

الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة

التعليم العالي والبحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة أبي بكر بلقايد -

تلمس -

Université Aboubakr Belkaïd – Tlemcen –

Faculté de TECHNOLOGIE



MEMOIRE

Présenté pour l'obtention du **diplôme** de **MASTER**

En : Télécommunications

Spécialité : Réseaux & Télécommunications

Par : **DIDI MOHAMMED REDA & SELADJI ABDELKRIM**

Sujet

**Implémentation d'une infrastructure à clé publique (PKI)
dans un environnement Windows et Linux**

Soutenu publiquement, en Juin 2020, devant le jury composé de :

Mr MERZOUGUI Rachid	Professeur	Univ. Tlemcen	Président
Mr MOUSSAOUI Djilali	Maitre de Conférences	Univ. Tlemcen	Examineur
Mr ABDELMALEK Abdelhafid	Maitre de Conférences	Univ. Tlemcen	Directeur de mémoire

Remerciements

En préambule à ce mémoire nous remercions ALLAH qui nous a aidé et nous a donné la patience et le courage durant ces longues années d'étude.

Nous souhaitons adresser nos plus sincères remerciements aux personnes qui nous ont apportées leur aide et qui ont contribuées à l'élaboration de ce mémoire, ainsi qu'à notre réussite au cours de cette année universitaire.

Ces remerciements vont tout d'abord au corps enseignant et administratif de la Faculté de technologie, pour les grands efforts fournis pour assurer à leurs étudiants une formation actualisée.

Nous tenons à remercier sincèrement Monsieur Abdelmalek Abdelhafid Maitre de conférences à l'université de Tlemcen qui est notre Directeur de mémoire, il fut toujours à l'écoute et très disponible tout au long de la réalisation de ce mémoire, pour l'inspiration, l'aide et le temps qu'il a bien voulu nous consacrer et sans son soutien ce mémoire n'aurait jamais vu le jour. Nos remerciements les plus sincères lui vont donc en particulier.

Nous exprimons notre gratitude à Monsieur Merzougui Rachid, Professeur à l'université de Tlemcen, pour l'honneur qu'il nous fait en présidant notre Jury, ainsi qu'à Monsieur MOUSSAOUI Djilali, Maitre de conférences à l'université de Tlemcen, pour l'honneur qu'il nous fait en participant à notre jury.

Nous les remercions sincèrement pour le temps qu'ils ont consacré à la lecture et à l'évaluation de notre travail.

Nous n'oublions pas nos parents pour leur contribution, leur soutien et leur patience. Enfin, nous adressons nos plus sincères remerciements à tous nos proches et amis, qui nous ont toujours encouragées au cours de la réalisation de ce mémoire.

Merci à tous et à toutes.

Résumé

Avec l'utilisation mondiale de l'Internet, l'aspect sécuritaire reste un point de faiblesse et cause de bien des tracas lorsqu'il survient.

Actuellement, les mots de passe sont en passe de devenir obsolètes sinon faibles et remplacés par l'utilisation de certificats pour une authentification bien plus sûre. Techniquement, une PKI est en définitive quelques serveurs, sur lesquels fonctionnent des logiciels spécifiques chargés de générer des certificats numériques et de contrôler leur validité, mais pas que.

Dans ce travail, nous nous sommes donc proposé d'utiliser une PKI pour assurer l'authentification lors de l'accès à un réseau Wifi, un site Web et un serveur mail, aussi bien sous Linux que sous Windows.

Ce travail se propose de détailler toutes les étapes importantes dans l'implémentation donc d'une PKI de A à Z.

Mot clés: Sécurité, PKI, Linux, Windows.

Abstract

With the global use of the Internet, the security aspect remains a point of weakness and causes great problems when it occurs.

Currently, passwords are becoming obsolete, if not weak, and replaced by the use of certificates for much more secure authentication.

Technically, a PKI is ultimately a few servers, on which specific software works, responsible for generating digital certificates and checking their validity, but not only.

In this work, we therefore proposed to use a PKI to ensure authentication when accessing a Wi-Fi network, a website and a mail server, both under Linux and under Windows. This work will detail all the important steps in the implementation of a PKI from A to Z.

Keywords: Security, PKI, Linux, Windows.

المخلص

مع الاستخدام العالمي للإنترنت ، يظل الجانب الأمني نقطة ضعف ويسبب مشكلات كبيرة عند حدوثه. في الوقت الحالي ، أصبحت كلمات المرور قديمة ، إن لم تكن ضعيفة ، ويتم استبدالها باستخدام الشهادات للحصول على مصادقة أكثر أمانًا. من الناحية الفنية ،

هي في النهاية عدد قليل من الخوادم ، حيث يتحمل برنامج معين مسؤولية إنشاء (PKI) فإن البنية التحتية للمفاتيح العمومية الشهادات الرقمية والتحقق من صلاحيتها ، ولكن ليس فقط. ولذلك اقترحنا في العمل استخدام البنية التحتية للمفاتيح العمومية لضمان يقترح هذا العمل التفصيل. Windows أو في Linux وموقع ويب وخادم بريد ، سواء في Wi-Fi المصادقة عند الوصول إلى شبكة جميع الخطوات الهامة في تنفيذ البنية التحتية للمفاتيح العمومية من الألف إلى الياءة

الكلمات المفتاحية : الأمان , Linux, Windows, PKI.

Table des matières

REMERCIEMENTS	2
RESUME	3
ABSTRACT	3
المخلص	3
TABLE DES MATIERES.....	4
LISTE DES FIGURES.....	5
LISTE DES TABLEAUX	8
LISTE DES ANNEXES	8
LISTE DES ABREVIATIONS	8
INTRODUCTION GENERALE	10
CHAPITRE 1 : LA SECURITE INFORMATIQUE	14
I. INTRODUCTION.....	14
II. LA SECURITE INFORMATIQUE : C'EST QUOI ?	14
III. LA SECURITE INFORMATIQUE : POURQUOI ?.....	16
IV. LA SECURITE INFORMATIQUE : COMMENT ?	17
1. <i>Faire les mises à jour</i>	18
2. <i>Protéger son réseau</i>	19
3. <i>Complexifier les mots de passe</i>	19
4. <i>Sauvegarder régulièrement</i>	19
5. <i>L'utilisateur, pilier de la sécurité</i>	20
6. <i>Défaillance matérielle</i>	21
7. <i>Défaillance logicielle</i>	21
8. <i>Accidents (pannes, incendies, inondations...)</i>	21
9. <i>Le Chiffrement</i>	22
V. CONCLUSION.....	22
CHAPITRE 2 : ATTAQUE INFORMATIQUE ET PRESENTATION DE LA PKI.....	24
I. INTRODUCTION.....	24
II. TOUR D'HORIZON DES TYPES D'ATTQUES INFORMATIQUES	24
1. <i>Le cryptojacking, minage de crypto monnaie malveillant</i>	24
2. <i>Les Ransomware, rançongiciels</i>	25
3. <i>Les intrusions sur les objets connectés</i>	25
4. <i>Les attaques géopolitiques</i>	25
5. <i>Les scripts intersites ou cross-site Scripting (XSS)</i>	25
6. <i>Les malwares sur mobile</i>	26
7. <i>Le phishing ou l'hameçonnage</i>	26
8. <i>Le spoofing</i>	26
9. <i>Les attaques cyber-physiques</i>	26
10. <i>Les attaques contre les appareils et dossiers médicaux électroniques</i>	27
11. <i>Les attaques contre les véhicules connectés et semi-autonomes</i>	27
12. <i>Les attaques contre les espaces de stockage cloud :</i>	27
III. LA CRYPTOGRAPHIE A CLE PUBLIQUE.....	28
IV. CERTIFICAT NUMERIQUE	30
V. INFRASTRUCTURE A CLE PUBLIQUE PKI.....	32
VI. LE CONCEPT PKI.....	32

VII. PRINCIPE DE FONCTIONNEMENT DE LA PKI.....	33
1. Types de CA.....	33
2. Types de certificats.....	34
VIII. CONCLUSION	34
CHAPITRE 3 : IMPLEMENTATIONS D'UNE INFRASTRUCTURE PKI SOUS LINUX.....	36
I. INTRODUCTION.....	36
II. IMPLEMENTATION D'UNE INFRASTRUCTURE A CLE PUBLIQUE PKI.....	36
1. Créations d'une autorité de certification racine.....	37
III. UTILISATION DE LA PKI.....	40
1. Mise en place d'un serveur web sécurisé.....	40
2. Mise en place d'un serveur DNS.....	45
3. Mise en place d'un réseau Wi-Fi avec authentification basée sur des certificats.....	52
4. Mise en place d'un serveur Mail sécurisé.....	69
IV. CONCLUSION.....	77
CHAPITRE 4 : IMPLEMENTATION D'UNE INFRASTRUCTURE D'ENTREPRISE SOUS WINDOWS.....	79
I. INTRODUCTION.....	79
II. IMPLEMENTATIONS D'UNE INFRASTRUCTURE A CLE PUBLIQUE PKI	79
1. Création d'un domaine.....	80
2. Créations d'une autorité de certification racine.....	88
3. Créations d'une autorité de certification intermédiaire.....	96
III. UTILISATION DE LA PKI.....	100
1. Mise en place d'un serveur web sécurisé.....	100
2. Mise en place d'un réseau Wi-Fi avec authentification basée sur des certificats.....	106
3. Mise en place d'un serveur Mail sécurisé	117
IV. CONCLUSION.....	120
CONCLUSION GENERALE	122
ANNEXE : PRESENTATION DE WINDOWS SERVER ET DEBIAN	124
BIBLIOGRAPHIE	128

Liste des figures

FIGURE 1.1 LES OBJECTIFS QUE VISE LA SECURITE INFORMATIQUE[2]	16
FIGURE 1.2 LES GESTES A ADOPTER [5]	21
FIGURE 2.1 CERTIFICAT NUMERIQUE	31
FIGURE 2.2 CONCEPT D'UNE PKI[12]	33
FIGURE 3.1 SCHEMA DE NOTRE PKI[12].....	36
FIGURE 3.2 HIERARCHIE DE NOTRE PKI.....	39
FIGURE 3.3 LE BON FONCTIONNEMENT DU SERVEUR APACHE2	41
FIGURE 3.4 AUTORITE DE CERTIFICATION NON RECONNUE PAR LE NAVIGATEUR	44
FIGURE 3.5 NOM D'HOTE PLEINEMENT NOMME DE NOTRE SERVEUR WEB.....	45
FIGURE 3.6 CONFIGURATION DU SERVEUR DNS	46
FIGURE 3.7 DECLARATIONS DES ZONES DNS.....	47
FIGURE 3.8 CREATION DE LA ZONE DNS DIRECT	47
FIGURE 3.9 CREATION DE LA ZONE DNS INVERSE	48
FIGURE 3.10 VERIFICATION DE LA SYNTAXE.....	48
FIGURE 3.11 VERIFICATION DU BON FONCTIONNEMENT DU SERVEUR DNS.....	49
FIGURE 3.12 SERVEUR CORRECTEMENT SECURISE PAS CERTIFICAT SSL.....	50
FIGURE 3.13 CERTIFICAT DU SERVEUR	50

FIGURE 3.14 CHAINE DE CERTIFICAT (HIERARCHIE).....	51
FIGURE 3.15 CONFIGURATION DE L'UTILISATEUR EXTERNE.....	52
FIGURE 3.16 SERVEUR CORRECTEMENT SECURISE.....	52
FIGURE 3.17 CONFIGURATION DU SERVEUR RADIUS.....	54
FIGURE 3.18 CONFIGURATION DE DALORADIUS.....	56
FIGURE 3.19 INTERFACE DALORADIUS FONCTIONNELLE.....	56
FIGURE 3.20 AJOUT DE CLIENT AUTORISE A CONSULTER LA BASE DE DONNEES (POINT D'ACCES).....	57
FIGURE 3.21 AJOUT D'UN UTILISATEUR AUTORISE A SE CONNECTER AU POINT D'ACCES.....	57
FIGURE 3.22 DEMANDE DE CERTIFICAT UTILISATEUR.....	60
FIGURE 3.23 SIGNATURE DE LA DEMANDE PAR UNE AUTORITE DE CERTIFICATION.....	61
FIGURE 3.24 CERTIFICAT UTILISATEUR INSTALLE.....	62
FIGURE 3.25 CONFIGURATION DU POINT D'ACCES.....	63
FIGURE 3.26 CONFIGURATION DU CLIENT WIFI.....	64
FIGURE 3.27 AJOUT D'UN NOUVEAU RESEAU.....	64
FIGURE 3.28 CONFIGURATION D'UN NOUVEAU RESEAU SUR WINDOWS.....	65
FIGURE 3.29 CONFIGURATION DE LA METHODE D'AUTHENTIFICATION.....	65
FIGURE 3.30 RECEPTIONS ET ACCEPTATION DE LA DEMANDE D'ACCES DU CLIENT LINUX.....	66
FIGURE 3.31 RECEPTIONS ET ACCEPTATION DE LA DEMANDE D'ACCES DU CLIENT WINDOWS.....	66
FIGURE 3.32 CONNEXION CONFIRME DU CLIENT WINDOWS.....	67
FIGURE 3.33 CONFIGURATION D'UN CLIENT WI-FI NON AUTORISE.....	67
FIGURE 3.34 ACCES REFUSE A L'UTILISATEUR.....	68
FIGURE 3.35 VERIFICATION DE LA BONNE CONFIGURATION DU FQDN.....	70
FIGURE 3.36 INSTALLATION DE POSTFIX 1/2.....	70
FIGURE 3.37 INSTALLATION DE POSTFIX 2/2.....	71
FIGURE 3.38 TEST D'ENVOI DE COURRIER.....	72
FIGURE 3.39 ACCES AU PANNEAU D'ADMINISTRATION DU SERVEUR MAIL.....	75
FIGURE 3.40 CONFIGURATION DE NOTRE DOMAINE D'EMAIL.....	75
FIGURE 3.41 ACCES A NOTRE BOITE EMAIL.....	76
FIGURE 3.42 PAGE PRINCIPALE DU SERVEUR MAIL.....	76
FIGURE 3.43 ENVOIE D'EMAIL DE LA PART DU WEBMASTER VERS UN UTILISATEUR.....	77
FIGURE 3.44 RECEPTION DE L'EMAIL DU WEBMASTER PAR L'UTILISATEUR.....	77
FIGURE 4.1 SCHEMA DE LA PKI.....	79
FIGURE 4.2 GESTIONNAIRE DE SERVEUR.....	80
FIGURE 4.3 AJOUT DE NOUVEAU ROLE OU FONCTIONNALITE.....	80
FIGURE 4.4 SERVEUR DESTINATAIRE DU NOUVEAU ROLE.....	81
FIGURE 4.5 AJOUT DE ROLE AD-DS.....	81
FIGURE 4.6 INSTALLATION D'AD-DS.....	82
FIGURE 4.7 FINALISATION DE L'INSTALLATION D'AD-DS.....	82
FIGURE 4.8 CONFIGURATION D'AD-DS 1/2.....	83
FIGURE 4.9 CONFIGURATION D'AD-DS 2/2.....	83
FIGURE 4.10 FINALISATION DE LA CONFIGURATION D'AD-DS.....	84
FIGURE 4.11 VERIFICATION DU BON FONCTIONNEMENT DU DOMAINE.....	84
FIGURE 4.12 AJOUT D'EXCEPTION AU PARE-FEU 1/3.....	85
FIGURE 4.13 AJOUT D'EXCEPTION AU PARE-FEU 2/3.....	85
FIGURE 4.14 AJOUT D'EXCEPTION AU PARE-FEU 3/3.....	86
FIGURE 4.15 INFORMATION DU DEUXIEME SERVEUR.....	86
FIGURE 4.16 CONNEXION DU DEUXIEME SERVEUR AU DOMAINE.....	87
FIGURE 4.17 CONNEXION AU DOMAINE REUSSI.....	87
FIGURE 4.18 IDENTIFICATION AU COMPTE LIE AU DOMAINE.....	88
FIGURE 4.19 INSTALLATION D'UNE AUTORITE DE CERTIFICATION RACINE 1/3.....	88
FIGURE 4.20 INSTALLATION D'UNE AUTORITE DE CERTIFICATION RACINE 2/3.....	89
FIGURE 4.21 INSTALLATION D'UNE AUTORITE DE CERTIFICATION RACINE 3/3.....	89

FIGURE 4.22 CONFIGURATION DE L'AUTORITE DE CERTIFICATION RACINE 1/10	90
FIGURE 4.23 CONFIGURATION DE L'AUTORITE DE CERTIFICATION RACINE 2/10	90
FIGURE 4.24 CONFIGURATION DE L'AUTORITE DE CERTIFICATION RACINE 3/10	91
FIGURE 4.25 CONFIGURATION DE L'AUTORITE DE CERTIFICATION RACINE 4/10	91
FIGURE 4.26 CONFIGURATION DE L'AUTORITE DE CERTIFICATION RACINE 5/10	92
FIGURE 4.27 CONFIGURATION DE L'AUTORITE DE CERTIFICATION RACINE 6/10	92
FIGURE 4.28 CONFIGURATION DE L'AUTORITE DE CERTIFICATION RACINE 7/10	93
FIGURE 4.29 CONFIGURATION DE L'AUTORITE DE CERTIFICATION RACINE 8/10	93
FIGURE 4.30 CONFIGURATION DE L'AUTORITE DE CERTIFICATION RACINE 9/10	94
FIGURE 4.31 CONFIGURATION DE L'AUTORITE DE CERTIFICATION RACINE 10/10	94
FIGURE 4.32 FINALISATION DE LA CONFIGURATION DE L'AC RACINE	95
FIGURE 4.33 ACCES A L'AUTORITE DE CERTIFICATION RACINE	95
FIGURE 4.34 AUTORITE DE CERTIFICATION RACINE OPERATIONNELLE.....	95
FIGURE 4.35 INSTALLATION DE L'AUTORITE DE CERTIFICATION SECONDAIRE.....	96
FIGURE 4.36 CONFIGURATION DE L'AUTORITE DE CERTIFICATION SECONDAIRE 1/3	96
FIGURE 4.37 CONFIGURATION DE L'AUTORITE DE CERTIFICATION SECONDAIRE 2/3	97
FIGURE 4.38 CONFIGURATION DE L'AUTORITE DE CERTIFICATION SECONDAIRE 3/3	97
FIGURE 4.39 ENVOIE DE DEMANDE DE CERTIFICATION AUTOMATIQUE A L'AC RACINE.....	98
FIGURE 4.40 FINALISATION DE LA CONFIGURATION DE L'AC SECONDAIRE	99
FIGURE 4.41 CERTIFICAT DELIVRE PAR L'AC RACINE	99
FIGURE 4.42 AUTORITE DE CERTIFICATION SECONDAIRE OPERATIONNELLE	99
FIGURE 4.43 SITE WEB ACCESSIBLE ET NON SECURISE	100
FIGURE 4.44 EXECUTION DE LA COMMANDE MMC	101
FIGURE 4.45 AJOUT D'UN COMPOSANT LOGICIEL ENFICHABLE	101
FIGURE 4.46 CREATION D'UNE DEMANDE DE CERTIFICAT 1/3	102
FIGURE 4.47 CREATION D'UNE DEMANDE DE CERTIFICAT 2/3	102
FIGURE 4.48 CREATION D'UNE DEMANDE DE CERTIFICAT 3/3	103
FIGURE 4.49 CERTIFICAT CORRECTEMENT GENERE	103
FIGURE 4.50 CONFIGURATION DU HTTPS DANS POUR IIS	103
FIGURE 4.51 IMPORTATION DU BUNDLE DE CERTIFICAT DANS LE NAVIGATEUR	104
FIGURE 4.52 CONFIRMATION QUE L'AC EST DE CONFIANCE	104
FIGURE 4.53 IMPORTATION REUSSI DANS LA LISTE DES AC DE CONFIANCE.....	105
FIGURE 4.54 SITE WEB ACCESSIBLE ET SECURISE	105
FIGURE 4.55 AJOUT DU ROLE NPS	106
FIGURE 4.56 INSCRIPTION DU SERVEUR NPS DANS LE DOMAINE	107
FIGURE 4.57 AJOUT D'UN CLIENT AUTORISE A ACCEDER AU SERVEUR NPS.....	107
FIGURE 4.58 NOUVELLES STRATEGIE DE DEMANDE AU SERVEUR NPS	108
FIGURE 4.59 AJOUT D'UNE CONDITION DE DEMANDE AU SERVEUR NPS	108
FIGURE 4.60 NOUVELLES STRATEGIE D'ACCES AU RESEAU	109
FIGURE 4.61 NOUVELLES CONDITIONS D'ACCES AU RESEAU	109
FIGURE 4.62 ACCORD D'ACCES AU RESEAU AUX UTILISATEURS REMPLISSANT LES CONDITIONS.....	110
FIGURE 4.63 AJOUT D'UN TYPE DE PROTOCOLE D'ACCES AU RESEAU	110
FIGURE 4.64 SELECTION DU CERTIFICAT DU SERVEUR UTILISE POUR SON AUTHENTIFICATION	111
FIGURE 4.65 AJOUT D'UN NOUVEL UTILISATEUR AUTORISE A SE CONNECTER AU RESEAU	111
FIGURE 4.66 INFORMATION DE CONNEXION DU NOUVEL UTILISATEUR.....	112
FIGURE 4.67 CONFIGURATION DU POINT D'ACCES (POINT D'ACCES).....	113
FIGURE 4.68 MACHINE UTILISATEUR	113
FIGURE 4.69 CONNEXION DE L'UTILISATEUR AU DOMAINE.....	114
FIGURE 4.70 CONNEXION AU DOMAINE REUSSI.....	114
FIGURE 4.71 DEMANDE DE CERTIFICAT UTILISATEUR	115
FIGURE 4.72 CONFIGURATION D'UNE NOUVELLE CONNEXION SANS FIL.....	115
FIGURE 4.73 SELECTION DE LA METHODE D'AUTHENTIFICATION	116

FIGURE 4.74 CONNEXION REUSSIE AU RESEAU	116
FIGURE 4.75 ACCES ACCORDE A L'UTILISATEUR	117
FIGURE 4.76 CONSOLE DE CONFIGURATION DE MAILEENABLE	117
FIGURE 4.77 CONFIGURATION DE MAILEENABLE	118
FIGURE 4.78 AJOUT D'UNE NOUVELLE BOITE MAIL (UTILISATEUR)	118
FIGURE 4.79 CONNEXION A LA BOITE MAIL	119
FIGURE 4.80 ENVOIE D'EMAIL DE LA PART DU REDADIDI VERS UN KARIMSLJ	119
FIGURE 4.81 RECEPTION DE L'EMAIL DE REDADIDI PAR KARIMSLJ.....	120

Liste des tableaux

TABEAU 1 CARACTERISTIQUES D'UN CERTIFICAT NUMERIQUE.....	32
TABEAU 2 LINUX ET WINDOWS SERVER LES DIFFERENCES	125

Liste des annexes

ANNEXE 1 QU'EST-CE QUE WINDOWS SERVER ?.....	124
ANNEXE 2 QU'EST-CE QUE DEBIAN ?.....	124
ANNEXE 3 DIFFERENCE ENTRE LINUX ET WINDOWS SERVER	126
ANNEXE 4 FORMATS DE FICHIER DES CERTIFICATS.....	126

Liste des abréviations

A			
AC		CN	
Autorité de Certification		Canonical name	
ACL		CSR	
Access Contrôle Liste		Certificate Signing Request	
AD DS		D	
Active Directory Domaine Service		DER	
AE		<i>Distinguished Encoding Rules</i>	
Autorité d'Enregistrement		DNS	
AES		Domain Name System	
Résultats de recherche		E	
AIA		EAP-TLS	
Authority Information Access		Extensible Authentication Protocol -	
ASP		Transport Layer Security	
Active Server Pages		F	
C			
CA		FQDN	
Certification Authority		Fully Qualified Domain Name	

H

HTTPS
Hypertext Transfer Protocol Secured

I

ICP
Infrastructure à Clés Publiques
IGC
Infrastructure de Gestion de Clés
IMAP
Internet Message Access Protocol
IP
Internet Protocol

ISO
International Organization for
Standardization

M

MIME
Multipurpose Internet Mail Extensions
MSSQL
Microsoft Structured Query Language
MTA
Mail Transfer Agent
MX
Mail for Exchange

N

NAS
Network Access Server
NS
Name Server

O

OS
Operating System

P

PC
Personal Computer
PEM
Privacy Enhanced Mail

PKI
Public Key Infrastructure

R

RADIUS
Remote Authentication Dial-In User Service

RAID
Redundant Arrays of Inexpensive Disks
RSA
Rivest-Shanir-Aldman

S

SMTP
Simple Mail Transfer Protocol
SOA
Start of Authority
SSL
Secure Sockets Layers

T

TLS
Transport Layer Security
TV
TéléVision

U

URL
Uniform Resource Locator

V

VLAN
Virtual Local Area Network
VPN
Virtual Privat Network

W

WAP
Wi-Fi Protected Access

X

XSS
Cross Site Scripting

Introduction générale

Introduction générale

Avant d'aborder le domaine technique, il est préférable de prendre un peu de recul et de considérer la sécurité dans son ensemble, pas comme une suite de technologies ou de processus remplissant des besoins bien spécifiques, mais comme une activité à part entière pour laquelle s'appliquent quelques règles simples.

- Pour une entreprise ou une institution connectée à l'Internet, le problème n'est pas de savoir si elle va se faire attaquer mais quand cela va arriver. Une solution est donc de repousser le risque dans le temps et dans les moyens à mettre en œuvre en augmentant le niveau de sécurité permettant d'écarter les attaques quotidiennes, pas forcément anodines et non spécifiquement ciblées.
- Aucun système d'information n'est sûr à 100%.

Ces deux premières règles ne sont pas du tout les manifestations d'une paranoïa mais bien un simple constat qu'il est bon d'avoir toujours en tête pour ne pas se sentir – à tort – à l'abri de tout « danger ».

En sécurité informatique, on ne parle pas d'éliminer complètement les risques mais de les réduire au minimum par rapport aux besoins/contraintes d'affaires.

Il ne faut pas oublier non plus de considérer les actions provenant de l'intérieur de l'organisation, qui forment une partie (la majorité selon certaines données) non négligeable des sources d'attaques.

Un des aspects sécuritaires d'une importance capitale est le contrôle d'accès aux ressources quelle qu'elles soient, pour se faire le mot de passe se fait vieux et est remplacé par le certificat.

Qui dit certificat, dit PKI, un serveur qui va générer, donner, révoquer les certificats.

Mais le véritable défi du déploiement d'une PKI est bien d'ordre organisationnel :

- Définir les modalités de déploiement,
- Définir les règles d'enregistrement,
- Définir les responsabilités de chaque entité,
- Définir les droits d'utilisation pour chaque application,
- Définir les modes de distribution des certificats ...

Ce sont autant de questions à se poser lorsque l'on souhaite mettre en place une PKI.

Malgré ces points de difficultés, la PKI conserve des atouts majeurs aussi bien pour les utilisateurs et que pour l'entreprise.

Les utilisateurs n'ont plus à se soucier des mots de passes perdus.

L'entreprise s'offre un socle technique permettant le contrôle d'accès au réseau, aux logiciels, des accès visiteurs ...

Dans ce travail, on s'est donc proposé de faire une implémentation d'une PKI sous Linux et sous Windows, dans le but de contrôler l'accès à un réseau d'entreprise.

Donc un contrôle très demandé aussi bien par les entreprises, que par les particuliers qui utilisent le Wifi, pour éviter le piratage de leurs ressources.

L'accès à un serveur Web et mail est aussi déployé, via l'utilisation d'une PKI, garantissant ainsi un contrôle strict et moins d'attaques de type Dos, Spoofing, l'hameçonnage, le social ingeneering, etc.

Pour se faire, nous avons structuré notre travail en quatre chapitres, comme suit :

Le chapitre 1 s'attaque aux notions générales ayant trait à notre thème qu'est la sécurité informatique, le chapitre 2 mentionne les attaques informatiques les plus répandues, avec les solutions utilisées, les chapitre 3 et 4 détaillent l'implémentation sous Linux, puis sous Windows respectivement, d'une PKI ainsi que son utilisation de A à Z et enfin une conclusion générale clôturera le manuscrit.

Chapitre 1

Chapitre 1 : La sécurité informatique

I. Introduction

Dans ce chapitre, nous allons passer en revue quelques notions de base sur la sécurité informatique, en particulier les cinq règles de base dans toute politique de sécurité valable aussi bien pour les entreprises que pour les particuliers, règles primordiales pour éviter toutes sortes d'attaques, qu'on détaillera dans le chapitre 2.

II. La sécurité informatique : C'est quoi ?

Les systèmes d'information occupent de plus en plus une position stratégique au sein de l'entreprise. Ainsi la notion du risque liée à ces derniers, devient une source d'inquiétude et une donnée importante à prendre en compte, ceci en partant de la phase de conception d'un système d'information jusqu'à son implémentation et le suivi de son fonctionnement.

Les pratiques liées à la sécurité des systèmes d'information deviennent de plus en plus importantes dans l'écosystème informatique, qui devient ouvert et accessible à tous les utilisateurs, partenaires et prestataires de services de l'entreprise. L'entreprise doit comprendre les ressources du système d'information et définir le périmètre de protection sensible afin de garantir une exploitation maîtrisée et raisonnée de ces ressources.

De plus, les nouvelles tendances du nomadisme et du cloud computing permettent non seulement aux utilisateurs d'accéder aux ressources, mais peuvent également transmettre une partie du système d'information en dehors de l'infrastructure sécurisée de l'entreprise. Par conséquent, des procédures et des mesures doivent être développées pour évaluer les risques et définir les objectifs de sécurité à atteindre.

Ainsi, la sécurité informatique est un ensemble de moyens techniques, organisationnels, juridiques et personnels nécessaires pour maintenir, restaurer et assurer la sécurité des systèmes d'information.

Nous pouvons déduire de ces constats que la démarche de sécurité informatique est une activité de gestion des systèmes d'information et qu'il convient aussi d'établir un

tableau de bord de pilotage associé à une politique de sécurité comprenant les organes vitaux constituant une entreprise.

La **protection** des ordinateurs, les serveurs, les appareils mobiles, les systèmes électroniques, les réseaux et les données informatisées contre les éventuelles attaques malveillantes, doit être assurée par un **système de sécurité** appelée «**la cyber sécurité** » Elle est également appelée **sécurité informatique** ou **sécurité des systèmes informatiques**.

Nous pouvons considérer que la sécurité informatique est divisée en deux parties :

- La sécurité organisationnelle
- La sécurité technique

La sécurité organisationnelle concerne la politique de sécurité d'une société (code de bonne conduite, méthodes de classification et de qualification des risques, plan de secours, plan de continuité, ...).

Une fois la partie organisationnelle traitée, il faut mettre en œuvre toutes les recommandations, et plans dans le domaine technique de l'informatique, afin de sécuriser les réseaux et systèmes : cet aspect relève de la sécurité technique.

- Le périmètre de la sécurité est très vaste :
- La sécurité des systèmes d'information
- La sécurité des réseaux
- La sécurité physique des locaux
- La sécurité dans le développement d'applications
- La sécurité des communications
- La sécurité personnelle

Un risque se définit comme une combinaison de menaces exploitant une vulnérabilité et pouvant avoir un impact. De manière générale, les risques sont soit des causes (attaques, pannes, ...) soit des conséquences (fraude, intrusion, divulgation ...).

Les objectifs de base de la sécurité sont simples (liste non exhaustive) : empêcher l'utilisation non autorisée de ressources, empêcher la divulgation de données confidentielles et la modification non autorisée de données, la non répudiation (càd la preuve que les données ont bien été envoyées et/ou reçues), et enfin garder les ressources toujours disponibles.[1]

La sécurité informatique vise généralement huit principaux objectifs :



Figure 1.1 Les objectifs que vise la sécurité informatique[2]

Les plus importantes d'entre elles sont au nombre de cinq :

- L'intégrité, Vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).
 - La confidentialité, Elle consiste à rendre l'information inintelligible aux personnes autres que les seuls acteurs de la transaction.
 - La disponibilité, L'objectif de la disponibilité est de garantir l'accès à un service ou à des ressources en tout temps.
 - La non-répudiation, permettant de garantir qu'une transaction ne peut être niée.
 - L'authentification, consiste à assurer l'identité d'un utilisateur, c'est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu'il croit être. Un contrôle d'accès peut permettre (par exemple par le moyen d'un mot de passe qui devra être crypté) l'accès à des ressources uniquement aux personnes autorisées.
- Une seule entrave à l'un de ces principes remet toute la sécurité en cause.

III. La sécurité informatique : Pourquoi ?

Une politique de sécurité informatique mal gérée peut conduire à trois types d'impacts négatifs :

- La pénétration d'un réseau,
- Le vol ou détérioration d'informations,
- Les perturbations.

La pénétration d'un réseau ou système peut se faire soit par vol d'identité soit par intrusion. Ce vol d'identité peut se faire par vol du « nom d'utilisateur/mot de passe » de connexion au système d'information. Tous les moyens sont bons pour obtenir des informations. Nous pouvons citer à titre d'exemples :

- L'écoute des réseaux,
- L'ingénierie sociale,
- Ou tout simplement le fait de regarder par-dessus l'épaule de l'utilisateur qui s'authentifie.

La pénétration d'un réseau ou système peut aussi se faire à distance : par exemple un hacker peut pénétrer le réseau via un serveur de messagerie. Mais il existe d'autres méthodes moins visibles, comme l'installation d'un logiciel à l'insu de l'utilisateur, suite à la lecture d'une page web sur un site. Ainsi un script contenu dans la page web chargée, peut envoyer des messages de votre logiciel de messagerie vers d'autres personnes.[3]

IV. La sécurité informatique : Comment ?

Des produits existent sur le marché tel que les antivirus, les Firewall en passant par les VPN permettent d'éviter ces problèmes. Néanmoins toutes ces solutions ne sont pas fiables à 100% :

Chacune de ces technologies ou produits dispose d'une couverture spécifique. Par exemple, l'antivirus va permettre de bloquer les virus ou Chevaux de Troie entrants par la messagerie ou par échange de fichiers.

Le très connu Firewall, dont la configuration n'est ni simple, ni rapide va permettre de filtrer les échanges entre deux réseaux afin de limiter les accès, et de détecter les éventuelles tentatives d'intrusion.

Une fonctionnalité supplémentaire a tendance à se retrouver intégrée dans les Firewalls : le VPN. Celui-ci permet de garantir la confidentialité des échanges d'informations passant par son intermédiaire en chiffrant le flux d'informations.

En outre il est possible de mettre en œuvre une signature numérique en place. Ainsi, dans le système de messagerie, le destinataire du message sera certain de l'identité de l'émetteur et de l'intégrité du message. Il pourra être le seul lecteur si le message a été chiffré (clé privée / clé publique). [1]

Le serveur Web reste vulnérable, car accessible directement depuis l'extérieur du réseau. La mise en place d'un reverse proxy résout l'affaire. En effet, toute tentative de connexion au serveur Web parvient au serveur proxy, qui lui-même envoie une requête au serveur Web. Ainsi le serveur Web n'est plus accessible depuis l'extérieur du réseau.

La sécurité d'un système informatique fait souvent l'objet de métaphores. En effet, on la compare régulièrement à une chaîne en expliquant que le niveau de sécurité d'un système est caractérisé par le niveau de sécurité du maillon le plus faible.

Ainsi, une porte blindée est inutile dans un bâtiment si les fenêtres sont ouvertes sur la rue.

Cela signifie que la sécurité doit être abordée dans un contexte global et notamment prendre en compte les aspects suivants :

- La sensibilisation des utilisateurs aux problèmes de sécurité.
- La sécurité logique, c'est-à-dire la sécurité au niveau des données, notamment les données de l'entreprise, les applications ou encore les systèmes d'exploitation.
- La sécurité des télécommunications : technologies réseau, serveurs de l'entreprise, réseaux d'accès, etc.
- La sécurité physique, soit *la sécurité au niveau des infrastructures matérielles* : salles sécurisées, lieux ouverts au public, espaces communs de l'entreprise, postes de travail des personnels, etc. [4]

Plusieurs techniques de préventions sont préconisées dont :

1. Faire les mises à jour

Le premier réflexe, et le plus évident, est de **mettre à jour le système d'exploitation, les logiciels et la solution antivirus** de tous les postes. Cette « réactualisation » permet la correction de failles critiques, l'amélioration de la protection et une diminution de la surface d'attaque. Les mises à jour participent donc à une augmentation de la fiabilité du système d'information. Les professionnels de l'information considèrent les mises à jour logicielles aussi importantes que les mises à jour de la solution anti-virus.

Ces MAJ préviennent surtout l'indisponibilité des ressources et certaines attaques d'intrusion. [4]

2. Protéger son réseau

Le **réseau est un des vecteurs d'attaques** des plus utilisé par les hackers. Il est donc nécessaire de le protéger afin de réduire les risques de contamination et de propagation. Pour se faire, il est recommandé d'utiliser un ou plusieurs pare-feu (avec des règles adaptées) et des technologies réseaux comme les **VLAN** ou encore le **802.1X**. Une authentification forte et efficace des utilisateurs voulant accéder au réseau, est primordiale, via les mots de passe et certificats.

De plus, il est important de protéger l'accès physique aux équipements réseaux et serveurs (accès protégés par clé ou par badges, ...). En effet, un hacker aura beaucoup plus de facilité à effectuer son attaque grâce à un accès physique au matériel en question. Ceci permet le contrôle d'accès.

3. Complexifier les mots de passe

La notion de sécurité nécessite également quelques actions de la part de l'entreprise et des utilisateurs. La première est le **renouvellement régulier des mots de passe**, différents selon les comptes, et la **complexification** de celui-ci afin d'éviter la compromission.

Pour créer un mot de passe correct, relativement difficile à «brute-forcer», il est recommandé qu'il soit composé d'au moins 8 caractères avec des minuscules, majuscules, chiffres et caractères spéciaux.

On référence deux méthodes pour générer des **mots de passe sécurisés** :

La méthode phonétique : «J'ai acheté 5Cds pour cent euros cet après-midi» :
ght5Cds%E7am

La méthode des premières lettres : « Allons enfants de la partie, le jour de gloire est arrivé » : aE2IP,IJ2Géa!» [4]

4. Sauvegarder régulièrement

L'année passée, une nouvelle attaque informatique nommée «**Ransomware**». Elle consiste en l'intrusion d'un logiciel malveillant, qui chiffrera l'ensemble des données d'un ordinateur, obligeant l'utilisateur à payer une rançon pour récupérer ses données.

Cette attaque est d'autant plus vicieuse pour une entreprise du fait de la nature des données stockées. La meilleure façon de se prémunir de cette attaque est d'effectuer

des **sauvegardes régulières** afin de toujours avoir une copie des données « propre » à disposition.

5. L'utilisateur, pilier de la sécurité

Le Discours récurrent en entreprise, est que la sécurité dépend principalement des **utilisateurs**. Pour les sensibiliser et les éduquer aux bonnes pratiques numériques, il est impératif qu'ils participent à des **formations**.

5.1 Faire de la prévention auprès des utilisateurs

Car c'est bien souvent du fait de mauvaises pratiques que des malwares s'implantent dans les postes. Prenons encore une fois l'exemple du Ransomware, le malware est souvent installé lorsqu'un utilisateur ouvre une pièce jointe ou un lien malveillant.

Cette action est souvent le fruit d'un manque de prévention et de formation auprès des utilisateurs.

5.2 Charte informatique et formations régulières

C'est pourquoi dès l'entrée dans l'entreprise, il est important que les nouveaux utilisateurs prennent connaissance de la **charte informatique**. A défaut d'avoir accès à une formation dès les premiers pas dans la structure, elle permet de fixer un cadre clair des conditions d'utilisation. Une prévention nécessaire pour garder l'écosystème de sécurité en place. Il reste néanmoins primordial de proposer des **formations régulières aux utilisateurs** pour les initier aux bonnes pratiques de la sécurité et les nouvelles menaces.

Ainsi, deux chantiers sont à privilégier pour préserver la **disponibilité, l'intégrité et la confidentialité des données** en entreprise : la protection des infrastructures mais également, l'éducation numérique des salariés.

Voici une infographie regroupant les **8 conseils à respecter pour une bonne sécurité informatique** dans chaque entreprise :

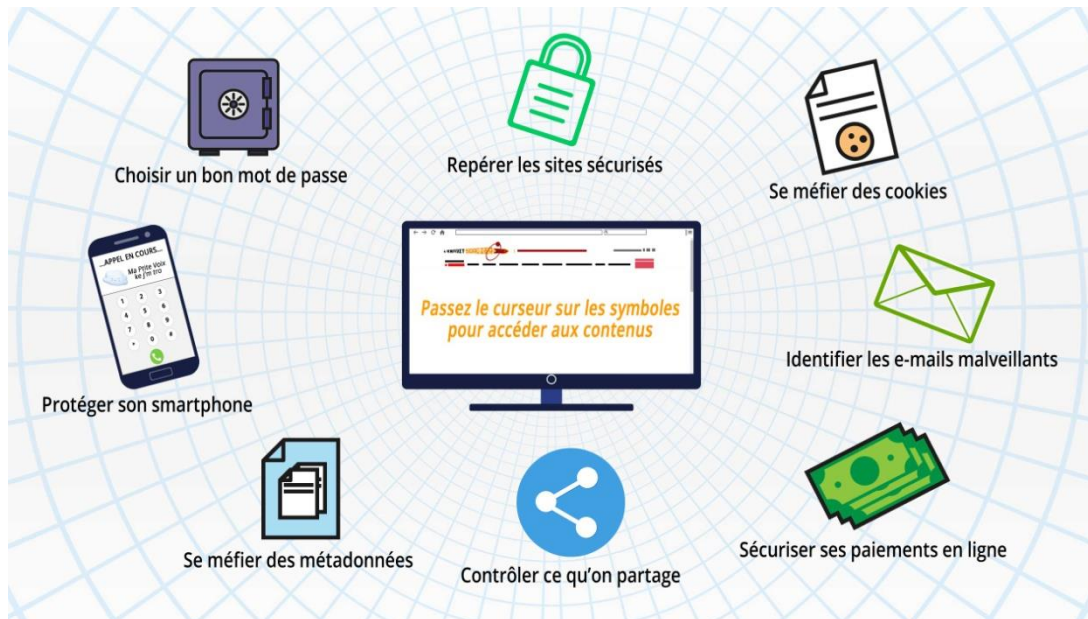


Figure 1.2 Les Gestes à adopter [5]

6. Défaillance matérielle

Tout équipement physique est sujet à défaillance (usure, vieillissement, défaut...). L'achat d'équipements de qualité et standard accompagnés d'une bonne garantie avec support technique est essentiel pour minimiser les délais de remise en fonction. Seule une forme de sauvegarde peut cependant protéger les données.

7. Défaillance logicielle

Tout programme informatique contient des bugs ou des failles. La seule façon de se protéger efficacement contre ceux-ci est de faire des copies de l'information à risque. Une mise à jour régulière des logiciels et la visite des sites consacrés à ce type de problèmes peuvent contribuer à en diminuer la fréquence.

8. Accidents (pannes, incendies, inondations...)

Une sauvegarde est indispensable pour protéger efficacement les données contre ces problèmes. Cette procédure de sauvegarde peut combiner plusieurs moyens fonctionnant à des échelles de temps différentes :

- Disques RAID pour maintenir la disponibilité des serveurs
- Copie de sécurité via le réseau (quotidienne)

- Copie de sécurité dans un autre bâtiment (hebdomadaire)
- La disposition et infrastructure des locaux peut aussi fournir une protection intéressante. pour des sites particulièrement importants (site informatique central d'une banque ...) il sera nécessaire de prévoir la possibilité de basculer totalement et rapidement vers un site de secours (éventuellement assuré par un sous-traitant spécialisé). Ce site devra donc contenir une copie de tous les logiciels et matériels spécifiques à l'activité de la société. [4]

9. Le Chiffrement

C'est une technique qui permet de préserver la confidentialité, il y a du chiffrement par clé privée et celle par clé publique (qui est plus forte et permet la signature numérique garantissant l'identité des antagonistes). Cette technique protège du vol de données, et de l'indiscrétion des gens. Ce domaine a vu apparaître des solutions très efficaces, très nombreuses, en perpétuel changement, et très fortes. La signature numérique a apporté la garantie de l'intégrité et la non répudiation.[6]

La gestion de ces clés à grande échelle et à distance, est compliquée, d'où les PKI.

V. Conclusion

La sécurité des systèmes d'information représente aujourd'hui une tâche essentielle, à prendre en compte par toute entreprise qui désire disposer d'un ensemble d'outils et de méthodes qui lui permettent et assurent la gouvernance de son système d'information. Ainsi plusieurs méthodes d'analyse des systèmes informatiques proposent des démarches de certification afin de garantir une image pérenne aux entreprises.

Bien évidemment la sécurité à 100% reste un idéal à atteindre, surtout devant le large éventail des menaces qui mettent en danger l'exploitation d'un système d'information. Ainsi il est important de bien formaliser une politique de sécurité en prenant en compte les risques réels qu'encourt un système informatique et en évaluant les coûts que peuvent engendrer les problèmes résultants de ces risques par rapport au coût nécessaire à la mise en place des solutions palliative à ces problèmes.

Chapitre 2

Chapitre 2 : Attaque informatique et présentation de la PKI

I. Introduction

Dans ce chapitre, nous allons passer en revue quelques mécanismes d'attaque très utilisées et/ou nouvelle génération, comment s'en défendre et/ou comment les prévenir. Puis nous détaillerons la PKI, qui est la notion de base de notre TRAVAIL, qu'est-elle et comment tout cela fonctionne t'il.

Ceci nous permettra de bien comprendre les étapes de notre implémentation, les protocoles qui vont intervenir, et les liens entre tous les serveurs que nous allons déployer, pour rendre efficace notre déploiement de la PKI.

