fonctionne la plupart du temps grâce à des règles de filtrage indiquant les adresses IP autorisées à communiquer avec les machines aux réseaux, il s'agit ainsi d'une passerelle filtrante. Il permet d'une part de bloquer des attaques ou connexions suspectes d'accéder au réseau interne. D'un autre côté, un firewall sert dans de nombreux cas également à éviter la fuite non contrôlée d'informations vers l'extérieur. Il propose un véritable contrôle sur le trafic réseau de l'entreprise, Il permet donc d'analyser, de sécuriser et de gérer le trafic réseau [11].



FIGURE 1.6 – Le principe de fonctionnement d'un par feu [11].

## 1.8 Certificats

Pour assurer l'intégrité des clés publiques, celles-ci sont publiées avec un certificat. Un certificat (ou certificat de clés publiques) est une structure de données qui est numériquement signée par une autorité certifiée (CA : Certification Authority). Il contient une série de valeurs, comme le nom du certificat et son utilisation, des informations identifiant le propriétaire de la clé publique et la clé publique elle-même, la date d'expiration et le nom de l'organisme de certificat. La CA utilise sa clé privée pour signer le certificat et assurer ainsi une sécurité supplémentaire. Si le récepteur connaît la clé publique de la CA, il peut vérifier que le certificat provient vraiment de l'autorité concernée et s'assurer que le certificat contient des informations viables et une clé publique valide [12].

## 1.9 Conclusion

Le proverbe dit : « Mieux vaut prévenir que guérir ». Au terme du parcours des divers aspects de la sécurité des systèmes d'information, nous pouvons dire qu'en ce domaine prévenir est impératif, parce que guérir est impossible et de toute façon ne sert à rien. Lorsqu'un accident ou un pirate détruit les données de l'Entreprise et que celle-ci n'a ni sauvegarde ni site de secours. La dépendance des particuliers et des organisations aux réseaux informatiques et aux technologies internet amènent ces dernières à se confronter à différents degrés de vulnérabilités qui sont loin d'être négligeables. La maîtrise des nouvelles technologies par le grand public engendre un accroissement des menaces et une diversification d'outils d'attaques qui ne cessent de se perfectionner.

Il devient donc urgent de mettre en place des mécanismes pour satisfaire au mieux les besoins de la sécurité. L'un des mécanismes incontournables est la mise en place d'une politique de sécurité qui doit être au préalable bien réfléchie et étudiée selon l'entreprise.

La politique de sécurité comprend un ensemble de bases définissant une stratégie, des directives, des procédures, des codes de conduite, des règles organisationnelles et techniques.

Dans ce chapitre, nous avons présenté quelques généralités sur les réseaux informatiques.

Dans le chapitre qui suit nous allons aborder une présentation générale de l'organisme d'accueil.

Chapitre **2**

## Présentation de l'organisme d'accueil

## 2.1 Introduction

Le port de Bejaia joue un rôle très important dans les transactions internationales vu sa place et sa position géographique. Aujourd'hui. Il est classé 1er port d'Algérie en marchandises générales et 3ème port pétrolier. Il est également le 1er port du bassin méditerranéen certifié pour les trois systèmes ISO 9001 ,2000 pour la qualité, ISO 14000 pour l'environnement et OHSAS 18001 pour l'hygiène, santé et sécurité au travail. Dans ce chapitre nous allons présenter l'organisme d'accueil : EPB (l'Entreprise Portuaire de Bejaïa) au sein duquel nous avons effectué le stage relatif au présent projet. Nous nous intéresserons plus exactement au centre informatique de l'EPB : après l'étude de l'existant dans l'EPB et aux améliorations proposées.

## 2.2 Présentation de l'organisme d'accueil

L'Entreprise Portuaire de Bejaïa, est un port algérien, situé dans la ville de Bejaia, dans la région de Kabylie. Il a été créé 14 Août 1982 suite au décret n°82-285, c'est une Entreprise socialiste à caractère économique, conformément aux principes de la charte de l'organisation des entreprises, Réputée commerçante dans ses relations avec les tiers, fut régie par la législation en vigueur et soumise aux règles édictées par le susmentionné décret. Pour accomplir ses missions, l'entreprise est substituée à l'Office National des Ports (ONP), à la Société Nationale de Manutention (SO.NA.MA) et pour partie à la Compagnie Nationale Algérienne de Navigation (CNAN). Vu sa situation géographique qui lui permet de jouer un rôle très important dans les transactions internationales. Il est notamment consacré au commerce international et aux hydrocarbures. De par sa position stratégique, les qualités nautiques remarquables et les infrastructures performantes dont il dispose, le port de Bejaia reste de développement économique pour la région du pays. Principale tournante du commerce, il constitue l'accès privilégié aux différentes industries, parce qu'il offre à ses clients des terminaux propices et compétitifs ainsi que des équipements modernes et performants, tous dédiés pour l'accueil et le traitement de tous types de marchandises.

## 2.3 Organigramme de l'EPB

L'EPB est organisée selon des différentes directions, dirigées par une Direction Générale qui s'occupe des actions liées à la gestion et au développement de l'entreprise. Chaque partie prenante de l'organisation remplit un rôle incontestablement important. Cependant, dans le cadre de ce mémoire, nous allons nous intéresser en exclusivité à la Direction des Systèmes d'Information (DSI).(figure 2.1)

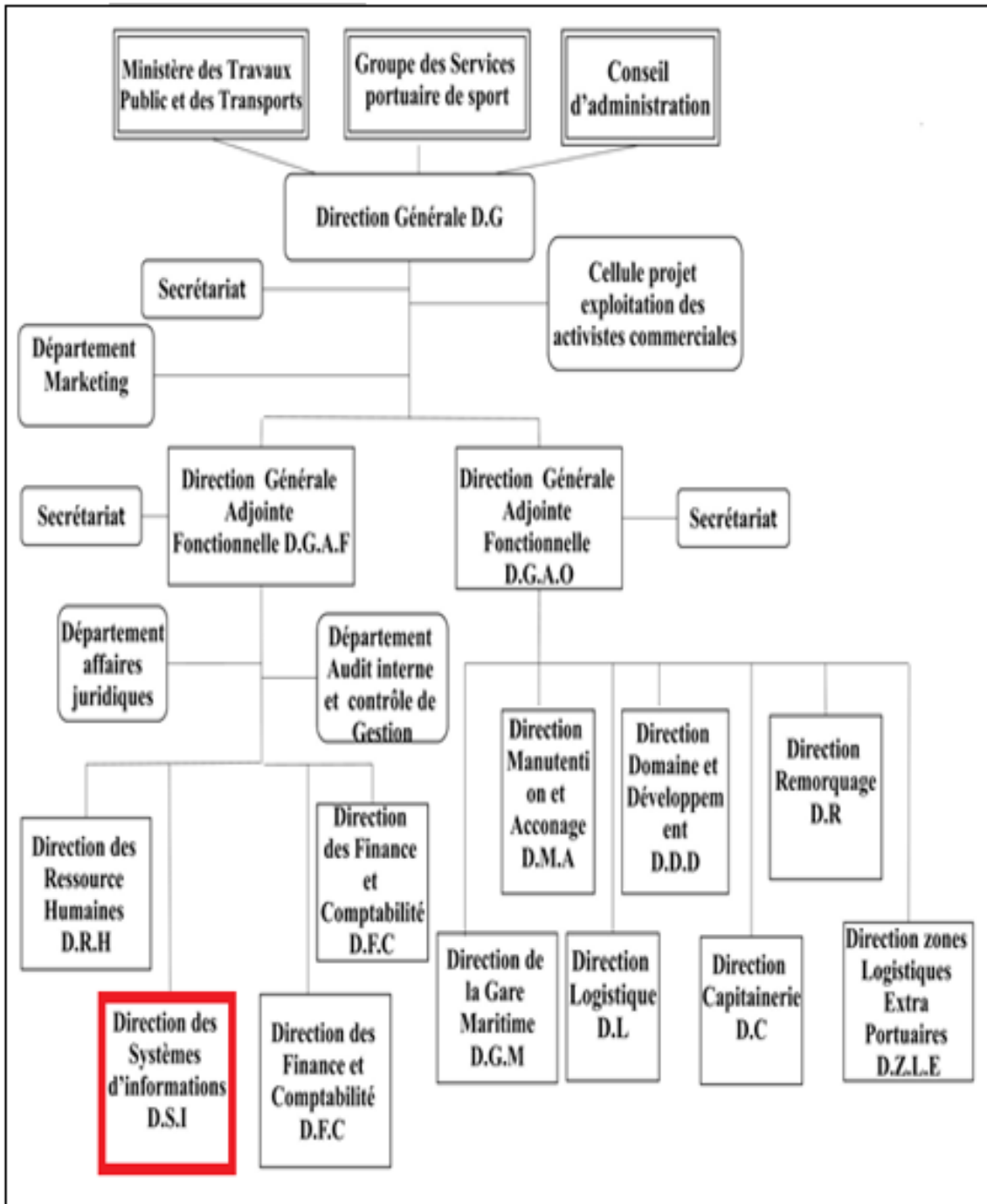


FIGURE 2.1 – Organigramme générale de l'EPB.

## 2.4 Direction des Systèmes d'Information (DSI)

Elle est chargée de gérer l'ensemble des systèmes d'information et de télécommunication de l'entreprise.

### 2.4.1 Présentation de la DSI

Le système d'information (SI) est un ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information. La DSI est une direction de l'EPB rattachée directement à la direction générale, elle a pour mission l'automatisation des métiers de l'entreprise portuaire de Bejaïa, et cela en mettant en place les logiciels et l'infrastructure nécessaire pour la gestion du système d'information.

### 2.4.2 Missions

Durant le stage effectué au niveau de la direction des systèmes d'information nous avons pu identifier les missions du système d'informations comme la montre la figure ci-dessous :

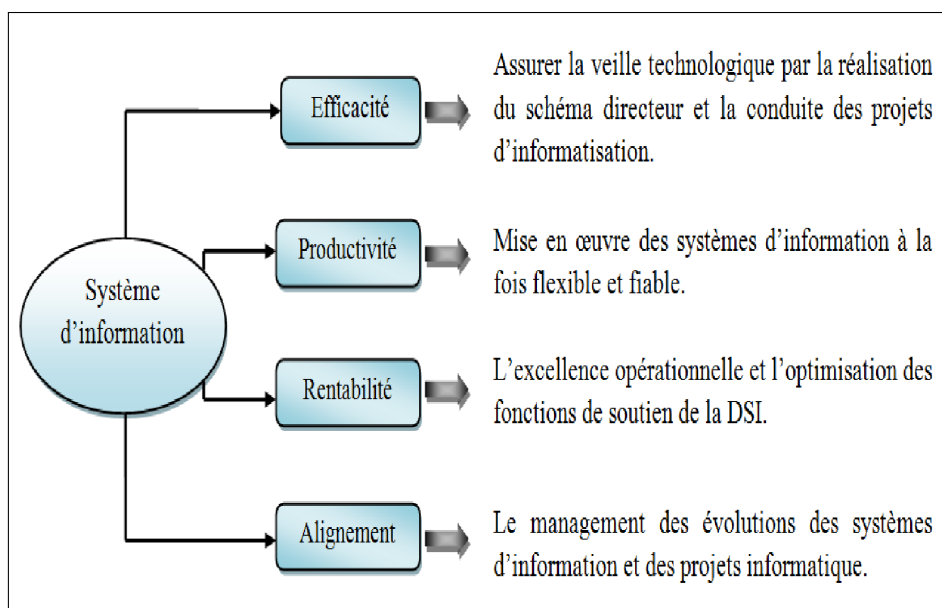


FIGURE 2.2 – Missions du système d'information de l'EPB.

### 2.4.3 Organisation humaine de la direction des systèmes d'information

La direction se compose de trois départements comme le montre l'organigramme suivant :(voir figure 2.3)

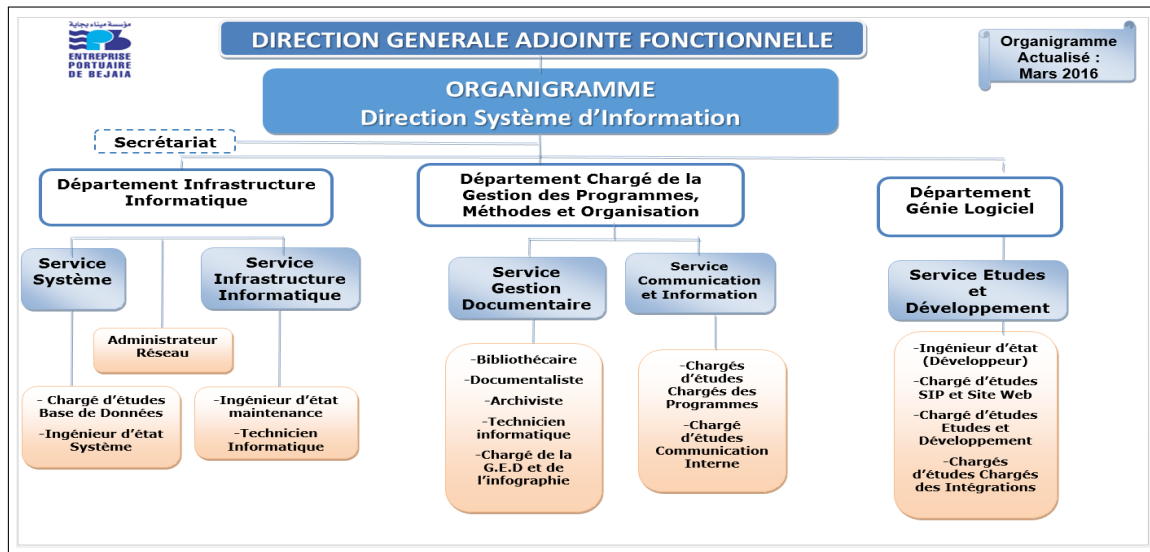


FIGURE 2.3 – Organigramme de la Direction des Systèmes d'Information.

## 2.5 Infrastructure informatique

Le réseau du port de Bejaia s'étend du port pétrolier (n°16) aux ports 13 et 18 (parc à bois). La salle machine du réseau local de l'EPB contient principalement une armoire de brassage et une autre armoire optique de grande taille, ces deux armoires servent à relier les différents sites de l'entreprise avec le département informatique par fibres optiques de type 4, et 12 brins, comme l'illustre la figure (Figure-2.4). Chaque site a une armoire de brassage contenant un/des convertisseur(s) media, un/plusieurs Switch où sont reliés les différents équipements par des câbles informatiques.

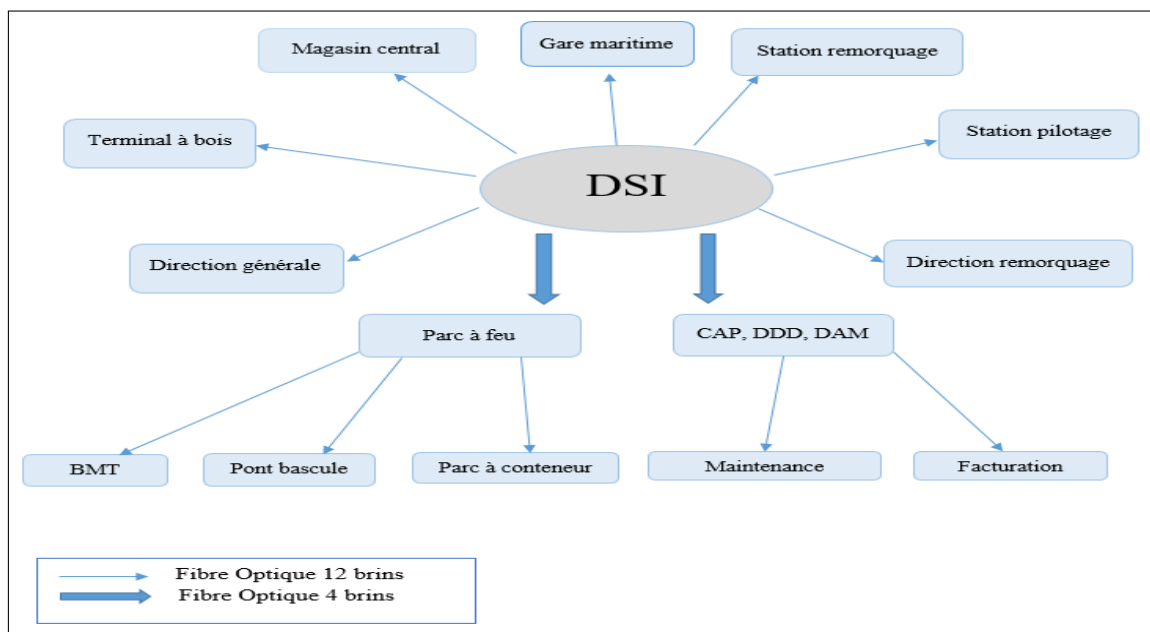


FIGURE 2.4 – Réseau fibre optique de l'EPB.

### 2.5.1 Réseau local de l'EPB

Le réseau local de l'EPB permet aux différents postes de travail d'échanger des informations, de se connecter vers l'extérieur et d'utiliser des applications hébergées en interne nécessaire à l'exécution des tâches quotidiennes des employés. Le réseau du port de Bejaïa s'étend du port pétrolier (N16) aux ports 13 et 18 (port à bois).(voir figure 2.5)

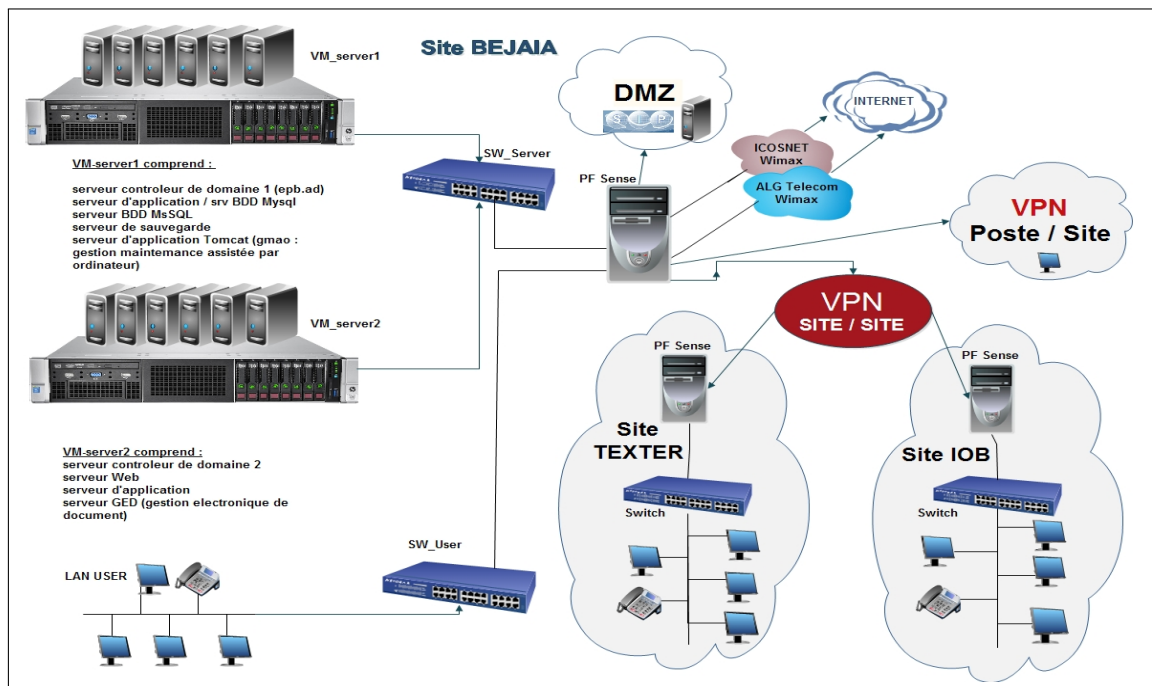


FIGURE 2.5 – L'architecture du réseau LAN de l'entreprise EPB.

## 2.6 Problématique

Durant le stage effectué au niveau de la direction des systèmes d'information de L'EPB, nous avons pu constater que cette entreprise possède de nombreux postes informatiques reliés entre eux par un réseau local.

Ce réseau permet d'échanger des données entre les divers collaborateurs internes à l'entreprise et aussi de se connecter à l'internet.

Ouvrir l'entreprise vers le monde extérieur signifie laisser une porte ouverte à divers acteurs étrangers. Cette porte peut être exploitée pour la destruction des données ou pour le piratage des données ,c'est pourquoi on doit Sécuriser notre réseau .

Pour cela il existe plusieurs protocoles d'authentification : le protocole Diameter, le protocole Tacacs+ et Radius .

### 1. Diameter

Diameter est un protocole d'Authentication conçu pour servir de support à l'architecture AAA, successeur du protocole Radius. Ce protocole est défini par la RFC 3588. Il a repris les principales fonctions de Radius



(Diameter est compatible avec Radius) et en a rajouté de nouvelles pour s'adapter aux nouvelles technologies et plus particulièrement offrir des services aux applications mobiles. Ce protocole se situe au niveau de la couche transport. Il utilise le port 3868 via le protocole TCP [16].

## 2. Tacacs+

Tacacs+ (Terminal Access Controller Access Control System Plus) est un protocole de sécurité inventé à la fin des années 90 par CISCO Systems. Même s'il a fini par remplacer les protocoles Tacacs et XTacacs, Tacacs+ n'est pas basé sur ces derniers. Ce protocole se situe au niveau de la couche transport. Il utilise le port 46 via le protocole TCP. Tacacs+ permet de vérifier l'identité des utilisateurs distants mais aussi, grâce au modèle AAA, d'autoriser et de contrôler leurs actions [16].

### A. Comparaison de l'existant (figure 2.6)

	Tacacs+	Diameter	Radius
Fonctionnalité	Sépare authentification et d'autorisation.	Combine authentification et d'autorisation.	Combine authentification et d'autorisation.
Standard	Partiellement Cisco.	Ouvrir norme / RFC.	Ouvrir norme / RFC.
Transport Protocol	TCP.	UDP.	TCP.
Chiffrement	Tout le paquet chiffré.	Mot de passe crypté.	Mot de passe crypté.

FIGURE 2.6 – Comparaison entre Radius , Diameter et Tacacs+

## 2.7 Solution

L'objectif principal de notre étude est la mise en œuvre d'une solution d'authentification qui nous permet de sécuriser l'accès aux services réseaux de l'EPB.

On a optée pour Radius car c'est le plus optimisé, sécurisée et fiable. De plus

il utilise le mode sans connexion ce qui permet à l'utilisateur de ne pas attendre pendant plusieurs minutes pour accéder à un équipement .

