IN/003-151/03.

République algérienne démocratique et populaire
Ministère de L'enseignement supérieur et de la recherche scientifique

Université Abou Bekr Belkaid — جامعة أبي بكر بلقايد

تلمسان الجزائر

Faculté des sciences
Département d'informatique

Mémoire pour l'Obtention du Diplôme
d'ingénieur d'état en informatique
Option : système d'information

Thème :

L'utilisation de RADIUS sous Windows Server 2008 pour sécuriser un réseau sans fil 802.11

Présenté par

Bouchikhi Mohamed El Amin
Derfouf Hicham

Encadré par

Mme DIDI Fedoua

Soutenu le 24 octobre 2011 Devant le Jury composé de

Mme Iles Nawel — *Présidente*

Mr Benmammar Badreddine — *Examinateur*

TABLE DES MATIERES

TABLE DES MATIERES

TABLE DES MATIERES

TABLE DES MATIERES

Introduction générale

Ces dernières années, les technologies sans fil ont connu un essor considérable que se soit au niveau commercial ou dans le domaine de la recherche, ceci revient aux multiples avantages qu'elles offrent (mobilité, faible coûts, etc.). Mais, comparer aux interfaces filaires, peu nombreuses sont les interfaces sans fil qui offrent un débit rapide (ondes hertziennes, l'infrarouge).

Les réseaux sans fil ont été créés pour permettre aux utilisateurs d'effectuer des communications de telle sorte, à garder la connectivité des équipements, tout en ayant la mobilité et sans avoir recours aux câbles utilisés dans les réseaux traditionnels et qui encombrent ces derniers.

Il existe plusieurs technologies pour les réseaux sans fil se distinguant d'une part par la fréquence d'émission utilisée ainsi que le débit et la portée des transmissions (Bluetooth, Zigbee, Hiperlan, Wi-Fi qui est l'objet de ce mémoire), leur arrivée a soulevée un engouement nouveau pour les réseaux radio qui étaient jusqu'alors le domaine exclusif des militaires.

La sécurité des réseaux sans fil s'étant considérablement développée dans l'espace des technologies de l'information au cours des dix dernières années, le Wi-Fi constitue désormais une solution viable pour les applications d'acquisition de données. Comme il utilise l'air comme média physique, le Wi-Fi présente des risques de sécurité spécifiques qui dépassent les risques intrinsèques aux systèmes filaires. Il est donc nécessaire de mettre en place les dispositions nécessaires de telle manière à assurer une confidentialité des données circulant sur les réseaux sans fil. Chose à laquelle on va s'attaquer dans ce PFE, dans le but de choisir la méthode la plus aboutie jusqu'à ce jour et la mettre en œuvre sur un réseau test.

Introduction

Les réseaux sans fil rencontrent aujourd'hui un succès important car ils permettent, via la norme IEEE1 802.11b, dite Wi-Fi, de déployer des moyens de transmissions sans contrainte d'immobilité liée aux câblages et aux prises (hormis l'alimentation). La promotion actuelle de ce type de solution, est uniquement axée sur les avantages qu'elle procure : facilité et rapidité d'installation, cout inférieur à un système filaire, mobilité, accès partagé à des services de haut débit – Internet. Toute fois, les induits par la gestion des risques associés sont bien souvent omis.

Bien que la norme 802.11b présente certaines options de sécurité, les protections des réseaux Wi-Fi restent faibles, même vis-à-vis d'attaques simples. La nature du signal transmis (onde électromagnétique) rend difficile, voire impossible la maitrise complète de la propagation. En conséquence, il est assez facile d'écouter les messages et même de s'introduire sur de tels réseaux, à l'insu des utilisateurs et de l'opérateur, pour y accomplir des actes malveillants sans laisser de trace. La disponibilité publique, la gratuité et la facilité de mise en œuvre des outils de localisation, d'interception passive et d'agression confirment l'importance de cette menace.

Ce document présente d'une part une analyse des différents types de risques, menaces, et attaques auxquels les réseaux Wi-Fi sont exposés, et d'autre part une série de conseils permettant à leurs administrateurs et usagers de mieux contrôler et si possible réduire les risques. Ces conseils concernent les questions de déploiement, de protection physique ou protection logique du réseau. Ils peuvent aider à mettre en place un réseau sécurisé (action à priori), ou à sécuriser physiquement ou logiquement un réseau déjà existant (action à posteriori).

I. Risques, Menaces et Attaques

I.1 Les risques

Les risques dépendent des paramètres que l'on peut maitriser.

Contrairement au réseau câblé, le contrôle des accès physique au réseau sans fil est difficile, voir impossible.

Il existe deux types de risques :

- Le risque structurel : dépend de l'organisation de l'entreprise.
- Le risque accidentel : indépendant de tous les facteurs de l'entreprise.

Et quatre niveaux de risque :

- Acceptables : pas de conséquences graves pour les utilisateurs de réseau ;

Exemple : panne électrique, perte de liaison...

- Courants : pas de préjudices graves au réseau, on répare facilement ;

  Exemple : gestion du réseau, mauvaise configuration, erreur utilisateur...

- Majeurs : dus à des facteurs graves et qui causent de gros dégâts mais récupérables ;

  Exemple : foudre qui tombe sur un routeur...

- Inacceptables : fatals pour l'entreprise, ils peuvent entrainer son dépôt de bilan ;

  Exemple : perte ou corruption des informations importantes... [1]

I.2 Les menaces

Ceux sont les résultantes d'actions et d'opérations du fait d'autrui. Il existe deux catégories :

- Passives : atteinte à la confidentialité (prélèvement par copie, écoute de l'information sur les voies de communication) souvent indétectable.
- Actives : nuisent à l'intégrité des données (brouillage, déguisement (se faire passer pour quelqu'un d'autre), interposition (vol de session)). [1]

I.3 Les attaques

Le réseau d'entreprise reste vulnérable à de nombreuses attaques potentielles, ces attaques peuvent compromettre la fiabilité des données de l'entreprise et donc réduire sa crédibilité.

Les ondes radio, le réseau d'entreprise et l'ordinateur client sans fil constituent les trois failles potentielles de la sécurité.

I.3.1 Attaques radio

Les faiblesses du WEP permettent aux pirates de contourner le chiffrement des données transmises sans fil. Ils peuvent espionner passivement le contenu des messages ou analyser le trafic d'un réseau WLAN en vue d'attaques futures. Ces intrus peuvent également lancer des attaques actives, par exemple en rediffusant ou en modifiant des messages. Le déversement massif d'ondes parasites sur un point d'accès sans fil est une autre attaque courante. Le pirate peut alors installer un point d'accès factice et détourner les systèmes de communications en se faisant passer pour une ressource légitime.

I.3.2 Attaques visant le réseau d'entreprise

Les réseaux WLAN représentent une double menace pour les ressources légitimes de l'entreprise. Tout d'abord, les faiblesses des mécanismes d'authentification permettent à

tout intrus non autorisé de pénétrer aisément le réseau de l'entreprise et d'accéder à ses ressources.

Ensuite, la plupart des implémentations sans fil ne contrôlent que très peu l'accès entre le segment du réseau sans fil et le réseau câblé. Les pirates peuvent donc diriger tout le trafic voulu vers les ressources de l'entreprise. Comparés à une passerelle Internet, les points d'accès sans fil ne cherchent quasiment pas, voir pas du tout, à détecter et à se protéger contre le trafic malveillant

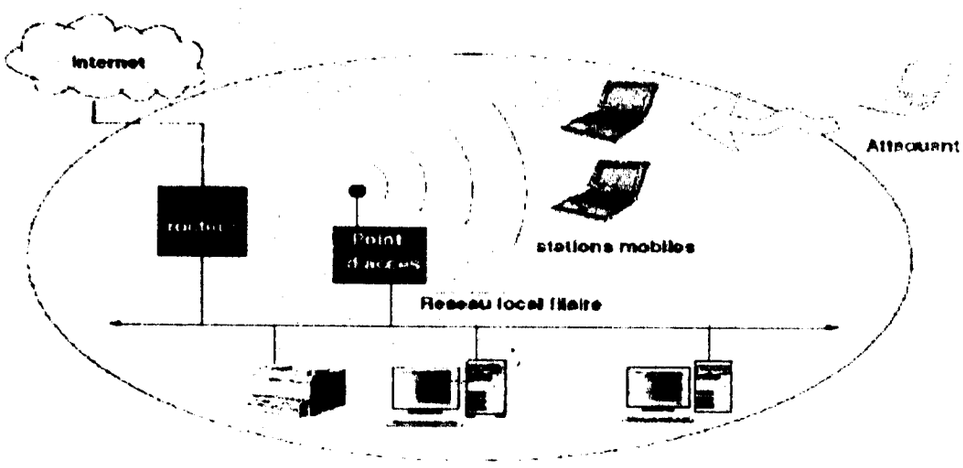


FIGURE1.1 : Attaques visant le réseau d'entreprise

I.3.3 Attaques visant les ordinateurs clients

Bien que les clients sans fil soient situés à l'extérieur du pare-feu de l'entreprise, plusieurs d'architectures réseau les traitent comme des clients internes. Les pirates peuvent alors compromettre des clients individuels, en les utilisant pour collecter des informations ou comme des tunnels d'entrée vers le réseau de l'entreprise. En mode 802.11 « ad-hoc », les ordinateurs clients sont autorisés à se connecter directement entre eux - ouvrant ainsi un véritable boulevard aux pirates. [2]

I.3.4 Attaques par TCP

Le protocole TCP utilise des numéros de ports qui permettent de déterminer une adresse de socket, c'est-à-dire un point d'accès au réseau. Cette adresse de socket est obtenue par la concaténation de l'adresse IP et de l'adresse de port. Une attaque par TCP revient à utiliser un point d'accès pour faire autre chose que ce dont le point d'accès a été défini. En particulier, un pirate peut utiliser un port classique pour entrer dans un ordinateur ou dans le réseau d'une entreprise. [3]

I.3.5 Attaques par cheval de Troie

Les chevaux de Troie ("Trojan horses" ou "Trojans" en anglais) tirent leur nom de la célèbre légende mythologique. Comme dans cette dernière, les troyens utilisent une ruse pour agir de façon invisible, le plus souvent en se greffant sur un programme anodin. Ils font partie des grandes menaces que l'on peut rencontrer sur le web, parmi les virus et autres vers. Pourtant, contrairement à ceux-ci.

Les chevaux de Troie ne se reproduisent pas (en tout cas, ce n'est pas leur objectif premier). Ce sont à la base de simples programmes destinés à être exécutés à l'insu de l'utilisateur.

Leur objectif est le plus souvent d'ouvrir une porte dérobée ("backdoor") sur le système cible, permettant par la suite à l'attaquant de revenir à loisir épier, collecter des données, les corrompre, contrôler voire même détruire le système. Certains chevaux de Troie sont d'ailleurs tellement évolués qu'ils sont devenus de véritables outils de prise en main et d'administration à distance. [3]

I.3.6 Attaque par dictionnaire

C'est une méthode utilisée pour trouver un mot de passe ou une clé. Elle consiste à tester une série de mot de passe potentiel, les uns à la suite des autres en espèrent que le mot de passe utilisé pour le chiffrement soit contenu dans le dictionnaire. Si tel n'est pas le cas l'attaque échouera. [4]

I.3.7 Attaque par force brute

L'attaque par force brute est une méthode utilisée en cryptanalyse pour trouver un mot de passe ou une clé. Il s'agit de tester, une à une, toutes les combinaisons possibles. Cette méthode de recherche exhaustive ne réussit que dans les cas où le mot de passe cherché est constitué de peu de caractères. Ces programmes tentent toutes les possibilités de mot de passe dans un ordre aléatoire afin de berner les logiciels de sécurité qui empêchent de tenter tous les mots de passe dans l'ordre.

Pour contrer cette méthode, il suffit simplement de choisir des mots de passe d'une grande longueur ou des clés suffisamment grandes. Ainsi, l'attaquant devra mettre beaucoup de temps pour trouver le bon mot de passe. Cette méthode est très sensible aux capacités de calcul des machines effectuant l'algorithme.

Cette méthode est souvent combinée avec l'attaque par dictionnaire et par table arc-en-ciel pour obtenir de meilleurs résultats.

Elle n'est pas une attaque à proprement parler car elle se contente de définir le plus petit temps qu'il faudra pour trouver le secret. Cette méthode étant applicable à n'importe quel

algorithme, lui donner le titre d'attaque signifierait que tous les protocoles sont attaqués et donc non fiables. Il s'agit donc d'un abus de langage fréquent. [4]

II. Service de sécurité

Les services de sécurité représentent les logiciels et matériels mettant en œuvre des mécanismes dans le but de mettre à la disposition des utilisateurs les fonctions de sécurité dont ils ont besoin.

II.1 Authentification

L'authentification a pour but de garantir l'identité des correspondants.

D'après le dictionnaire de l'informatique, l'authentification est l'opération par laquelle le destinataire et/ou l'émetteur d'un message s'assure(nt) de l'identité de son interlocuteur.

La norme 802.11 initiale spécifie deux modes d'authentification : ouvert ou partagé **(open** ou **shared).**

L'authentification ouverte signifie l'absence d'authentification et l'authentification partagée signifie l'utilisation d'un secret partagé, en l'occurrence une clef WEP dans un mécanisme challenge/réponse. Il est vite apparu que ce mode d'authentification était très largement insuffisant, induisant même une dégradation du chiffrement par l'intermédiaire du challenge/réponse donnant de la matière à des attaques cryptographiques. [5]

II.1.a Les protocoles

Un protocole d'authentification est un moyen de contrôle d'accès caractérisé par les trois A **(AAA)** : Authentication (authentification), Authorization (autorisation), Accounting (rapport).

Les protocoles d'authentification utilisent différentes manières d'authentifier un utilisateur ou une machine. Il existe différents algorithmes, différentes techniques, mais tous, dans un souci de sécurité utilisant le principe de chiffrement qui est à base de clés.

Il existe quatre principaux protocoles d'authentification.

II.1.a.1 PAP (Password Authentication Protocol)

Le protocole PAP est, comme son nom l'indique, basé sur l'authentification par mot de passe. Les mots de passe sont envoyés en clair sur le réseau, ce qui représente un danger important. PAP est un protocole d'autorisation d'accès pour l'ouverture d'une session sur le réseau. Il est de moins en moins utilisé au profit de CHAP.

II.1.a.2 CHAP (Challenge-Handshake Authentication Protocol)

Le protocole CHAP est basé sur le mode d'authentification "Défi-Réponse". Le serveur d'authentification envoie un identifiant au hasard, c'est le défi. Le client transforme le défi avec sa clé et l'algorithme MD5 puis le renvoie au serveur : c'est la réponse. Le serveur applique le même algorithme avec la clé du client, compare les deux résultats puis accorde ou rejette la connexion. Ce processus de défi-réponse peut être répété à tout moment pendant la connexion, ce qui le rend relativement sécurisé.

II.1.a.3 TACACS (Terminal Access Controller Access Control System)

TACACS est le plus ancien des protocoles d'authentification. Il a été récemment actualisé dans une nouvelle variante appelée TACACS+. TACACS supporte plusieurs types d'authentification : l'authentification dite classique avec nom d'utilisateur/mot de passe complétée par l'utilisation des challenges. Le mécanisme d'authentification donne la possibilité, après la transaction du login (nom d'utilisateur) et du mot de passe, de vérifier son identité en lui posant un certain nombre de questions.

II.1.a.4 RADIUS (Remote Authentication Dial-In User Service)

Le protocole **RADIUS** (Remote Authentication Dial-In User Service), mis au point initialement par Livingston, est un protocole d'authentification standard, qui fonctionne selon le mode Client/serveur.

Un point d'accès (routeur, switch, serveur) fonctionne comme un client RADIUS qui effectue des requêtes sur le serveur. Le standard RADIUS est basé sur un ensemble d'attributs relatifs aux utilisateurs mais beaucoup d'implémentations spécifiques du protocole apportent leur propre jeu d'attributs. De plus, toutes les transactions RADIUS entre le client et le serveur sont protégées par un secret partagé qui n'est jamais transmis sur le réseau, ce qui représente une sécurité supplémentaire.

➢ **Fonctionnement de RADIUS**

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

- Un utilisateur envoie une requête au NAS afin d'autoriser une connexion à distance ;
- Le NAS achemine la demande au serveur RADIUS ;
- Le serveur RADIUS consulte la base de données d'identification afin de connaître le type de scénario d'identification demandé pour l'utilisateur. Soit le scénario actuel convient, soit une autre méthode d'identification est demandée à l'utilisateur.

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

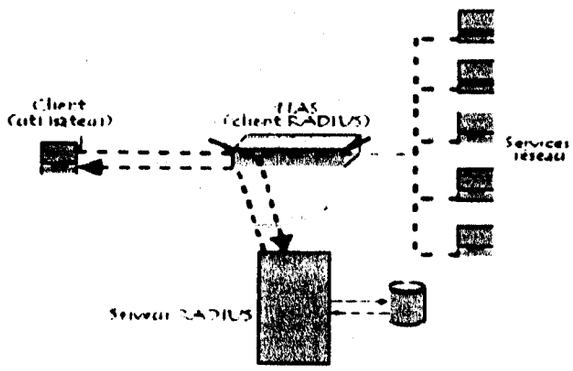


FIGURE 1.2: Le schéma suivant récapitule les éléments entrant en jeu dans un système utilisant un serveur RADIUS

Tous ces protocoles permettent l'authentification sur un réseau filaire mais le degré de sécurité sur un réseau sans fil, doit être encore supérieur. C'est pourquoi il est nécessaire de crypter les données. [6]

II.2 Le contrôle d'accès

Il empêche l'utilisation (lecture, écriture, création, suppression) non autorisée des ressources (utilise l'authentification). [1]

II.3 Intégrité des données

Dans certains cas, il peut être nécessaire d'assurer simplement que les données sont intègres, c'est à dire qu'elles n'ont pas été au passage falsifiées par un intrus. Ces données restent "claires", au sens où elles ne sont pas secrètes.

II.4 La non-répudiation

Elle fournit au récepteur/émetteur une preuve qui empêche l'émetteur/récepteur de l'envoi du message. [1]

II.5 Confidentialité

Le service de confidentialité garantit aux deux entités communicantes à être les seules à pouvoir comprendre les données échangées. Ceci implique la mise en œuvre d'algorithmes de chiffrement en mode flux, c'est-à-dire octet par octet, ou en mode bloc. Un message écrit en clair est transformé en un message chiffré, appelé « *cryptogramme* » grâce aux algorithmes de chiffrement. Cette transformation est fondée sur une ou plusieurs clés.

II.5.a Chiffrements

II.5.a.1 Le chiffrement symétrique

Le chiffrement symétrique (aussi appelé chiffrement à clé privée ou chiffrement à clé secrète) consiste à utiliser la même clé pour le chiffrement et le déchiffrement. C'est le plus facile à comprendre, c'est aussi la méthode de chiffrement la plus facile à réaliser et qui consomme le moins de ressources de calcul et de bande passante.

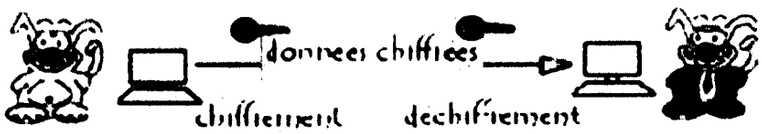


FIGURE1.3 : Chiffrement symétrique

Les deux hôtes qui doivent échanger des données confidentielles (secrètes) disposent tous deux d'une clé identique. L'émetteur chiffre les données avec, puis les envoie au récepteur .Ce dernier déchiffre avec la même clé pour récupérer des données lisibles.

Cette méthode assure la confidentialité des données, celui qui intercepterait la communication ne pourra pas lire les données échangées tant qu'il n'aura pas pu se procurer la clé. Il n'y a aucune authentification de faite sur l'émetteur comme sur le récepteur, sauf si deux personnes seulement disposent de la clé.

Le principal souci avec cette méthode, c'est qu'il faut s'échanger la clé et lors de cet échange, sans précautions particulières, n'importe quoi peut se produire. [6]

II.5.a.2 Le chiffrement asymétrique

Le principe de base de cette méthode et que chaque personne dispose d'un jeu de clés comportant :

- une clé privée : elle est unique et confidentielle, elle appartient exclusivement à l'hôte concerné, il ne la distribue à personne, aucun double de cette clé ne doit être créé,

➢ Une clé publique : elle est unique également, mais tout le monde peut s'en procurer une copie, il suffit d'aller la chercher chez un dépositaire, dit "tiers de confiance"(c'est un organisme de réputation sérieuse, à qui l'on confiera sa clé publique). Il s'agit en quelque sorte d'un concierge qui garde ces clés publiques et certifie qu'elles appartiennent bien à la personne indiquée.

Ce qui est chiffré avec une clé publique ne peut être déchiffré qu'avec la clé privée correspondante, Ce qui est chiffré avec la clé privée ne peut être déchiffré qu'avec la clé publique correspondante. [6]

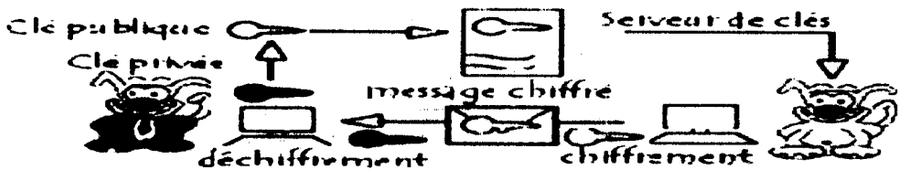


FIGURE1.4 : Chiffrement asymétrique

II.5.a.3 Les algorithmes de chiffrement

- **DES (Data Encryption Standard) :** 1977, à clés symétriques, le plus connu des algorithmes de chiffrement. Pour chaque bloc de 64 bits, le DES produit un bloc chiffré de 64 bits. La clé de longueur de 56 bits, est complétée par un octet de détection d'erreur. De cette clé de 56 bits, on extrait de manière déterministe 16 sous clés de 48 bits.

Chacune. À partir de là, la transformation s'effectue par des sommes modulo 2 du bloc à coder et de la sous clé correspondante.

Cet algorithme est très utilisé dans les applications financières. Il est également utilisé dans un chaînage dit par bloc CBC (Cipher Block Chaining).

Il existe de nombreuses variantes de l'algorithme DES, comme triple DES, ou 3DES, qui utilise trois niveaux de chiffrement, ce qui implique une clé de chiffrement sur 168 bits.

- **RC4, RC5** (Ron's Code #4, #5). 1987, à clé symétrique, propriété de la société RSASecurity Inc. Ils utilisent des clés de longueur variable pouvant atteindre 2048 bits et sont destinés à des applications fortement sécurisées. Ils demandent une forte puissance de calcul, qui ne pourrait être maintenue sur un flot continu à haut débit à des niveaux inférieurs de l'architecture.

- **IDEA**.1992, à clés symétriques, développé en Suisse et surtout pour la messagerie Sécurisée.

- **Blowfish.** 1993, à clés symétriques.

- **AES**. 2000, à clés symétriques.

- **RSA**. 1978, à clés asymétriques.
- **Diffie-Hellman.** 1996, à clés asymétriques.
- El **Gamal.** 1997, à clés asymétriques.

La mise en œuvre de ces techniques est difficile lorsque le débit d'une application est important. C'est pour cela que les techniques symétriques et asymétriques sont utilisées conjointement.

Cependant, on recourt à des clés de session, qui ne sont valables que pour une communication déterminée. Les informations de la session sont codées grâce à une clé secrète permettant de réaliser un chiffrement avec beaucoup moins de puissance qu'une clé asymétrique. Uniquement la clé secrète est codée par un algorithme de chiffrement asymétrique pour être envoyée au destinataire.

II.5.b Certificats

Un certificat permet d'associer une clé publique à une entité (une personne, une machine,...) afin d'en assurer la validité. Le certificat est en quelque sorte la carte d'identité de la clé publique, délivré par un organisme appelé *autorité de certification* (souvent notée CA pour *Certification Authority).*

L'autorité de certification est chargée de délivrer les certificats, de leur assigner une date de validité (équivalent à la date limite de péremption des produits alimentaires), ainsi que de révoquer éventuellement des certificats avant cette date en cas de compromission de la clé (ou du propriétaire).

Les certificats sont des petits fichiers divisés en deux parties :

- La partie contenant les informations.
- La partie contenant la signature de l'autorité de certification.

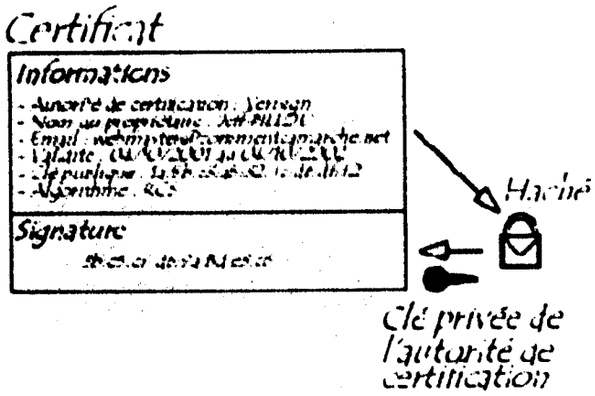


FIGURE 1.5 : Certificats

La structure des certificats est normalisée par le standard X.509 de TUIT (plus exactement X.509v3), qui définit les informations contenues dans le certificat :

- La version de X.509 à laquelle le certificat correspond ;
- Le numéro de série du certificat ;
- L'algorithme de chiffrement utilisé pour signer le certificat ;
- Le nom (DN, pour *Distinguished Name)* de l'autorité de certification émettrice ;
- La date de début de validité du certificat ;
- La date de fin de validité du certificat ;
- L'objet de l'utilisation de la clé publique ;
- La clé publique du propriétaire du certificat ;
- La signature de l'émetteur du certificat (thumbprint).

L'ensemble de ces informations (informations + clé publique du demandeur) est signé par l'autorité de certification, cela signifie qu'une fonction de hachage crée une empreinte de ces informations, puis ce condensé est chiffré à l'aide de la clé privée de l'autorité de certification; la clé publique ayant été préalablement largement diffusée afin de permettre aux utilisateurs de vérifier la signature avec la clé publique de l'autorité de certification. [6]

III. Sécurité du Wi-Fi

Les points d'accès Wi-Fi diffusent les données vers toutes les stations situées dans leur champ d'émission. Du coup, un attaquant peut s'introduire au sein du réseau, récupérer des informations et obtenir l'accès au réseau.

Pour remédier à ce problème, un client doit établir une relation particulière, appelée une association avec un point d'accès.

Pour qu'un client puisse s'associer au point d'accès, il doit passer par les trois états suivants :

- Non authentifié, non associé ;
- Authentifié, non associé ;
- Authentifié, associé.

Le schéma qui suit illustre une machine d'état de l'authentification dans un réseau **802.11.**

Les trames échangées entre le point d'accès et le client peuvent être de deux types, de données ou de gestion (ce sont les trames échanger qui permettent le transite d'un état vers un autre).

Pour sécurisé un réseau sans fil on a besoin des protocoles spécifiques.

Les différents protocoles sont :

III.1 WEP (Wired Equivalent Privacy)

Le WEP est une option proposée dans le standard IEEE 802.11 ratifiée en septembre 1999; en plus de chiffrement, traite de l'authentification et de l'intégrité. Le WEP utilise l'algorithme de chiffrement par flot RC4 pour assurer la confidentialité et la somme de contrôle CRC-32 pour assurer l'intégrité. Il nécessite un secret partagé encore appelé clé.

Le WEP 64 bits utilise une clé de chiffrement de 40 bits à laquelle est concaténé un vecteur d'initialisation ***(initialization vector*** ou IV en anglais) de 24 bits. La clé et le vecteur d'initialisation forment ainsi une clé RC4 de 64 bits permettant de chiffrer les données échangées. Au moment où la norme WEP a été rédigée, les restrictions imposées par le gouvernement des États-Unis d'Amérique sur l'export des moyens cryptographiques limitaient la taille des clés. Une fois ces restrictions retirées, les principaux fabricants étendirent le WEP à 128 bits en utilisant une clé de 104 bits.

Une clé WEP de 128 bits est saisie comme une suite de 13 caractères ASCII ou 26 caractères hexadécimaux. Chaque doublet hexadécimal représente 8 bits de la clé WEP. 8 * 13 = 104 bits. En ajoutant le vecteur d'initialisation (IV) de 24 bits, on obtient ce que l'on appelle « une clé WEP de 128 bits ».

Un mécanisme utilisant des clés WEP de 256 bits est disponible. Comme pour les mécanismes précédemment mentionnés, 24 bits sont réservés pour le vecteur d'initialisation (IV), laissant ainsi 232 bits pour la clé de chiffrement. Cette clé est habituellement saisie comme une suite de 58 symboles hexadécimaux. (58 * 4 = 232 bits) + 24 = 256 bits. Malheureusement, la longueur des clés n'est pas le problème de sécurité le plus sévère du WEP.

Le chiffrement proposé par le protocole WEP s'est révélé rapidement inapte à offrir un niveau de sécurité suffisant pour la plupart des utilisateurs. Parce que RC4 est un algorithme de chiffrement par flot, la même clé ne doit pas être utilisée deux fois pour chiffrer les données échangées. C'est la raison de la présence d'un vecteur d'initialisation (IV). Ce vecteur, transmis sans protection, permet d'éviter la répétition. Cependant, un IV de 24 bits n'est pas assez long pour éviter ce phénomène sur un réseau très actif. De plus, le vecteur d'initialisation est utilisé de telle façon qu'il rend le WEP sensible à une attaque par clé apparentée.

De nombreux systèmes WEP requièrent que la clé soit saisie en hexadécimal. Certains utilisateurs choisissent des clés qui forment des mots avec les symboles 0 à 9 et A à F ; de telles clés peuvent le plus souvent être facilement devinées.

En août 2001, Fluhrer et Al ont publié une analyse cryptologique qui exploite la manière selon laquelle l'algorithme RC4 et l'IV sont utilisés dans le WEP. Cette analyse révèle une attaque passive qui permet de retrouver la clé RC4 après une écoute clandestine du réseau pendant quelques heures. L'attaque a rapidement été implantée et des outils automatisés ont été publiés depuis lors. Il est possible de réaliser ce type d'attaque avec un ordinateur personnel, du matériel courant et des logiciels disponibles gratuitement.

Cam-Winget *et* Al. (2003) ont étudié une série d'imperfections dans le WEP. Ils écrivent : « *Des* expérimentations dans ce domaine indiquent qu'avec un équipement adéquat il est aisé d'espionner des réseaux protégés par du WEP à une distance d'un mile ou plus »). De surcroît, ils rapportent deux faiblesses générales :

- Le WEP est optionnel, de nombreuses installations ne l'ont donc jamais activé;
- Le WEP n'inclut pas un protocole de gestion des clés, le mécanisme se reposant à la place sur une unique clé partagée entre tous les utilisateurs. Ainsi, tout utilisateur peut écouter les autres utilisateurs comme si aucun chiffrement n'était en place.

Depuis juillet 2006, il est possible de pénétrer les réseaux protégés par WEP en quelques secondes seulement, en tirant parti de la fragmentation des paquets pour accélérer le cassage de la clé. [4]

III.2 WPA (Wi-Fi Protected Access)

Comme on l'a vu précédemment, le WEP possède de très nombreuses lacunes en raison de la faiblesse de l'algorithme de cryptage RC4. Ces failles de sécurité ont été résolues par l'émergence d'un nouveau standard: WPA (Wireless Protected Access).

En 2003, la Wi-Fi Alliance a introduit WPA pour faire face à la faiblesse du WEP. WPA utilise l'algorithme de cryptage TKIP (Temporal Key Integrity Protocol) qui permet la génération aléatoire de clés et offre la possibilité de modifier la clé de chiffrement plusieurs fois par secondes, pour plus de sécurité, avec vérification des messages MIC (Message Integrity Check) c'est un code d'intégrité du message, permet de vérifier l'intégrité de la trame, sa mise en place nécessite seulement une mise à jour logicielle des points d'accès et des pilotes de cartes Wi-Fi pour fonctionner.