II. Tour d'horizon des types d'attaques informatiques

Dans un contexte où le progrès technologique avance à une vitesse effrénée et dans lequel les attaques informatiques sont de plus en plus fréquentes, la cyber-sécurité occupe une place de plus en plus importante. Nous sommes tous vulnérables : États, grands groupes, petites et moyennes entreprises, organismes, particuliers...

Bien se protéger sur le web est devenu une véritable préoccupation pour préserver ses actifs informatiques, qu'ils soient matériels ou immatériels. Une multitude d'attaques peuvent être menées par des pirates informatiques pour infecter notre système. Un tour d'horizon non exhaustif est listé ci-dessous :[4]

1. Le cryptojacking, minage de crypto monnaie malveillant

L'arrivée des crypto monnaies et l'engouement autour du Bitcoin ont engendré de nouvelles menaces comme le cryptojacking, également appelé minage de crypto monnaie malveillant. Les hackers introduisent des logiciels pour corrompre les systèmes et ressources d'une machine (PC, smartphone, serveur...), afin d'exploiter la crypto monnaie en arrière-plan et engendrer du profit de façon cachée.[4]

2. Les Ransomware, rançongiciels

D'autres hackers vont plus loin, avec des Ransomware. C'est un type d'attaque de plus en plus fréquent : une personne pirate un ordinateur ou un serveur, le chiffre et demande une rançon, en bitcoin, à l'utilisateur ou l'administrateur. Pendant ce temps, les données sont bloquées : le hacker vous contraint de payer pour récupérer vos données. [4]

3. Les intrusions sur les objets connectés

De plus en plus de personnes se procurent des objets connectés : montres, assistants vocaux, dispositifs d'éclairage ou de sécurité... Il y en a une multitude pour des usages de plus en plus répandus dans la vie quotidienne, et ce à domicile comme dans les entreprises. Mais quel est leur degré de vulnérabilité et quels sont les risques encourus par les possesseurs de ces objets ? Les sociétés qui commercialisent ces solutions doivent redoubler d'efforts pour mettre en place des pare-feu et implémenter des programmes de mises à jour récurrentes lors de leur conception, afin de les protéger d'éventuelles attaques et empêcher que des failles soient exploitées par des personnes mal intentionnées. [4]

4. Les attaques géopolitiques

Certains pays sont connus pour leurs attaques informatiques, menées par des organismes gouvernementaux ou des activistes locaux. Ces hacks peuvent être réalisés contre un autre pays pour le déstabiliser, l'intimider, mais également voler certaines technologies dans le cadre de l'espionnage industriel. Dans ce cas précis il est important pour les entreprises technologiques de prendre des précautions, notamment dans la mise en place de normes de sécurité, le choix du lieu où elles hébergent leurs données et leurs prestataires.[7]

5. Les scripts intersites ou cross-site Scripting (XSS)

Les hackers qui ont recours à cette pratique lancent des attaques XSS en injectant du contenu dans une page, ce qui corrompt le navigateur de la cible. Un pirate peut ainsi modifier la page web selon ses envies, voler des informations sur des cookies,

lui permettant de détourner des sites à volonté afin de récupérer des données sensibles, ou d'injecter un code malveillant qui sera par la suite exécuté. [7]

6. Les malwares sur mobile

Nous passons désormais plus de temps sur mobile que devant la TV, les hackers l'ont bien compris et n'ont pas tardé à exploiter cette opportunité. En 2018, 116,5 millions d'attaques sur mobile se sont produites selon Kaspersky, soit quasiment 2 fois plus qu'en 2017 (66,4 millions). De nombreuses solutions de gestion des appareils mobiles sont disponibles sur le marché, et peuvent être utilisées par les entreprises pour protéger leurs salariés et les données stratégiques.

7. Le phishing ou l'hameçonnage

La fameuse fenêtre pop-up qui s'affiche et vous propose de cliquer pour récupérer le million d'euros que vous avez gagné par tirage au sort. Dès que l'on clique sur un lien de ce type, on expose ses données personnelles. Les pirates peuvent voler des numéros de carte de crédit ou des informations financières, ainsi que des identifiants de connexion ou des données confidentielles en reproduisant des interfaces de saisie. [7]

8. Le spoofing

Vous avez reçu un email d'un proche (voir un email de vous-même) un peu bizarre ? Vous êtes sûrement victime de spoofing. Il s'agit d'une méthode consistant à usurper l'adresse email d'envoi. Ce type d'attaque est très fréquent (et parfois crédible). Généralement, le pirate tente de vous faire croire des choses qui sont en réalité totalement fausses : il détient des informations sur vous, un proche a besoin de vous etc. [7]

9. Les attaques cyber-physiques

Le piratage de systèmes de transport, d'usines, de réseaux électriques ou d'installations de traitement de l'eau, arrive réellement, pour neutraliser un site spécifique ou réaliser tout autre projet hostile via la propagation d'un virus

informatique. La protection de systèmes sensibles repose sur un ensemble de pratiques dont la segmentation du réseau par exemple. [7]

10. Les attaques contre les appareils et dossiers médicaux électroniques

Le milieu médical est lui aussi friand des nouvelles technologies et des nouveaux appareils mis à sa disposition. De nombreuses données sensibles et confidentielles sont hébergées, ce qui là encore augmente l'intérêt des pirates et par conséquent la vulnérabilité du secteur aux cyberattaques. Quand les hackers s'introduisent dans les systèmes d'hôpitaux et arrivent à voir accès à ces informations, le préjudice en termes de vie privée est considérable. Les conséquences que pourraient avoir une intrusion et le piratage d'appareils médicaux seraient quant à elles dramatiques.[8]

11. Les attaques contre les véhicules connectés et semi-autonomes

Des véhicules possèdent des capteurs qui font appel à des programmes informatiques. Certaines fonctionnalités peuvent même être contrôlées via un smartphone, ce qui les rend d'autant plus vulnérables aux attaques orchestrées par des pirates. En plus d'accéder là encore à des données sensibles, les hackers pourraient accéder aux systèmes du véhicule et causer des pannes, voire des accidents. [8]

12. Les attaques contre les espaces de stockage cloud :

Beaucoup de particuliers et d'entreprises ont abandonné le stockage traditionnel au profit du cloud computing, accessible partout. Les pirates informatiques peuvent cependant utiliser des mécanismes pour voler des clés de chiffrement et ainsi accéder à des informations sensibles et autres données confidentielles. Pour contrer ce fléau, il est conseillé d'investir dans un système de chiffrement sécurisé et un certificat SSL, fournis par un prestataire de confiance afin de protéger les données de votre société. [8]

III. La cryptographie à clé publique

A l'heure actuelle, la sécurité des données informatiques est au centre des préoccupations de tout utilisateur. Pour se protéger des vols de données, il est important de les chiffrer afin que seuls ceux qui sont autorisés à les manipuler puissent y avoir accès. La méthode de cryptographie la plus répandue est sans doute la cryptographie à clé publique. Et l'ensemble des solutions techniques permettant de manipuler ces clés à un niveau mondial (un nombre très élevé de paires de clés) est appelé infrastructure à clé publique ou PKI (Public Key Infrastructure). [4]

La PKI a pour rôle de délivrer les certificats numériques (qui sont les clés publiques et privées à acheminer aux différents antagonistes intervenant dans une communication à distance comme dans Internet). Ces derniers permettent d'entreprendre des opérations cryptographiques telles que le chiffrement et la signature numérique. Ces opérations servent à garantir la confidentialité, l'authentification, l'intégrité et la non-répudiation lors des transactions électroniques. Une application de processus de vérification d'identité sévère et une mise en œuvre de solutions cryptographiques fiables sont les conditions sinéquanones à la production et à la gestion des certificats électroniques. C'est pourquoi, la PKI ou aussi infrastructure de gestion de clé est généralement composée d'une autorité de certification, d'une autorité d'enregistrement, d'une autorité de dépôt.

L'autorité de certification (ou AC) est le composant décisionnel et de confiance dans le processus de certification. Elle cautionne l'application de la politique de certification de l'organisme. Elle signe les demandes de certificat et les listes de révocation. L'apposition de sa signature, électronique évidemment, garantit l'association de l'identité du demandeur à la clé publique. Cette autorité a pour rôle principal de gérer le cycle de vie des certificats. Ainsi, mis à part l'émission de certificat électronique, elle détermine la durée de vie de celui-ci et sa destitution.

Quant à l'autorité d'enregistrement (ou AE), elle constitue l'interface entre l'utilisateur et l'autorité de certification. Elle est chargée d'identifier de façon certaine les demandeurs ou les porteurs de certificat et de s'assurer que les contraintes liées à l'usage d'un certificat soient remplies. En outre, les requêtes des utilisateurs sont traitées par l'autorité d'enregistrement conformément à la politique de certification c'est-à-dire à un ensemble de règles à respecter lors de la mise en place de

prestations adaptées à certains types d'applications. Cet ensemble de règles est identifié par un identificateur alphanumérique unique selon la norme d'enregistrement ISO. L'AE a aussi pour rôle de récupérer la clé publique du demandeur.[9]

En ce qui concerne l'autorité de dépôt, elle a pour tâche de stocker les certificats numériques. Elle centralise et organise l'archivage des certificats. Par ailleurs, elle gère aussi la liste des certificats expirés ou révoqués et met à disposition, à l'ensemble des utilisateurs, les certificats des clés publiques émis par l'autorité de certification.

L'autorité de séquestre est un autre composant de la PKI. Bien qu'elle soit moins connue, elle joue un grand rôle à savoir le stockage sécurisé des clés de chiffrement créées par les autorités d'enregistrement afin de les restaurer éventuellement.

La cryptographie à clé publique est une clé de chiffrement qui est accessible à tous les membres d'une organisation. Elle permet d'un côté de transmettre des messages en toute confidentialité à son unique propriétaire et de l'autre côté d'authentifier les messages qui ont été émis par le propriétaire. Ainsi, la PKI offre à ses utilisateurs un niveau de service élevé dans la protection de la vie privée mais aussi le contrôle d'accès à l'information, l'intégrité, l'authentification et la non-répudiation lors des transactions électroniques.

La confidentialité garantit le fait que le destinataire légitime soit le seul à avoir accès aux données.

L'authentification garantit le fait que le destinataire d'un message et son expéditeur soient ceux qui ont vraiment accès aux données et qu'ils aient une identité électronique authentifiée.

L'intégrité garantit la non-altération accidentelle ou intentionnelle du message.

La non-répudiation garantit le fait qu'on ne puisse en aucun cas renier l'auteur d'un message.

L'exemple le plus tangible sur le fonctionnement d'une infrastructure de gestion de clés est la signature électronique. Les certificats numériques de la signature assurent le fait que la clé privée ne soit détenue que par un unique titulaire (personne physique ou serveur).

IV. Certificat numérique

Un certificat numérique est une sorte de passeport électronique qui permet à une personne, un ordinateur ou une organisation d'échanger de manière sûre des informations sur Internet en s'appuyant sur une infrastructure à clé publique (PKI).

A l'instar d'un passeport, un certificat numérique fournit des informations d'identité, se veut résistant aux tentatives de réalisation de faux, et peut être vérifié parce qu'il est émis par une agence officielle, de confiance. Le certificat contient le nom de son porteur, un numéro de série, des dates de validité, une copie de clé publique de son porteur – utilisée pour chiffrer des messages et produire des signatures électroniques – et la signature électronique de l'autorité qui l'a émis (CA) afin de permettre au destinataire d'en vérifier l'authenticité.[4]

Pour prouver son authenticité et sa validité, un certificat est signé numériquement par un certificat racine appartenant à une autorité de certification de confiance. Les systèmes d'exploitation et les navigateurs Web tiennent à jour des listes de certificats racines afin de pouvoir vérifier aisément les certificats émis et signés par les autorités de certification.

La PKI est un système de gestion de clef publique permettant d'en assurer la fiabilité. La PKI pose des problèmes organisationnels mais pas techniques et a plus d'avantage que de contrainte.

Mais les quelques désavantages de cette technique sont rapidement éclipsée par leur forte sécurité, mais alors quesqu'un certificat à clé publique :

Un certificat à clé publique est un certificat numérique qui lie l'identité d'un système à une clé publique, et éventuellement à d'autres informations.

C'est une structure de donnée signée numériquement qui atteste de l'identité du possesseur de la clé privée correspondante à une clé publique.[6]

Un certificat apparaît sous la forme suivante :

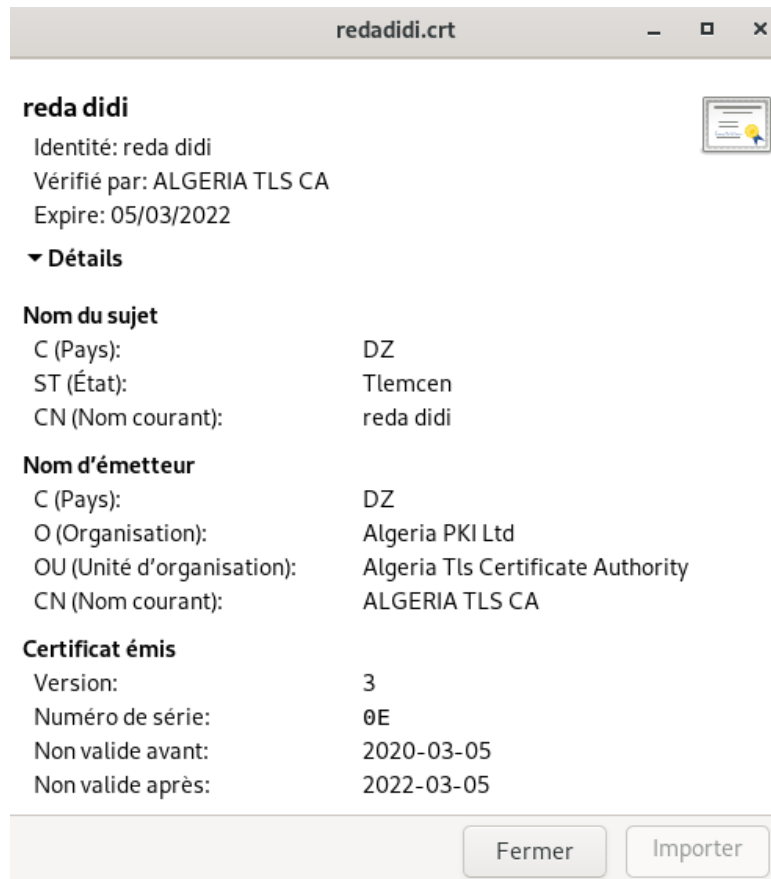


Figure 2.1 Certificat numérique

Version	Ce champ identifie à quelle version de X.509 correspond ce certificat.
Serial number	Numéro de série du certificat (propre à chaque AC).
Signature Algorithm ID	Désigne l'algorithme utilisé par l'AC pour signer le certificat, ainsi que tous les paramètres de l'algorithme.
Issuer Name	Permet d'identifier l'AC qui a délivré le certificat. Il existe un formalisme bien défini pour attribuer un nom à chaque entité sans ambiguïté.
Validity period	C'est une paire de date durant laquelle le certificat est valide.
Subject Name	Identifie le détenteur de la clé publique.

Subject public key info	Le nom de l'algorithme à clé publique (ex RSA), ainsi que tous les paramètres concernant cette clé, et la clé proprement dite.
Issuer Unique ID/Subject Unique Id	Extensions optionnelles introduites avec la version 2 de X.509.
Extensions	Extensions génériques optionnelles, introduites avec la version 3 de X.509, Il permet aux autorités de certification de rajouter leurs propres informations aux certificats qu'elles délivrent.
Signature	Signatures numériques de l'AC sur l'ensemble des champs

Tableau 1 Caractéristiques d'un certificat numérique[10]

V. Infrastructure à clé publique PKI

Une infrastructure à clés publiques (ICP) ou infrastructure de gestion de clés (IGC) ou encore *Public Key Infrastructure* (PKI), est un ensemble de composants physiques, de procédures humaines (vérifications, validation) et de logiciels (système et application) destiné à gérer les clés publiques des utilisateurs d'un système. Une infrastructure de gestion de clés permet de lier des clés publiques à des identités (comme des noms d'utilisateurs ou d'organisations). Une infrastructure de gestion de clés fournit des garanties permettant de faire à **priori** confiance à une clé publique obtenue par son biais.[11]

VI. Le Concept PKI

Au fond, une PKI X.509 standardisé est une architecture de sécurité qui utilise des mécanismes cryptographiques bien établis pour prendre en charge des cas d'utilisation tels que la protection des e-mails et l'authentification des serveurs Web. À cet égard, il est similaire à d'autres systèmes basés sur la cryptographie à clé publique. Dans le domaine de X.509 cependant, et grâce à ses racines dans un schéma mondial conçu par l'industrie des télécommunications, ces mécanismes

s'accompagnent d'une quantité considérable de frais administratifs. Une chose à garder à l'esprit est que X.509 n'est pas une application, mais une spécification sur laquelle sont basées des applications telles que les extensions de messagerie Internet polyvalentes sécurisées (S / MIME) et Transport Layer Security (TLS). Les éléments constitutifs sont très génériques et tirent l'essentiel de leur sens des relations qui existent entre eux. C'est ce qu'on appelle une infrastructure.[9]

VII. Principe de fonctionnement de la PKI

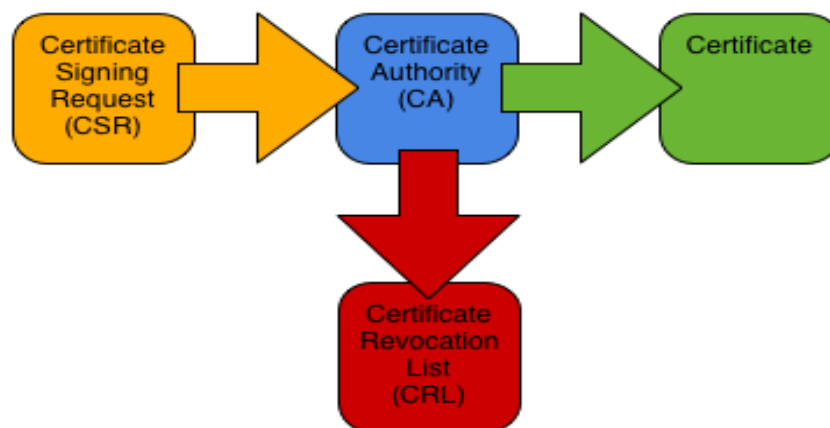


Figure 2.2 Concept d'une PKI[12]

Un demandeur génère un fichier .CSR (demande de certification) et le soumet à l'AC. L'autorité de certification émet un certificat basé sur le CSR et le renvoie au demandeur.

Si le certificat est révoqué à un moment donné, l'autorité de certification l'ajoute à sa liste de révocation de certificats.

1. Types de CA

CA Racine :

CA à la racine d'une hiérarchie PKI. Émet uniquement des certificats CA.

CA intermédiaire :

Autorité de certification inférieure à l'autorité de certification racine mais n'est pas à une autorité de certification signataire. Émet uniquement des certificats CA.

CA Signataire :

CA au bas d'une hiérarchie PKI. Délivre uniquement des certificats utilisateur.

2. Types de certificats

Certificat CA :

Certificat d'une CA. Utilisé pour signer les certificats et les listes de révocation de certificats.

Certificat racine :

Certificat CA auto-signé à la racine d'une hiérarchie PKI. Sert d'ancrage de confiance à la PKI.

Certificat croisé :

Certificat CA émis par une autorité de certification externe à la hiérarchie PKI principale. Utilisé pour connecter deux PKI et se présente donc généralement par paires.

Certificat utilisateur :

Certificat d'utilisateur final émis à une ou plusieurs fins : protection des e-mails, authentification du serveur, authentification du client, signature de code, etc. Un certificat d'utilisateur ne peut pas signer d'autres certificats.

VIII. Conclusion

Toutes ces attaques très dangereuses, pouvant induire des dégâts irrémediables, surviennent à coup sûr, si vous ne prévoyez aucun moyen de vous en préserver ou du moins de diminuer les conséquences. Une des techniques de prévention, est le chiffrement via l'utilisation de clés publiques, et donc il faut déployer une PKI, pour assurer l'authenticité des clés publiques.

La certification électronique via des clés publiques et les données associées à des individus et des systèmes est une technique devenue de plus en plus performante, indispensable en informatique, notamment du fait de l'expansion d'Internet et de la dématérialisation des documents. Tout serveur informatique, désirant communiquer de façon sécurisée avec des utilisateurs, utilise aujourd'hui le protocole SSL/TLS qui exige de posséder un certificat électronique.

Ils ne sont rien d'autre qu'une facette d'une toile de plus en plus complexe et mondiale et même s'ils s'avèrent très utiles en tant que technologie de vérification d'identité, ils ne sont nullement sûrs à 100%. Ils comportent depuis longtemps des problèmes immanents.

Chapitre 3

Chapitre 3 : Implémentations d'une infrastructure PKI sous Linux

I. Introduction

Dans ce chapitre, nous détaillons toutes les étapes de notre implémentation de la PKI sous Linux, ce qui pourra être utilisé comme un guide pour les éventuels étudiants intéressés par un tel sujet. Cela peut servir de base pour aller plus loin dans le domaine de la sécurité informatique, qui est un des aspects essentiels dans les réseaux et l'administration des réseaux.

II. Implémentation d'une infrastructure à clé publique PKI

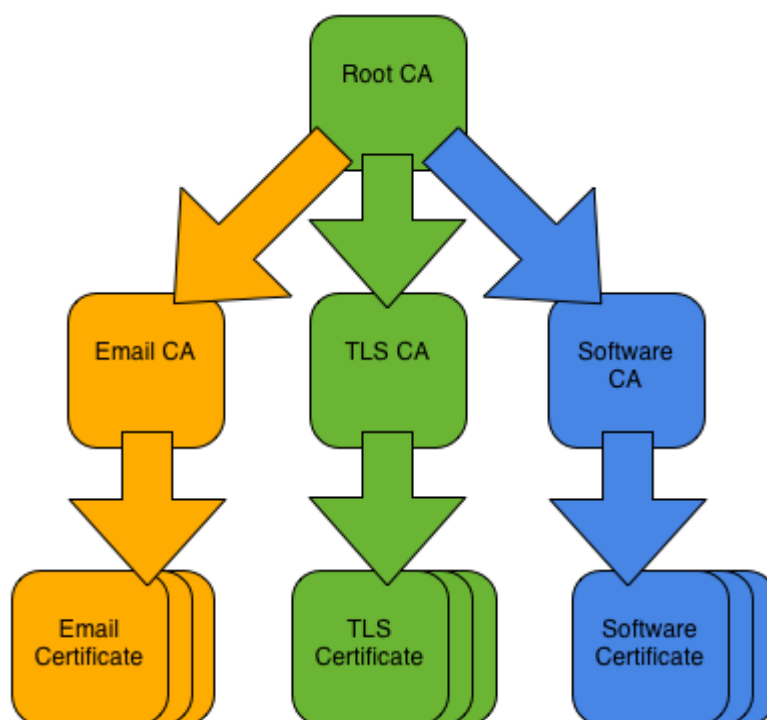


Figure 3.1 Schéma de notre PKI[12]

Pour l'implémentation d'une PKI dépend des besoins de l'organisme demandeur, nous créons d'abord la CA racine ALGERIA ROOT CA et son certificat CA.

Nous utilisons ensuite l'autorité de certification racine pour créer les trois autorités de certification signataires : l'autorité de certification ALGERIA EMAIL CA, l'autorité de certification ALGERIA TLS CA et l'autorité de certification ALGERIA SOFT CA.

Les autorités de certification en place, sont montrées en fonctionnement, en train d'émettre des certificats utilisateur, à des fins de protection par courrier électronique, d'authentification TLS et de signature de logiciel, respectivement.

La suite sera une succession de commandes à utiliser dans un terminal linux ayant au préalable Openssl installé, si ce n'est pas le cas alors la commande suivante sera nécessaire :

```
apt install openssl
```

Fichiers de configuration :

Nous utilisons un fichier de configuration par CA :

Fichier de configuration de l'autorité de certification racine

Fichier de configuration de l'autorité de certification d'email

Fichier de configuration de l'autorité de certification TLS

Fichier de configuration de l'autorité de certification logicielle

Et un fichier de configuration par type CSR :

Fichier de configuration de la demande de certificat de messagerie

Fichier de configuration de la demande de certificat du serveur TLS

Fichier de configuration de la demande de certificat client TLS

Fichier de configuration de la demande de certificat de signature de code

1. Créations d'une autorité de certification racine

1.1 Créations des répertoires

```
mkdir -p /ca/root-ca/private /ca/root-ca/db /ca/crllist /ca/root-ca/certs /ca/root-ca/certsreq /ca/root-ca/newcerts/  
chmod 700 ca/root-ca/private
```

Le répertoire « **ca** » contient tous les dossiers et ressources de la PKI, le répertoire « **crllist** » contient des listes de révocation de certificats et le répertoire « **certs** » contient le certificat de la CA racine et enfin « **certsreq** » contient toute les

demandes de certificats. La disposition du répertoire reste la même pour les autres CA (email, tls, soft).

1.2 Créations d'une base de données

```
touch /ca/root-ca/db/root-ca.db
touch /ca/root-ca/db/root-ca.db.attr
echo 01 > /ca/root-ca/db/root-ca.crt.srl
echo 01 > /ca/root-ca/db/root-ca.crl.srl
```

Les fichiers de base de données doivent exister avant que les commandes openssl puissent être utilisées, l'initialisation est une étape importante.

La même opération doit être faite pour les autres CA (email, tls, soft).

1.3 Créations d'une demande d'AC

```
openssl req -new
-config /ca/root-ca/root-ca.cnf
-out /ca/root-ca/certsreq/root-ca.csr
-keyout /ca/root-ca/private/root-ca.key
```

Avec la commande `openssl req -new`, nous générons une paire de clé (privée et publique) et un CSR (certificat request) pour l'autorité de certification racine. La configuration est extraite de la section [req] du fichier de configuration de l'autorité de certification racine.

1.4 Créations d'un certificat AC

```
openssl ca -selfsign \
  -config /ca/root-ca/root-ca.cnf \
  -in /ca/root-ca/certsreq/root-ca.csr \
  -out /ca/root-ca/certs/root-ca.crt \
  -extensions root_ca_ext \
  -enddate 20301231235959Z
```

NOTE: (-enddate YYMMDDHHMMSSZ) signifie year/ month /day /hour/ minute/ second).

Avec la commande openssl « **ca** », nous créons un certificat de CA racine auto-signé à partir du CSR. La configuration provient de la section [ca] du fichier de configuration de l'autorité de certification racine. Notez que nous spécifions une date de fin en fonction de la longueur de clé.

1.5 Créations d'une liste CRL initiale

```
openssl ca -gencrl \  
  -config /ca/root-ca/root-ca.cnf \  
  -out /ca/crllist/root-ca.crl
```

Avec la commande openssl « **ca -gencrl** », nous générons une liste CRL initiale (vide).

La même opération doit être faite pour les autres CA (email, tls, soft).

Mise à part lors de la signature du certificat qui se fait par la CA racine.

```
openssl ca \  
  -config /ca/root-ca/root-ca.cnf \  
  -in /ca/tls-ca/certsreq/tls-ca.csr \  
  -out /ca/tls-ca/certs/tls-ca.crt \  
  -extensions signing_ca_ext \  
  -enddate 20251231235959Z
```

Nous créons un certificat de CA intermédiaire signé par la CA racine à partir du CSR.

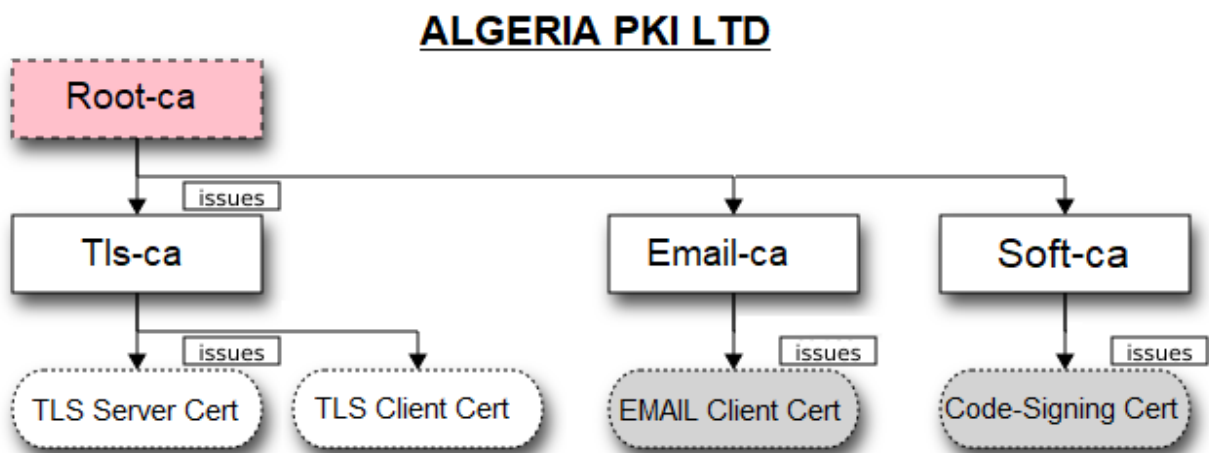


Figure 3.2 Hiérarchie de notre PKI

III. Utilisation de la PKI

1. Mise en place d'un serveur web sécurisé

1.1 Installation et configurations d'apache

```
apt update -y  
apt install apache2 -y
```

Mettre à jour le système Debian et installation du package apache2

```
systemctl status apache2
```

Vérification de l'état du serveur Web

```
systemctl start apache2
```

Si le service n'est pas en cours d'exécution, nous devons démarrer le service à l'aide de la commande.

```
systemctl enable apache2
```

Pour activer le serveur Web Apache au démarrage, exécutons la commande.

```
systemctl restart apache2
```

Pour redémarrer Apache.

NOTE : Le pare-feu peut être très utile dans le cas de grand réseau, mais peut aussi causer beaucoup de problème, c'est donc pour cela que nous allons le configurer puis le désactiver, le temps de tout mettre en place, et à la fin de toute la procédure il faudra alors le réactiver.

Si le pare-feu UFW standard de Linux n'est pas déjà installé, nous devons le faire.

```
apt install ufw
```

Installation du package ufw (pare-feu).

```
ufw enable
```

Activer le pare-feu.

Si le pare-feu UFW est déjà configuré, nous devons autoriser le service Apache sur le pare-feu afin que les utilisateurs externes puissent avoir accès au serveur Web.

```
ufw allow 80/tcp  
ufw allow 443/tcp
```

Pour se faire, nous devons autoriser le trafic sur le port 80 du pare-feu.

```
ufw status
```


Pour vérifier que le port a été autorisé sur le pare-feu.

```
ufw disable
```

Désactiver le pare-feu.

Nous ouvrons n'importe quel navigateur et nous entrons comme URL <http://192.168.15.50/> Pour vérifier que le serveur Web Apache fonctionne correctement.

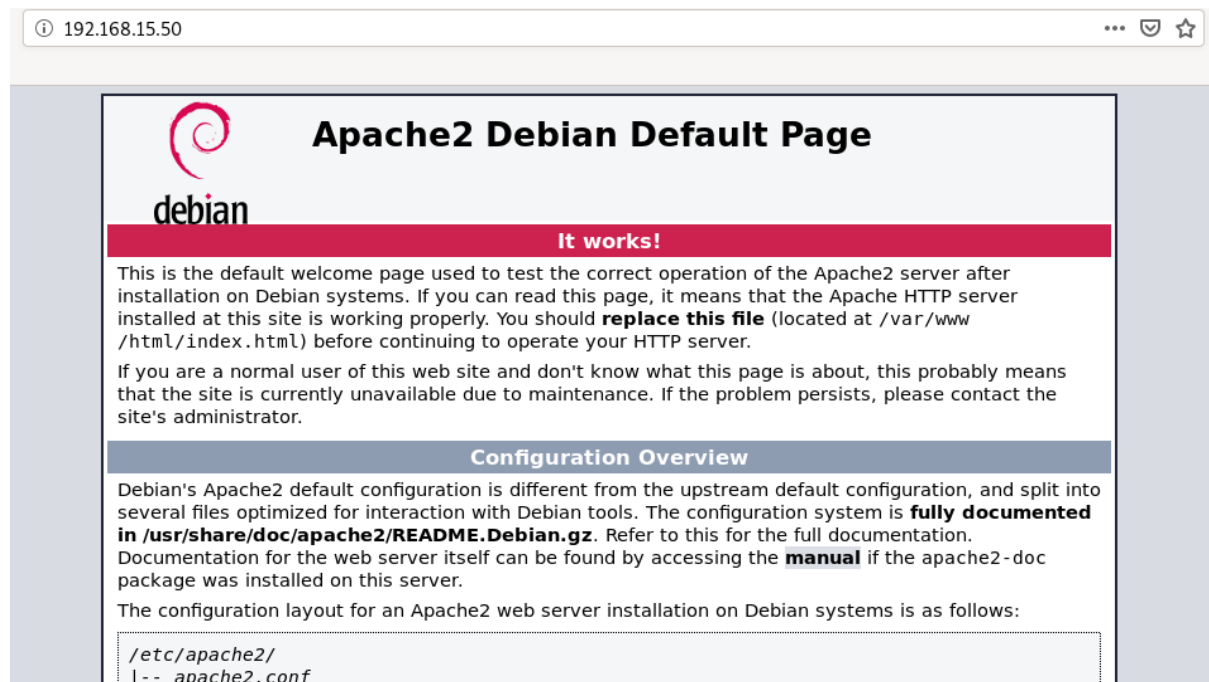


Figure 3.3 Le bon fonctionnement du serveur APACHE2

Le serveur Web Apache étant déjà configuré, il est temps d'héberger notre site Web.

La page Web Apache par défaut index.html se trouve dans /var/www/html/ qui est le répertoire root.

Pour héberger notre site, nous allons tout simplement déposer tous les fichiers de ce dernier dans le dossier /var/www/algeria/.

1.2 Sécurisations du serveur web grâce au certificat SSL

1.2.1 Créations d'une demande de certification pour un serveur TLS

```
SAN=DNS:algeria-pki.dz,DNS:www.algeria-pki.dz \
```

```
openssl req -new \
```

```
-config /ca/tls-ca/tls-req.cnf \
```

```
-out /ca/tls-ca/certsreq/algeria-pki.dz.csr \
```

```
-keyout /ca/tls-ca/private/algeria-pki.dz.key
```

Nous générons une paire de clé (privée et publique) et le fichier CSR pour un certificat de serveur TLS en utilisant le fichier de configuration de demande approprié.

Lorsque nous y avons été invité, nous entrons ces composants DN : C = DZ, O = Algeria PKI Ltd, CN = www.algeria-pki.dz. Le subjectAltName doit être spécifié comme variable d'environnement.

1.2.2 Créations d'un certificat pour un serveur TLS

```
openssl ca \  
  -config /ca/tls-ca/tls-ca.cnf \  
  -in /ca/tls-ca/certsreq/algeria-pki.dz.csr \  
  -out /ca/tls-ca/certs/algeria-pki.dz.crt \  
-extensions tls_ext
```

Nous utilisons l'autorité de certification TLS pour émettre le certificat du serveur.

1.2.3 Créations d'un bundle PEM

```
cat /ca/tls-ca/certs/algeria-pki.dz.crt /ca/tls-ca/certs/tls-ca.crt  
/ca/root-ca/certs/root-ca.crt > /ca/tls-ca/certs/algeria-pki.dz-  
chain.pem
```

Nous créons un fichier de chaîne de certificats qui va contenir toute la hiérarchie allant de la CA racine jusqu'au certificat du site web.

NOTE : il ne faut pas oublier de placer les certificats et le bundle et la paire de clé dans le dossier où se trouve le site web.

1.3 Configuration d'hôtes virtuels sur Apache

```
touch /etc/apache2/sites-available/algeria-pki.dz.conf
```

Maintenant, Nous créons un fichier hôte virtuel pour le domaine.

```
nano /etc/apache2/sites-available/algeria-pki.dz.conf
```

Nous modifions ce dernier avec l'éditeur de texte intégré « **nano** ».

```
<VirtualHost *:80>
```

```
ServerAdmin webmaster@algeria-pki.dz
ServerName algeria-pki.dz
ServerAlias www.algeria-pki.dz
Redirect permanent / https://www.algeria-pki.dz/
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Maintenant, Nous modifions le fichier pour qu'il ressemble à ça, avec comme nom de domaine **algeria-pki.dz**.

Ce fichier se traduit par :

Si n'importe quelle adresse IP (*) fait une requête sur le port 80 et demande algeria-pki.dz dans son URL alors nous le redirigeons vers https donc le port 443.

```
<VirtualHost *:443>
    ServerName algeria-pki.dz
    ServerAlias www.algeria-pki.dz
    ServerAdmin webmaster@algeria-pki.dz
    DocumentRoot /var/www/site/
    Protocols h2 http/1.1
    SSLEngine on
    SSLCertificateFile      /var/www/site/certificat/algeria-pki.dz-
chain.pem
    SSLCertificateKeyFile    /var/www/site/certificat/algeria-
pki.dz.key
    ErrorLog /var/log/apache2/error.algeria-pki.dz.log
    CustomLog /var/log/apache2/access.algeria-pki.dz.log combined
</VirtualHost>
```

Cette partie se traduit par :

Si n'importe quelle adresse IP (*) fait une requête sur le port 443 et demande algeria-pki.dz dans son URL alors nous lui servons les fichiers qui se trouve dans /var/www/site/

« **SSLCertificateKeyFile** » : La paire de clé du site que nous avons générée précédemment

« **SSLCertificateFile** » : La chaîne de certificat (bundle PEM) que nous avons générée précédemment

« **SSLEngine on** » : Pour activer le chiffrement SSL.

```
a2ensite algeria-pki.dz.conf
```

À ce stade, Nous activons le fichier hôte virtuel.

```
a2dissite 000-défaut.conf
```

Désactivons maintenant le site par défaut.

```
a2enmod ssl
```

Nous activons le module ssl sans quoi le https ne marchera pas.

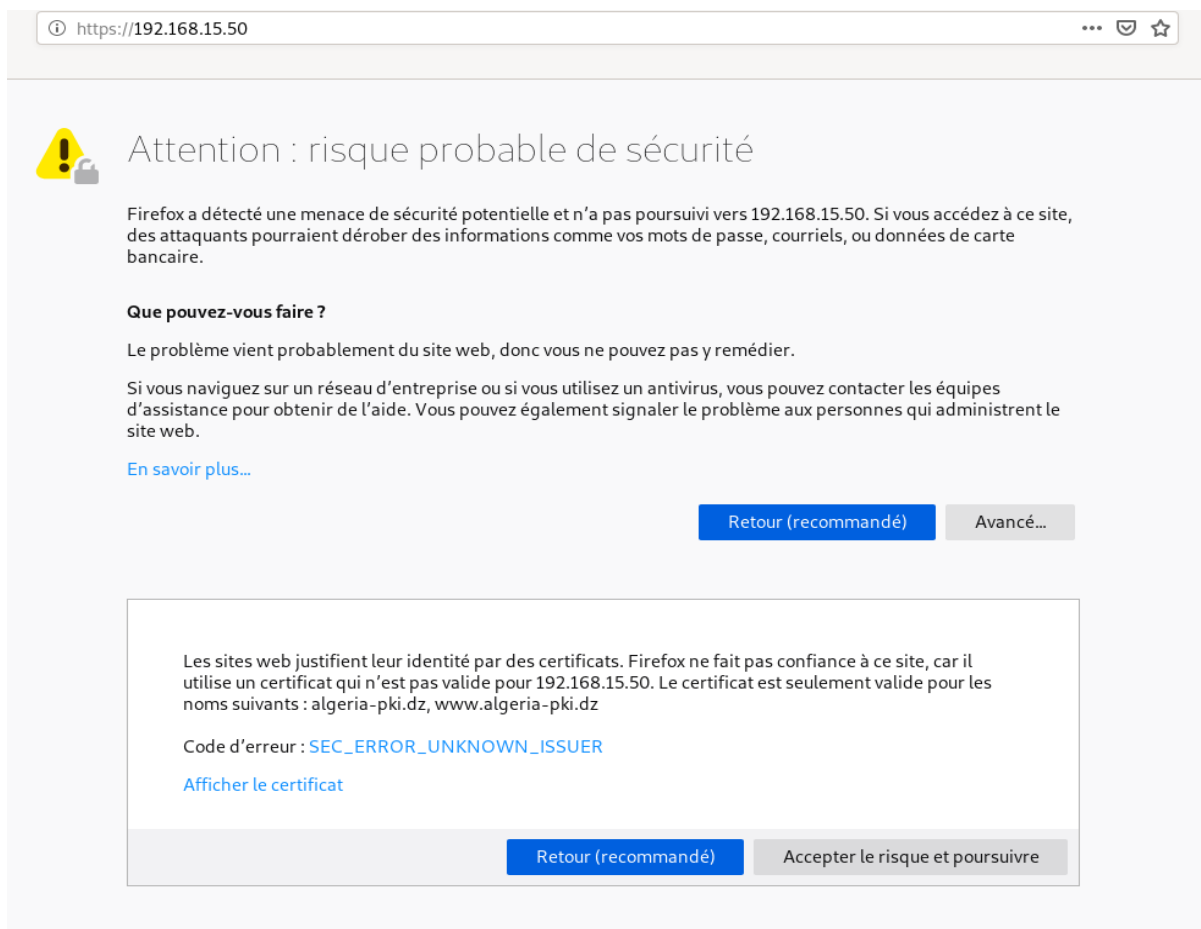
```
systemctl reload apache2
```

Pour effectuer les modifications, nous rechargeons le serveur Web Apache.

```
systemctl restart apache2
```

Maintenant Nous redémarrerons le serveur Web et nous accédons à l'adresse <https://192.168.15.50> dans n'importe quel navigateur.

Lorsque nous y accédons cette page apparaît :



The screenshot shows a Firefox browser window with the address bar displaying `https://192.168.15.50`. The main content area features a yellow warning icon and the heading "Attention : risque probable de sécurité". The text below explains that Firefox has detected a potential security threat and did not proceed to the site because it uses a certificate not valid for the IP address. It lists the valid domains as `algeria-pki.dz` and `www.algeria-pki.dz`. The error code is `SEC_ERROR_UNKNOWN_ISSUER`. At the bottom, there are two buttons: "Retour (recommandé)" and "Accepter le risque et poursuivre".

Figure 3.4 Autorité de certification non reconnue par le navigateur

C'est normal car notre certificat est émis au nom de www.algeria-pki.dz ou algeria-pki.dz et non pas 192.168.15.50, Il a fallu alors trouver un moyen de rediriger l'utilisateur vers l'adresse du site et la solution la plus évidente fut le serveur DNS.

2. Mise en place d'un serveur DNS

2.1 Installation et configuration d'un serveur DNS

```
apt install bind9 dnsutils
```

Le nom du paquet du serveur DNS dans Debian est bind9 et est disponible dans le dépôt de base. Nous installons dès lors le package bind9.

Il faut maintenant préparer notre serveur avant de configurer bind9.

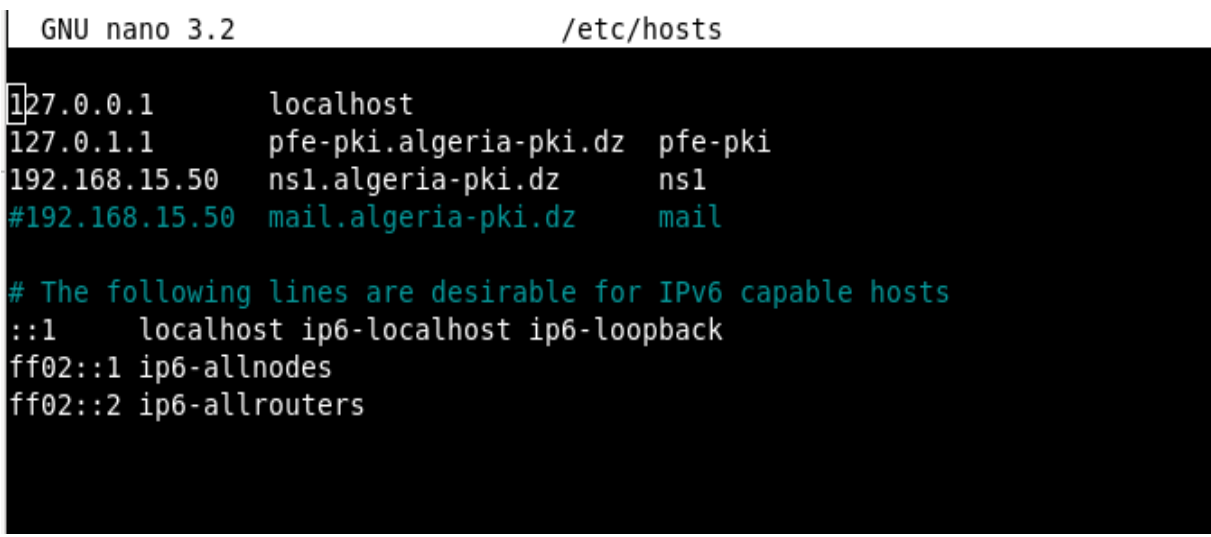
Notre serveur aura ici pour adresse IP : **192.168.15.50**

Tout d'abord, il est nécessaire de placer le nom FQDN (FQDN signifie textuellement : "**Fully Qualified Domain Name**", qu'on pourrait traduire par "**Nom d'hôte pleinement nommé**").

Un serveur de messagerie par exemple doit être entièrement nommé sur Internet. Un serveur de mail ne peut pas s'appeler : « mail.dz » mais il doit impérativement avoir un nom complet du type "mail.algeria-pki.dz".)

Notre FQDN sera tout au long de ce mémoire « **algeria-pki.dz** ».