Il est performant car il utilise l'UDP .UDP fournit les meilleures performances, fournit en plus de l'authentification, un moyen de gérer les autorisations d'accès et la journalisation des échanges.

Radius nous permet de centraliser nos identifiants , de gérer les mots de passe et les authentifications pour ses clients.

Radius iL nous permet de définir les accès des utilisateurs distants à un réseau et de sécuriser l'accès à distance aux réseaux , on utilise un certificat. Chaque utilisateur aura son propre certificat.

## **2.8 Conclusion**

Ce chapitre nous a permis de présenter l'organisme d'accueil l'EPB . L'étude de l'existant nous a permis de nous familiariser avec le réseau actuel de l'EPB ,et de comprendre son fonctionnement , nous a permis de voir les lacunes et les faiblesses du réseau. L'étude de ces lacunes nous a conduit à proposer une solution pour pallier à ses dernières et qui nous aide à mieux gérer les mots de passe, sécuriser l'accès à distance et faire la liaison entre des besoins d'identification et une base d'utilisateurs en assurant le transport des données d'authentification de façon normalisée.

# Chapitre 3

## Serveur d'authentification Radius

## 3.1 Introduction

Pour sécuriser l'accès au réseau nous utilisons généralement l'authentification. Celle-ci est basée sur une indentation par nom d'utilisateur et mot de passe. Il faut définir l'ensemble des couples autorisés. Pour ce faire, nous pouvons créer des utilisateurs en local sur chaque équipement utilisé dans le réseau.

Nous pouvons aussi créer nos utilisateurs sur un serveur, ce qui a pour avantage de ne pas avoir à configurer les couples sur tous les équipements, mais de tout centraliser, ceci nous permet de gagner du temps.

Ce chapitre a pour but d'apporter une solution à la problématique citée dans le chapitre 2. Nous ferons appel à la norme 802.1x, en mettant en œuvre une solution d'authentification autour de serveurs Radius.

## 3.2 Protocole Radius

Radius avait tout d'abord pour objet de répondre aux problèmes d'authentification pour des accès distants, par liaison téléphonique, vers les réseaux des fournisseurs d'accès ou des entreprises. C'est de là qu'il tient son nom qui signifie Remote Access Dial In User Service. Au fil du temps, il a été enrichi et aujourd'hui il peut être utilisé pour authentifier les postes de travail sur les réseaux locaux, qu'ils soient filaires ou sans fil. Le protocole Radius est décrit dans la RFC 2865 de l'IETF<sup>1</sup>. Radius est un système client/serveur qui permet de sécuriser des réseaux contre des accès à distance non autorisés. Ce protocole répond au modèle AAA [14].

Résumant ses trois fonctions comme suit :

- A = Authentication : authentifier l'identité du client.
- A = Authorization : accorder des droits au client.
- A = Accounting : enregistrer les données de comptabilité de l'usage du réseau par le client.

Ce dernier connaît nativement deux protocoles de mot de passe : PAP (échange en clair du nom et du mot de passe), et CHAP (échange basé sur un hachage de part et d'autre avec échange seulement du « challenge ») [14].

### 3.2.1 Fonctionnement de Radius

Le fonctionnement de Radius est basé sur un système client/serveur chargé de définir les accès d'utilisateurs distants à un réseau en utilisant le protocole UDP et les ports 1812 et 1813. Le protocole Radius repose principalement sur un serveur (le serveur Radius), relié à une base d'identification (base de données, Active Directory, annuaire LDAP, etc.) et un client Radius, appelé NAS (Network Access Server), agir comme d'intermédiaire entre l'utilisateur final et le serveur [14].

---

1. (Internet Engineering Task Force)

L'ensemble des transactions entre le client Radius et le serveur Radius est chiffrée et authentifiée grâce à un secret partagé.

La figure ci-dessous montre le mécanisme d'authentification sur le serveur Radius :

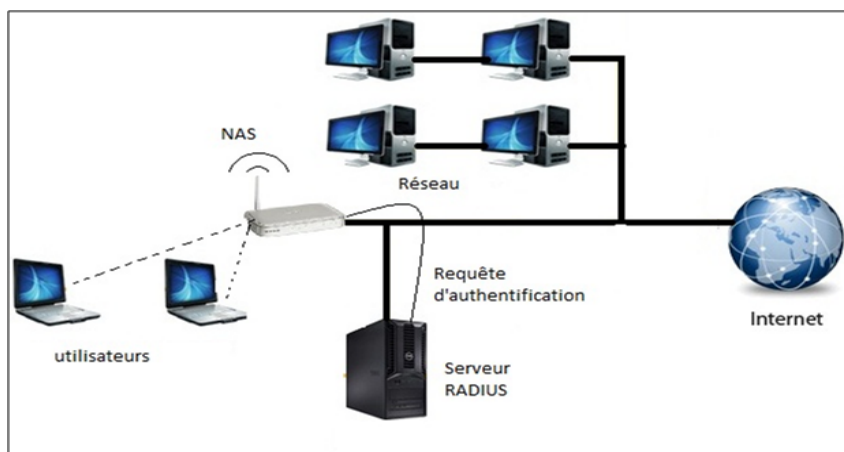


FIGURE 3.1 – Architecture Radius [14].

- **Scénario du principe de fonctionnement est le suivant**

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. Soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur.

Le serveur Radius retourne ainsi l'une des quatre réponses suivantes :

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

### 3.2.2 Format de l'en-tête du paquet Radius

L'en-tête du paquet Radius comporte 5 champs 5 (figure 3.2) :

Code	Identifiant	length
Request Authenticator / Response Authenticator		
Attributes...		

FIGURE 3.2 – En-tête du paquet Radius.

- **Code** : Définit le type de trame (acceptation, rejet, challenges, requête).
- **Identifiant** : Associe les réponses reçues aux requêtes envoyées.
- **Length** : Champ longueur.
- **Authenticator** : champ d'authentification comprenant les éléments nécessaires.
- **Attribuées** : Ensemble de couples (attribut, valeur).

### 3.2.3 Rôles de protocole Radius

- Authentifier les machines/utilisateurs pour l'accès au réseau local.
- Placer les machines dans des sous-réseaux virtuels.
- Initialiser les algorithmes de chiffrement des communications (WPA).
- Les communications Wifi peuvent être sécurisées.
- Interfaçage avec des logiciels de portails captifs.

### 3.2.4 Caractéristiques de Radius

Les caractéristiques principales de Radius sont :

- Modèle client/serveur.
- Sécurité réseau.
- Mécanismes flexibles d'authentification.
- Protocole extensible.

#### 1. Modèle client/serveur

Un serveur d'accès de réseau NAS fonctionne en tant que client Radius. Le client est responsable pour passer l'information utilisateur vers les serveurs Radius, et puis d'effectuer les traitements en fonction de la réponse qui est retournée. Les serveurs Radius sont chargés de recevoir les demandes de connexion d'utilisateur, d'authentifier l'utilisateur, et puis de renvoyer toute l'information de configuration nécessaire pour que le client puisse fournir le service à l'utilisateur.

## 2. Sécurité réseau

Les transactions entre le client et le serveur Radius sont authentifiées par l'utilisation d'un secret partagé, qui n'est jamais envoyé en dehors du réseau. En outre, tous les mots de passe utilisateur sont envoyés chiffrés entre le client et le serveur, pour éliminer la possibilité que quelqu'un sur un réseau suffisamment sécurisé puisse espionner le transit réseau pour déterminer le mot de passe d'un utilisateur.

## 3. Mécanismes flexibles d'authentification

Le serveur Radius peut supporter une variété de méthodes pour authentifier un utilisateur. Quand on lui fournit le nom d'utilisateur et le mot de passe initial donnés par l'utilisateur, il peut supporter la procédure de connexion de PPP, PAP, CHAP, login Unix ou d'autres mécanismes d'authentification.

## 4. Protocole extensible

Toutes les transactions sont composées de triplets (Attribut, Longueur, Valeur). Des nouvelles valeurs d'attribut peuvent être ajoutées sans perturber les implémentations existantes du protocole

### 3.2.5 Avantages du Radius

- **Sécurité forte** : L'utilisation d'un certificat Radius permet de demander à toute personne souhaitant se connecter au réseau de s'authentifier, il consiste à faire présenter un certificat électronique dont la validité sera vérifiée par le serveur. Chaque utilisateur aura son propre certificat. La transaction entre un client radius et le serveur radius est cryptée.
- **Fiabilité** : La méthode d'authentification par certificat est très fiable.
- **Administré** : Radius permet de centraliser des données d'authentification.

### 3.2.6 Protocole Radius et la couche de transport UDP

Le protocole établit une couche applicative au-dessus de la couche de transport UDP. Les ports utilisés seront :

- 1812 pour recevoir les requêtes d'authentification et d'autorisation.
- 1813 pour recevoir les requêtes de traçabilité [14].

Le Protocol Radius utilise le protocole UDP. Pourquoi UDP ?

- Il permet la réémission d'une demande d'authentification à un serveur secondaire si le serveur primaire ne répond pas.
- Radius est un protocole sans état.
- UDP simplifie la mise en œuvre du serveur.

### 3.2.7 Éléments d'authentification Radius

- **Authentification avec l'adresse Ethernet (adresse MAC)**

L'authentification par adresse MAC, appelée Radius-MAC, est la plus simple à mettre en œuvre. En revanche, c'est la moins sûre. La figure 3.3 représente un réseau sur lequel est connecté un serveur Radius et un poste de travail par l'intermédiaire « commutateur ». Les étapes du protocole sont :

1. Le poste de travail se branche sur un des ports du commutateur.
2. Le commutateur détecte cette connexion et envoie une requête d'authentification (AccessRequest) au serveur Radius. Dans cette requête, l'adresse MAC du poste de travail fait office d'identifiant.
3. Le serveur reçoit ce paquet et utilise l'adresse MAC comme point d'entrée dans sa base de données.
4. Le serveur envoie sa réponse au commutateur. Si elle est négative (Access-Reject), le port du commutateur reste fermé et le poste n'est pas connecté au réseau. Si la réponse est positive (Access-Accept), elle contient le numéro de VLAN autorisé. Le commutateur ouvre alors le port sur ce VLAN et le poste peut commencer à travailler. Donc, dans ce type d'authentification, il n'y a pas de communication entre le poste de Travail et le serveur Radius. Tous les échanges interviennent entre le commutateur Et le serveur [15].

Dans le cas des réseaux sans fil, le schéma est exactement le même. Certes, il n'y a pas de port physique, mais l'opération d'association est équivalente au "branchement" D'un poste sur la borne. Celle-ci crée alors un port virtuel et tout se passe ensuite Comme en filaire. Le serveur dialogue avec la borne exactement comme avec un Commutateur [15].

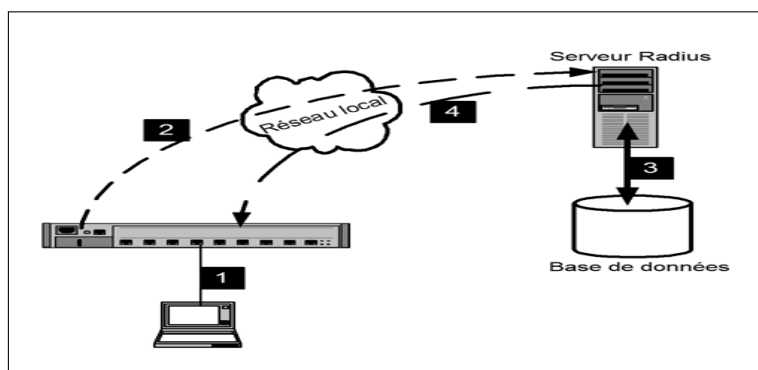


FIGURE 3.3 – principes de l'authentification Radius-MAC [15].

- **Authentification avec 802.1X (EAP)**

Le schéma général de l'authentification 802.1X ressemble à celui de Radius-MAC, les deux méthodes sont, en réalité, très différentes. L'authentification 802.1X est plus compliquée et délicate à mettre en œuvre.



Tout d'abord, la différence la plus importante est que, cette fois, un logiciel particulier sera indispensable sur le poste de travail. Ce logiciel est appelé supplican. Suivant le schéma de la figure 3.4, c'est lui qui va envoyer (1) vers le serveur Radius les éléments d'authentification (certificat, identifiant, mot de passe. . .). Cependant, il ne communique pas directement avec le serveur. C'est le commutateur qui va servir d'intermédiaire (2), car il connaît l'adresse du serveur.

Pour interroger sa base de données (3), le serveur Radius a besoin d'un identifiant qu'il utilise comme point d'entrée. Dans ce cas, il ne s'agira pas de l'adresse MAC. L'identifiant sera configuré et envoyé par le supplican [15].

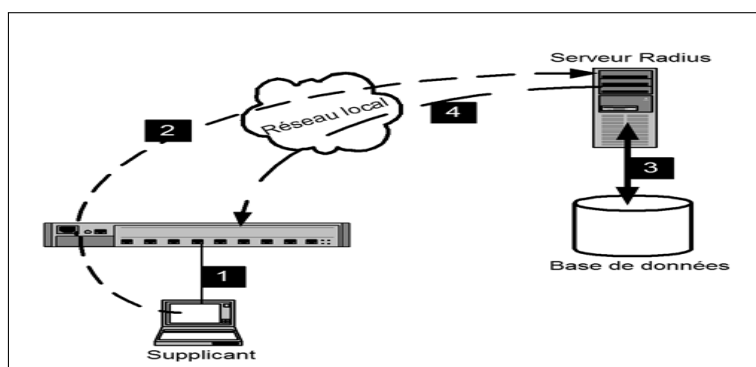


FIGURE 3.4 – principe d'authentification 802.1X [15].

Comme précédemment, le serveur accepte ou refuse l'authentification et renvoie sa réponse au commutateur (4). Et celui-ci ouvre le port sur le VLAN commandé par le serveur. Mais l'opération est complètement différente du cas précédent.

Avec Radius-MAC, l'authentification est réalisée sans aucune communication entre le poste de travail et le serveur. En 802.1X, dans la mesure où c'est le supplican qui envoie les éléments d'authentification, il y a bien une communication. Or, comment peut-il y avoir une communication, et donc un trafic réseau, puisque le port du commutateur n'est pas ouvert et qu'il ne le sera que lorsque le poste aura été authentifié ?

C'est justement là que tient tout le protocole 802.1X. Les ports du commutateur seront configurés d'une façon particulière. Avant d'être complètement ouverts, ils ne laisseront passer qu'un seul type de protocole : EAP. D'ailleurs, l'autre nom de 802.1X est « Port-Based Network Access Control » qui, traduit littéralement, signifie « Accès au réseau basé sur le contrôle de port ».

Tout se passe comme si chaque port était coupé en deux. Une moitié est appelée port contrôlé au départ, elle est maintenue fermée par le commutateur. L'autre moitié est appelée port non contrôlé. Par cette voie, le commutateur n'accepte que le protocole EAP.

Dans notre cas, nous avons choisi l'authentification Radius 802.1x par identifiant et mot de passe [15].

a. **Port non contrôlé**

Au début de la connexion, le port est dans l'état non contrôlé. Seuls les paquets 802.1X permettant d'authentifier le client qui sont autorisés (figure 3.5).

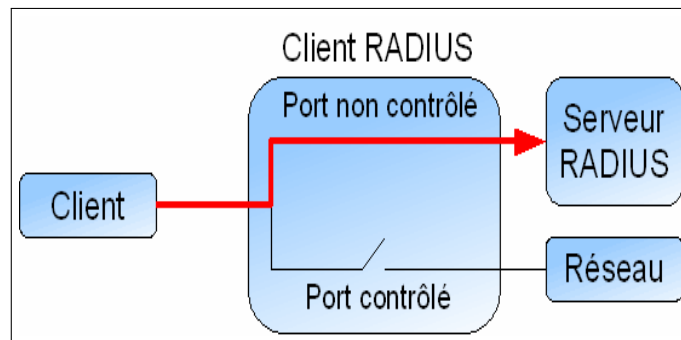


FIGURE 3.5 – État du port avant la phase d'authentification .

b. **Port contrôlé**

Une fois l'authentification effectuée, le port passe dans l'état contrôlé. Alors, tous les flux du client sont acceptés et le client peut accéder aux ressources partagées (figure 3.6).

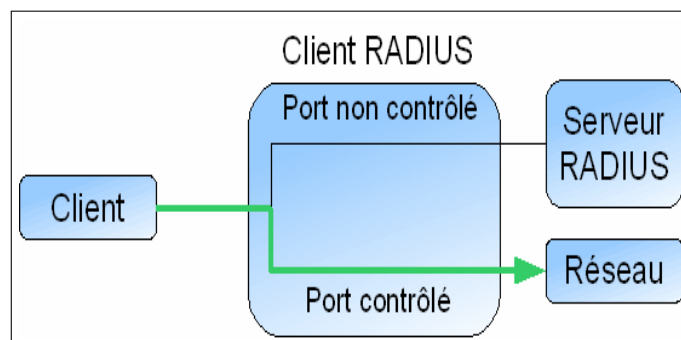


FIGURE 3.6 – État du port après une authentification réussie .

### 3.3 Protocole 802.1x

Le standard 802.1x est une solution de sécurisation, mise au point par l'IEEE en juin 2001. Il permet d'authentifier les équipements connectés sur un port avant d'accéder à un réseau (sans fil ou filaire) grâce à un serveur d'authentification. Elle repose sur le protocole EAP (Extensible Authentication Protocol).

802.1X définit EAP over LAN (EAPOL) pour l'échange de paquets entre le client et le point de contrôle dans un réseau filaire et sans fil. Entre le point de contrôle et le point de décision, les paramètres sont transmis en utilisant EAP over Radius (EAPOR) qui encapsule les paquets EAP dans Radius [16].

### 3.3.1 Composants 802.1x

Les composants du 802.1x sont ( figure 3.7) :

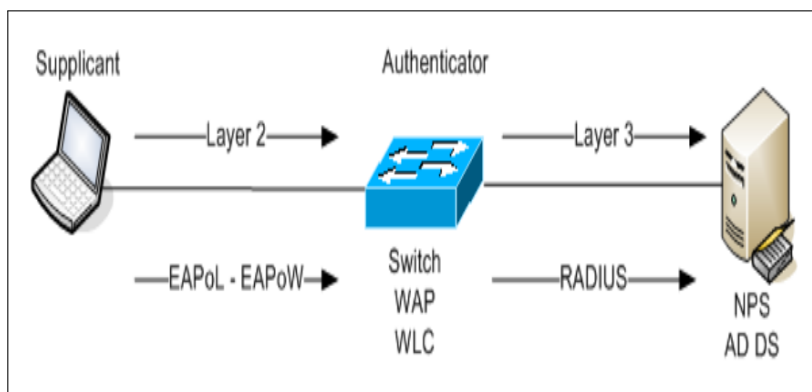


FIGURE 3.7 – Composants 802.1x.

- **Suppliant (poste de travail) :** est un client qui demande l'accès au réseau local et répond aux demandes du commutateur.
- **Serveur d'authentification (Radius / serveur NPS) :** Ce serveur authentifie le client. Le serveur d'authentification valide l'identité du client et informe le commutateur si le client est autorisé à accéder au réseau local.
- **Authenticator (commutateur) :** Contrôle d'accès physique au réseau en fonction du statut d'authentification du client. Ce dispositif relaie les informations d'identification suppliante au serveur d'authentification

### 3.3.2 Étapes d'authentification 802.1X

L'état du port de commutateur détermine si le client est autorisé à accéder au réseau local ou non. Il existe plusieurs types de paquets qui interviennent dans les étapes d'authentification 802.1x. ( figure 3.8 )

- **EAP-Start :** permet au client d'alerter le contrôleur d'accès qu'il souhaite se connecter.
- **EAP Request :** Envoyé par le contrôleur d'accès au client.
- **EAP Response :** Réponse du client au contrôleur d'accès.
- **EAP Success :** Paquet envoyé au client en fin d'authentification si elle est réussie.
- **EAP Failure :** Paquet envoyé au client en fin d'authentification si elle est ratée.

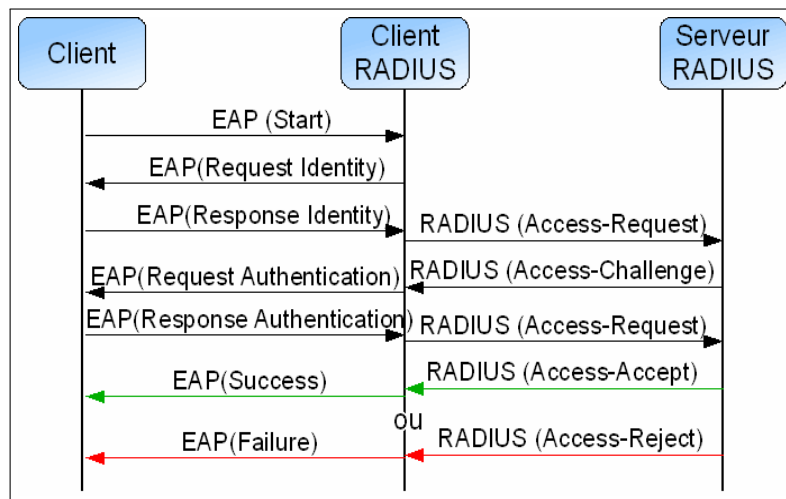


FIGURE 3.8 – Processus d’authentification.

### 3.3.3 Protocole EAP

La communication entre l’équipement réseau (authenticator) et le serveur d’authentification est assurée par le protocole EAP (Extensible Authentication Protocol) qui assure le transport des informations d’authentification et permet d’utiliser différentes Méthodes d’authentification d’où le terme “Extensible”. Le domaine d’application de ce protocole correspond donc à tous les modes de connexion [17].

#### a. Méthodes associées à EAP

Le protocole EAP ne propose pas qu’une seule méthode d’authentification c’est-à-dire qu’il utilise ces différents éléments pour identifier un client :

- Le login / mot de passe.
- Le certificat électronique.
- La biométrie.
- Une puce (SIM).

Certaines méthodes combinent plusieurs critères (certificat et login/mot de passe . . . ). En plus de l’authentification, EAP gère la distribution dynamique des clés de chiffrement. Parmi les méthodes de l’authentification les plus communes sur EAP on distingue :

- **EAP-MD5** : Authentification avec un mot de passe [18].
- **EAP-TLS** : Authentification par certificat du client et du serveur [19].
- **EAP-TTLS** : Authentification par certificat et mot de passe grâce à la génération d’un tunnel sécurisé [20].
- **PEAP (Protected EAP)** : Authentification avec mot de passe via une encapsulation sécurisée [21].
- **LEAP (protocole Cisco)** : Authentification avec mot de passe via une encapsulation sécurisée .