Le standard WPA définit deux modes distincts :

- **WPA-PSK Mode** : repose sur l'utilisation d'un secret partagé pour l'authentification ;
- **WPA Enterprise Mode** : repose sur l'utilisation d'un serveur RADIUS pour l'authentification

Le mode WPA-PSK est vulnérable à des attaques par dictionnaire. Il est donc très important de choisir un secret (passphrase) fort afin de limiter ces risques. Cependant, en ce qui concerne le chiffrement dans les réseaux sans fil, le WPA apporte un niveau de sécurité supérieur à celui fourni par le WEP. Il permet aujourd'hui de se prémunir contre la plupart des attaques cryptographiques connues contre le protocole de chiffrement WEP.

III.3 WPA2 (Wi-Fi Protected Access 2)

En 2004, la Wi-Fi Alliance a introduit WPA2, la nouvelle génération de la sécurité des réseaux Wi-Fi. WPA et WPA2 assurent une authentification mutuelle entre le client et le serveur d'authentification à travers le point d'accès. WPA et WPA2 font partie de la norme IEEE 802.11i qui assure enfin un cryptage fort et une protection optimale des données sur un réseau Wi-Fi.

WPA2 utilise quant à lui l'algorithme de cryptage CCMP *(Counter-Mode/CBC-MAC Protocol) appelé également AES (Advanced Encryption Standard)* qui nécessite, en raison de sa complexité, une mise à jour matérielle des points d'accès et des adaptateurs Wi-Fi clients. CCMP est une méthode de chiffrement qui gère les clés et l'intégrité des messages. Il s'agit d'une alternative considérée comme plus sûre que TKIP qui est utilisé dans WPA.

III.4 La norme IEEE 802.1X

Le standard 802.1x est une solution de sécurisation, mise au point par IEEE en juin 2001, permettant d'authentifier (identifier) un utilisateur souhaitAnt accéder à un réseau (filaire ou non) grâce à un serveur d'authentification.

Le 802.1x repose sur le protocole **EAP** *(Extensible Authentication Protocol)*, défini par l'IETF, dont le rôle est de transporter les informations d'identification des utilisateurs. [6]

L'équipement d'accès au réseau sans fil (point d'accès) relaie les trames entre le client et le serveur d'authentification (serveur RADIUS), sans connaître le protocole EAP utilisé. Dans le cas où le protocole d'authentification prend en charge la gestion des clés, celles-ci sont transmises à l'équipement d'accès puis au client dans le cadre du chiffrement.

III.4.1 Définition

Le 802.1x porte le nom de « **Port Based Network Access Control** » que l'on peut traduire par « Contrôle d'Accès au Réseau par Port ». Des infrastructures d'authentification, d'autorisation et de comptabilité (AAA) étant déjà en place pour d'autres types de connexions (sortie sur Internet par exemple), il paraissait judicieux de se servir de ces infrastructures.

Le standard présente les caractéristiques suivantes :

- spécifie le protocole entre l'élément voulant accéder au réseau et l'élément connecté au réseau,
- spécifie les conditions requises pour le protocole entre l'élément connecté au réseau et le serveur d'authentification,
- spécifie les opérations de supervision via SNMP (Simple Network Management Protocol).

Chaque élément de l'architecture comporte un nom spécifique :

- Le **Client** (en anglais, supplicant) est l'élément (souvent un ordinateur) qui désire se connecter sur le réseau,
- Le **Point d'Accès** (en anglais, Access Point : AP ou encore Authenticator) est l'élément qui va demander l'authentification,
- Le **Serveur d'Authentification** (en anglais, Authentication Server : AS) est l'élément qui fournit les services d'authentification à l'AP.

Ainsi, la topologie courante de l'architecture est la suivante voir Figure2.7 :

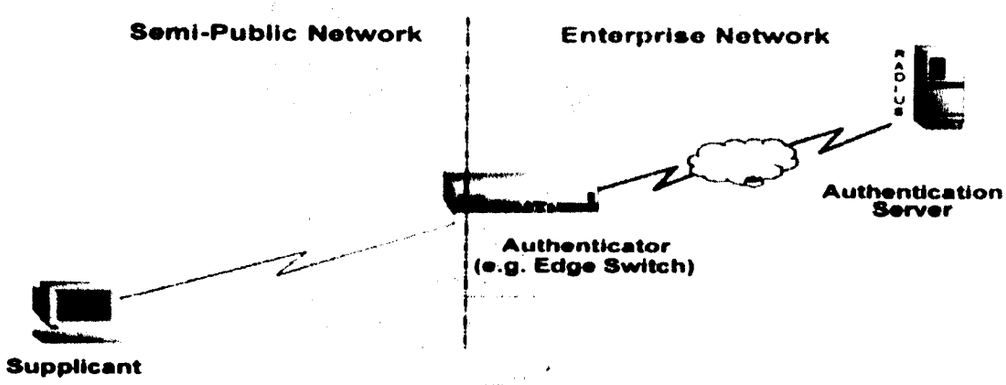


FIGURE 1.7 : Topologie générale d'un réseau 802.1x

La communication entre ces éléments fait intervenir différents protocoles suivant un principe de fonctionnement spécifique.

III.4.2 Principe de fonctionnement

Le mécanisme de l'authentification est complexe. En effet, il ne faut pas autoriser des machines à accéder au réseau tant qu'elles n'ont pas été authentifiées mais il faut quand même autoriser les demandes de connexion et d'authentification. C'est dans cette optique qu'un élément important fut créé sur les points d'accès : le **PAE (Port Access Entity).**

Le PAE est une sorte de port virtuel qui filtre les communications pour ne laisser passer que les demandes d'authentifications ; voir figure 1.8 :

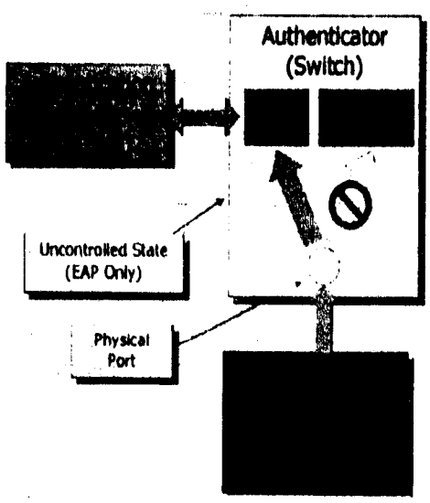


FIGURE 1.8 : Utilisation du PAE

Le point d'accès verrouille les services associés au réseau. Seul le port qui sert à l'authentification est virtuellement ouvert. Le PAE ne laisse alors passer que les paquets EAP. Dès lors que l'authentification aura réussi, le point d'accès déverrouillera les fonctionnalités réseaux. Le PAE restera cependant ouvert pour permettre d'éventuelles demandes de reconnexion ; voir Figure2.9

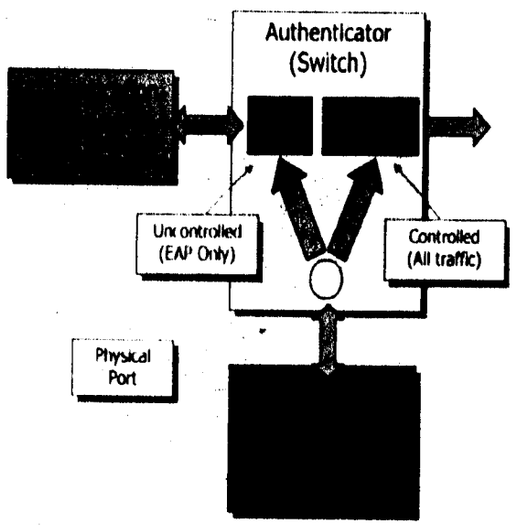


FIGURE 1.9 : Trafic autorisé après une authentification réussie.

Ce procédé implique de faire la différence entre une trame destinée au réseau et une trame correspondant à une demande de connexion. Or, cette différence est prévue dans le protocole EAP. [7]

III.4.3 Le protocole EAP

On retrouve le protocole EAP tout au long de la chaîne d'authentification et à plusieurs niveaux du modèle OSI. [8]

III.4.3.a Composition du paquet EAP

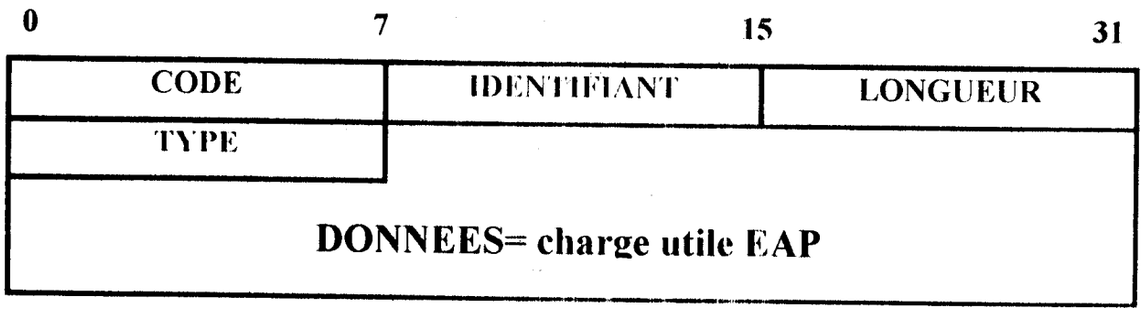


FIGURE1.10 : Paquet EAP

La taille du champ donné est déterminée par le champ code.

Les 4 types de paquet :

Le champ code : Dans l'en-tête du paquet EAP, le champ code correspond au premier octet.

Il en existe 4 types :

- Request : le système authentificateur émet une requête d'information auprès du supplicant.
- Response : le supplicant répond à la requête du système authentificateur.
- Success: le système authentificateur informe le supplicant du succès de la demande d'authentification.
- Failure : le système authentificateur informe le supplicant de l'échec de la demande d'authentification.

Le champ identifiant : Codé sur un octet également, il sert à identifier une session d'authentification. Ce champ change pour chaque nouvelle requête ou réponse. Si une duplication d'une requête doit être faite, l'identifiant ne change pas.

Le champ longueur : Codé sur 2 octets, il indique la longueur de l'ensemble du paquet EAP, il prend donc en compte la longueur des données mais aussi des longueurs des autres champs de l'entête comme le type, le code...

Ainsi on connaitra la taille des données utiles même en cas de bourrage par la couche liaison.

Le champ type : Ce champ est codé sur un octet et définit le type de données que contient le paquet EAP. Logiquement, Requête et réponse possèdent des trames de même type.

Nous allons particulièrement nous intéresser au champ type lors des communications requête/réponse.

III.4.3.b L'encapsulation

Les paquets EAP ne sont pas directement transportables sur les réseaux classiques du type 802. Les paquets EAP sont donc dépendants des couches inférieures du modèle OSI. C'est pourquoi on parle de « EAP over LAN » : **EAPOL** ou « EAP over WLAN » : **EAPOW**. Les variantes EAPOL et EAPOW se situent entre le client et le point d'accès. Entre le point d'accès et le serveur Radius, on parle cette fois de « EAP over RADIUS ».

Donc voici l'installation classique ; voire Figure2.11 :

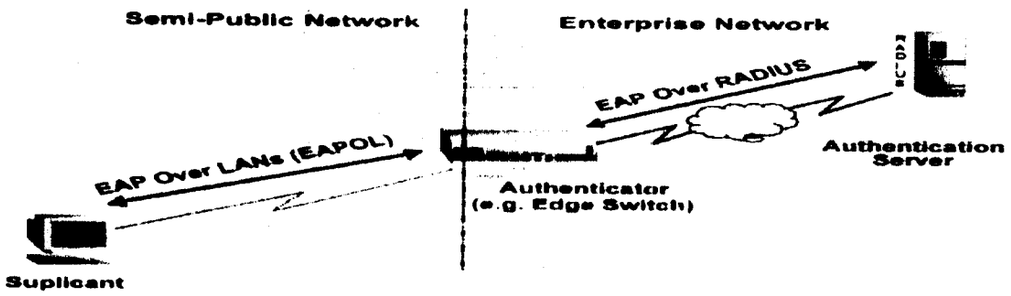


FIGURE 1.11 : Vue générale du protocole EAP

III.4.3.c Mécanismes d'authentification

II existe plusieurs méthodes d'authentification portées par les paquets EAP. Le login de l'utilisateur sera parfois en clair, parfois chiffré comme nous montre la Figure2.12. Ces paquets contiennent aussi la clé WEP dynamique utilisée.

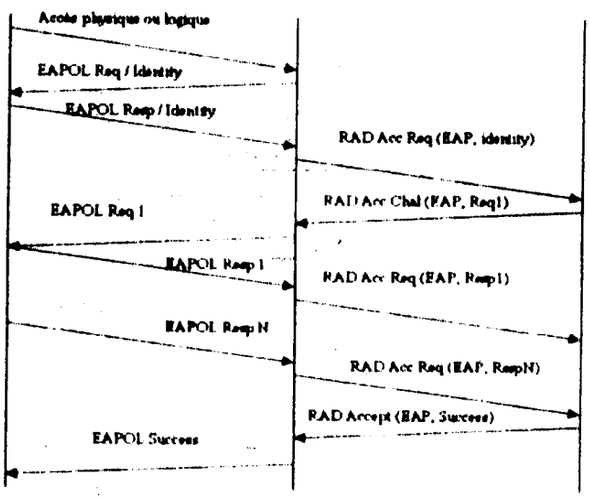


FIGURE1.12 : Mécanismes d'authentification

Dans le cadre de l'authentification en environnement sans fil basée sur le protocole 802.1X, différentes variantes d'EAP sont disponibles aujourd'hui.

Ces principaux mécanismes sont de trois types différents :

- méthode par mot de passe
- méthode par certificats
- méthode par carte à puce ou calculette.

Nous allons décrire les méthodes les plus courantes.

III.4.3.c.1 Méthodes basées sur les mots de passes

- **LEAP** : Lightweight Extensible Authentification Protocol

C'est la méthode la plus utilisée pour les points d'accès. Il gère la distribution dynamique de clés WEP. C'est aussi à la base une solution propriétaire de Cisco (CISCO-EAP) mais qui a aussi été implémentée par la suite par d'autres constructeurs.

- **EAP - MD5:** EAP-Message Digest 5 challenges Handshake Authentification Protocol.

Il est souvent utilise pour les informations d'authentification des supplicants, par un système basé sur le nom d'utilisateur et le mot de passe. Il n'existe pas d'authentification du serveur. Une machine qui se fait passer pour un serveur peut ainsi facilement récupérer les authentifiant (login, mot de passe) de la machine qui cherche à s'authentifier.

- **EAP - SKE:** EAP-Shared Key Exchange

II permet une authentification mutuelle ainsi qu'une itinérance entre les réseaux de <plusieurs fournisseurs d'accès Internet.

- **EAP - SRP** : Il s'agit de l'adaptation du protocole SRP (RFC2945) à l'EAP

III.4.3.c.2 Méthodes basées sur les certificats

- **EAP-TLS** : Transport Layer Security défini par la RFC2716.

C'est la méthode la plus répandue. Elle permet une authentification mutuelle basée sur SSL (Secure Socket Layer). Cette méthode se base sur les certificats X.509. L'utilisateur doit posséder un certificat que le serveur peut valider et l'utilisateur doit également pouvoir valider celui du serveur d'authentification. On parle alors d'une authentification mutuelle; ainsi l'utilisateur se connecte au serveur approprié. Si ce dernier ne s'authentifie pas, il y a déconnexion.

Pour cette double authentification, le système s'appuie sur des clés publiques. Son implémentation est assez lourde par rapport à l'EAP MD5 par exemple, aussi plus coûteuse par l'achat de certifications pour les terminaux, mais plus efficace.

Le serveur possède une copie des certificats des clients, de même le client possède une copie du certificat du serveur. Ainsi grâce aux clés publiques de chiffrement et aux certificats échangés, le serveur et le système à authentifier peuvent vérifier l'identité de l'autre.

Ceci est important dans le cadre des réseaux sans fil, car un utilisateur doit être sûr qu'il se connecte bien au réseau auquel il croit et non à un AP qu'un pirate aurait déposé pour détourner le trafic. TLS apporte une solution pour protéger les données d'authentification entre l'utilisateur et l'AP, mais également pour s'échanger les clés de session de manière sûre, ce qui limite certains défauts de WEP.

Ce système est implémenté sur les bornes des constructeurs 3Com, Proxim.

- **EAP-TTLS** : Tunneled-TLS

Il s'agit ici d'une extension de l'EAP-TLS. L'EAP-TTLS utilise la connexion TLS, génère des clefs aléatoires protégées par le tunnel IPSec.

TTLS permet de ne pas faire appel à un organisme de certification, car le serveur génère une clef privée 128 bits à chaque transaction, donc gère les certificats. Ce système est plus sécurisé qu'avec les clefs WEP habituelles (qui se contentent du login/password) et permet toujours l'allocation dynamique des serveurs d'authentification. Cette solution est celle qui parait la plus sûre.

Le serveur attribue une clé privée au supplicant pour le temps de sa connexion et sera vérifiée par le mécanisme de clé publique du serveur.

- **PEAP** : Protected Extensible Authentification

Le PEAP agit en deux phases. Tout d'abord il crée un tunnel TLS entre le supplicant et le serveur. Puis a lieu l'authentification par EAP-TLS. Il s'agit là aussi d'une authentification mutuelle, par certificat au niveau du serveur, par OTP du côté du supplicant.

Ce système est implémenté sur les bornes des constructeurs Cisco et Microsoft notamment.

Il existe encore d'autres méthodes basées sur les certificats : EAP-Make,...

III.D.3.c.3 Méthodes basées sur des éléments supplémentaires

- **EAP-SIM:** Subscriber Identity Module

Ici est utilisée la carte Sim du GSM.

- **EAP - AKA** : Authentification and Key Agreement:

Dans ce cas, c'est la carte USIM de l'UMTS.

- **L'EAPOL :** Les trames EAP sont encapsulées dans des trames EAPOL (EAP Over Lan) pour transiter sur les réseaux locaux. Elles sont définies pour les trois types de réseaux suivants : Ethernet, Token Ring et FDDI.

III.4.3.d Messages EAP

Tout utilisateur qui désire s'authentifier doit commencer par s'associer avec l'authentificateur (l'AP dans notre cas) au niveau liaison. Ceci peut se faire de plusieurs manières suivant la configuration de l'AP. Si le mode d'authentification est paramétré open, n'importe qui peut s'associer avec l'AP en utilisant les paquets *probe request* et *probe response* définis par la norme 802.11. Par contre, si le mode d'association par clé partagée (shared secret) ou encore par filtrage MAC est paramétré, l'utilisateur doit d'abord respecter les critères d'association. C'est uniquement après cette étape que l'échange des trames EAP peut commencer. Quelque soit la méthode d'authentification employée, c'est toujours les mêmes paquets qui sont utilisés. La figure 2.13 représente le flux des messages échangés entre l'utilisateur et l'authentificateur. L'utilisateur peut commencer par émettre une trame start, mais ceci n'est pas obligatoire.

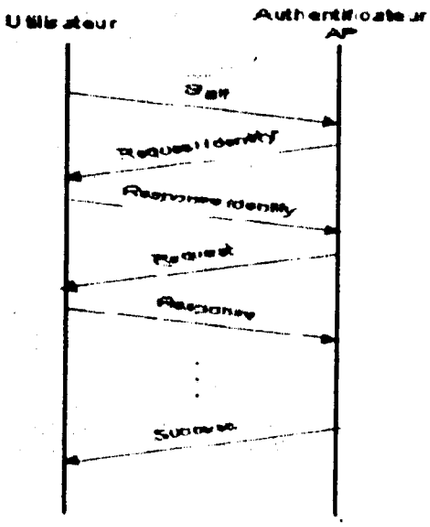


FIGURE1.13 : Echange des messages EAP

Ensuite, l'authentificateur demande à l'utilisateur son identité à l'aide d'un paquet *Request Identity*. L'utilisateur répond avec un paquet *Response Identity*, qui contient notamment son nom d'utilisateur. Une fois l'identité vérifiée, le challenge peut commencer. L'authentificateur transmet à l'utilisateur au moyen du paquet *Request*, le challenge qui doit être effectué. L'utilisateur calcule alors la réponse et l'envoi grâce au paquet *Response*. Si le challenge est réussi, le paquet Success confirmera à l'utilisateur qu'il est bien authentifié. Sinon le paquet *Failure* se charge d'annoncer le challenge lors d'une seule session d'authentification.

III.4.3.e Schéma d'authentification

Il est temps maintenant de mettre ensemble ces quelques concepts venant d'être vu pour réaliser un système d'authentification fort, robuste et fiable. La figure 2.14 nous monte cette solution. Un utilisateur voulant accéder au réseau doit d'abord s'associer avec l'AP au niveau liaison. Ensuite seulement, il peut s'authentifier au prêt du serveur RADIUS. Pour ce faire, étant donné que tous les ports d'application lui sont fermé au niveau de l'AP, l'utilisateur doit employer les ports du protocole EAP pour communiquer avec l'AP ses données d'authentification (trame EAP *Request Identity* et *Response Identity).* L'AP va ensuite transmettre ces données vers le serveur RADIUS par l'intermédiaire du protocole RADIUS et du paquet *Access Request.*

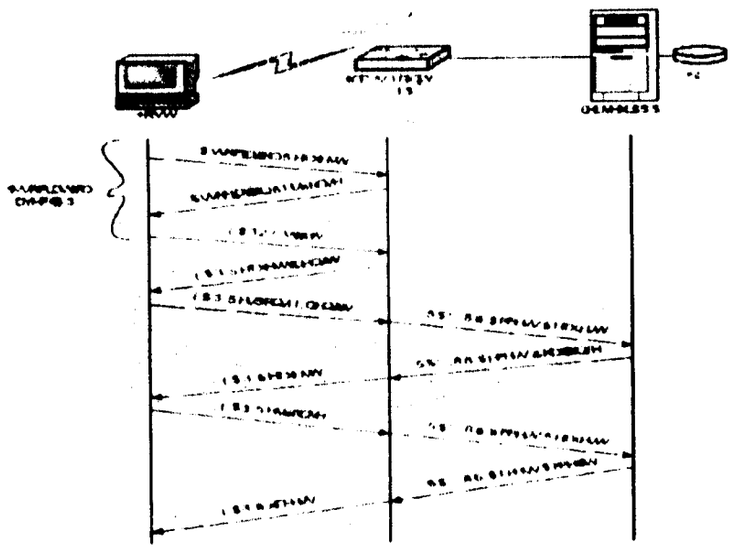


FIGURE1.14 : Réalisation de l'authentification

Le serveur RADIUS va alors vérifier l'identité de l'utilisateur et transmettre le challenge vers l'AP. Ce dernier va faire suivre ce challenge vers l'utilisateur sous la forme d'un paquet EAP *Request.* Une fois le challenge rempli, l'utilisateur peut envoyer la réponse à l'AP qui va la rediriger vers le serveur RADIUS grâce au paquet *Access request.* Si le challenge est réussi, le serveur RADIUS confirme l'authentification avec le paquet *Access Accept* qui va transiter par l'AP avant d'arriver à l'utilisateur sous la forme d'un paquet *Success* du protocole EAP.

Nous avons donc maintenant un schéma d'authentification tout à fait sécurisé et très flexible du point de vu des nombreuses méthodes d'authentification qui peuvent exister. Il va être question maintenant de crypter les données qui vont transiter dans les airs.

Il faut noter une chose très importante : les paquets EAP qui circulent dans les airs entre l'utilisateur et l'AP ne sont pas cryptés si vous n'avez pas activé WPA2 ou tous autres

systèmes de cryptage au niveau liaison ! Bien qu'aucun mot de passe, secrets partagés ou encore certificats ne circulent directement en clair, mais plutôt sous la forme d'un digest ou de clés publiques, ne suffit pas forcément pour garantir une bonne sécurité. Comme nous avons vu plus haut que WEP n'est pas suffisant, alors pour ce projet de fin d'étude nous avons utilisé l'IEEE 802.11i, se basant sur 802.1x, EAP, l'authentification forte, et l'algorithme d'encryption nommé AES.

Certaines de ces variantes se sont révélées trop faible pour prendre en charge une authentification de qualité satisfaisante. Ainsi EAP-MD5 et LEAP sont peu à peu abandonnés car ils sont sujet à des attaques par dictionnaire et des attaques de type homme du milieu (man-in-the-middle).

La norme IEEE 802.1X est incluse dans les standards WPA et WPA2 (IEEE 802.11i).

Il est évident que les recommandations de sécurité portent également sur le serveur d'authentification (serveur RADIUS) qui devra être à jour en ce qui concerne les vulnérabilités. En plus de la sécurité logicielle, une attention particulière devra être prise quant à l'insertion du serveur RADIUS dans son architecture réseau.

L'utilisation du protocole IEEE 802.1X est recommandée si l'on désire un mécanisme d'authentification robuste et il est déconseiller d'utiliser une authentification qui s'appuie sur une clé partagée ou sur un filtrage des adresses MAC. En ce qui concerne l'authentification EAP-TLS semble aujourd'hui s'imposer comme un protocole robuste s'il est mis en place selon une politique de sécurité bien définie et mise en place avec rigueur. La sécurité du serveur d'authentification doit être également prise en compte. [5]

III.5 VPN (Virtual Private Network)

Pour toutes les communications nécessitant un haut niveau de sécurisation, il est préférable de recourir à un chiffrement fort des données en mettant en place un réseau privé virtuel (VPN).

Les réseaux VPN se basent sur la technique du tunneling. Après avoir identifié l'émetteur et le destinataire un chemin virtuel est construit. Ensuite les données seront chiffrées et acheminées par la source en empruntant ce chemin virtuel.

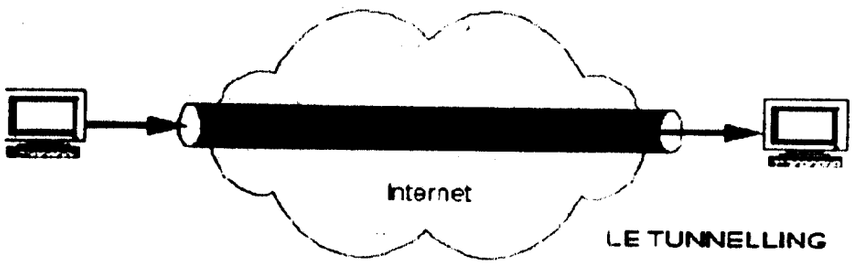


FIGURE1.15 : Principe du VPN

Les données à transmettre peuvent appartenir à un protocole différent d'IP. Le routage des trames dans le tunnel se fait grâce au protocole de tunneling qui encapsule les données en rajoutant un entête. Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de dés encapsulation. [6]

III.5.1 Applications des VPNs

L'application principale des VPN est de garantir et de permettre à un hôte distant d'accéder à l'intranet de son entreprise ou à celui d'un client grâce à Internet tout en garantissant la sécurité des échanges. Il crée un réseau privé virtuel entre l'appelant et le serveur VPN de l'entreprise.

Les VPN peuvent également être utilisé à l'intérieur même de l'entreprise, sur l'intranet, pour l'échange de données confidentielles. [6]

III.5.2 Services des VPN

La sécurité des échanges est assurée à plusieurs niveaux et par différentes fonctions comme le cryptage des données, l'authentification des deux extrémités communicantes et le contrôle d'accès des utilisateurs aux ressources. [6]

Ces VLANs sont à prendre en compte lors de la mise en place du Wi-Fi car il faudra sans doute séparer les flux sans fil en WVLANs *(Wireless VLANs)* grâce au serveur RADIUS qui pourra faire basculer l'utilisateur dans un certain WVLAN juste après la phase d'authentification.

Conclusion

II est très important de savoir que lors de la conception d'un réseau sans fil il faut se fixer des objectifs sur sa sécurisation car gérer un réseau sans fil nécessite de s'appuyer sur une équipe ayant une bonne connaissance des réseaux et de la sécurité des systèmes d'information .et aussi faire le bon chois sur les procédures et les protocoles de sécurités.

Les nonnes présentées dans ce chapitre permettent de donner une vue claire sur l'évolution de la sécurité.

Introduction

Dans ce chapitre on va détailler notre travail, qui consiste à installer et sécuriser un réseau test, en utilisant une architecture WPA2 avec AES comme algorithme de cryptage de données, et en choisissant en particulier la méthode EAP-TLS(certificat électronique) comme méthode d'authentification, puis l'installation et la configuration d'un serveur RADIUS fourni par Microsoft Windows Serveur 2008, via l'authentification 802. 1X.

I. Installation du réseau Wi-Fi

Pour commencer, on a va monter notre réseau test, qui se compose de :

- Un point d'accès D-Link-DSL-2640U.
- Un Windows Serveur 2008 installé sur un ordinateur de bureau-Pentium 4.
- Un ordinateur portable Toshiba utilisé comme un client autorisé.
- Un ordinateur portable utilisé comme un client non autorisé (Pirate)
- Le serveur est relié au point d'accès par un câble droit.

La figure suivante représente notre réseau test :

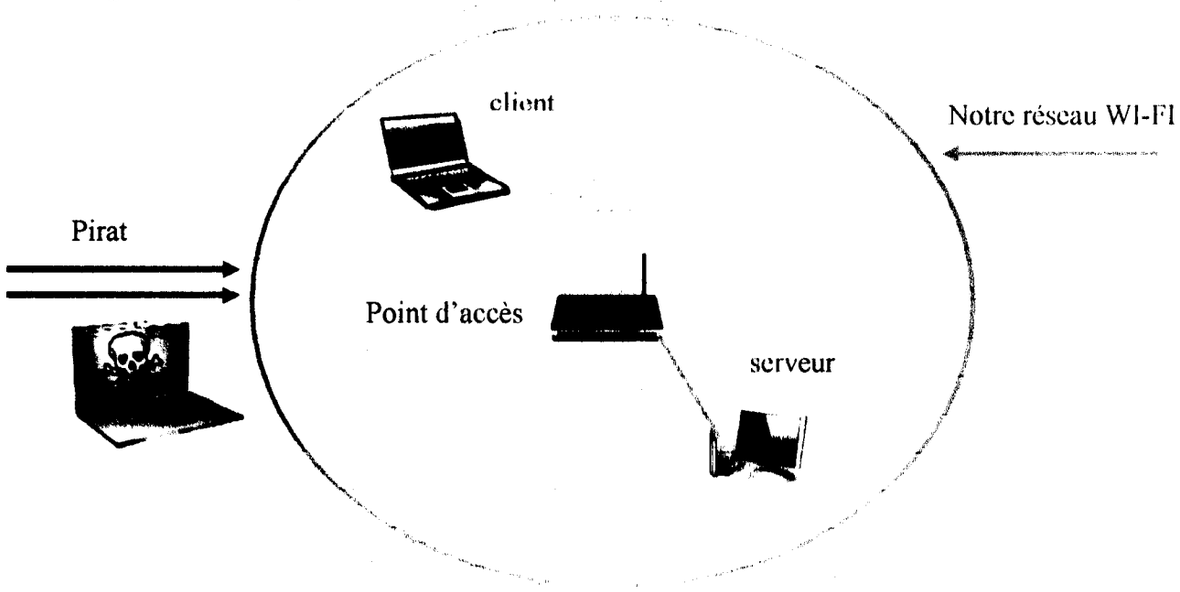


FIGURE2.1 : Architecteur de notre réseau wifi

II. Implémentation de la sécurité sur le réseau Wi-Fi

Dans cette partie on va montrer les étapes à suivre pour implémenter la sécurité sur un réseau Wi-Fi infrastructure en utilisant la méthode WPA2 comme solution de sécurisation (AES comme cryptage et EAP-TLS) avec un serveur RADIUS (de Windows Serveur 2008).

Avant d'entamer cette étape on va donner quelques définitions sur Microsoft Windows Serveur 2008, une présentation du serveur RADIUS sous Windows Serveur 2008 et une présentation des certificats.