```
/etc/hosts
```



```
GNU nano 3.2 /etc/hosts
127.0.0.1    localhost
127.0.1.1    pfe-pki.algeria-pki.dz  pfe-pki
192.168.15.50 ns1.algeria-pki.dz    ns1
#192.168.15.50 mail.algeria-pki.dz    mail

# The following lines are desirable for IPv6 capable hosts
::1        localhost ip6-localhost ip6-loopback
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
```

Figure 3.5 Nom d'hôte pleinement nommé de notre serveur web

```
nano /etc/bind/named.conf.option
```

Il s'agit du fichier de configuration bind9. Les modifications à faire seront :

D'autoriser la requête depuis un réseau privé.

D'autoriser la requête récursive.

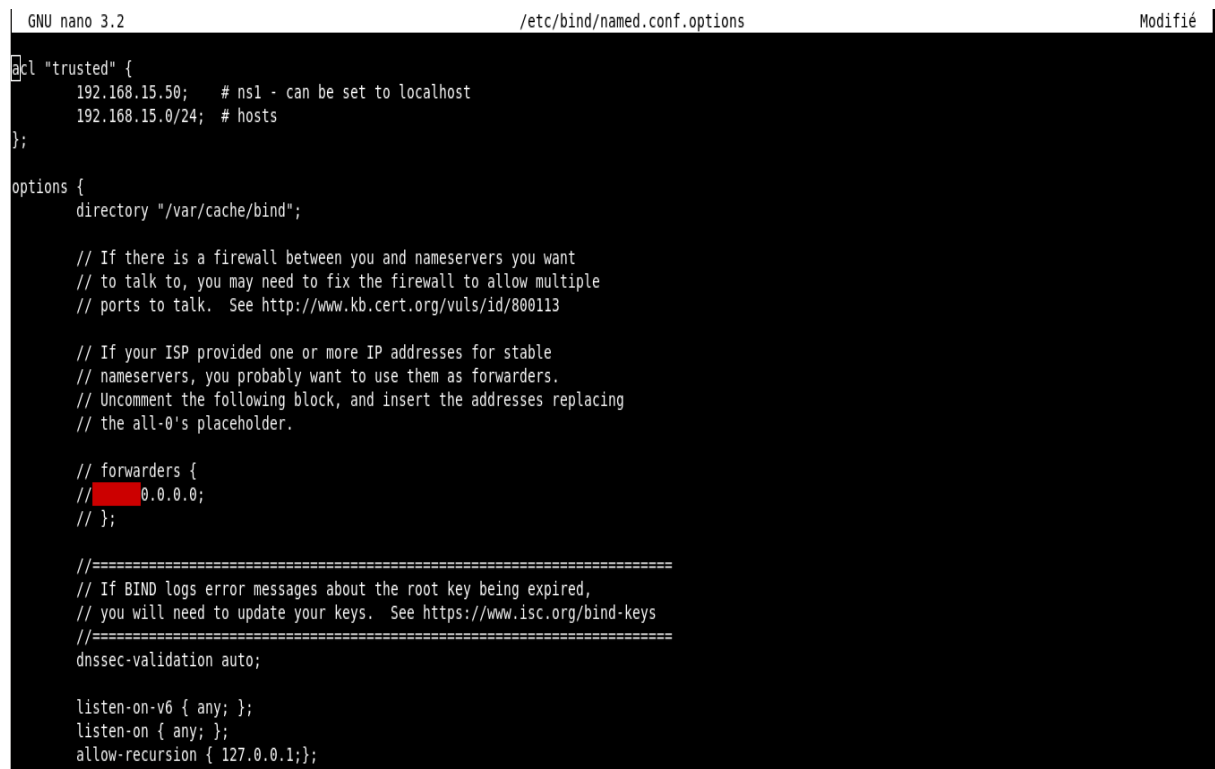
```
listen-on {any;};  
allow-recursion {127.0.0.1 ;} ;
```

Permet à n'importe quel utilisateur de faire des requêtes au serveur DNS.

Nous ajoutons aussi une liste d'ACL autoriser de confiance ACL, c'est entre autre une exception pour le pare-feu.

Nous y mettons les adresses des utilisateurs autorisés et celui du serveur DNS.

```
Acl " trusted " {  
    192.168.15.50      # Notre serveur DNS  
    192.168.15.0/24  # Notre réseau local  
};
```



```
GNU nano 3.2 /etc/bind/named.conf.options Modifié  
acl "trusted" {  
    192.168.15.50; # ns1 - can be set to localhost  
    192.168.15.0/24; # hosts  
};  
  
options {  
    directory "/var/cache/bind";  
  
    // If there is a firewall between you and nameservers you want  
    // to talk to, you may need to fix the firewall to allow multiple  
    // ports to talk. See http://www.kb.cert.org/vuls/id/800113  
  
    // If your ISP provided one or more IP addresses for stable  
    // nameservers, you probably want to use them as forwarders.  
    // Uncomment the following block, and insert the addresses replacing  
    // the all-0's placeholder.  
  
    // forwarders {  
    // 0.0.0.0;  
    // };  
  
    //=====  
    // If BIND logs error messages about the root key being expired,  
    // you will need to update your keys. See https://www.isc.org/bind-keys  
    //=====  
    dnssec-validation auto;  
  
    listen-on-v6 { any; };  
    listen-on { any; };  
    allow-recursion { 127.0.0.1};
```

Figure 3.6 Configuration du serveur DNS

2.2 Création des zones DNS

```
nano /etc/bind/named.conf.local
```

Commençons par créer une zone avant pour notre domaine.

Nous ne devons pas utiliser le fichier de configuration globale pour la zone DNS locale, nous devons déclarer nos zones DNS à savoir la zone « **algeria-pki.dz** » et

sa zone inverse associée « **15.168.192.in-addr.arpa** » afin que les adresses IP puissent être traduites en noms de domaines.

```
GNU nano 3.2 /etc/bind/named.conf.local

//
// Do any local configuration here
//

// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";

zone "algeria-pki.dz" {
    type master;
    file "/etc/bind/forwarde.algeria-pki.dz.db";
};

zone "15.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/reverse.algeria-pki.dz.db";
};
```

Figure 3.7 Déclarations des zones DNS

NOTE : Type master (car DNS primaire)

Nous devons maintenant créer nos zones.

Il faut pour cela créer et modifier le fichier suivant comme ci-dessous :

```
nano /etc/bind/forwarde,algeria-pki.dz.db
nano /etc/bind/reverse,algeria-pki.dz.db
```

```
GNU nano 3.2 /etc/bind/forwarde.algeria-pki.dz.db
[?] BIND data file for local loopback interface
;
;TTL      604800
@        IN      SOA      ns1.algeria-pki.dz. root.algeria-pki.dz. (
                                4          ; Serial
                                604800     ; Refresh
                                86400      ; Retry
                                2419200    ; Expire
                                604800 )   ; Negative Cache TTL
;
;@        IN      NS       localhost.
;@        IN      A        127.0.0.1
;@        IN      AAAA     ::1

;Name Server Information
@        IN      NS       ns1.algeria-pki.dz.

;IP address of Name Server
ns1      IN      A        192.168.15.50

;Mail Exchanger
algeria-pki.dz. IN  MX     50     mail.algeria-pki.dz.

;A - Record HostName To Ip Address
        IN      A        192.168.15.50
www      IN      A        192.168.15.50
mail     IN      A        192.168.15.50
```

Figure 3.8 Création de la zone DNS direct

```

GNU nano 3.2 /etc/bind/reverse.algeria-pki.dz.db
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA      algeria-pki.dz. root.algeria-pki.dz. (
                        3          ; Serial
                        604800     ; Refresh
                        86400      ; Retry
                        2419200    ; Expire
                        604800 )   ; Negative Cache TTL
;
;@         IN      NS       localhost.
;1.0.0     IN      PTR     localhost.

;Name Server Information
@         IN      NS       ns1.algeria-pki.dz.

;Reverse lookup for Name Server
50        IN      PTR     ns1.algeria-pki.dz.

;PTR Record IP address to HostName
50        IN      PTR     www.algeria-pki.dz.
50        IN      PTR     mail.algeria-pki.dz.
50        IN      PTR     algeria-pki.dz.

```

Figure 3.9 Création de la zone DNS inverse

NOTE : les types dans le fichier de zone :

- SOA - Début de l'autorité
- NS - Noms de serveur
- A - Une entrée
- MX - Mail for Exchange
- CN - Nom canonique

```
named-checkconf -z
```

Pour vérifier si tous le fichier sont correctement configurés et qu'il n'y a pas d'erreur

```

Fichier  Édition  Affichage  Rechercher  Terminal  Aide
root@pfe-pki:~# named-checkconf -z
zone algeria-pki.dz/IN: loaded serial 4
zone 15.168.192.in-addr.arpa/IN: loaded serial 3
zone localhost/IN: loaded serial 2
zone 127.in-addr.arpa/IN: loaded serial 1
zone 0.in-addr.arpa/IN: loaded serial 1
zone 255.in-addr.arpa/IN: loaded serial 1
root@pfe-pki:~#

```

de syntaxe

Figure 3.10 Vérification de la syntaxe

```
service bind9 restart
```

Redémarrer le serveur DNS pour prendre en compte les modifications.

2.3 Vérification du serveur DNS

2.3.1 Test sur machine local

Accédons au fichier resolv.conf dans laquelle est déposée l'adresse du DNS principal et secondaire.

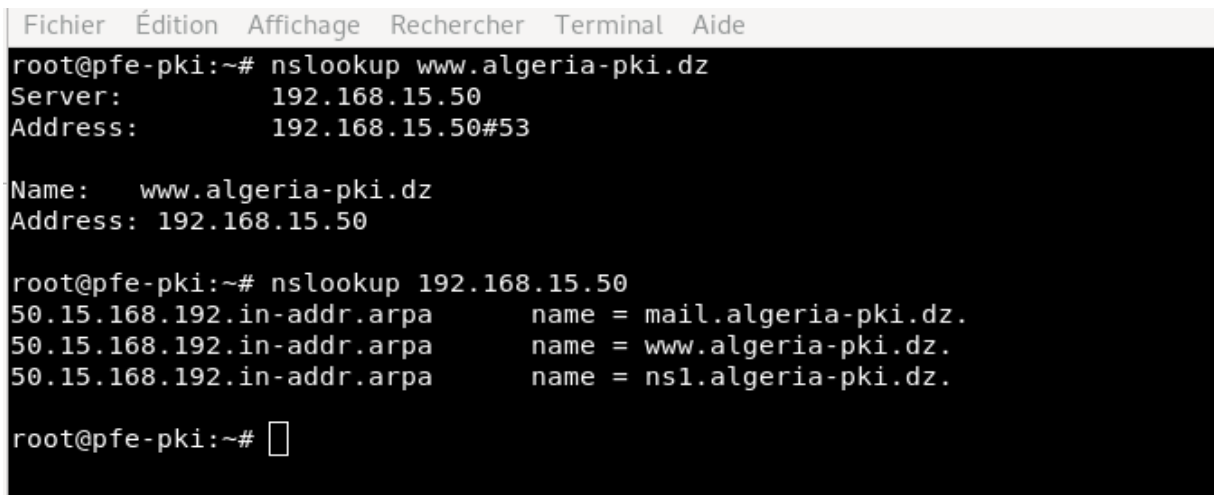
```
nano /etc/resolv.conf
```

Nous ajoutons les entrées suivantes :

nameserver 192.168.15.50 (adresse du serveur DNS local)

nameserver 8.8.8.8 (adresse du serveur DNS de Google pour pouvoir accéder à internet)

```
nslookup www.algeria-pki.dz donnera l'adresse du site
```



```
Fichier  Édition  Affichage  Rechercher  Terminal  Aide
root@pfe-pki:~# nslookup www.algeria-pki.dz
Server:      192.168.15.50
Address:     192.168.15.50#53

Name:   www.algeria-pki.dz
Address: 192.168.15.50

root@pfe-pki:~# nslookup 192.168.15.50
50.15.168.192.in-addr.arpa    name = mail.algeria-pki.dz.
50.15.168.192.in-addr.arpa    name = www.algeria-pki.dz.
50.15.168.192.in-addr.arpa    name = ns1.algeria-pki.dz.

root@pfe-pki:~#
```

Figure 3.11 Vérification du bon fonctionnement du serveur DNS

nslookup permet de donner s'il y a une correspondance entre adresse IP et nom de domaine et vice versa.

Maintenant sur notre navigateur nous entrons l'URL : www.algeria-pki.dz

Mais au préalable il faudra installer le certificat de la CA racine dans le navigateur, dans le but qu'elle devienne CA de confiance.

Sur Windows :

Il suffira de double cliquer sur le fichier **root-ca.crt** et de cliquer sur installer et suivre les étapes.

Sur linux : Il faudra tout simplement glisser déposer le fichier **root-ca.crt** dans la fenêtre du navigateur et spécifier ca root de confiance.

Ainsi le serveur DNS est opérationnel sur la machine locale, nous pourrons accéder à notre site web de manière à chiffrer par SSL (https).

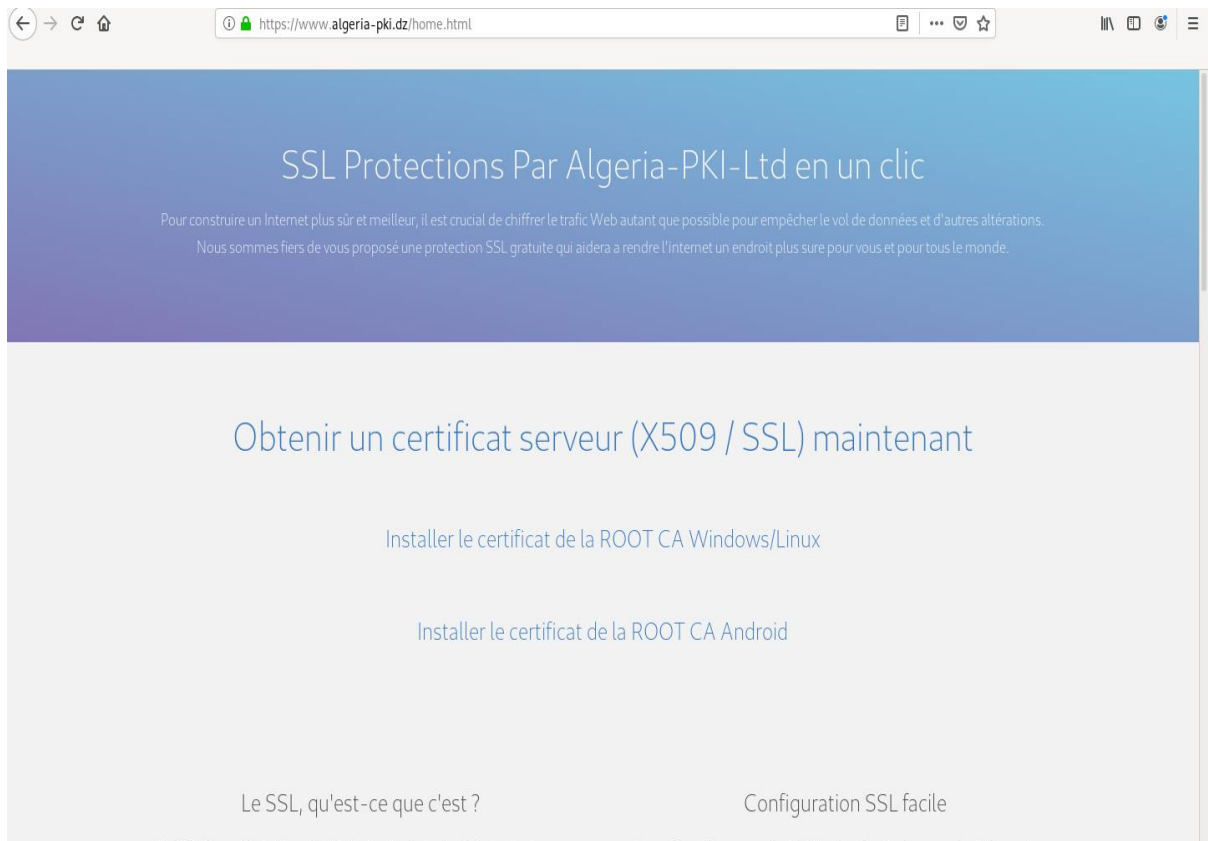


Figure 3.12 Serveur correctement sécurisé pas certificat SSL

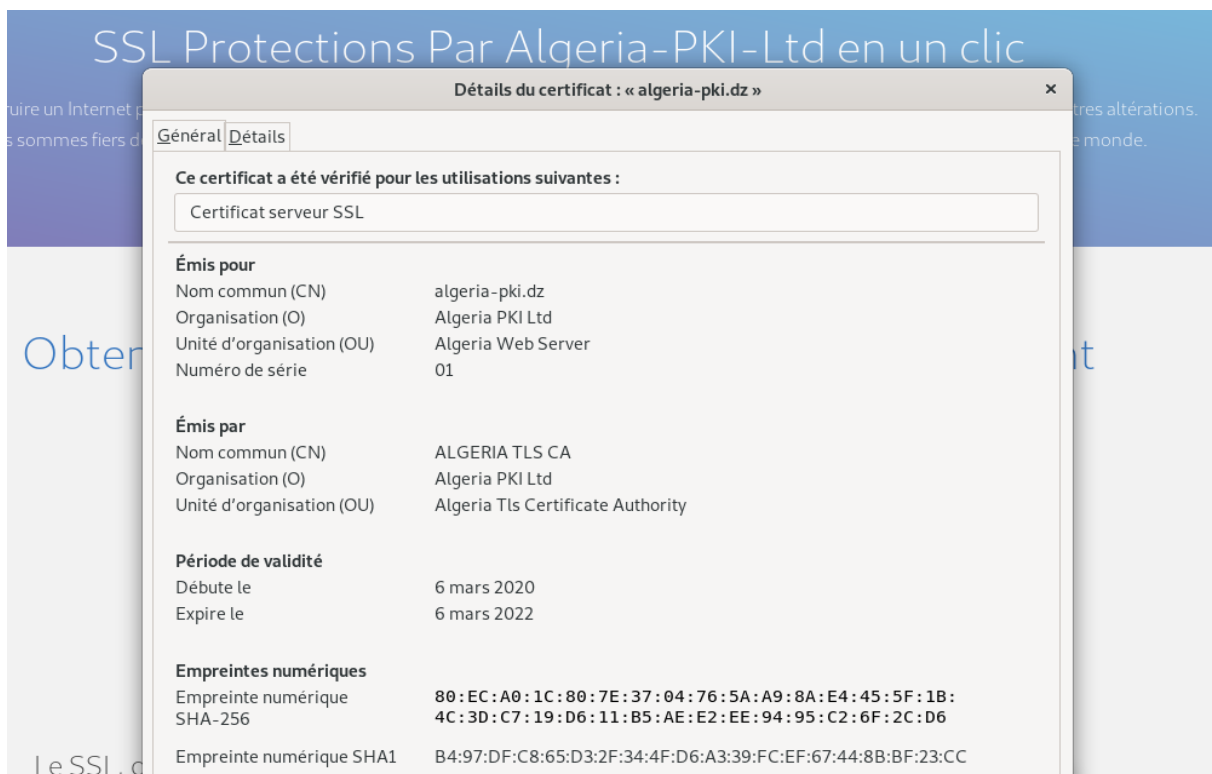


Figure 3.13 Certificat du serveur

La hiérarchie des CA est complète grâce à l'AIA

L'extension Authority Information Access (AIA) permet aux clients SSL/TLS (le plus souvent des navigateurs web) d'aller rechercher des certificats intermédiaires manquants, non-présentés par le serveur. Cette extension, qui place dans le certificat final un "CA Issuer" contenant une URL, permet au navigateur d'aller chercher le certificat manquant, puis de retenter la vérification de la chaîne avec.

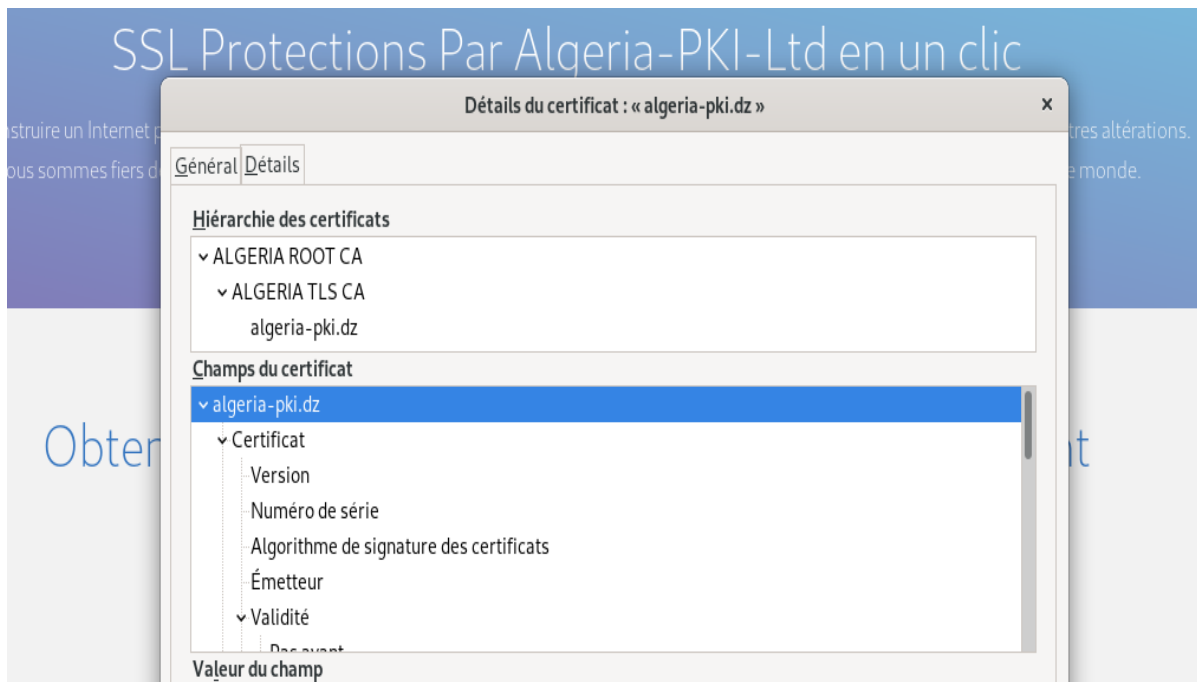


Figure 3.14 Chaîne de certificat (hiérarchie)

Reste maintenant à tester sur une machine externe mais dans le même réseau.

2.3.2 Test sur machine externe

Pour tester si le serveur DNS fonctionne correctement dans le réseau local Nous utilisons une autre machine qui se trouve dans le même réseau local donc avec une adresse de type 192.168.15.XXX.

Il faudra alors lui attribuer comme adresse DNS primaire 192.168.15.50 et tenter d'accéder dans un navigateur à l'url www.algeria-pki.dz.

Maintenant que le serveur DNS fonctionne parfaitement sur toutes les machines autorisées nous avons réussi à sécuriser un site web grâce à notre PKI.



3.15 Configuration de l'utilisateur externe

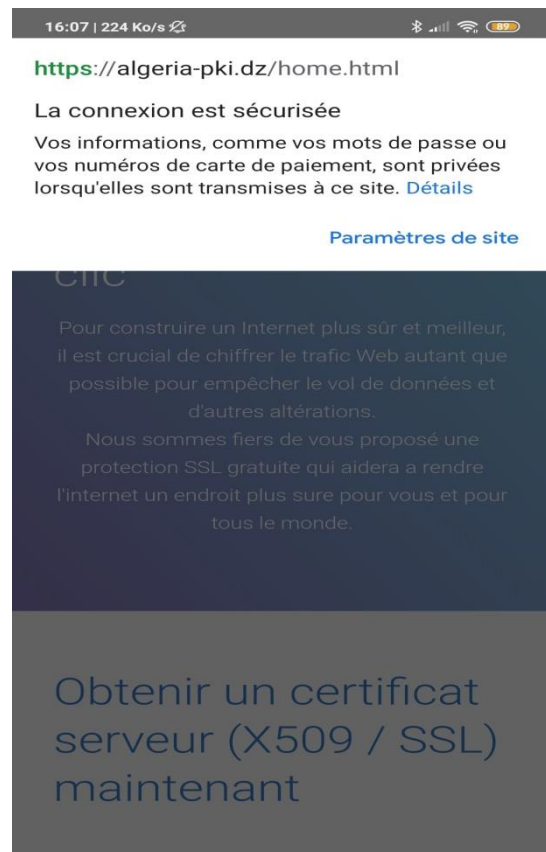


Figure 3.16 Serveur correctement sécurisé

3. Mise en place d'un réseau Wi-Fi avec authentification basée sur des certificats

3.1 Installation et configuration d'un serveur Radius (serveur d'authentification) et DaloRADIUS (interface graphique pour Radius)

```
apt -y install mariadb-server mariadb-client
```

Nous utiliserons Mariadb mais tout autre serveur de base de données pris en charge peut être utilisé.

```
systemctl status mariadb
```

Vérifier si Mariadb est active.

```
systemctl start mariadb
```

Sinon la lancer.

```
mysql_secure_installation
```

Sécuriser Mariadb en supprimant les utilisateurs et la base de données test et en attribuant un mot de passe root.

```
mysql -u root -p
```

Tester **Mariadb**, un mot de passe sera demandé, celui du root une fois de retour à la ligne de commande **Mariadb** nous devront créer une base de données et un utilisateur pour **FreeRADIUS / DaloRADIUS**.

```
CREATE DATABASE radius;
```

Crée une base de données pour notre serveur radius.

```
GRANT ALL ON radius.* TO radius@localhost IDENTIFIED BY "toor";  
FLUSH PRIVILEGES;
```

Crée un utilisateur et lui attribue un accès à la base de données radius.

```
mysql -u radius -p
```

Nous accédons à Mariadb en tant que l'utilisateur radius pour vérifier qu'il a bien été créé et est actif. Le mot de passe choisi lors de la création de l'utilisateur sera demandé.

```
SHOW DATABASES;
```

Pour afficher toute les bases de données existantes.

3.2 Installation de PHP

PHP est primordial au bon fonctionnement de DaloRADIUS la version graphique qui permet de gérer le serveur FreeRADIUS plus facilement.

```
apt -y install php libapache2-mod-php php-{gd,common,mail,mail-  
mime,mysql,pear,mbstring,xml,curl}
```

Installation de tous les modules de PHP.

```
php -v
```

Vérifier la version de PHP ici dans notre cas nous somme à la V 7.3.14.

3.3 Installation et configuration de FreeRADIUS

```
apt -y install freeradius freeradius-mysql freeradius-utils
```

Installation des package pour FreeRADIUS.

```
systemctl enable --now freeradius.service
```

Activations du service FreeRADIUS.

```
systemctl status freeradius
```

Nous vérifions que le service est actif.

NOTE : pour lancer FreeRADIUS en mode debug Nous utilisons ces commandes :

```
netstat -tulp | grep "18120"
```

```
kill «numéro du processus»
```

```
freeradius -X
```

Nous saurons que nous sommes en debug mode une fois qu'apparaîtra la ligne suivante :

```
« Listening on auth address 127.0.0.1 port 18120 bound to server »
```

```
mysql -u root -p radius < /etc/freeradius/3.0/mods-config/sql/main/mysql/schema.sql
```

Importer le schéma de base de données Radius pour remplir la base de données radius.

```
ln -s /etc/freeradius/3.0/mods-available/sql /etc/freeradius/3.0/mods-enabled/
```

Nous créons un lien entre la base de données et FreeRADIUS.

```
nano /etc/freeradius/3.0/mods-enabled/sql
```

Nous modifions les fichiers de configurations pour s'adapter à notre environnement

```
sql {
  driver = "rlm_sql_mysql"
  dialect = "mysql"

  # Connection info:

  server = "localhost"
  port = 3306
  login = "radius"
  password = "StrongradIusPass"

  # Database table configuration for everything except Oracle

  radius_db = "radius"
}

# Set to 'yes' to read radius clients from the database ('nas' table)
# Clients will ONLY be read on server startup.
read_clients = yes

# Table to keep radius client info
client table = "nas"
```

Figure 3.17 Configuration du serveur radius

```
sudo chgrp -h freerad /etc/freeradius/3.0/mods-available/sql
sudo chown -R freerad:freerad /etc/freeradius/3.0/mods-enabled/sql
```

Changer les droits des fichiers

```
systemctl restart freeradius
```

Redémarrer le service FreeRADIUS pour prendre en compte les modifications.

3.4 Installation et configuration de DaloRADIUS

Nous allons utiliser DaloRADIUS pour gérer le serveur radius à partir d'une interface Web.

```
apt -y install wget unzip
wget https://github.com/lirantal/daloradius/archive/master.zip
unzip master.zip
mv daloradius-master/ daloradius
```

Téléchargement de l'archive de DaloRADIUS depuis Github.

```
cd daloradius
```

Accéder au dossier que nous venons de télécharger.

```
mysql -u root -p radius < contrib/db/fr2-mysql-daloradius-and-
freeradius.sql
mysql -u root -p radius < contrib/db/mysql-daloradius.sql
```

Importer la base de donnée DaloRADIUS que nous venons de télécharger, dans MariaDB.

```
cd ..
sudo mv daloradius /var/www/algeria/
```

Déplacer le dossier qui contient l'interface de DaloRADIUS dans le serveur que nous venons d'installé dans les étapes précédente, pour qu'il y soit accessible directement depuis le site www.algeria-pki.dz.

```
sudo chown -R www-data:www-data /var/www/algeria/daloradius/
sudo chmod 664 /var/www/algeria/daloradius/library/daloradius.conf.php
```

Changer les droits des dossiers.

```
nano /var/www/algeria/daloradius/library/daloradius.conf.php
```

Nous modifions le fichier de configurations de DaloRADIUS pour le faire correspondre avec la configuration de notre base de données.

```
$configValues['CONFIG_DB_HOST'] = 'localhost';  
$configValues['CONFIG_DB_PORT'] = '3306';  
$configValues['CONFIG_DB_USER'] = 'radius';  
$configValues['CONFIG_DB_PASS'] = 'StrongradIusPass';  
$configValues['CONFIG_DB_NAME'] = 'radius';
```

Figure 3.18 Configuration de DaloRADIUS

```
systemctl restart freeradius.service apache2
```

Nous redémarrons FreeRADIUS et apache2 pour appliquer les changements.

Nous pouvons maintenant accéder à l'interface DaloRADIUS depuis n'importe quel navigateur par l'adresse suivante :

<https://www.algeria-pki.dz/daloradius>

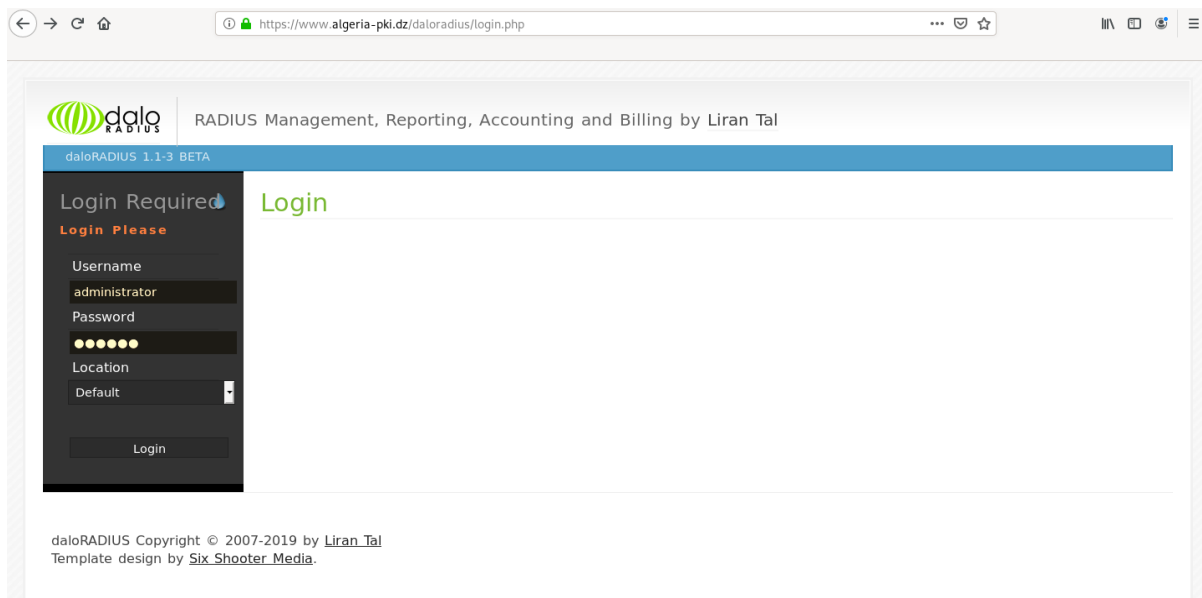


Figure 3.19 Interface DaloRADIUS fonctionnelle

Une fois sur la page de login de DaloRADIUS :

Le nom d'utilisateur et le mot de passe par défaut, sont respectivement :

« **administrator/radius** »

NOTE : Un problème auquel, nous avons dû faire face, était celui de la page blanche après avoir appuyé sur **login**, le problème se trouver dans **PHP** :

La correction s'est faite comme suit :

```
cd /var/lib/php/session/  
chown -R root:nginx *
```



```
apt install php7.3-dba
apt install php-pear
pear install DB
systemctl restart freeradius.service apache2
```

Il faut maintenant ajouter un NAS (appareil qui peut consulter la base de donnée de radius donc le point d'accès).

Accéder à DaloRADIUS et se connecter :

<https://www.algeria-pki.dz/daloradius/index.php>

Aller dans management/Nas/new NAS

Et ajouter l'@ IP du point d'accès (192.168.15.1) et un mot de passe dans la page de configuration de notre point d'accès. Mettre « Nas type » sur **other** « Nas

The screenshot shows the 'New NAS Record' page in the DaloRADIUS web interface. The page has a navigation menu with 'Management' selected. The 'NAS Info' tab is active, showing fields for 'NAS IP/Host' (192.168.15.1), 'NAS Secret' (monrouter), 'NAS Type' (other), and 'NAS Shortname' (Broadcom). An 'Apply' button is at the bottom.

ShortName » le nom de Notre point d'accès (Broadcom)

Figure 3.20 Ajout de client autorisé à consulter la base de données (point d'accès)

Maintenant il est temps d'ajouter des utilisateurs, autorisés à se connecter à notre point d'accès une fois leurs certificats vérifiés Aller dans management/Users/new User

New User | ?

The screenshot shows the 'New User' page in the DaloRADIUS web interface. The 'Account Info' tab is active, showing fields for 'Username' (pfe-pki), 'Password' (ipwEDmKB), 'Password Type' (Cleartext-Password), and 'Group' (Select Groups). An 'Apply' button is at the bottom.

Figure 3.21 Ajout d'un utilisateur autorisé à se connecter au point d'accès

Nous ajoutons un Username (le nom de la machine ou un alias « pfe-pki ») un mot de passe random, et dans user info (optionnelle) le nom et prénom de la personne ensuite appliquer les changements.

Nous devons Configurer FreeRADIUS pour le faire fonctionner avec l'authentification EAP-TLS (Extensible Authentication Protocol - Transport Layer Security) :

```
nano /etc/freeradius/eap.conf
```

Nous modifions :

```
défaut_eap_type a "tls"
```

Nous commentons en ajoutant « # » au début de la ligne :

« **Toutes les méthodes d'authentification sauf celle de tls.** »

«**private_key_password** ».

Changer:

```
private_key_file
```

En

```
private_key_file = /etc/freeradius/3.0/certs/daloradius.key
```

```
certificate_file
```

En

```
certificate_file = /etc/freeradius/3.0/certs/daloradius.crt
```

```
CA_file
```

En

```
CA_file = /etc/freeradius/3.0/certs/daloradius-chain.pem
```

Nous changeons aussi les droit des fichiers avec :

```
chmod 555 /etc/freeradius/3.0/certs/ daloradius-chain.pem
```

```
chmod 555 /etc/freeradius/3.0/certs/ daloradius.key
```

```
chmod 555 /etc/freeradius/3.0/certs/ daloradius.crt
```

Nous modifions les droits des fichiers pour les rendre non modifiables (par mesure de sécurité).

```
nano /etc/freeradius/3.0/clients.conf
```

Nous ajoutons :

```
clients Broadcom {
    ipaddr = 192.168.15.1
    secret = monrouter
    shortname = Broadcom
nastype = other
}
```

Nous ajoutons ces lignes pour autoriser le point d'accès à consulter la base de données radius.

Maintenant Nous devons générer un certificat pour l'utilisateur et pour le serveur radius.

3.4.1 Création d'un certificat server TLS (radius)

3.4.1.1 Créations d'une demande de certification pour un serveur TLS

Serveur: «**daloradius** »

```
openssl req -new \
    -config /ca/tls-ca/tls-req.cnf \
    -out /ca/tls-ca/certsreq/daloradius.csr \
    -keyout /ca/tls-ca/private/daloradius.key
```

Nous générons une paire de clé (privée et publique) et le fichier CSR pour un certificat de serveur TLS en utilisant le fichier de configuration de demande approprié. Lorsque nous y sommes invité, entrons ces composants DN : C = DZ, O = Algeria PKI Ltd, CN = daloradius.

3.4.1.2 Créations d'un certificat pour un serveur TLS

```
openssl ca \
    -config /ca/tls-ca/tls-ca.cnf \
    -in /ca/tls-ca/certsreq/daloradius.csr \
    -out /ca/tls-ca/certs/daloradius.crt \
    -extensions server_ext
```

Nous utilisons l'autorité de certification TLS pour émettre le certificat du serveur.

3.4.1.3 Créations d'un bundle PEM

```
cat /ca/tls-ca/certs/daloradius.crt /ca/tls-ca/certs/tls-ca.crt  
/ca/root-ca/certs/root-ca.crt > /ca/tls-ca/certs/daloradius-  
chain.pem
```

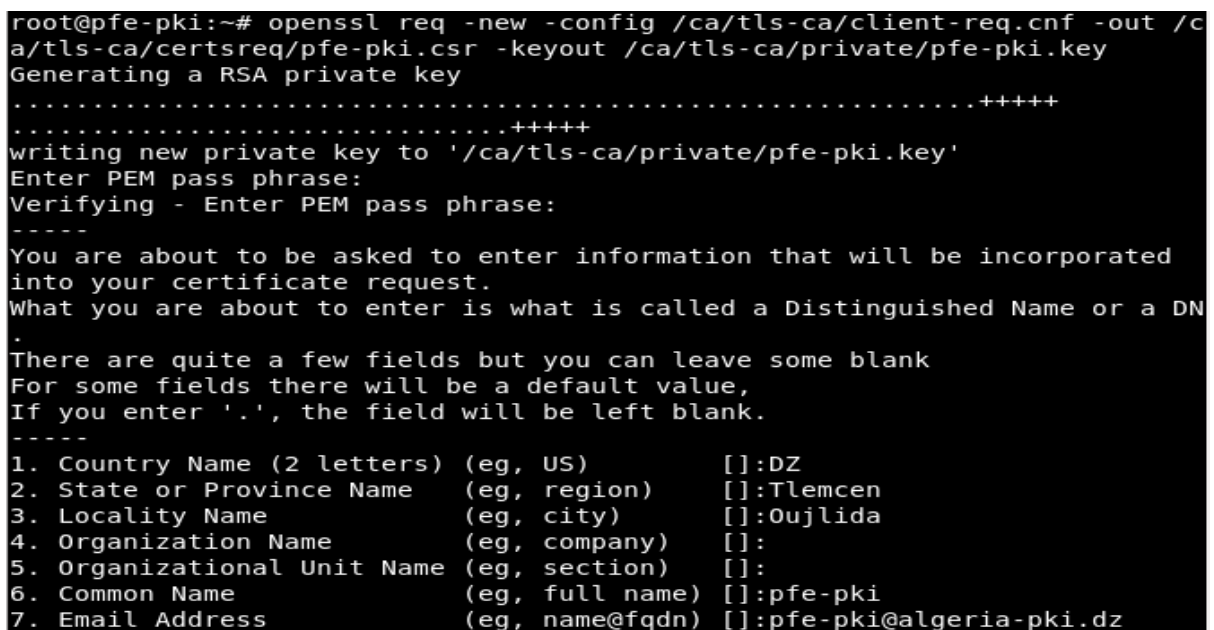
3.4.2 Création d'un certificat client TLS (utilisateur)

3.4.2.1 Créations d'une demande de certification pour un client TLS

Utilisateur : **pfe-pki**.

```
openssl req \  
-new -config /ca/tls-ca/client-req.cnf \  
-out /ca/tls-ca/certsreq/pfe-pki.csr \  
-keyout /ca/tls-ca/private/pfe-pki.key
```

Avec la commande openssl **req-new**, Nous générons une paire de clé (privée et publique) et un fichier CSR (certificat request) pour l'utilisateur **pfe-pki**.



```
root@pfe-pki:~# openssl req -new -config /ca/tls-ca/client-req.cnf -out /c  
a/tls-ca/certsreq/pfe-pki.csr -keyout /ca/tls-ca/private/pfe-pki.key  
Generating a RSA private key  
.....+++++  
.....+++++  
writing new private key to '/ca/tls-ca/private/pfe-pki.key'  
Enter PEM pass phrase:  
Verifying - Enter PEM pass phrase:  
-----  
You are about to be asked to enter information that will be incorporated  
into your certificate request.  
What you are about to enter is what is called a Distinguished Name or a DN  
.  
There are quite a few fields but you can leave some blank  
For some fields there will be a default value,  
If you enter '.', the field will be left blank.  
-----  
1. Country Name (2 letters) (eg, US)          []:DZ  
2. State or Province Name (eg, region)       []:Tlemcen  
3. Locality Name (eg, city)                  []:Oujlida  
4. Organization Name (eg, company)          []:  
5. Organizational Unit Name (eg, section)    []:  
6. Common Name (eg, full name)              []:pfe-pki  
7. Email Address (eg, name@fqdn)            []:pfe-pki@algeria-pki.dz
```

Figure 3.22 Demande de certificat utilisateur

3.4.2.2 Créations d'un certificat pour un client TLS

```
openssl ca \  
-config /ca/tls-ca/tls-ca.cnf \  
-in /ca/tls-ca/certsreq/pfe-pki.csr \  
-out /ca/tls-ca/certs/pfe-pki.crt \  
-extensions client_ext
```

Nous créons un certificat pour l'utilisateur **pfe-pki** signé par la CA intermédiaire **tls-ca**.