## 3.4 Conclusion

L'étude d'une solution a pour objectif de permettre une bonne réalisation. L'authentification, l'autorisation et la traçabilité (AAA) est un concept de sécurité informatique courant qui définit la protection des ressources du réseau. Il est utilisé pour prendre en charge les objectifs principaux de la sécurité, en plus de fournir un cadre pour l'accès aux réseaux et aux équipements à l'aide des protocoles Radius. Dans ce chapitre on a bien détaillé le protocole Radius qui convient à la norme 802.1X et supporte les protocoles EAP et qui a un avantage de sécurité, fiabilité et centralisation de l'authentification. Le chapitre qui suit va être consacré à la mise œuvre d'un service Radius pour l'authentification 802.1X.

Chapitre **4**

## Mise en œuvre et réalisation

## 4.1 Introduction

Notre projet s'inscrit dans le domaine de la sécurité informatique, il vise à apporter une solution au problème de l'authentification dans le réseau de l'entreprise EPB de Bejaia.

Ce chapitre est consacré à la mise en oeuvre des solutions proposées pour la réalisation d'un système d'authentification permettant d'authentifier des utilisateurs avant tout accès au réseau de l'entreprise, ce système est le serveur Radius qui s'appuie sur l'authentification 802.1x et utilise le protocole EAP .

## 4.2 Composantes utilisées

Pour implémenter ce système d'authentification, quatre composantes sont nécessaires

- Un Windows Server 2016 exécutant NPS (Network Policy Server).
- Un client sous Windows 10.
- Deux commutateurs prenant en charge le protocole 802.1X.
- Un pare-feu « pfsense ».

## 4.3 Présentation des outils utilisés

Pour notre projet on a utilisé les outils suivants :

### 4.3.1 Logiciel GNS3

GNS3 est un simulateur graphique d'équipement réseau qui nous permet de créer des topologies de réseaux complexes et d'établir des simulations.

### 4.3.2 VM WARE Workstation 15 pro

Pour l'émulation de notre réseau, nous avons choisi d'utiliser la VMware Workstation 15 pro (figure 4.1) . Cette dernière permet la création d'une ou plusieurs machines virtuelles au sein d'un même système d'exploitation. Ceux-ci pouvant être reliés au réseau local avec une adresse IP différente, tout en étant sur la même machine physique.

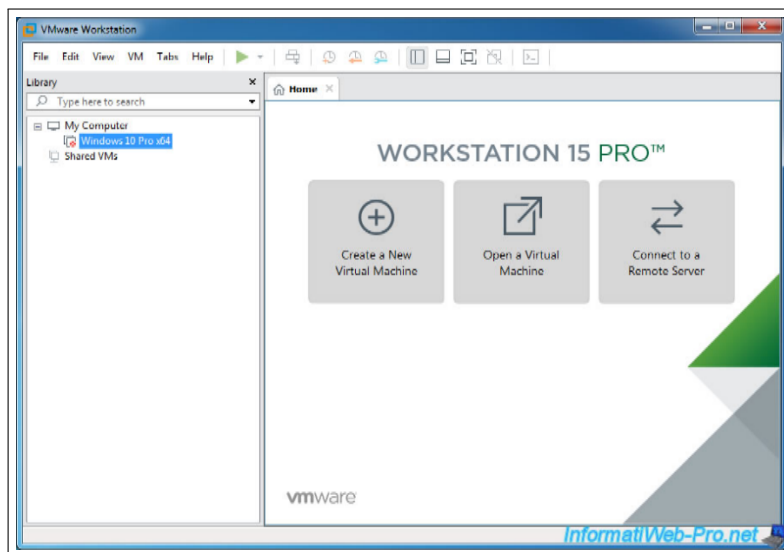


FIGURE 4.1 – La fenêtre principale du VMware.

### 4.3.3 Wireshark

c'est un outil de capture et d'analyse de paquets réseau Open Source destiné aux administrateurs réseau et aux développeurs, Wireshark est une référence en matière d'analyse des transactions réseau. Cet outil puissant supporte plusieurs centaines de protocoles et dispose de fonctions de filtrage avancées pour la capture et l'interprétation des données [22].

### 4.3.4 Windows server 2016

Le Windows server 2016 est un système d'exploitation pour serveurs de Microsoft, il permet de créer des solutions plus simples à planifier, il est destinée aux serveurs d'entreprise.

## 4.4 Configuration du serveur Radius

Dans cette partie tout ce fait à l'intérieur de Windows serveur 2016.

### 4.4.1 Création du contrôleur de domaine et DNS

Avant de promouvoir le serveur en tant que contrôleur de domaine dans notre domaine, il faut installer (le rôle Service de domaine Active Directory) (figure 4.2).

1. Dans le gestionnaire de serveur, nous allons cliquer sur (Ajouter des rôles et des fonctionnalités) .
2. Au niveau des rôles, choisir (serveur DNS) et (Service AD DS) qui correspond au service de domaine Active Directory en cochant la case. Une fenêtre va apparaître pour indiquer que d'autres éléments requis AD DS doivent être installés, cliquez sur "Ajouter des fonctionnalités".



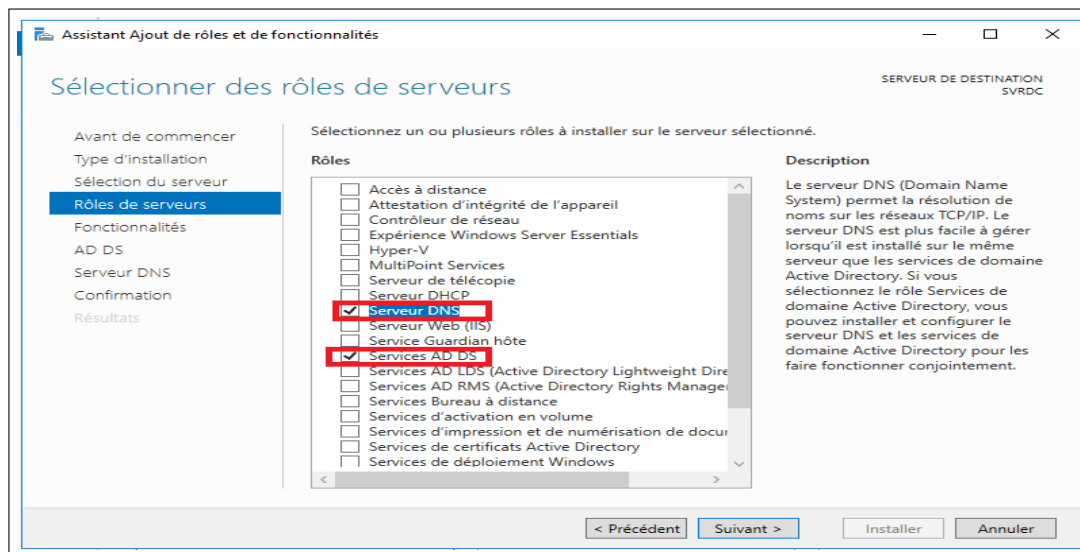


FIGURE 4.2 – Ajout du service AD DS et serveur.

3. Une fois les fonctionnalités d'AD DS installées. Nous devons promouvoir ce serveur en tant que contrôleur de domaine, sinon le domaine ne sera pas créé (figure 4.3).

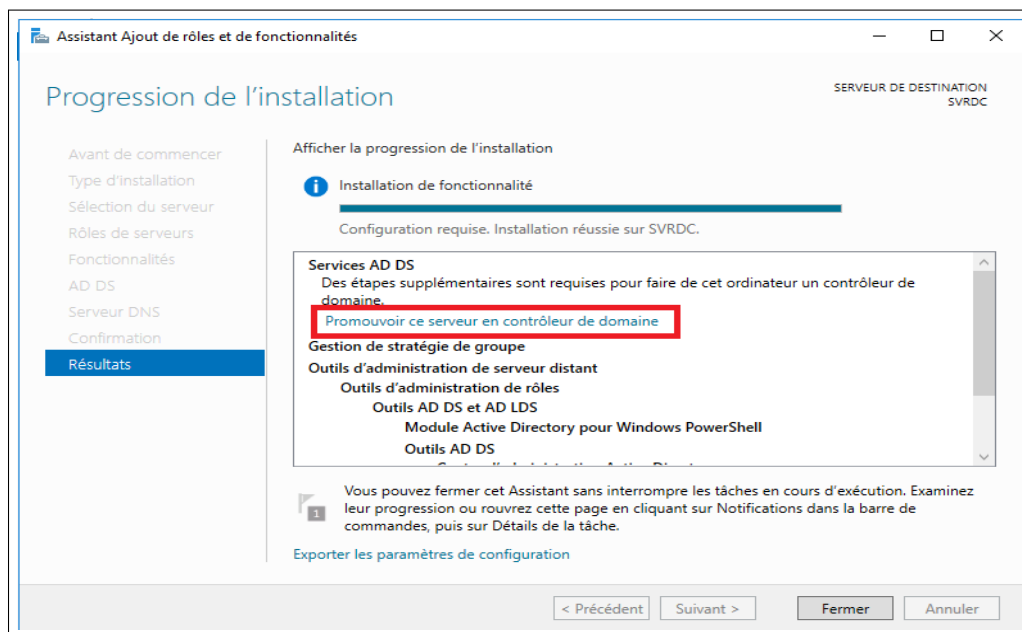


FIGURE 4.3 – Promouvoir le serveur en contrôleur de domaine.

4. Vu que nous souhaitons créer un nouveau domaine, nous devons déployer une nouvelle forêt en cliquant sur Ajouter une nouvelle forêt et en spécifiant le nom de notre domaine «EPB.local » (figure 4.4).

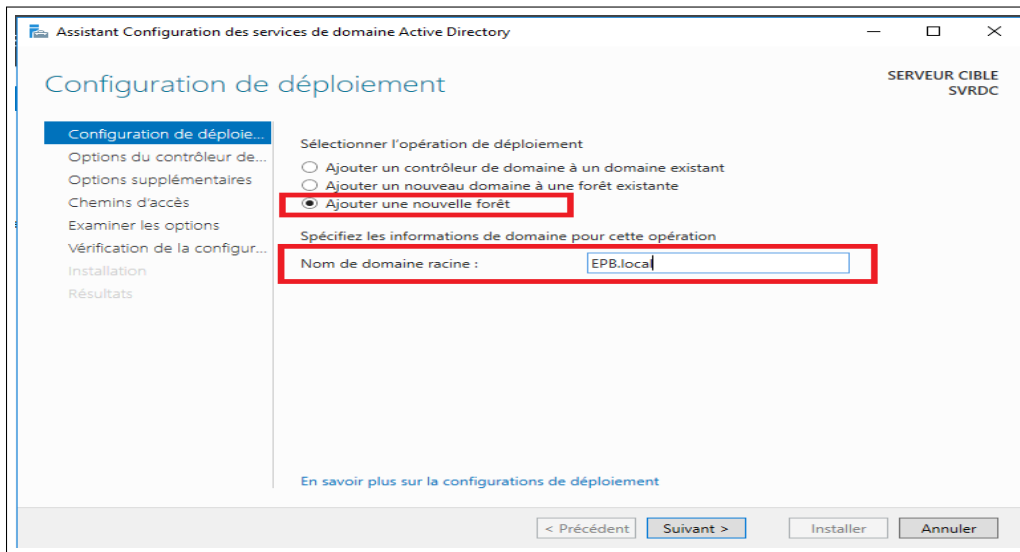


FIGURE 4.4 – Création du domaine « EPB.local ».

5. L'étape suivante consiste à choisir le niveau fonctionnel de la forêt et du domaine ainsi pour éviter les restaurations non souhaitées d'Active Directory, il est demandé de saisir un mot de passe de restauration (figure 4.5).

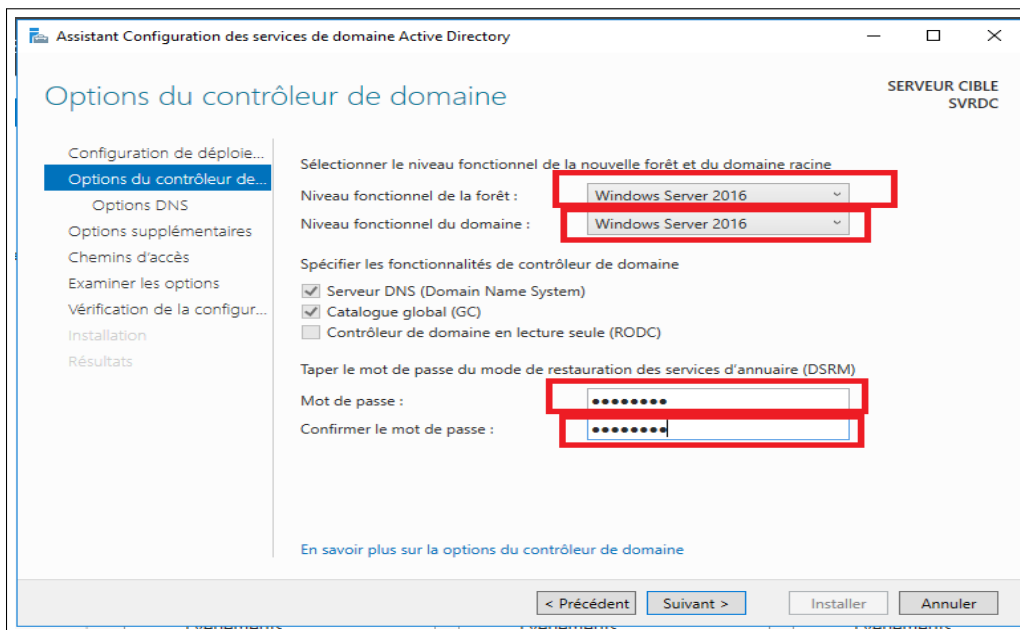


FIGURE 4.5 – Niveau fonctionnel de la forêt et du domaine.

6. L'assistant suivant montre le nom NetBIOS de domaine : pour poursuivre l'installation on clique sur suivant (figure 4.6).

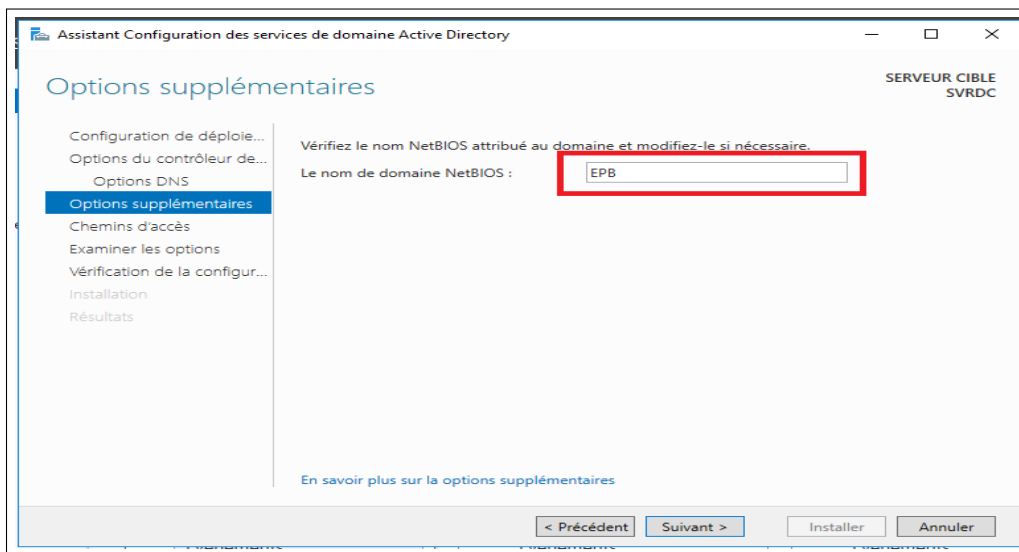


FIGURE 4.6 – Nom NetBIOS de domaine.

7. Ensuite on spécifie les dossiers qui contiendront la base de données du contrôleur de domaine Active directory, les fichiers journaux et SYSVOL (figure 4.7).

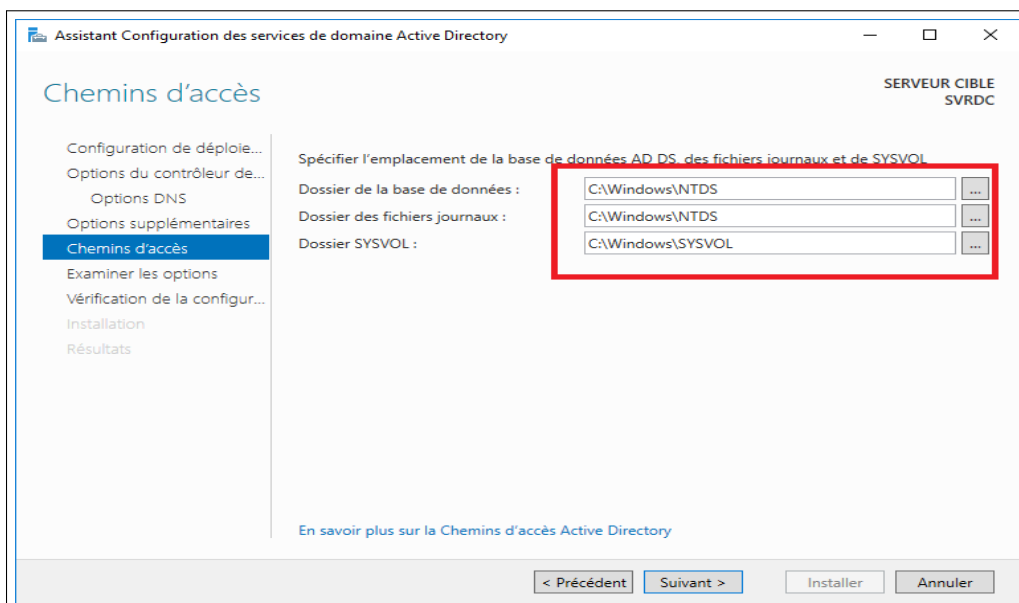


FIGURE 4.7 – l'emplacement des fichiers Active Directory.

8. Lorsque nous installons les services de domaine Active Directory (AD DS), celui-ci nous donne la possibilité d'installer et de configurer automatiquement un serveur DNS. La zone DNS résultante est intégrée à AD DS contrôlé par le serveur SVRDC. Après configuration, le serveur redémarre automatiquement. A présent, les outils de gestion d'Active Directory sont présents dans le menu outils, notre domaine est créé et l'ouverture d'une session s'effectue avec le compte d'administrateur du domaine EPB/Administrateur (figure 4.8).

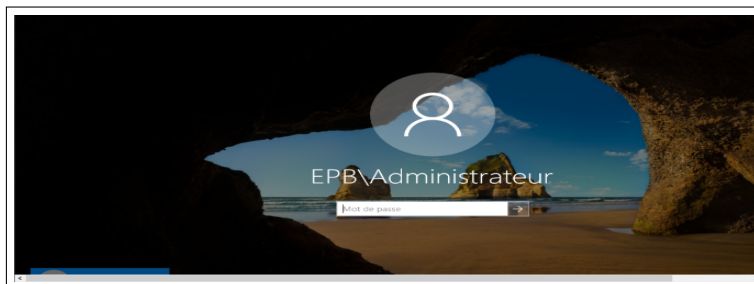


FIGURE 4.8 – Ouverture de la session Administrateur.

### A. Création des groupes et des utilisateurs dans l'Active Directory

1. Pour créer un groupe, un clic droit sur notre domaine "EPB.local", "new" puis "group" (figure 4.9).

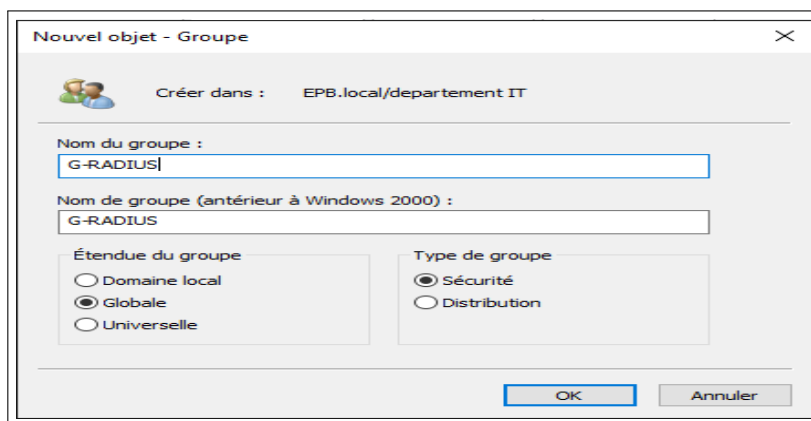


FIGURE 4.9 – Création de groupe G-Radius.

2. Pour créer un utilisateur, un clic droit sur le domaine "EPB.local" puis "New user" (figure 4.10).

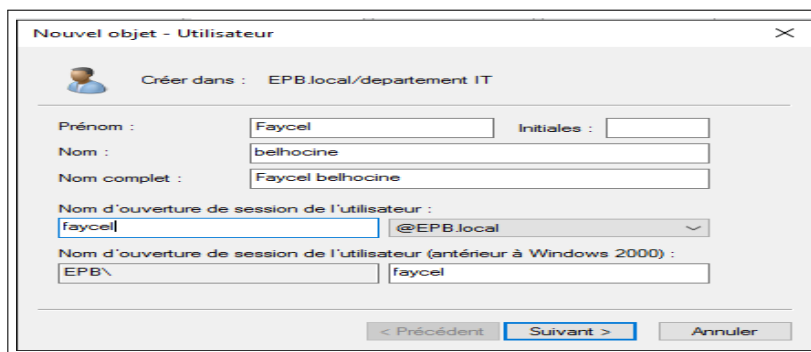


FIGURE 4.10 – Création d'un utilisateur.

3. Après avoir cliqué sur "Suivant", on doit introduire le mot de passe, et cocher les deux cases " l'utilisateur ne peut pas changer le mot de passe " et " le mot de passe n'expire jamais (figure 4.11).

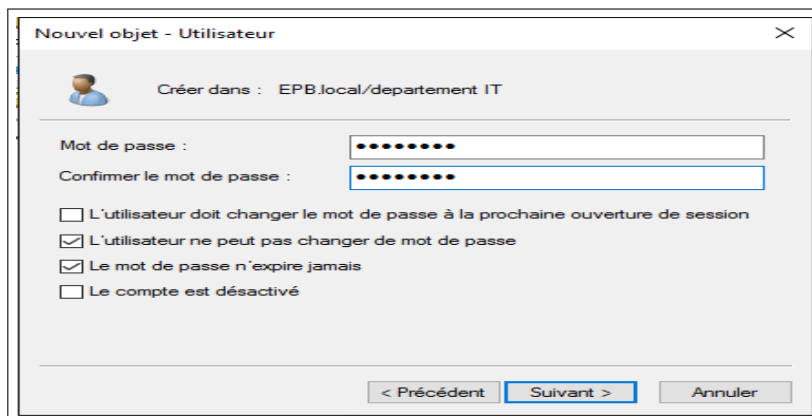


FIGURE 4.11 – Introduction de mot de passe d'utilisateur.