II.1 Présentation de Windows Server 2008

Microsoft Windows Server 2008 est le système d'exploitation Windows Server de nouvelle génération qui aide les administrateurs système à optimiser leur contrôle sur l'infrastructure. Il offre une disponibilité et des fonctionnalités sans précédent. Les administrateurs bénéficient d'un environnement serveur davantage sécurisé, fiable et robuste. Par ailleurs, Windows Server 2008 propose aux organisations une nouvelle valeur ajoutée en garantissant à tous les utilisateurs l'accès à l'ensemble des services du réseau, où qu'ils se trouvent. Windows Server 2008 offre également une vue approfondie sur les fonctions du système d'exploitation et de diagnostic, permettant aux administrateurs de consacrer davantage de temps à la valeur métier de l'entreprise.

Windows Server 2008 s'appuie sur les points forts du système d'exploitation Windows Server 2003 et sur les innovations du Service Pack 1 et de Windows Server 2003 R2. Cependant, Windows Server 2008 est bien plus qu'une version perfectionnée des systèmes d'exploitation précédents. Il a été conçu pour offrir aux entreprises la plateforme la plus efficace pour prendre en charge des applications, des réseaux et des services Web, du groupe de travail jusqu'au centre de données. Pour cela, Windows Server 2008 est doté de nouvelles fonctionnalités très élaborées.[9]

II.2 Améliorations apportées au système d'exploitation Windows Server

En plus de ses fonctionnalités innovantes, Windows Server 2008 apporte de puissantes améliorations au cœur du système d'exploitation par rapport à Windows Server 2003. Quelques-unes de ces améliorations notables concernent : le réseau, des fonctionnalités de sécurité avancées, l'accès aux applications distantes, la gestion centralisée des rôles de

serveur, les outils d'administration de la performance et de la fiabilité, le cluster à basculement, le déploiement et le système de fichiers. Grâce à ces perfectionnements, et à bien d'autres encore, les entreprises optimisent la flexibilité, la disponibilité et le contrôle de leurs serveurs. [9]

II.3 Technologies Windows Server 2008

❖ Un contrôle renforcé

Assurer le contrôle des serveurs sur un réseau et, plus important encore, l'accès aux serveurs, est une priorité fondamentale pour les administrateurs. Dans cette optique, Windows Server 2008 propose deux fonctionnalités innovantes qui aident les administrateurs à développer et à optimiser leur contrôle sur l'accès aux serveurs : Network Access Protection et Internet Information Services 7.0.

❖ Network Access Protection (NAP)

Grâce à cette nouvelle solution, les administrateurs définissent la configuration minimale des ordinateurs qui ont le droit de se connecter au réseau, et restreignent l'accès aux systèmes qui ne répondent pas à ces critères. NAP met en application des stratégies définies par l'administrateur, qui décrivent les exigences de l'entreprise. Par exemple, les stratégies peuvent exiger l'installation de toutes les mises à jour sur le système d'exploitation, ou l'installation et la mise à jour de logiciels antivirus ou de protection contre les messages indésirables. Ainsi, les administrateurs établissent la protection de base dont doivent être dotés les ordinateurs lorsqu'ils se connectent au réseau.

❖ Internet Information Services 7.0

Windows Server 2008 offre une plateforme unifiée pour la publication Web qui intègre Internet Information Services (IIS) 7.0, ASP.NET, Windows Communication Foundation, Windows Workflow Foundation et Windows SharePoint Services 3.0. La solution IIS 7.0 est une version très améliorée du serveur Windows Web actuel. Elle joue un rôle central dans l'intégration des technologies Web. IIS 7.0 aide les développeurs et les administrateurs à optimiser leur contrôle sur les interfaces de réseau/Internet grâce à des fonctionnalités fondamentales telles que l'administration déléguée, le renforcement de la sécurité, la réduction de la surface d'attaque, la gestion intégrée des applications et des états pour les services Web, et des outils d'administration perfectionnés.

❖ **Une plus grande disponibilité**

La disponibilité des serveurs commence par le déploiement rapide de nouveaux serveurs qui répondent aux besoins de l'entreprise, et elle se poursuit avec le maintien en état de ces serveurs. Grâce à la nouvelle option de déploiement fournie par Windows Server 2008, les entreprises améliorent la disponibilité de leurs serveurs de fichiers et d'impression dédiés, de leurs serveurs Dynamic Host Configuration Protocol (DHCP) et Domain Name System (DNS) et enfin, de leurs contrôleurs de domaine.

❖ **Serveur de base**

À présent, avec la version bêta 2 de Windows Server 2008, les administrateurs peuvent installer le système d'exploitation Windows Server en le dotant uniquement des services nécessaires pour activer les rôles DHCP ou DNS, les rôles de serveur de fichiers ou de contrôleur de domaine. Cette nouvelle option d'installation inclura uniquement les services et applications nécessaires et offrira des fonctionnalités serveur de base sans service supplémentaire. Le serveur de base fonctionne exactement comme un système d'exploitation qui prend en charge l'un des rôles désignés mais n'inclut pas l'interface utilisateur graphique (GUI) de serveur. Les installations serveur de base comportent uniquement les éléments nécessaires pour les rôles désignés. Ainsi, toute installation serveur de base nécessite généralement moins de maintenance et de mises à jour puisqu'elle comporte moins d'éléments à gérer. En d'autres mots, le serveur exécute moins de processus et comporte moins d'éléments : cela réduit la surface d'attaque. Ainsi, si vous repérez une défaillance ou une vulnérabilité sur un élément qui n'a pas été installé, vous n'avez pas besoin d'installer de correctif.

❖ **Une plus grande souplesse**

Les exigences des entreprises sur leurs serveurs suivent l'évolution de leurs besoins métier. De même, les avancées technologiques apportées aux serveurs modifient leur mode d'utilisation par les organisations et les utilisateurs. Windows Server 2008 a été conçu pour vous permettre de modifier votre infrastructure afin de l'adapter aux besoins changeants de l'entreprise tout en maintenant sa souplesse. Windows Server 2008 offre une nouvelle option de configuration aux entreprises qui ont besoin de contrôleurs de domaine en des lieux moins sécurisés physiquement ou pour une utilisation exclusivement cantonnée aux applications métier : le contrôleur de domaine en lecture seule RODC (Read-Only Domain Controller). Pour les entreprises qui ont des utilisateurs itinérants, Windows Server 2008 intègre aux services

Terminal Server des améliorations et des innovations qui favorisent notamment : une intégration facile des applications distantes et locales sur les ordinateurs clients, l'accès à ces programmes à distance via un navigateur Web, et l'accès aux terminaux et aux applications distants au-delà des pare-feu. Enfin, Windows Déploiement Services aide les entreprises qui doivent déployer plusieurs serveurs et PC en même temps à déployer rapidement et facilement de nouveaux ordinateurs sur le réseau via des images disque.

- **Contrôleur de domaine en lecture seule RODC (Read-Only Domain Controller)**

Avec cette nouvelle méthode de configuration des contrôleurs de domaine fournie par Windows Server 2008, les entreprises déploient facilement un contrôleur de domaine sur des sites sur lesquels la sécurité physique d'un contrôleur ne peut pas être garantie. Un contrôleur de domaine RODC héberge une copie en lecture seule d'une base de données Active Directory pour un domaine donné. Auparavant, les utilisateurs d'une filiale qui devaient s'identifier sur un contrôleur de domaine dont la sécurité physique n'était pas garantie, devaient s'identifier via un réseau longue distance. Dans de nombreux cas, cette solution s'avérait inefficace. Ainsi, en plaçant une copie en lecture seule d'une base de données Active Directory à proximité des utilisateurs des filiales, ces derniers profitent d'un temps de connexion accéléré et d'un accès plus efficace aux ressources d'authentification du réseau. Cette solution est également applicable aux environnements qui ne disposent pas d'une sécurité physique appropriée pour déployer un contrôleur de domaine traditionnel.

- **Services Terminal Server**

Windows Server 2008 apporte aux services Terminal Server de nouvelles fonctionnalités pour la connexion aux applications et aux ordinateurs distants. Les programmes à distance des services Terminal Server s'exécutent sur les postes de travail des utilisateurs comme s'il s'agissait d'applications locales. L'utilisateur peut parfaitement exécuter des programmes distants en parallèle avec ses programmes locaux sur site. L'accès Web aux services Terminal Server permet d'utiliser des applications distantes via un navigateur Web, ce qui donne aux utilisateurs encore plus de souplesse pour l'accès et l'utilisation des programmes distants. Enfin, grâce à la passerelle des services Terminal Server, les utilisateurs accèdent aux terminaux et à leurs programmes distants tout en étant protégés par un pare-feu.

❖ **Services de déploiement Windows (WDS)**

Les services de déploiement Windows (WDS, Windows Deployment Services), version mise à jour et repensée des services d'installation à distance (RIS, Remote Installation Services) et fournie par Windows Server 2008, favorise l'adoption et le déploiement rapides des systèmes d'exploitation Windows à partir d'une image. Avec WDS, vous pouvez effectuer une installation réseau de Windows Vista et Windows Server 2008 sur des ordinateurs nus (qui ne disposent pas de système d'exploitation). Par ailleurs, WDS prend en charge des environnements mixtes tels que Microsoft Windows XP et Microsoft Windows Server 2003. Ainsi, les services de déploiement Windows offrent une solution complète pour le déploiement des systèmes d'exploitation Windows sur les ordinateurs clients et serveur, et réduit le coût total de possession (TCO) et la complexité des déploiements Windows Server 2008 et Windows Vista. [9]

II.4 Présentation du serveur RADIUS sous Windows Server 2008

Network Policy Server (NPS) peut être utilisé comme serveur RADIUS afin d'effectuer l'authentification, l'autorisation et la gestion des clients RADIUS. Un client RADIUS peut être un serveur d'accès réseau ou un proxy RADIUS. Lorsque NPS est utilisé en tant que serveur RADIUS, il fournit les services suivants :

Un service d'authentification et d'autorisation central pour toutes les demandes de connexion envoyées par des clients RADIUS.

NPS utilise un domaine Microsoft® Windows NT® Server 4.0, un domaine Active Directory® ou la base de données de comptes d'utilisateurs SAM (Security Accounts Manager) locale afin d'authentifier les informations d'identification des utilisateurs pour les tentatives de connexion. NPE utilise les propriétés de numérotation du compte d'utilisateur et des stratégies réseau pour autoriser une connexion.

Un service d'enregistrement de gestion central pour toutes les demandes de gestion envoyées par des clients RADIUS. Les demandes de gestion sont stockées dans un fichier journal local ou dans une base de données Microsoft® SQL Server™ à des fins d'analyse.

NPS utilisé en tant que serveur RADIUS pour différents clients d'accès, ainsi qu'un proxy RADIUS. NPS utilise un domaine Active Directory® pour l'authentification des informations d'identification utilisateur des messages de demande d'accès RADIUS entrants.

Lorsque NPS est utilisé comme serveur RADIUS, les messages RADIUS fournissent l'authentification, l'autorisation et la gestion des connexions d'accès réseau.

Les serveurs d'accès, tels que les serveurs d'accès réseau à distance, les serveurs VPN et les points d'accès sans fil reçoivent des demandes de connexion de la part des clients d'accès. Le serveur d'accès, configuré de façon à utiliser RADIUS comme protocole d'authentification, d'autorisation et de gestion, crée un message de demande d'accès et l'envoie au serveur NPS.

Le serveur NPS évalue le message de demande d'accès. Si nécessaire, le serveur NPS envoie un message de challenge d'accès au serveur d'accès. Celui-ci traite le challenge et envoie un message de demande d'accès mis à jour au serveur NPS.

Les informations d'identification utilisateur sont vérifiées et les propriétés de numérotation du compte d'utilisateur sont obtenues par le biais d'une connexion sécurisée à un contrôleur de domaine. La tentative de connexion est autorisée avec les propriétés de numérotation du compte d'utilisateur et avec les stratégies d'accès.

Si la tentative de connexion est authentifiée et autorisée, le serveur NPS envoie un message d'acceptation d'accès au serveur d'accès.

Si la tentative de connexion n'est pas authentifiée ou n'est pas autorisée, le serveur NPS envoie un message de refus d'accès au serveur d'accès. Le serveur d'accès achève le processus de connexion avec le client d'accès et envoie un message de demande de compte au serveur NPS, où le message est enregistré dans le journal. Le serveur NPS envoie une réponse de compte au serveur d'accès.

Le serveur d'accès envoie également des messages de demande de compte durant la période où la connexion est établie, lorsque la connexion de client d'accès est fermée et lorsque le serveur d'accès est démarré et arrêté.

Vous pouvez utiliser NPS comme serveur RADIUS dans les cas suivants :

- Vous utilisez un domaine Windows NT Server 4.0, un domaine Active Directory ou la base de données de comptes d'utilisateurs SAM locale comme base de données de comptes d'utilisateurs pour les clients d'accès.
- Vous utilisez Routage et accès à distance sur plusieurs serveurs d'accès à distance, serveurs VPN ou commutateurs d'accès à distance et vous souhaitez centraliser la configuration des stratégies réseau et la journalisation des connexions pour la gestion des comptes.
- Vous externalisez votre accès à distance, VPN ou sans fil à un fournisseur de services. Les serveurs d'accès utilisent RADIUS pour authentifier et autoriser les connexions établies par des membres de votre organisation.

- Vous souhaitez centraliser l'authentification, l'autorisation et la gestion pour un ensemble hétérogène de serveurs d'accès. [10]

II.5 Présentation des certificats

Les certificats sont des documents numériques délivrés par des autorités de certification, telles que les services de certificats Active Directory® (AD CS, Active Directory® Certificate Services) ou l'autorité de certification publique Verisign. Les certificats peuvent être utilisés à de nombreuses fins, telles que la signature de code et la sécurisation des communications de messagerie électronique, mais avec Network Policy Server (NPS) ils sont utilisés pour l'authentification de l'accès réseau.

Les certificats sont utilisés pour l'authentification de l'accès réseau car ils procurent une sécurité élevée pour l'authentification des utilisateurs et des ordinateurs et évitent d'avoir à utiliser des méthodes d'authentification moins sécurisées basées sur mot de passe.

Deux méthodes d'authentification, lorsqu'elles sont configurées avec des types d'authentification basée sur certificats, utilisent des certificats : EAP et PEAP. Avec EAP, vous pouvez configurer le type d'authentification TLS (EAP-TLS), tandis qu'avec PEAP vous pouvez configurer les types d'authentification TLS (PEAP-TLS) et MS-CHAP v2 (PEAP-MS-CHAP v2). Ces méthodes d'authentification utilisent toujours des certificats pour l'authentification de serveur. Selon le type d'authentification configuré avec la méthode d'authentification, les certificats peuvent également être utilisés pour l'authentification des utilisateurs et l'authentification des ordinateurs clients.

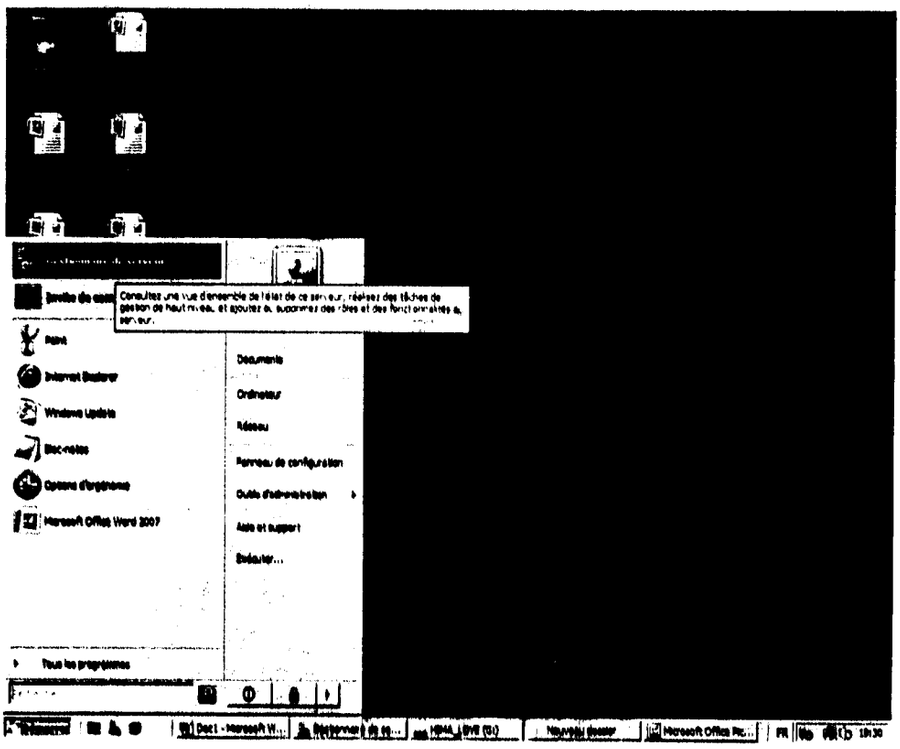
- **Authentification basée sur les certificats et clients sans fil**

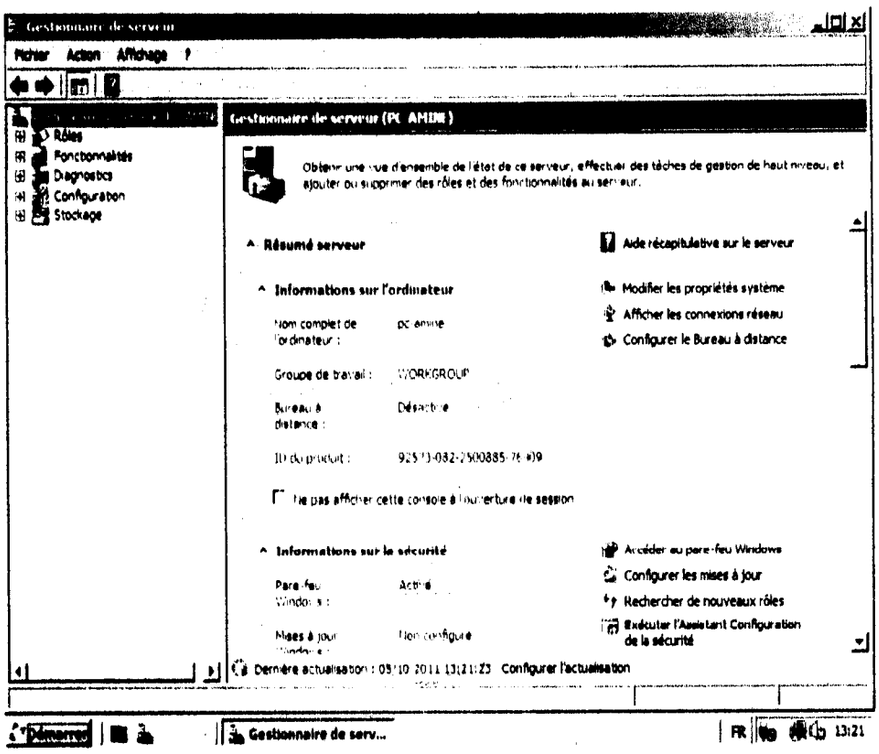
L'authentification IEÉE 802. 1X permet un accès authentifié aux réseaux sans fil 802.11 et aux réseaux Ethernet câblés. 802. IX assure la prise en charge des types EAP sécurisés, tels que TLS avec des cartes à puce ou des certificats. Vous pouvez configurer 802. IX avec EAP-TLS de plusieurs manières. Si l'option Valider le certificat du serveur est configurée sur le client, celui-ci authentifie le serveur en utilisant ce certificat. L'authentification de l'ordinateur client et de l'utilisateur peut être accomplie à l'aide de certificats contenus dans le magasin de certificats de client ou d'une carte à puce, ce qui permet de disposer d'une authentification mutuelle. Avec les clients sans fil, PEAP-MS-CHAP v2 peut être utilisé comme méthode d'authentification. PEAP-MS-CHAP v2 est la méthode d'authentification utilisateur basée sur mot de passe qui utilise TLS avec des certificats de serveur. Durant

l'authentification PEAP-MS-CHAP v2, le serveur LAS ou RADIUS fournit un certificat afin de valider son identité au client (si l'option Valider le certificat du serveur est configurée sur le client Windows Vista® et Windows XP Professionnel). L'authentification de l'ordinateur client et de l'utilisateur est accomplie à l'aide de mots de passe, ce qui élimine certaines des difficultés liées au déploiement de certificats sur les ordinateurs clients sans fil. Les clients de commutation avec ou sans fil 802. 1X peuvent également utiliser PEAP-EAP-TLS pour une sécurité renforcée. PEAP-EAP-TLS utilise une infrastructure de clé publique (PKI, Public Key Infrastructure) avec les certificats pour l'authentification du serveur, et des cartes à puces ou des certificats pour l'authentification de l'utilisateur et de l'ordinateur client. [10]

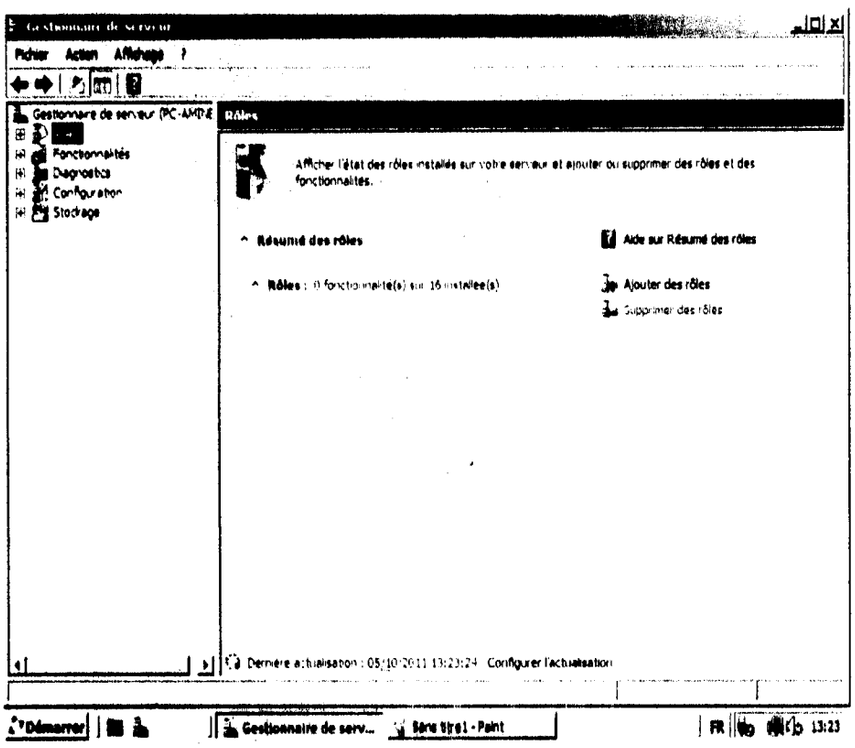
III Sécuriser un réseau WI-FI avec Windows Server 20008

L'accès au gestionnaire de serveur se fait par **Démarrer** puis **Gestionnaire de serveur.**





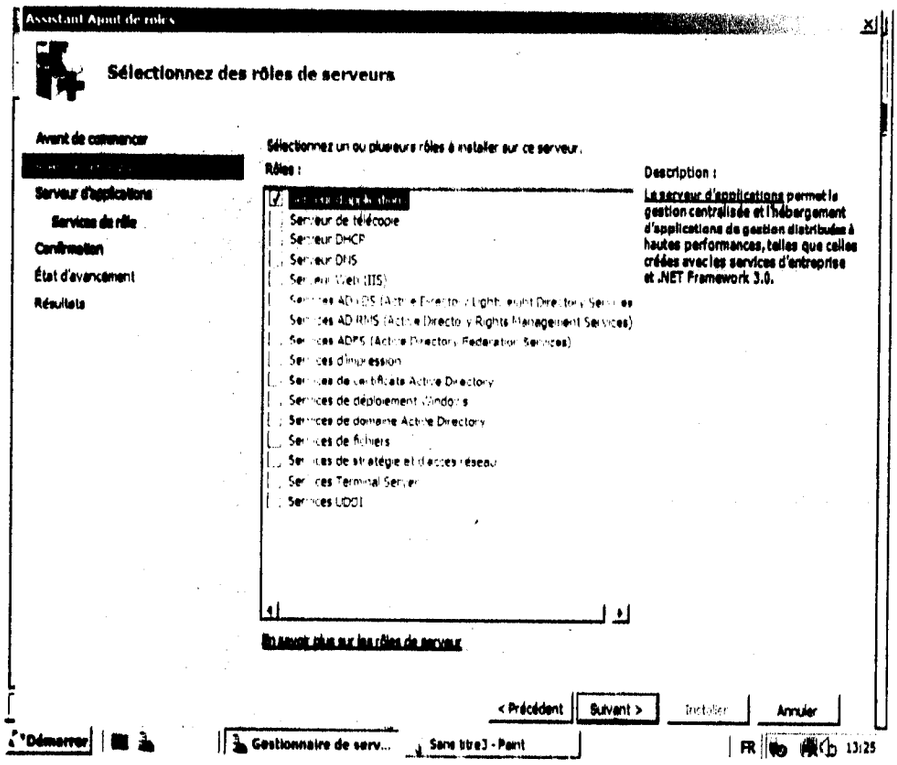
Il faut ajouter des rôles à notre serveur :



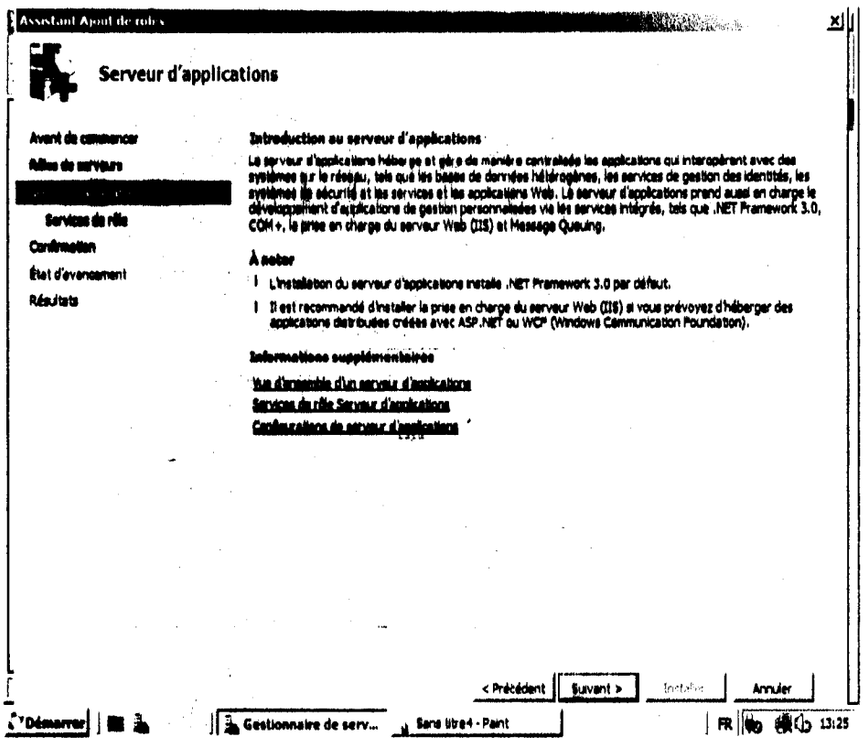
Il faut installer une autorité de certificat racine, tout d'abord nécessite l'installation du serveur d'application, le serveur web (IIS) et l'installation du domaine Active Directory.

III.1 Serveur d'applications

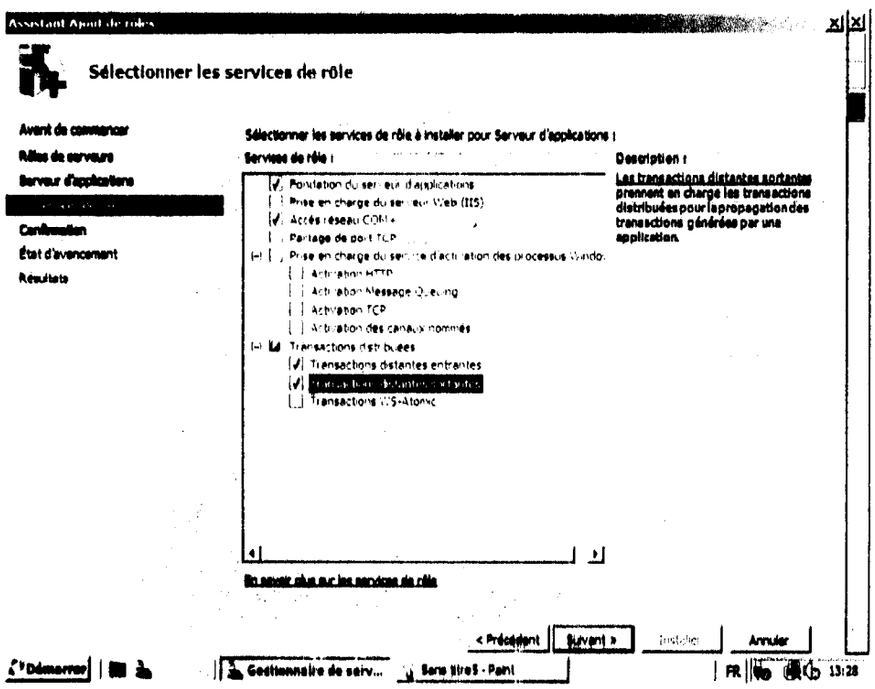
On a sélectionné le rôle à ajouter **Serveur d'application** et on cliqué sur **suivant.**



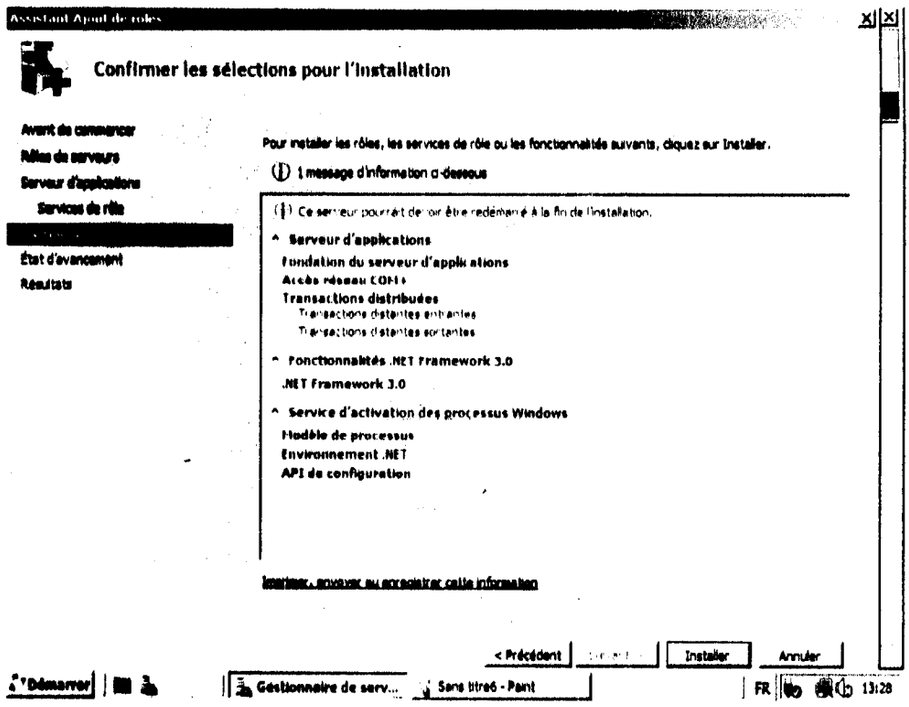
Des informations à propos du serveur d'applications, on clique sur **Suivant.**



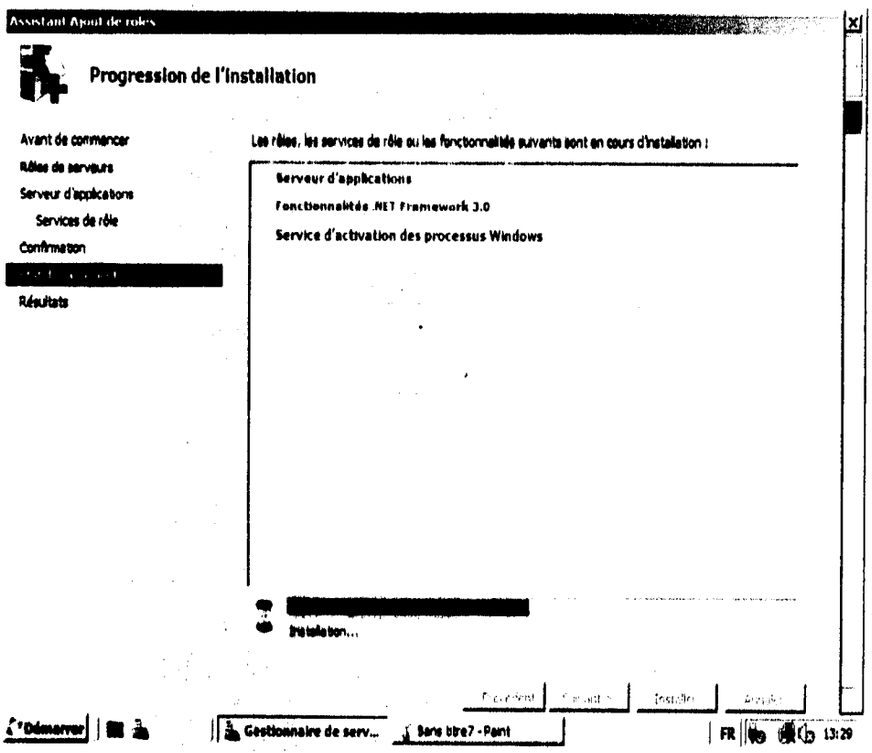
On a coché les services de rôle requis à installer pour le serveur d'applications et ensuite on a cliqué sur **suivant.**



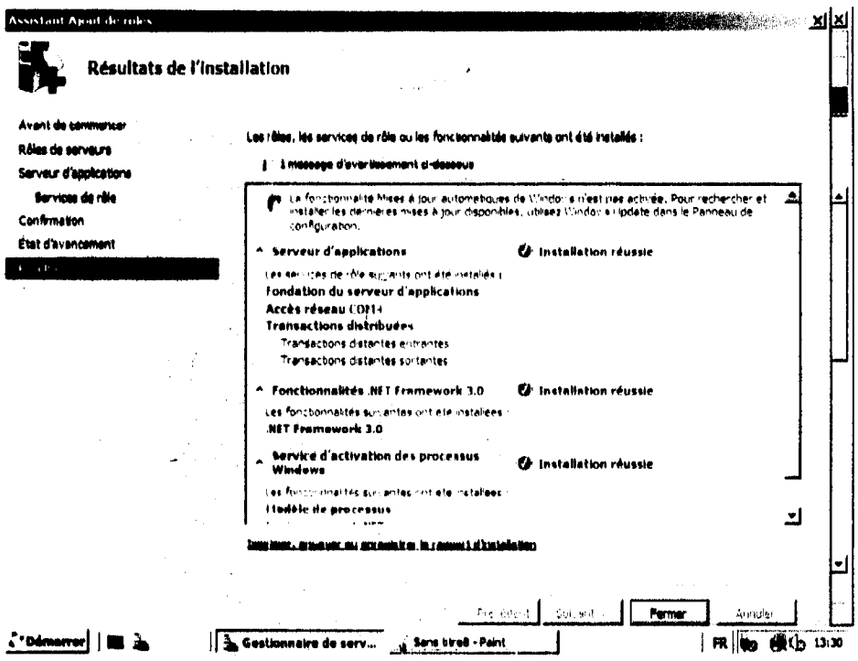
Un récapitulatif des choix apparait, il faut cliquer sur **installer** pour lancer l'installation.