```
Check that the request matches the signature
Signature ok
Certificate Details:
  Serial Number: 2 (0x2)
  Validity
    Not Before: Mar  7 16:26:50 2020 GMT
    Not After : Mar  7 16:26:50 2022 GMT
  Subject:
    countryName           = DZ
    stateOrProvinceName  = Tlemcen
    localityName          = Oujlida
    commonName            = pfe-pki
  X509v3 extensions:
    X509v3 Key Usage: critical
      Digital Signature
    X509v3 Basic Constraints:
      CA:FALSE
    X509v3 Extended Key Usage:
      TLS Web Client Authentication
    X509v3 Subject Key Identifier:
      0C:87:41:48:7A:A7:FC:F3:4A:AB:02:07:20:82:69:32:A7:AD:CA:89
    X509v3 Authority Key Identifier:
      keyid:16:83:51:5F:90:25:0E:1D:01:6A:21:C3:B7:FE:9E:D9:F0:0E:E9:36

  Authority Information Access:
    CA Issuers - URI:https://algeria-pki.dz/ca/tls-ca/tls-ca.cer

  X509v3 CRL Distribution Points:

  Full Name:
```

Figure 3.23 Signature de la demande par une autorité de certification

Maintenant nous avons notre certificat utilisateur mais pour que l'utilisateur puisse installer son certificat comme certificat personnel, il lui faut un fichier PKCS12 (.p12) (un bundle de toute la chaîne de certificat + sa paire de clé)

3.4.1.3 Créations d'un bundle PKCS12

```
openssl pkcs12 -export -name "pfe-pki" \
-inkey /ca/tls-ca/private/pfe-pki.key \
-in /ca/tls-ca/certs/pfe-pki.crt \
-certfile /ca/tls-ca/certs/tls-chain.pem \
-out /ca/tls-ca/certs/pfe-pki.p12
```

Nous installons maintenant le fichier sur la machine de l'utilisateur pour notre cas c'est la machine hôte.

Dans un environnement linux, il n'y a pas de gestionnaire de certificat comme sur Windows, c'est directement à partir du navigateur que ça se joue. Nous allons dans Firefox/paramètre dans la recherche Nous tapons certificats/afficher les certificats.

Dans l'onglet vos certificat Nous cliquons sur importer et Nous sélectionnons notre fichier .p12

Le mot de passe est demandé taper le et maintenant nous voyons notre certificat affiché.

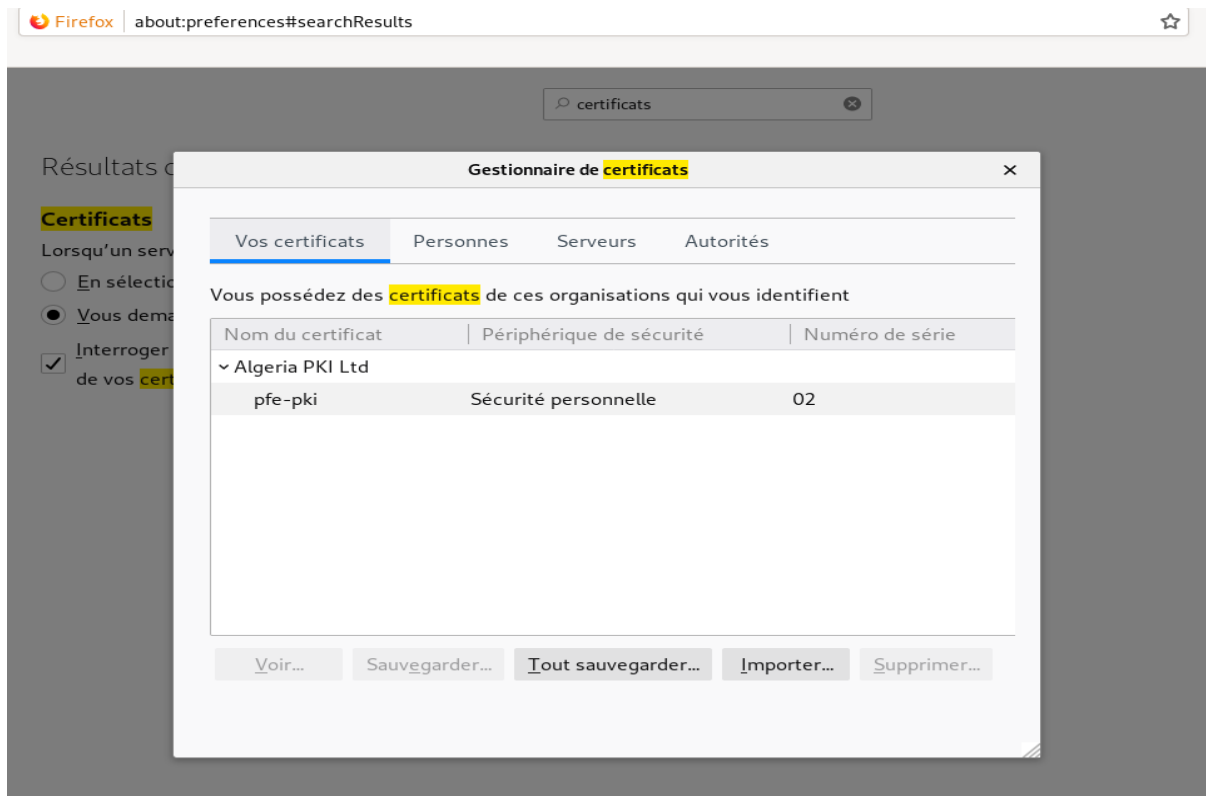


Figure 3.24 Certificat utilisateur installé

3.5 Configuration du point d'accès et de l'interface réseau client

3.5.1 Configuration du point d'accès

Il faut d'abord se connecter au point d'accès à l'adresse 192.168.15.1.

Nom d'utilisateur et mot de passe par défaut :

admin/admin

Ensuite aller dans Wireless/Security et modifier :

- Network authentication : **WPA2**
- RADIUS server IP : **192.168.15.50**
- RADIUS key : **monrouter** (la clé donner lors de la création du NAS)
- WPA encryptions : **AES**

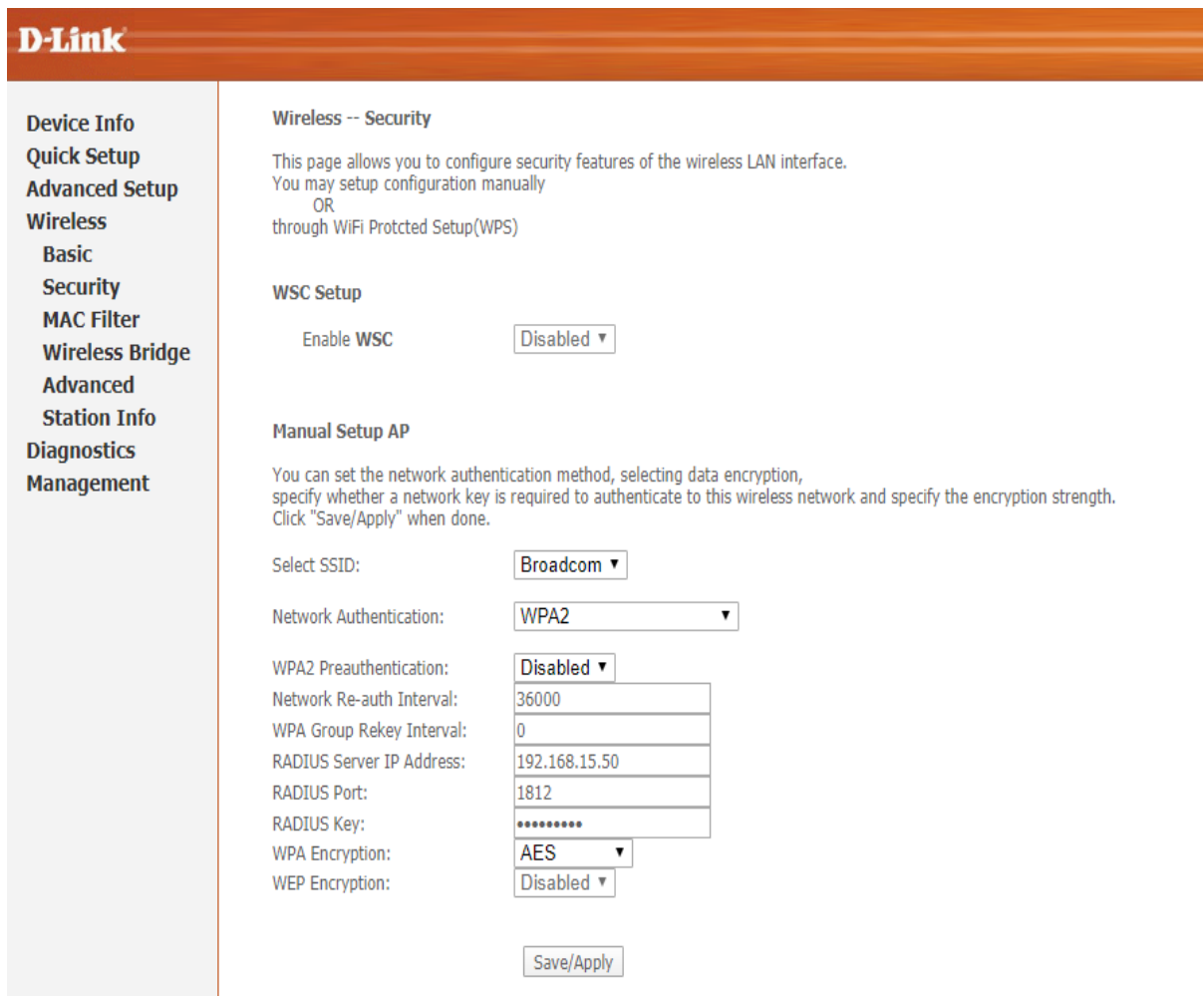


Figure 3.25 Configuration du point d'accès

3.5.2 Configuration du réseau du client Linux

Maintenant nous allons configurer notre wifi, Nous allons dans paramètre wifi, connexion à un réseau masqué et Nous entrons l'information suivante :

- **Le nom de notre point d'accès** (Broadcom).
- **Sécurité** : WAP et WPA2 entreprise (le « entreprise » est primordiale).
- **Authentification** : TLS.
- **Identité** : (pfe-pki) le nom de votre machine.
- **Certificat CA** : la chaine complète de algeriapki.dz jusqu'à la CA racine (bundle crée précédemment).
- **Certificat utilisateur** : le fichier PKCS12 que vous avez créé pour votre machine.
- **Mot de passe** : le mot de passe de la paire de clé ou bien celui du fichier PKCS12.

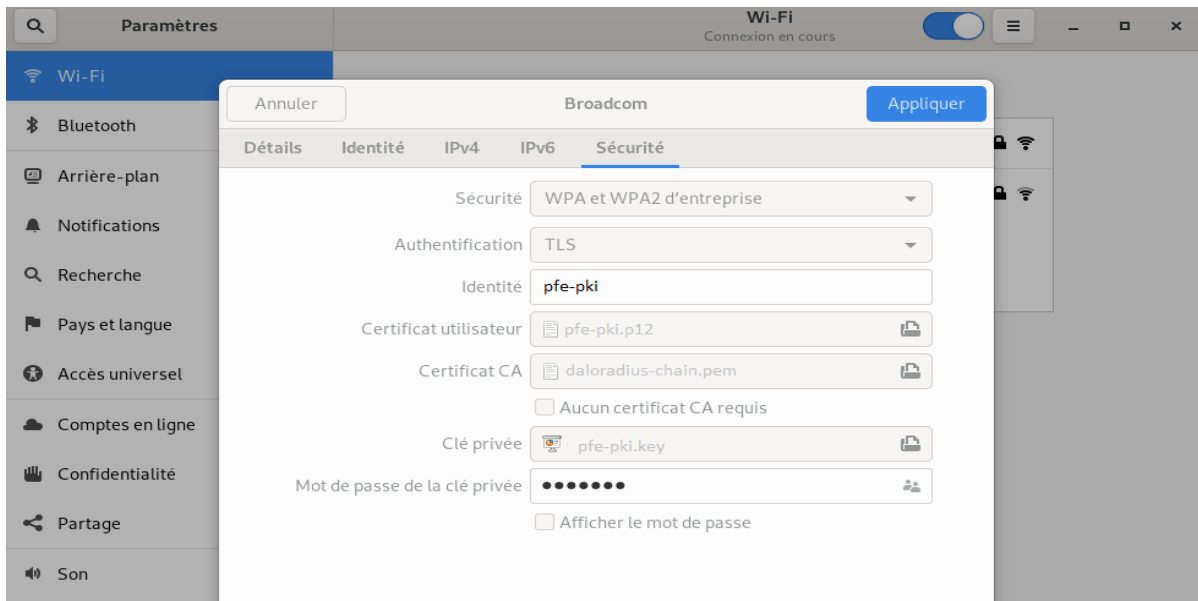


Figure 3.26 Configuration du client WIFI

3.5.3 Configuration du réseau du client Windows

Maintenant nous allons configurer notre nouvelle connexion au Wi-Fi sur Windows, dans centre de réseau et partage. Nous cherchons « configurer une nouvelle connexion ou un nouveau réseau » puis Nous cliquons sur « se connecter manuellement à un réseau sans fil » :

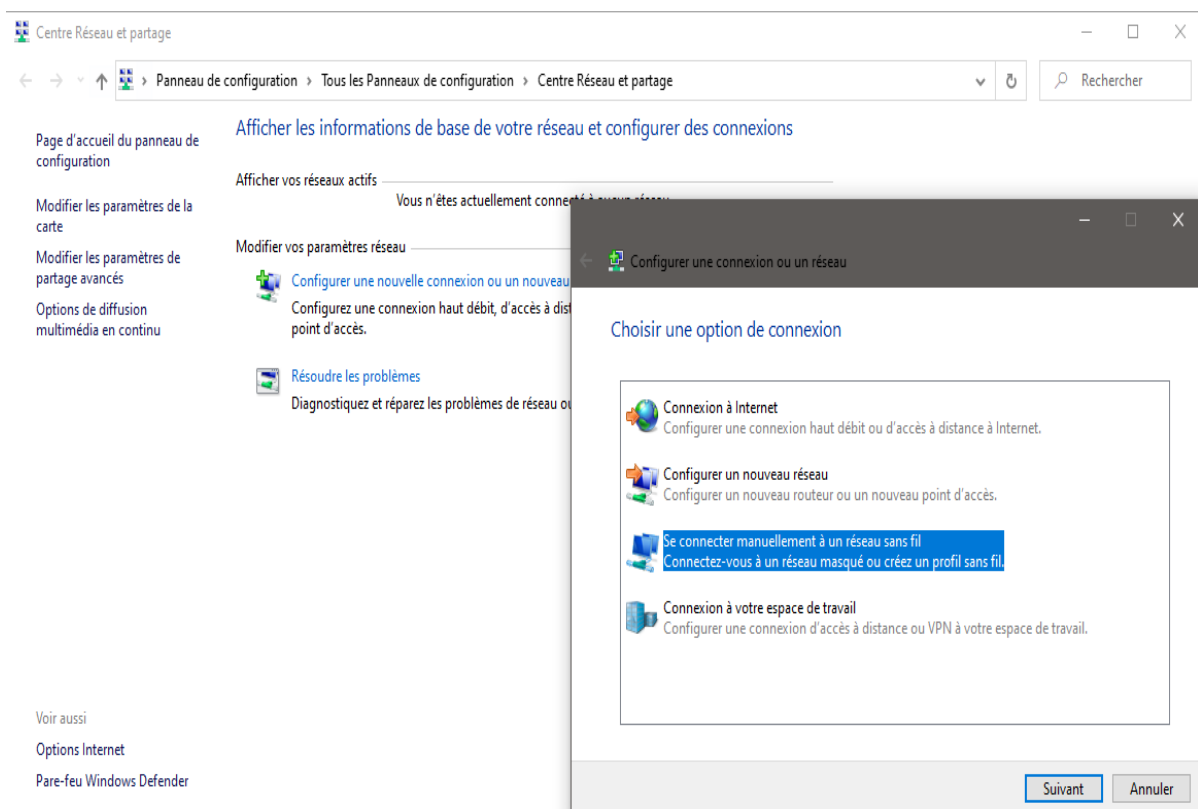


Figure 3.27 Ajout d'un nouveau réseau

- **Nom du réseau** (Broadcom).
- **Type de Sécurité** : WPA2 entreprise (le « entreprise » est primordiale).

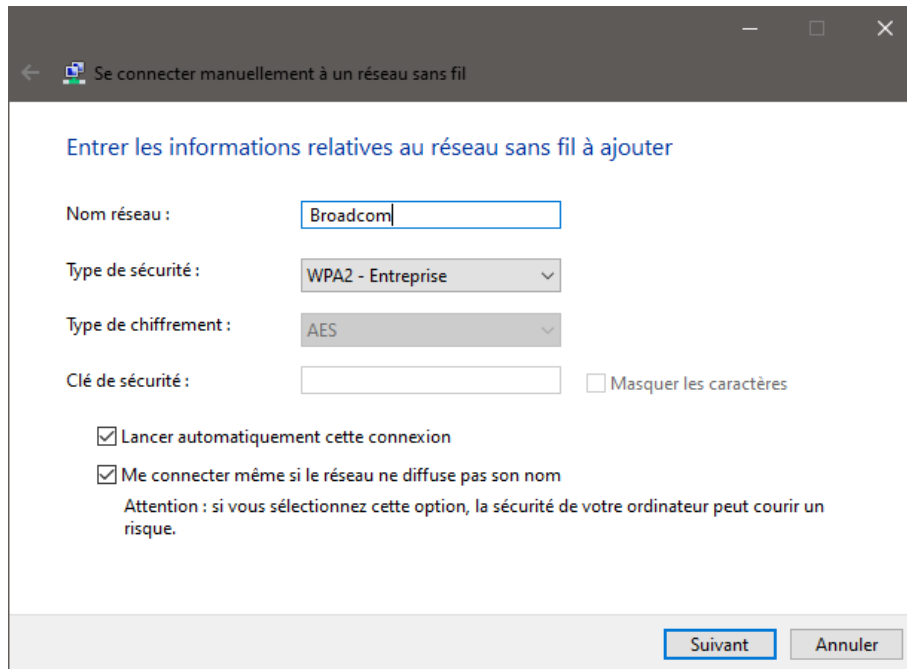


Figure 3.28 Configuration d'un nouveau réseau sur Windows

Puis Nous cliquons sur suivant et Modifier les paramètres de connexion.

Nous allons dans l'onglet sécurité, et Nous choisissons comme méthode d'authentification :

- Carte à puce ou autre certificat.

Maintenant il faut indiquer à l'ordinateur, quel certificat accepter pour identifier le serveur, donc Nous cliquons sur paramètre et Nous cochons « **daloradius.local** »

Note : il faut au préalable installer les certificats des CA ROOT et TLS et du serveur.

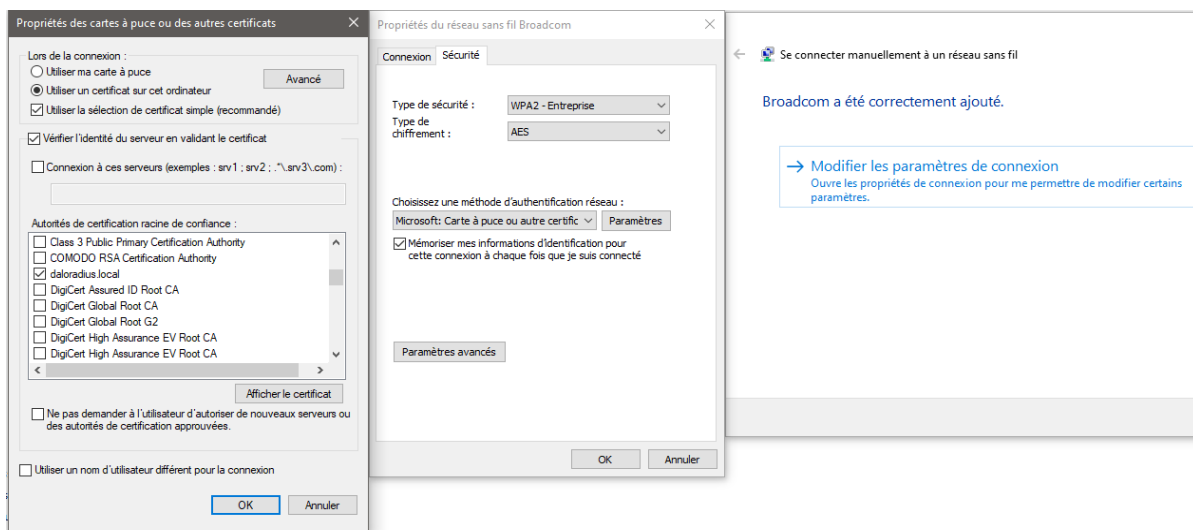
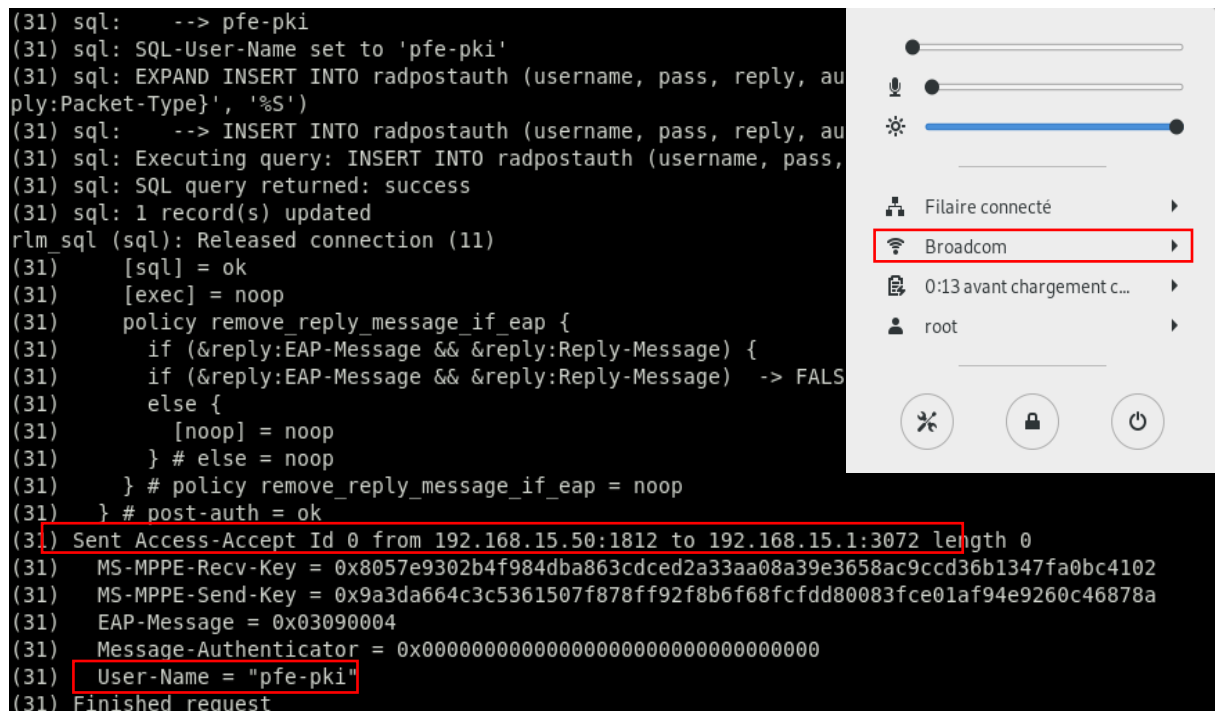


Figure 3.29 Configuration de la méthode d'authentification

3.6 Test d'authentification d'un utilisateur linux

Maintenant nous allons lancer notre serveur radius en debug mode (freeradius -X) pour voir si le serveur nous accorde l'accès ou pas.



The image shows a terminal window on the left and a network settings window on the right. The terminal window displays the following logs:

```
(31) sql: --> pfe-pki
(31) sql: SQL-User-Name set to 'pfe-pki'
(31) sql: EXPAND INSERT INTO radpostauth (username, pass, reply, au
ply:Packet-Type}', '%S')
(31) sql: --> INSERT INTO radpostauth (username, pass, reply, au
(31) sql: Executing query: INSERT INTO radpostauth (username, pass,
(31) sql: SQL query returned: success
(31) sql: 1 record(s) updated
rlm_sql (sql): Released connection (11)
(31) [sql] = ok
(31) [exec] = noop
(31) policy remove_reply_message_if_eap {
(31)   if (&reply:EAP-Message && &reply:Reply-Message) {
(31)     if (&reply:EAP-Message && &reply:Reply-Message) -> FALS
(31)   else {
(31)     [noop] = noop
(31)   } # else = noop
(31) } # policy remove_reply_message_if_eap = noop
(31) } # post-auth = ok
(31) Sent Access-Accept Id 0 from 192.168.15.50:1812 to 192.168.15.1:3072 length 0
(31) MS-MPPE-Recv-Key = 0x8057e9302b4f984dba863cdced2a33aa08a39e3658ac9ccd36b1347fa0bc4102
(31) MS-MPPE-Send-Key = 0x9a3da664c3c5361507f878ff92f8b6f68fcfd80083f9ce01af94e9260c46878a
(31) EAP-Message = 0x03090004
(31) Message-Authenticator = 0x00000000000000000000000000000000
(31) User-Name = "pfe-pki"
(31) Finished request
```

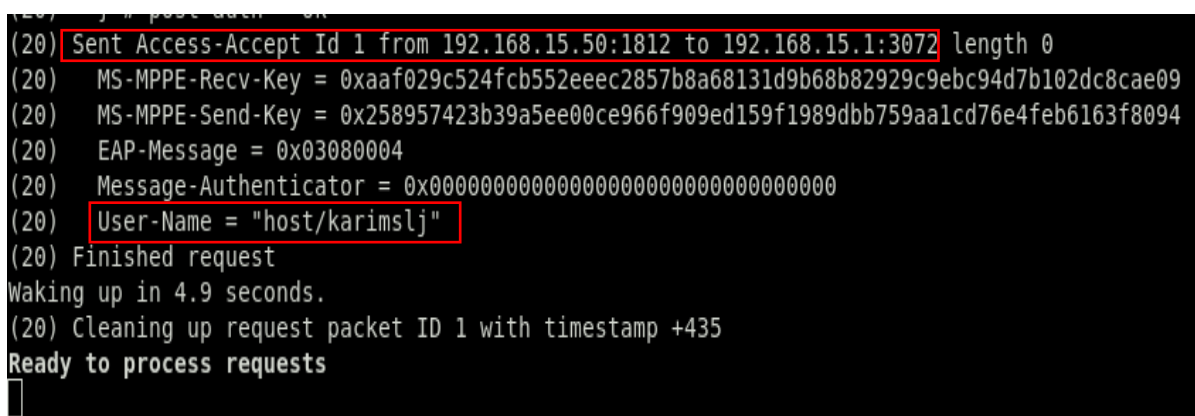
The network settings window on the right shows the following options:

- Filaire connecté
- Broadcom
- 0:13 avant chargement c...
- root

Figure 3.30 Réceptions et acceptation de la demande d'accès du client Linux

Ici Nous lisons Access-accepte, UserName : pfe-pki, donc nous sommes bien connectés au point d'accès.

3.7 Test d'authentification d'un utilisateur Windows



The image shows a terminal window displaying the following logs:

```
(20) Sent Access-Accept Id 1 from 192.168.15.50:1812 to 192.168.15.1:3072 length 0
(20) MS-MPPE-Recv-Key = 0xaaaf029c524fcb552ecec2857b8a68131d9b68b82929c9ebc94d7b102dc8cae09
(20) MS-MPPE-Send-Key = 0x258957423b39a5ee00ce966f909ed159f1989dbb759aa1cd76e4feb6163f8094
(20) EAP-Message = 0x03080004
(20) Message-Authenticator = 0x00000000000000000000000000000000
(20) User-Name = "host/karimslj"
(20) Finished request
Waking up in 4.9 seconds.
(20) Cleaning up request packet ID 1 with timestamp +435
Ready to process requests
```

Figure 3.31 Réceptions et acceptation de la demande d'accès du client Windows

Afficher les informations de base de votre réseau et configurer des connexions

Afficher vos réseaux actifs

Broadcom
Réseau public

Type d'accès : Pas d'accès Internet
Connexions : Wi-Fi (Broadcom)

Modifier vos paramètres réseau

Configurer une nouvelle connexion ou un nouveau réseau

Configurez une connexion haut débit, d'accès à distance ou VPN, ou configurez un routeur ou un point d'accès.

Réseau de confiance

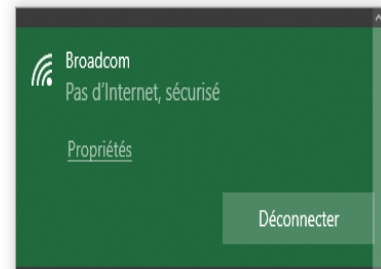


Figure 3.32 Connexion confirmé du client Windows

Nous sommes bel et bien connectés au point d'accès grâce à notre certificat.

3.8 Test d'authentification d'un utilisateur non autorisé

Ici un utilisateur nommé :

« **Mohammed** » essaie de se connecter à notre réseau Wi-Fi, avec un certificat signé par une autre CA « **algeria-pki.dz-inter-ca** », qui n'est donc pas la même que celle dont le serveur a confiance.

Ça implique que lorsque l'utilisateur va essayer de se connecter, il aura un refus de la part du serveur radius car son certificat n'est pas reconnu comme valide.

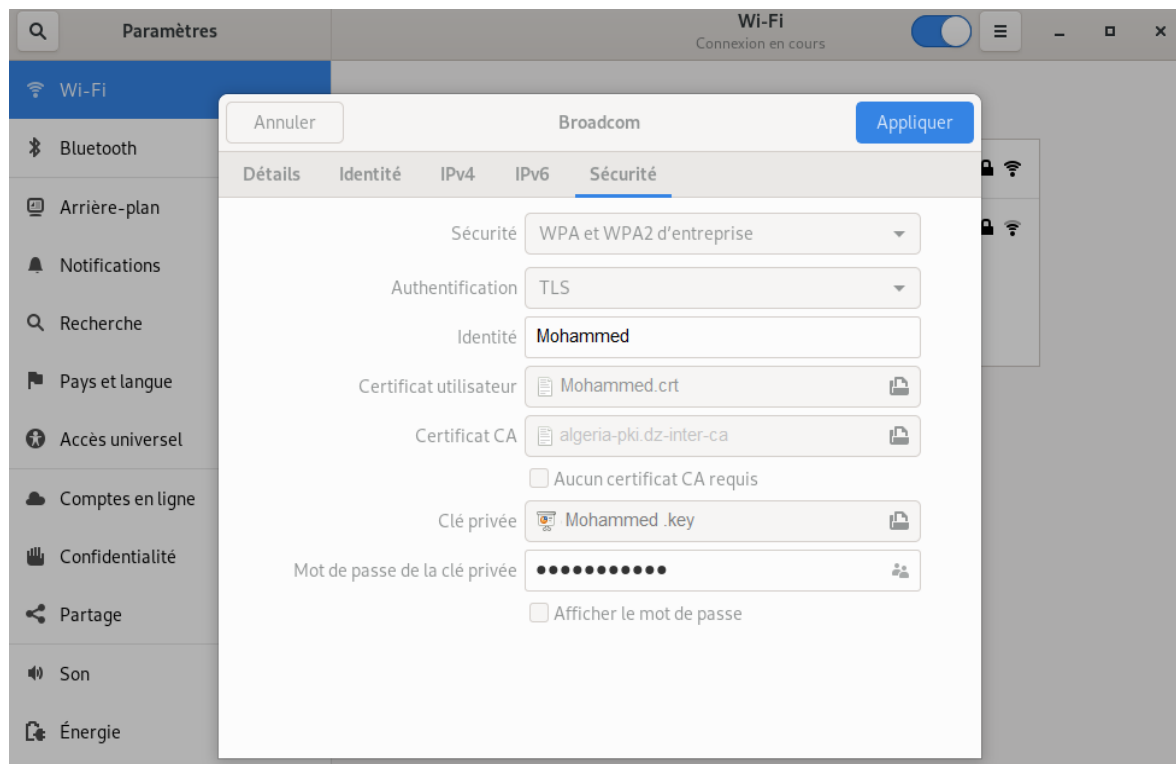


Figure 3.33 Configuration d'un client Wi-Fi non autorisé

```

(1) attr_filter.access_reject: EXPAND %{User-Name}
(1) attr_filter.access_reject: --> Mohammed
(1) attr_filter.access_reject: Matched entry DEFAULT at line 11
(1) [attr_filter.access_reject] = updated
(1) [eap] = noop
(1) policy remove_reply_message_if_eap {
(1)   if (&reply:EAP-Message && &reply:Reply-Message) {
(1)     if (&reply:EAP-Message && &reply:Reply-Message) -> FALSE
(1)   else {
(1)     [noop] = noop
(1)   } # else = noop
(1) } # policy remove_reply_message_if_eap = noop
(1) } # Post-Auth-Type REJECT = updated
(1) Delaying response for 1.000000 seconds
Waking up in 0.2 seconds.
Waking up in 0.7 seconds.
(1) Sending delayed response
(1) Sent Access-Reject Id 0 from 192.168.15.50:1812 to 192.168.15.1:3072 length 44
(1) EAP-Message = 0x04010004
(1) Message-Authenticator = 0x00000000000000000000000000000000
Waking up in 3.9 seconds.
(1) Cleaning up request packet ID 0 with timestamp +50
Ready to process requests

```

Figure 3.34 Accès refusé à l'utilisateur

Ici Nous lisons Access-reject, l'utilisateur Mohammed a été rejeté et n'a donc pas accès au wifi car son certificat n'a pas été reconnu par le serveur comme étant valide, le filtrage a été fait correctement.

3.8.1 Révoquer un utilisateur

Voyons comment révoquer un certificat d'un utilisateur :

```

openssl ca \
-config /ca/tls-ca/tls-ca.cnf \
-revoke /ca/tls-ca/certs/redmi.crt \
-crl_reason unspecified

```

NOTE : Si un utilisateur utilise un certificat qui n'a pas été attribué par la PKI ALGERIA TLS CA, il sera automatiquement rejeté de même si l'utilisateur se fait révoqué. Son certificat est supprimé de la base de données des utilisateurs.

C'est bien pour cela que la PKI est utilisé pour délivrer des certificats, uniquement sur un réseau local d'entreprise, et non sur internet (pour éviter de se retrouver avec des usurpations d'identité).

4. Mise en place d'un serveur Mail sécurisé

4.1 Installation et configuration d'un serveur Mail

```
apt update
apt upgrade
```

En premier lieu, Nous nous connectons avec un compte avec des privilèges root ou directement avec l'utilisateur root et nous nous assurons que notre système Debian est à jour.

```
apt install curl net-tools bash-completion wget lsof nano
```

Ensuite, Nous installons les packages logiciels qui seront utilisés pour l'administration du système.

```
nano /etc/host.conf
```

Ensuite, Nous ouvrons le fichier host.conf pour le modifier en ajoutant la ligne suivante au début du fichier afin que la résolution DNS lise d'abord le fichier hosts :

```
order hosts,bind
multi on
hostnamectl set-hostname mail.algeria-pki.dz
echo "192.168.15.50  algeria-pki.dz  mail.algeria-pki.dz  " >>
/etc/hosts
init 6
```

Après cela, Nous configurons le nom de domaine complet FQDN de notre machine dans le fichier hosts. Nous utilisons l'adresse IP du système (192.168.15.50) pour résoudre le nom du domaine et le nom de domaine complet (mail.algeria-pki.dz).

Et Nous redémarrons la machine afin d'appliquer correctement le nom d'hôte (init 6).

```
hostname
hostname -s
hostname -f
hostname -A
hostname -i
cat /etc/hostname
```

Après le redémarrage, Nous vérifions si le nom d'hôte a été correctement configuré en émettant la série de commandes suivante. Le nom de domaine, le FQDN, le nom d'hôte et l'adresse IP du système doivent être renvoyés par la commande hostname.

```

root@mail:~# hostname
mail.algeria-pki.dz
root@mail:~# hostname -s
mail
root@mail:~#
root@mail:~# hostname -f
algeria-pki.dz
root@mail:~#
root@mail:~# hostname -A
ns1.algeria-pki.dz
root@mail:~#
root@mail:~# hostname -i
192.168.15.50
root@mail:~#
root@mail:~# cat /etc/hostname
mail.algeria-pki.dz

```

Figure 3.35 Vérification de la bonne configuration du FQDN

```

getent ahosts mail.algeria-pki.dz
ping algeria-pki.dz
ping mail.algeria-pki.dz

```

Nous testons si le domaine répond correctement aux requêtes locales en lançant des Ping.

```
apt install postfix
```

Le logiciel le plus important requis pour qu'un serveur de messagerie fonctionne correctement est l'agent MTA. Le MTA est un logiciel construit dans une architecture serveur-client, qui est responsable du transfert de courrier entre les serveurs de messagerie. Nous utiliserons Postfix comme agent de transfert de courrier.

Nous Avons eu à répondre à 2 questions lors de l'installation notamment :

```

Postfix Configuration
-----
Veuillez choisir la configuration type de votre serveur de
messagerie la plus adaptée à vos besoins.

Pas de configuration :
  Devrait être choisi pour laisser la configuration actuelle
inchangée.
Site Internet :
  L'envoi et la réception s'effectuent directement en SMTP.
Site Internet avec un smarthost :
  Les messages sont reçus directement en SMTP ou grâce à un
utilitaire comme fechtmail. Les messages sortants sont envoyés en
utilisant un smarthost.
Système satellite :
  Tous les messages sont envoyés vers une autre machine, nommée un
smarthost.
Local uniquement :
  Le seul courrier géré est le courrier pour les utilisateurs
locaux. Il n'y a pas de mise en réseau.

Configuration type du serveur de messagerie :

  Pas de configuration
  Site Internet
  Internet avec un « smarthost »
  Système satellite
  Local uniquement

<Ok>                               <Annuler>

```

Figure 3.36 Installation de Postfix 1/2

Configuration du type de serveur de messagerie, ici vu que c'est un site web Nous choisissons site internet.

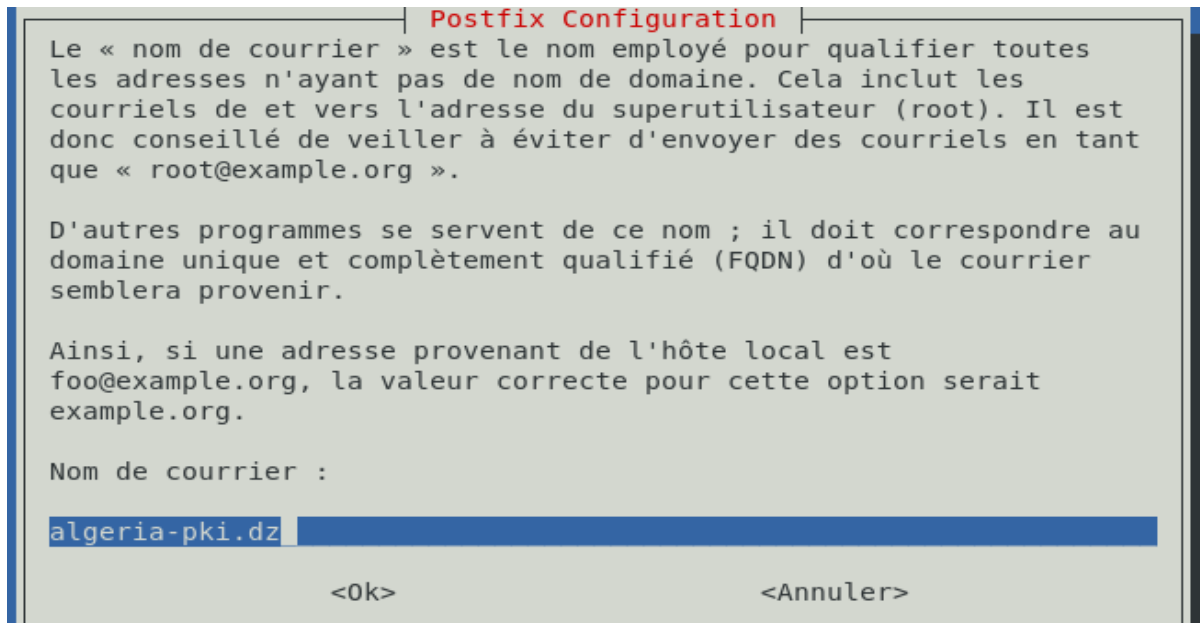


Figure 3.37 Installation de Postfix 2/2

Nom de courrier : ici nous donnons le FQDN donc algeria-pki.dz (sans le mail.)

```
cp /etc/postfix/main.cf{,.backup}
nano /etc/postfix/main.cf
```

Ensuite, Nous sauvegardons le fichier de configuration principal de Postfix et Nous configurons Postfix pour notre domaine en utilisant les commandes suivantes :

Nous attribuons au variable suivante les valeurs qui leur sont correspondantes :

- Myhostname **mail.algeria-pki.dz**
- mydomain **algeria-pki.dz**
- mynetworks **192.168.15.0/24** pour correspondre à notre réseau local.

```
systemctl restart postfix
systemctl status postfix
netstat -tln
```

Une fois toutes les configurations en place, Nous redémarrons le daemon Postfix pour appliquer les modifications et puis Nous vérifions si le service est en cours d'exécution en inspectant si le service maître Postfix se lie au port 25 en exécutant la commande netstat.

4.2 Test du serveur mail Postfix

```
apt install mailutils
```

Afin de tester si postfix peut gérer le transfert de courrier, Nous installons d'abord le paquet mailutils.

```
echo "mail body" | mail -s "test mail" root
mailq
mail
ls Maildir/
ls Maildir/new/
cat Maildir/new/
```

Ensuite, à l'aide de l'utilitaire de ligne de commande de messagerie, nous envoyons un e-mail teste au compte localhost et nous vérifions si le courrier a été transmis avec succès, en émettant les commandes précédentes afin de vérifier la file d'attente de messagerie et de répertorier le contenu du répertoire Maildir de la racine.

```
Mail queue is empty
root@mail:~#
root@mail:~# mail
"/var/mail/root": 2 messages 2 nouveaux
>N  1 root          sam. mars  7 23:  13/469  test mail
  N  2 root          sam. mars  7 23:  13/469  test mail
?
Return-Path: <root@mail.algeria-pki.dz>
X-Original-To: root@mail.algeria-pki.dz
Delivered-To: root@mail.algeria-pki.dz
Received: by mail.algeria-pki.dz (Postfix, from userid 0)
        id 9E03A245AA; Sat,  7 Mar 2020 23:39:00 +0100 (CET)
Subject: test mail
To: <root@mail.algeria-pki.dz>
X-Mailer: mail (GNU Mailutils 3.5)
Message-Id: <20200307223900.9E03A245AA@mail.algeria-pki.dz>
Date: Sat,  7 Mar 2020 23:39:00 +0100 (CET)
From: root <root@mail.algeria-pki.dz>

mail body
? ls Maildir/
Commande inconnue : ls
?
Return-Path: <root@mail.algeria-pki.dz>
X-Original-To: root@mail.algeria-pki.dz
Delivered-To: root@mail.algeria-pki.dz
Received: by mail.algeria-pki.dz (Postfix, from userid 0)
        id 0A33D245AA; Sat,  7 Mar 2020 23:42:06 +0100 (CET)
Subject: test mail
To: <root@mail.algeria-pki.dz>
X-Mailer: mail (GNU Mailutils 3.5)
Message-Id: <20200307224207.0A33D245AA@mail.algeria-pki.dz>
Date: Sat,  7 Mar 2020 23:42:07 +0100 (CET)
From: root <root@mail.algeria-pki.dz>
```

Figure 3.38 Test d'envoi de courrier

Nous avons donc bien un message qui a transité par le serveur Postfix.

4.3 Installation et configuration de Dovecot IMAP

L'agent de distribution de courrier que nous utiliserons pour remettre des messages électroniques d'un destinataire local à un autre est Dovecot IMAP. IMAP est un protocole qui s'exécute sur les ports 143 et 993 (SSL), qui est responsable de la lecture, de la suppression ou du déplacement des courriers électroniques sur plusieurs clients de messagerie.

Le protocole IMAP utilise également la synchronisation afin de garantir qu'une copie de chaque message est enregistrée sur le serveur et permet aux utilisateurs de créer plusieurs répertoires sur le serveur et de déplacer des e-mails vers ces répertoires afin de trier les e-mails.

```
apt install dovecot-core dovecot-imap
```

Pour installer le serveur principal Dovecot et le paquet Dovecot IMAP sur Debian.

```
nano /etc/dovecot/dovecot.conf
```

Une fois Dovecot installé, Nous ouvrons les fichiers dovecot.conf pour le modifier et apportez les modifications suivantes :

```
#listen = *, ::      listen = *, ::
```

Nous enlevons le « # » pour permettre à dovecot d'écouter sur toute les IP.

```
nano /etc/dovecot/conf.d/10-auth.conf
```

Ensuite, nous éditons les lignes ci-dessous :

```
disable_plaintext_auth = no
auth_mechanisms = plain login
```

Respectivement autoriser pour activer l'authentification par mot de passe, et spécifier le format du mot de passe.

```
nano /etc/dovecot/conf.d/10-master.conf
```

Le dernier fichier à modifier est 10-master.conf.

Ici, Nous cherchons le bloc Postfix smtp-auth et apportez la modification suivante :

```
# Postfix smtp-auth
unix_listener /var/spool/postfix/private/auth {
  mode = 0666
  user = postfix
  group = postfix
}
```

```
systemctl restart dovecot.service
systemctl status dovecot.service
```

Nous relançons le service dovecot pour appliquer les modifications.

```
adduser karim
nc localhost 25
ehlo localhost
mail from: root
rcpt to: karim
data
subject: test
Mail body
.
quit
```

Nous testons si le serveur de messagerie fonctionne correctement en ajoutant un nouveau compte d'utilisateur au système et Nous essayons de nous connecter au serveur SMTP et d'envoyer un nouveau courrier au nouvel utilisateur ajouté.

```
nc localhost 143
x1 LOGIN redadidi votremotdepasse
x2 LIST "" "*"
x3 SELECT Inbox
x4 LOGOUT
```

Nous nous connectons à la boîte aux lettres de l'utilisateur à partir de la ligne de commande via le protocole IMAP. Le nouveau courrier doit être répertorié dans la boîte de réception de l'utilisateur.

4.4 Installation et configuration de RainLoop

Nous avons aussi installé une interface graphique pour que les utilisateurs gèrent leurs e-mails via le client Rainloop Webmail. Rainloop a besoin d'apache et de PHP or nous l'avons déjà configuré avant.