4. Ajouter les utilisateurs créé au groupe, la figure suivante montre que les utilisateurs sont bien membres de notre groupe radius (figure 4.12) .

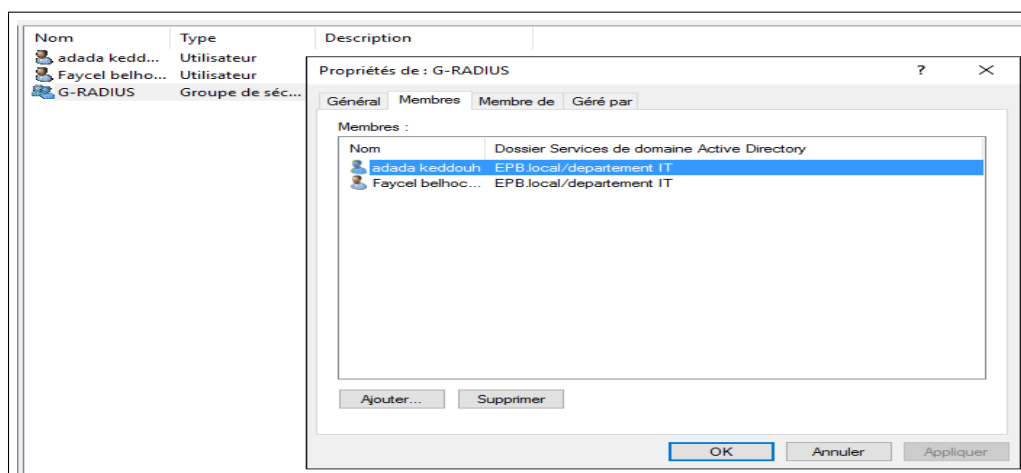


FIGURE 4.12 – Membres du groupe-Radius.

#### 4.4.2 Installation et configuration du service DHCP

Pour que les pc et les serveurs communique nous devons leur donner une adresse IP, un masque de sous réseau, une passerelle et un serveur DNS qui est obligatoirement un DNS d'Active Directory.

1. Dans l'assistant de gestion des rôles, au niveau des rôles de serveurs, choisir (serveur DHCP) en cochant la case (serveur DHCP).et faire suivant jusqu'à installer cliquer dessous (figure 4.13) .

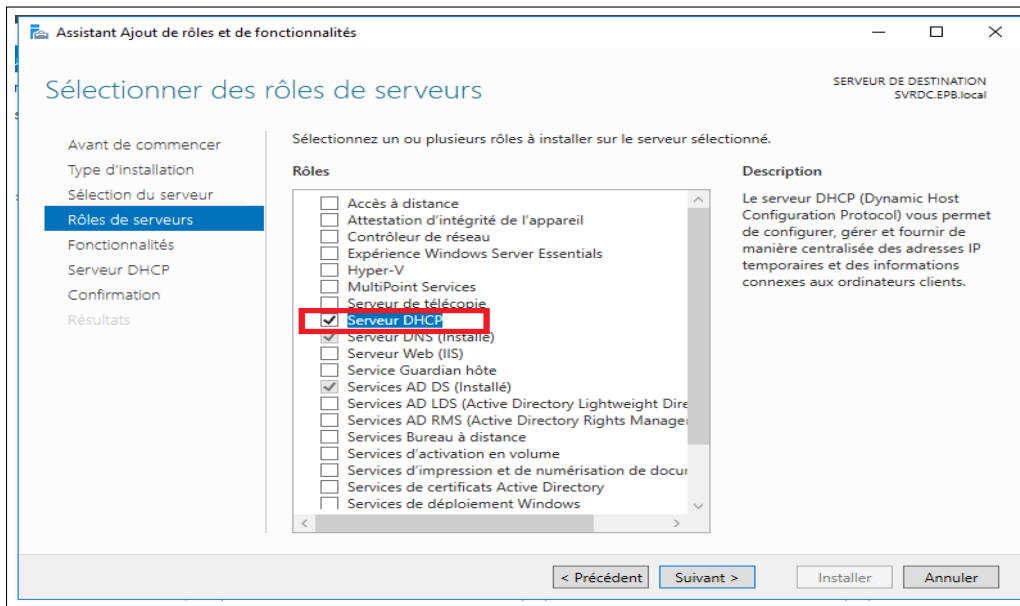


FIGURE 4.13 – Ajout du serveur DHCP.

2. Après quelques minutes le rôle est installé, nous procédons à la configuration du DHCP en IP pour le client (figure 4.14).

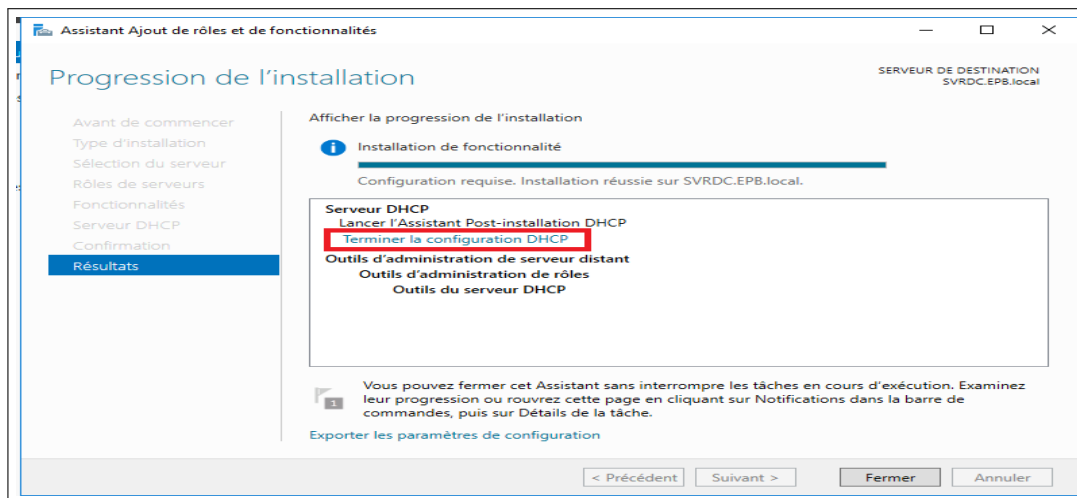


FIGURE 4.14 – Installation du serveur DHCP.

3. Ensuite spécifiez les informations d'identification qui Permettent à ce DHCP d'être authentifié par Active Directory puis nous appuyons sur "valider" pour confirmer qu'il est bien authentifié (figure 4.15).

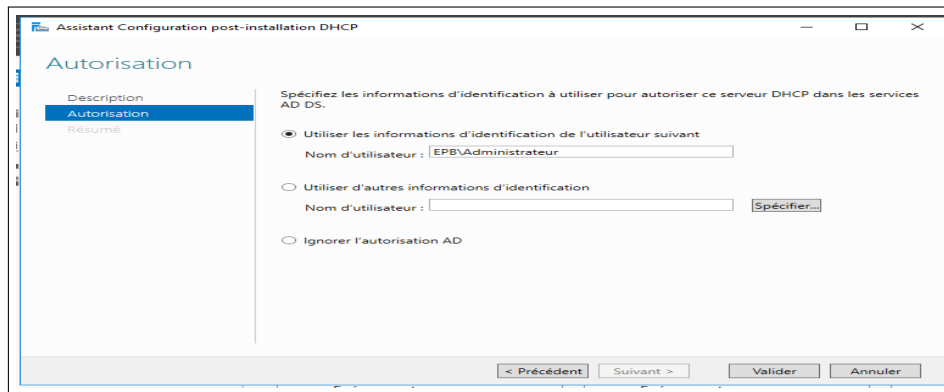


FIGURE 4.15 – Autorisation du serveur DHCP dans les services AD DS.

4. Création de nos étendues DHCP à l'aide de la console d'administration DHCP qui a été lancée depuis le menu outils du gestionnaire de serveur (figure 4.16).

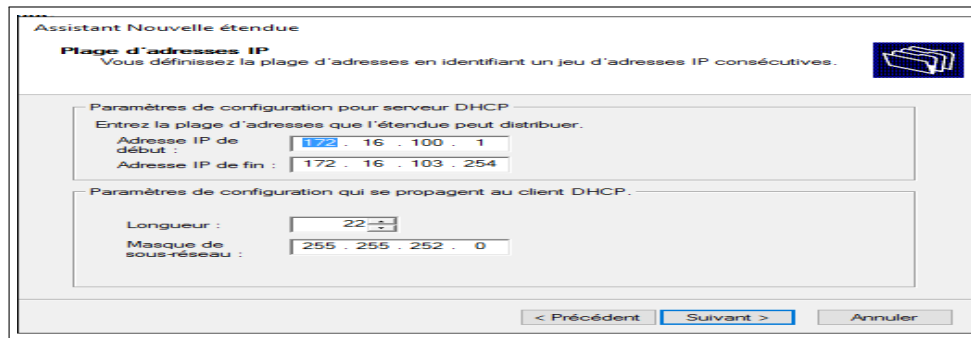


FIGURE 4.16 – Plage d'adresse allouée aux machines clientes.

5. Ajouter les exclusions des adresses ou des plages qui ne sont pas distribuées par le serveur afin de ne pas provoquer de conflit avec un périphérique qui serait configuré sur ces adresses (figure 4.17).

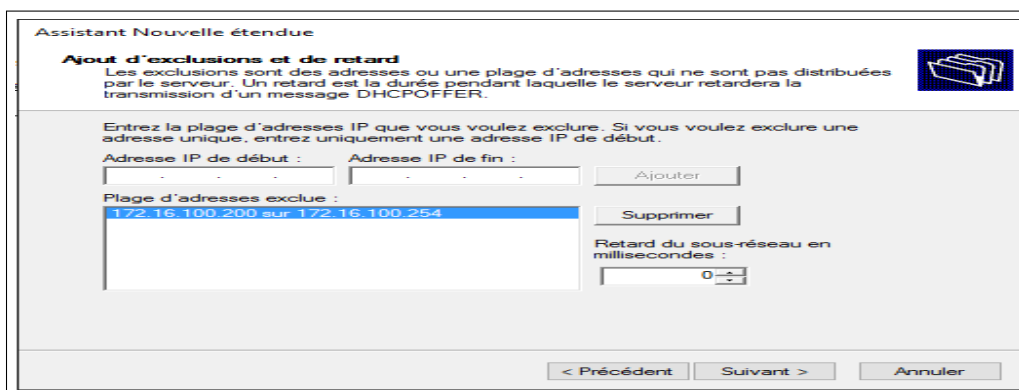


FIGURE 4.17 – Ajout d'exclusion DHCP.

6. Ajouter adresse IP du routeur dans notre cas pfsense « pare-feu » (figure 4.18).

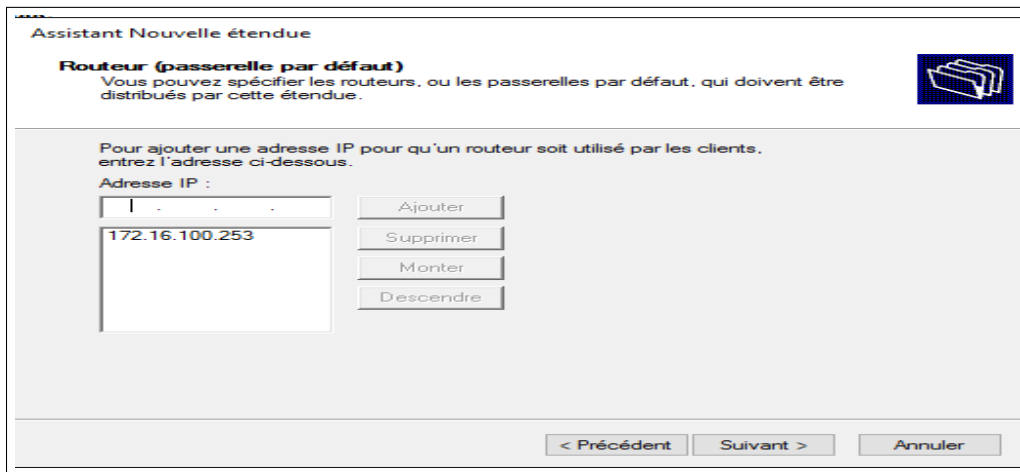


FIGURE 4.18 – Ajout de l'adresse IP du pare-feu.

7. Si on utilise un serveur DNS, saisissons le nom du serveur. Cliquons sur Ajouter pour inclure ce serveur dans la liste des serveurs DNS affectés aux clients DHCP puis cliquons sur suivant et terminer (figure 4.19).

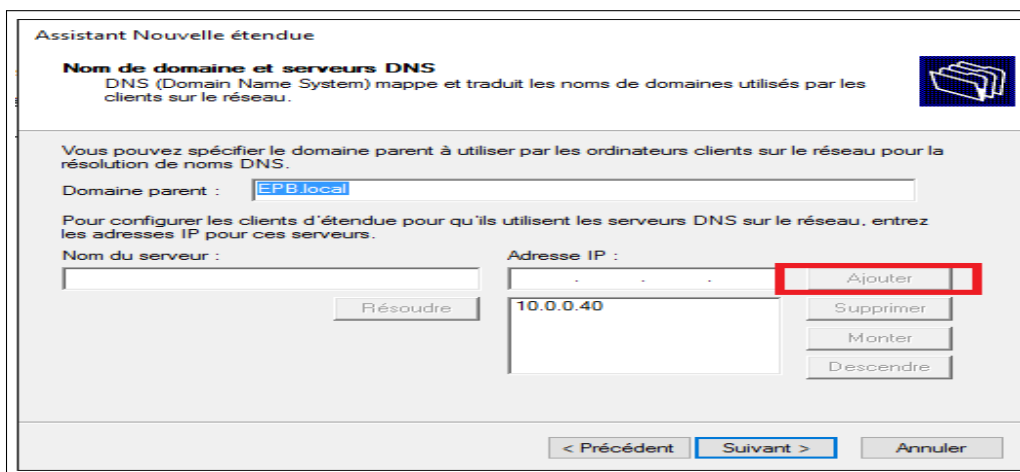


FIGURE 4.19 – Ajout du nom de domaine serveur DNS.

#### 4.4.3 Mise en œuvre de l'autorité de certification Active

1. Directory Certificat Services (AD CS) Dans cette partie, nous allons créer une autorité de certification racine d'entreprise. Dans l'assistant de gestion des rôles, Au niveau des rôles de serveurs, choisir (services de certificats Active directory) (figure 4.20).



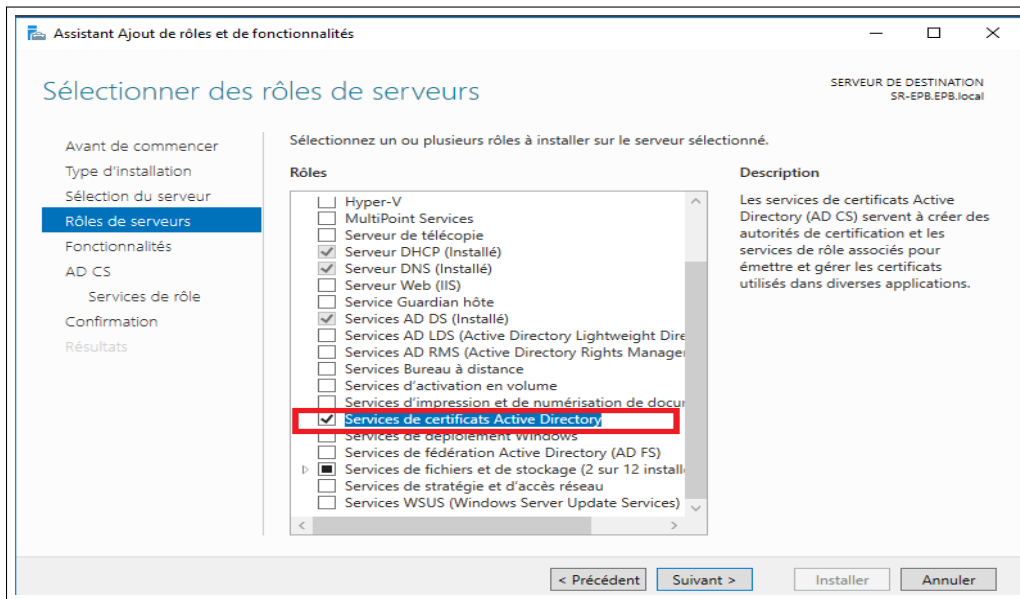


FIGURE 4.20 – Ajout des services de certificats Active Directory.

2. Après l'installation du " Service de certificats Active Directory " sur le gestionnaire de serveur, et avoir coché la case "Autorité de certification " pour configurer ce rôle. La figure suivante présente un résumé des configurations post installation (figure 4.21).

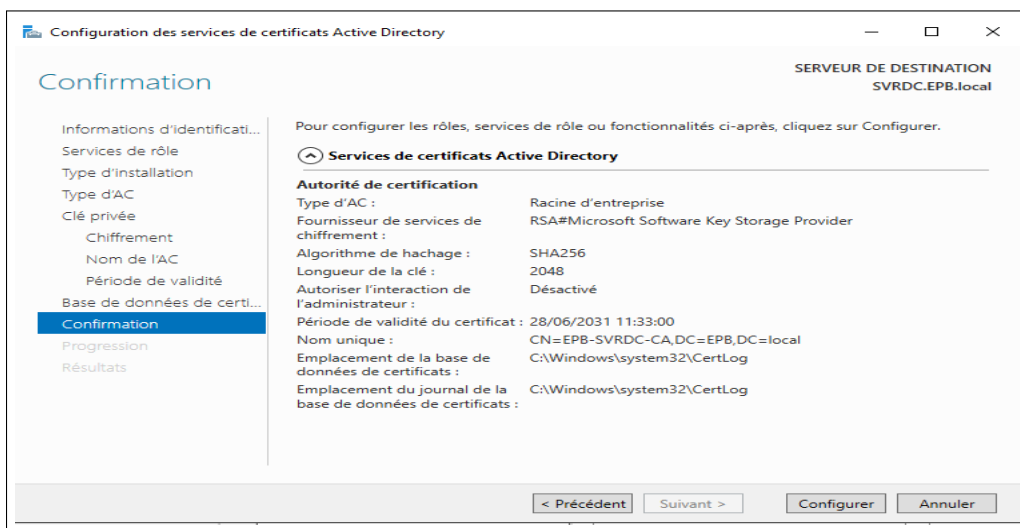


FIGURE 4.21 – Configuration d'une PKI.

#### 4.4.4 Installation du service "Network Policy and Access Services"(Services de Stratégie Et d'accès réseau)

C'est par le « serveur NPS » que radius sera ensuite configuré on retrouve le raccourci,comme pour les services habituels, dans les outils d'administration du système. Le serveur NPS permet de créer et de mettre en œuvre des stratégies d'accès réseau à l'échelle d'une entreprise pour assurer l'intégrité des clients, l'authentification et l'autorisation des demandes de connexion. Pour l'installation, on procède comme suit :

1. Dans la console server manager  $\implies$  Rôles  $\implies$  add rôles  $\implies$  Network Policy and Access Services  $\implies$  Suivant  $\implies$  cocher (Network Policy Server) "NPS"  $\implies$  Install (figure 4.22).

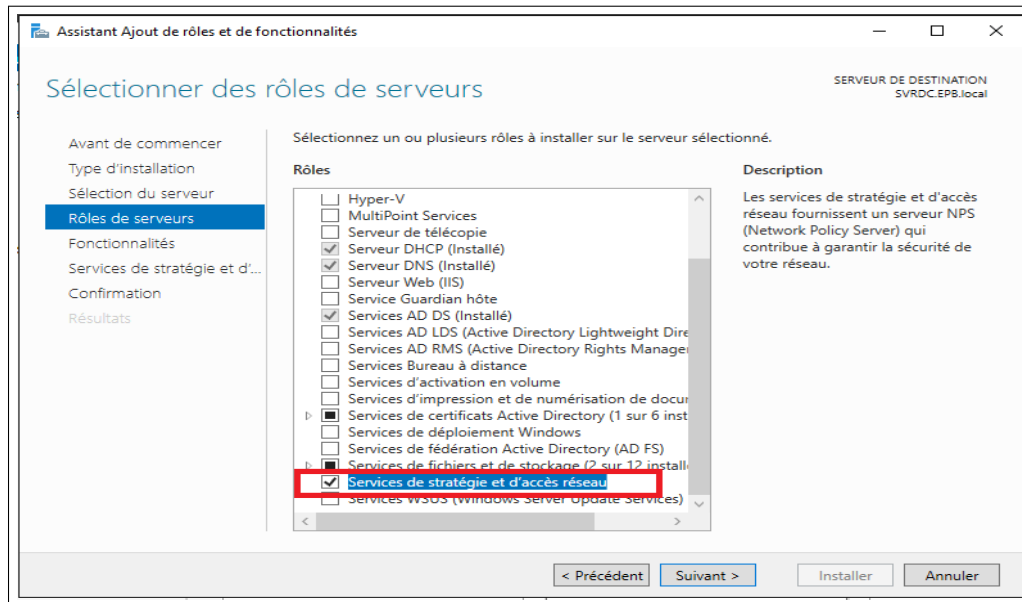


FIGURE 4.22 – Ajout des services de stratégie et d'accès réseau.

#### A. Configuration de "NPS" en tant que Serveur RADIUS

Lorsque nous déployons NPS (Network Policy Server) en tant que serveur protocole Radius (Remote Authentication Dial-in User Service), NPS effectue l'authentification, l'autorisation et la gestion des comptes pour les demandes de connexion pour le domaine local. Il procède aussi à l'autorisation des demandes de connexion en utilisant la stratégie réseau et en vérifiant les propriétés de numérotation du compte d'utilisateur dans les services de domaine Active Directory (AD DS).

##### 1. Inscrire le serveur NPS dans le domaine

Pour que NPS soit autorisé à accéder aux informations d'identification et aux propriétés d'accès distant des comptes d'utilisateurs dans les services de domaine Active Directory (AD DS), le serveur exécutant NPS doit être inscrit dans ces derniers. Pour cela : En doit autoriser le serveur Radius sur la base de données d'annuaire Active. Cliquez à droite sur NPS (LOCAL) et en sélectionne le serveur enregistrer en option Active Directory sur l'écran de confirmation, on clique sur le bouton OK (figure 4.23).