Progression de l'installation…

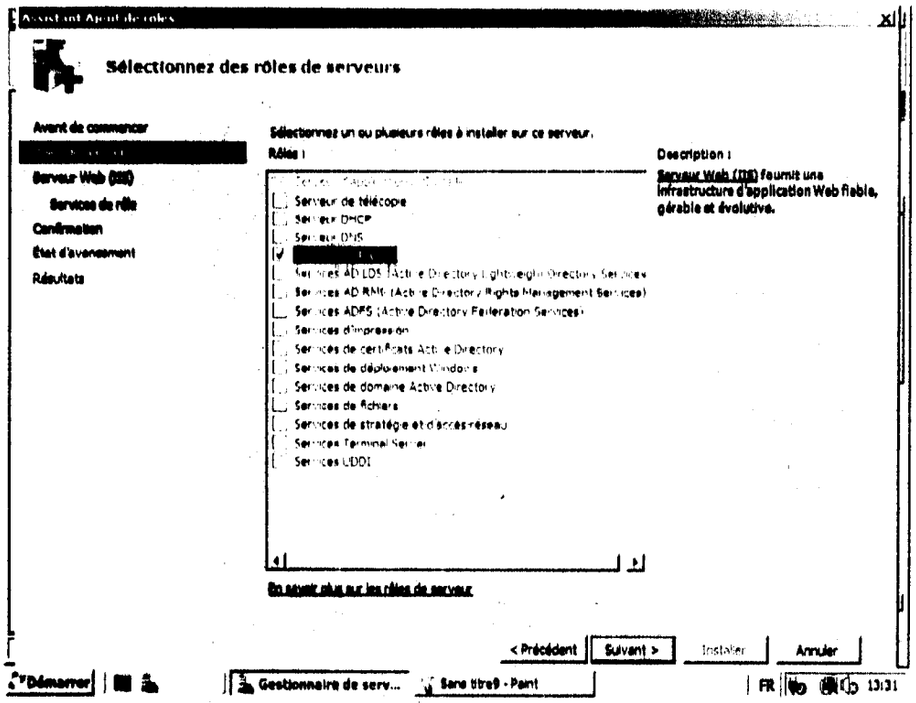


Une fois l'installation terminée un récapitulatif des éléments installés et l'état d'installation s'affiche, on a cliqué sur **Fermer.**

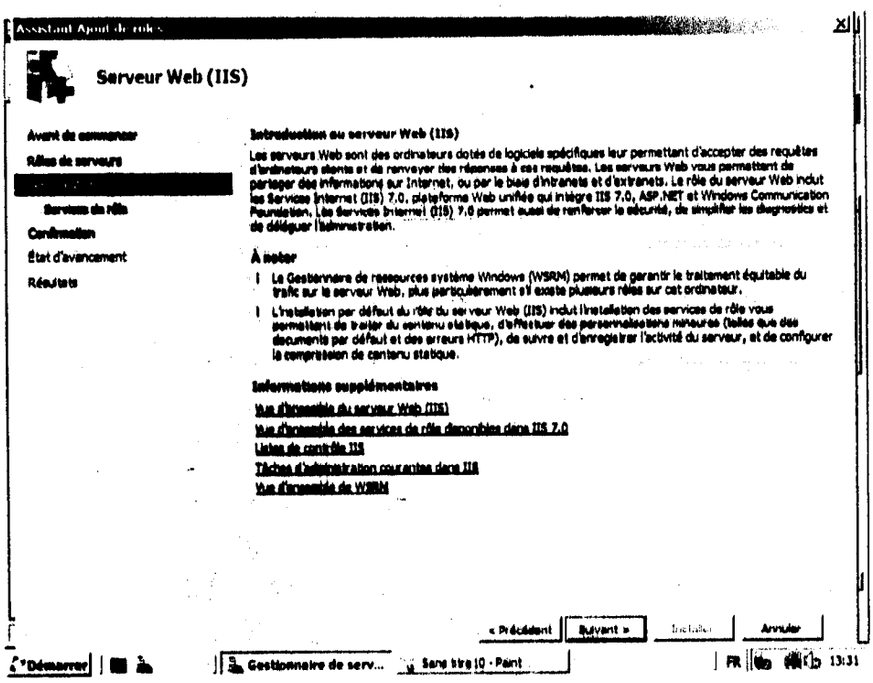


III.2 Serveur Web (IIS) : (internet information Serveur).

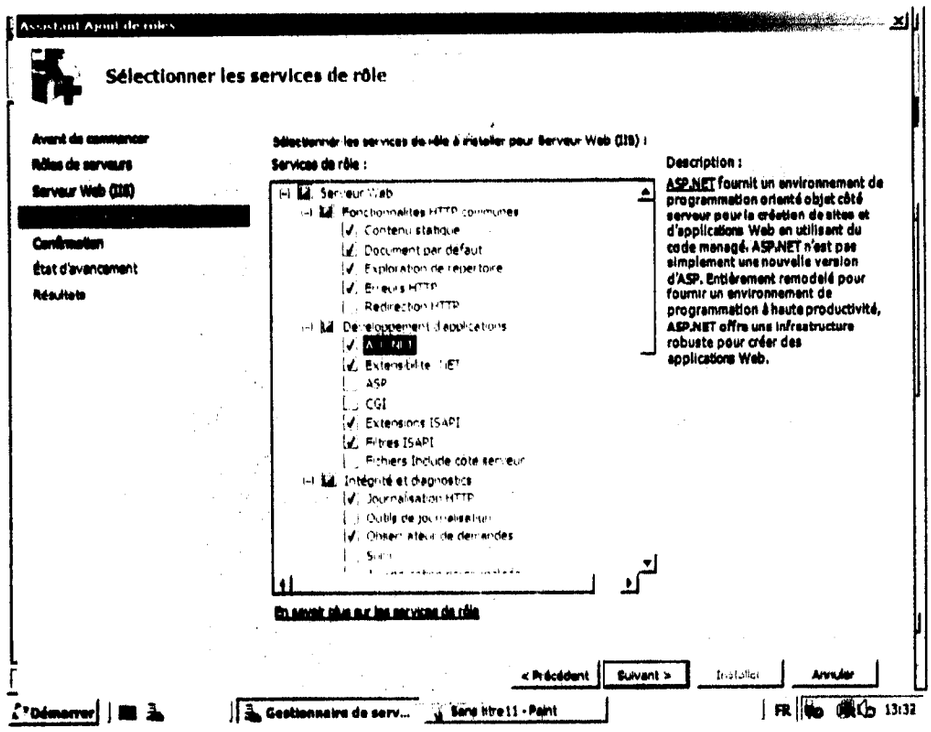
On a sélectionné le rôle à ajouter **Serveur Web (IIS).**



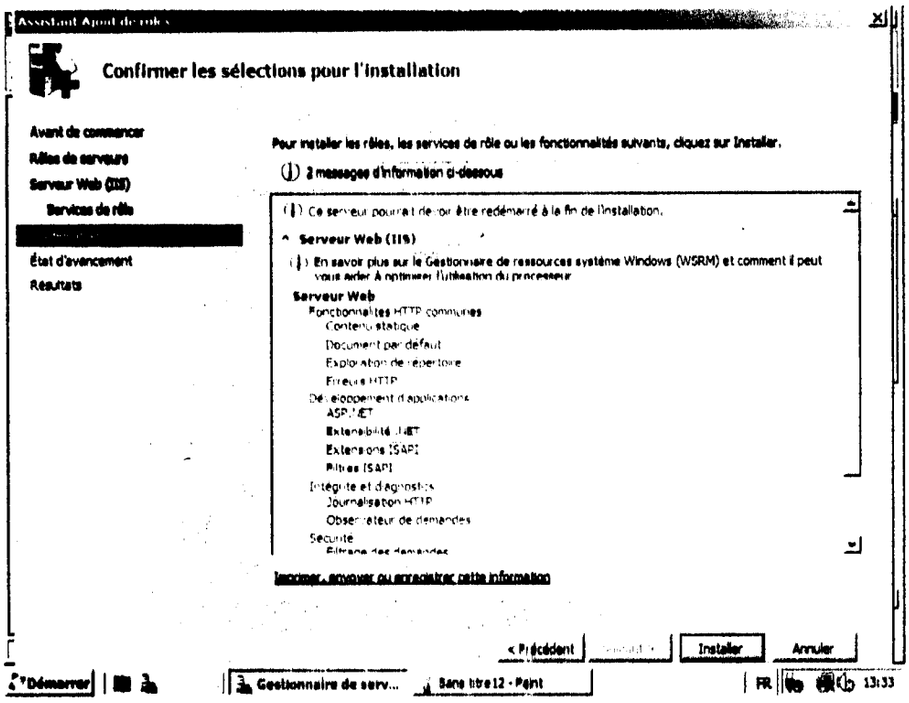
Des informations à propos le serveur Web, on clique sur **suivant** pour continuer.



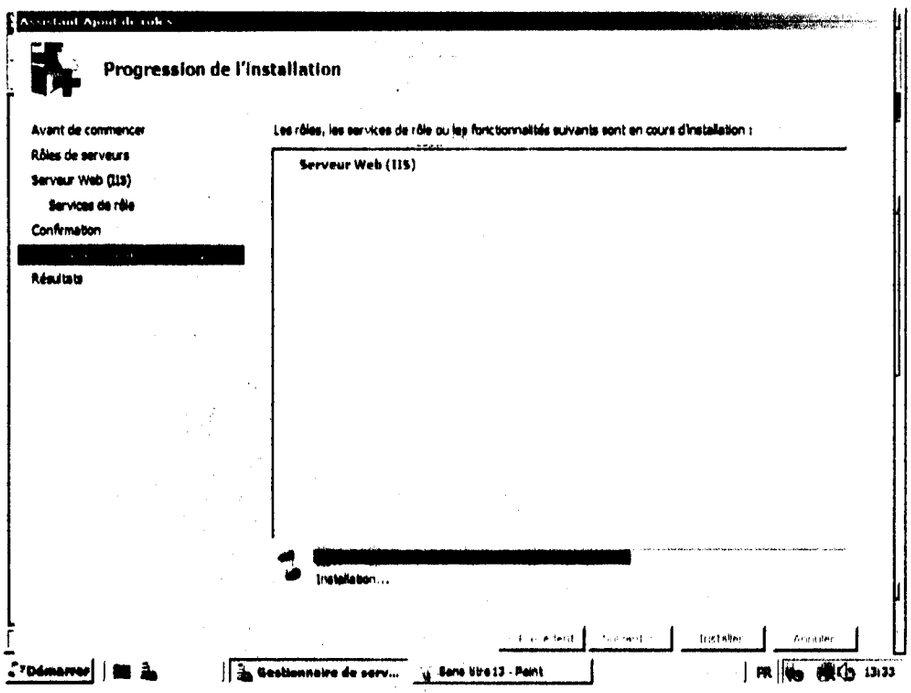
Il faut cocher les services de rôle requis à installer pour le serveur Web, ensuite on clique sur **suivant.**



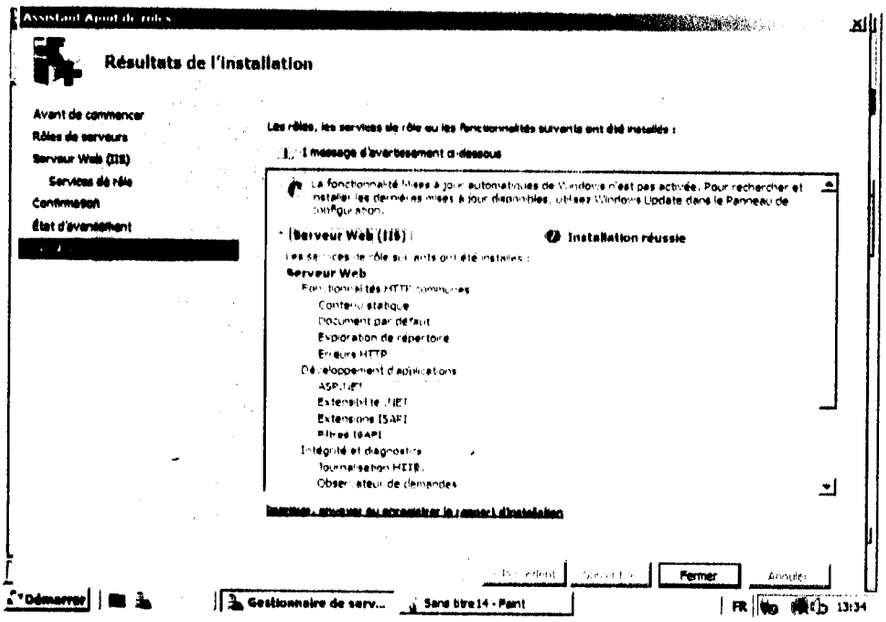
Un récapitulatif apparait, il faut cliquer sur **Installer** pour lancer l'installation.



Progression de l'installation…



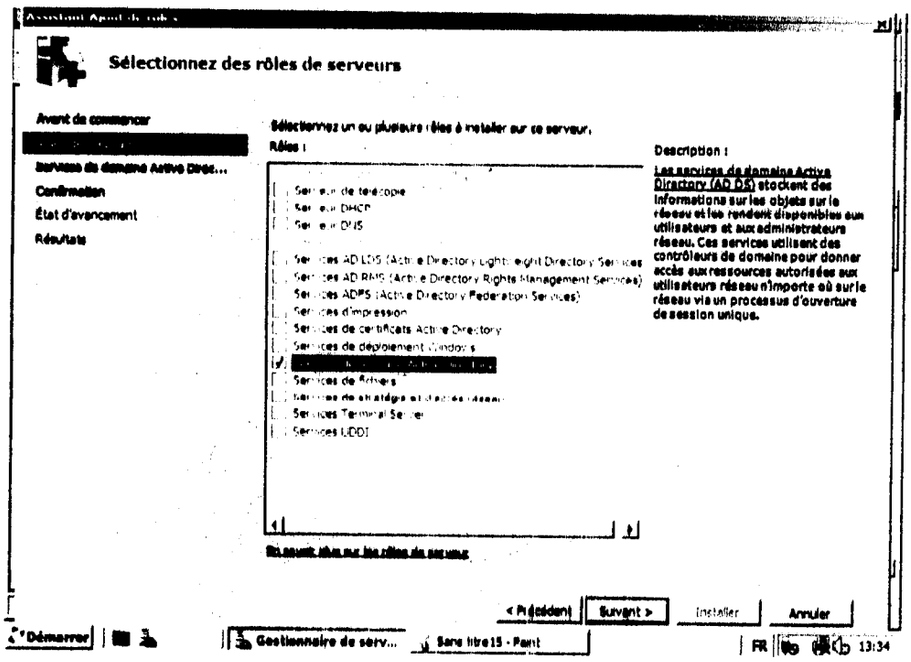
Une fois l'installation terminée un récapitulatif des éléments installés et l'état d'installation s'affiche, **Fermer.**



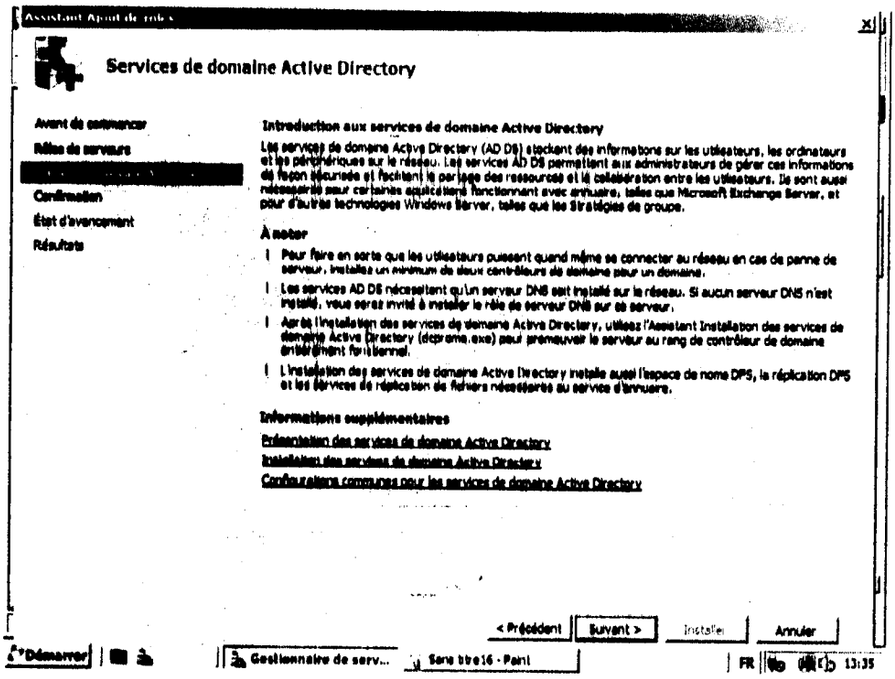
III.3 Services de domaine Active Directory

Utiliser pour l'installation d'active Directory, Ce rôle correspond aux désormais classiques Contrôleur de domaine.

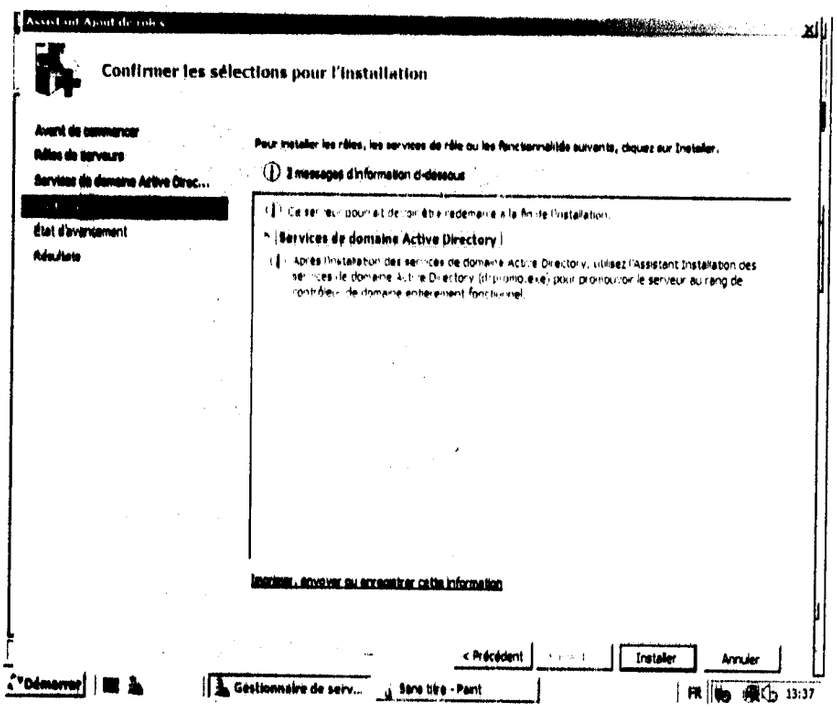
On a coché le rôle **Services de domaine Active Directory** et on a cliqué sur **suivant.**



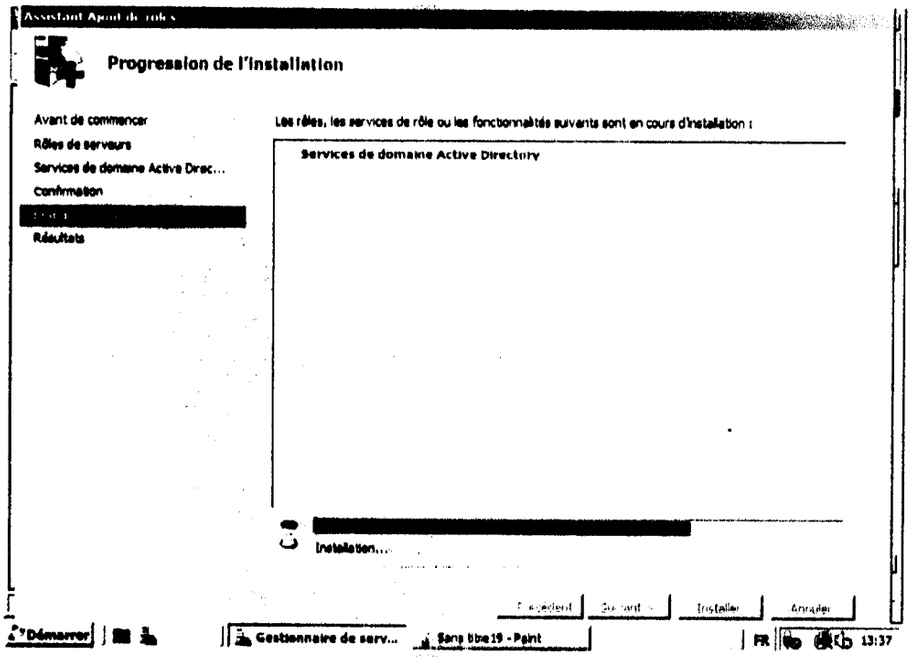
Les informations à propos les services de domaine Active Directory



On aura ensuite le résumé de l'installation qui va être faite. Il faut cliquer sur **installer** pour lancer l'installation.

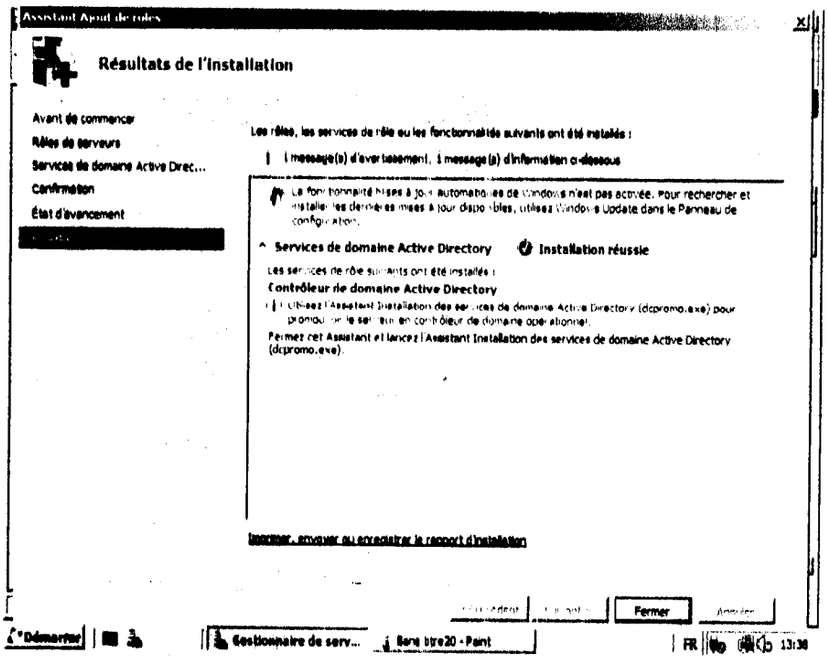


Progression de l'installation...

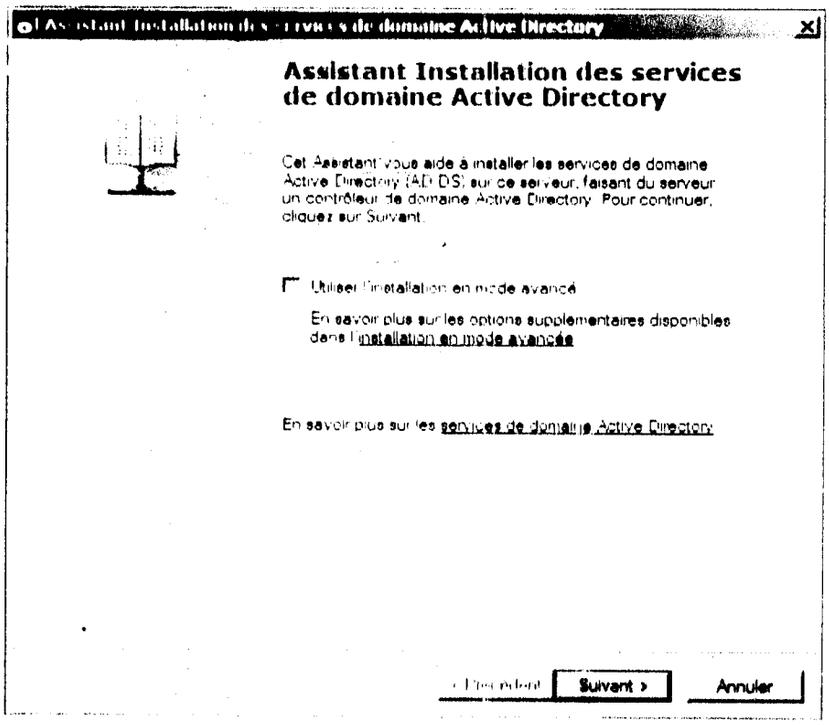


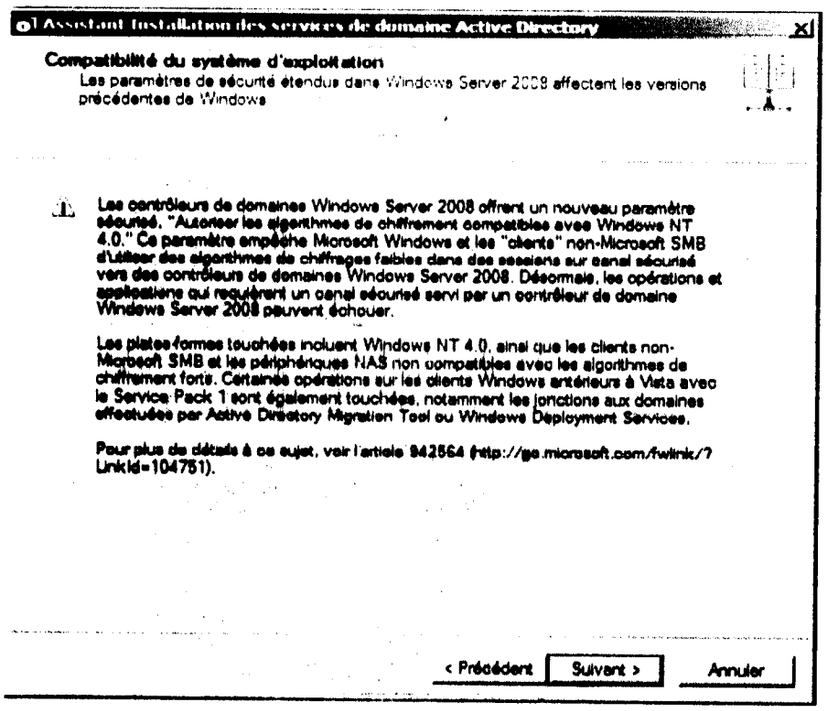
Une fois l'installation terminée un récapitulatif des éléments installés et l'état d'installation s'affiche.

Nous allons maintenant pouvoir commencer l'installation d'active Directory. On a cliqué sur le lien **Fermez cet assistant et lancer l'assistant installation des services de domaine Active Directory (dcpromo.exe)**

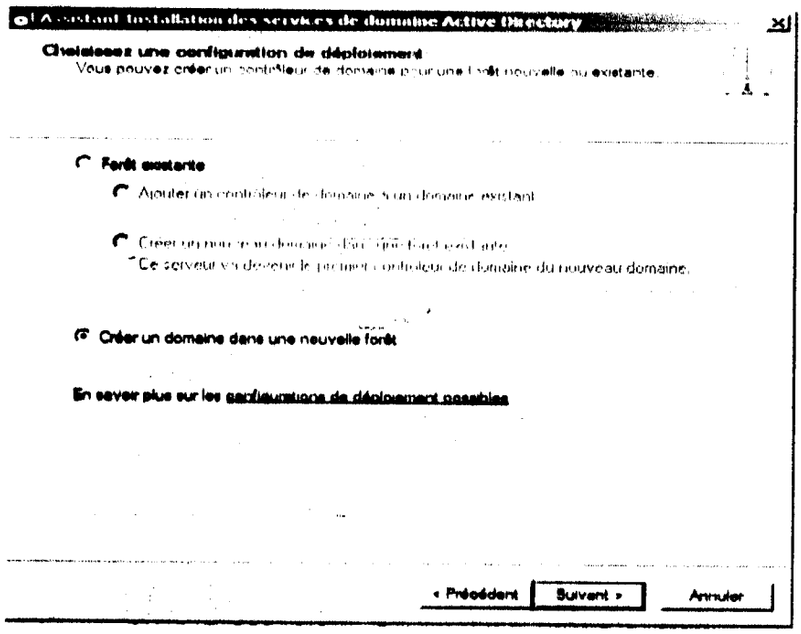


On clique sur **suivant** pour continuer.