```
cd /var/www/algeria/
curl -sL https://repository.rainloop.net/installer.php | php
```

Nous allons dans le dossier de notre site web et nous copions le dossier de Rainloop Webmail depuis leur site.

Une fois le client Rainloop Webmail installé sur le système, Nous pouvons accéder à l'adresse : <https://www.algeria-pki.dz/webmail/?admin> et se connecter à l'interface Web d'administration Rainloop avec les informations d'identification par défaut suivantes :

Nom d'utilisateur et mot de passe respectivement :

admin/12345

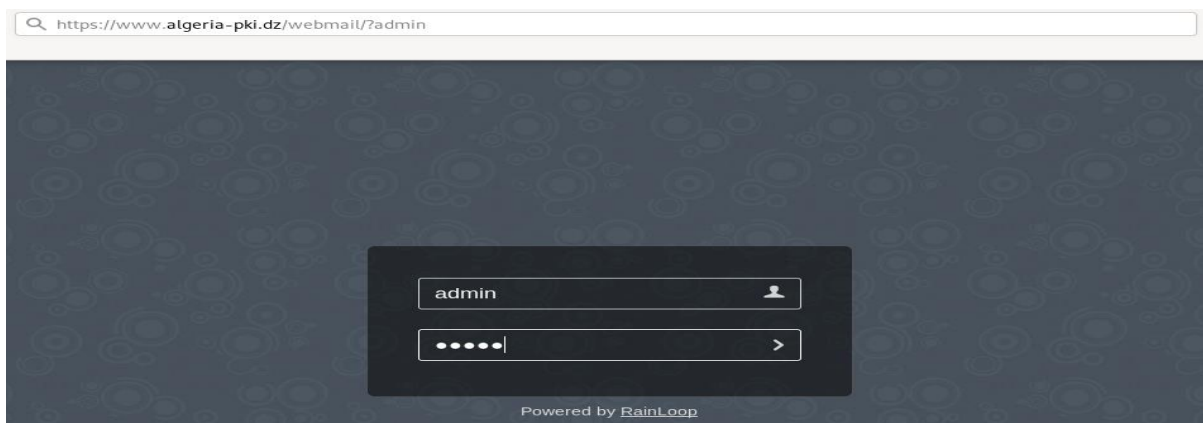


Figure 3.39 Accès au panneau d'administration du serveur mail

NOTE : le « ?admin » dans l'URL est très important sinon nous ne pourrions pas nous connecter à la plateforme d'administration.

Nous accédons au menu Domaines, appuyer sur le bouton Ajouter un domaine et indiquer le nom de domaine et le type de chiffrement utilisé dans notre cas SSL/TLS pour IMAP et STARTTLS pour SMTP.

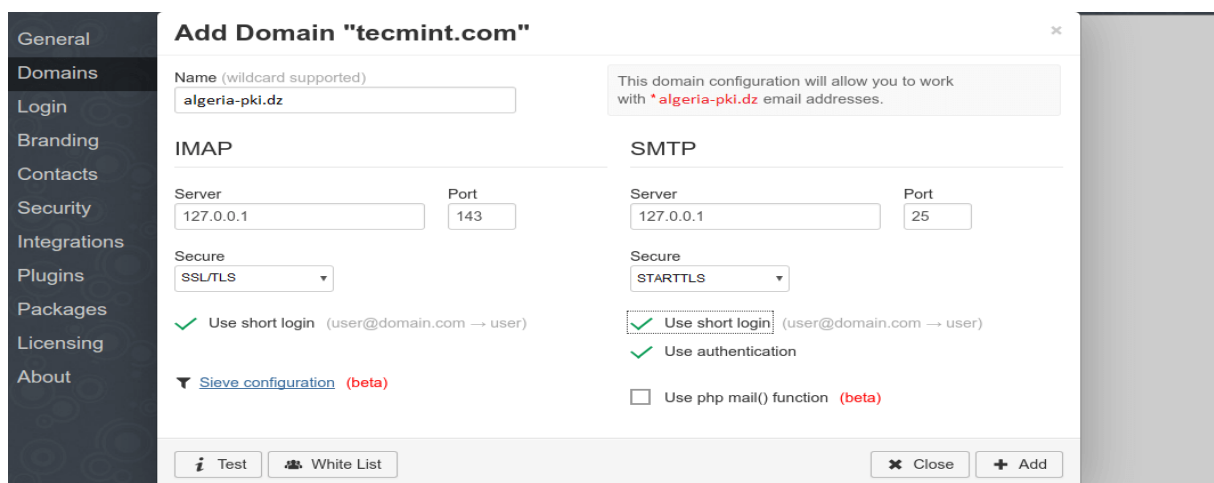


Figure 3.40 Configuration de notre domaine d'email

Une fois terminé Nous cliquons sur ajouter, Nous nous déconnectons de l'interface d'administration Rainloop.

Pour ajouter un nouvel utilisateur il suffit de taper :