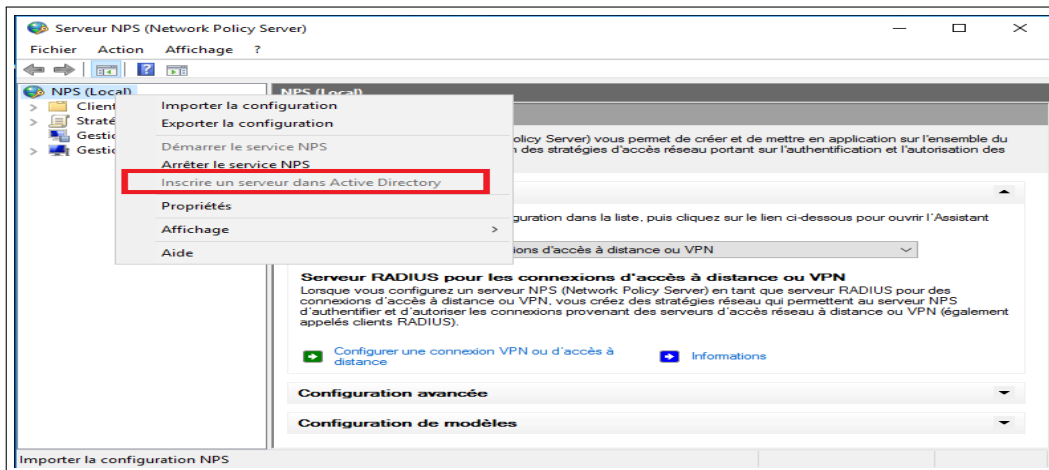


FIGURE 4.23 – Inscription du serveur NPS dans le domaine.

### B. Configuration de "NPS" en tant que Client Radius

Les clients Radius tel que (switch, routeur, point d'accès) sont des appareils qui seront autorisés à demander l'authentification à partir du serveur Radius. Pour la configuration du client Radius, il faut suivre les étapes suivantes :

1. NPS  $\implies$  Radius Clients and Servers  $\implies$  Radius Clients  $\implies$  Nouveau  $\implies$  cocher pour Activer ce client Radius et remplir ces paramètres (figure 4.24) :

- **Nom convivial** : Nom pour identifier le client.
- **Adresse (IP ou DNS)** : Saisir l'IP du client ou son nom DNS .
- **Secret partagé** : Indiquer un code qui sera partagé par le client et le serveur Radius puis cliquer sur **OK**.

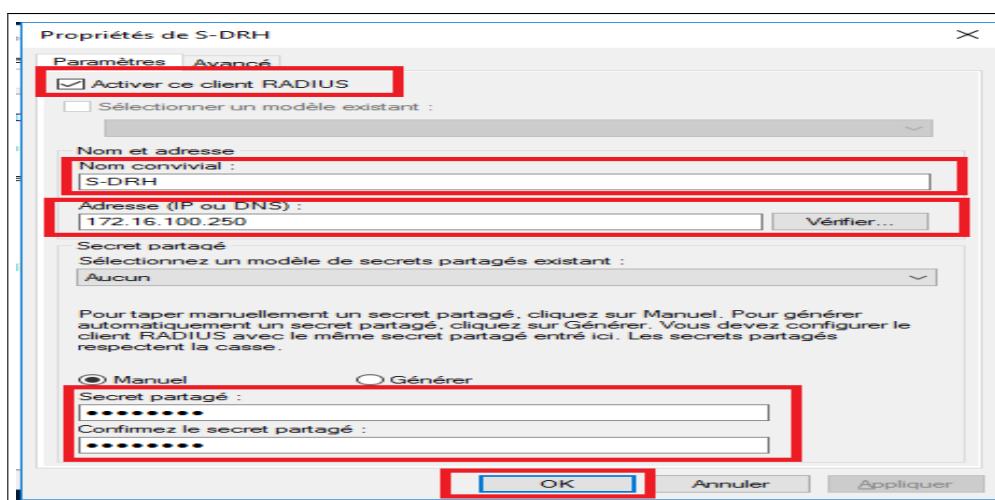


FIGURE 4.24 – Création du client Radius.

### C. Création d'une nouvelle stratégie réseau pour switch

Les stratégies de réseau sont utilisées par NPS pour déterminer si les demandes de connexion reçus des clients Radius sont autorisées.

1. Nous allons créer une nouvelle politique 802.1x pour authentifier les utilisateurs lors de la connexion à notre commutateur. Pour cela on doit sélectionner le serveur Radius pour les connexions câblées ou sans fil 802.1x puis cliquer sur configurer 802.1x (figure 4.25).

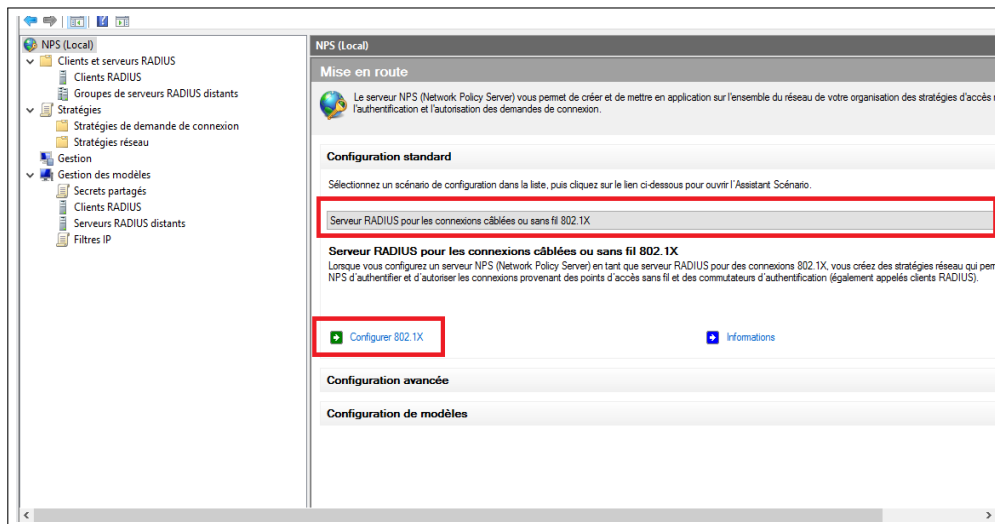


FIGURE 4.25 – Sélection d'un scénario de configuration.

2. On sélectionne le type de connexion 802.1x. cocher la case « connexions câblées (Ethernet) sécurisées  $\implies$  et nommez la politique qu'on a créé ensuite on clique sur suivant (figure 4.26).

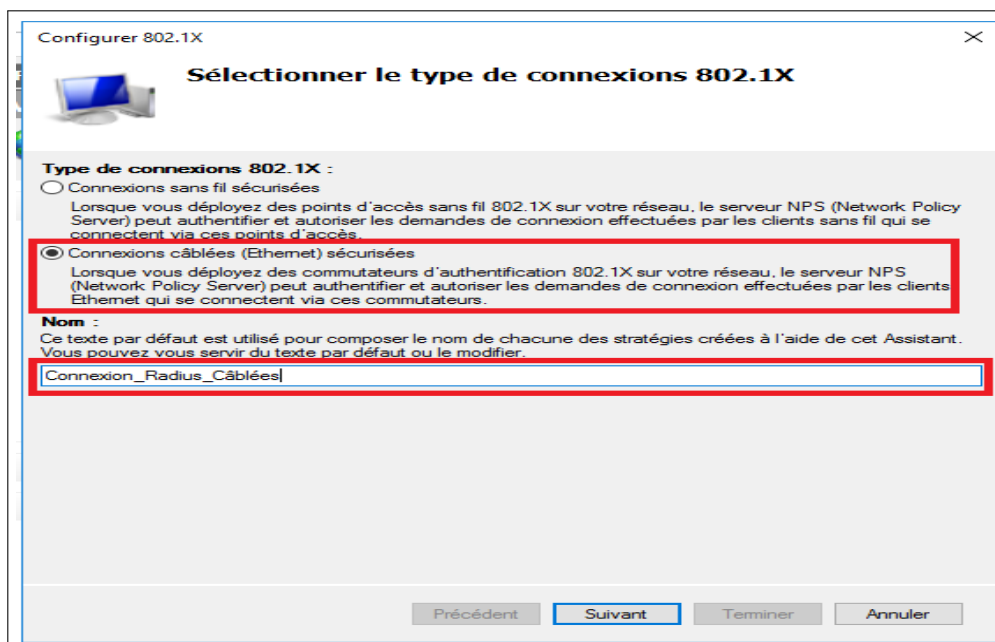


FIGURE 4.26 – Type de connexion 802.1X.

3. On ajoute notre client Radius "Client-Radius", l'authentificateur est le commutateur. Lorsque l'utilisateur est connecté à un port sur le commutateur, le commutateur nécessite une authentification de l'utilisateur. Nous avons signalé le client Radius "S-DRH" ci-dessus (figure 4.27).

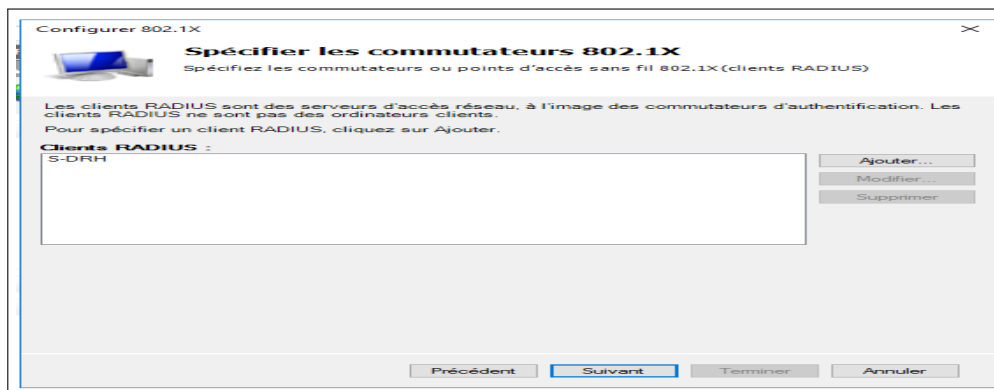


FIGURE 4.27 – Ajout de client Radius.

4. Configurez en utilisant n'importe quelle méthode d'authentification. On va utiliser "Microsoft : Protected EAP (PEAP)" (figure 4.28).

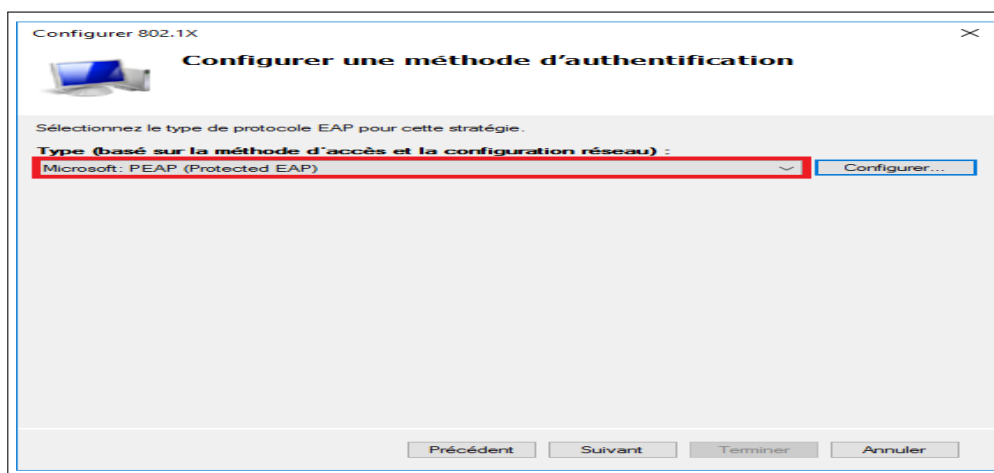


FIGURE 4.28 – Type de protocole pour cette stratégie.

5. Configurez la demande d'authentification pour l'utilisateur. Lorsque l'utilisateur est authentifié conformément aux conditions qu'on a définies ici, il sera autorisé à y accéder. On vas effectuer l'authentification avec les utilisateurs du groupe Active Directory, on spécifier le groupe d'utilisateurs "G-Radius" pour cette stratégie (figure 4.29).

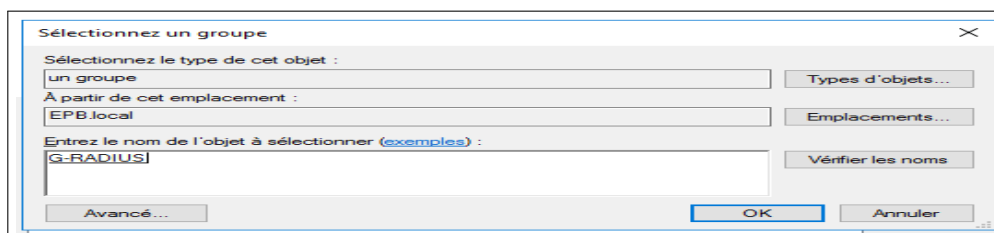


FIGURE 4.29 – Spécification de groupe d'utilisateurs pour la connexion 802 .1x câblée.

6. Après la création de la stratégie NPS 802.1x pour les connexions câblées, on configure les conditions (figure 4.30) :

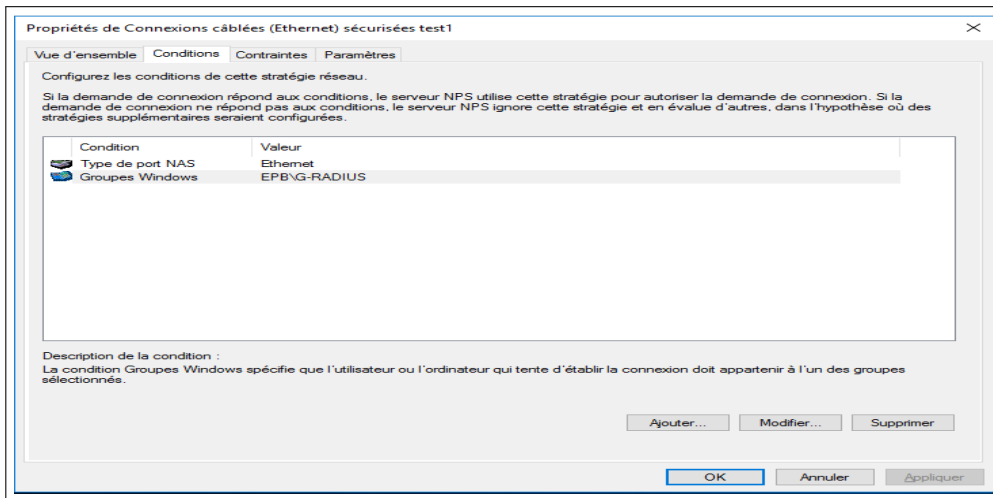


FIGURE 4.30 – Configuration des conditions de cette stratégie réseau.

7. Dans l'onglet "contraints" (contraintes), on choisit les méthodes d'authentification dans notre cas en a ajouté type de protocole EAP : « Protected EAP » et on a coché les cases « authentification chiffrée Microsoft version 2 (MS-CHAP v2) » et « authentification chiffrée Microsoft (MS-CHAP) » (figure 4.31).

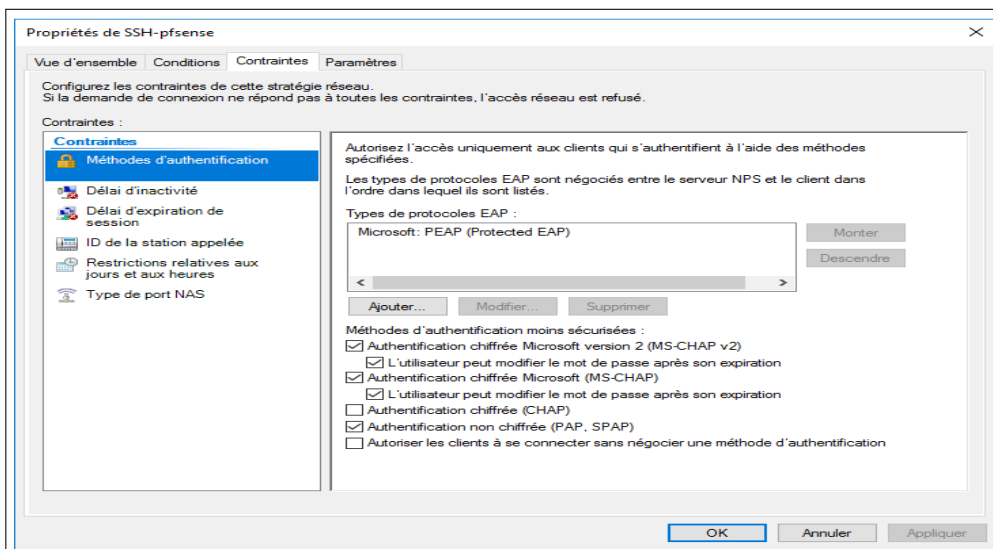


FIGURE 4.31 – Choix des méthodes d'authentification.

8. Dans le même onglet " Paramètres "  $\implies$  " Attributs Radius "  $\implies$  " Standard ", on ajoute les attributs : Filter-Id, Tunnel-Medium-Type, et l'attribut " tunnel-Type " (figure 4.32).

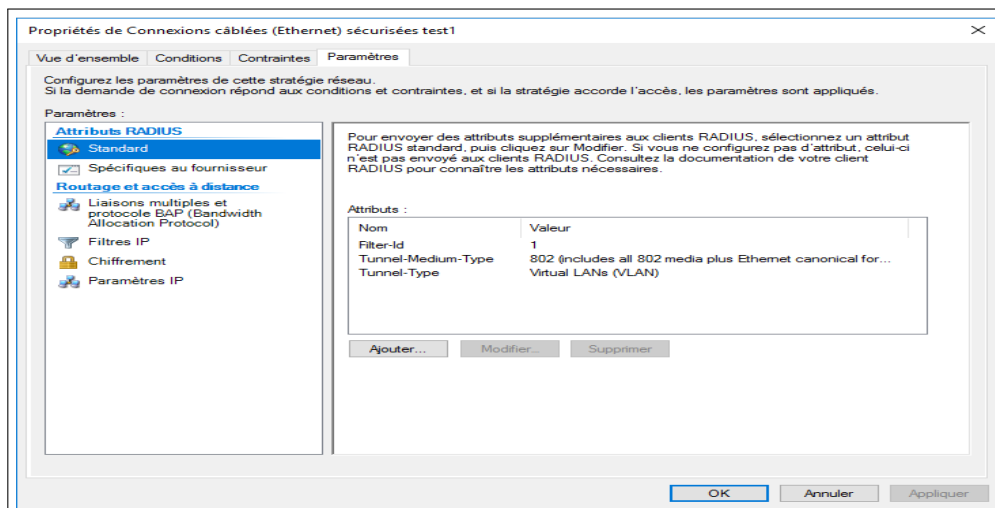


FIGURE 4.32 – Ajout d’attributs Radius.

#### D. Configurations du client Radius « pfsense »

1. Pour configuration du client Radius « pfsense » on suit les mêmes étapes que celles de switch.

#### E. Création d’une nouvelle stratégie réseau pour pare-feu « pfsense »

1. On va créer une politique réseau pour permettre l’authentification. Cliquez à droite sur le dossier des stratégies réseau et sélectionner la nouvelle option  $\Rightarrow$  saisir le nom  $\Rightarrow$  next  $\Rightarrow$  configuré les conditions « Nous allons permettre aux membres du groupe G-Radius de s’authentifier » (figure 4.33).

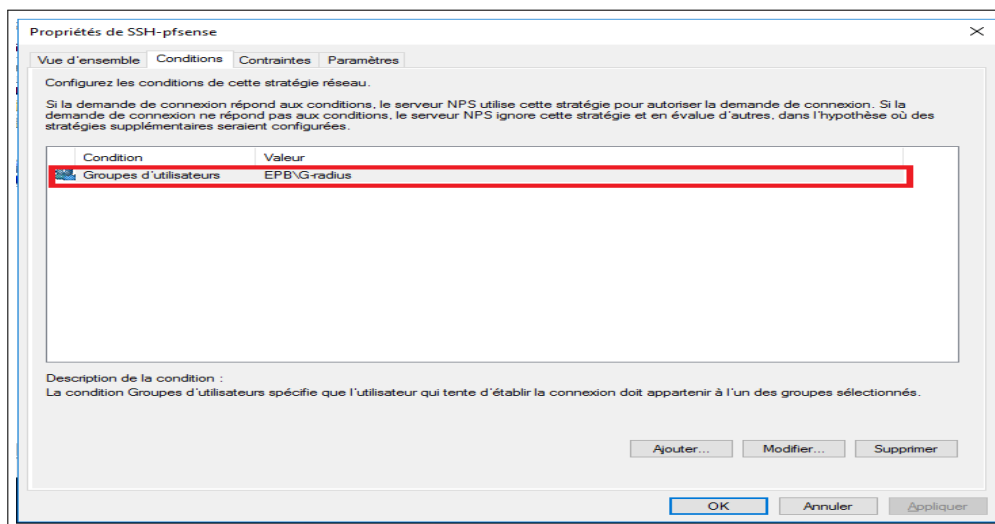


FIGURE 4.33 – Configuration des conditions de cette stratégie réseau.

2. Dans l’onglet "contraints" (contraintes), on choisit les méthodes d’authentification dans notre cas en a ajouté type de protocole EAP : « Protected EAP » et on a coché les cases suivante, « authentification chiffrée Microsoft version 2 (MS-CHAP v2) » et « authentification chiffrée Microsoft (MS-CHAP) » ainsi « authentification non chiffrée » (figure 4.34).

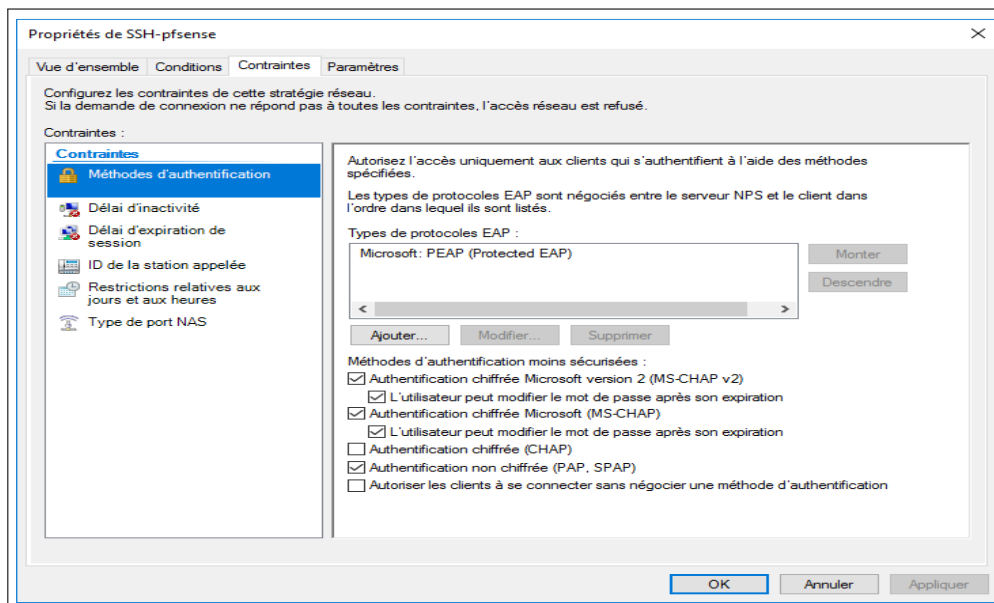


FIGURE 4.34 – Choix des méthodes d'authentification.