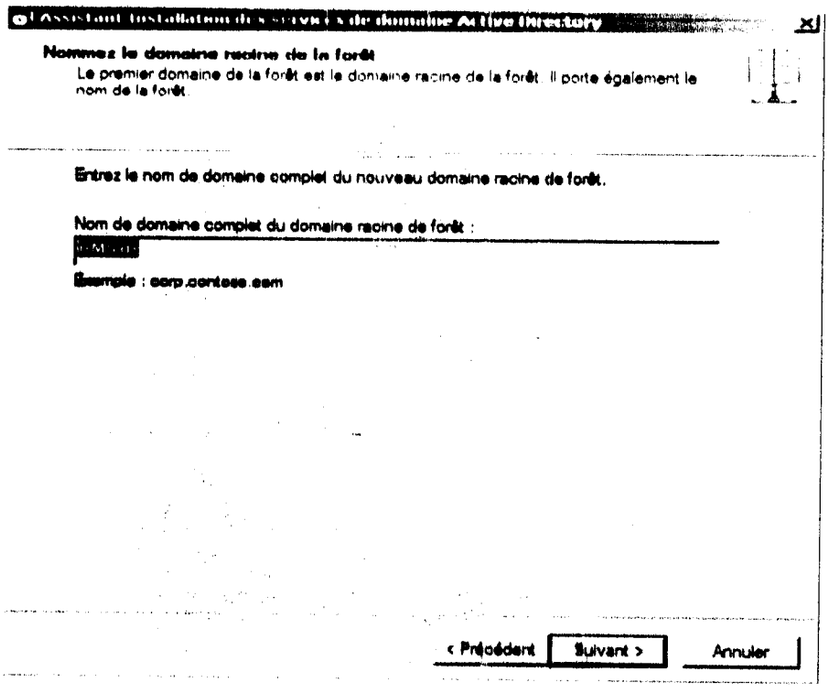




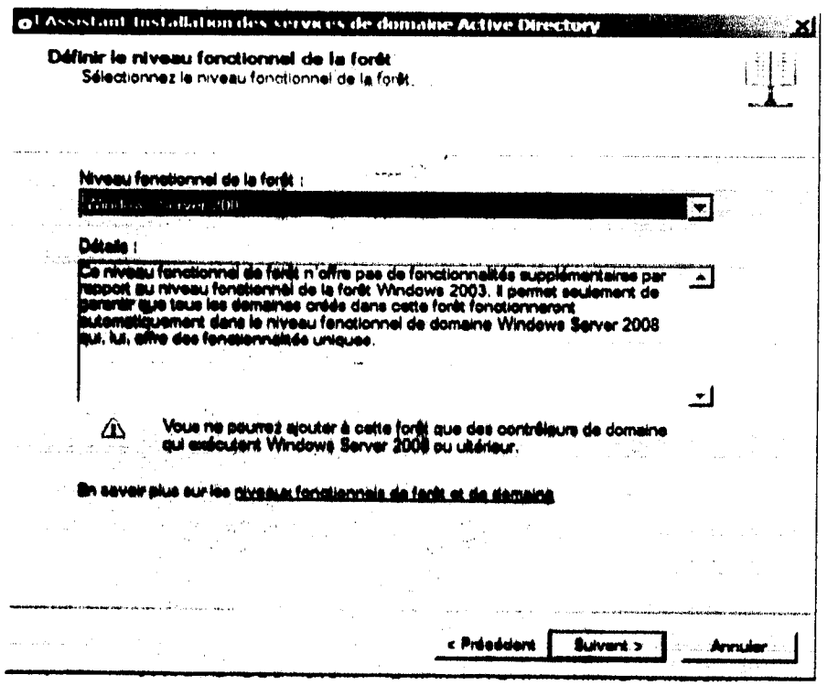
Nous allons maintenant commencer la création de notre Active Directory. On a le choix entre rejoindre une forêt existante ou créer un nouveau domaine dans une nouvelle forêt. Nous allons créer un nouveau domaine.



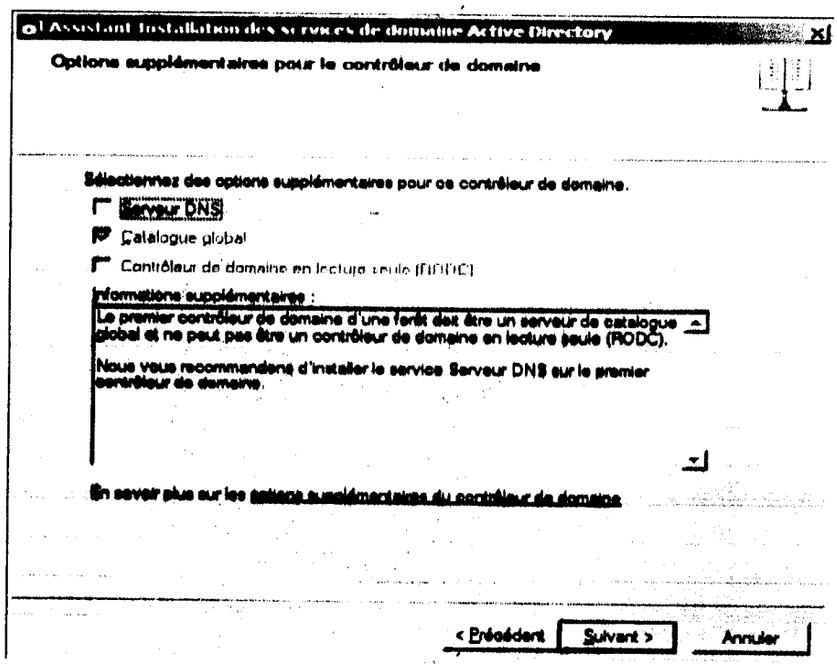
On a donné un nom de domaine racine de forêt : **RMS.dz**



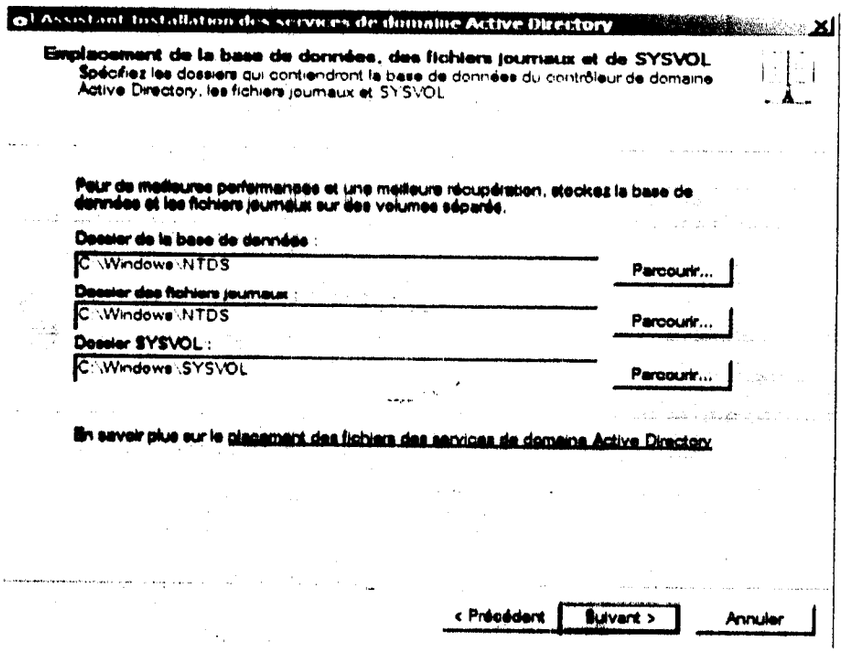
On a choisit donc le niveau fonctionnel le plus élevé afin de profiter de toutes les spécificités Propres à Windows Server 2008.



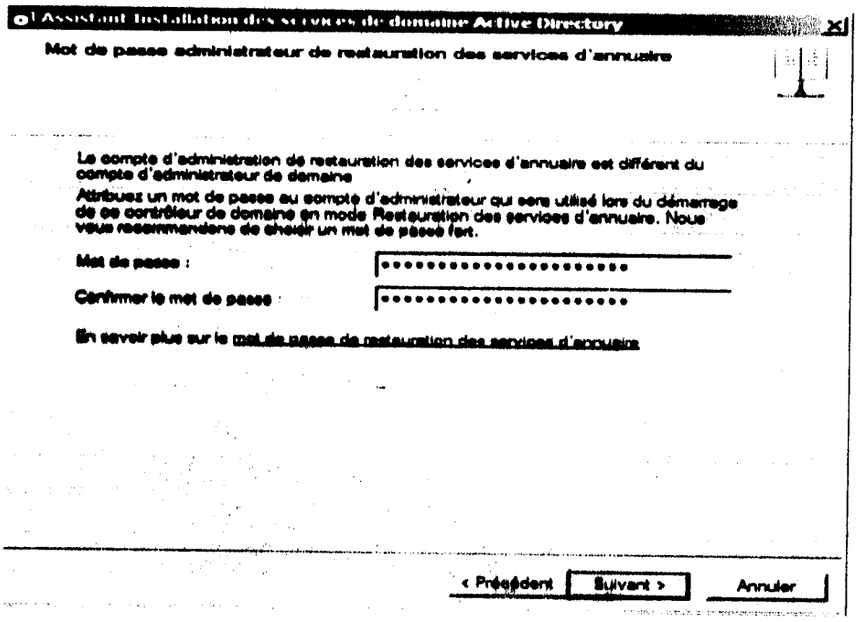
Des options supplémentaires pour le contrôleur de domaine



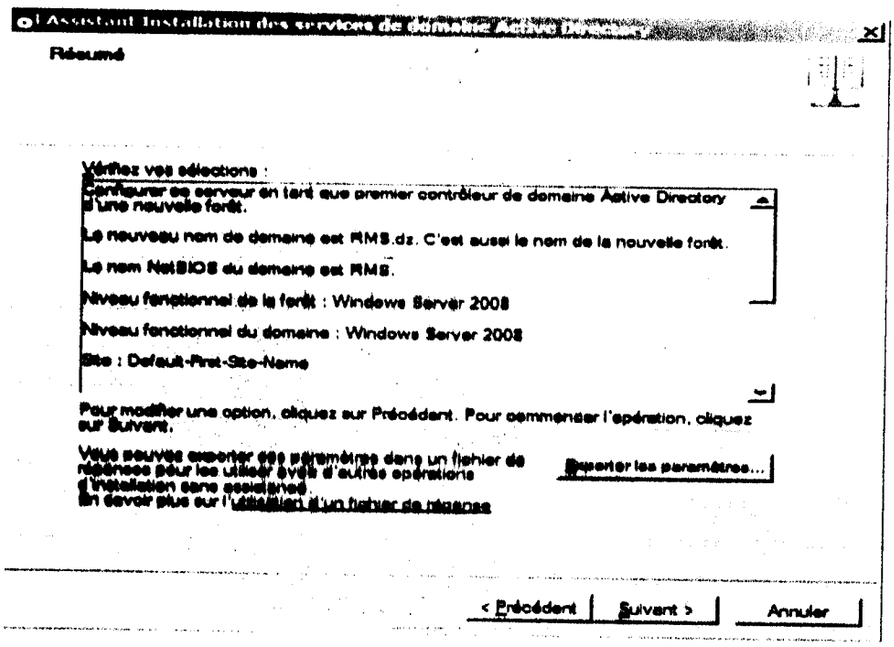
Emplacement de la base de données du contrôleur de domaine Active Directory. On a cliqué sur **Suivant.**



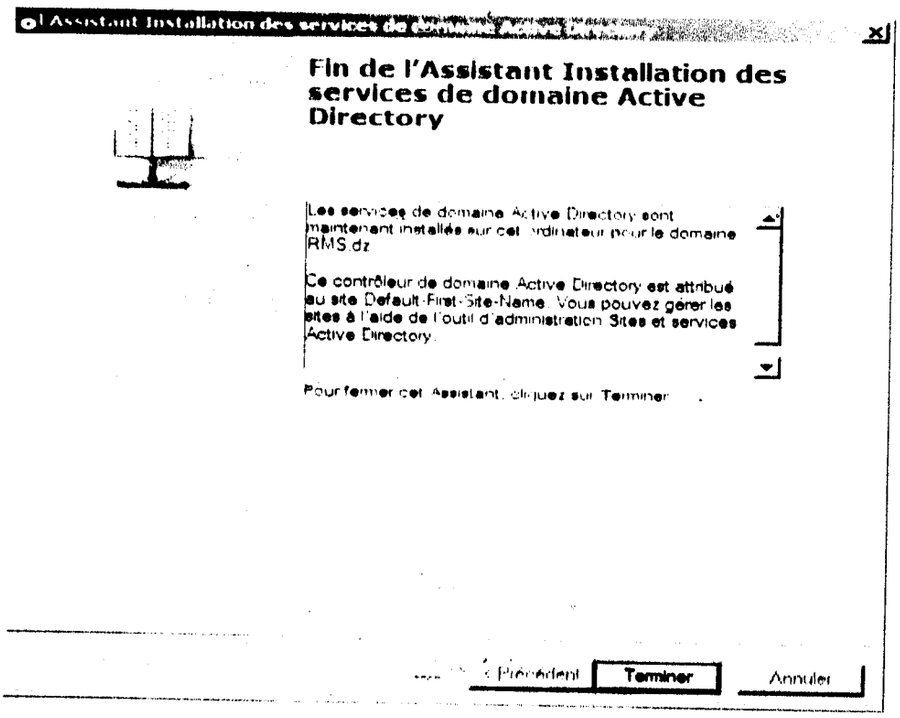
La création d'un mot de passe de restauration (**bouchikhiamine-inf2011).** A conserver précieusement ! Ce mot de passe sera indispensable pour réaliser des opérations de maintenance.



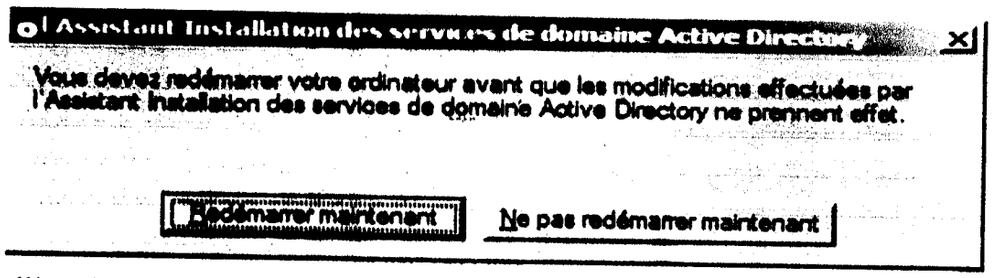
Un résumé de l'installation va être fait.



L'installation peut commencer



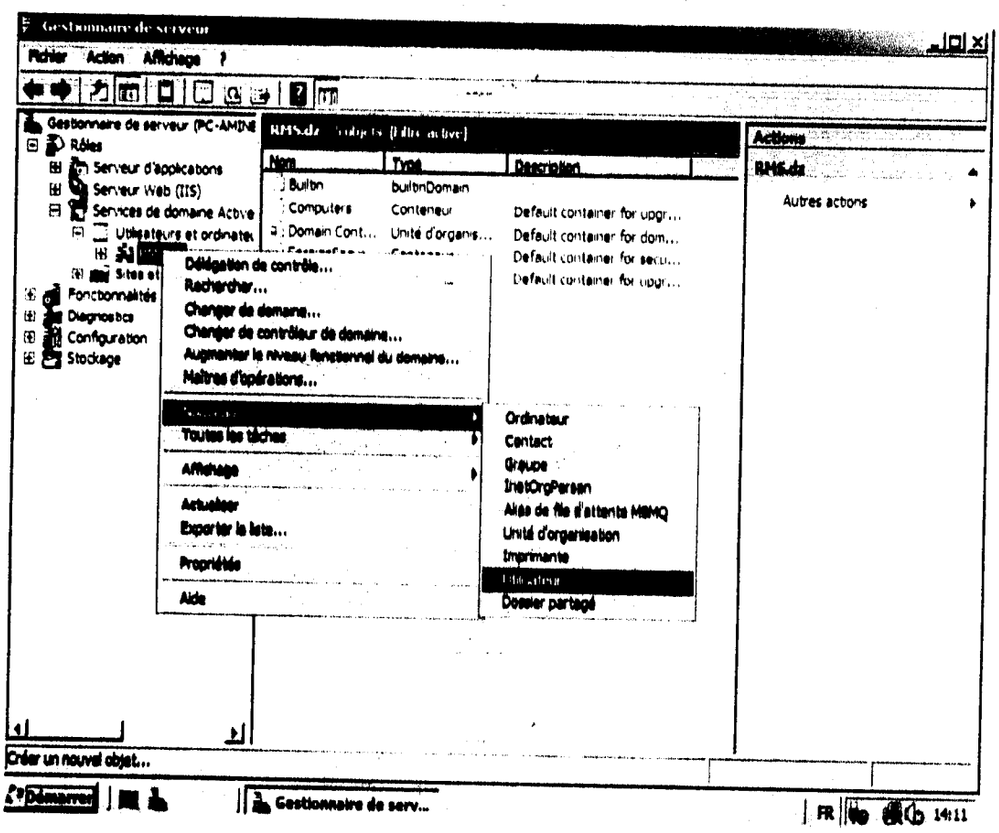
Une fois terminée on est invité à redémarrer notre système.



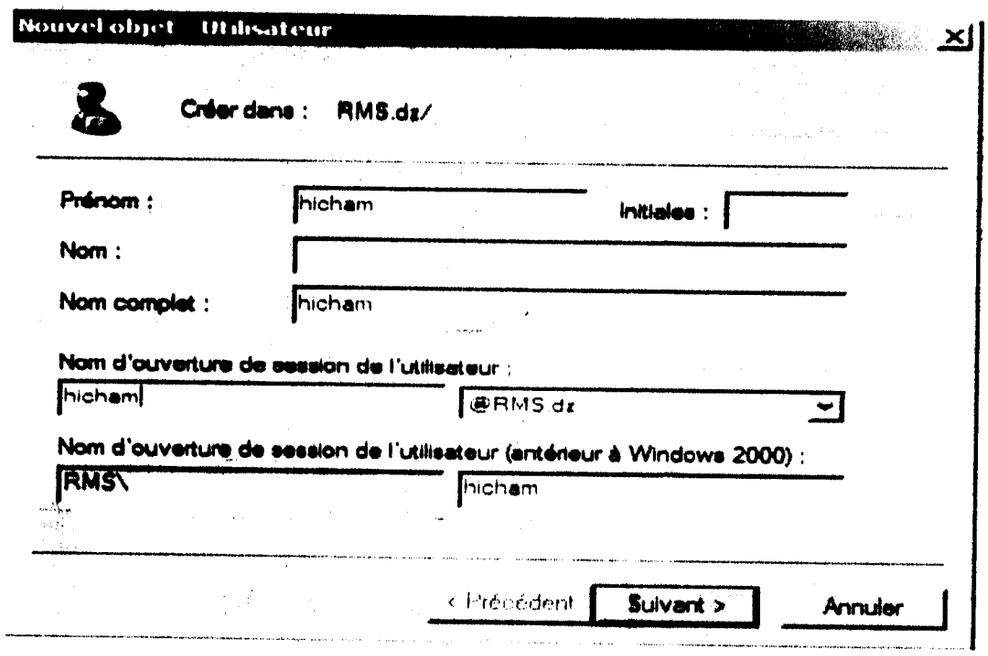
Après l'installation nous allons créer un utilisateur et un groupe dans Active Directory pour les utilisateurs du réseau WI-FI.

III.3.a La création d'un utilisateur dans Active Directory

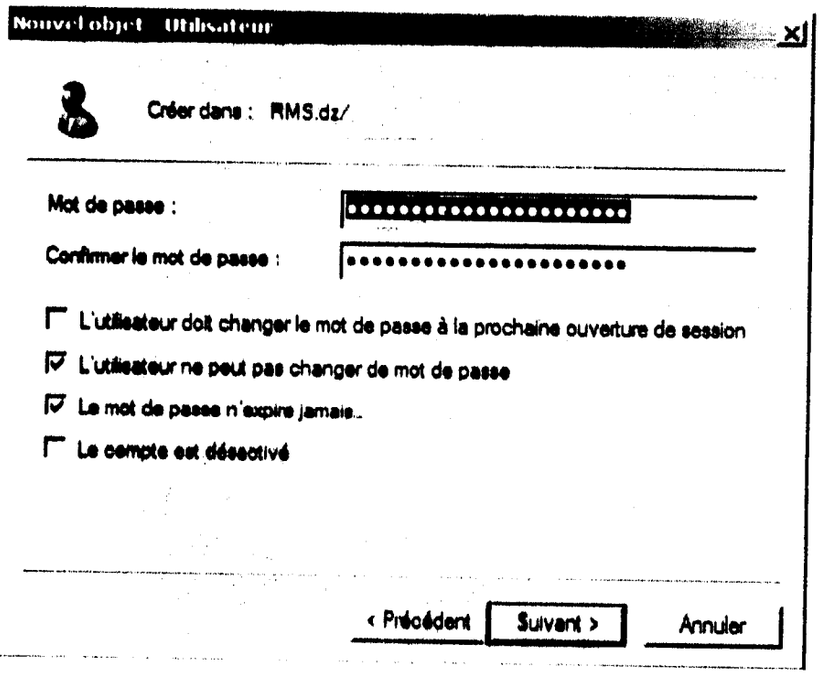
On a accédé au **Rôle** puis **Services de domaine Active Directory,** ensuite Utilisateur et **ordinateurs Active Directory,** puis on a fais un clic droit de la souris sur **RMS.dz après Nouveau** et à la fin **Utilisateur.**



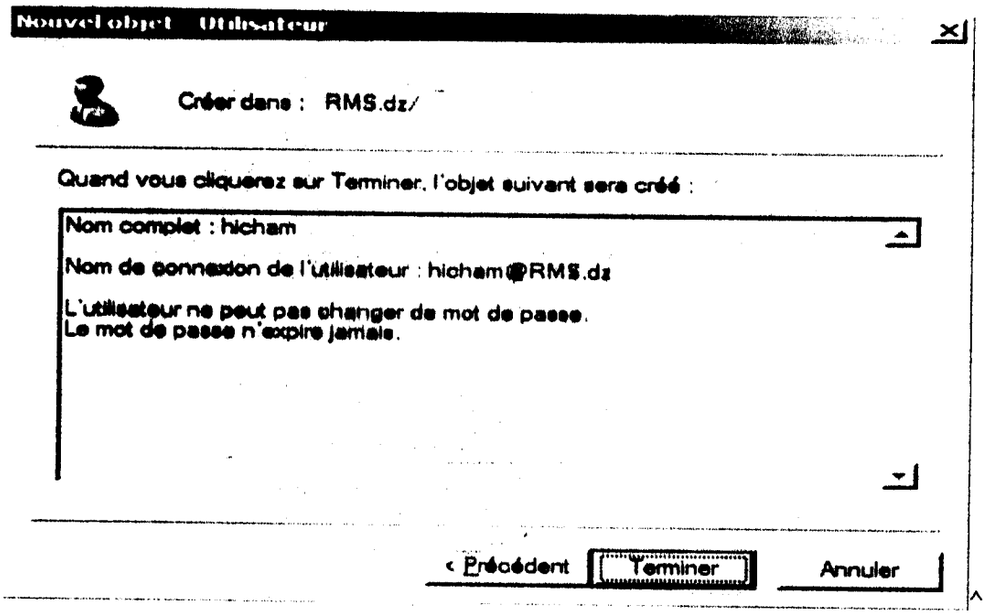
On a créé un utilisateur qu'on a nommé **hicham**, puis un clic sur **suivant.**



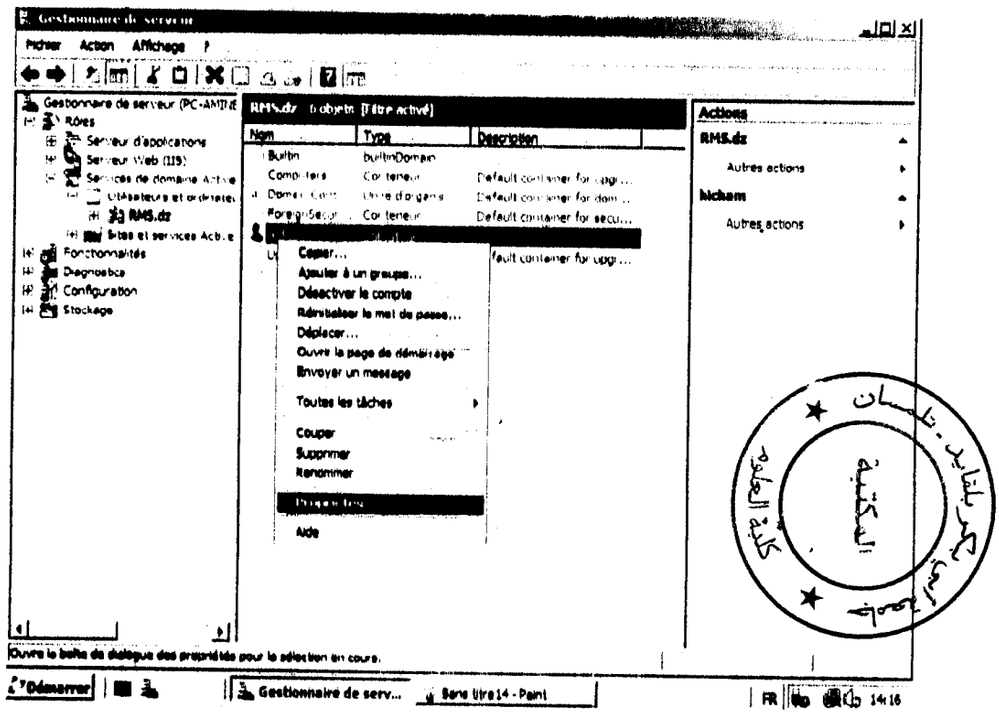
Ensuite faut taper le mot de passe et les options du compte du hicham, puis **Suivant.**



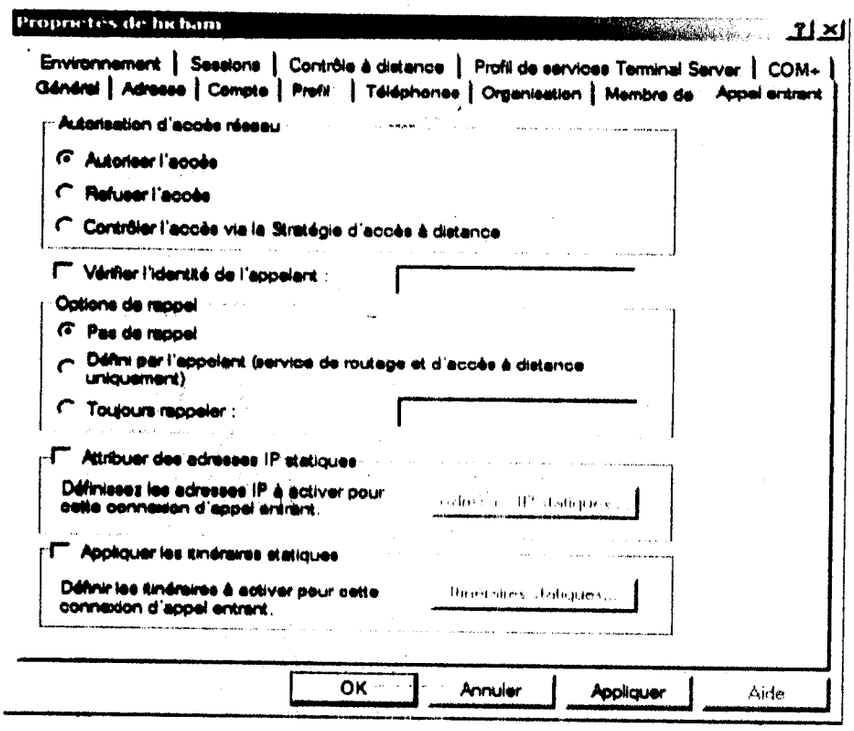
Maintenant on a créé hicham comme étant un utilisateur, cliqué **Terminer.**



Ensuite un clic droit sur **hicham** puis **propriété**.



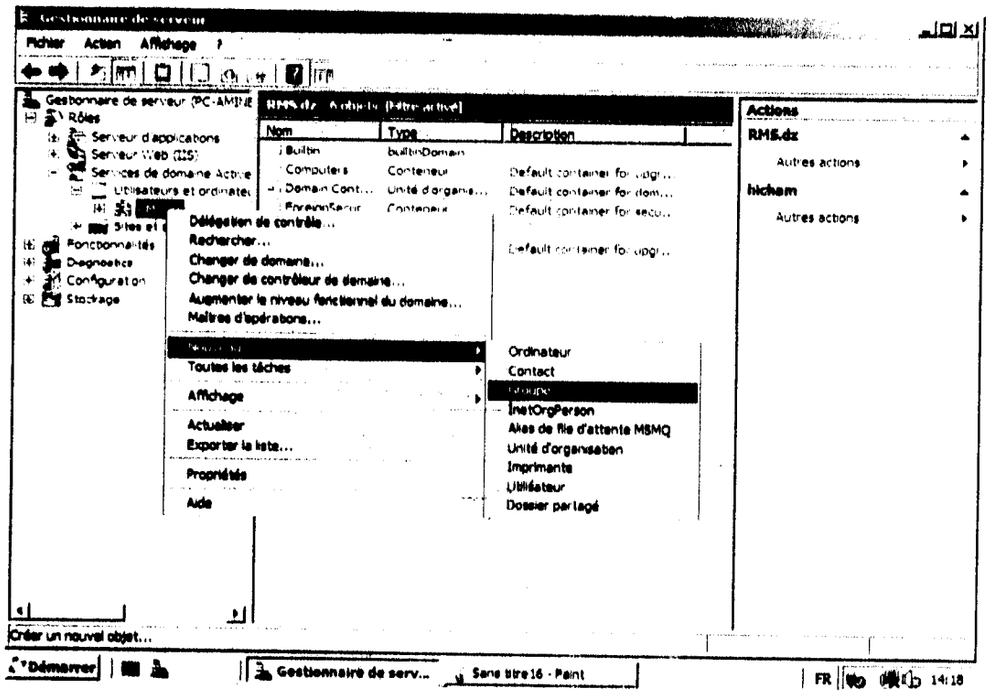
Dans l'onglet **Appel entrant** puis **Autorisation d'accès réseau** on a coché **Autoriser l'accès** et à la fin **OK**



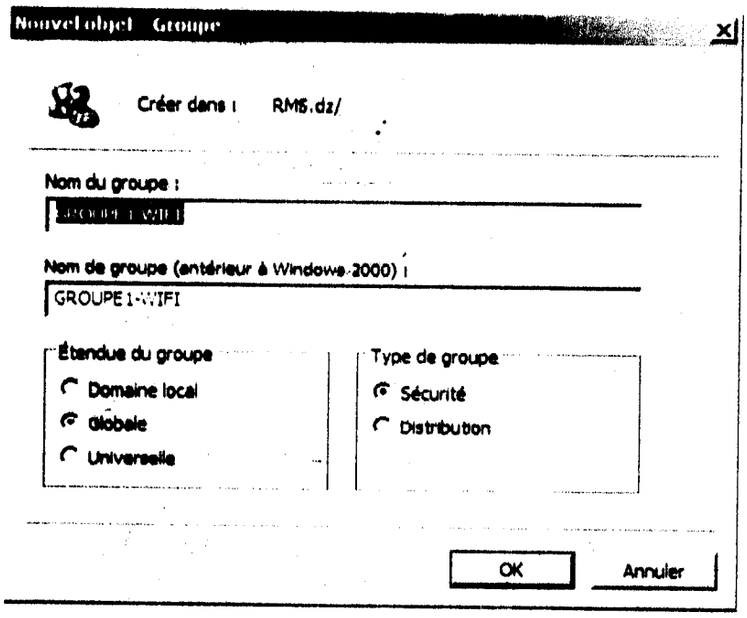
Maintenant on va créer un groupe d'utilisateurs contenant des utilisateurs autorisés pour accéder à notre réseau WI-FI.