```
echo 'export MAIL=$HOME/Maildir' >> /etc/profile
useradd -m webmaster
passwd webmaster
```

(Webmaster = nom d'utilisateur)

En cas de problème d'envoi de message il faut tout simplement désactiver l'authentification sur SMTP

4.5 Test du serveur mail RainLoop

Pour se connecter à notre boîte mail il faut entrer dans un navigateur l'adresse :

<https://algeria-pki.dz/webmail> et se connecter avec les identifiants du client de messagerie Web créé précédemment.

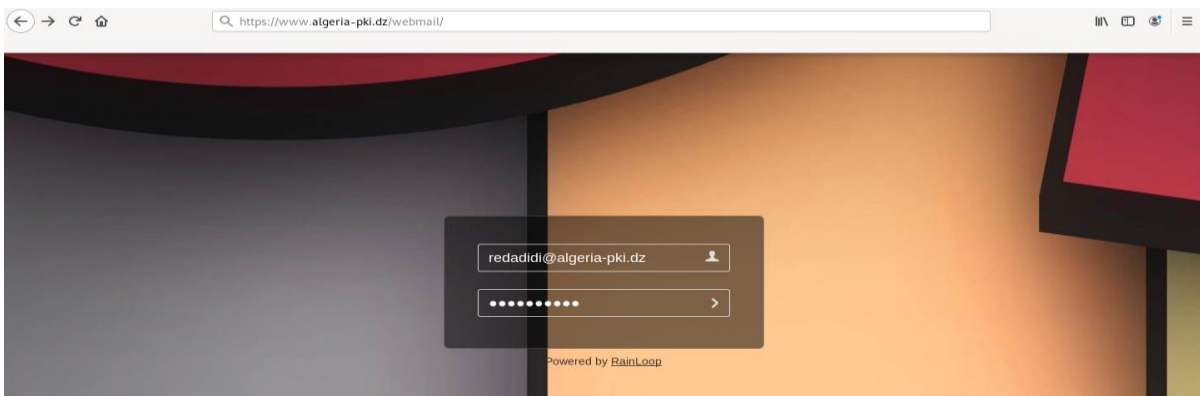


Figure 3.41 Accès à notre boîte email

Après s'être connecté avec succès à la messagerie Web Rainloop, nous voyons l'e-mail envoyé précédemment depuis la ligne de commande dans notre dossier Boîte de réception.

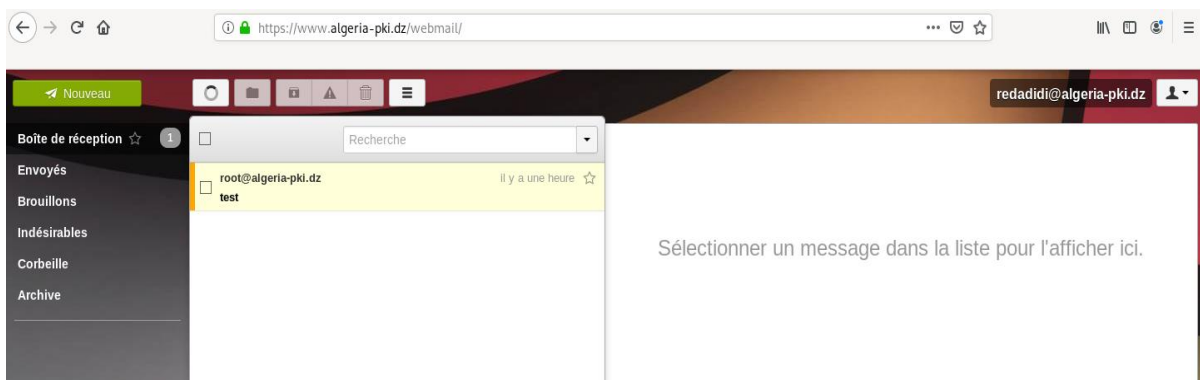


Figure 3.42 Page principale du serveur mail

Nous nous connectons maintenant à la boîte créée précédemment.

Le webmaster (**webmaster@algeria-pki.dz**) va envoyer un email à l'utilisateur

redadidi@algeria-pki.dz :

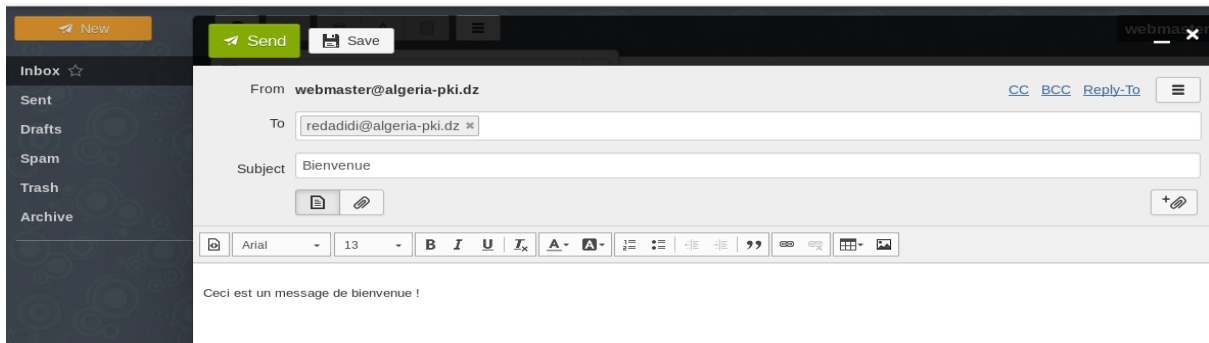


Figure 3.43 Envoie d'email de la part du Webmaster vers un utilisateur

Nous vérifions que l'email a bien été envoyé et reçu.

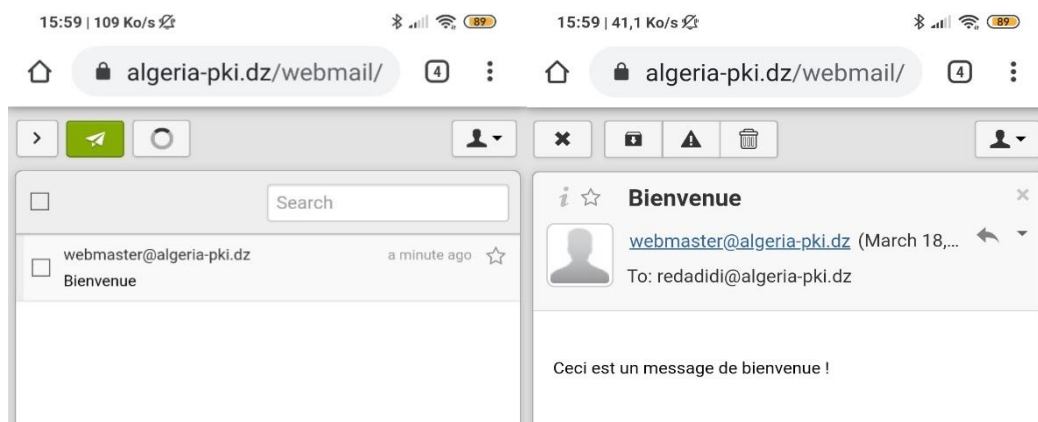


Figure 3.44 Réception de l'email du Webmaster par l'utilisateur

IV. Conclusion

Notre objectif principal était de déployer une PKI sous Linux version Debian, et l'utiliser pour contrôler l'accès à un réseau Wifi, puis pour accéder à un serveur Web sous le protocole HTTPS, pour finir l'accès à un serveur web mail a été testé en mode sécurisé. Particulièrement via l'utilisation de certificats, qui s'avèrent être une méthode beaucoup plus sûre que celle des mots de passe. Pour se faire, nous avons dû installer d'autres serveurs et outils intermédiaires, comme le DNS, PHP, une base de données, des logiciels interface graphique pour Radius, le serveur mail et Apache.

Tous les tests ont été concluants et nous voyons bien que le contrôle d'accès est réussi. Quelques problèmes techniques nous on bloqués quelques temps, mais nous les avons résolus et avons fait des notes, pour éviter aux futurs étudiants de tels pièges.

Chapitre 4

Chapitre 4 : Implémentation d'une infrastructure d'entreprise sous Windows

I. Introduction

Dans ce chapitre, le même travail précédemment fait a été repris sous Windows, mais nous avons eu moins de problèmes, suite à l'interface graphique du serveur Windows, qui intègre tous les serveurs web, mail, DNS, base de données, AC, LDAP, Active Directory (Annuaire)et Radius au même endroit et interopérable automatiquement, avec plein d'options possibles, comme nous allons le voir ci-dessous.

II. Implémentations d'une infrastructure à clé publique

PKI

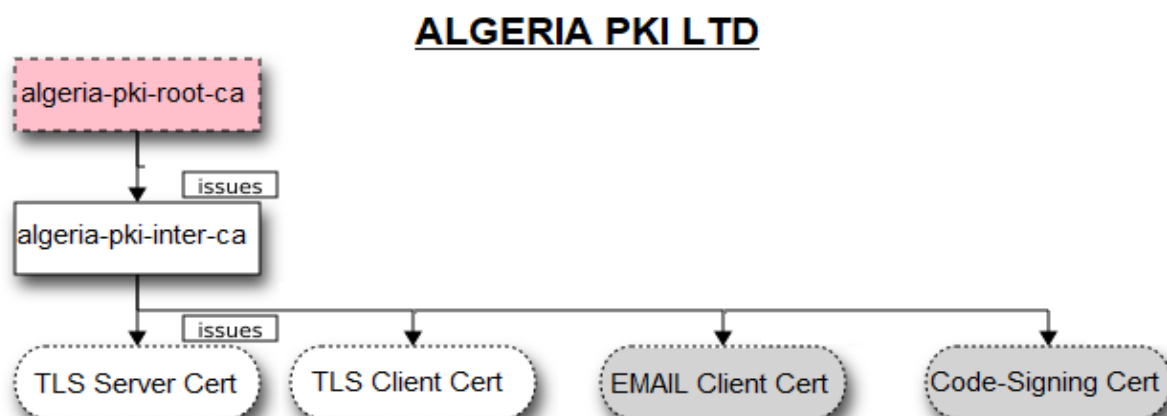


Figure 4.1 Schéma de la PKI

Pour implémenter une infrastructure à clé publique, nous créons d'abord la CA racine **ALGERIA-PKI-ROOT-CA**.

Nous utilisons ensuite l'autorité de certification racine pour signer le certificat de l'autorité de certification signataire qui se nommera : **ALGERIA-PKI-INTER-CA**.

Nous aurons l'occasion de montrer cette dernière en fonctionnement, émettant des certificats d'utilisateur que ce soit pour les identifier ou à des fins de protection.

1. Création d'un domaine

1.1 Installation du domaine

Avant d'installer PKI nous aurons besoin d'installer le rôle Service de Domaine Active Directory ou « AD DS », Ce rôle sert à organiser de façon hiérarchique les éléments d'un réseau tels que les utilisateurs, les ordinateurs et autres périphériques. Le serveur qui va exécuter l'AD DS se nomme : contrôleur de domaine.

De plus, l'AD DS est sécurisé grâce à l'authentification d'ouverture de session et le contrôle d'accès aux ressources de l'annuaire et facilite le partage de la liste CRL ainsi que la distribution des certificats, pour éviter de le faire manuellement.

NOTE : Nous nommerons « **server0** » le serveur qui abritera la CA racine et qui sera relié au domaine, et « **server** » le serveur qui aura le rôle de contrôleur de domaine et qui hébergera la CA.

Donc pour commencer, nous allons tout d'abord ajouté un nouveau rôle sur le serveur « **server** », qui sera donc un le contrôleur du Domaine.

Pour cela, dans le gestionnaire du serveur Nous cliquons sur "Gérer" "Ajouter des rôles et des fonctionnalités"



Figure 4.2 Gestionnaire de serveur

Nous sélectionnons "Installation basée sur un rôle ou une fonctionnalité".



Figure 4.3 Ajout de nouveau rôle ou fonctionnalité

Nous sélectionnons le serveur de destination.

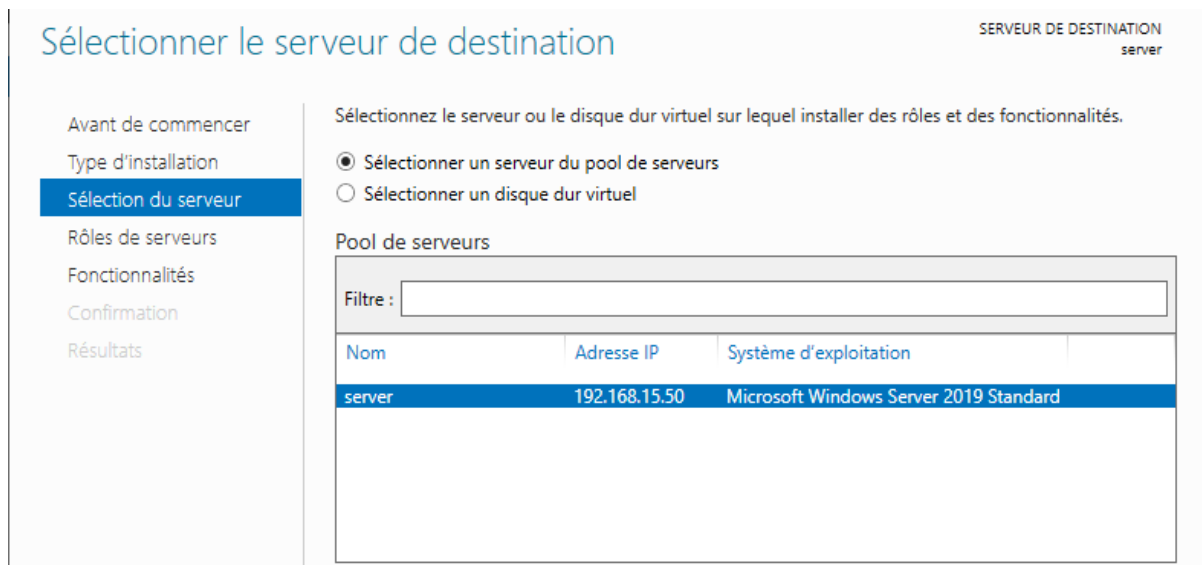


Figure 4.4 Serveur destinataire du nouveau rôle

Nous sélectionnons AD DS comme rôle

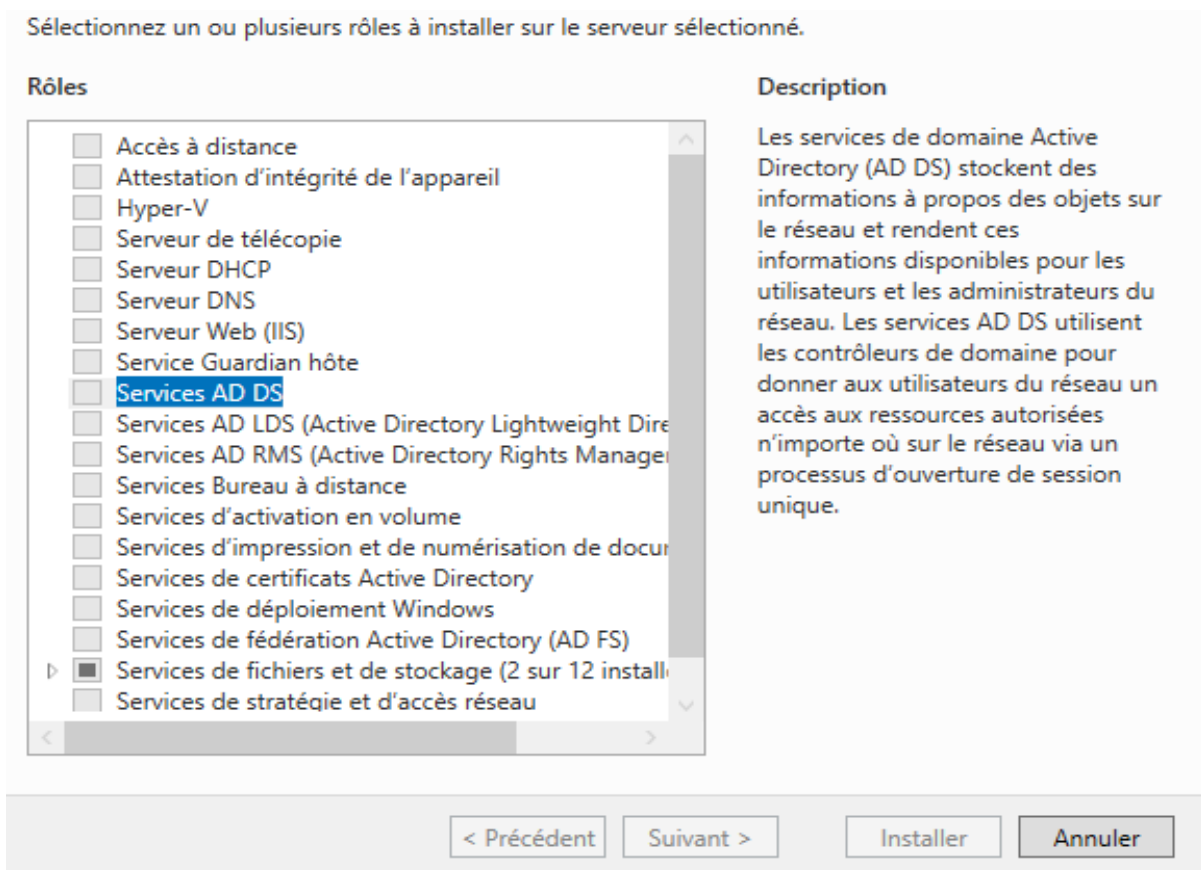


Figure 4.5 Ajout de rôle AD-DS

Nous suivons les étapes jusqu'à l'installation.

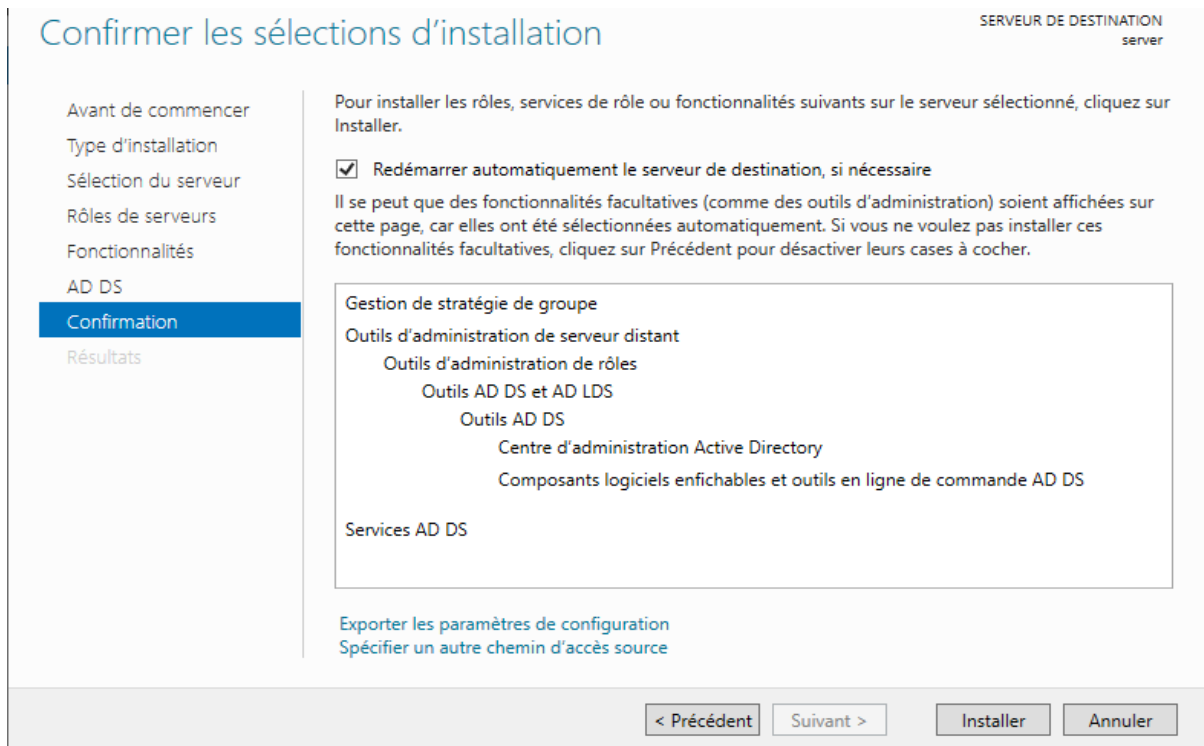


Figure 4.6 Installation d'AD-DS

Une fois terminé Nous devons promouvoir le serveur comme contrôleur de domaine pour cela Nous cliquons sur « promouvoir ce serveur en contrôleur de domaine »

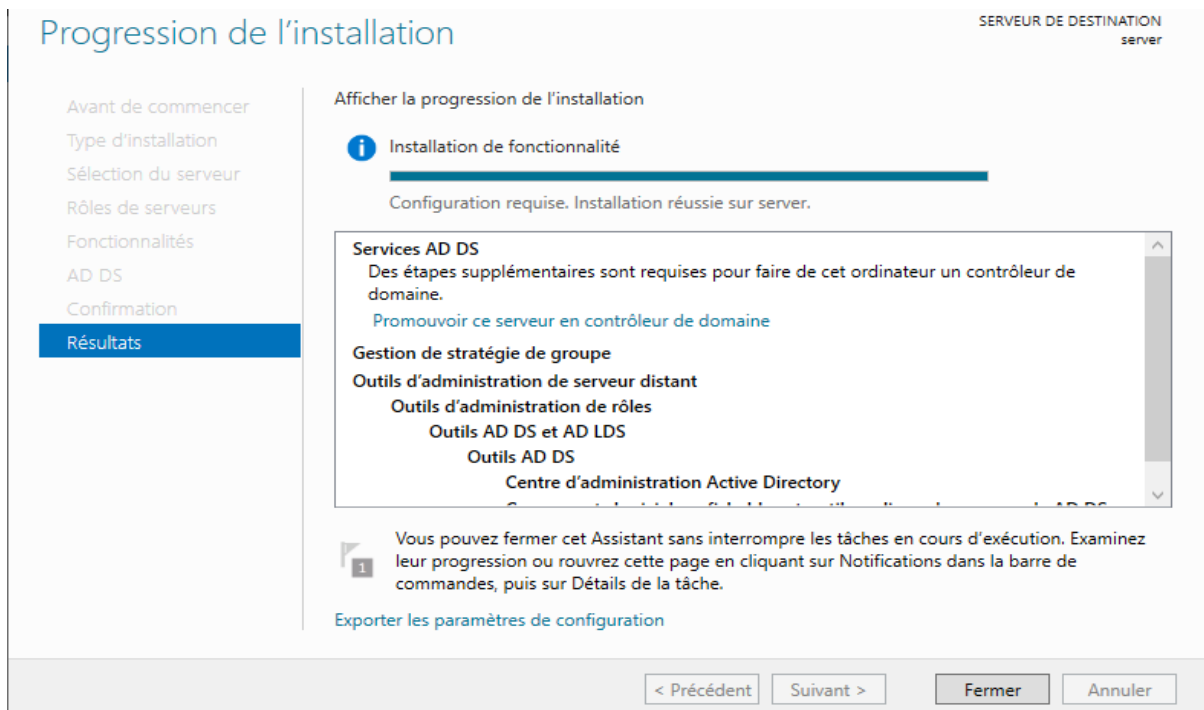


Figure 4.7 Finalisation de l'installation d'AD-DS

1.2 Configuration du domaine

Nous devons choisir un nom pour notre domaine qui sera dans notre cas « algeria-pki.dz »

Configuration de déploiement

SERVEUR CIBLE
server

Configuration de déploie...

Options du contrôleur de...

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la configur...

Installation

Résultats

Sélectionner l'opération de déploiement

Ajouter un contrôleur de domaine à un domaine existant

Ajouter un nouveau domaine à une forêt existante

Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Nom de domaine racine :

[En savoir plus sur les configurations de déploiement](#)

< Précédent Suivant > Installer Annuler

Figure 4.8 Configuration d'AD-DS 1/2

Un mot de passe devra être attribué dans le cas où le serveur devra être rétrogradé.

Options du contrôleur de domaine

SERVEUR CIBLE
server

Configuration de déploie...

Options du contrôleur de...

Options DNS

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la configur...

Installation

Résultats

Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine

Niveau fonctionnel de la forêt :

Niveau fonctionnel du domaine :

Spécifier les fonctionnalités de contrôleur de domaine

Serveur DNS (Domain Name System)

Catalogue global (GC)

Contrôleur de domaine en lecture seule (RODC)

Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

Mot de passe :

Confirmer le mot de passe :

[En savoir plus sur les options pour le contrôleur de domaine](#)

< Précédent Suivant > Installer Annuler

Figure 4.9 Configuration d'AD-DS 2/2

Il ne reste plus qu'à suivre les étapes en laissant tout par défaut.

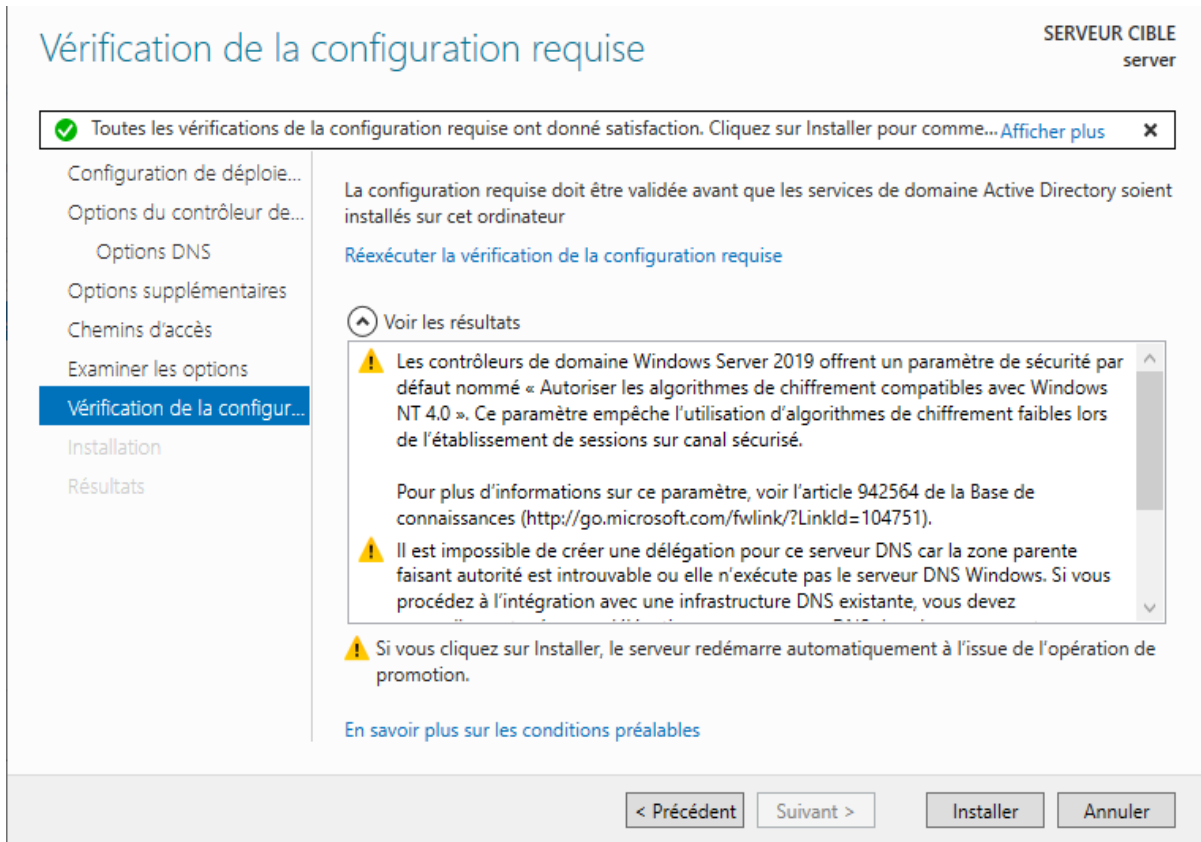


Figure 4.10 Finalisation de la configuration d'AD-DS

NOTE : des avertissements seront affichés avant l'installation mais tout cela est normal.

Après l'installation l'ordinateur devrait normalement redémarrer pour appliquer le changement de domaine, et pour vérifier cela nous allons dans les paramètres système et vérifier le domaine.

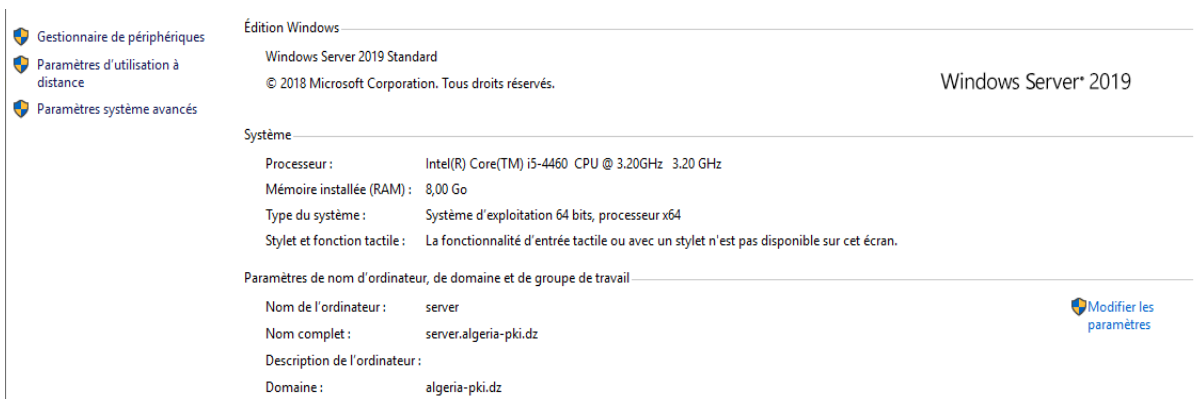


Figure 4.11 Vérification du bon fonctionnement du domaine

1.3 Configuration du pare-feu du contrôleur de domaine

Nous aurons aussi besoins d'ajouter des exceptions au pare-feu, pour permettre au flux d'information de circuler entre les différentes machines, donc dans « règles de trafic entrants » et « règles de trafic sortant » Nous sélectionnons « nouvelle règle ». Sur la fenêtre qui s'affiche Nous cliquons sur la case « personnalisée » puis sur « suivant ».

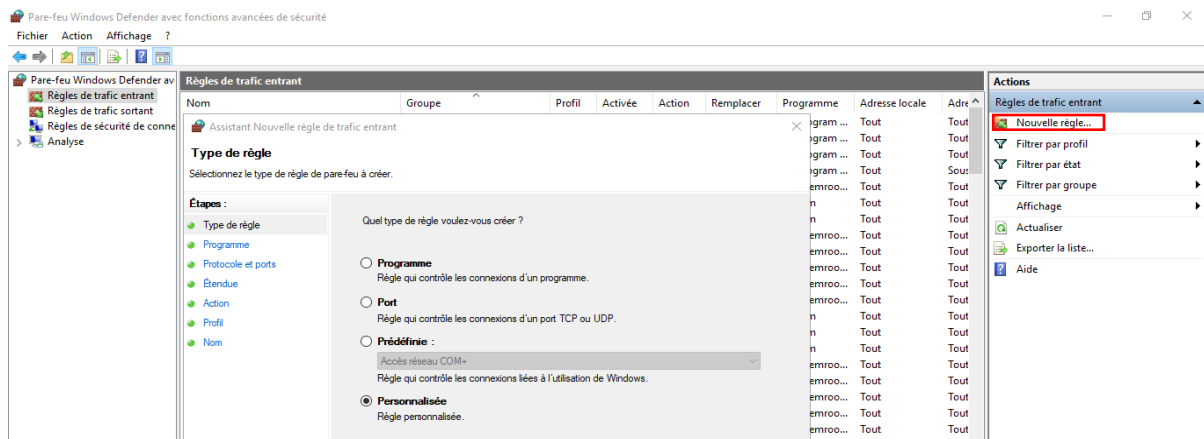


Figure 4.12 Ajout d'exception au pare-feu 1/3

Nous sélectionnons ensuite « Tous les programmes » et nous laissons les autres paramètres par défaut, Puis nous autorisons la connexion pour toutes ces dernières.

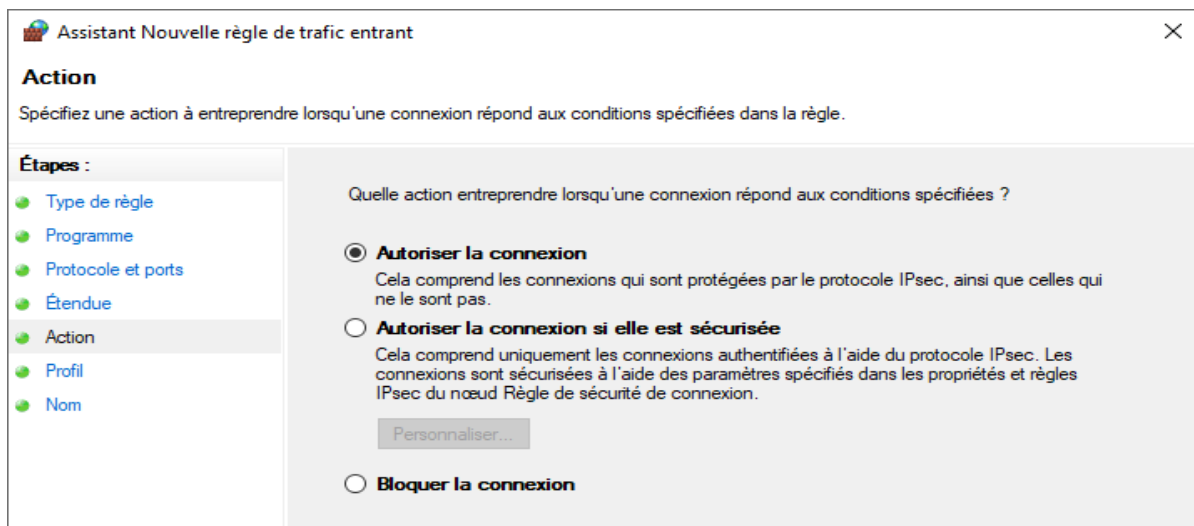


Figure 4.13 Ajout d'exception au pare-feu 2/3

Enfin Nous choisissons un nom à notre règle et Nous cliquons sur terminer.

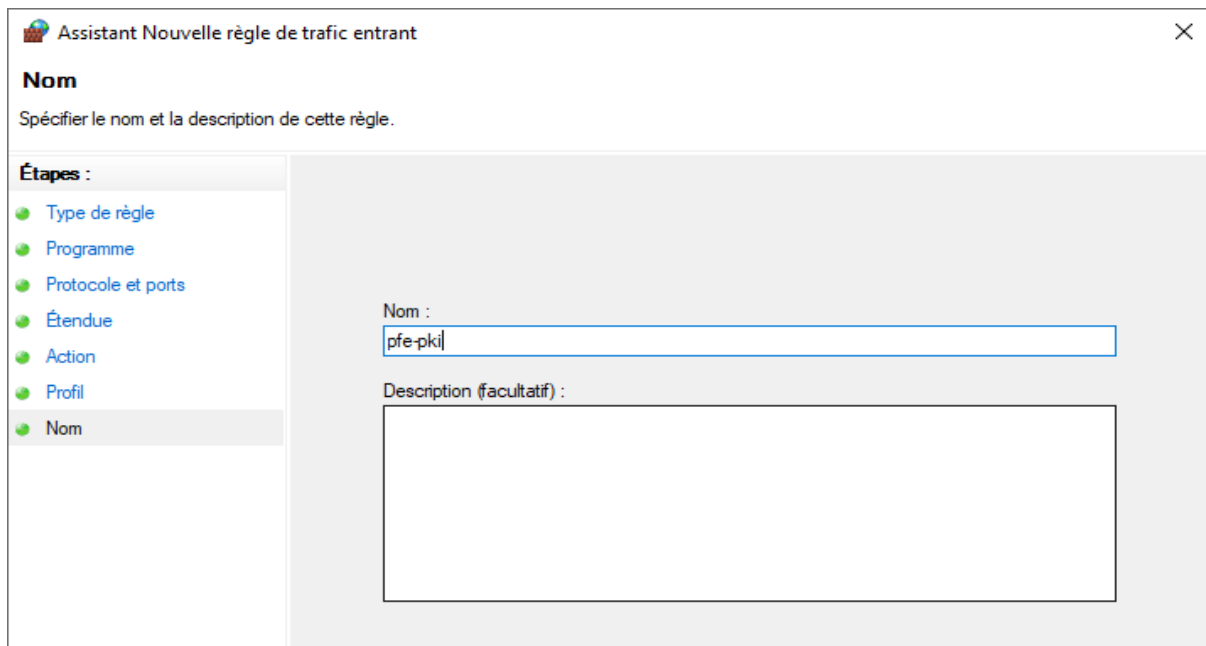


Figure 4.14 Ajout d'exception au pare-feu 3/3

1.4 Connexion du deuxième serveur au domaine

Maintenant que le serveur qui va abriter la CA intermédiaire est connecté à un domaine, il faut en faire de même pour celui qui abritera la CA racine.

Il nous faut garder en permanence un lien filaire entre les deux serveurs pour les garder connectés au même domaine ce qui est primordiale.

Donc dans le panneau de configuration du **server0** et Nous allons dans « system » Nous cherchons « Modifier les paramètres »

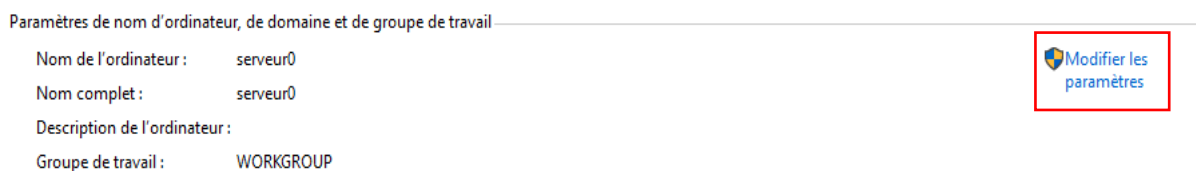


Figure 4.15 Information du deuxième serveur

Dans nom de l'ordinateur Nous cliquons sur « modifier » Nous cochons la case « domaine » et nous remplissons la barre par le nom de domaine (algeria-pki.dz)

Une fenêtre s'affiche et nous demande d'introduire les informations relatives au compte pour joindre le domaine, nous y introduisons les identifiants du compte administrateur du serveur « **server** »

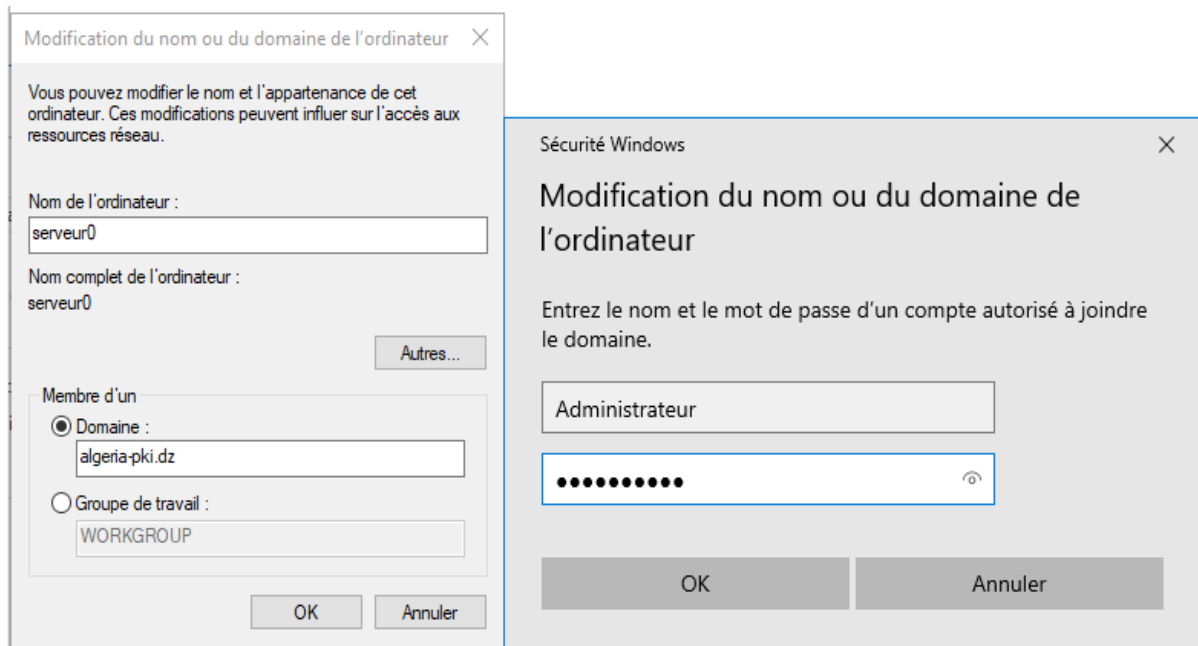


Figure 4.16 Connexion du deuxième serveur au domaine

Nous nous assurons que l'opération a été faite avec succès puis l'ordinateur redémarre automatiquement.

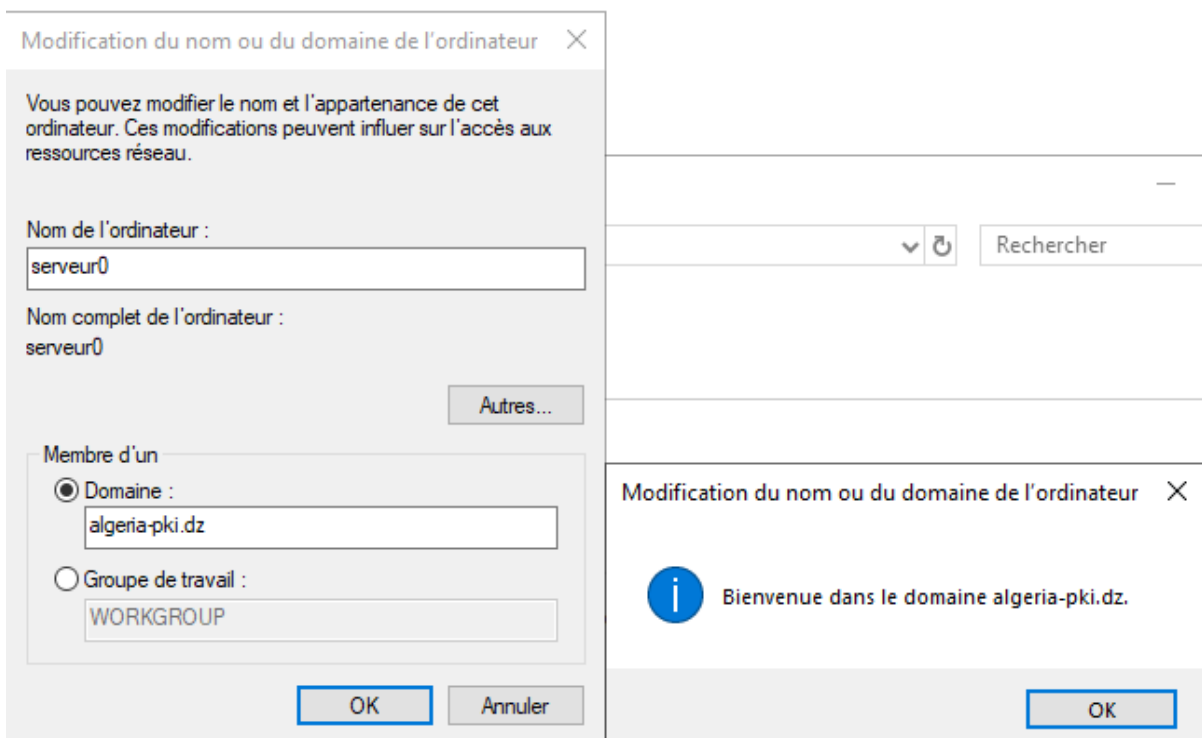


Figure 4.17 Connexion au domaine réussie

Nous devons alors nous connecter au système avec les identifiants du compte administrateur du contrôleur de domaine « **server** ».



Figure 4.18 Identification au compte lié au domaine

2. Créations d'une autorité de certification racine

2.1 Installation de l'autorité racine

Maintenant que nous sommes connectés au domaine, nous pouvons commencer, nous allons installer notre autorité de certification racine. Pour cela, dans le gestionnaire du serveur Nous cliquons sur "Gérer" "Ajouter des rôles et des fonctionnalités"

Nous cochoons la case "Services de certificats Active Directory" (AD CS). Puis Nous cliquons sur ajouter des fonctionnalités



Figure 4.19 Installation d'une autorité de certification racine 1/3

Pas de fonctionnalités supplémentaires.

Nous cochons la case "Autorité de certification".

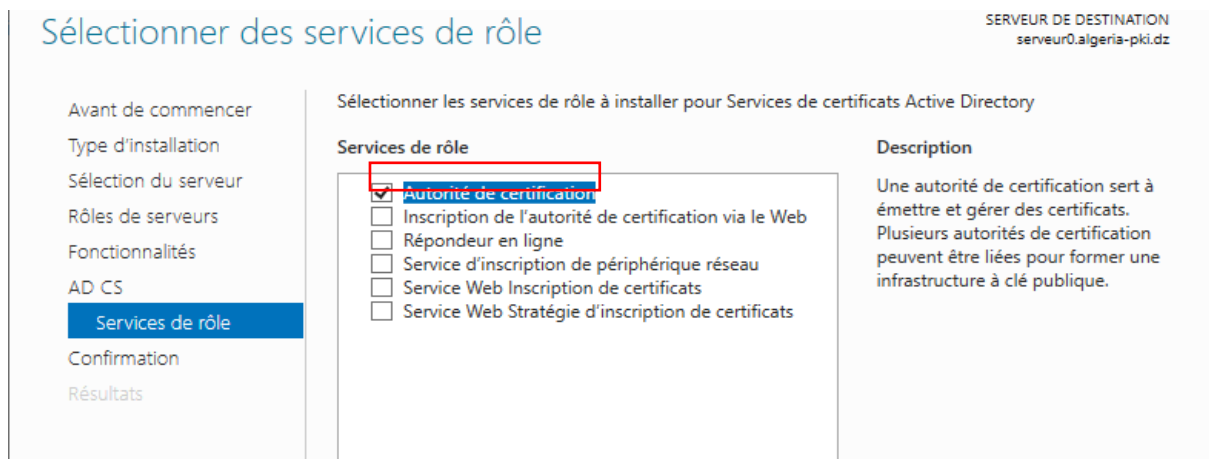


Figure 4.20 Installation d'une autorité de certification racine 2/3

Nous cochons la case "Redémarrer automatiquement ..." puis Nous cliquons sur "Installer".

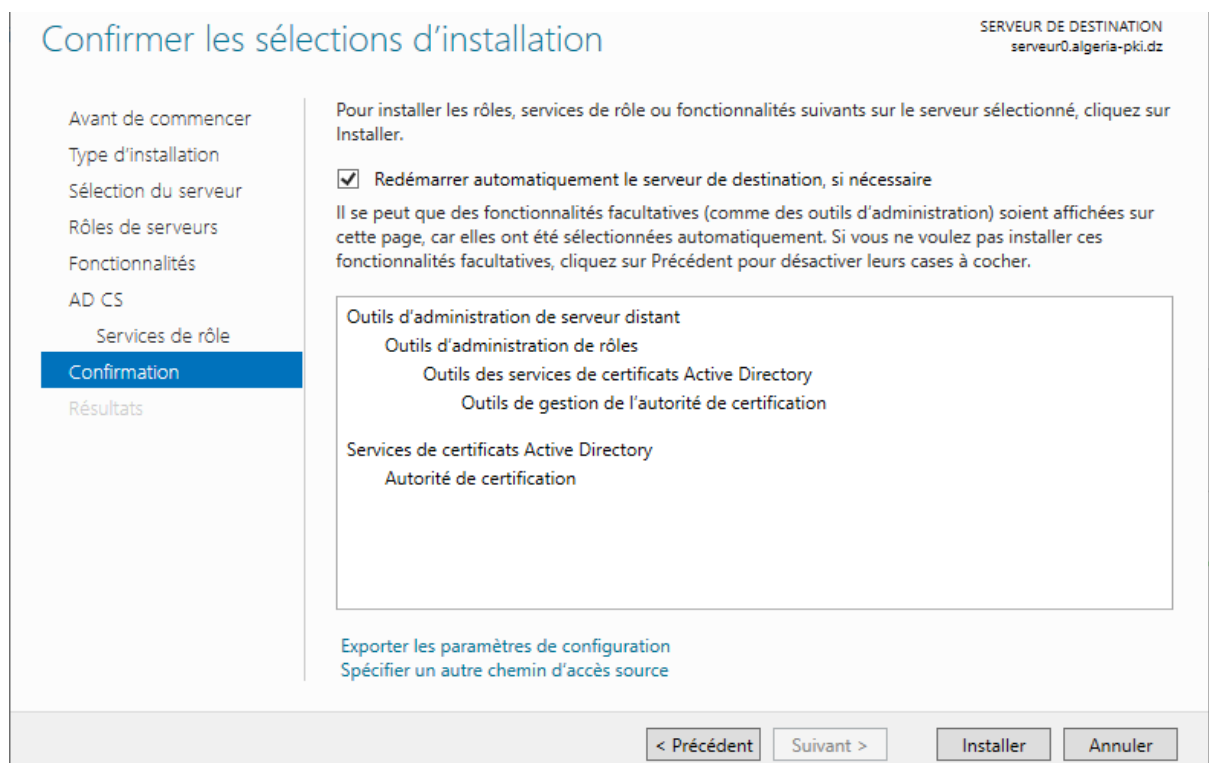


Figure 4.21 Installation d'une autorité de certification racine 3/3

2.2 Configuration de l'autorité racine

Une fois l'installation terminée, Nous cliquons sur le lien "Configurer les services de certificats Active Directory sur le serveur de destination".

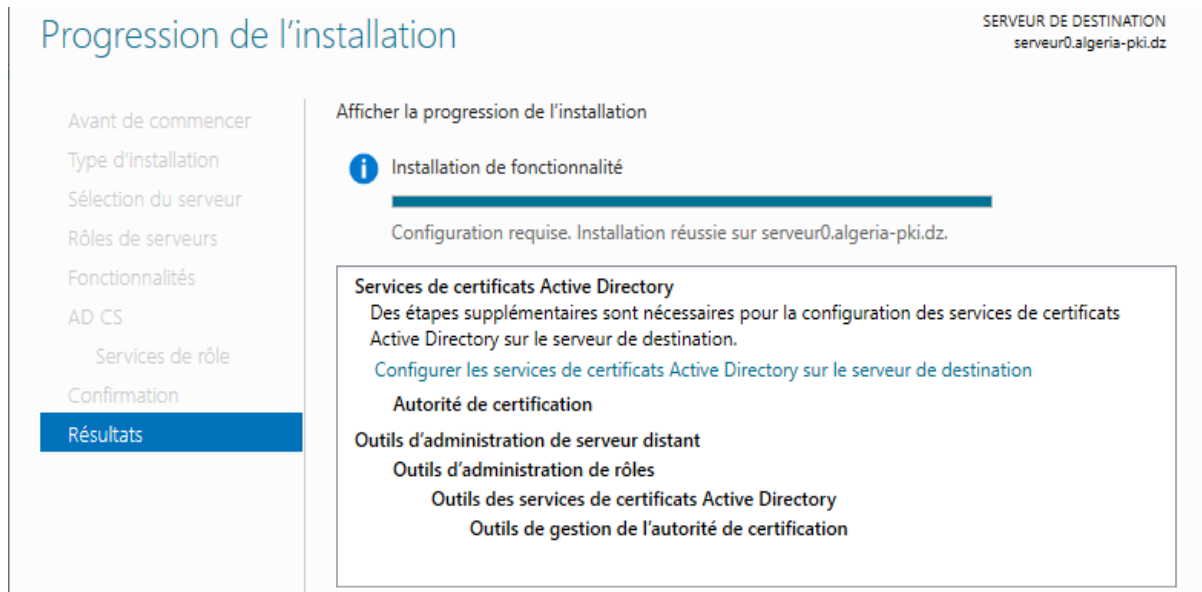


Figure 4.22 Configuration de l'autorité de certification racine 1/10

La fenêtre "Configuration des services de certificats Active Directory" s'affiche. Nous cochons la case "Autorité de certification" pour configurer ce rôle.

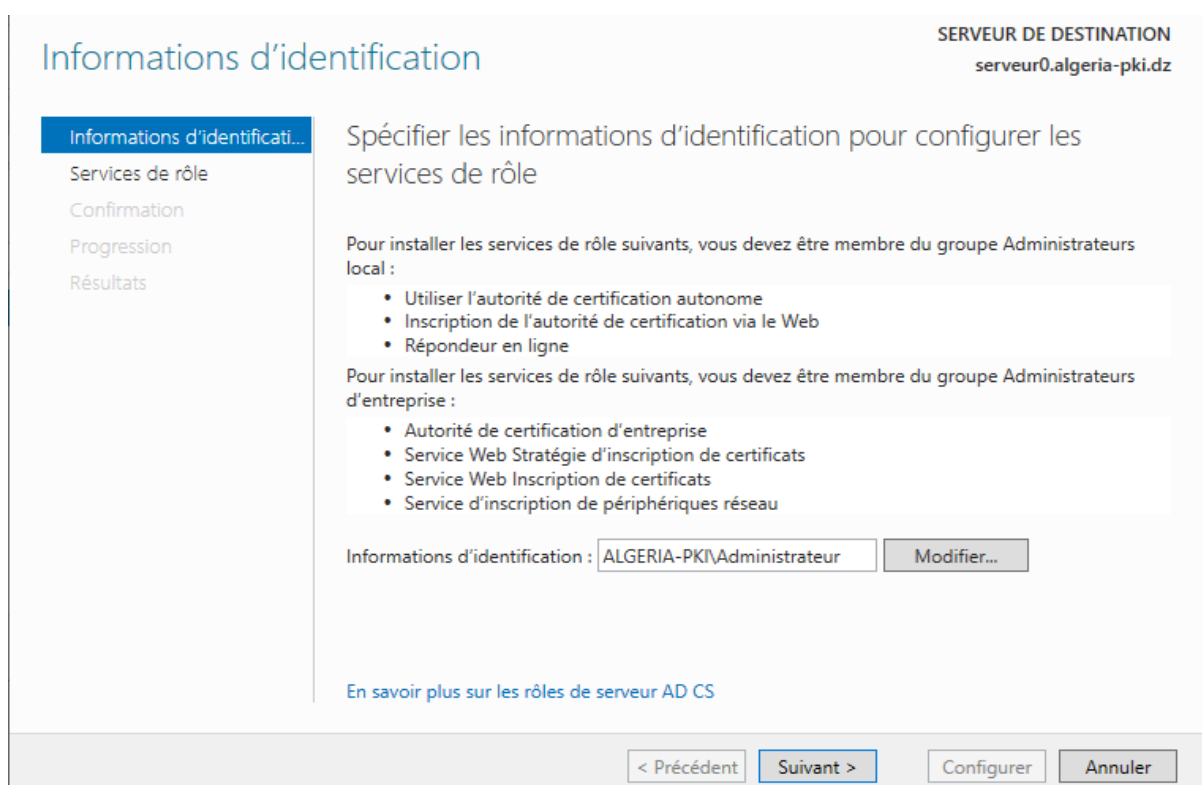


Figure 4.23 Configuration de l'autorité de certification racine 2/10

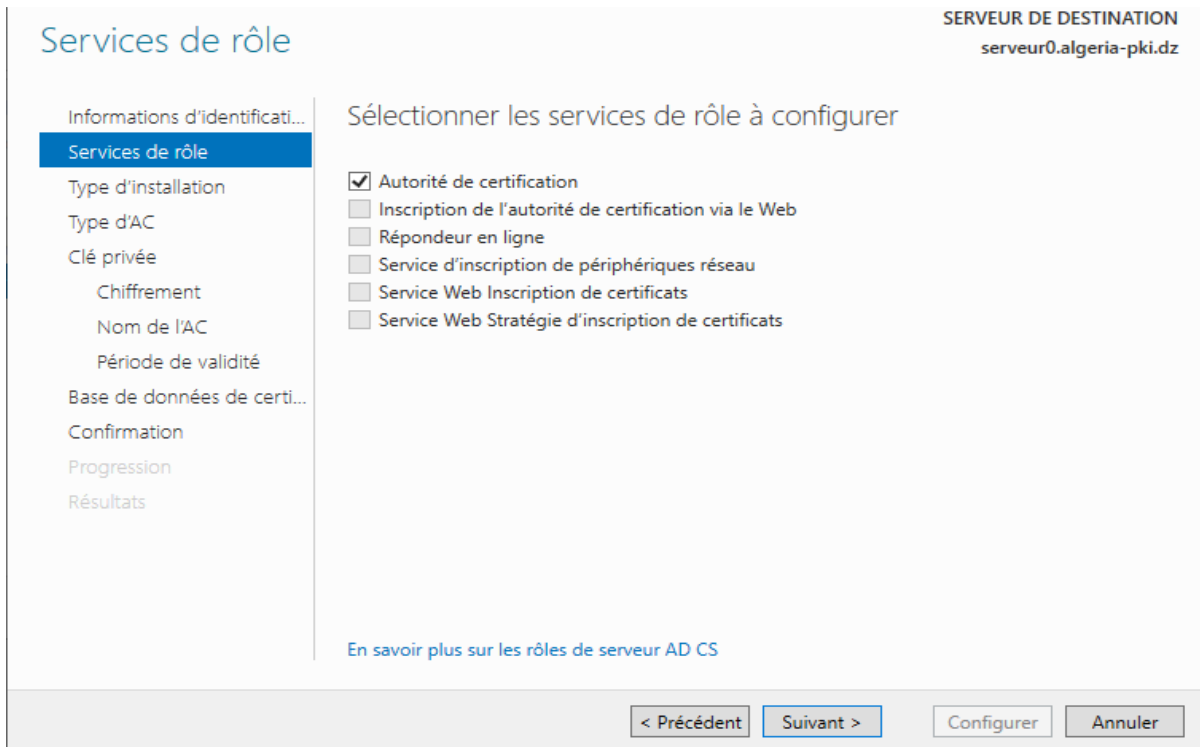


Figure 4.24 Configuration de l'autorité de certification racine 3/10

Nous sélectionnons "Autorité de certification d'entreprise" puisque notre PKI est membre du domaine **algeria-pki.dz**.

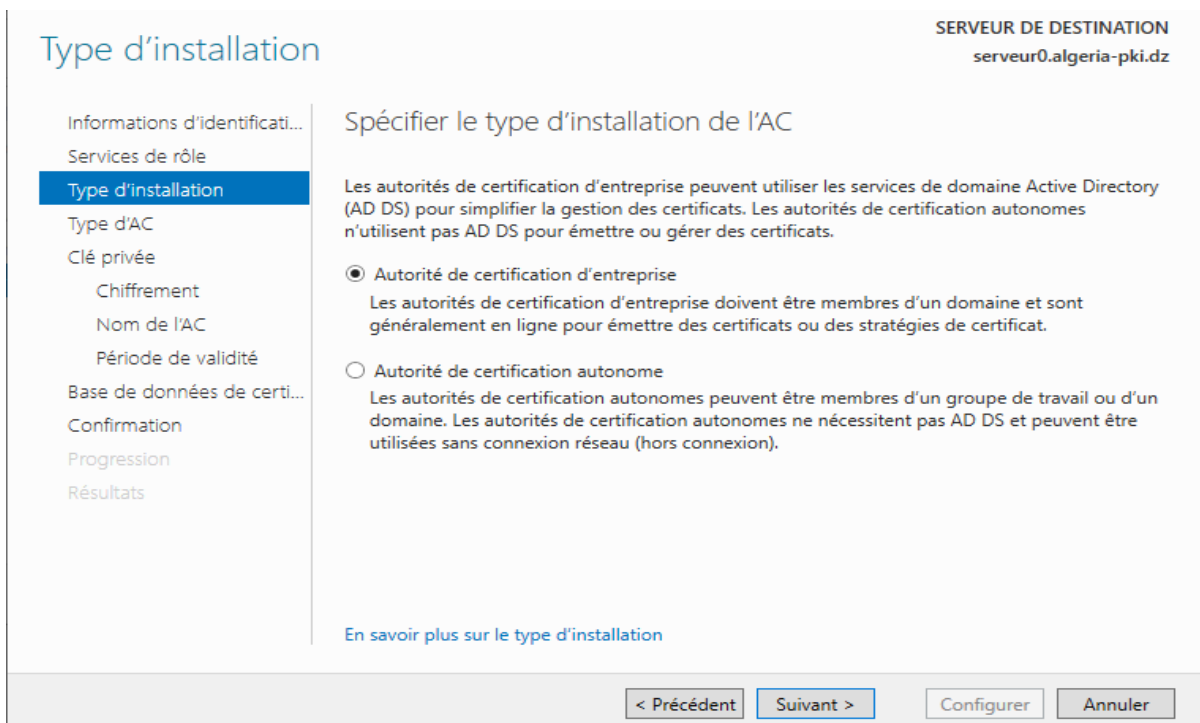


Figure 4.25 Configuration de l'autorité de certification racine 4/10

Nous sélectionnons "Autorité de certification racine" car notre autorité ne sera pas dépendante d'une autre.

Figure 4.26 shows the configuration window for the Certificate Authority (CA) type. The window title is "Type d'autorité de certification" and the server destination is "serveur0.algeria-pki.dz". The left sidebar shows a list of steps: Informations d'identificati..., Services de rôle, Type d'installation, Type d'AC (selected), Clé privée, Chiffrement, Nom de l'AC, Période de validité, Base de données de certi..., Confirmation, Progression, Résultats. The main content area is titled "Spécifier le type de l'AC" and contains a paragraph explaining the hierarchy of PKI. There are two radio button options: "Autorité de certification racine" (selected) and "Autorité de certification secondaire". At the bottom, there are buttons for "< Précédent", "Suivant >", "Configurer", and "Annuler".

Figure 4.26 Configuration de l'autorité de certification racine 5/10

Etant donné qu'il s'agit de la première installation de notre autorité de certification, nous allons créer une nouvelle clé privée.

Le 2ème choix nous permet de choisir la clé privée venant d'une ancienne installation de notre autorité de certification et nous permettra de garantir la continuité des certificats émis antérieurement à cette nouvelle installation.

Figure 4.27 shows the configuration window for the private key. The window title is "Clé privée" and the server destination is "serveur0.algeria-pki.dz". The left sidebar shows a list of steps: Informations d'identificati..., Services de rôle, Type d'installation, Type d'AC, Clé privée (selected), Chiffrement, Nom de l'AC, Période de validité, Base de données de certi..., Confirmation, Progression, Résultats. The main content area is titled "Spécifier le type de la clé privée" and contains a paragraph explaining the requirements for a private key. There are three radio button options: "Créer une clé privée" (selected), "Utiliser la clé privée existante", and "Sélectionner un certificat et utiliser sa clé privée associée". At the bottom, there are buttons for "< Précédent", "Suivant >", "Configurer", and "Annuler".

Figure 4.27 Configuration de l'autorité de certification racine 6/10

Pour les options de chiffrement Nous modifions juste la longueur de la clé (4096) et l'algorithme de hachage (SHA256).

Chiffrement pour l'autorité de certification

SERVEUR DE DESTINATION
serveur0.algeria-pki.dz

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats

Spécifier les options de chiffrement

Sélectionnez un fournisseur de chiffrement : Longueur de la clé :

RSA#Microsoft Software Key Storage Provider 4096

Sélectionnez l'algorithme de hachage pour signer les certificats émis par cette AC :

SHA256
SHA384
SHA512
SHA1

Autorisez l'interaction de l'administrateur lorsque l'autorité de certification accède à la clé privée.

[En savoir plus sur le chiffrement](#)

< Précédent Suivant > Configurer Annuler

Figure 4.28 Configuration de l'autorité de certification racine 7/10

Puis Nous choisissons un nom pour cette autorité de certification.

Nom de l'autorité de certification

SERVEUR DE DESTINATION
serveur0.algeria-pki.dz

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Période de validité
Base de données de certi...
Confirmation
Progression
Résultats

Spécifier le nom de l'AC

Tapez un nom commun pour identifier cette autorité de certification. Ce nom est ajouté à tous les certificats émis par l'autorité de certification. Les valeurs des suffixes du nom unique sont générées automatiquement, mais elles sont modifiables.

Nom commun de cette AC :

algeria-pki-root-ca

Suffixe du nom unique :

DC=algeria-pki,DC=dz

Aperçu du nom unique :

CN=algeria-pki-root-ca,DC=algeria-pki,DC=dz

[En savoir plus sur le nom de l'autorité de certification](#)

< Précédent Suivant > Configurer Annuler

Figure 4.29 Configuration de l'autorité de certification racine 8/10

Nous indiquons une période de validité pour le certificat de notre autorité de certification.

SERVEUR DE DESTINATION
serveur0.algeria-pki.dz

Période de validité

Informations d'identificati...

Services de rôle

Type d'installation

Type d'AC

Clé privée

Chiffrement

Nom de l'AC

Période de validité

Base de données de certi...

Confirmation

Progression

Résultats

Spécifier la période de validité

Sélectionnez la période de validité du certificat généré pour cette autorité de certification :

Années

Date d'expiration de l'AC : 03/04/2040 18:50:00

La période de validité configurée pour ce certificat d'autorité de certification doit dépasser la période de validité pour les certificats qu'elle émettra.

En savoir plus sur la période de validité

< Précédent
Suivant >
Configurer
Annuler

Figure 4.30 Configuration de l'autorité de certification racine 9/10

Nous laissons les dossiers des bases de données, par défaut.

Enfin l'assistant nous affiche un résumé de notre configuration.

SERVEUR DE DESTINATION
serveur0.algeria-pki.dz

Confirmation

Informations d'identificati...

Services de rôle

Type d'installation

Type d'AC

Clé privée

Chiffrement

Nom de l'AC

Période de validité

Base de données de certi...

Confirmation

Progression

Résultats

Pour configurer les rôles, services de rôle ou fonctionnalités ci-après, cliquez sur Configurer.

↶ **Services de certificats Active Directory**

Autorité de certification

Type d'AC :	Racine d'entreprise
Fournisseur de services de chiffrement :	RSA#Microsoft Software Key Storage Provider
Algorithme de hachage :	SHA256
Longueur de la clé :	4096
Autoriser l'interaction de l'administrateur :	Désactivé
Période de validité du certificat :	03/04/2040 18:50:00
Nom unique :	CN=algeria-pki-root-ca,DC=algeria-pki,DC=dz