3. Dans le même onglet " Paramètres "  $\implies$  " Attributs Radius "  $\implies$  " Standard ", on ajoute les attributs : Class, Framed-Protocol et Service-Type (figure 4.35).

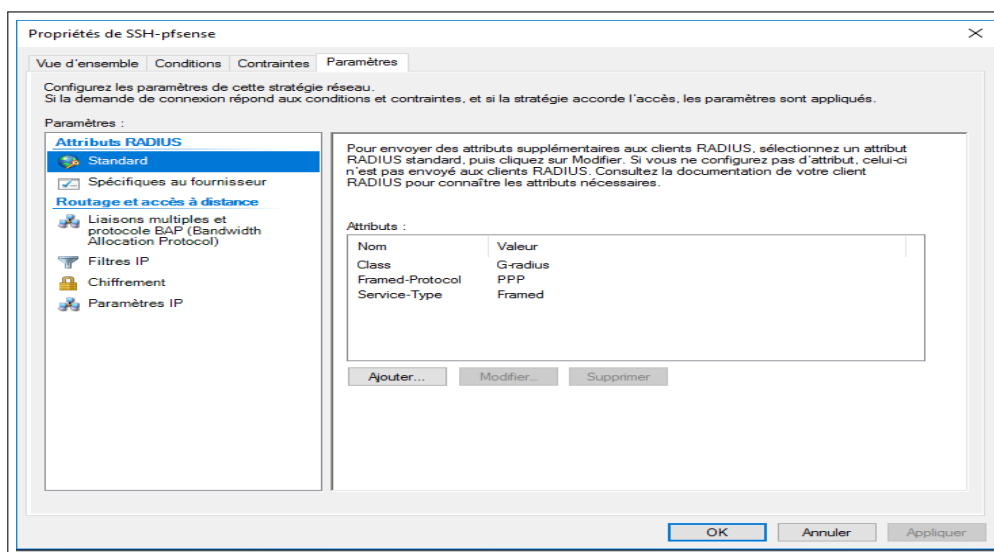


FIGURE 4.35 – Ajout d'attributs Radius.

#### 4.4.5 Configuration de serveur

1. dans cette partie en vas attribuer une adresse IP statique au serveur ( figure 4.36).



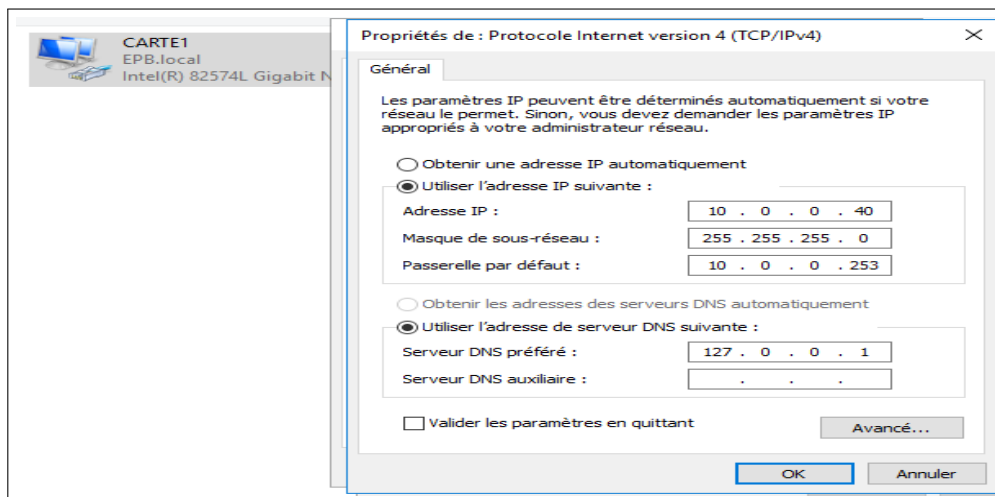


FIGURE 4.36 – Attribution d'une adresse statique au serveur.

#### 4.4.6 Activer Radius dans pare-feu « Pfsense »

##### A. Authentification pfsense Radius sur l'annuaire actif

1. Ouvrir le navigateur  $\implies$  saisir l'adresse IP « 172.16.100.253 » du pare-feu « Pfsense »  $\implies$  saisir username et password une fois à l'intérieur de l'interface du pare-feu  $\implies$  Accéder au menu Pfsense System et sélectionner option du gestionnaire d'utilisateur  $\implies$  sur l'écran du gestionnaire utilisateur, accéder à l'onglet Authentication Serveurs  $\implies$  remplir les paramètres (figure 4.37).

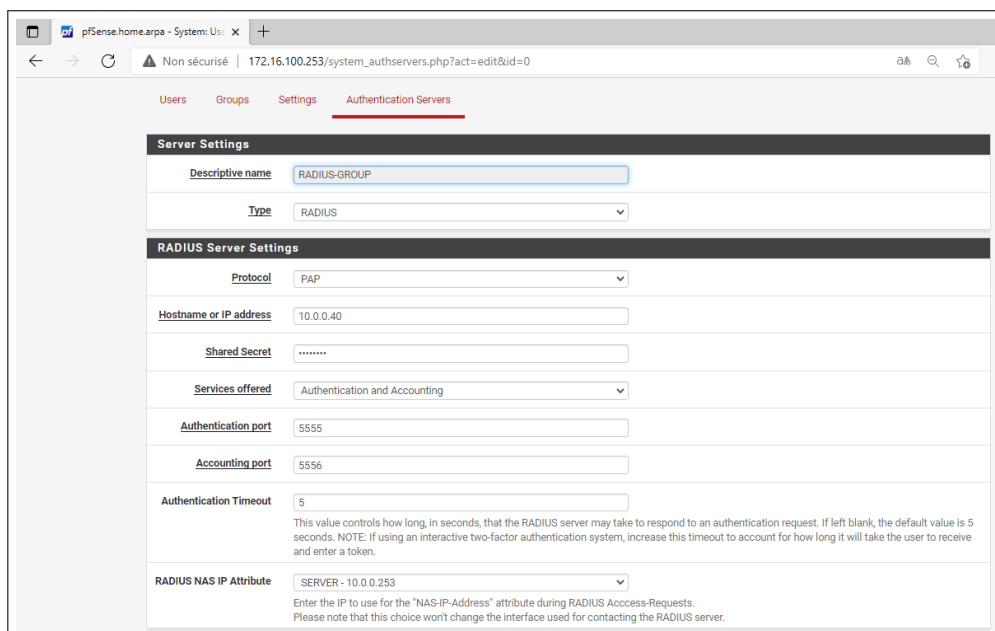


FIGURE 4.37 – Configuration l'authentification du serveur Radius.

### B. PFSense - Autorisation active du groupe d'annuaires

1. Sur l'écran du gestionnaire utilisateur, accéder à l'onglet Groupes et effectuer la configuration suivante (figure 4.38) :

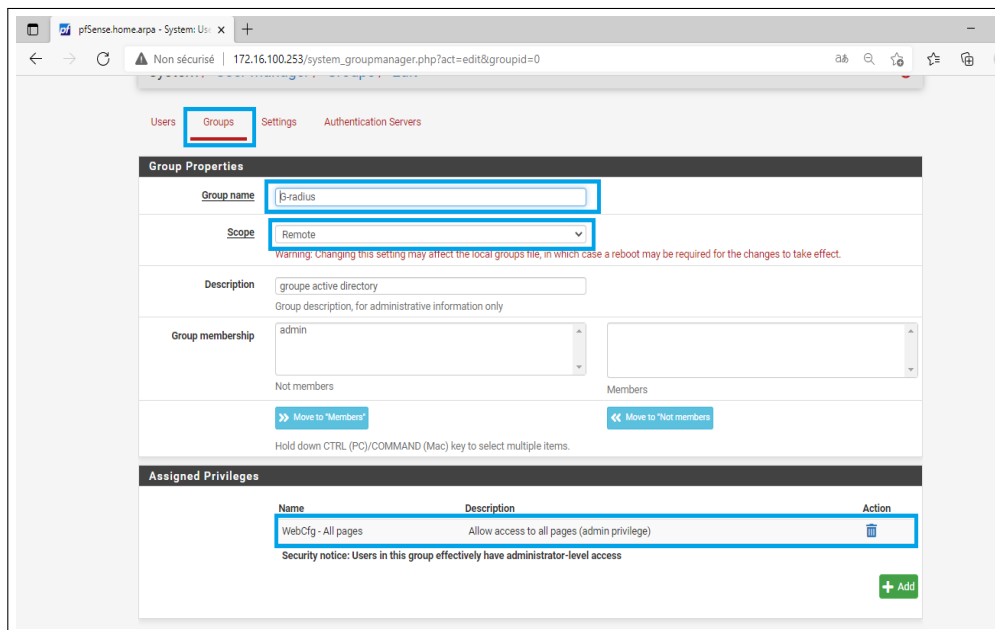


FIGURE 4.38 – Configuration autorisation active du groupe d'annuaires.

### C. PFSense - Activer l'authentification active du répertoire

1. Sur l'écran du gestionnaire utilisateur, accéder à l'onglet paramètres (figure 4.39).

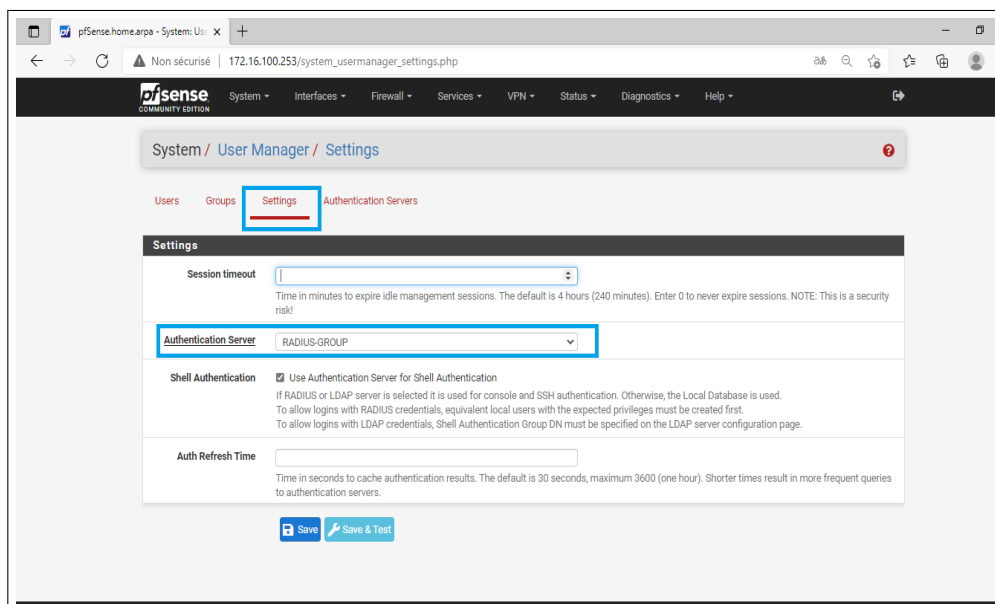


FIGURE 4.39 – Activer l'authentification du répertoire.

La configuration de notre serveur Radius sous Windows server 2016 est achevée, alors on passe à la configuration de la machine utilisateur (client sous Windows 10).

## 4.5 Configuration de client d'accès (Windows 10)

Pour la configuration de la machine de l'utilisateur (machine cliente) "Windows 10", on a suivi les étapes suivantes :

### A. Etape 1 :

Activer le service de configuration automatique de réseau câblé, qui est désactivé par défaut. Pour cela on doit taper "services" dans le champ de recherche présent dans la barre des tâches, On clique sur le service "configuration automatique du réseau câblé", "automatique" puis "démarrer" (figure 4.40).

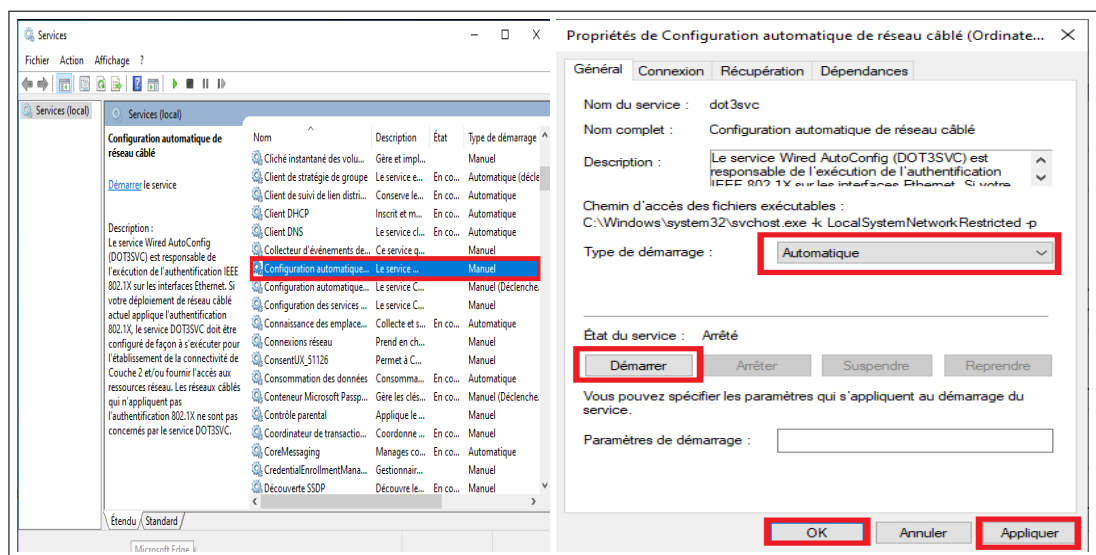


FIGURE 4.40 – Démarrage de service " Configuration automatique de réseau câblé".

### B. Etape 2 :

Pour ouvrir la connexion réseau, cliquer sur les boutons suivants : Démarrer, Panneau de configuration, Réseau et Internet, Centre réseau et partage, puis sur Gérer les connexions réseau. On clique avec le bouton droit sur la connexion pour laquelle on souhaite activer l'authentification 802.1X, puis sur Propriétés. On clique sur l'onglet " Authentification " ==> "Activer l'authentification IEEE 802.1X" puis on sélectionne "EAP protégé (PEAP)" comme Type EAP (figure 4.41).

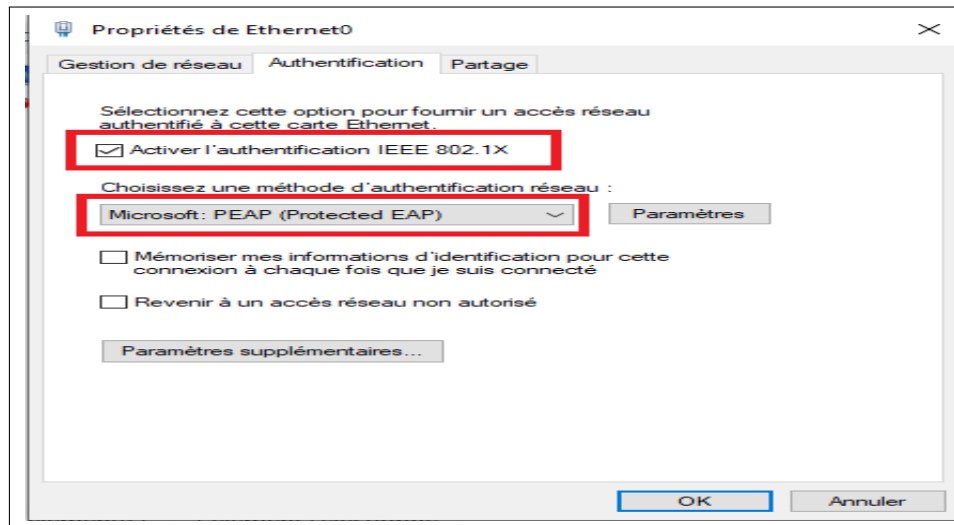


FIGURE 4.41 – Activation de l'authentification 802.1x.

### C. Etape 3 :

Cliquer sur propriétés du Type EAP puis décocher "Valider le certificat du Serveur" puis sélectionner "EAP-MSCHAP v2" comme méthode d'authentification et cliquer sur "Configurer" pour décocher "Utiliser automatiquement mon nom et mon mot de passe Windows d'ouverture de session" (figure 4.42).

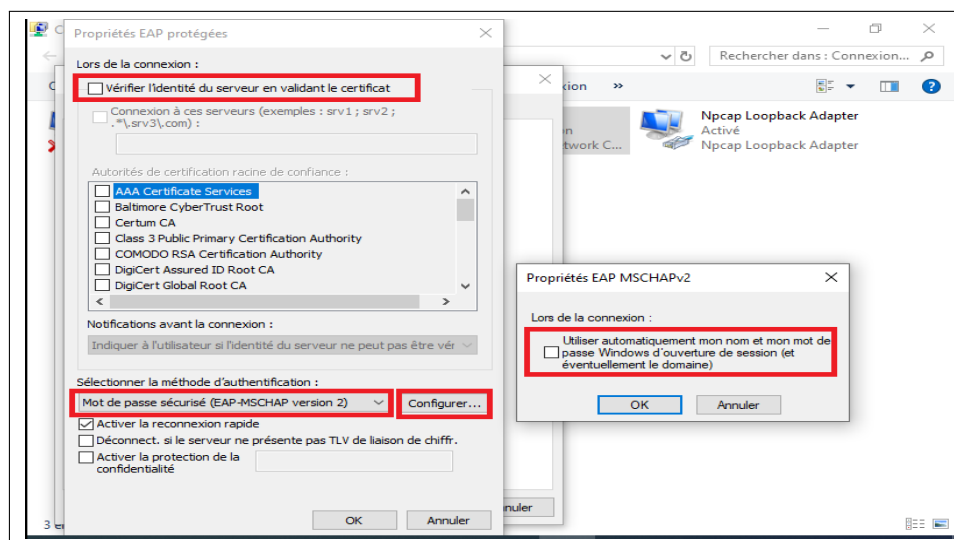


FIGURE 4.42 – Sélection de méthode d'authentification " EAP-MSCHAP v2 ".

### D. Etape 4 :

L'ajout de la machine au domaine "démarrer", un clic droit sur "poste de travail", puis sur "propriétés", "Nom de l'ordinateur", "Modifier", indiquer le nom de domaine (EPB.local) et en fin sur OK (figure 4.43).

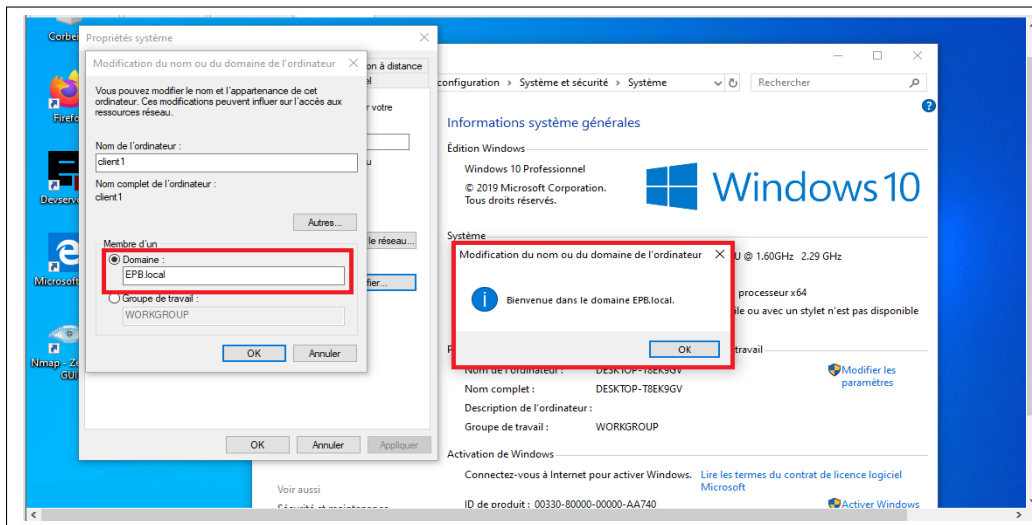


FIGURE 4.43 – Ajout de la machine au domaine.

## 4.6 Présentation de l'architecture réseau

Dans le but de mettre en évidence les étapes nécessaires à l'installation de Radius, nous avons choisi le réseau représenté par la figure 4.44. L'utilisation de Radius dans ce cas permettra d'authentifier le client pour accéder à un service quelconque.

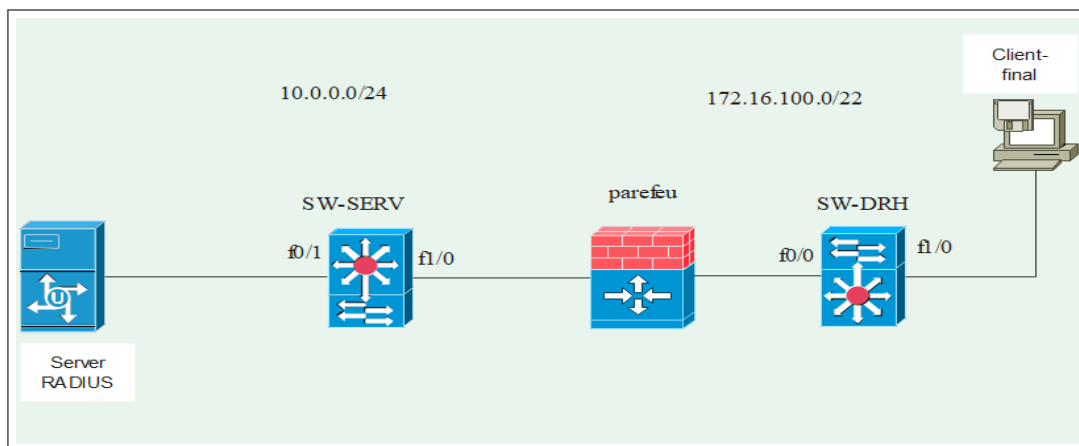


FIGURE 4.44 – Architecture du réseau proposé.