III.3.b La création d'un groupe dans Active Directory

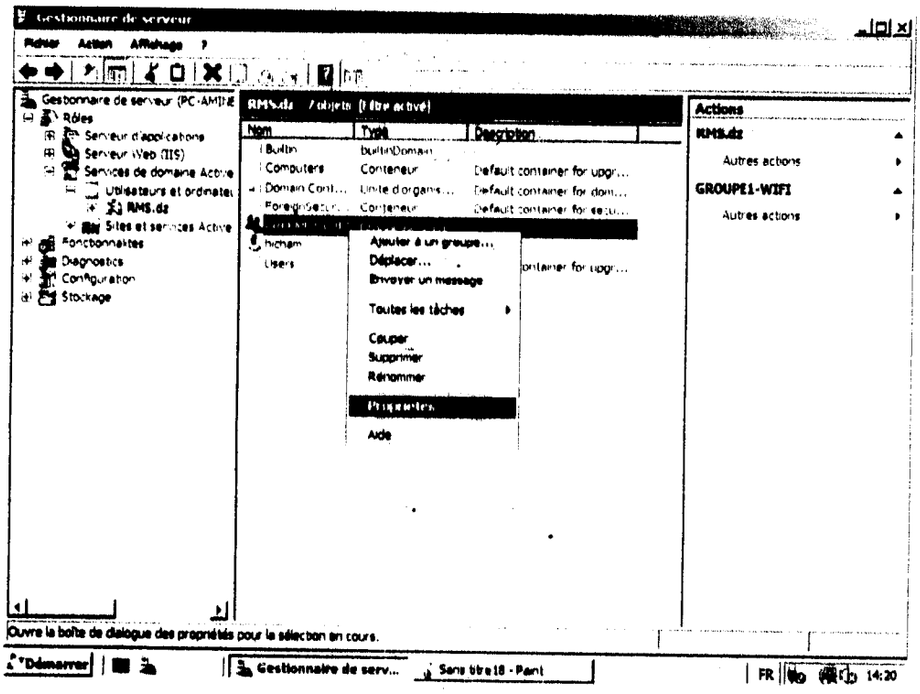
On a fait un clic droit sur **RMS.dz**, puis Nouveau ensuite **Groupe.**



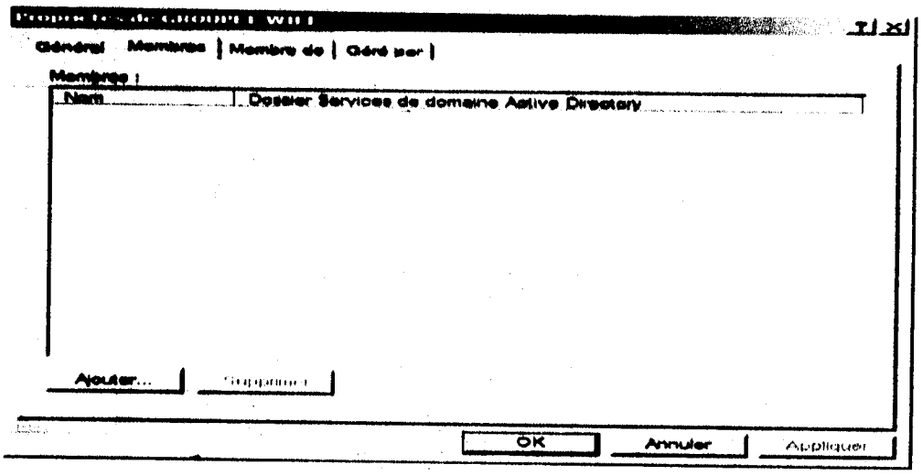
On a nommé notre groupe **GROUPE1-WIFI.**



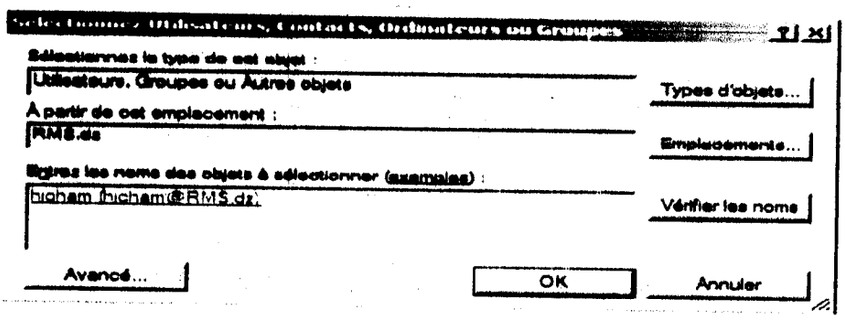
On a cliqué sur le groupe **GROUPE1-WIFI** puis **Propriétés**



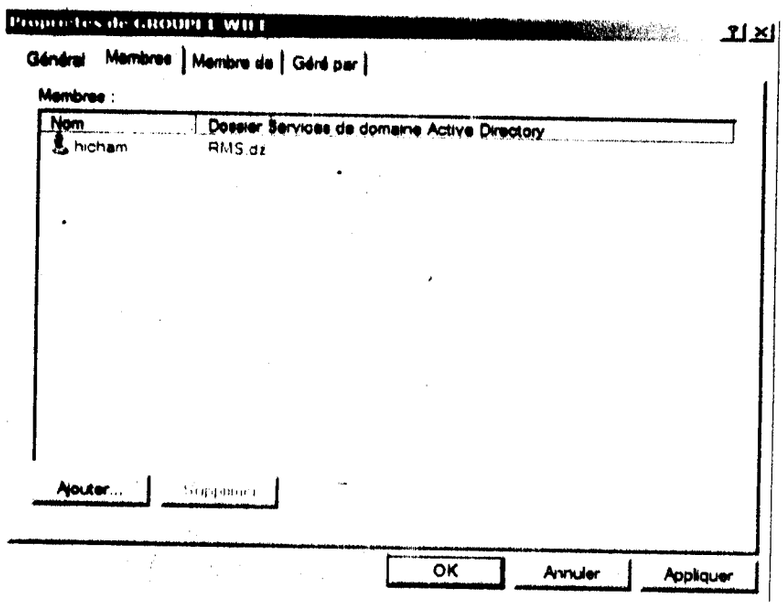
Dans l'onglet **Membres**, on a sélectionné **Ajouter.**



On a ajouté l'utilisateur **hicham,** en suite **OK.**



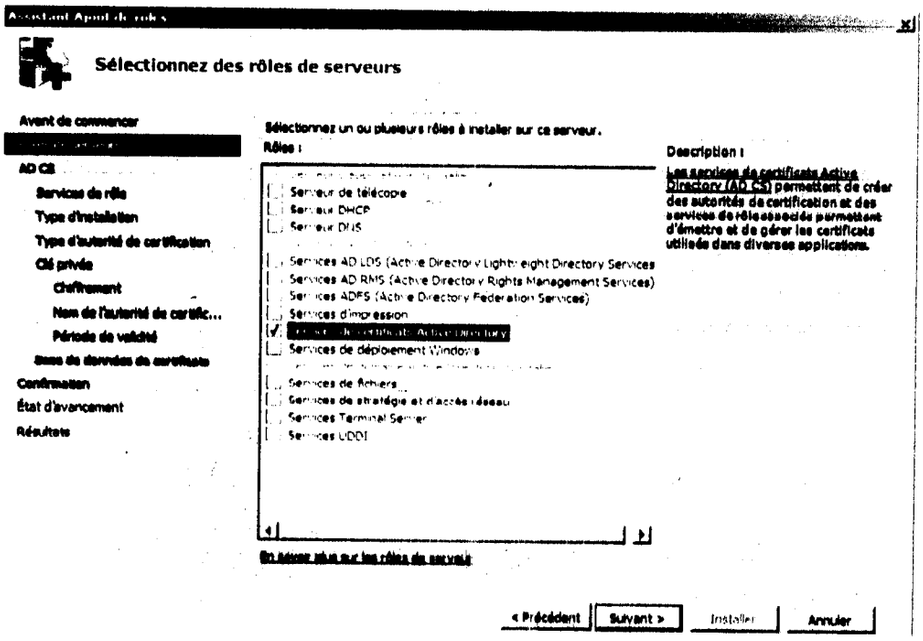
Ensuite on a validé par **OK.**



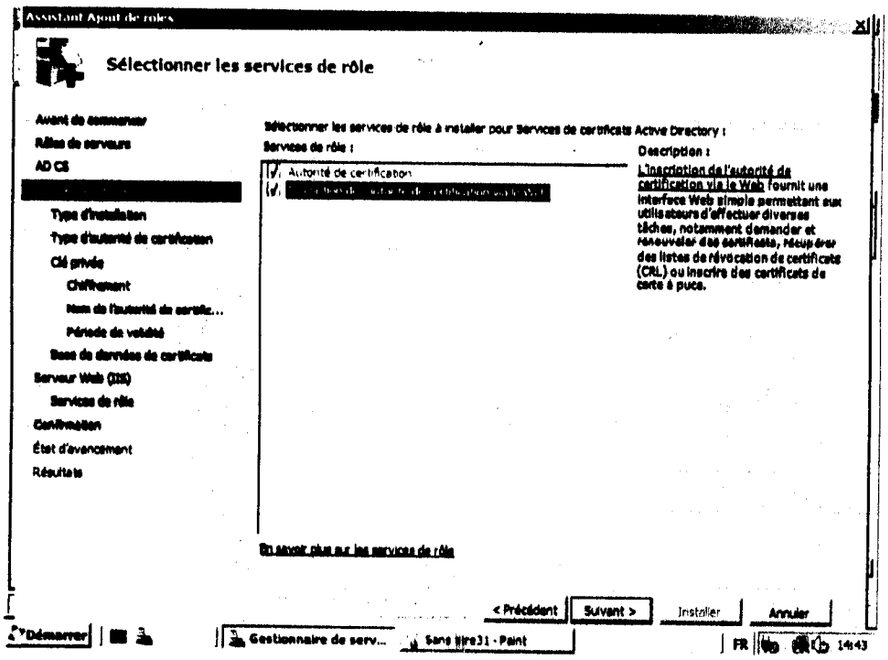
Donc maintenant **hicham** fait partie de **GROUPE-WIFI.** On peut répéter la procédure autant de fois pour créer d'autres utilisateurs.

III.4 Services de certificats Active Directory

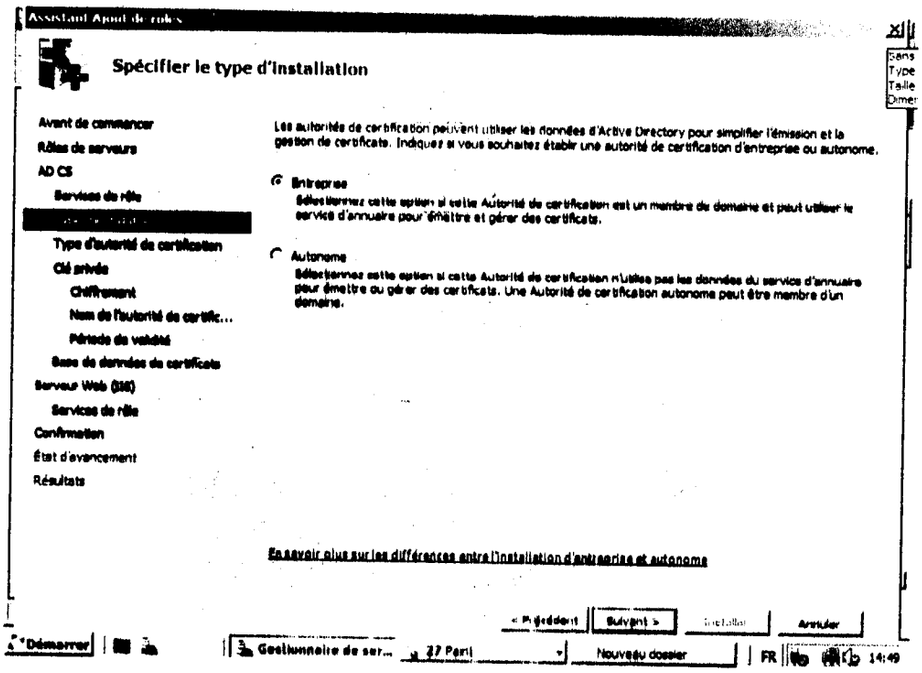
Utiliser pour l'installation des Autorités de certification Racine, qui permettent de délivrer des certificats.



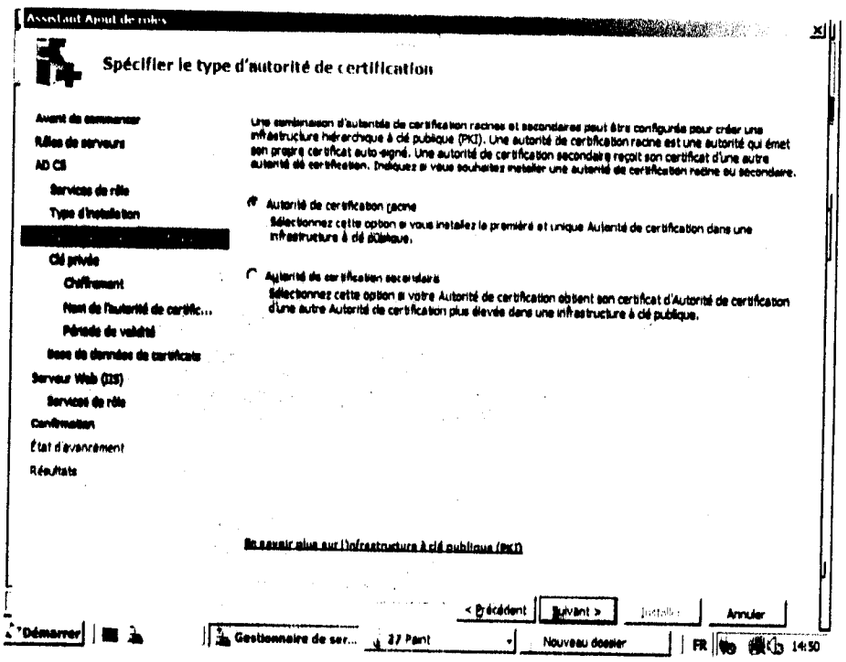
On a coché les services de rôle requis à installer pour services de certificats Active Directory, ensuite on a cliqué sur **Suivant.**



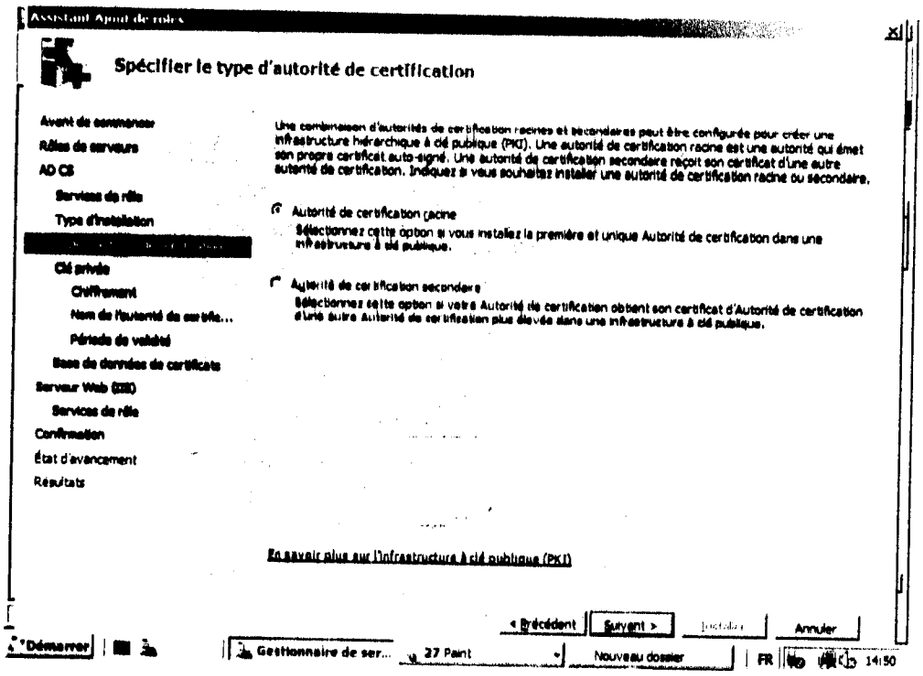
Nous sommes sur la page Spécifiée le type d'installation, on a sélectionné le mode **Entreprise**, puis sur **Suivant.**



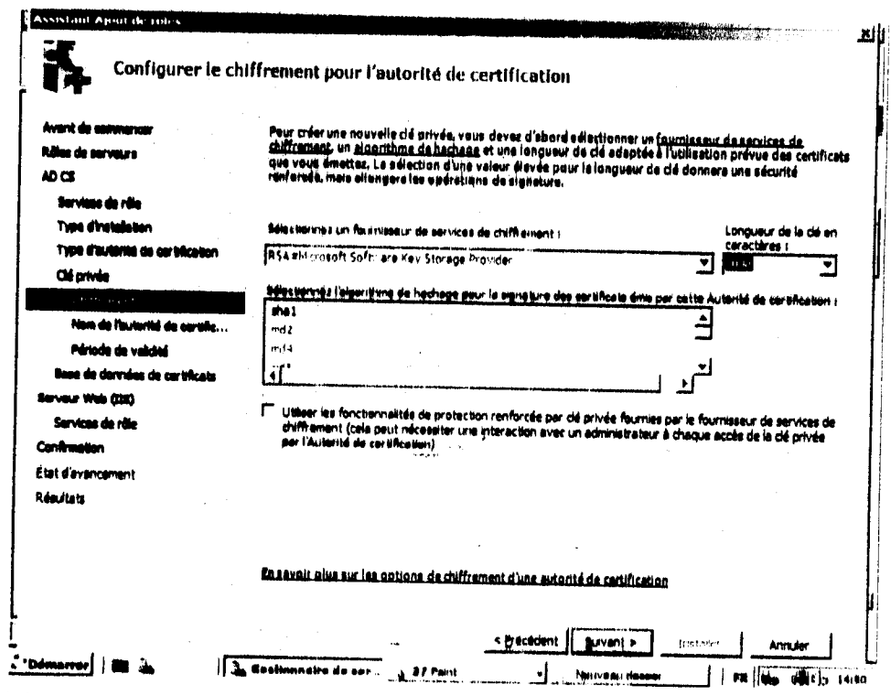
Nous sommes dans la page Spécifier le type d'autorité de certification, on a cliqué sur **Autorité de certification racine**, car ceci est notre première autorité de certificat, puis sur **Suivant**.



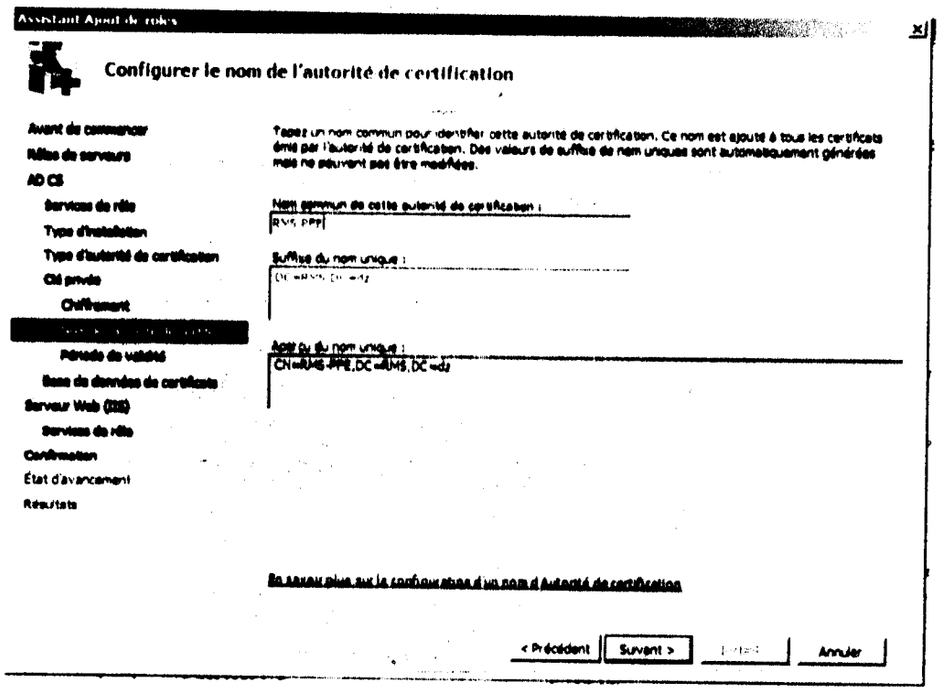
Dans cette page on clique su **Créer une nouvelle clé privée,** puis sur **Suivant.**



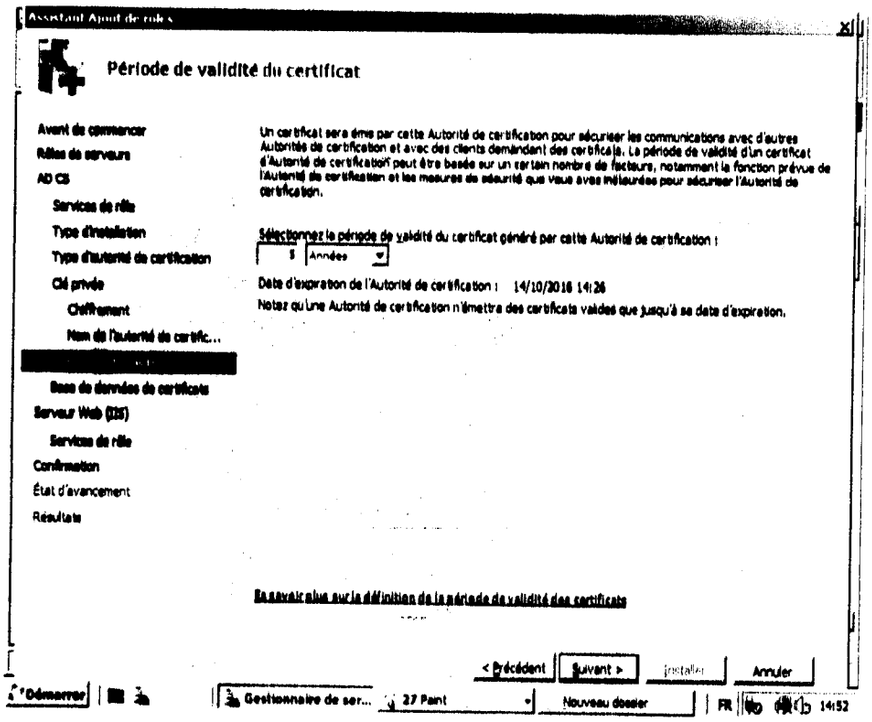
Encore **Suivant.**



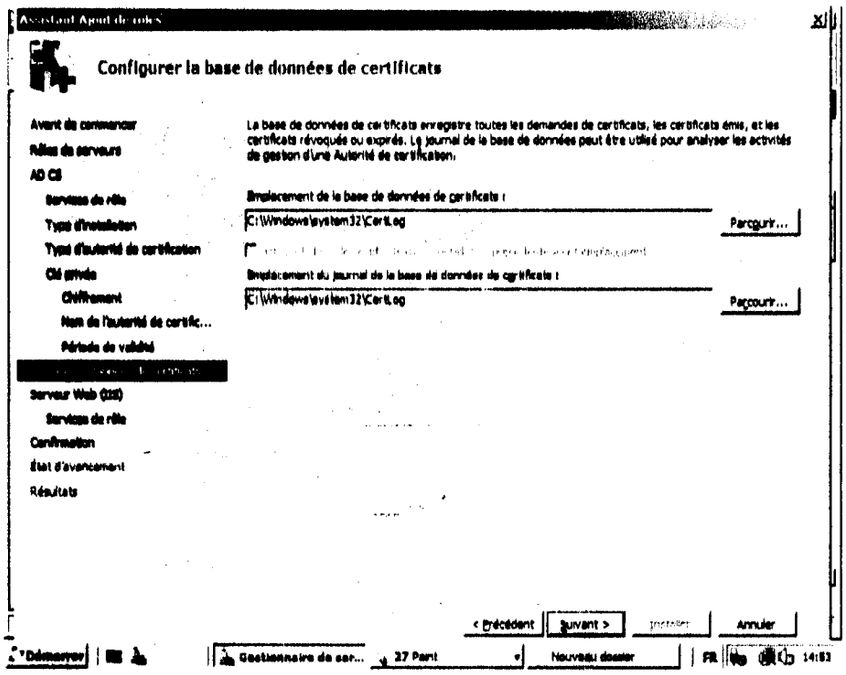
On a choisit **RMS-PFE** comme un nom de l'autorité de certification, et on clique sur **Suivant.**



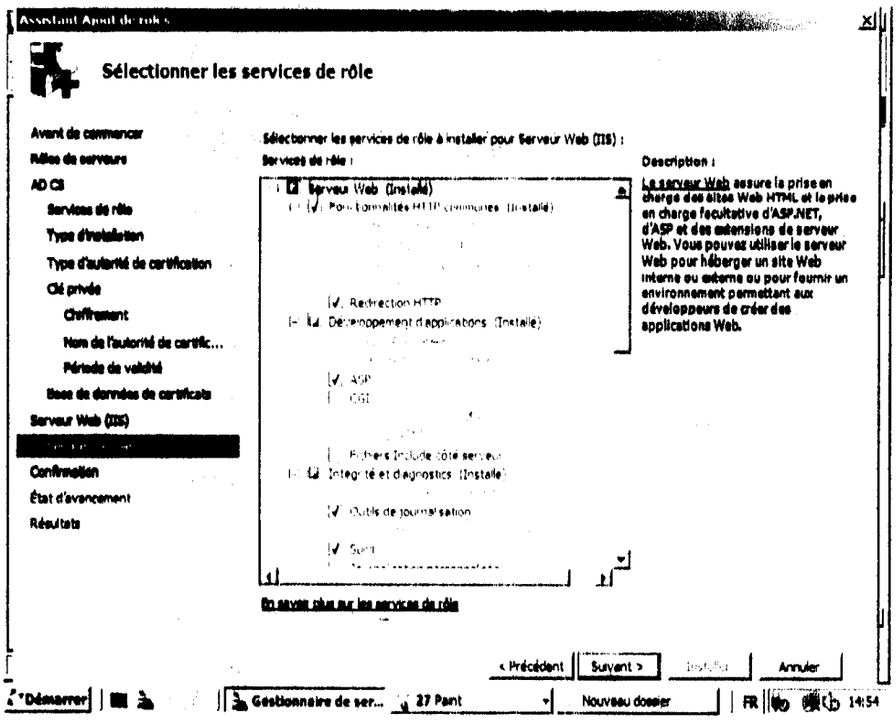
On a sélectionné la durée de validité de notre autorité de certification racine, puis on a cliqué sur **Suivant.**



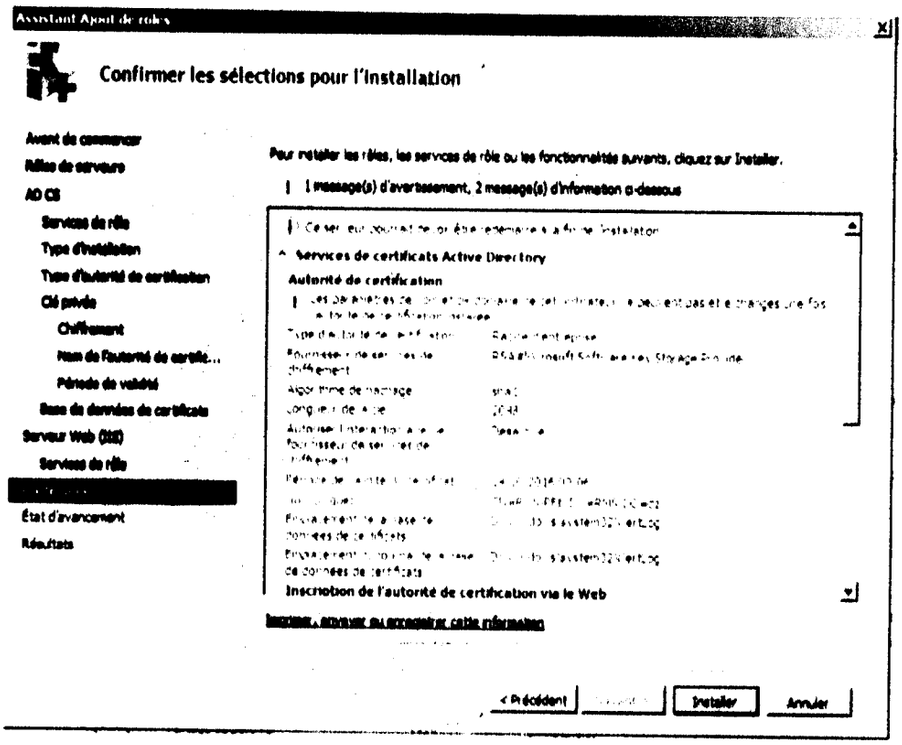
On a accepté les valeurs par défaut pour l'emplacement de stockage pour la base de données de certificats et son journal, puis on clique sur **Suivant.**



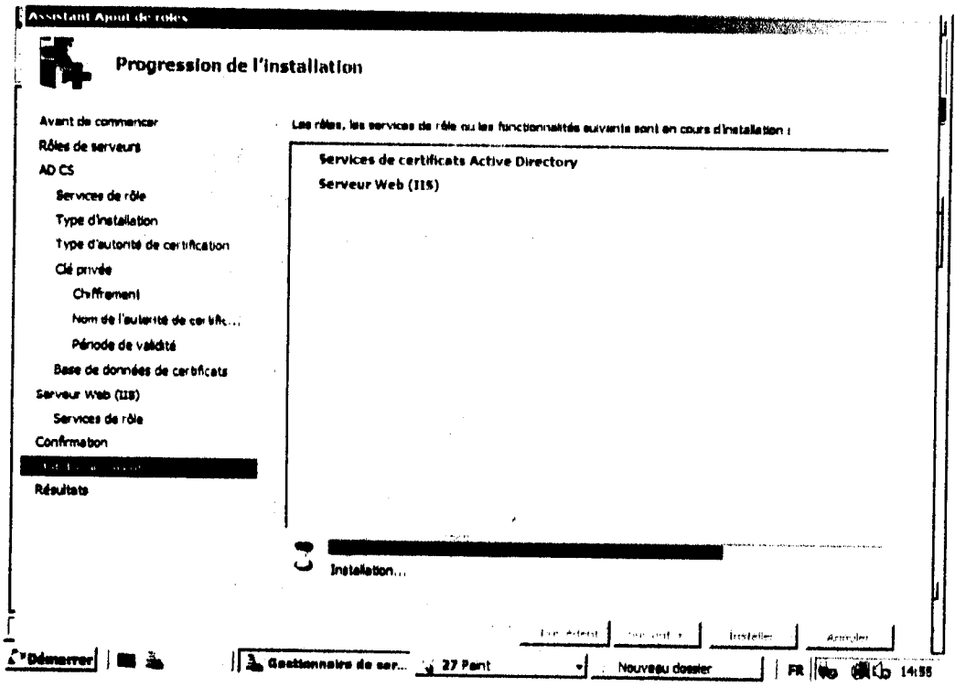
Il faut cocher les services de rôle requis, à installer et on a cliqué sur **Suivant.**