Emplacement de la base de données de certificats :	C:\Windows\system32\CertLog
Emplacement du journal de la base de données de certificats :	C:\Windows\system32\CertLog

< Précédent
Suivant >
Configurer
Annuler

Figure 4.31 Configuration de l'autorité de certification racine 10/10

Notre autorité de certification est maintenant installée et configurée.

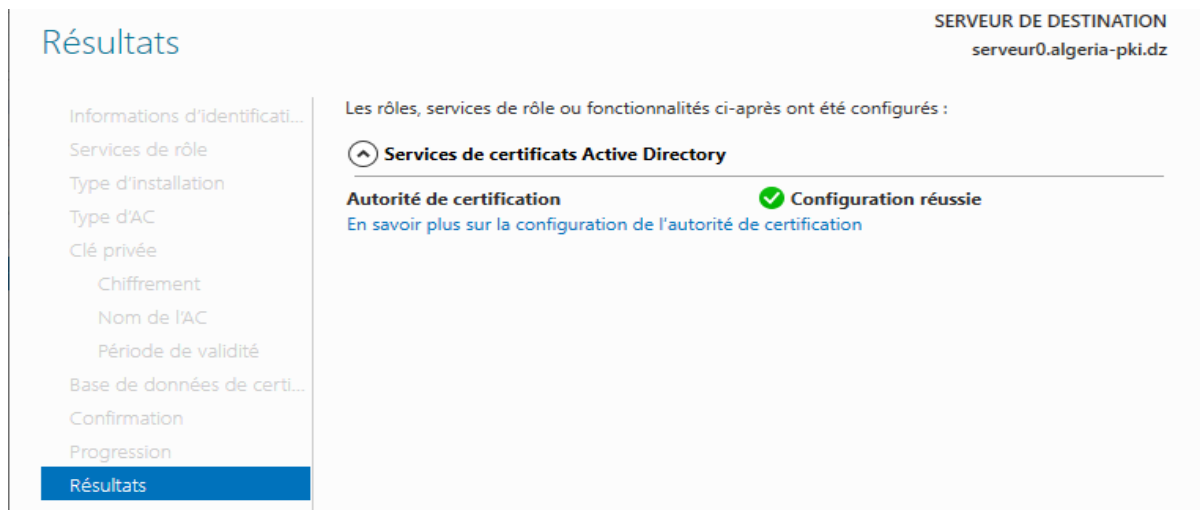


Figure 4.32 Finalisation de la configuration de l'AC racine

Pour accéder à l'autorité de certification Nous cliquons sur "outils" puis sur "autorité de certification".

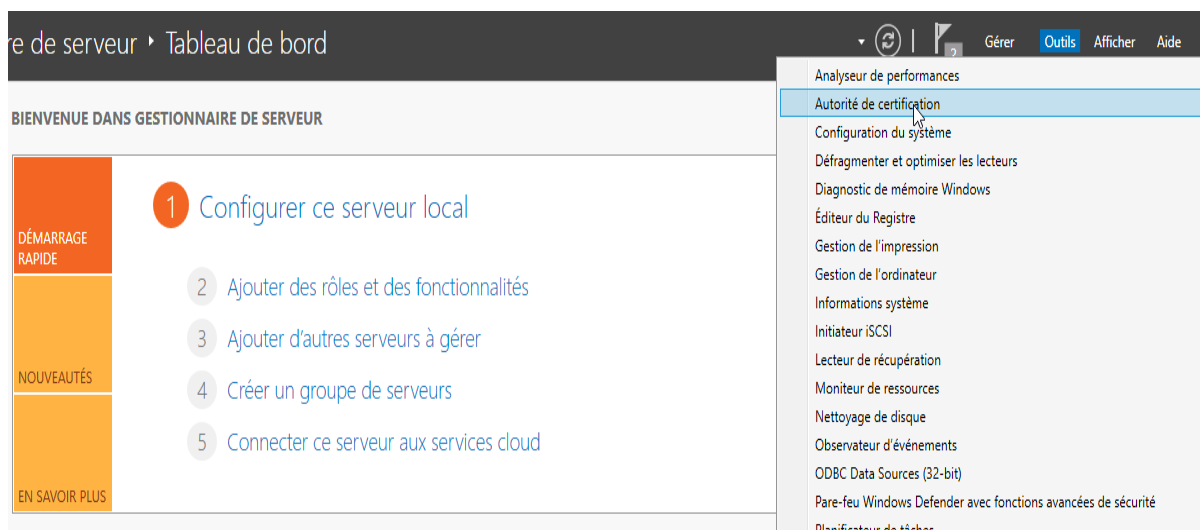


Figure 4.33 Accès à l'autorité de certification racine

La fenêtre suivante s'affiche.

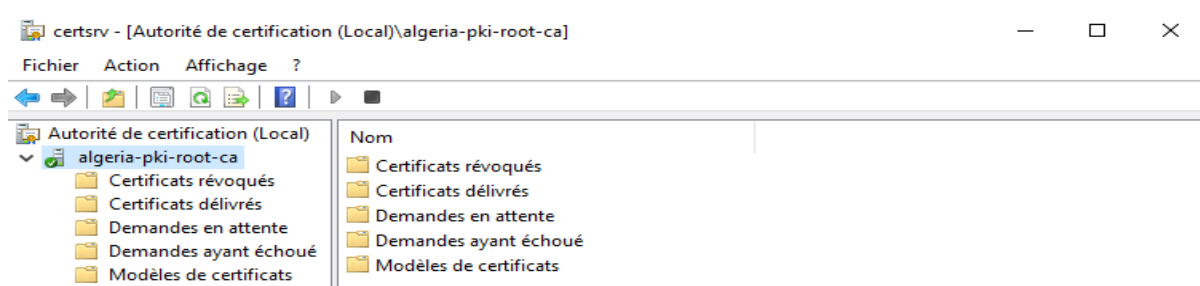


Figure 4.34 Autorité de certification racine opérationnelle

3. Créations d'une autorité de certification intermédiaire

3.1 Installation de l'autorité de certification intermédiaire

En ce qui concerne l'installation et la configuration de la CA intermédiaire, nous répétons quasiment les mêmes étapes sauf pour quelques paramètres propres à cette autorité.

Nous cochons la case "inscription de l'autorité de certification via le web" cela a pour but de permettre à l'utilisateur de faire sa demande de certificat directement depuis internet.

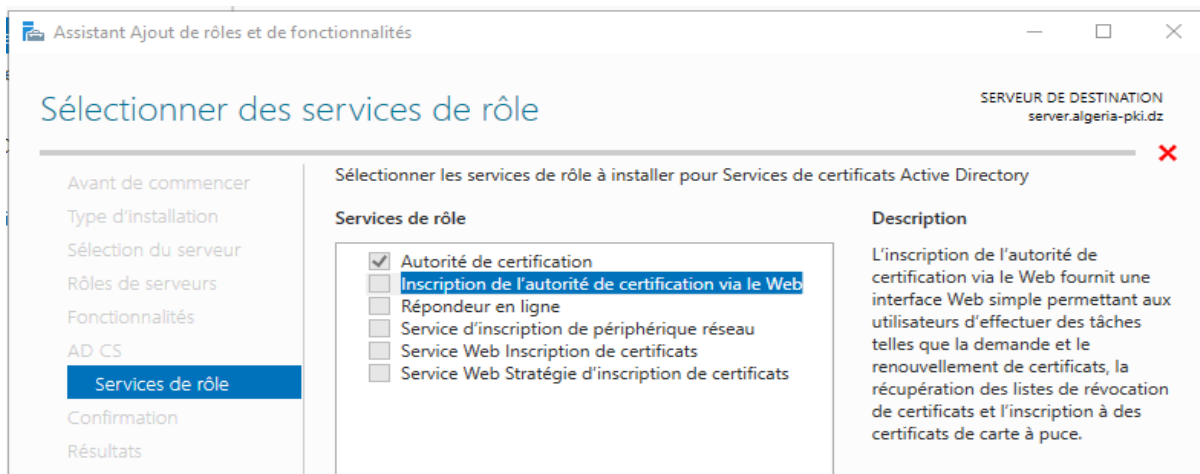


Figure 4.35 Installation de l'autorité de certification secondaire

3.2 Configuration de l'autorité de certification intermédiaire

Après l'installation réussie nous configurons la CA intermédiaire, en cochant alors les deux cases disponibles et nous suivons les mêmes étapes que pour la CA racine mise à part qu'au lieu de racine nous choisissons secondaire.

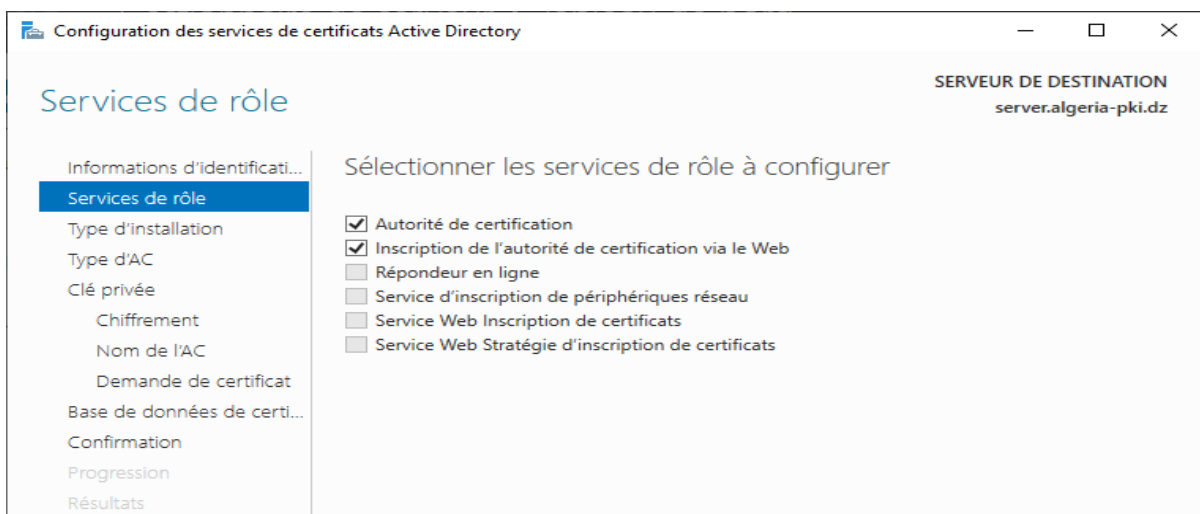


Figure 4.36 Configuration de l'autorité de certification secondaire 1/3

Nous sélectionnons "Autorité de certification secondaire " car notre autorité dépend de l'autorité racine ou parente.

SERVEREUR DE DESTINATION
server.algeria-pki.dz

Type d'autorité de certification

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Demande de certificat
Base de données de certi...
Confirmation
Progression
Résultats

Spécifier le type de l'AC

Lorsque vous installez les services de certificats Active Directory (AD CS), vous créez ou étendez une hiérarchie d'infrastructure à clé publique (PKI). Une autorité de certification racine se trouve au sommet de la hiérarchie PKI et émet ses propres certificats auto-signés. Une autorité de certification secondaire reçoit un certificat de l'autorité de certification de rang plus élevé dans la hiérarchie PKI.

Autorité de certification racine
Les autorités de certification racines sont les premières voire les seules autorités de certification configurées dans une hiérarchie PKI.

Autorité de certification secondaire
Les autorités de certification secondaires nécessitent une hiérarchie PKI établie et sont autorisées à émettre des certificats par l'autorité de certification de rang plus élevé dans la hiérarchie.

[En savoir plus sur le type d'autorité de certification](#)

< Précédent Suivant > Configurer Annuler

Figure 4.37 Configuration de l'autorité de certification secondaire 2/3

Nous choisissons un nom pour notre CA.

SERVEREUR DE DESTINATION
server.algeria-pki.dz

Nom de l'autorité de certification

Informations d'identificati...
Services de rôle
Type d'installation
Type d'AC
Clé privée
Chiffrement
Nom de l'AC
Demande de certificat
Base de données de certi...
Confirmation
Progression
Résultats

Spécifier le nom de l'AC

Tapez un nom commun pour identifier cette autorité de certification. Ce nom est ajouté à tous les certificats émis par l'autorité de certification. Les valeurs des suffixes du nom unique sont générées automatiquement, mais elles sont modifiables.

Nom commun de cette AC :

Suffixe du nom unique :

Aperçu du nom unique :

[En savoir plus sur le nom de l'autorité de certification](#)

< Précédent Suivant > Configurer Annuler

Figure 4.38 Configuration de l'autorité de certification secondaire 3/3

Pour être actif, la CA racine doit avoir un certificat, de ce fait elle en génère un et le signe elle-même « certificat auto-signé » mais pour l'intermédiaire elle devra obtenir un certificat signé par la CA racine. Donc nous allons automatiquement transférer sa demande de certification à l'autorité racine puisqu'elles appartiennent au même domaine d'où l'avantage d'avoir un domaine.

Figure 4.39 Envoie de demande de certification automatique à l'AC racine

La demande ayant été transmise signée et retournée à la CA intermédiaire, pour être totalement opérationnelle.

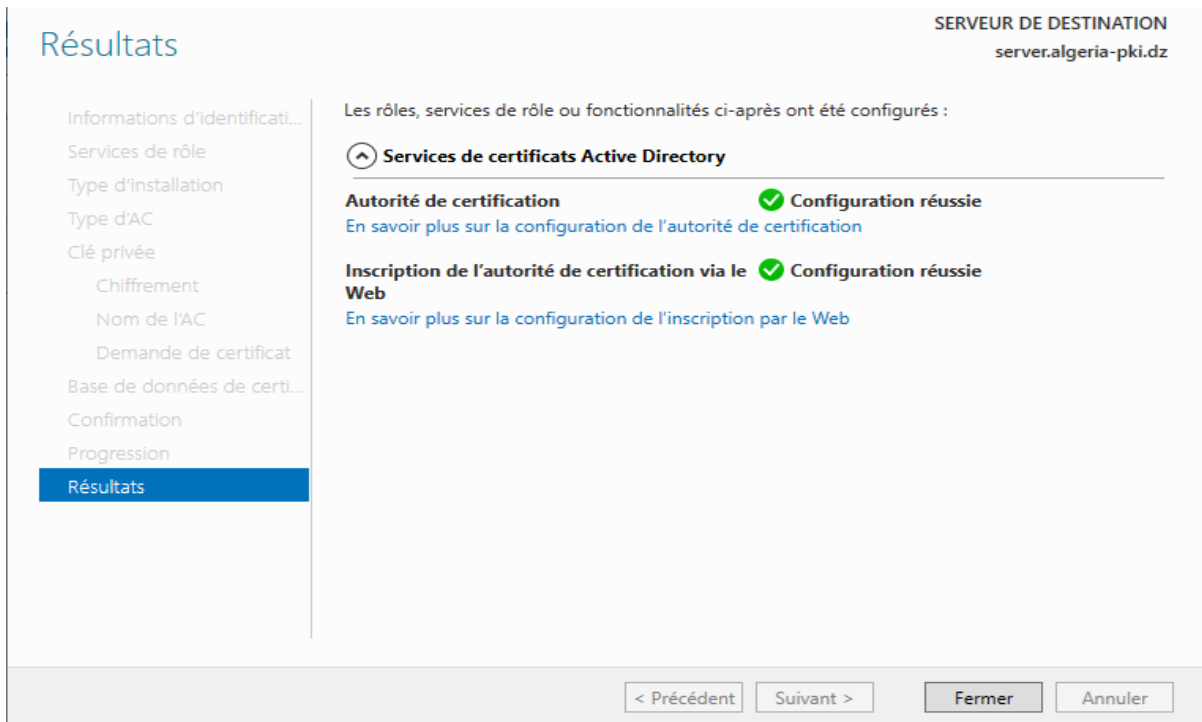


Figure 4.40 Finalisation de la configuration de l'AC secondaire

Pour vérifier cela nous pouvons aller consulter la liste des certificats délivrés par la CA racine, nous pourrions voir un certificat émis pour « algeria-pki-inter-ca ».

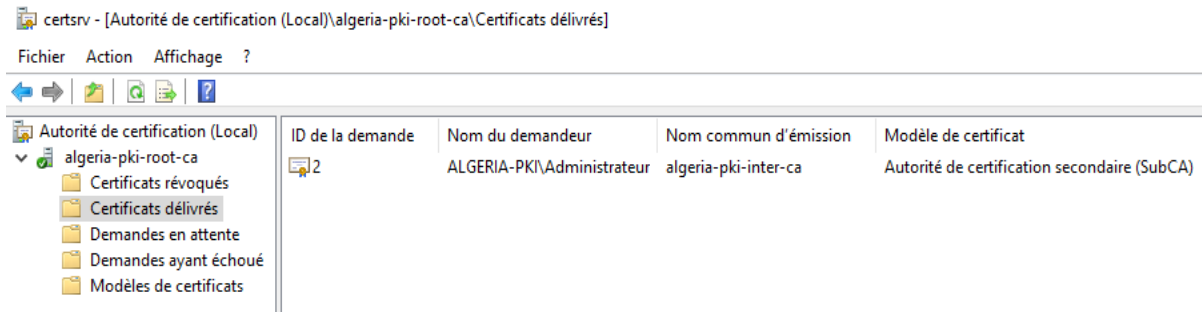


Figure 4.41 Certificat délivré par l'AC racine

Et dans outil autorité de certification notre ca est opérationnelle.

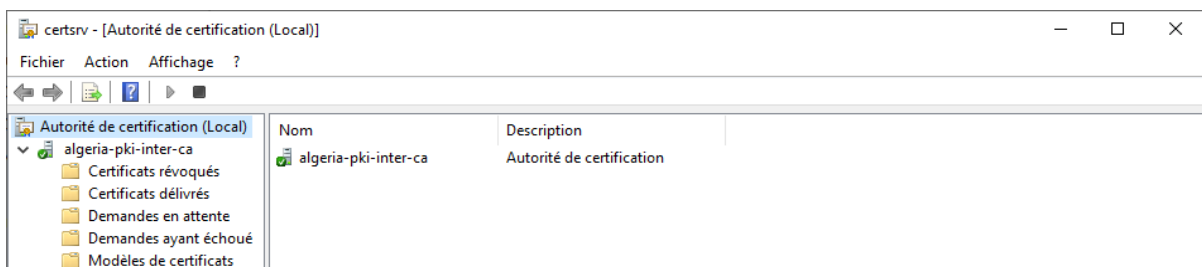


Figure 4.42 Autorité de certification secondaire opérationnelle

III. Utilisation de la PKI

1. Mise en place d'un serveur web sécurisé

Lors de l'installation de l'AC secondaire nous avons coché la case « inscription de l'autorité via le web » cette opération nous a permis d'installer et de configurer partiellement le serveur IIS de manière automatique.

D'où le fait qu'un serveur IIS soit déjà présent dans les rôles du serveur.

Ainsi le serveur DNS aussi a déjà été installé lors de la création du domaine et a donc été lui aussi configuré.

Nous allons tout d'abord tester l'accès au site en entrant l'adresse du serveur dans un navigateur web :

server.algeria-pki.dz

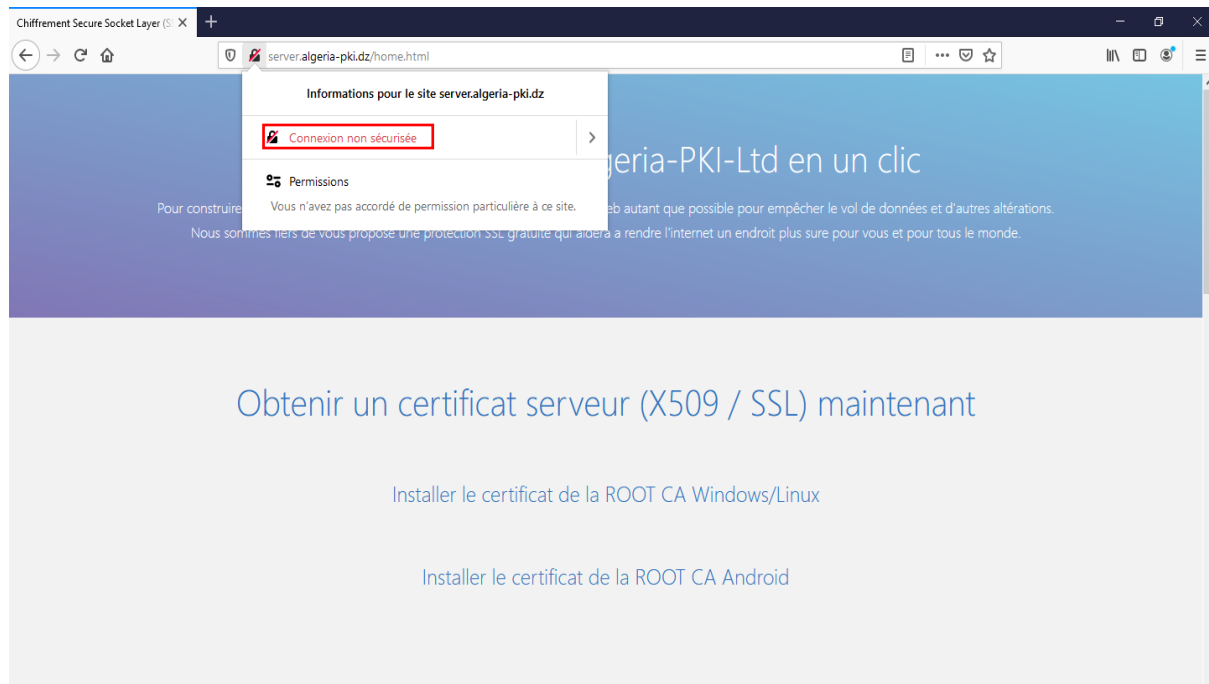


Figure 4.43 Site web accessible et non sécurisé

Le site est bel et bien accessible par son adresse, ce qui confirme que le serveur DNS est fonctionnel.

Nous remarquons néanmoins que notre site n'est pas sécurisé par https, il faut alors le sécuriser pour chiffrer toutes les opérations qui s'y produisent, tel que le transit de mot de passe.

1.1 Sécurisations du serveur web grâce au certificat SSL

1.1.1 Créations d'un certificat pour un serveur

Nous devons pour cela générer et signer un certificat pour notre serveur TLS
Nous nous dirigeons alors vers la console « mmc » en exécutant cette même commande dans la fenêtre qui s'affiche lorsque nous appuyons sur « **Windows+R** »

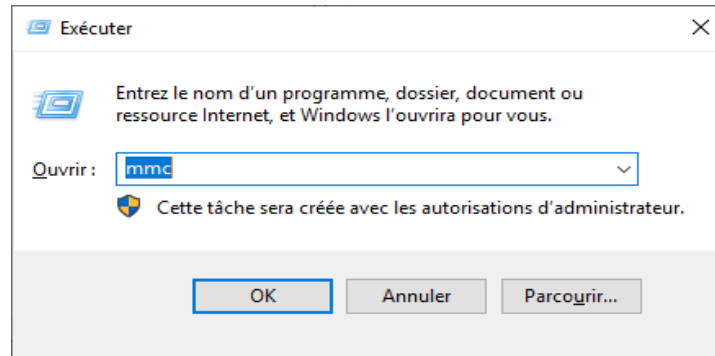


Figure 4.44 Exécution de la commande mmc

Nous cliquons ensuite sur l'onglet « fichier », puis sur « ajouter ou supprimer des composants logiciel enfichables ».

Nous y ajoutons l'élément « certificat » et Nous sélectionnons « un compte d'ordinateur ».

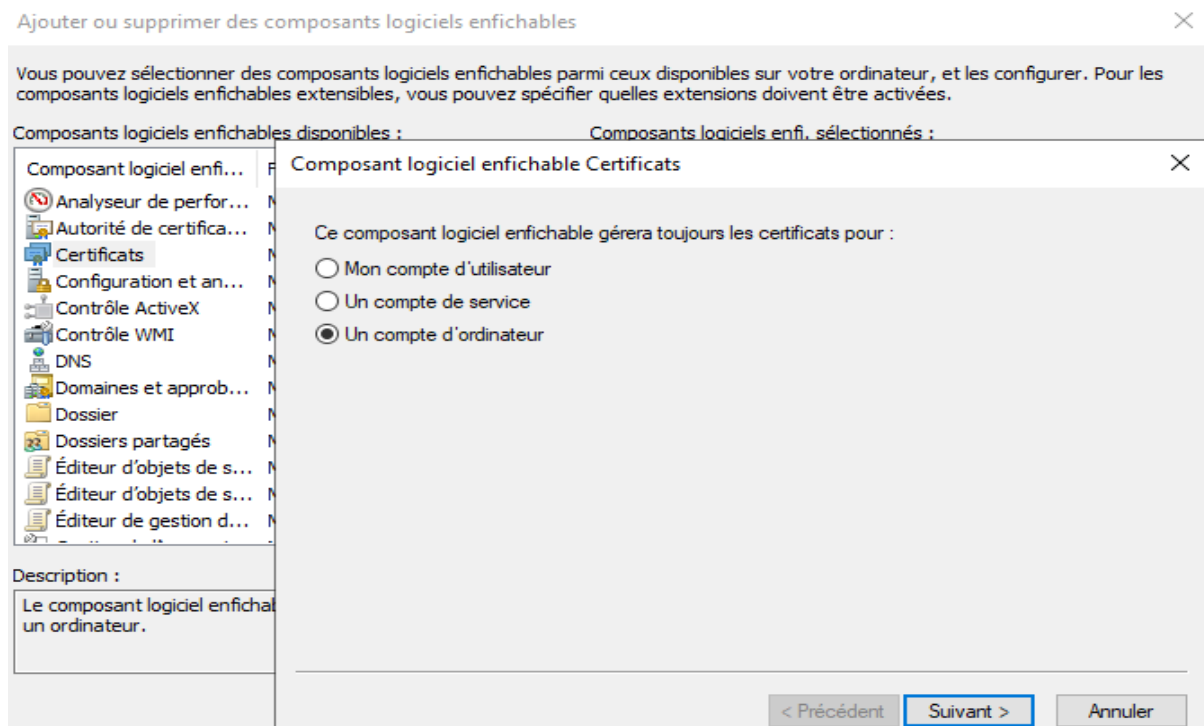


Figure 4.45 Ajout d'un composant logiciel enfichable

Et dans « personnel » Nous faisons un clic droit sur « certificats » puis « toutes les tâches »

Ensuite « demander un nouveau certificat ».

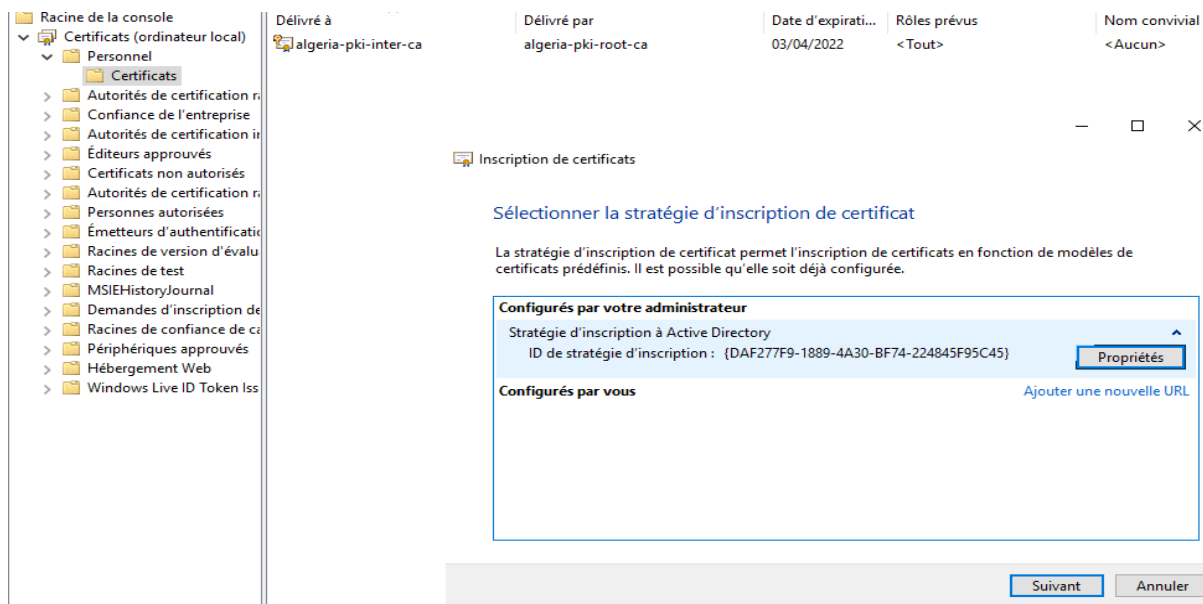


Figure 4.46 Création d'une demande de certificat 1/3

Nous arrivons jusqu'à la « stratégie d'inscription à active directory », et c'est ici que notre Choix de CA d'entreprise prend tout son sens, car si elle ne l'était pas, la soumission aurait dû être faite manuellement.

Nous sélectionnons ensuite « contrôleur de domaine » et nous appuyons sur « inscription ».

Demander des certificats

Vous pouvez demander les types de certificats suivants. Sélectionnez les certificats que vous voulez demander, puis cliquez sur Inscription.

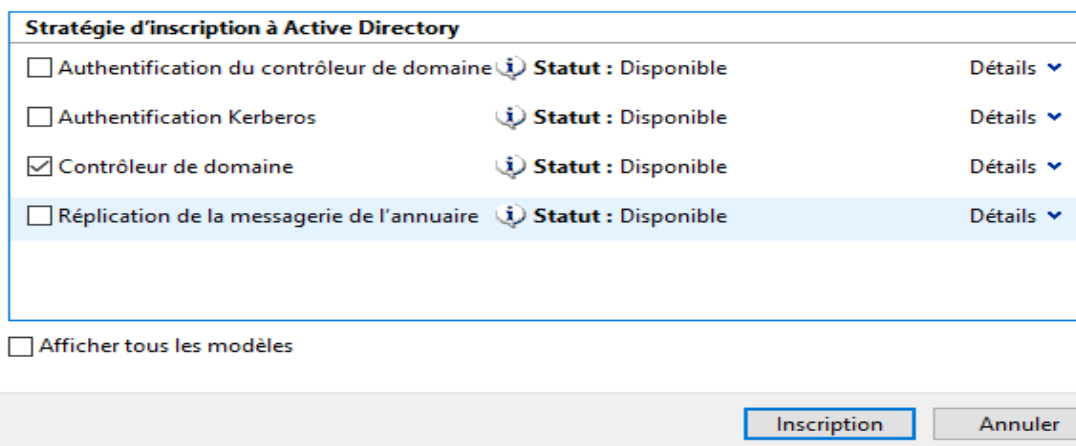


Figure 4.47 Création d'une demande de certificat 2/3

Résultats de l'installation des certificats

Les certificats suivants ont été inscrits et installés sur cet ordinateur.

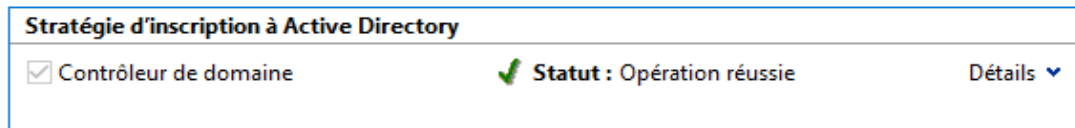


Figure 4.48 Création d'une demande de certificat 3/3

Voilà maintenant notre serveur a désormais un certificat à son nom, il faut alors attribuer ce certificat au site web pour qu'il soit sécurisé.

Délivré à	Délivré par	Date d'expirati...	Rôles prévus
algeria-pki-inter-ca	algeria-pki-root-ca	03/04/2022	<Tout>
server.algeria-pki.dz	algeria-pki-inter-ca	03/04/2021	Authentification du client, Authentification du serveur

Figure 4.49 Certificat correctement généré

1.1.2 Attributions du certificat au serveur

Sur la page de configuration du serveur IIS Nous cliquons sur « défaut web site » Nous cherchons « liaison » pour y ajouter la connexion https sécurisé alors Nous cliquons sur « ajouter » Nous sélectionnons ensuite « https » puis le certificat délivré au serveur.

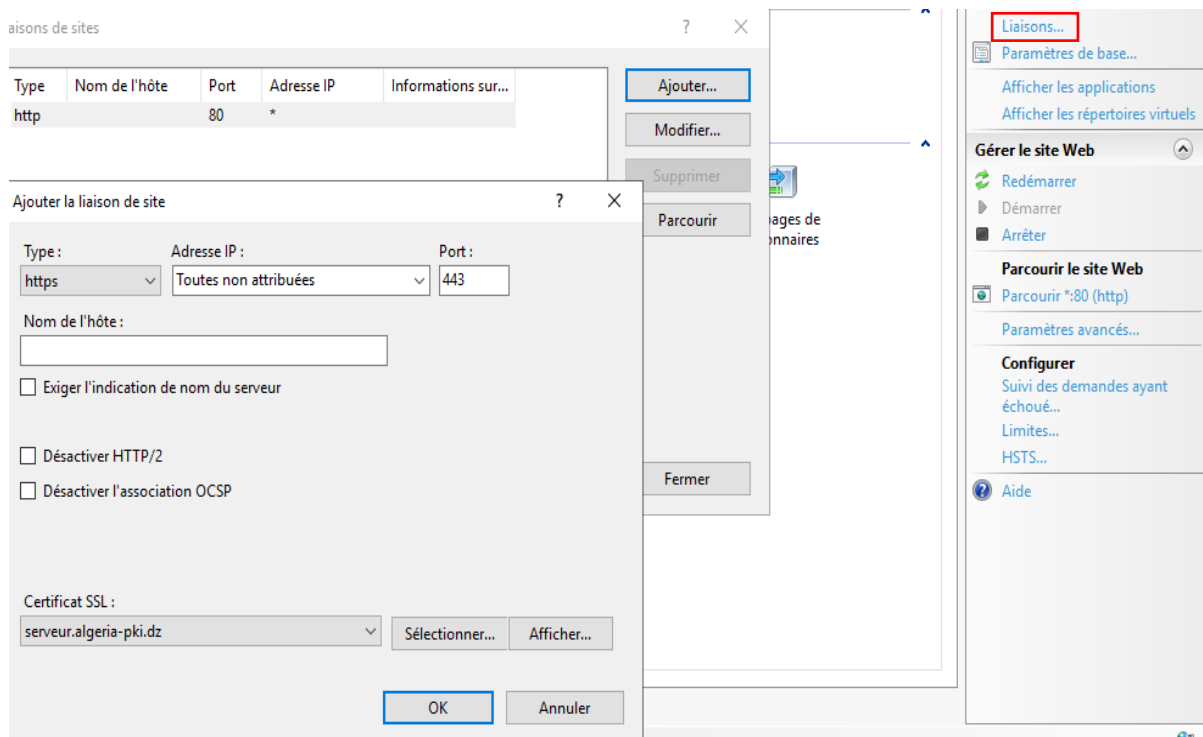


Figure 4.50 Configuration du HTTPS dans pour IIS

Maintenant notre serveur dispose d'un certificat valide et signé par notre PKI, mais avant de pouvoir accéder à notre site de manière sécurisée, il faut tout d'abord configurer le navigateur pour qu'il fasse confiance à notre autorité de certification « auto-signée ». Pour cela il faut se diriger vers options, ensuite gestionnaire de certificats, puis importer un bundle qui contient le certificat de la CA racine et intermédiaire.

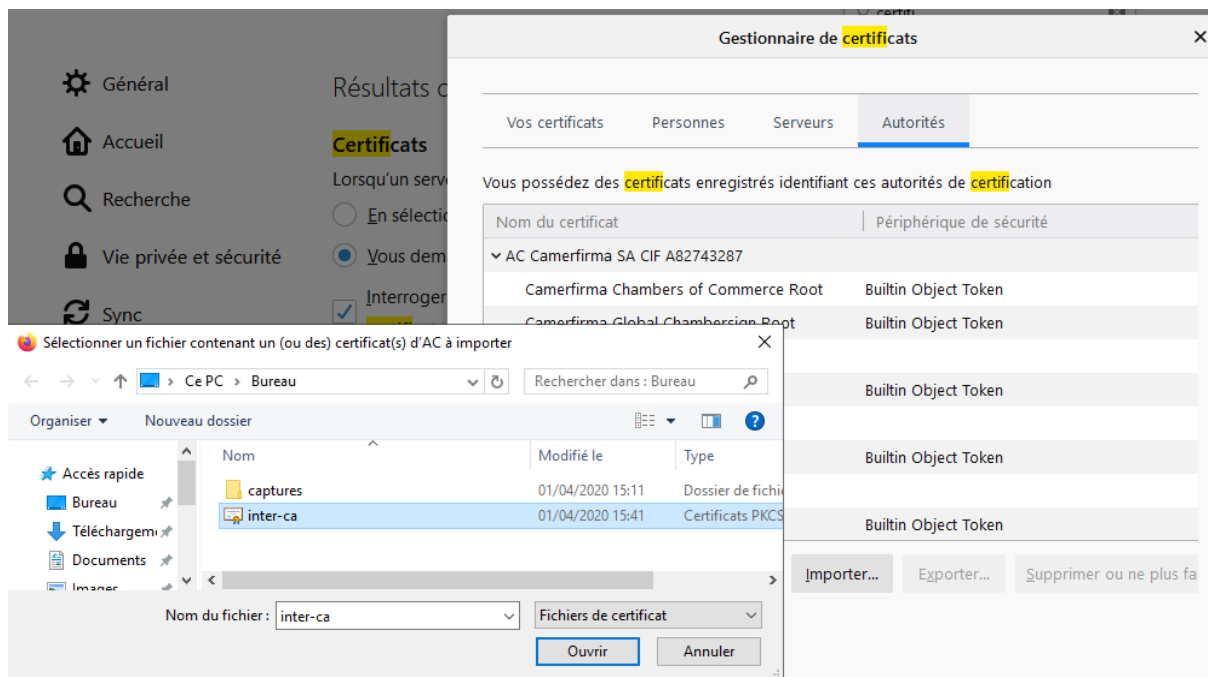


Figure 4.51 Importation du bundle de certificat dans le navigateur

Nous cliquons sur ok pour confirmer l'opération.

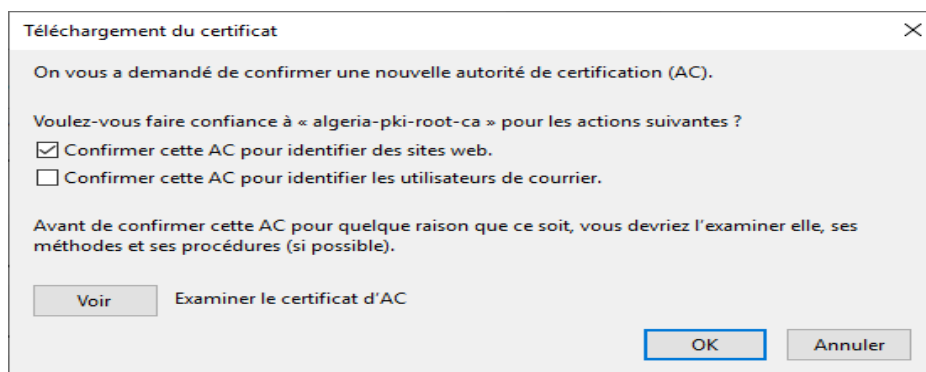


Figure 4.52 Confirmation que l'AC est de confiance

Nous nous assurons que notre certificat a été correctement ajouté à la liste auquel le navigateur fait confiance.

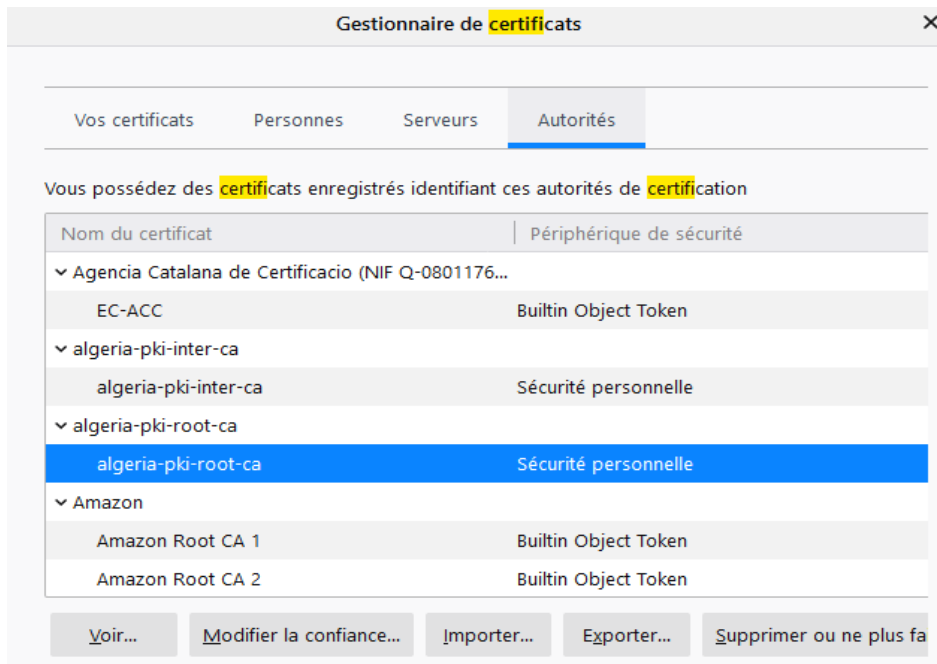


Figure 4.53 Importation réussie dans la liste des AC de confiance

Nous allons alors tenter d'accéder à notre site web par l'adresse :

<https://server.algeria-pki.dz>

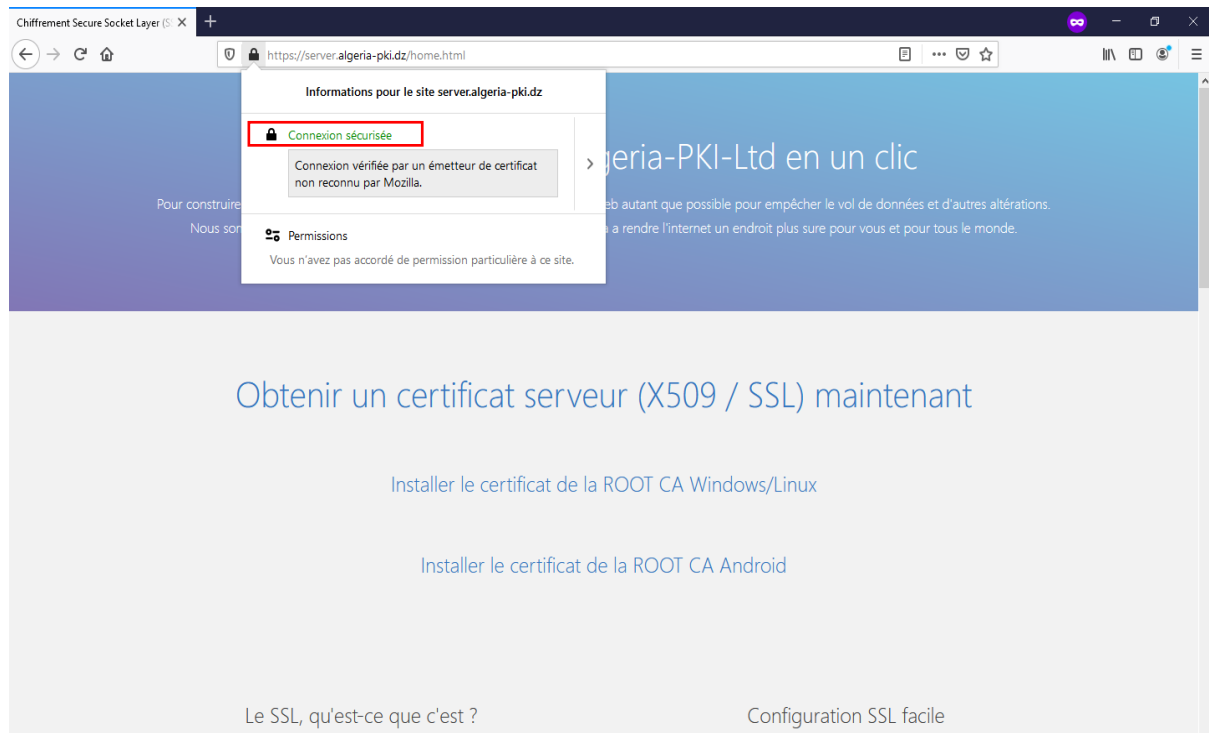


Figure 4.54 Site web accessible et sécurisé

Et voilà nous arrivons bel et bien à accéder à notre site de manière sécurisé en **https**.

2. Mise en place d'un réseau Wi-Fi avec authentification basée sur des certificats

2.1 Installation et configuration d'un serveur Radius

Pour permettre aux utilisateurs de s'authentifier par certificat il nous faut ajouter un nouveau rôle pour le serveur qui sera « services de stratégie et d'accès réseau »

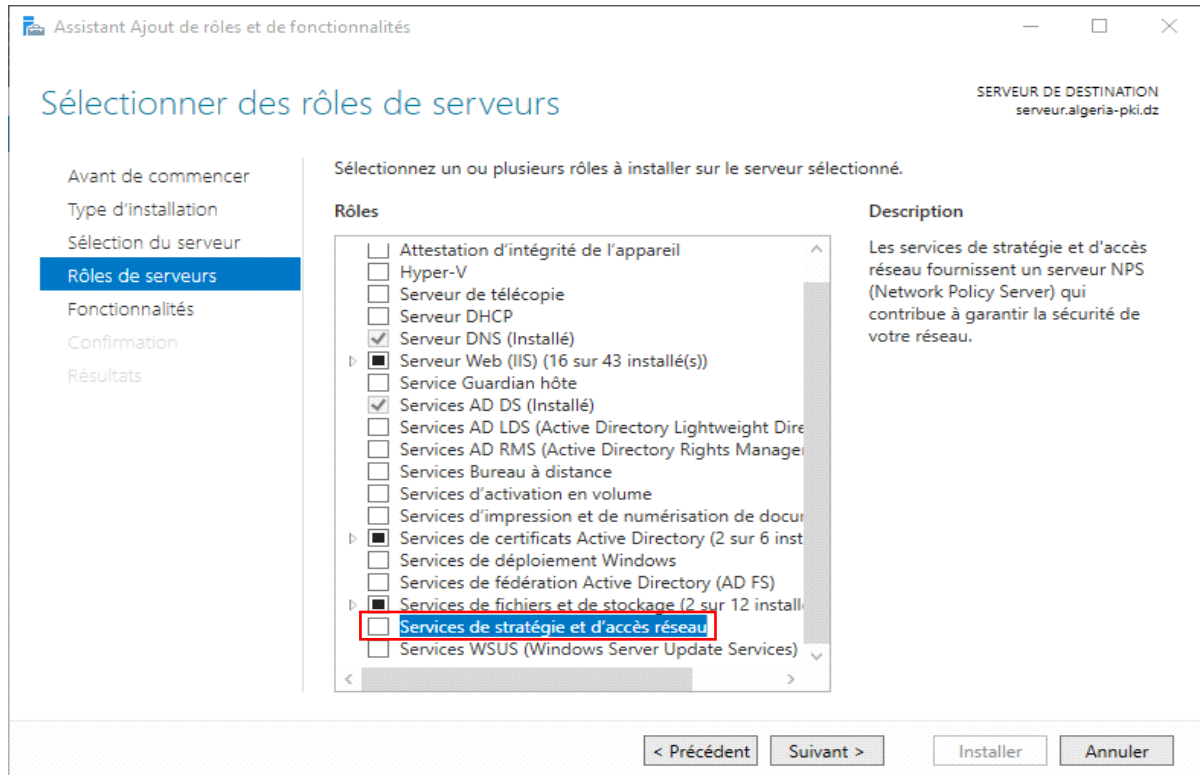


Figure 4.55 Ajout du rôle NPS

Après une installation réussie il faut configurer le serveur pour lui indiquer les règles et les contraintes à appliquer.

Nous ouvrons alors le (Network Policy services) dans le menu Outils, nous devons tout d'abord inscrire le service dans le domaine en faisant un clic droit sur NPS puis « inscrire le serveur dans active directory ».

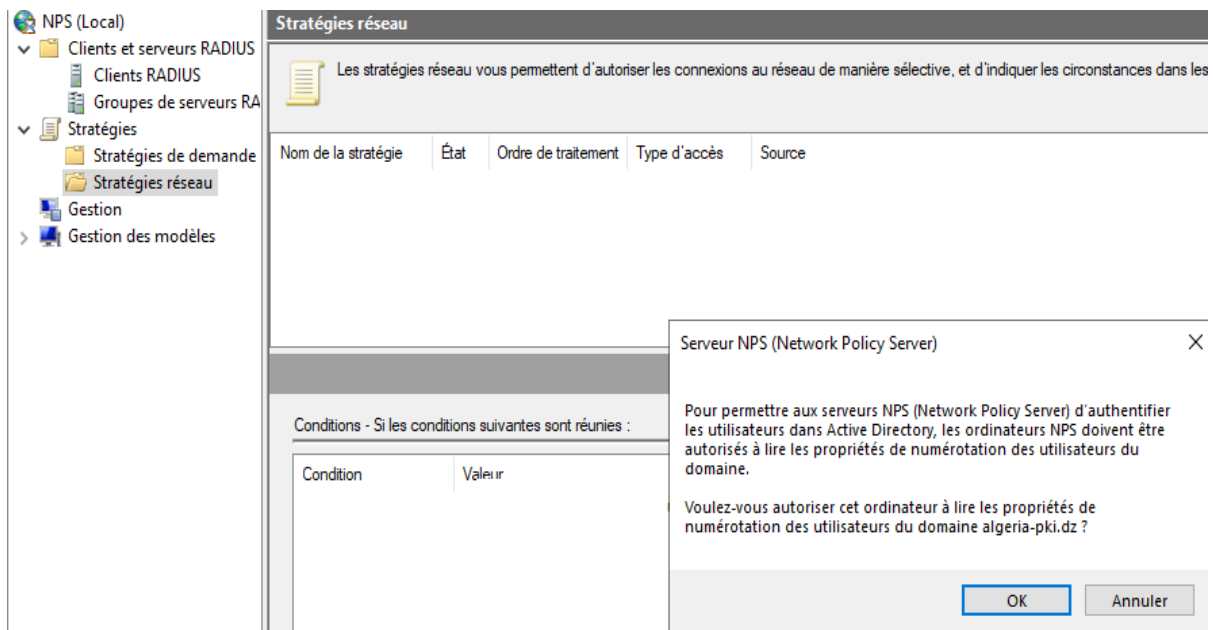


Figure 4.56 Inscription du serveur NPS dans le domaine

Une fois fait Nous devons configurer les clients qui pourront consulter le serveur pour authentifier des utilisateurs (Point d'accès) donc clic droit sur « Client RADIUS » puis sur "nouveau".

Nous choisissons un nom convivial « **Broadcom** » ainsi que l'adresse IP du point d'accès et un secret partagé qui permettra au point d'accès d'accéder au serveur.

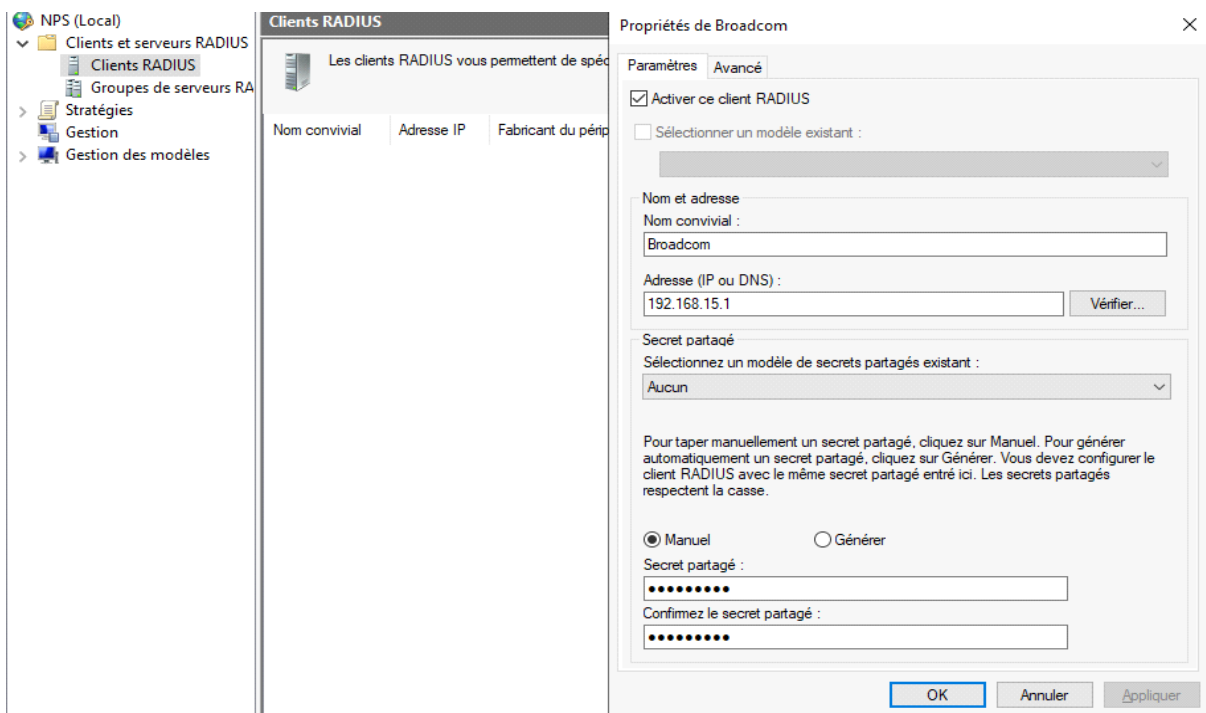


Figure 4.57 Ajout d'un client autorisé à accéder au serveur NPS

Nous déroulons ensuite « stratégies », Nous devons spécifier les règle d'accès de ce dernier Nous faisons un clic droit sur « stratégie de demande » puis sur "nouveau".

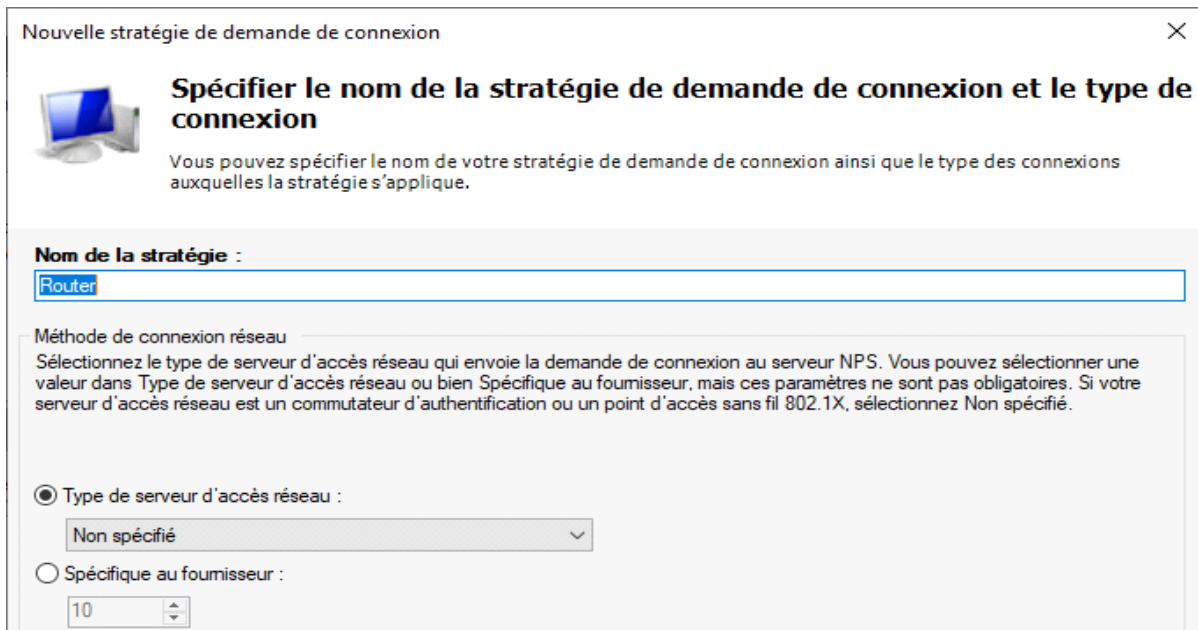


Figure 4.58 Nouvelles stratégie de demande au serveur NPS

Et Nous ajoutons la règle « nom convivial du client » qui signifie que l'accès au client sera autorisé uniquement s'il a comme nom convivial « **Broadcom** ».

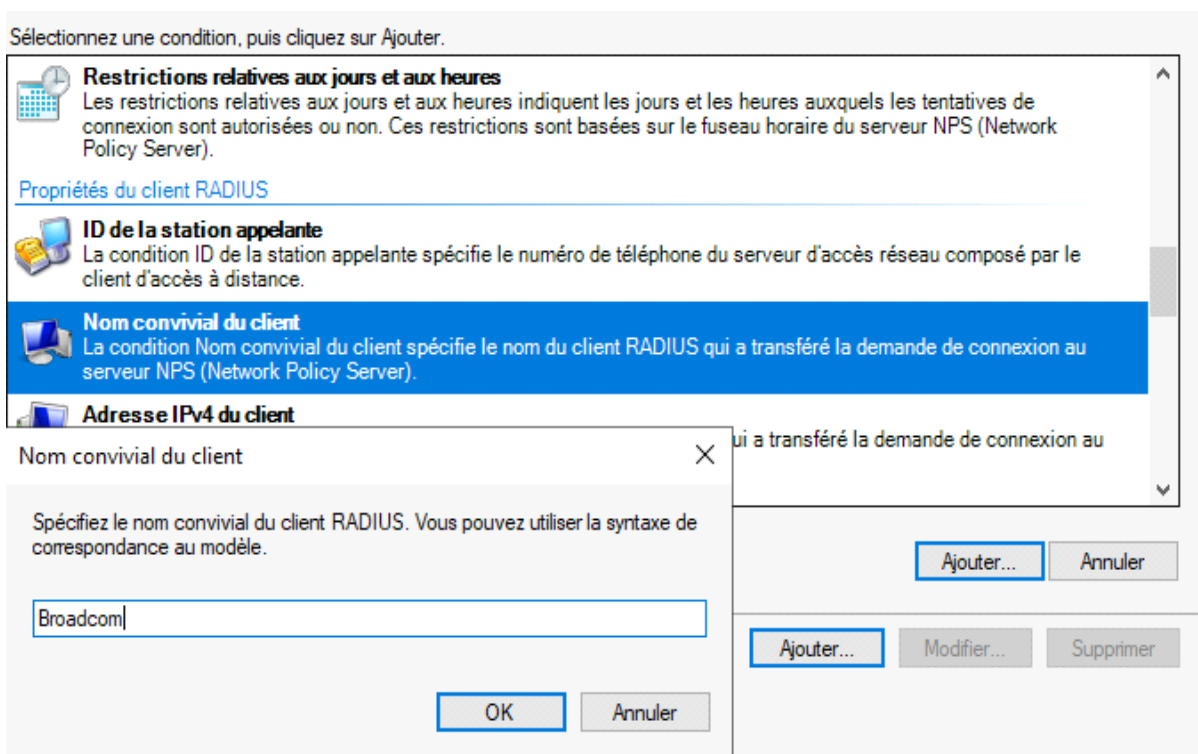
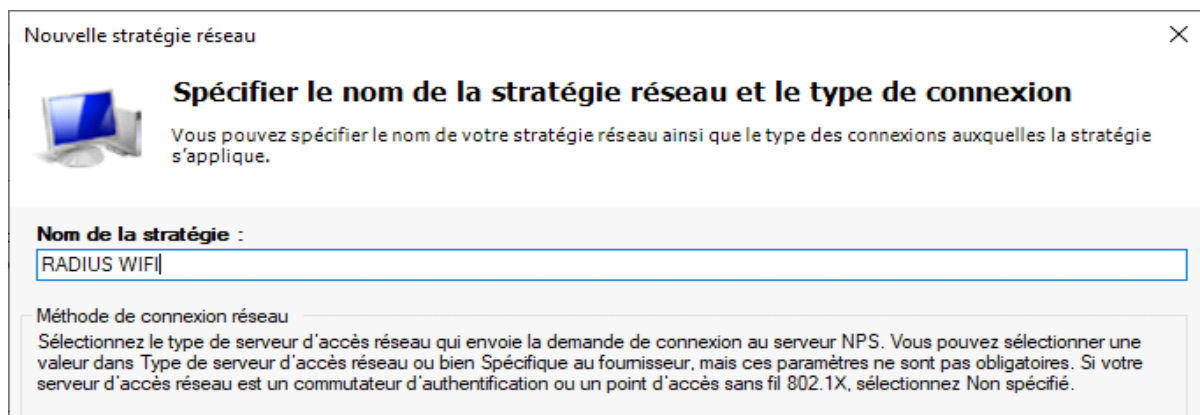


Figure 4.59 Ajout d'une condition de demande au serveur NPS

Maintenant Nous devons spécifier les règles que doivent remplir les utilisateurs pour pouvoir accéder au réseau Wi-Fi donc dans « stratégies de réseaux » clic droit « nouveau »



Nouvelle stratégie réseau

Spécifier le nom de la stratégie réseau et le type de connexion

Vous pouvez spécifier le nom de votre stratégie réseau ainsi que le type des connexions auxquelles la stratégie s'applique.

Nom de la stratégie :
RADIUS WIFI

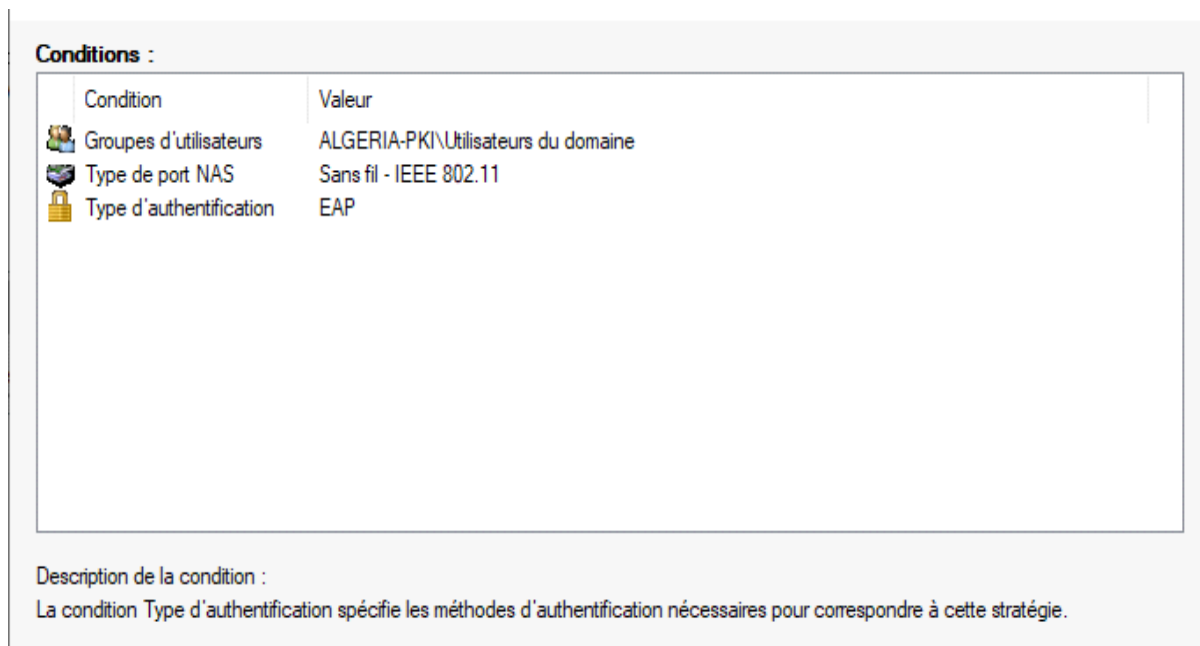
Méthode de connexion réseau
Sélectionnez le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouvez sélectionner une valeur dans Type de serveur d'accès réseau ou bien Spécifique au fournisseur, mais ces paramètres ne sont pas obligatoires. Si votre serveur d'accès réseau est un commutateur d'authentification ou un point d'accès sans fil 802.1X, sélectionnez Non spécifié.

Figure 4.60 Nouvelles stratégie d'accès au réseau

Ici Nous allons sélectionner trois règles :

- Groupe d'utilisateur : « utilisateur de domaine »
- Type de port NAS : « sans fil-IEEE 802.11 »
- Type d'authentifications : « EAP »

Ces règles signifient que l'utilisateur aura accès, seulement s'il fait partie du groupe d'utilisateur « utilisateur de domaine », et qu'il fait une demande de connexion sans fil, et que le type d'authentification est de type « EAP » (certificat).



Conditions :

Condition	Valeur
Groupes d'utilisateurs	ALGERIA-PK\Utilisateurs du domaine
Type de port NAS	Sans fil - IEEE 802.11
Type d'authentification	EAP

Description de la condition :
La condition Type d'authentification spécifie les méthodes d'authentification nécessaires pour correspondre à cette stratégie.

Figure 4.61 Nouvelles conditions d'accès au réseau

Nous accordons ensuite l'accès aux utilisateurs qui respectent ces conditions

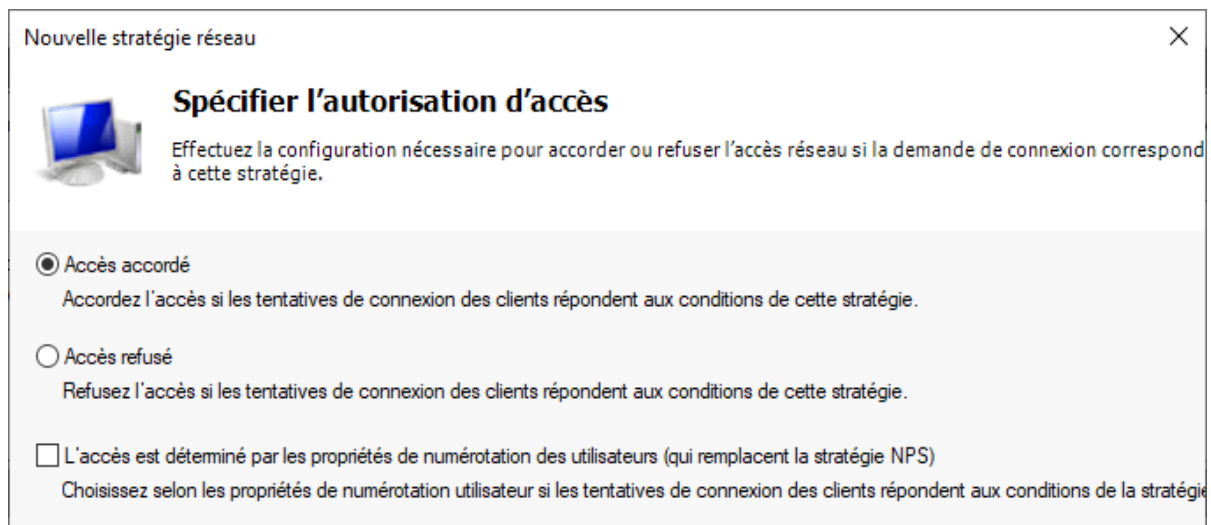


Figure 4.62 Accord d'accès au réseau aux utilisateurs remplissant les conditions

Nous devons maintenant spécifier une méthode d'authentification nous cliquons sur « ajouter » et ont choisi « Microsoft : Carte à puce ou autre certificat »

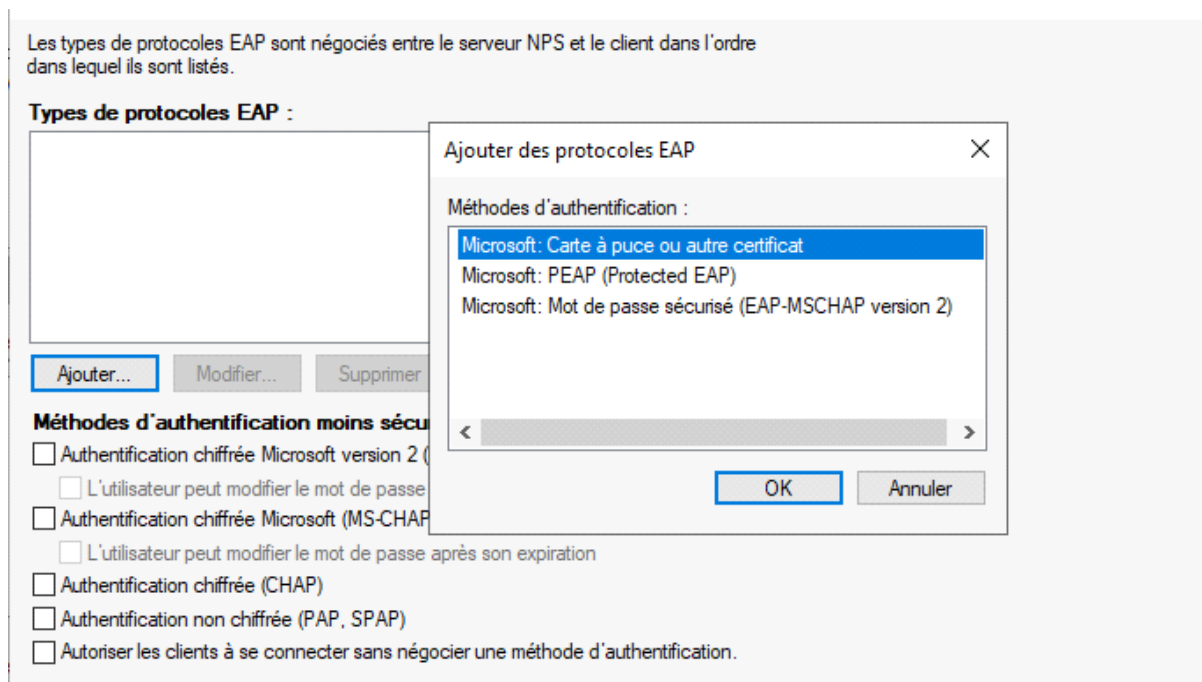


Figure 4.63 Ajout d'un type de protocole d'accès au réseau

Nous devons alors attribuer un certificat au serveur pour qu'il puisse être identifié alors nous double cliquons sur « Microsoft : Carte à puce ou autre certificat » puis "modifier" et Nous sélectionnons le certificat délivré au serveur précédemment.

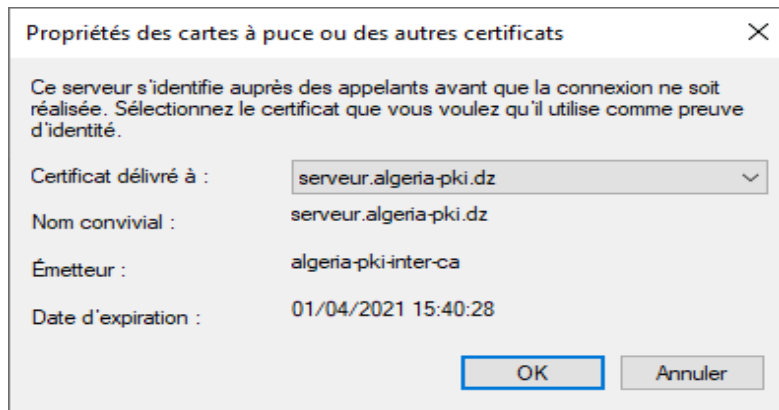


Figure 4.64 Sélection du certificat du serveur utilisé pour son authentification

Voilà la configuration est terminée à ce stade, les autres paramètres restent par défaut.

2.2 Ajout d'utilisateur autorisé

Nous devons ajouter des utilisateurs qui auront accès à notre réseau, pour cela sur le gestionnaire de serveur Nous cliquons sur « outils » puis sur « utilisateurs et ordinateurs active directory ».

Sur la fenêtre qui apparait Nous sélectionnons "users" puis Nous cliquons sur "nouveau" ensuite "utilisateur"

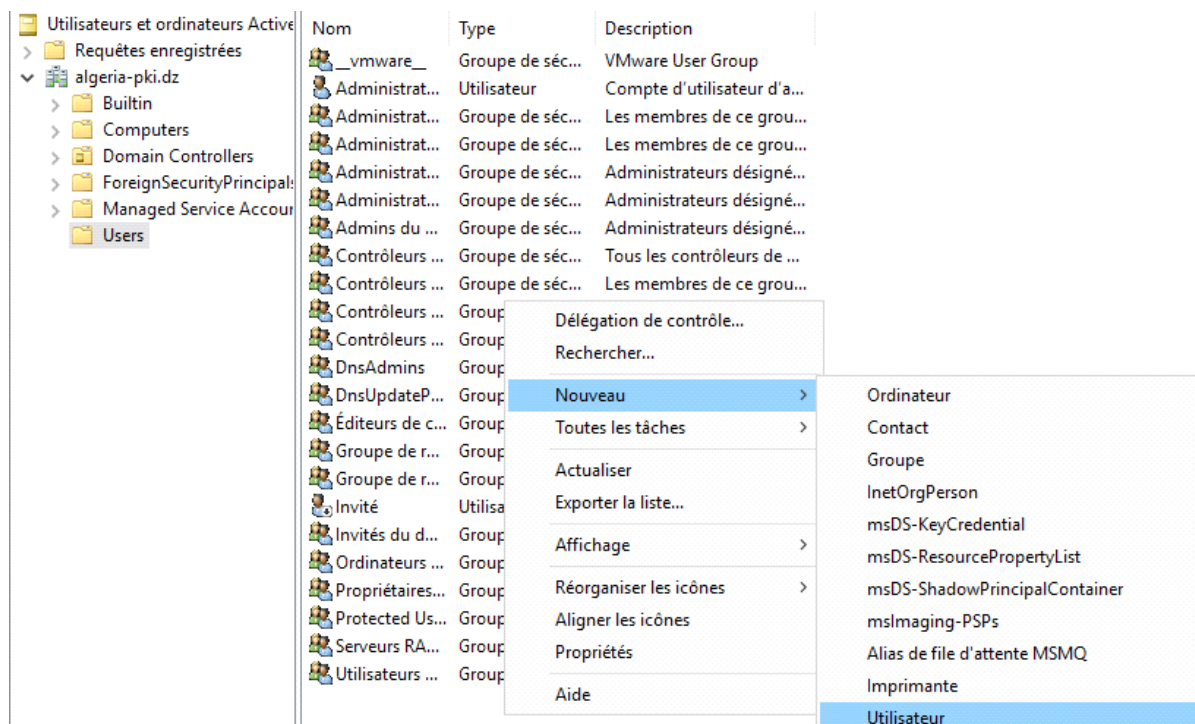


Figure 4.65 Ajout d'un nouvel utilisateur autorisé à se connecter au réseau

Nous introduisons ensuite les informations relatives à l'utilisateur.

Nouvel objet - Utilisateur

Créer dans : algeria-pki.dz/Users

Prénom : REDA2010 Initiales :

Nom :

Nom complet : REDA2010

Nom d'ouverture de session de l'utilisateur :
REDA2010@algeria-pki.dz

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :
ALGERIA-PKI\ REDA2010

< Précédent Suivant > Annuler

Figure 4.66 Information de connexion du nouvel utilisateur

2.3 Configuration du point d'accès et de l'interface réseau client

2.3.1 Configuration du point d'accès

Il faut d'abord se connecter au point d'accès à l'adresse 192.168.15.1.

Nom d'utilisateur et mot de passe par défaut :

admin/admin

Ensuite aller dans Wireless/Security et modifier :

- Network authentication : **WPA2**
- RADIUS server IP : **192.168.15.50**
- RADIUS key : **monrouter** (la clé donner lors de la création du NAS)
- WPA encryptions : **AES**

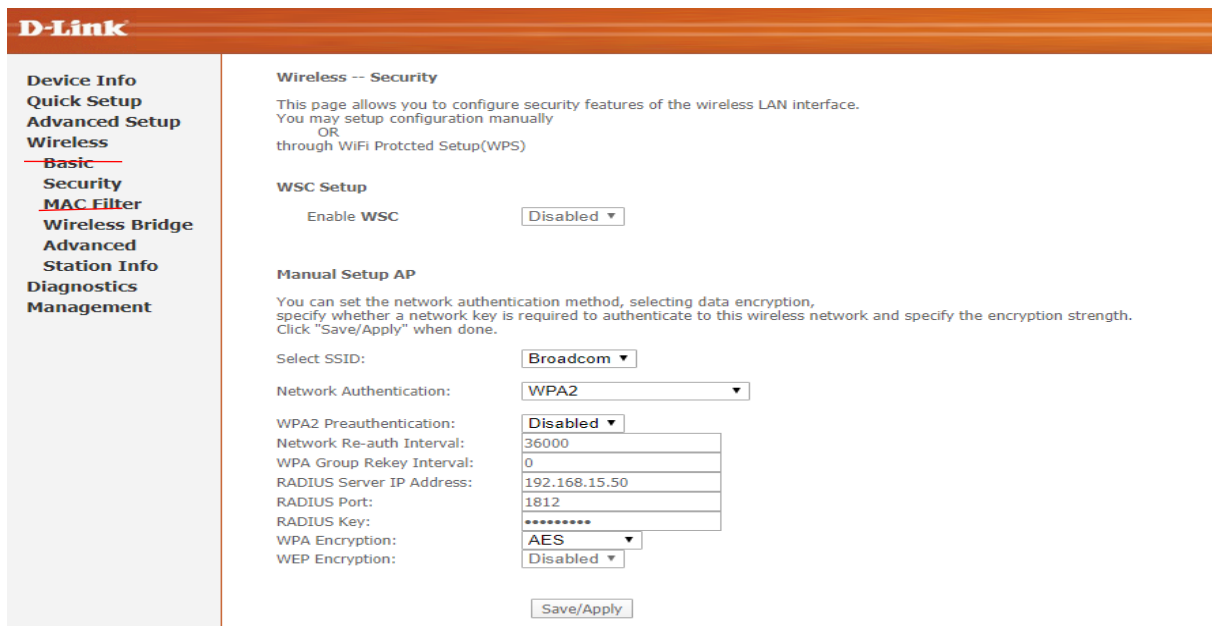


Figure 4.67 Configuration du point d'accès (point d'accès)

2.3.2 Configuration du réseau du client

2.3.2.1 Connexion au domaine

Pour la première étape, il nous faut garder en permanence un lien filaire avec le modem pour obtenir un certificat qui nous permettra d'accéder au réseau sans fil.

Pour cela Nous accédons à la machine de l'utilisateur.

Informations système générales

Édition Windows

Windows 10 Professionnel

© 2019 Microsoft Corporation. Tous droits réservés.



Système

Processeur : Intel(R) Core(TM) i5-4460 CPU @ 3.20GHz 3.20 GHz

Mémoire installée (RAM) : 8,00 Go

Type du système : Système d'exploitation 64 bits, processeur x64

Stylet et fonction tactile : La fonctionnalité d'entrée tactile ou avec un stylet n'est pas disponible sur cet écran.

Paramètres de nom d'ordinateur, de domaine et de groupe de travail

Nom de l'ordinateur : REDA

Nom complet : REDA

Description de l'ordinateur :

Domaine : WORKGROUP



Figure 4.68 Machine utilisateur

Nous devons nous connecter au domaine « algeria-pki.dz » grâce au compte utilisateur créé au préalable par l'administrateur, pour se faire nous répétons l'opération que nous avons faite avec le « **server0** » pour la CA racine.

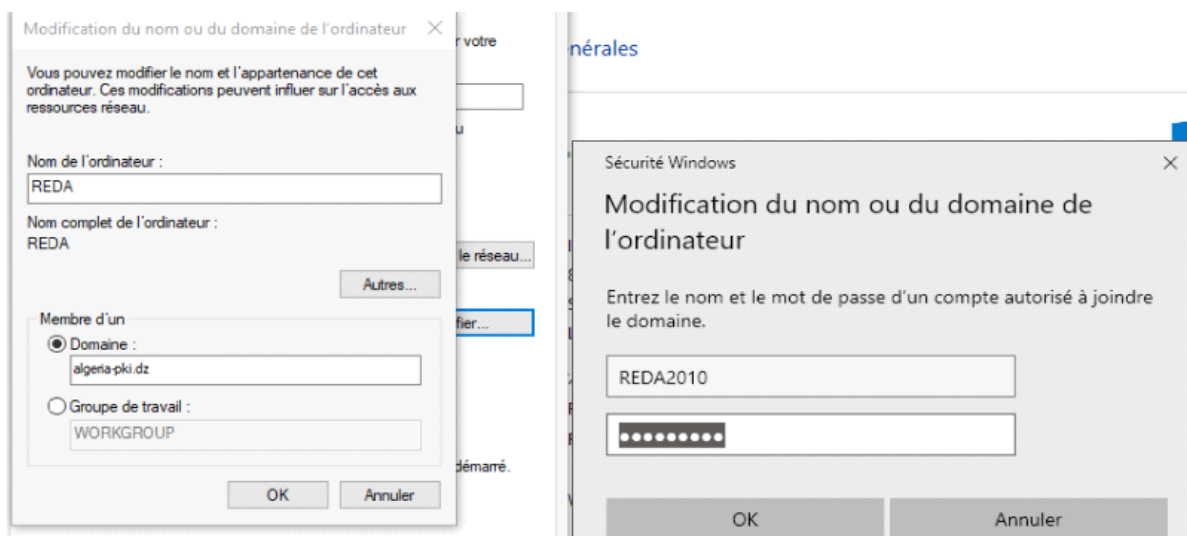


Figure 4.69 Connexion de l'utilisateur au domaine