### 4.6.1 Configuration de la partie réseau

A. les adresses utilisées sont résumés dans le tableau suivant :

On a deux réseaux un du côté Lan l'autre du coté serveur :

- Adresse réseau serveurs : **10.0.0.0/24**
- Adresse réseau utilisateurs : **172.16.100.0/22**

Pour les switches on a utilisé un vlan par défaut qui est le vlan 1.

Cette figure représente tableau adressage utilisé :

Equipement	adresse	Masque	Adresse vlan1	Masque vlan1	Gateway
Serveur	10.0.0.40	255.255.255.0			
Pfsense coté Serveur	10.0.0.253	255.255.255.0			
Pfsense coté utilisateurs	172.16.100.253	255.255.252.0			
S-SERV			10.0.0.20	255.255.255.0	10.0.0.253
S-DRH			172.16.100.250	255.255.252.0	172.16.100.253

FIGURE 4.45 – Tableau d’adressage .

## B. pare-feu « pfsense »

A installation de pfsense on aura par défaut deux carte réseau une sur le LAN et l’autre sur le WAN, dans notre cas le LAN est devisé par deux : coté serveurs et coté utilisateurs, pour modifier les adresses et donenr une adresse de notre réseau à l’aide de-la console du pare-feu (figure 4.46) en clique sur 2 puis on choisit 1 et on inscrit l’adresse de l’interface qui est du coté utilisateurs et son masque ensuite en saisie l’adresse dans le navigateur en aura l’interface du pfsense et on ajoute une carte réseau qui est du coté serveur et on inscrit son adresse et son masque (figure 4.47).

```

Starting CRON... done.
pfSense 2.5.1-RELEASE amd64 Mon Apr 12 07:50:14 EDT 2021
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 4d66cc371e8a00c0e970

*** Welcome to pfSense 2.5.1-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/PPP4: 192.168.211.134/24
LAN (lan)      -> em1      -> v4: 172.16.100.253/22
SERVER (opt1)  -> em2      -> v4: 10.0.0.253/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                    16) Restart PHP-FPM
8) Shell

Enter an option: █
    
```

FIGURE 4.46 – console du pare-feu après insertion de nos adresses.

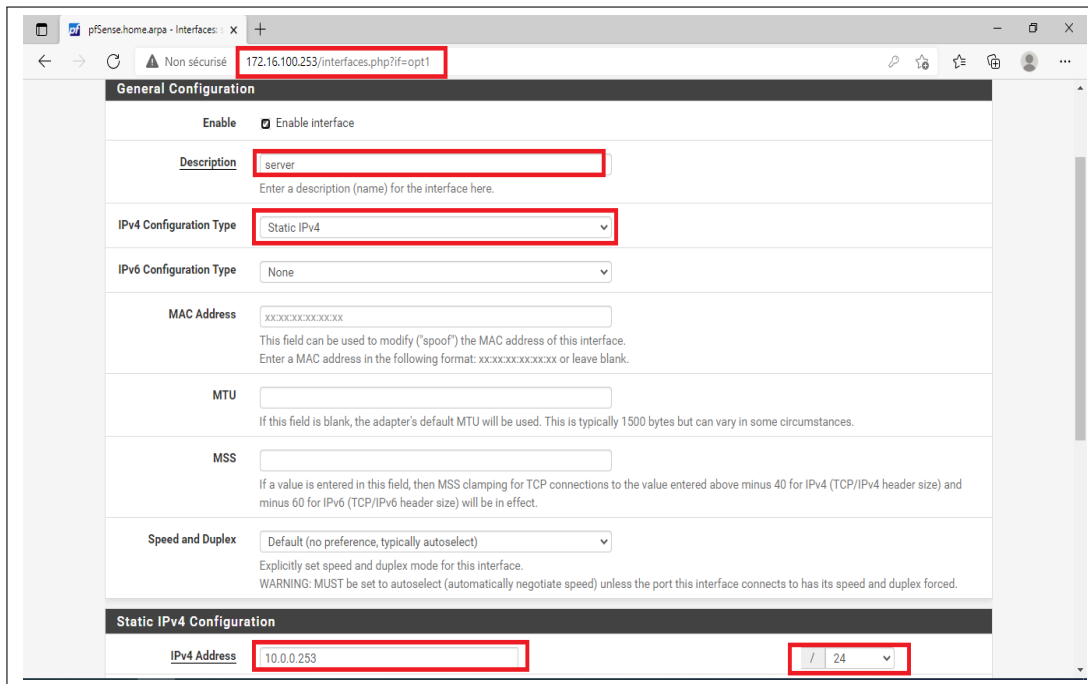


FIGURE 4.47 – Ajout de la carte réseau coté serveur sur pare-feu.

### C. Configuration du Commutateur

Nous on a utilisé (Switch S-DRH) comme exemple en ce que concerne autre switch en suis les mêmes étapes.

1. Définit l'adresse IP de l'interface VLAN 1 pour le client (figure 4.48).

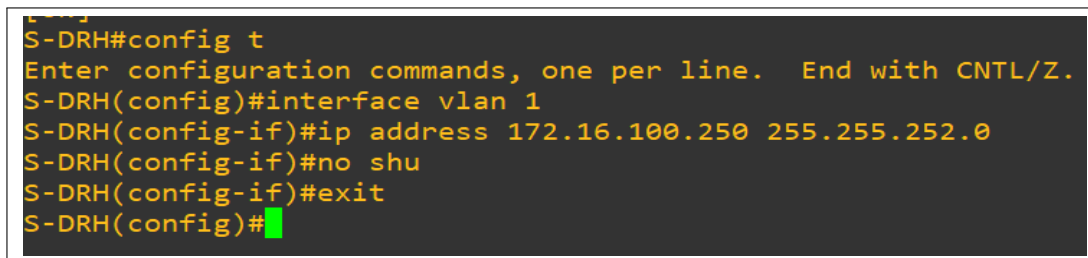


FIGURE 4.48 – Configuration de l'interface vlan 1.

### D. Configuration de l'authentification sur commutateur

- **Authentification Radius 802.1x**

Nous avons pris comme exemple (Switch S-DRH) en ce qui concerne autre Switch en suit les mêmes étapes.

1. Activer le modèle AAA en utilisant la commande : « aaa new model » (figure 4.49).



FIGURE 4.49 – Activer le modèle AAA.

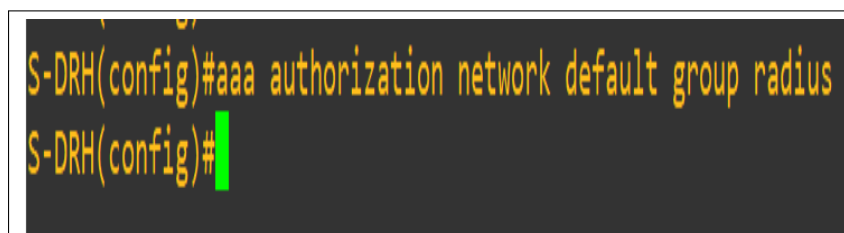
2. Créer une liste d'authentification "default" qui indique que L'authentification des utilisateurs se fera en 802.1x grâce au protocole Radius (figure 4.50).



```
S-DRH(config)#aaa authentication dot1x default group radius
```

FIGURE 4.50 – Authentification.

3. L'autorisation d'accès au réseau par le serveur Radius (figure 4.51).



```
S-DRH(config)#aaa authorization network default group radius  
S-DRH(config)#
```

FIGURE 4.51 – Autorisation d'accès au réseau.

4. Après, on active le protocole 802.1x sur le switch (Client-Radius) (figure 4.52).



```
S-DRH(config)#dot1x system-auth-control
```

FIGURE 4.52 – Activation du protocole 802.1x sur Client Radius.



5. Configurer les paramètres du serveur Radius et le port d'authentification et d'accès ainsi que la clé de Cryptage partagé entre le client Radius (switch) et le serveur Radius (figure 4.53).

```
S-DRH(config)#radius-server host 10.0.0.40 auth-port 1812 acct-port 1813 key Ryma1308
```

FIGURE 4.53 – Configuration de l'adresse IP de serveur Radius.

6. Activer le 802.1X sur le port relié à l'utilisateur : « Configurer L'authentification basée sur le port f1/0» (figure 4.54).

```
S-DRH(config)#int f1/0
S-DRH(config-if)#switchport mode access
S-DRH(config-if)#dot1x port-control auto
S-DRH(config-if)#
*Mar 1 01:24:15.575: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to down
S-DRH(config-if)#
```

FIGURE 4.54 – Activation du protocole 802.1x sur le port de l'utilisateur.

- **Authentification Radius sur un switch avec SSH**

Lorsqu'un utilisateur souhaite se connecter à son équipement réseau, Switch Cisco en SSH il doit spécifier un login et un mot de passe pour être autorisé à rentrer. On peut stocker username et secret password en local mais ce n'est pas ça qui nous intéresse nous on veut utiliser l'authentification avec les utilisateurs créé dans active directory qui appartient au groupe radius pour que le Serveur Radius sera chargé de valider l'authentification des utilisateurs qui souhaitent se connecter aux équipements réseaux. Pour que le Switch demande au Serveur Radius d'authentifier les utilisateurs il faut spécifier quelques informations (figure 4.55).

```
S-DRH#config t
Enter configuration commands, one per line. End with CNTL/Z.
S-DRH(config)#aaa new-model
S-DRH(config)#aaa authentication login default group radius local
S-DRH(config)#aaa authentication enable default group radius enable
S-DRH(config)#aaa authorization console
S-DRH(config)#aaa authorization exec default group radius local
S-DRH(config)#ip radius source-interface f1/0
S-DRH(config)#radius-server host 10.0.0.40 key Ryma1308
S-DRH(config)#line console 0
S-DRH(config-line)#login authentication default
S-DRH(config-line)#authorization exec default
S-DRH(config-line)#line vty 0 15
S-DRH(config-line)#login authentication default
S-DRH(config-line)#authorization exec default
S-DRH(config-line)#
```

FIGURE 4.55 – Authentification Radius.

1. Maintenant il faut Activer le protocole SSH au niveau du switch (figure 4.56).

```

switch#config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)#hostname S-DRH
S-DRH(config)#end
S-DRH#
S-DRH#
*Mar 1 00:01:11.671: %SYS-5-CONFIG_I: Configured from console by console
S-DRH#
S-DRH#
S-DRH#config t
Enter configuration commands, one per line. End with CNTL/Z.
S-DRH(config)#ip domain-name EPB.local
S-DRH(config)#crypto key generate rsa
The name for the keys will be: S-DRH.EPB.local
Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

S-DRH(config)#
*Mar 1 00:02:06.255: %SSH-5-ENABLED: SSH 1.99 has been enabled
S-DRH(config)#ip ssh version 2
S-DRH(config)#ip ssh logging events
S-DRH(config)#ip ssh time-out 100
S-DRH(config)#ip ssh authentication-retries 3
S-DRH(config)#line vty 0 15
S-DRH(config-line)#transport input ssh
S-DRH(config-line)#transport output ssh
S-DRH(config-line)#exit
S-DRH(config)#

```

FIGURE 4.56 – Activer le protocole SSH.

## 4.7 Tests

Le serveur Radius est le « moteur » de la mobilité c’est l’élément structurant du réseau.

### A. Wireshark

Le but d’utiliser Wireshark c’est pour la capture et l’analyse du trafic réseau.

1. Pour ouvrir Wireshark, un clic droit sur les bulles vertes des interfaces sous GNS3, puis un clic sur "Start Wireshark " (figure 4.57).

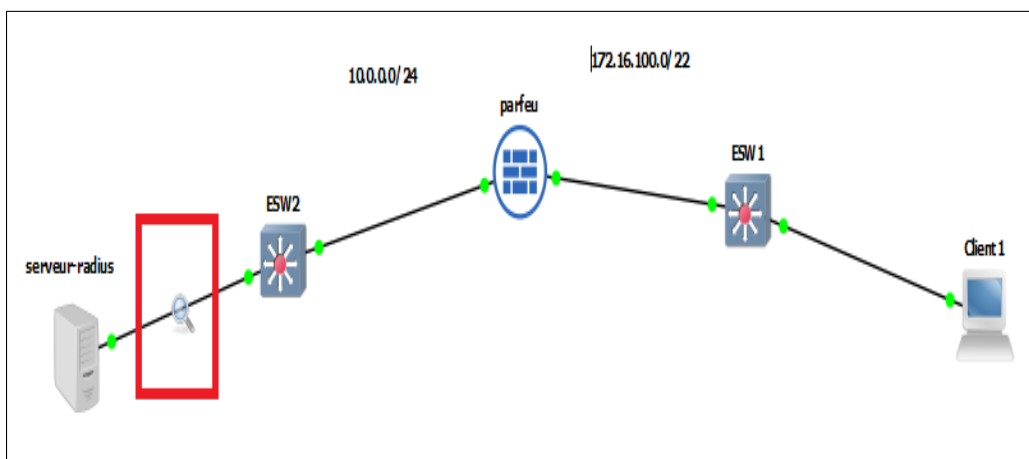


FIGURE 4.57 – Wireshark sous GNS3.

- Wireshark nous permet aussi de suivre la conversation autrement dit les différents types de paquets Radius échanger entre le switch et le serveur Radius. Sans serveur Radius y'aura pas du client Radius qui se charge du filtrage des entrées des connexions. Il demande à l'utilisateur ses identifiants de connexion et les communiquent de manière sécurisée avec le serveur Radius (figure 4.58) .

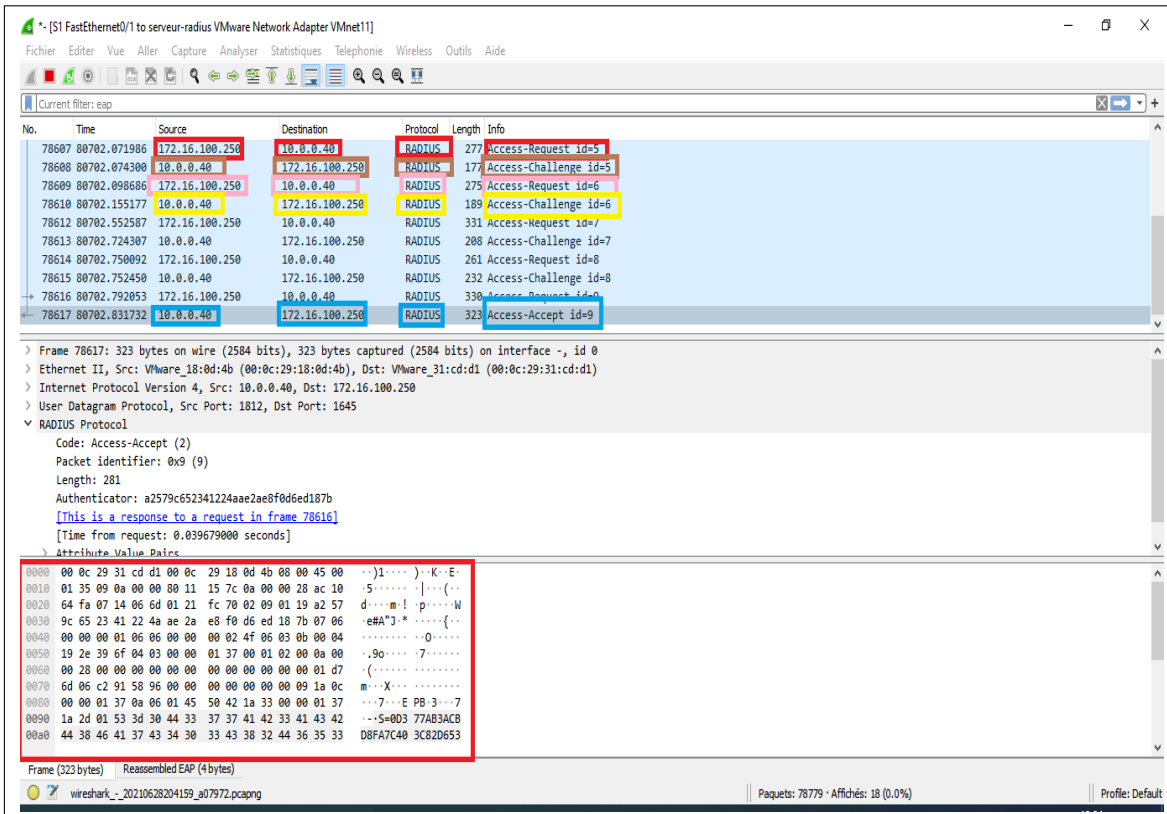


FIGURE 4.58 – Analyse de la conversation entre switch et serveur.

## B. Authentification d'un utilisateur au serveur radius

- Avec le client sous Windows 10 en test l'authentification par rapport au serveur Radius en utilisant les utilisateurs créés sur active directory qui appartient au groupe Radius. A la connexion du client une fenêtre s'affiche lui demandant de saisir nom de l'utilisateur ainsi que le mot de passe. Selon la zone d'accès demandée, sans Radius y'aura pas une verification de l'identité celui-ci utilise les protocoles d'authentification PAP, CHAP ou EAP qui se chargent de définir comment l'information est cryptée et comment fonctionne le mécanisme de clé privée / clé publique sur le réseau. Ce dernier pourra exiger des informations supplémentaires pour l'authentification. Il est capable de bloquer une connexion en cours, suite par exemple à un délai d'inactivité dépassé. Enfin, il assure la journalisation des accès à partir de l'étude des ports UDP (figure 4.59).

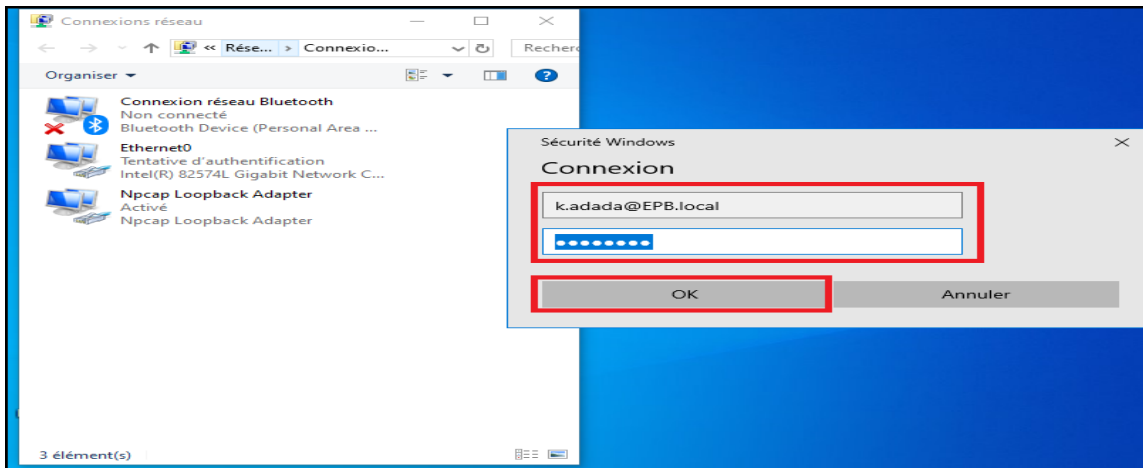


FIGURE 4.59 – Test d’authentification d’un utilisateur.

- Sur le serveur Radius on vérifie que s’est connecté au serveur autrement dit vérifie la traçabilité de l’utilisateur en utilisant « observateur d’évènements », les étapes à suivre : cliquer sur observateur d’évènements puis sur affichage personnalisés aller sur rôles de serveurs et cliquer sur services de stratégie et d’accès réseau. Sans Radius ya pas de traçabilité des utilisateurs connectés au serveur , c’est pour cela il est conseiller d’utiliser Radius car il permet de garder trace de chaque activité (figure 4.60).

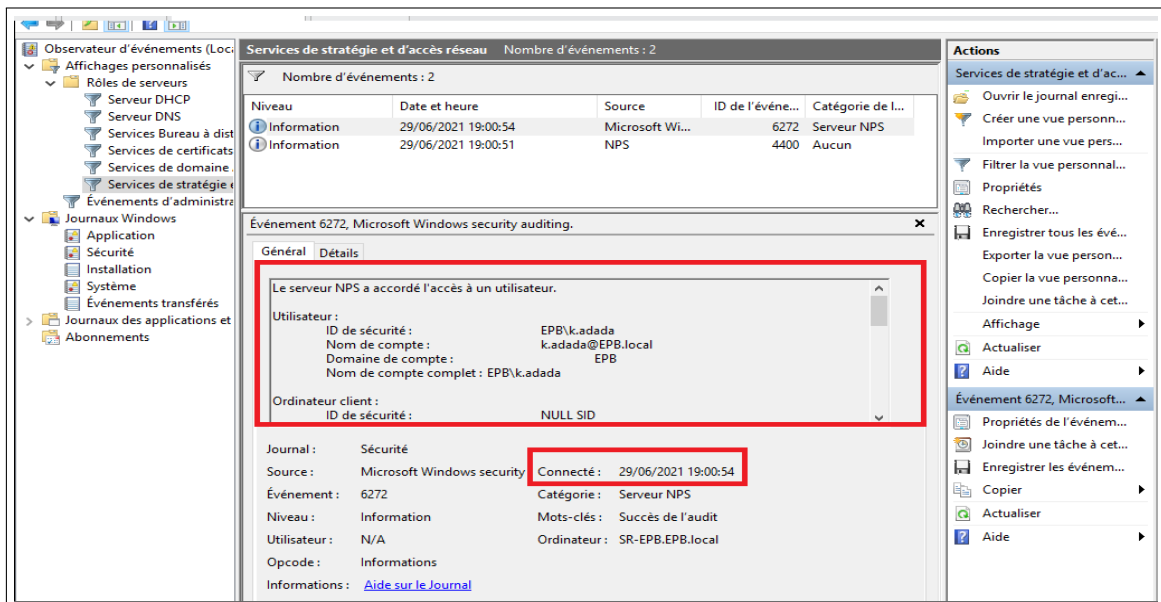


FIGURE 4.60 – Traçabilité de l’utilisateur connecté au serveur Radius.

### C. Test de connexion à partir de la machine cliente XP avec Putty au serveur d’accès

- il faut d’abord vérifier que notre machine Windows 10 à une adresse IP (attribuée par le serveur DHCP) (figure 4.61).