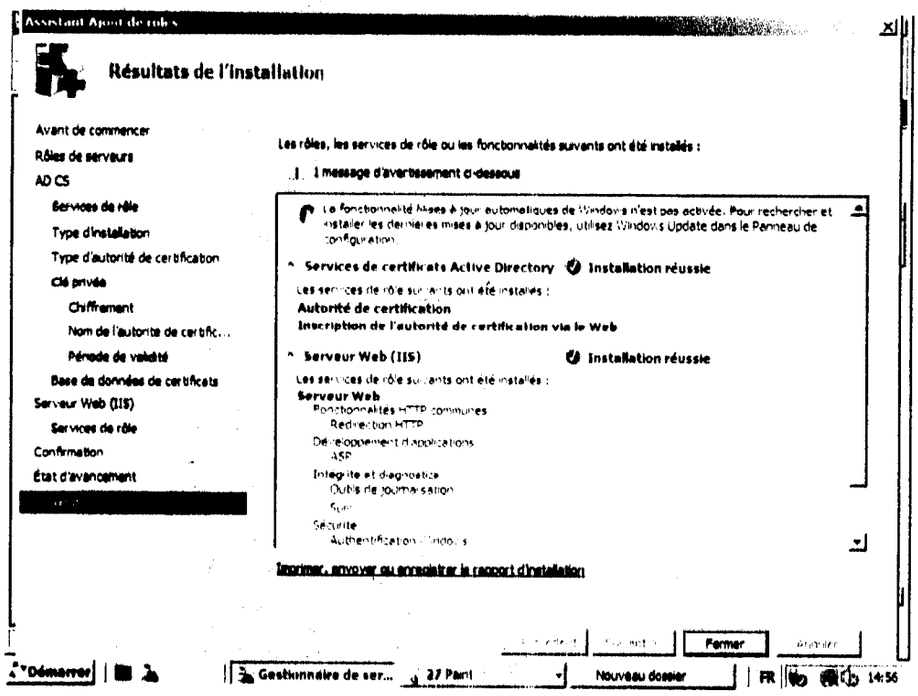
On a cliqué sur **Installer.**



L'installation en cours…

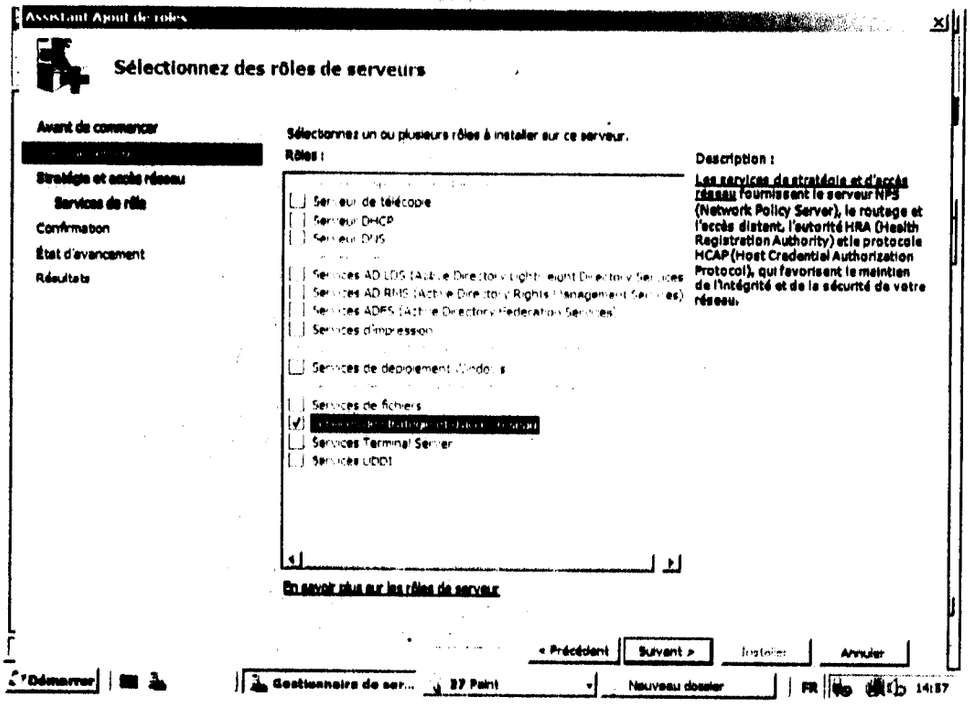


Une fois l'installation terminée, on a cliqué sur **Fermer.**

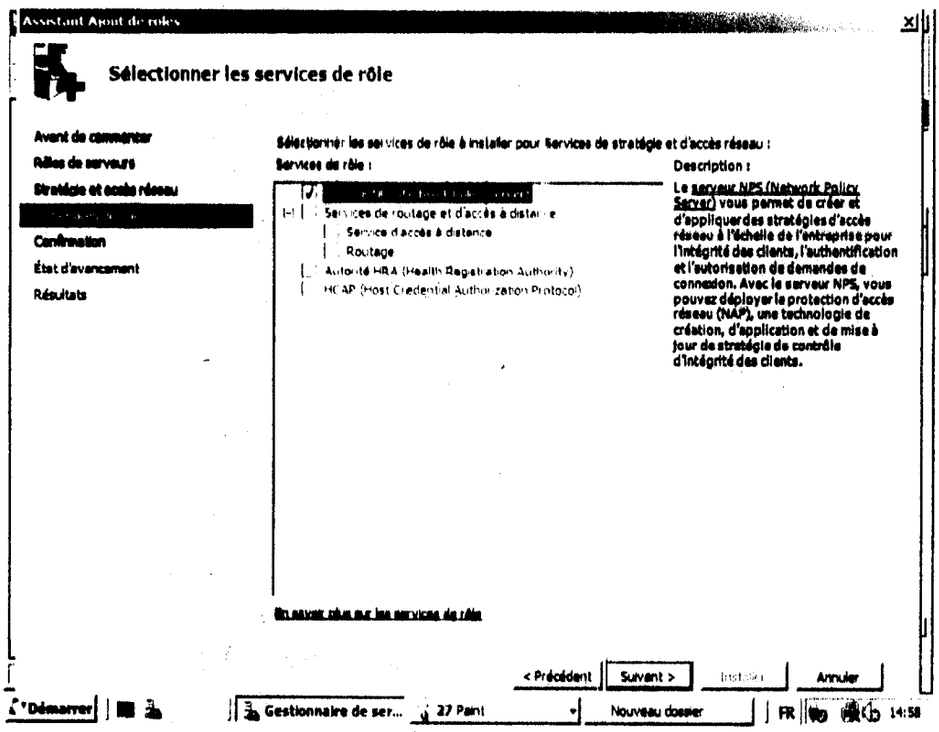


III.5 Services de Stratégies et d'accès réseau

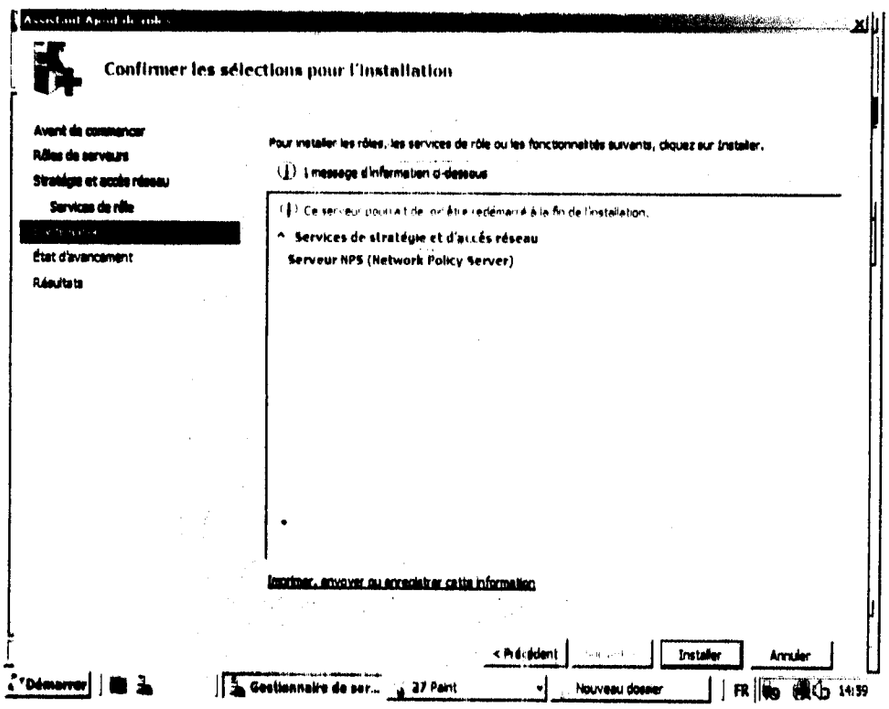
On a utilisé ce service pour la configuration de serveur RADIUS.



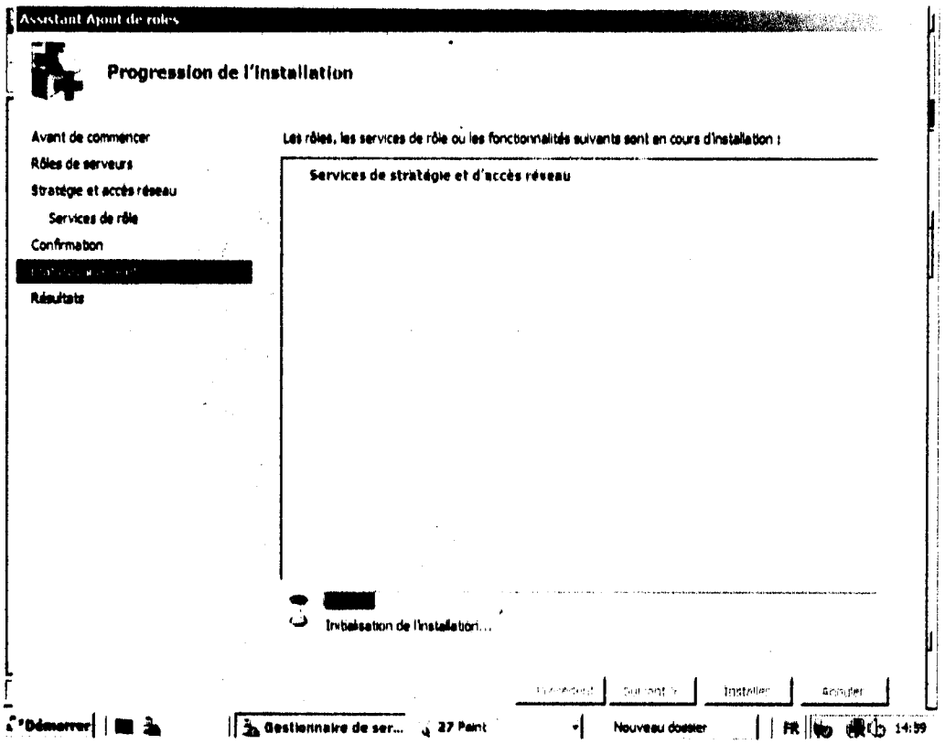
On a coché les services de rôle requis à installer pour services de stratégie et d'accès réseau, puis on a cliqué sur **Suivant.**



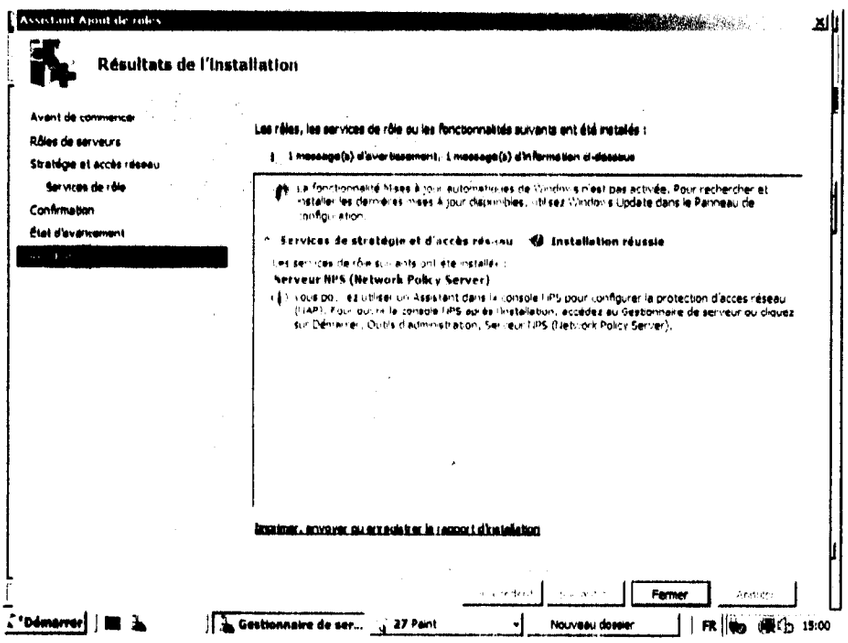
On suite on a cliqué sur **Installer** pour commencer l'installation.



L'installation en cours…



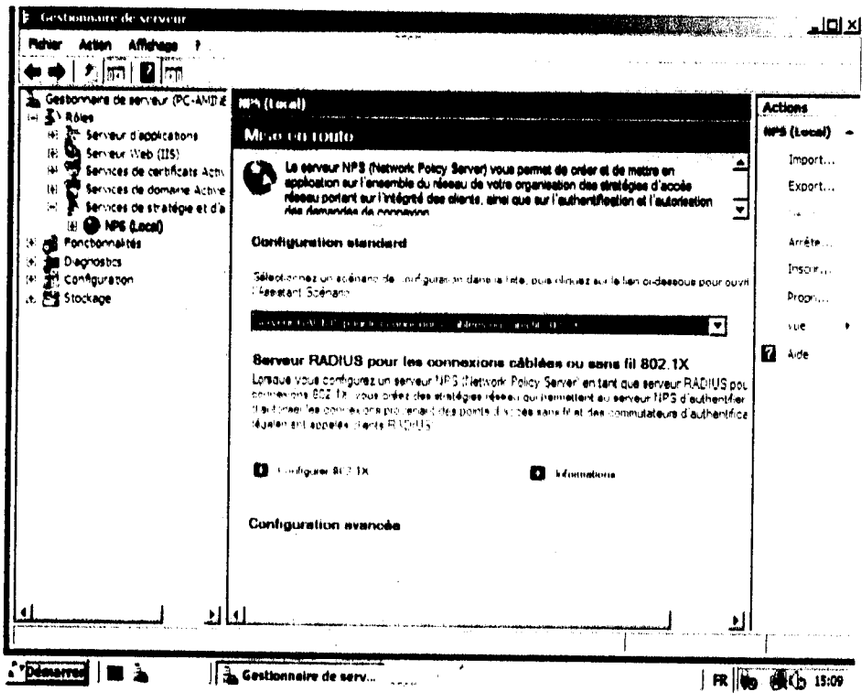
Une fois l'installation terminée on clique sur **Fermer.**



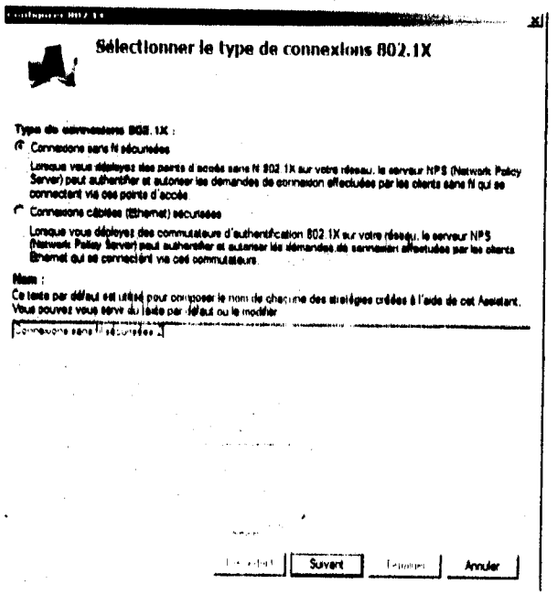
En suite on a redémarré le serveur.

III.5.1 Configuration du serveur RADIUS

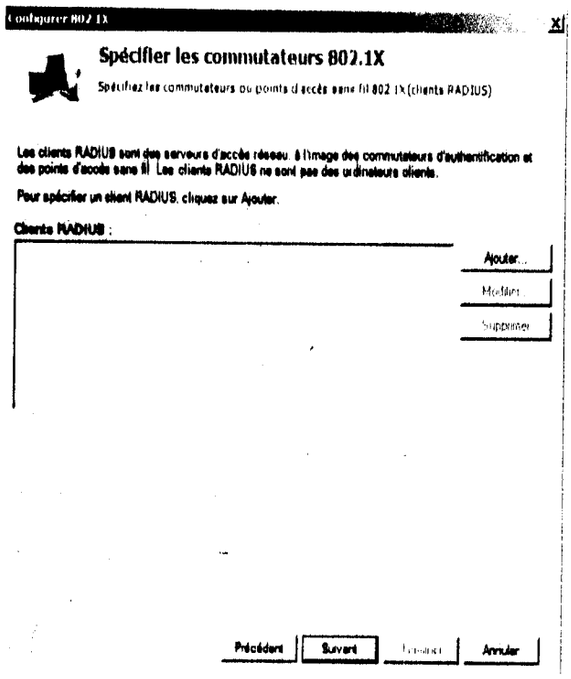
On a accéder aux **Rôles, Services de stratégie et d'accès réseau** ensuite **NPS** puis on a choisit **Serveur RADIUS pour les connexions câblées ou sans fil 802.1X** et après on a cliqué sur **Configurer 802.1X.**



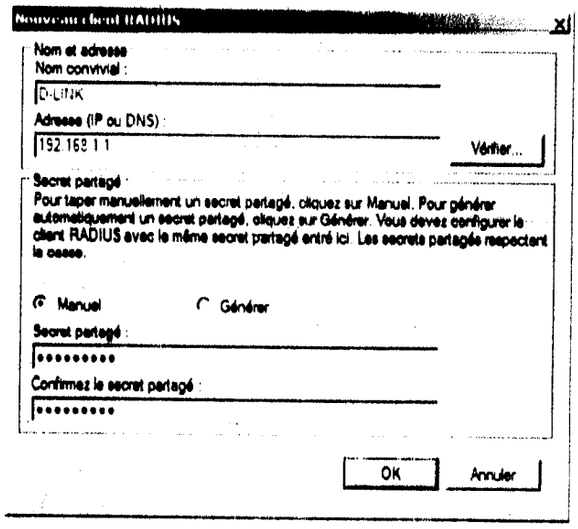
Il faut choisir comme type de connexion 802.1X **Connexions sans fil sécurisées**, et on a donné un nom : **Connexions sans fil sécurisées2.**



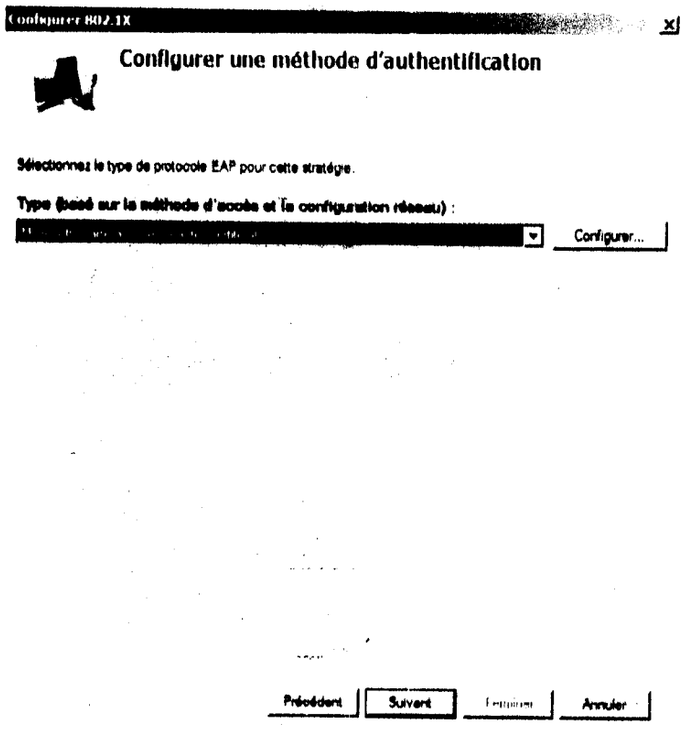
On a cliqué sur **Ajouter** pour spécifier notre point d'accès à sécuriser.



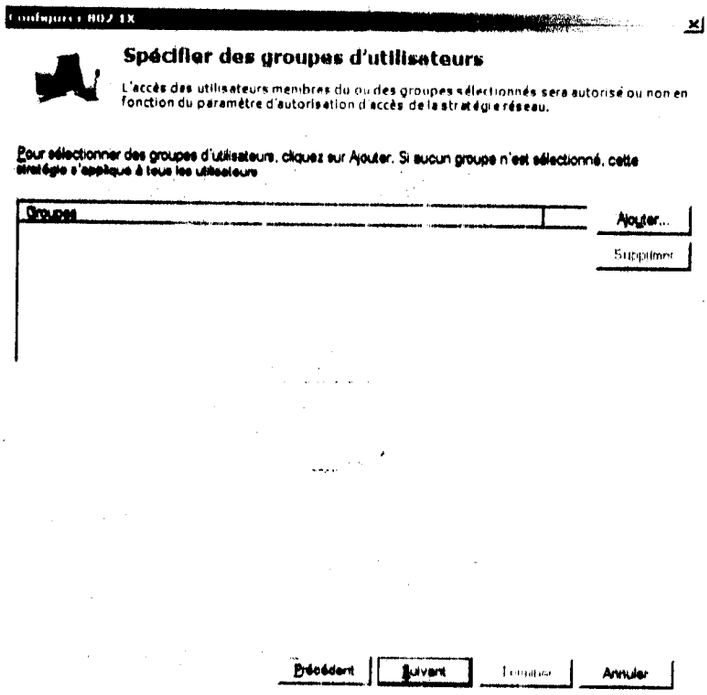
Dans cette fenêtre on a remplis le **nom** et l'**adresse** de notre point d'accès à sécuriser puis le secret partagé et on validé par **OK.**



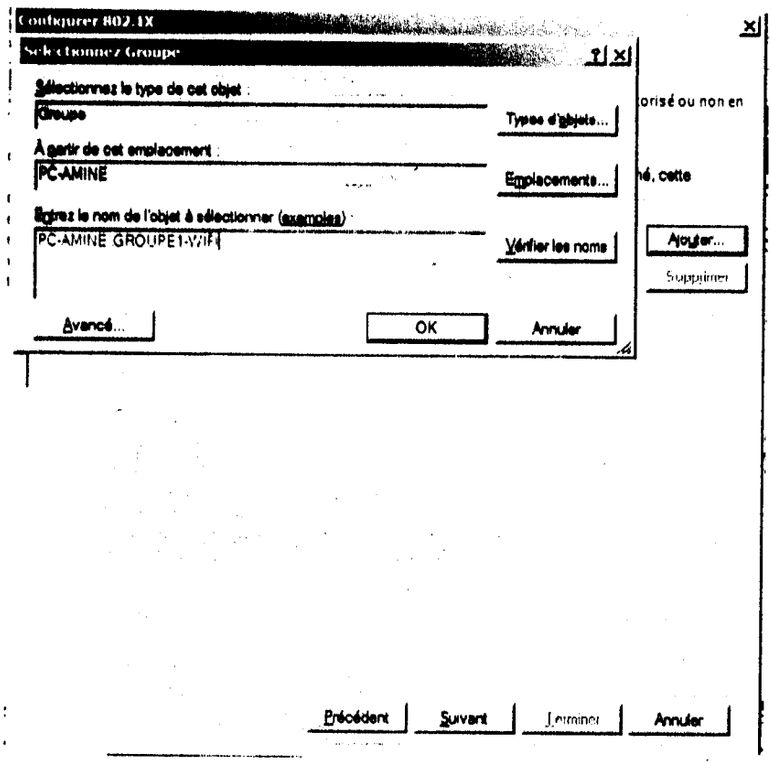
On a choisit le type de protocole EAP souhaité, pour l'utilisation des certificats.



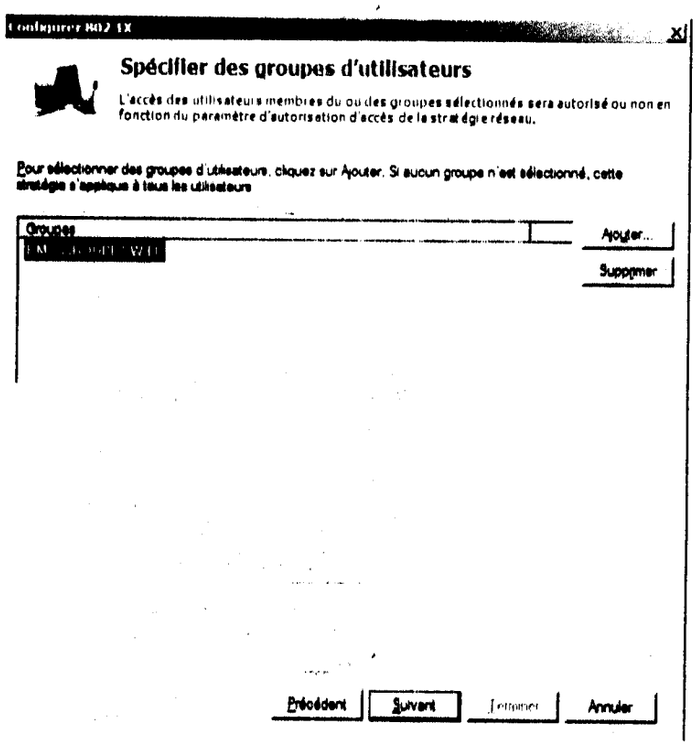
Maintenant on a ajouté le groupe qui aura accès à notre réseau WI-FI sécurisé avec RADIUS, pour cela on a cliqué sur **Ajouter.**



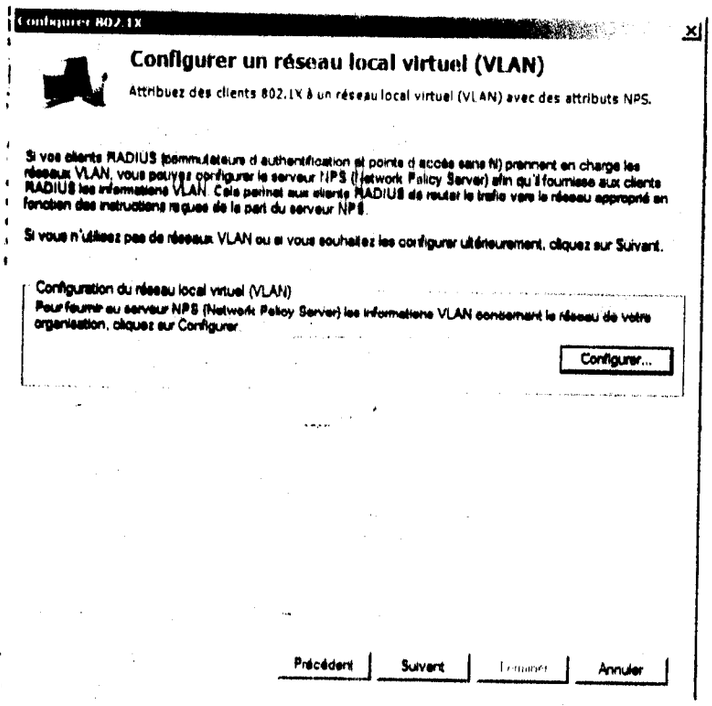
Donc on a ajouté le groupe qu'on a créé (GROUPE1-WIFI) et on a validé par **OK.**



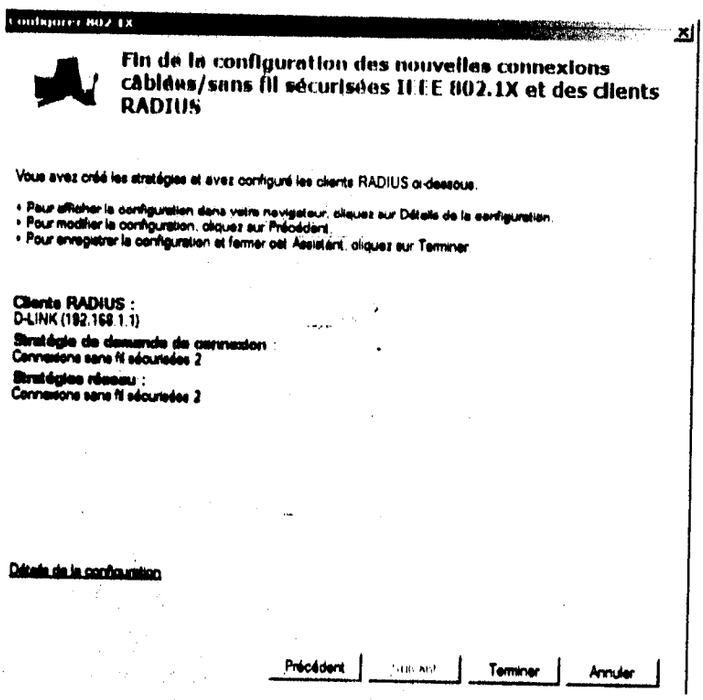
On a cliqué sur **Suivant** pour continuer.



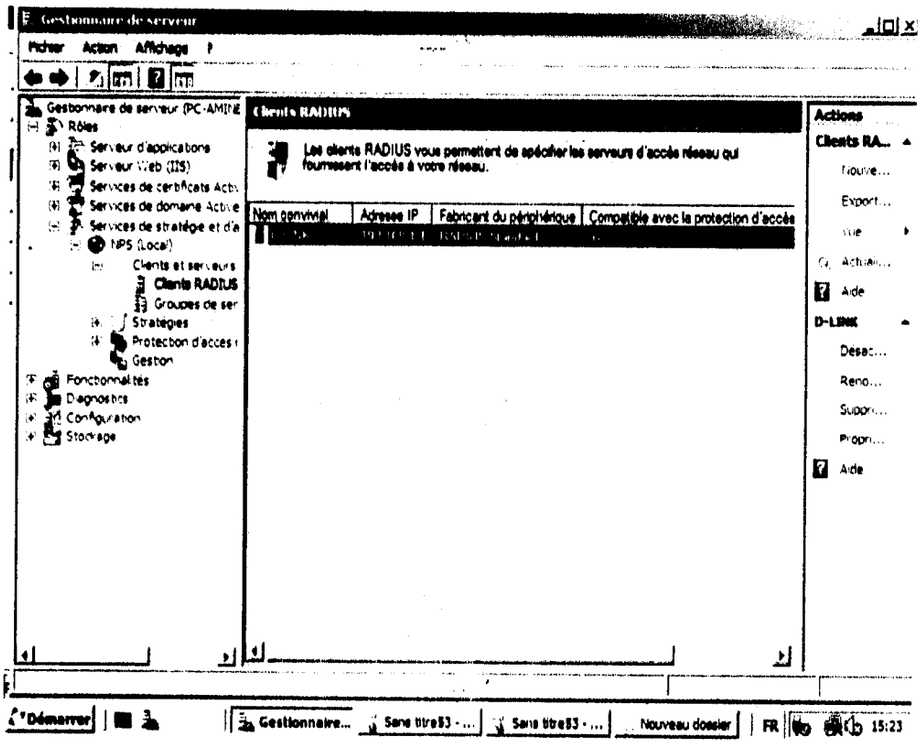
Encore **Suivant.**



En suite **Terminer.**

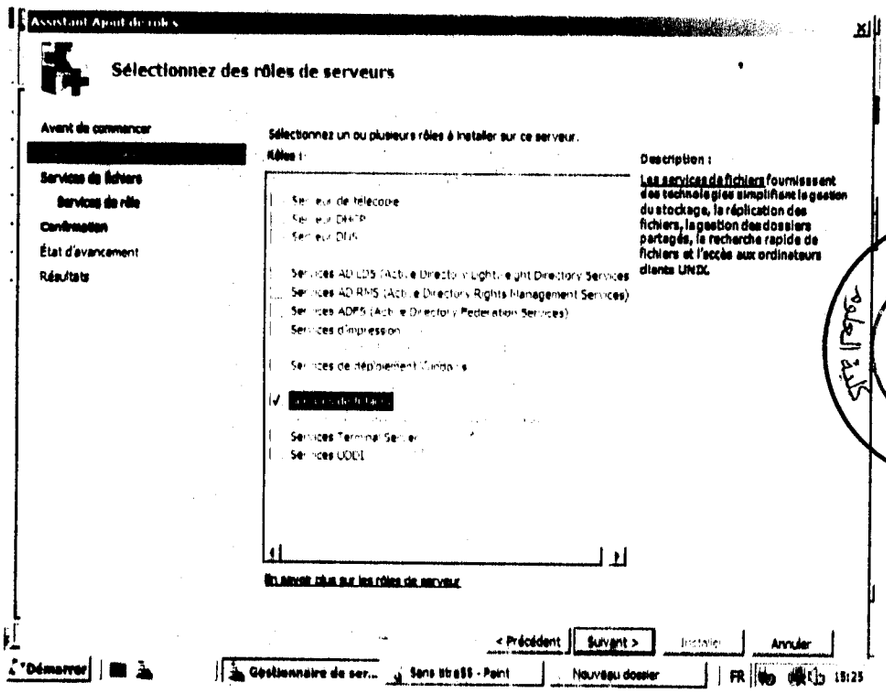


On a trouvé le nom de notre point d'accès dans la liste des clients RADIUS.