Nous nous assurons que l'opération a été faite avec succès puis Nous redémarrons le système et Nous nous connectons avec le compte lié au domaine.

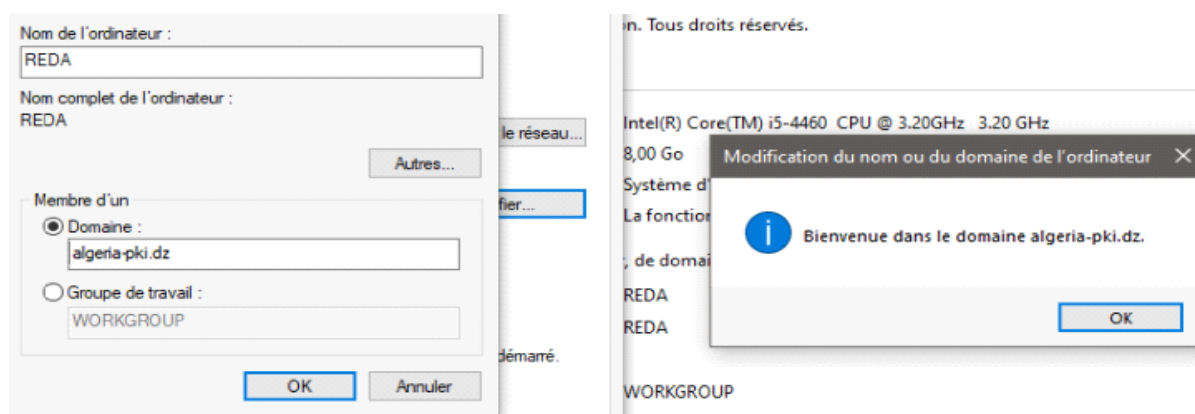


Figure 4.70 Connexion au domaine réussi

L'ordinateur va alors redémarrer et Nous devons nous connecter avec nos nouveaux identifiant

« **REDA2010** ».

2.3.2.2 Obtention d'un certificat utilisateur

Nous devons alors obtenir un certificat de la part du serveur « server » Nous ouvrons la console **mmc** comme montrer précédemment mais cette fois si Nous ajoutons un compte utilisateur

Nous sélectionnons « certificats », puis « ajouter », ensuite Nous cochons « un compte d'utilisateur ».

Nous déroulons ensuite « personnel », puis Nous faisons un clic droit sur « certificats », ensuite « toutes les tâches », et « demander un nouveau certificat ». Nous sélectionnons le type de certificat : « utilisateur » et nous appuyons sur « inscription »

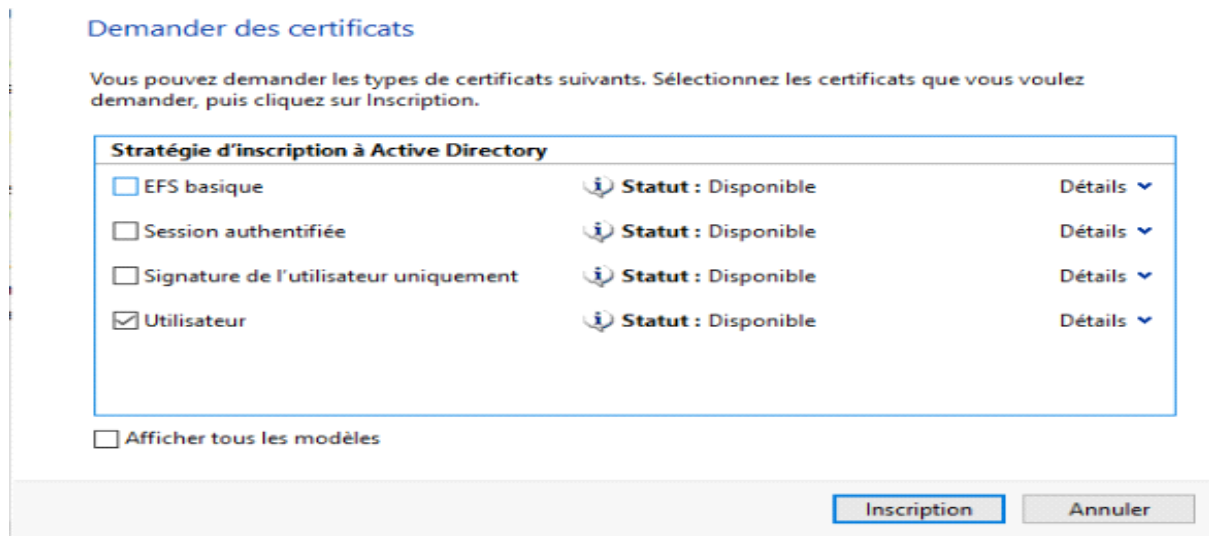


Figure 4.71 Demande de certificat utilisateur

Une fois le Certificat obtenu, nous n'avons à présent plus besoin d'une connexion filaire avec le modem.

2.3.2.3 Configuration du Wi-Fi

Pour nous connecter au réseau Wi-Fi, Nous aurons besoin de configurer manuellement la connexion sans fil, car pour un souci de sécurité nous avons caché le SSID du modem.

Pour cela Nous ouvrons le « centre réseau et partage » et Nous cliquons sur « configurer une nouvelle connexion ou un nouveau réseau » et Nous sélectionnons « se connecter manuellement à un réseau sans fil ».

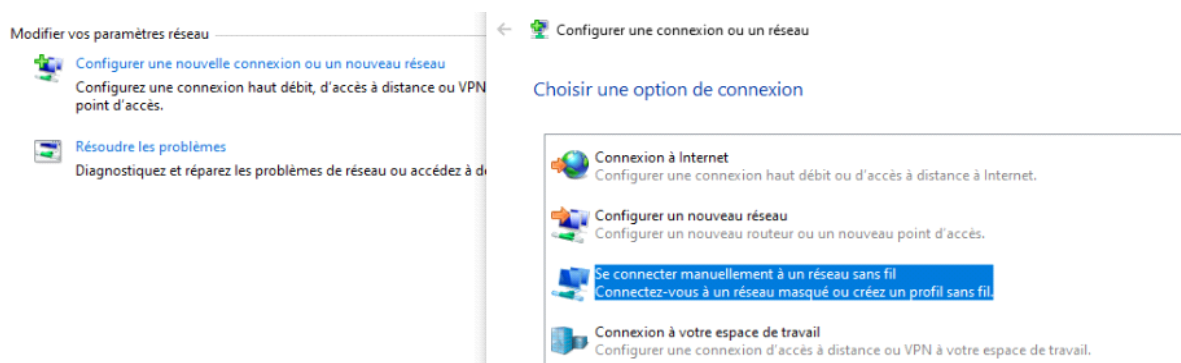


Figure 4.72 Configuration d'une nouvelle connexion sans fil

Nom du réseau (Broadcom) et type de sécurité « **wpa2-entreprise** » puis suivant.

Nous cliquons sur « modifier les paramètres de connexion ».

Dans l'onglet « sécurité » Nous sélectionnons la méthode d'authentification « carte à puce ou autre certificat ».Puis sur « paramètre avancés » Nous cochons la case « spécifier le mode d'authentification » et Nous sélectionnons « authentification utilisateur ».

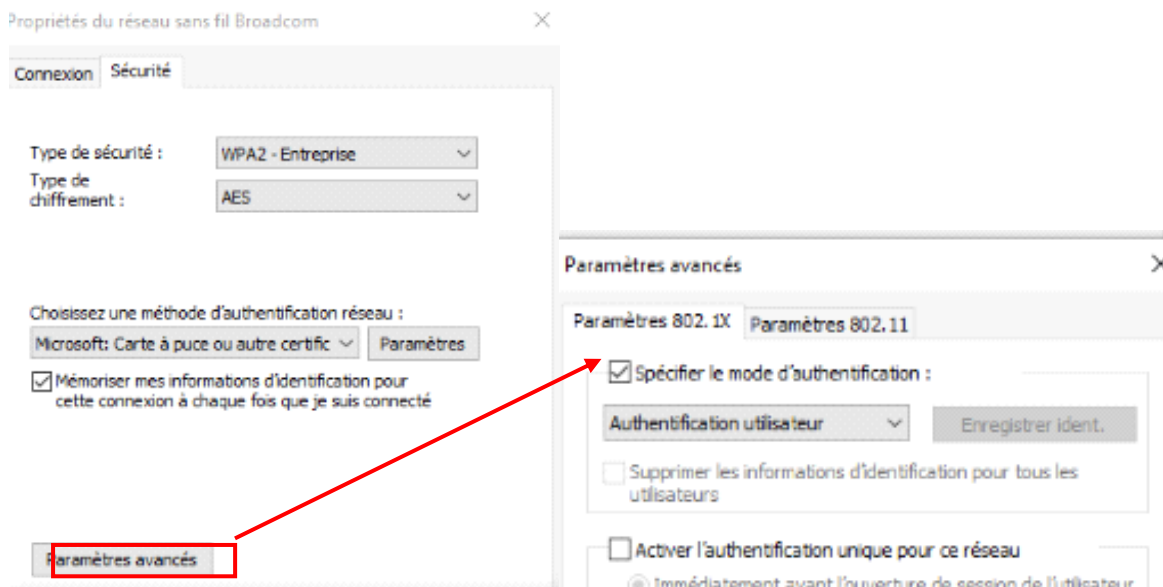


Figure 4.73 Sélection de la méthode d'authentification

2.4 Test d'authentification d'un utilisateur

Maintenant que toutes les modifications sont faites, Nous allons tenter de nous connecter et voir que le serveur nous accorde bel et bien l'accès au Wi-Fi, l'utilisateur arrive à se connecter au réseau Broadcom.

[Afficher les informations de base de votre réseau et configurer des connexions](#)

Afficher vos réseaux actifs

Réseau non identifié
Réseau public


Type d'accès : Pas d'accès réseau
Connexions :  Wi-Fi 20 (Broadcom)

Figure 4.74 Connexion réussie au réseau

Sur le serveur NPS pour vérifier que l'utilisateur a bien reçu l'accès Nous ouvrons « l'observateur d'événement » Nous déroulons « Rôles de serveur » et Nous faisons double clic sur « services de stratégies... »

Nous lisons très clairement que le serveur NPS a accordé l'accès à l'utilisateur

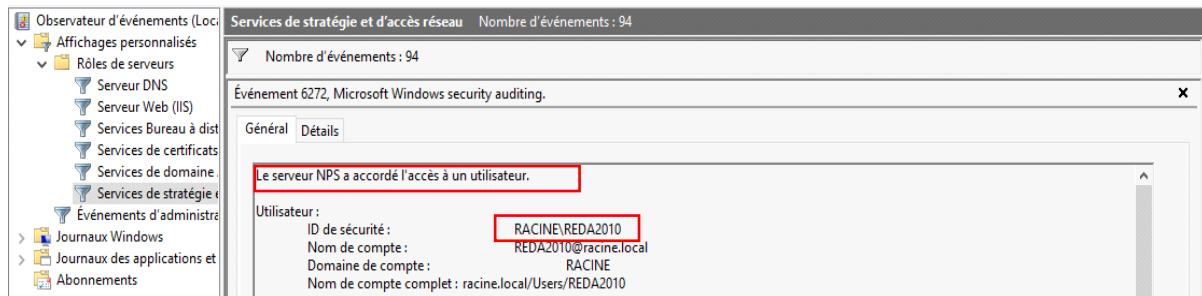


Figure 4.75 Accès accordé à l'utilisateur

3. Mise en place d'un serveur Mail sécurisé

3.1 Installation et configuration d'un serveur Mail

En premier lieu Nous devons télécharger « **MailEnable** » ce dernier est un serveur de messagerie disponible sur Windows et distribué par MailEnable Pty Ltd.

Après installation (tous les paramètres sont par défaut) pour accéder à notre serveur de messagerie Nous cliquons sur le menu démarrer puis Nous cherchons « MailEnable ».



Figure 4.76 Console de configuration de MailEnable

Nous déroulons le menu « servers » puis « local host » ensuite « services and connectors » et Nous faisons clic droit sur « smtp » puis Nous sélectionnons « propriété »

Dans l'onglet « General » nous remplissons les informations concernant le nom de domaine ainsi que l'adresse IP du serveur.

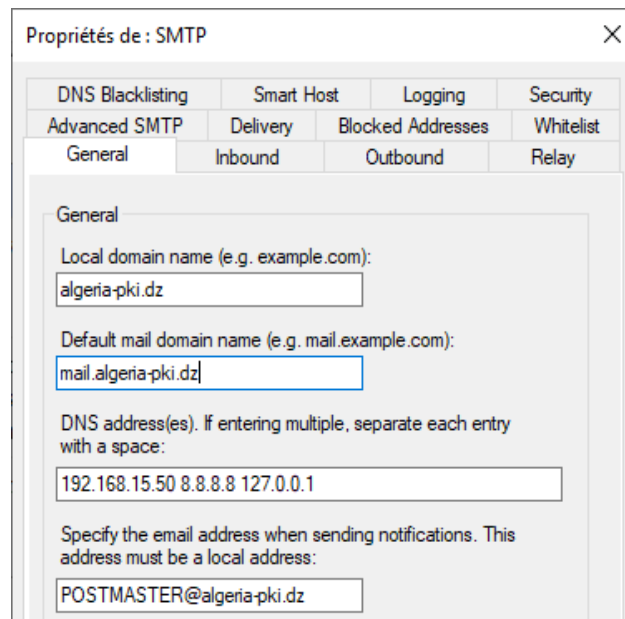


Figure 4.77 Configuration de MailEnable

Nous faisons un redémarrage pour que les changements soient pris en compte, pour cela Nous nous dirigeons vers « Localhost » puis « System », ensuite « service status », et Nous cliquons sur « restart all services ... »

Il nous faut maintenant ajouter des boîte email (des utilisateurs) Nous déroulons alors « Messaging Manager » depuis la console puis « Post Offices » jusqu'à « Mailboxes », un clic droit sur « Mailboxes » puis Nous sélectionnons « new Mailboxes... »

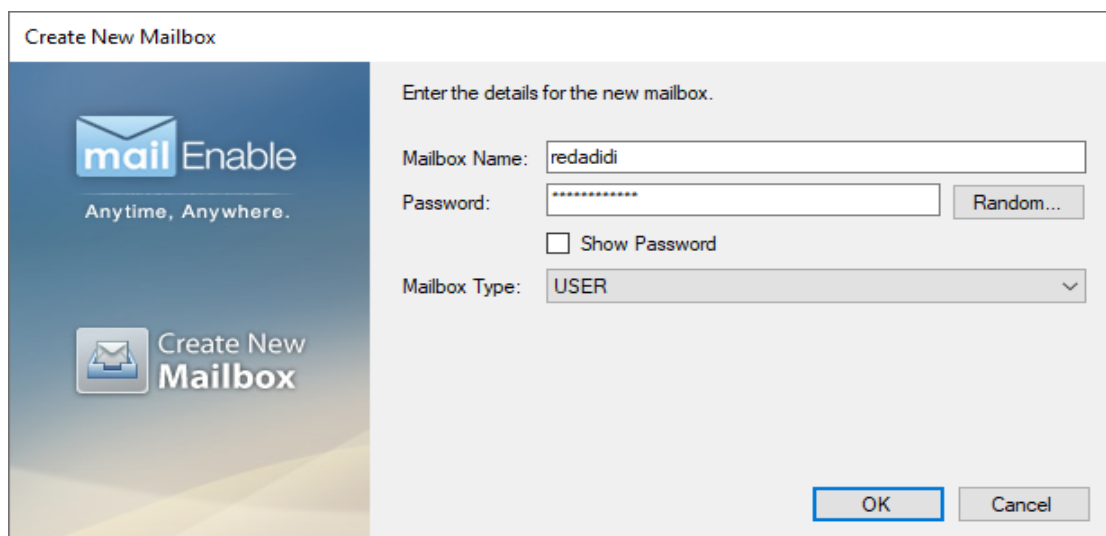


Figure 4.78 Ajout d'une nouvelle boîte mail (utilisateur)

Nous rentrons l'identifiant et le mot de passe de ce dernier et OK.

NOTE : l'utilisateur aura la possibilité de changer son mot de passe ultérieurement.

3.2 Test du serveur mail MailEnable

Nous accédons au serveur messagerie depuis notre site IIS dans laquelle nous avons placé les fichiers du serveur mail au préalable.

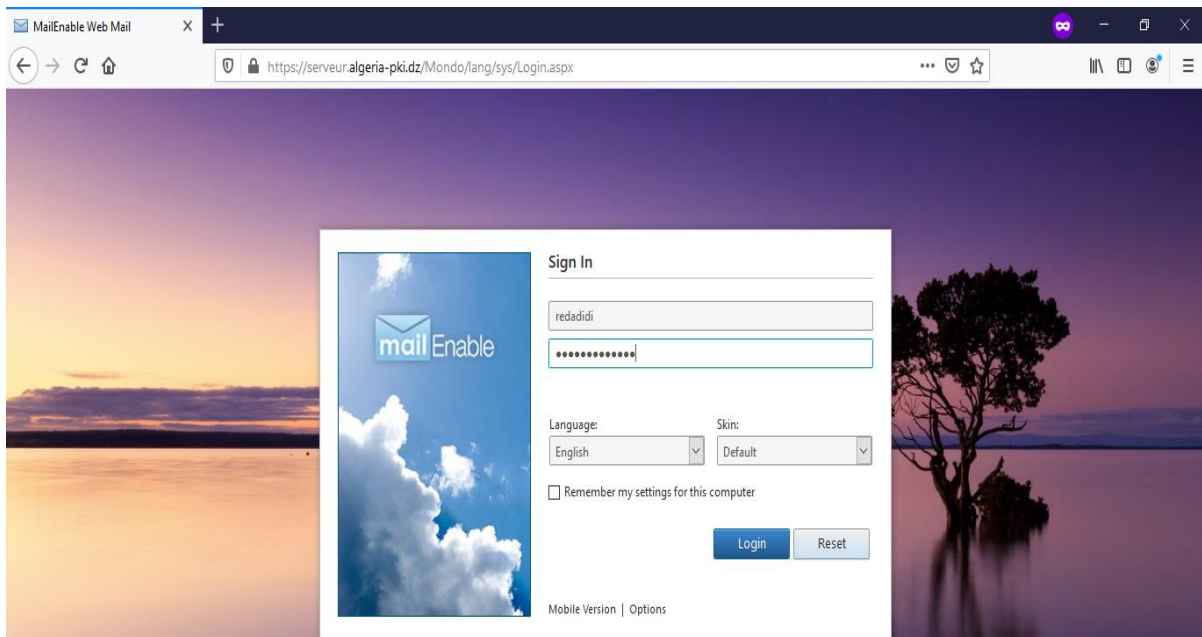


Figure 4.79 Connexion à la boîte mail

Nous nous identifions avec notre login et mot de passe et Nous aurons accès à notre boîte mail.

Nous envoyons un message de test à l'utilisateur « **karimslj** » de la part de « **redadidi** » pour vérifier si notre serveur est correctement configuré.

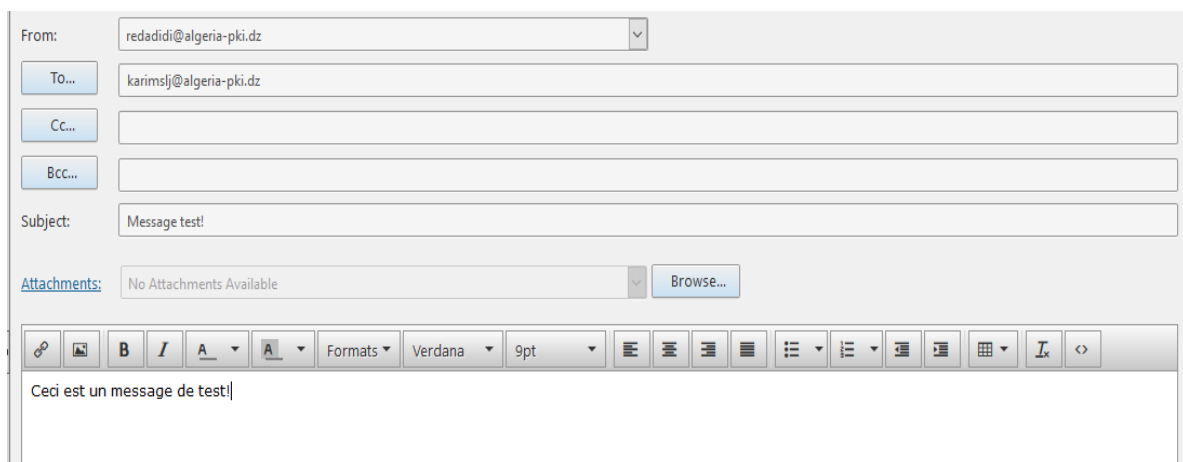


Figure 4.80 Envoie d'email de la part du redadidi vers un karimslj

Puis Nous nous connectons avec le compte de « **karimslj** » pour voir si le message a bel et bien été délivrée.

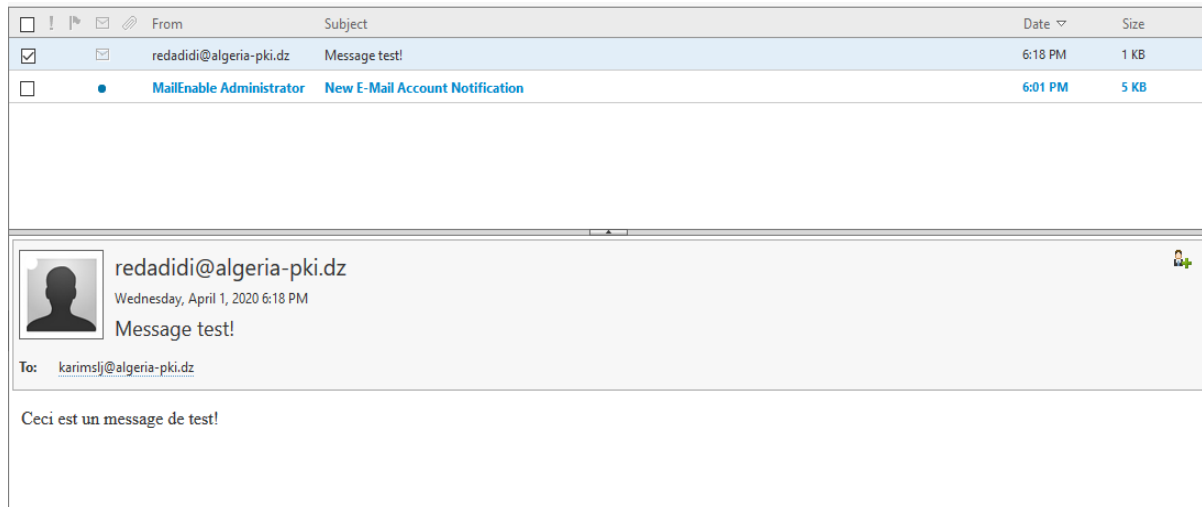


Figure 4.81 Réception de l'email de redadidi par karimslj

L'email à bien été reçu notre serveur mail est opérationnel et prêt à être utilisé.

IV. Conclusion

Dans ce chapitre, nous avons donc montré les étapes d'installation et configuration d'une PKI, des serveurs web, mail, DNS, Active Directory, d'utilisateurs autorisés, du serveur d'authentification Radius, le tout est testé pour mettre en évidence l'efficacité de l'utilisation des certificats. Les problèmes que nous avons rencontrés dès le début, c'est le fait que Windows exige d'avoir deux CA une root et une autre secondaire dans deux serveurs différents. Pour renforcer la sécurité, dans le cas où la CA secondaire est corrompu l'autre CA prend le relais, et nous évitons ainsi que la PKI ne soit hors usage. Pour résoudre ce problème, nous avons dû installer une machine virtuelle simulant ainsi un deuxième serveur ou nous avons installé la CA primaire. La deuxième chose qu'il faut noter c'est l'interface graphique du Windows Server qui facilite grandement les installations et quelques configurations sont automatiques, cependant il faut toutefois connaître les différents protocoles, les différentes techniques et autres méthodes d'authentifications existantes, pour faire le bon choix lors des installations. La troisième chose sur laquelle nous attirons l'attention, c'est que le mode « commandes » sur terminal de Linux est bien évidemment conseillé et privilégié au mode graphique, moins sûr. Il est bien plus difficile de corrompre la PKI en mode « Commandes », qu'en mode graphique.

Conclusion générale

Conclusion générale

Dans ce travail, nous nous sommes intéressés à un des plus importants aspects sécuritaires d'un réseau informatique, qui est le contrôle d'accès aux ressources du réseau, comme l'accès aux serveurs Web, Mail....

Surtout l'accès aux ressources d'un réseau sans fil Wifi, type de réseau très plébiscité, aussi bien par les utilisateurs particuliers, que par les entreprises, du fait de la grande mobilité qu'il fournit.

Cependant le sans-fil malgré son côté pratique, a un gros problème de facilité de pénétrations et d'intrusion par des personne non autorisé.

Et généralement les attaques les plus craintes par les entreprises du Net, sont les attaques DOS, le spoofing, l'hameçonnage, qui mettent hors usage les ressources du réseau ou des serveurs, créant des pertes considérables de profit, et font perdre aux entreprises des données accumulées pendant des années, ou récupèrent vos données sensibles avec une facilité déconcertante.

Donc il est primordial de sécuriser son réseau, son système d'information, ses serveurs contre les accès non autorisés, dans un but de nuire intentionnellement ou pas.

L'authentification par mot de passe, a montré quelques limites, comme l'oubli des mots de passe trop nombreux et trop longs et complexes, ou subtilisés par des méthodes de social engineering, ou craqué par l'attaque du dictionnaire ou la force brute, etc.

Et alors est apparue l'utilisation des certificats qui se sont montrés beaucoup plus robustes et impossibles à subtiliser que le mot de passe.

Cela évite plusieurs attaques types, comme le spoofing, et le brute force, néanmoins cela ne remplacera jamais les mots de passe qui grâce à ça facilité d'implémentation restera toujours le moyen le plus rependue.

L'utilisation des clés publiques, à grande échelle et sur un grand réseau tel que Internet, passe nécessairement par le déploiement de PKI privée ou publique pouvant être payante, comme « VERISIGN » très utilisé par les serveurs de vente en ligne(e-commerce), des organismes gouvernementaux, et autres institutions.

Nous nous sommes posé comme objectif, de déployer notre propre PKI, dans notre Intranet, et l'utiliser pour sécuriser l'accès à notre serveur Web, puis Mail et enfin à notre réseau d'entreprise.

Pour se faire, nous l'avons fait sous Linux, en mode « Commandes » et sous Windows via le logiciel Windows Server, qui est interfacé graphiquement et très complet.

Malgré les difficultés rencontrées, surtout à cause du fait qu'il faut avoir une grande maîtrise de toutes les techniques (protocoles) existantes, cela nous a poussés à approfondir nos connaissances et à s'attaquer au thème de la sécurité qui est très vaste.

Ce travail nous a poussé à améliorer notre maîtrise de la sécurité, sécurité essentielle à tout réseau informatique, suite aux nouvelles attaques que les hackers s'ingénient à mettre au point, et coupables de beaucoup de pertes financières, de faillites, de mise hors usage de centaines d'ordinateurs et de pertes de données sensibles ou de leur vol.

Les nombreux tests tels que les tentatives d'accès non autorisé, bloqué avec succès et la vérification du chiffrement par TLS version 1.2, démontrent l'atteinte de notre objectif.

En perspectives, nous nous proposons de tester plus en avant notre PKI contre des intrusions ou des attaques DOS.

ANNEXE : Présentation de Windows

Server et Debian

Windows Server est un système d'exploitation pour serveur créé par Microsoft.

Basé sur l'architecture Windows NT, il fournit toutes les capacités, fonctionnalités des mécanismes de fonctionnement d'un OS pour serveur standard.

Il propose ainsi différents services orientés serveur, comme la possibilité d'héberger un site web, des boîtes mail, un serveur DNS, une CA,...La gestion des ressources entre les différents utilisateurs et applications, ainsi que des fonctionnalités de messagerie et de sécurité.

Il est compatible avec la plupart des langages de programmation web et systèmes de bases de données comme .NET Core, ASP.NET, PHP, MySQL et MS SQL.[13]

Et une version d'essai est disponible gratuitement.[14]

Annexe 1 Qu'est-ce que Windows Server ?

Debian est un système d'exploitation GNU/Linux présentant deux caractéristiques principales :

C'est la distribution libre qui offre le plus de stabilité pour les outils GNU et le noyau Linux.

C'est une distribution non commerciale suffisamment crédible pour concurrencer les distributions commerciales ;

GNU/Linux Debian est également un système d'exploitation multi-plates-formes.

Il supporte douze architectures et ses milliers de paquets couvrent presque tous les matériels existants et des domaines d'application imaginables. [15]

Nous allons utiliser pour notre démonstration Debian-Desktop v 10.3.0. [16]

Annexe 2 Qu'est-ce que Debian ?

Linux et Windows sont des systèmes d'exploitation très puissants et adaptés à l'hébergement Web.

Linux est un logiciel basé sur UNIX et il flexible, évolutif et abordable, plus apprécié car il est open source et disponible gratuitement.

Avec Windows, il y a des frais de licence que nous devons payer pour chaque version.

Windows est compatible avec la plupart des principaux systèmes d'exploitation, mais nous ne pouvons pas exécuter Linux sur la plupart des technologies Windows de manière transparente.

Si notre site Web a été conçu sur Microsoft ASP.net, avec des technologies MSSQL, nous sommes obligés d'utiliser les serveurs Windows car Linux ne prend pas en charge ces technologies.

Une comparaison entre les deux systèmes a été faite et résumé dans le tableau ci-dessous.

Mais d'abord définissons ce qu'ils sont.

Linux	Windows Server
Linux est un système d'exploitation open source qui s'articule autour du noyau Linux.	Windows Server est essentiellement un produit Microsoft.
Dans le cas de Linux, il s'agit d'une combinaison de formes, appelée distribution Linux à la fois pour les ordinateurs et les serveurs. Il est principalement centré sur le noyau Linux	Dans le cas du serveur Windows, il s'agit d'un ensemble de systèmes d'exploitation créé par Microsoft et l'architecture de base est mise en couches en mode utilisateur et en mode noyau.
Linux est principalement basé sur le mode de fonctionnement en ligne de commande	Les serveurs Windows utilisent l'interface graphique pour implémenter des opérations
Il existe également un support communautaire pour Linux et ses utilisateurs.	Bien que cela soit coûteux, ils fournissent une plus grande gamme de support communautaire. Normalement, toutes les versions de serveur utilisé pour fournir un support client à long terme

Tableau 2 Linux et Windows Server les différences [17]

Linux et Windows sont stables, bien que Windows ne soit pas aussi flexible que Linux, mais Windows est beaucoup plus facile pour l'intégration d'applications. Windows est convivial.

Nous n'avons pas eu besoin d'écrire de nombreux codes, comme nous l'avons fait sous Linux, qui autrement peuvent être gérés en quelques clics.

Annexe 3 Différence entre Linux et Windows Server

Privacy Enhanced Mail (PEM) :

Format texte. Données codées en base 64 avec lignes d'en-tête et de pied de page. Format préféré dans Openssl et la plupart des logiciels basés sur lui (par exemple Apache mod_ssl, stunnel). [18]

Distinguished Encoding Rules (DER) :

Format binaire. Format préféré dans les environnements Windows. Également le format officiel pour le téléchargement sur Internet des certificats et des CRL. [19]

Annexe 4 Formats de fichier des certificats

BIBLIOGRAPHIE

BIBLIOGRAPHIE

- [1] J. F. Carpentier, *La sécurité informatique dans la petite entreprise : état de l'art et bonnes pratiques*. Editions ENI, 2009.
- [2] « Sécuriser ses données, un enjeu majeur pour les cabinets comptables ». <https://www.numen.expert/fr/vos-enjeux/securiser-vos-donnees/#> (consulté le fév. 10, 2020).
- [3] D. Godart, *Sécurité informatique : risques, stratégies et solutions : échec au cyber-roi*. Edipro, 2002.
- [4] D. Godart, *Sécurité informatique : risques, stratégies et solutions : échec au cyber-roi*. Edipro, 2002.
- [5] « Comment protéger sa vie privée ? - L'Esprit Sorcier - Dossier #31 | Education & Numérique », *Scoop.it*. <https://www.scoop.it/topic/agora/p/4095513698/2018/03/14/comment-protoger-sa-vie-privee-l-esprit-sorcier-dossier-31> (consulté le fév. 10, 2020).
- [6] G. RIBIÈRE, *Certification Electronique*. Ed. Techniques Ingénieur.
- [7] ACISSI., *Sécurité informatique - Ethical Hacking : Apprendre l'attaque pour mieux se défendre*. Editions ENI, 2009.
- [8] C. Pernet, *Sécurité et espionnage informatique : Connaissance de la menace APT (Advanced Persistent Threat) et du cyberespionnage*. Eyrolles, 2015.
- [9] S. Reguigui, *Les déploiements d'infrastructure à clé publique à grande échelle*. 2003.
- [10] « Certificats X509 v3 - cryptosec ». <https://www.cryptosec.org/?Certificats-X509-v3> (consulté le fév. 10, 2020).
- [11] C. Adams et S. Lloyd, *Understanding PKI : Concepts, Standards, and Deployment Considerations*. Addison-Wesley, 2003.
- [12] J. Viega, M. Messier, et P. Chandra, *Network Security with OpenSSL : Cryptography for Secure Communications*. O'Reilly Media, 2002.
- [13] N. Bonnet, *Windows Server 2019 : Le déploiement*. linkedin.com, 2019.

- [14] « Try Windows Server 2019 on Microsoft Evaluation Center ».
<https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2019?filetype=ISO>
(consulté le jan. 2, 2020).
- [15] « Debian -- À propos de Debian ». <https://www.debian.org/intro/about> (consulté le avr. 10, 2020).
- [16] « Debian sur CD et DVD ». <https://www.debian.org/CD/> (consulté le jan. 2, 2020).
- [17] E. Bradford et L. Mauget, *Linux and Windows Interoperability Guide*. Prentice Hall PTR, 2002.
- [18] J. Linn, « Privacy Enhancement for Internet Electronic Mail : Part I : Message Encryption and Authentication Procedures ». <https://tools.ietf.org/html/rfc1421> (consulté le fév. 10, 2020).
- [19] « ISO/IEC 8825-1:2002 », ISO.
<https://www.iso.org/cms/render/live/en/sites/isoorg/contents/data/standard/03/56/35688.html> (consulté le fév. 28, 2020).