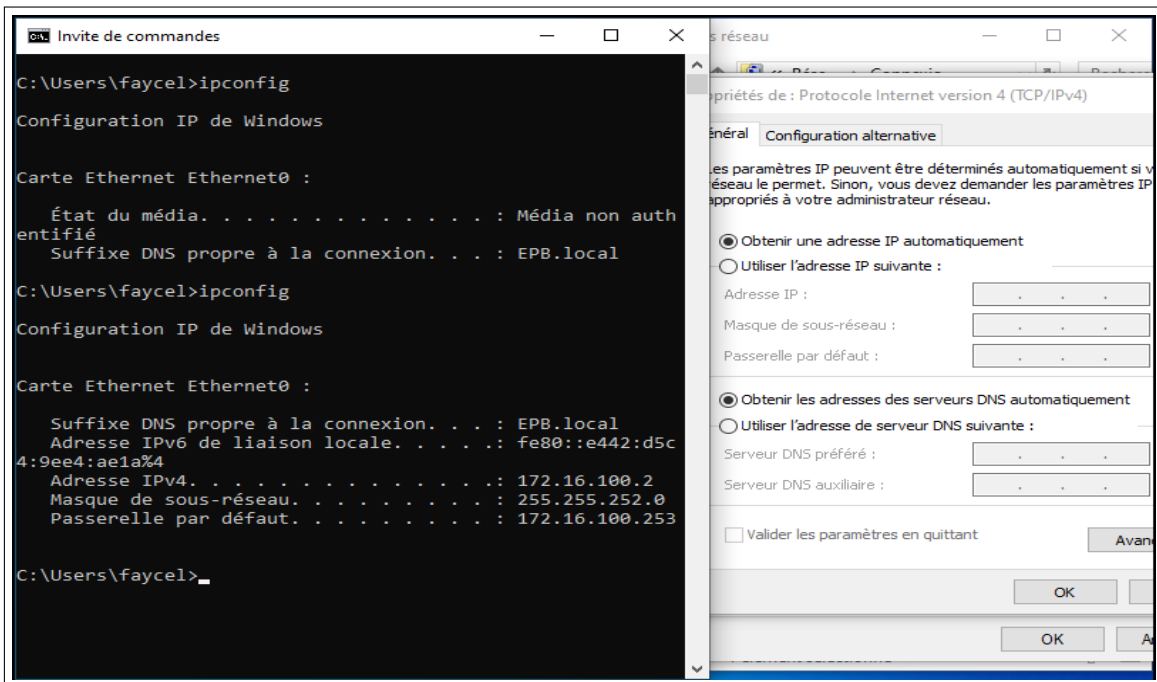


FIGURE 4.61 – Vérification d’adresse IP de la machine Windows 10.

Une fois l’adresse est attribuée, le client sous Windows 10 utilise le logiciel putty en SSH pour accéder à son équipement réseau désiré.

2. l’accès au switch avec un client SSH (**SSH (Secure Shell)** : permet de se connecter à une machine distante avec une liaison sécurisée )[23].

Afin de s’assurer de notre bonne configuration, nous avons effectué des tests en faisant appel à " PUTTY " qui est un logiciel (et un protocole) permettant de se connecter à un ordinateur distant de façon sécurisée et permet en particulier d’ouvrir un Shell à distance sur le client d’accès [23] (figure 4.62).

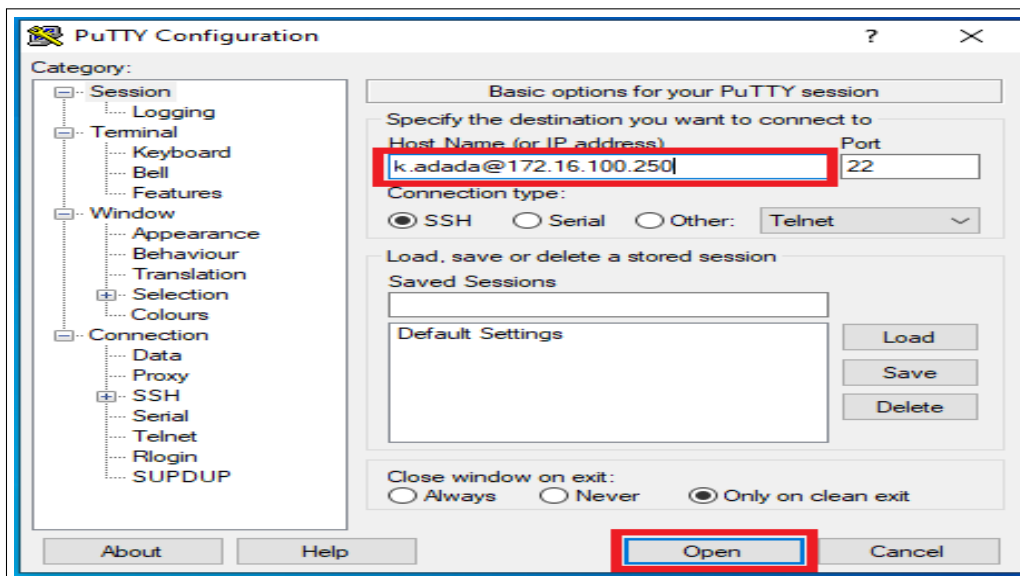


FIGURE 4.62 – L’accès au switch avec un client SSH.

- Il faut maintenant introduire le mot de passe pour accéder au switch. Sans Radius pas de gestion des mots de passe et pas de gestion des connexions d'utilisateurs à des services distants. Ce dernier permet qu'aux membres du groupe Radius d'accéder à ces services en utilisant leur propre mot de passe (figure 4.63).

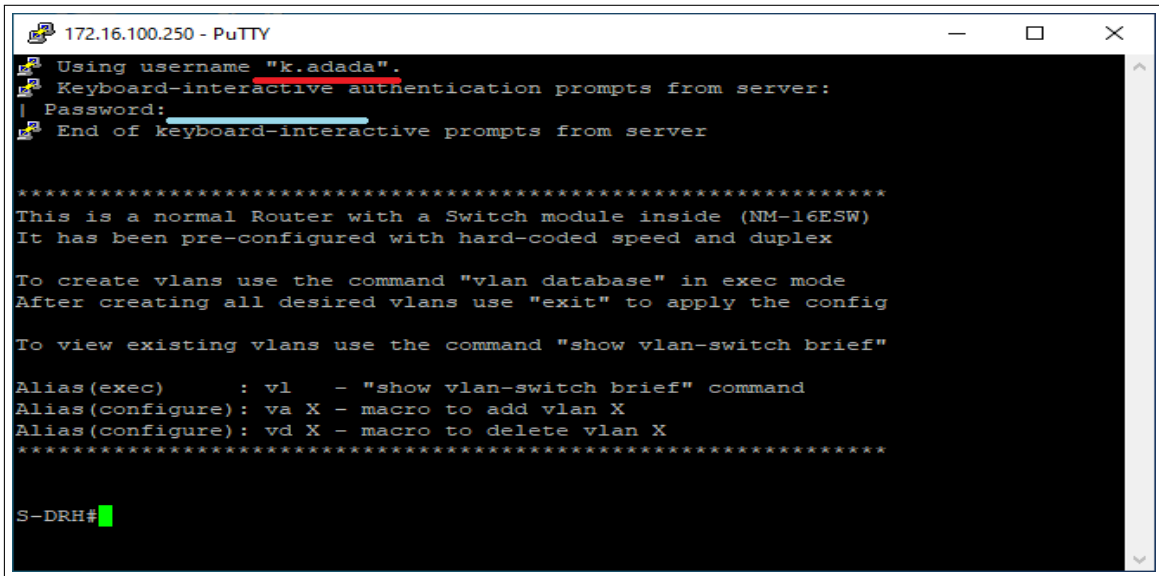


FIGURE 4.63 – L'accès au switch avec mot de passe .

- Comme on a vérifié précédemment l'utilisateur qui est membre du groupe Radius, prenant maintenant un utilisateur qui n'est pas un membre du groupe (sachant que notre stratégie NPS n'autorise que les utilisateurs qui ne sont pas membre du groupe) (figure 4.64).

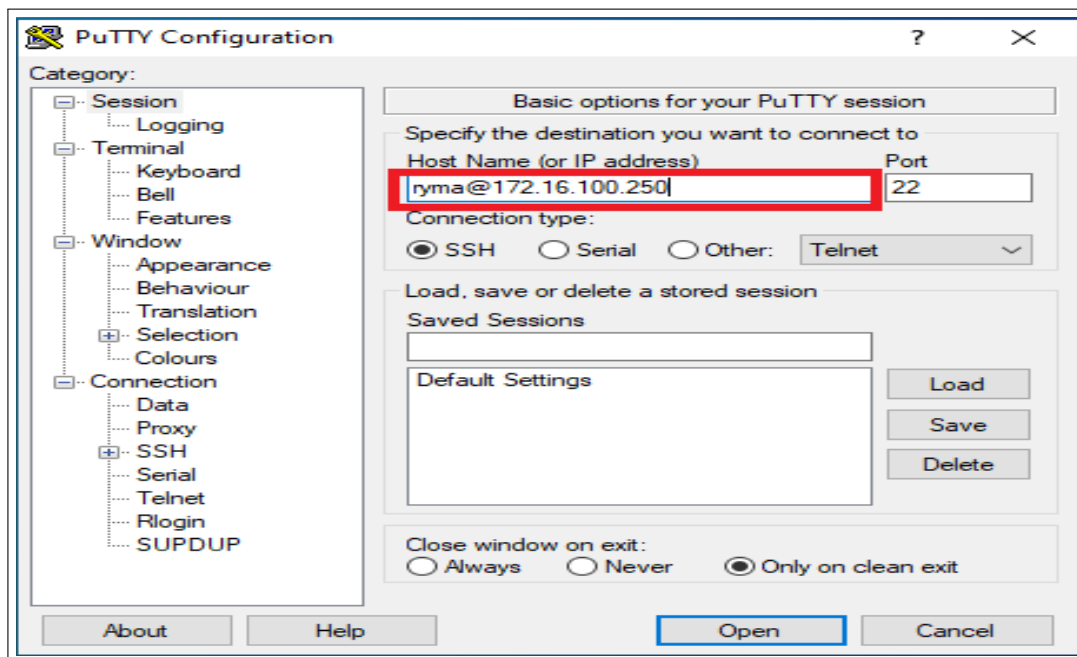


FIGURE 4.64 – L'accès au switch avec un client SSH.

- Il faut maintenant introduire le mot de passe pour accéder au switch (figure 4.65).

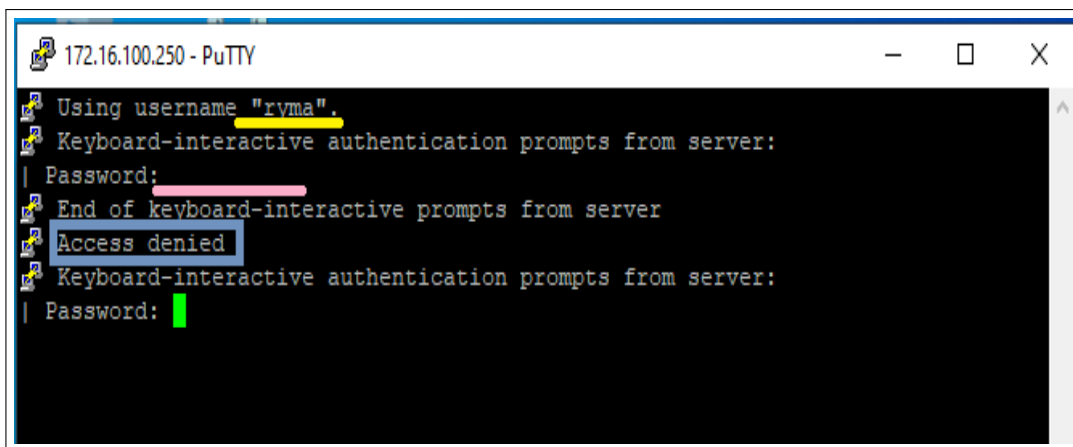


FIGURE 4.65 – L'accès au switch avec password.

Delà on conclut que sans Radius l'accès n'est pas sécurisée ce dernier permet qu'aux utilisateurs qui sont membres du groupe Radius d'accéder pour les autres utilisateurs y'aura un accès refusé « Access denied ».

#### D. PFSense Radius – Teste de L'Authentification active Directory

- Sur menu Pfsense Diagnostics : sélectionner l'option Authentification ⇒ sélectionner le serveur d'authentification du répertoire Actif ⇒ saisir le nom d'utilisateur qui appartient à G-Radius, son mot de passe et cliquer sur le bouton Test (figure 4.66).

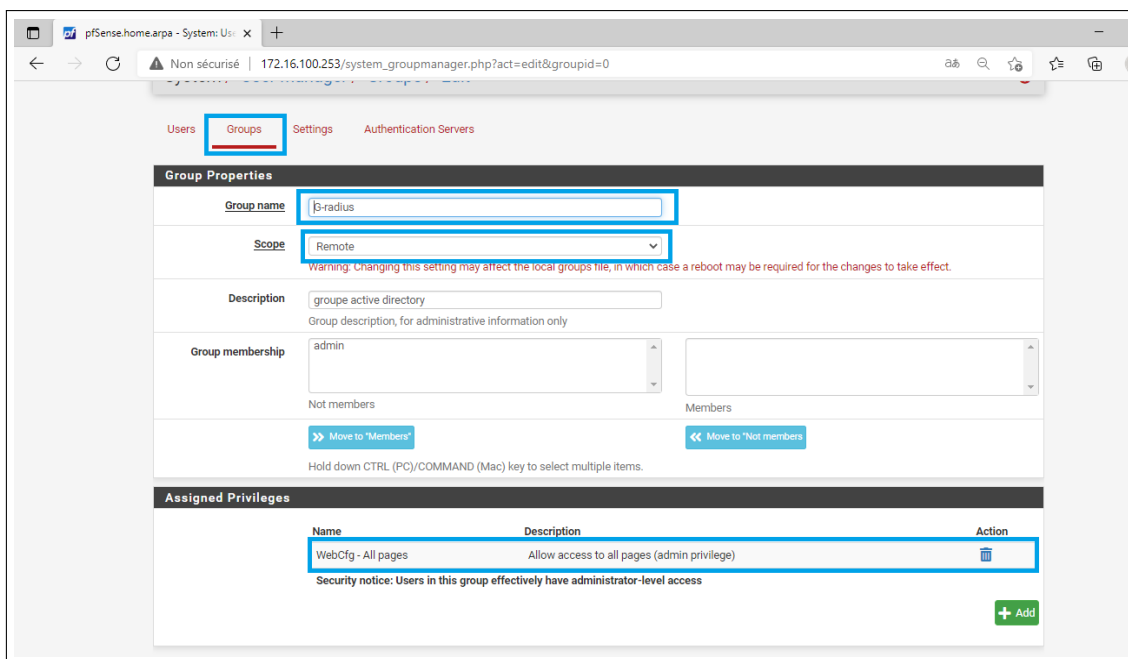


FIGURE 4.66 – Succès de L'authentification du serveur PFSense Radius sur Active Directory.

## 4.8 Conclusion

Le Serveur de contrôle d'accès Radius constitue une réponse aux problématiques de connexion au réseau local et permet de mieux contrôler l'accès au réseau. Radius présente l'avantage d'être simple à installer. De plus, le fait qu'il reconnait les comptes déjà existants dans Active Directory, l'administrateur réseau ne va pas recréer ces comptes une deuxième fois sur équipement. Parvenu au terme de notre étude, on peut retenir qu'après l'identification des utilisateurs, leur Authentification est nécessaire pour accéder aux données d'un système.

Cette authentification, ce fait par l'intermédiaire d'un serveur d'authentification, chargé d'autoriser ou non l'accès aux données. Afin de permettre le service d'authentification, ce serveur nécessite une configuration de ses composantes, ce fut là le but de notre travail.



# Conclusion Générale

La protection d'un réseau est une étape délicate qui permet de le sécuriser contre les risques les plus courants. Les hackers emploient de plus en plus de stratégies pour dissimuler leurs caractères intrusifs et les applications sont de plus en plus nomades. Il faut alors prendre au sérieux les risques provenant du réseau et analyser régulièrement son trafic, afin de détecter les utilisateurs non autorisés.

Dans ce mémoire, nous avons mis en œuvre une technique de sécurisation d'accès au réseau informatique de l'entreprise portuaire de Bejaïa, afin de mieux garantir les critères de la sécurité : authentification, intégrité et la confidentialité des données échangées entre différents utilisateurs. Cette technique permet de contrôler l'accès physique aux équipements d'infrastructures réseaux en utilisant le protocole EAP pour le transport des informations d'identification en mode client/serveur, et un serveur d'identification Radius utilisant une base de données Active Directory. Radius permet d'assurer l'authentification des clients avant tout accès au réseau d'EPB de Bejaïa. L'avantage de ce dernier est d'utiliser le protocole AAA, permettant aux opérateurs d'authentifier les utilisateurs et de leur autoriser certains services.

Pour la réalisation de service d'authentification Radius, nous avons installé et configuré Windows serveur 2016 (serveur DHCP, DNS, serveur NPS), et on a pu configurer le protocole 802.1x. Ensuite nous avons appliqué l'authentification sur différents équipements de notre réseau. Lors de la configuration du protocole 802.1x au niveau de l'authentificateur nous avons acquis beaucoup de connaissances sur le fonctionnement et la configuration des équipements Cisco.

Nous avons également eu beaucoup de plaisir à apprendre et à nous familiariser avec le Windows server 2016 pour mieux gérer la sécurité de notre architecture réseau.

La mise en œuvre de ce projet, nous a permis d'apporter une contribution à l'entreprise EPB de Bejaïa mais aussi d'acquérir de nouvelles connaissances sur le protocole authentification Radius grâce à une étude détaillée sur son fonctionnement, ses principes et les protocoles qu'il utilise. Durant notre formation, nous avons mis en pratique ces connaissances.

Pour finir, nous pensons que la mise en œuvre du protocole Radius est d'une importance capitale pour le bon fonctionnement du réseau informatique

## CONCLUSION GÉNÉRALE

---

de n'importe quelle entreprise. Ce dernier permet uniquement de remédier au problème d'authentification et ne permet pas de faire face aux autres attaques telles que le DoS. Par conséquent, dans le cas d'un réseau d'entreprise nous devons utiliser des outils supplémentaires pour la sécurité comme les antivirus .

# Bibliographie

- [1] G. Pujolle, « *Les réseaux* », EYROLLES, Paris, 8<sup>ème</sup> édition, 2014.
- [2] A. Sider, « *Cours Modèle Client/serveur* », Cours de 2<sup>ème</sup> année licence académique en informatique, Université de Bejaïa, 2018.
- [3] Z. Farah, « *Cours Introduction à la sécurité* », Cours Master 1 professionnel informatique, Université de Bejaïa, 2019.
- [4] S. Ghernouati-Hélie, « *sécurité informatique et réseaux* », Dunod, 3<sup>ème</sup> édition, 2008.
- [5] M. Rizcallah, « *annuaire LDAP* », EYROLLES, édition 2002.
- [6] G. Mathieu, « *Tester la sécurité de son annuaire Active Directory V2* », version du 30 janvier 2016.
- [7] D. Lachiver, « *Utilisation du réseau pédagogique* », édition 2013.
- [8] B. Lloyd, W. Simpson, « *PPP Authentication Protocol* », édition octobre 1992.
- [9] W. Simpson, « *PPP Challenge Handshake Authentication Protocol (CHAP)* », édition 1996.
- [10] G. Desgeorge, « *La sécurité des réseaux* », édition 2000.
- [11] R. Kanneganti, « *sécurité des réseaux* », 1<sup>ere</sup> édition, Ed. Manning, 1 juin 2008.
- [12] G. Hallen, « *CCNP Security IPS 642-627 quick referencen Cisco presse Library of Bolvon Calin Borgdan* », édition 2011.
- [13] S. Rigney et al., « *remote authentication dial in user service (radius)* », édition juin 2000.

- [14] S. Bordères, « *Authentification réseau avec Radius* », EYROLLES, édition 2006.
- [15] S. Bordères, « *Authentification réseau avec Radius* », EYROLLES, édition 2000.
- [16] A. Mazouzi, « *Services d'Authentification et Annuaire* », UFR Informatique, UCB Lyon1, 14 décembre 2009.
- [17] W. Simpson, « *The Point-to-Point Protocol (PPP)* », édition 1994.
- [18] B. Aboba et al., « *PPP Extensible Authentication Protocol (EAP)* », RFC 3748, édition Juin 2004.
- [19] B. Aboba, D. Simon, « *PPP EAP TLS authentication protocol* », RFC 2716, édition October 1999.
- [20] P. Funk, S. Blake-Wilson, « *EAP Tunneled TLS Authentication Protocol (EAP-TTLS)* », draft-ietf-pppext-eap-ttls-05.txt, Internet-Draft, édition Juillet 2004.
- [21] A. Géron, « *WiFi Déploiement et sécurité* », Dunod, édition 2006.
- [22] J. Sebban, « *Analyseur de paquets réseau pour les pros* », édition 1997.
- [23] W. Lucas, « *SSH Mastery* », openSSH, PUTTY, Tunnels and keys, 2<sup>ème</sup> édition, octobre 2010.
- [24] J.Delduca, « *la sécurité informatique en mode projet-organisez la sécurité du SI de votre entreprise* », ENI, 2010.
- [25] M.Chateau et al., *Windows Server 2008 R2 administration avancée*, 2<sup>ème</sup> édition, Eni édition, 2011.

# Résumé

De nos jours, la sécurité informatique est quasi-indispensable pour le bon fonctionnement d'un réseau filaire ou non filaire, pour cela les administrateurs réseau d'entreprise doivent mettre des mécanismes de sécurité plus performante.

L'objectif de notre projet consiste à implémenter une solution d'authentification pour le réseau Ethernet de l'EPB, pour cela, nous avons choisi le protocole Radius qui est l'un des protocoles d'authentification les plus performants.

Pour la réalisation de ce travail, nous avons fait d'abord un rappel sur les notions de bases de réseau et la sécurité informatique pour bien comprendre les concepts répondant à la problématique, et pour l'implémentation de la solution, nous avons choisi Windows Server 2016 qui inclut le serveur d'authentification Radius et la base de données Active Directory pour l'enregistrement des comptes utilisateurs.

**Mots clés :** authentication,Ethernet,Radius, Windows Server 2016,Active Directory.

# Abstract

Nowadays, computer security is almost essential for the proper functioning of a wired or non-wired network, for this corporate network administrators must put more efficient security mechanisms.

The objective of our project is to implement an authentication solution for the Ethernet network of the EPB, for this we have chosen the Radius protocol which is one of the most efficient authentication protocols.

For the realization of this work, we first made a reminder on the basic notions of Network and security to fully understand the concepts that address the problem, and for the implementation of the solution, we chose Windows Server 2016 which includes the Radius authentication server and the Active Directory database for the registration of user accounts.

**Keywords :** authentication,Ethernet,Radius, Windows Server 2016,Active Directory.