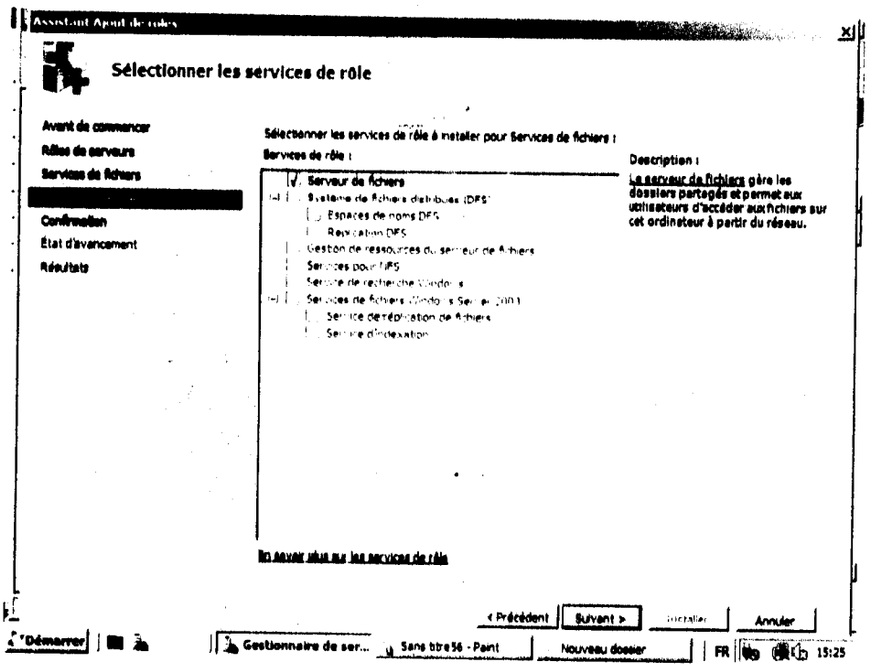


III.6 Services de fichiers

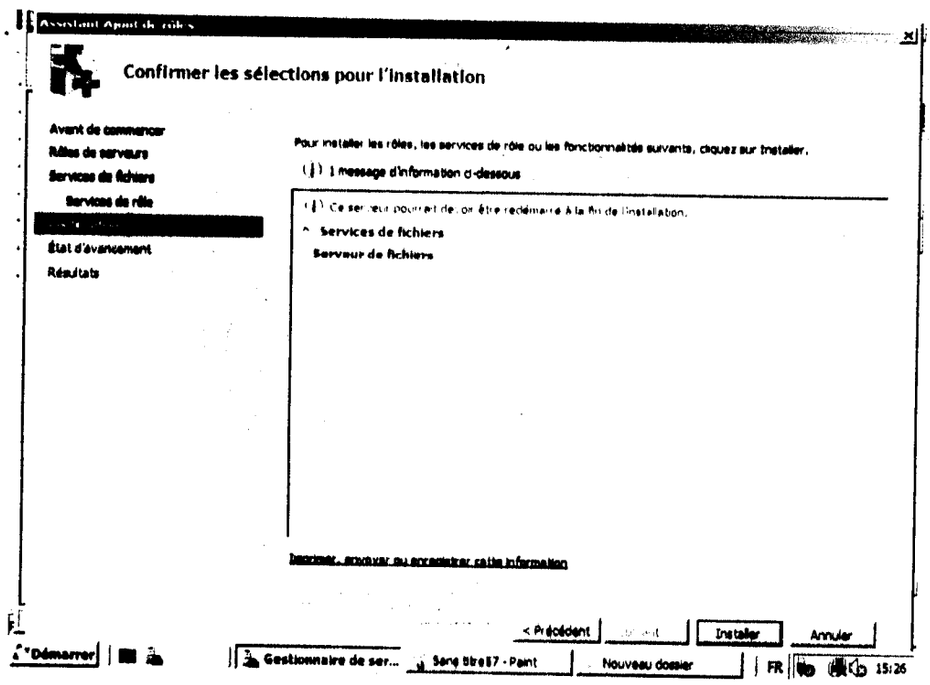
Utiliser pour partager des fichiers entre le serveur et les clients.



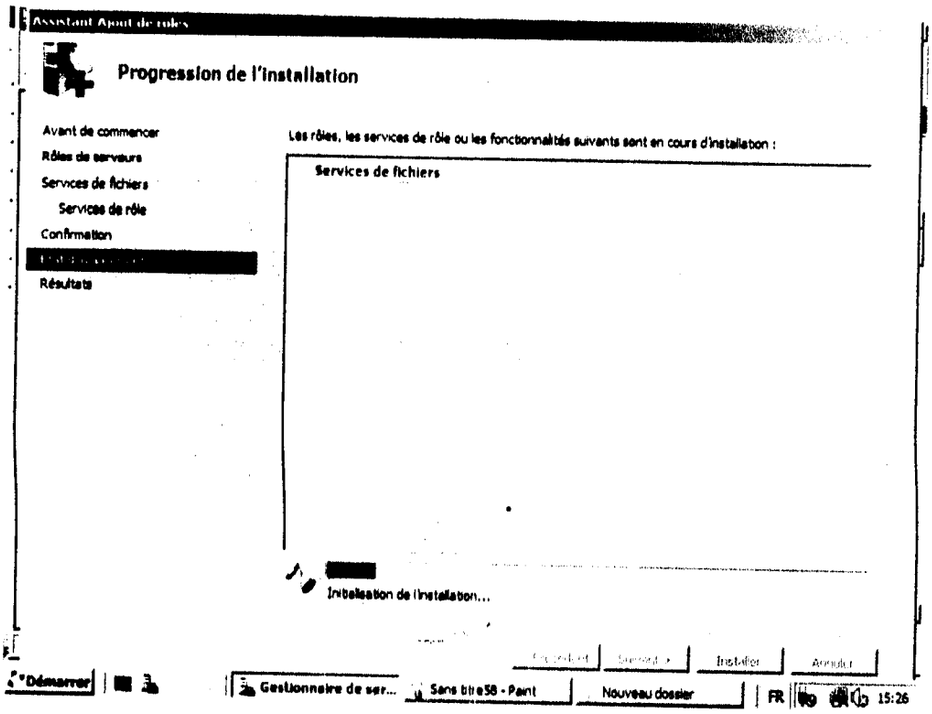
On a coché les services de rôle requis à installer pour le serveur de fichiers et on a cliqué sur **Suivant.**



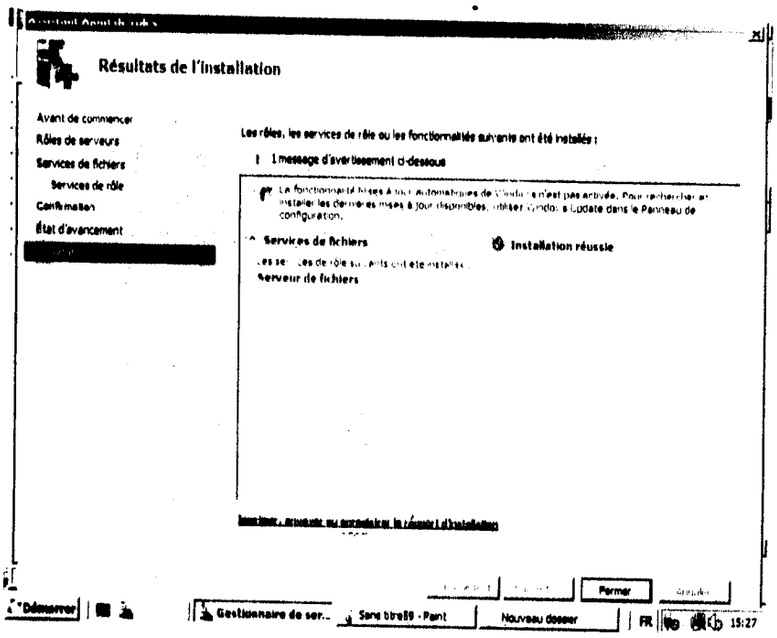
On a cliqué sur **Installer.**



L'installation en cours…



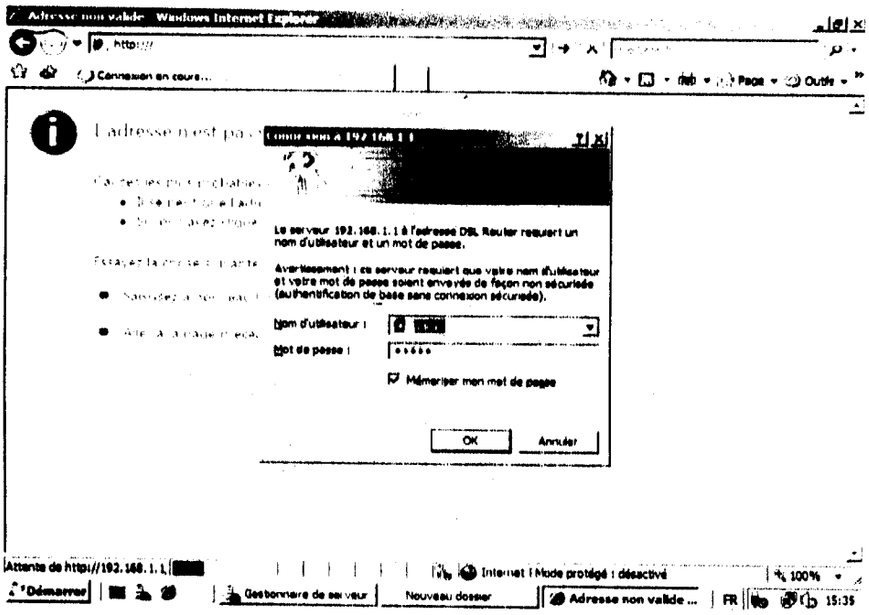
Une fois l'installation terminée on clique sur **Fermer.**



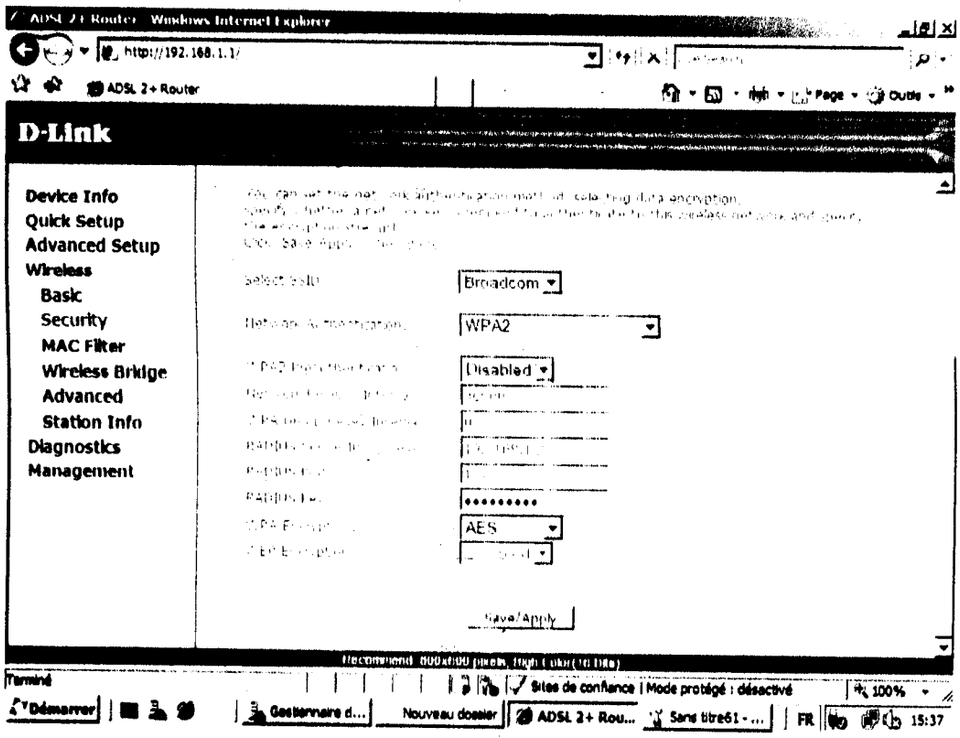
III.7 Configuration du point d'accès Wi-Fi

On a ouvert notre navigateur web et on a saisi l'adresse IP de notre point d'accès, **http://192.168.1.1**

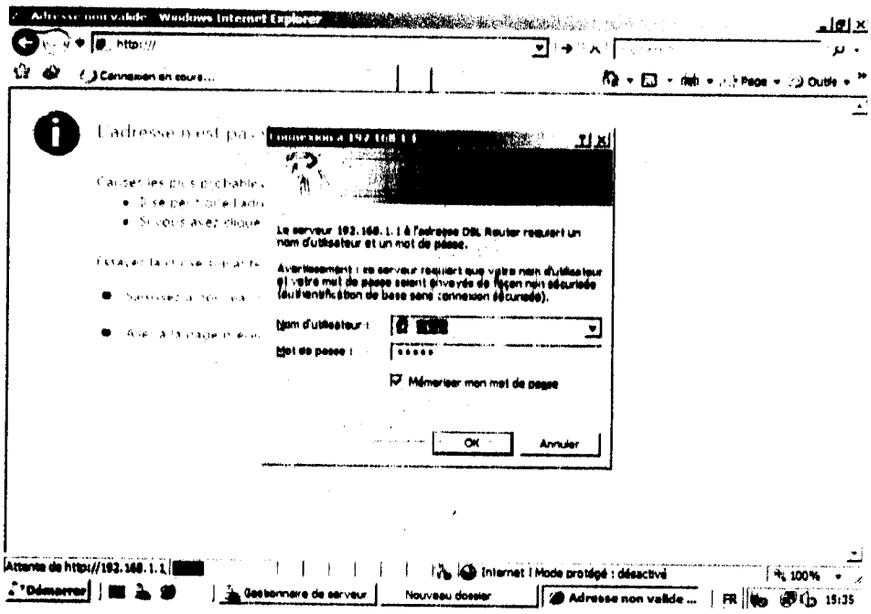
Une fenêtre de connexion s'est affichée alors on a entré notre login et notre mot de passe puis **OK.**



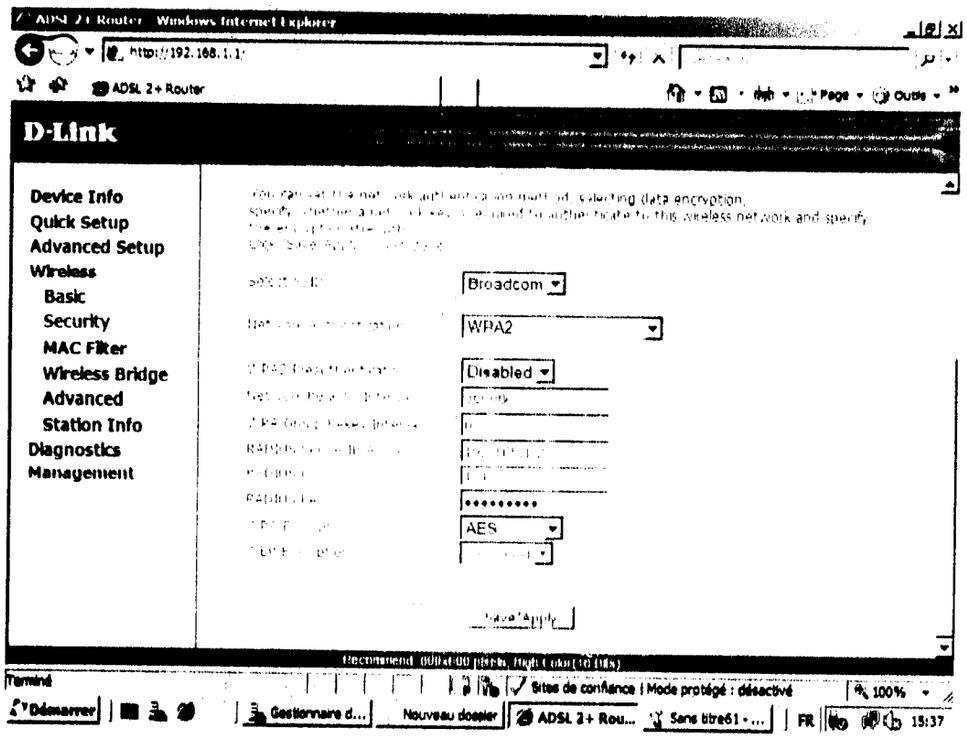
On a choisit le **Select SSID** et l'option de sécurité **WPA2** et le type de chiffrement **AES.** On a saisi **l'adresse IP de notre Serveur RADIUS** et le port de communication (par défaut 1812), puis on a introduit la **clé partagée** qu'on a saisie le serveur RADIUS.



Une fenêtre de connexion s'est affichée alors on a entré notre login et notre mot de passe puis **OK.**



On a choisit le **Select SSID** et l'option de sécurité **WPA2** et le type de chiffrement **AES.** On a saisi **l'adresse IP de notre Serveur RADIUS** et le port de communication (par défaut 1812), puis on a introduit la **clé partagée** qu'on a saisie le serveur RADIUS.



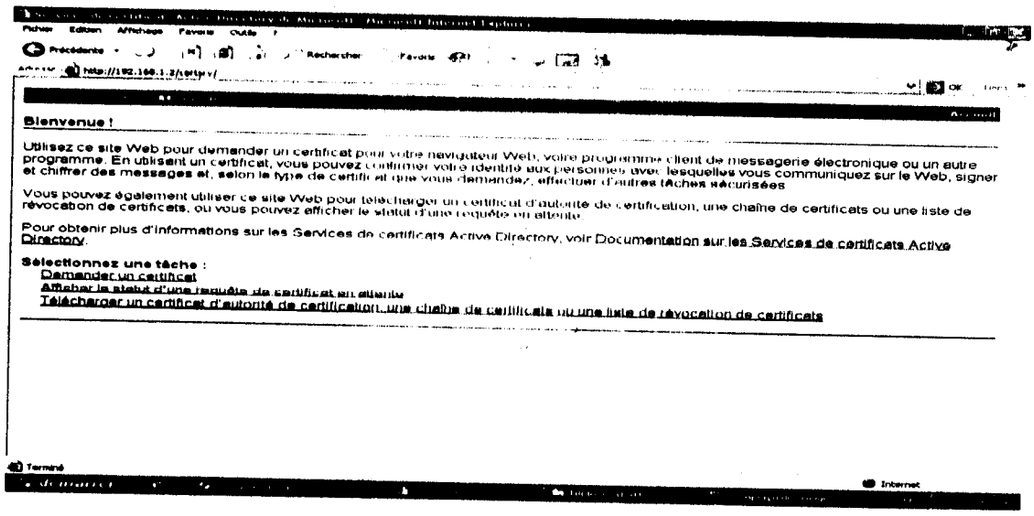
Nous avons validé en cliquant sur **Save/Apply** puis **Reboot** pour l'activation de la configuration.

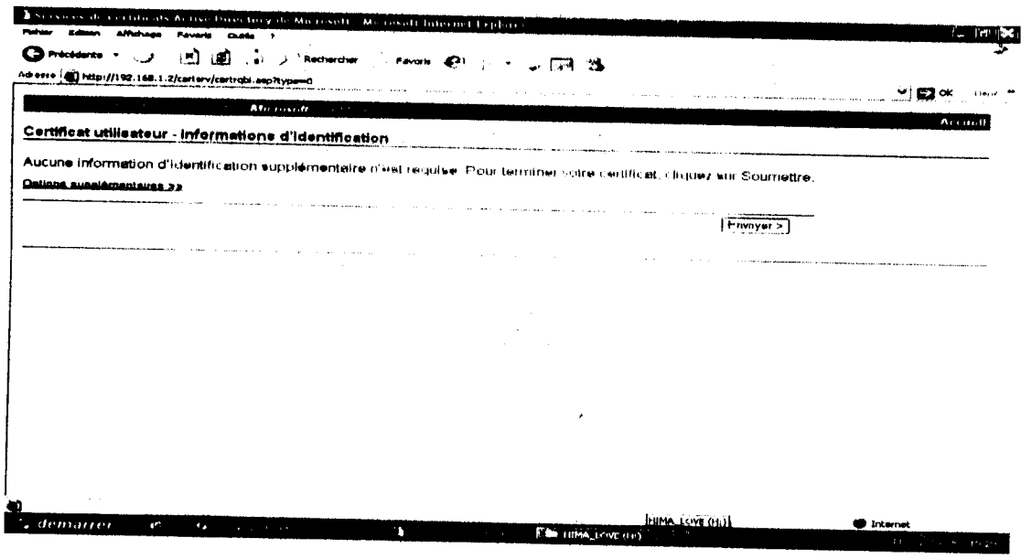
La configuration de la borne d'accès est maintenant terminée.

Nous allons pouvoir passer à la configuration des clients d'accès Wi-Fi.

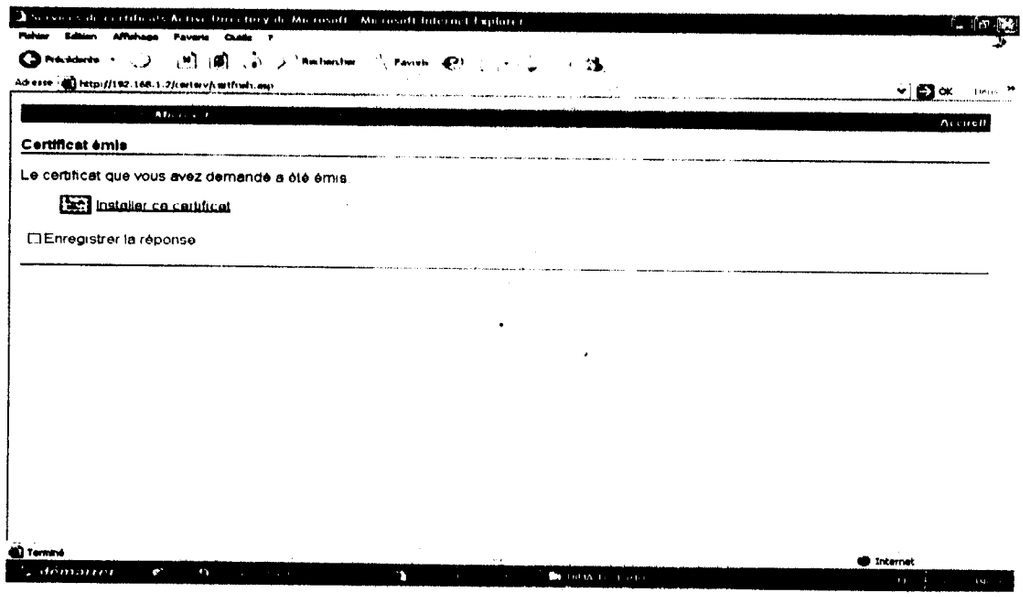
Téléchargement des certificats

Pour le téléchargement des certificats écrivons dans la barre des adresses 192.168.1.2/certsrv ou PC-AMINE/certsrv après un click sur **demander un sertificat**

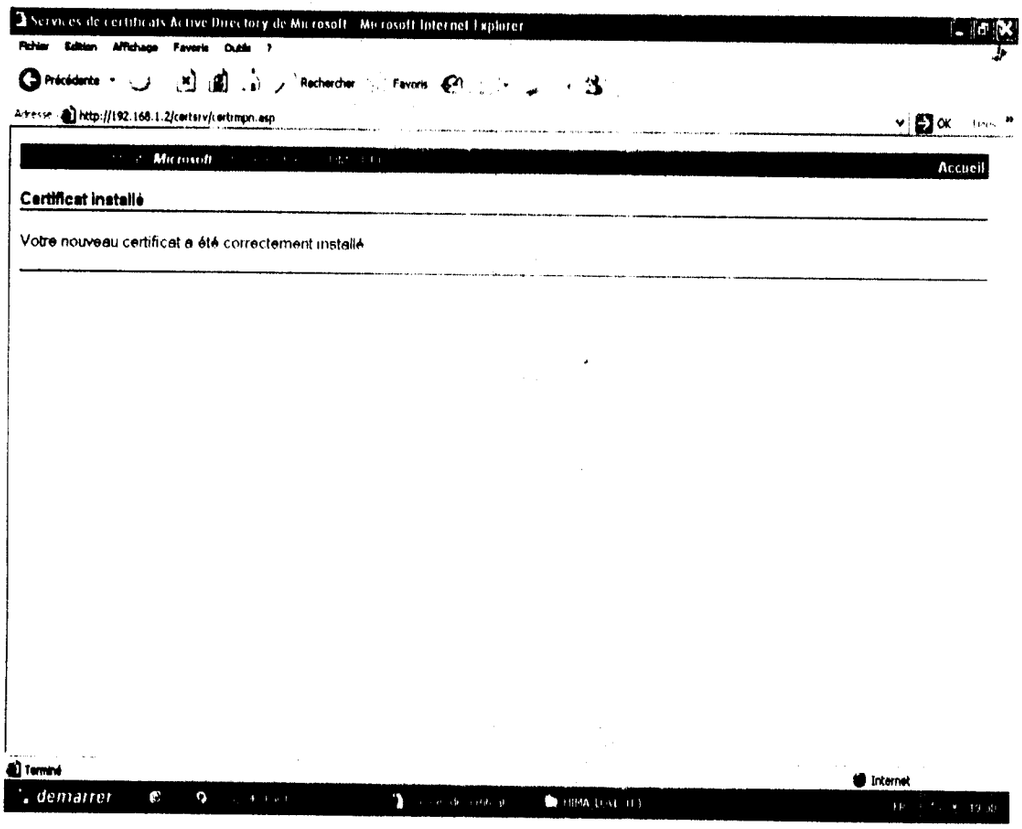




Après un click sur envoyer pour télécharger cette certificat.

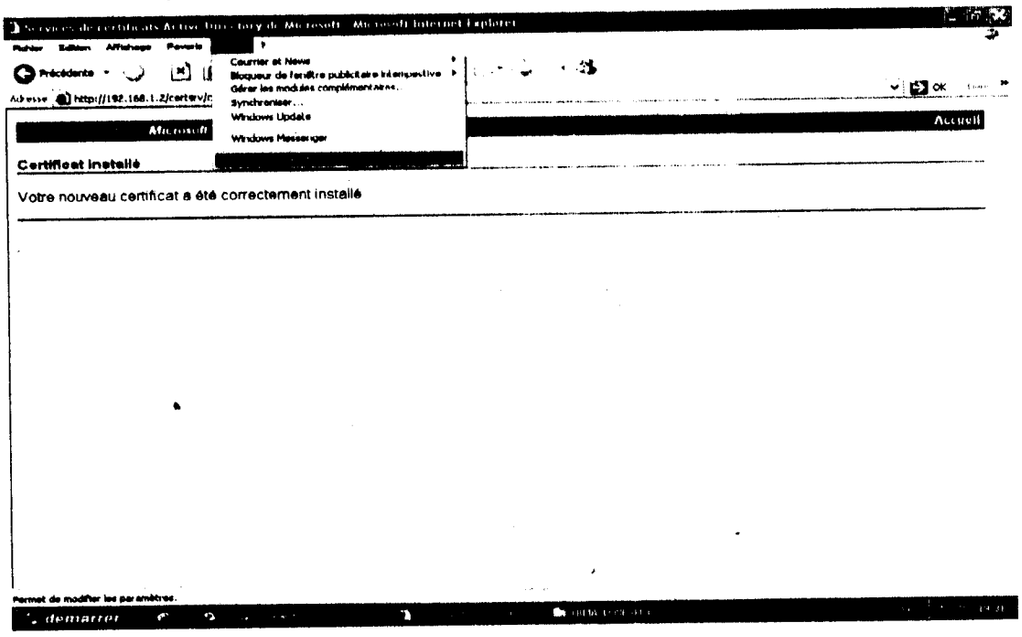


Ensuit on click sur installer ce certificat

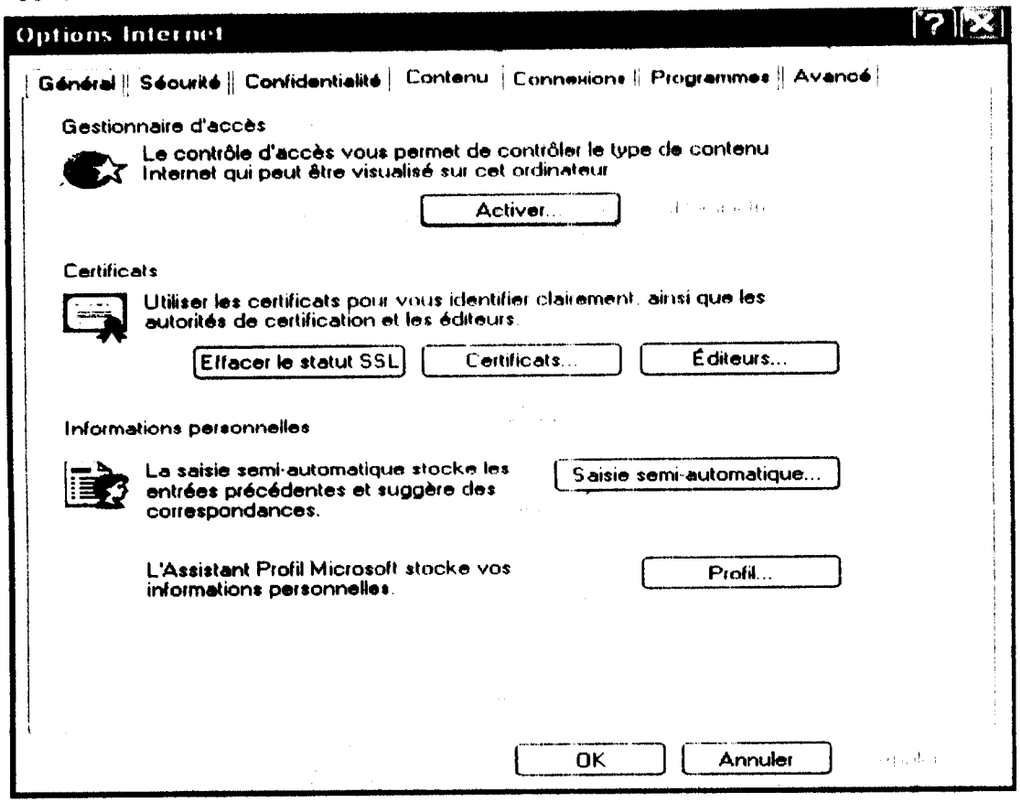


Maintenant notre certificat est installé.

Pour vérifier que notre certificat bien installer allons sur **outil** puis **options internet**

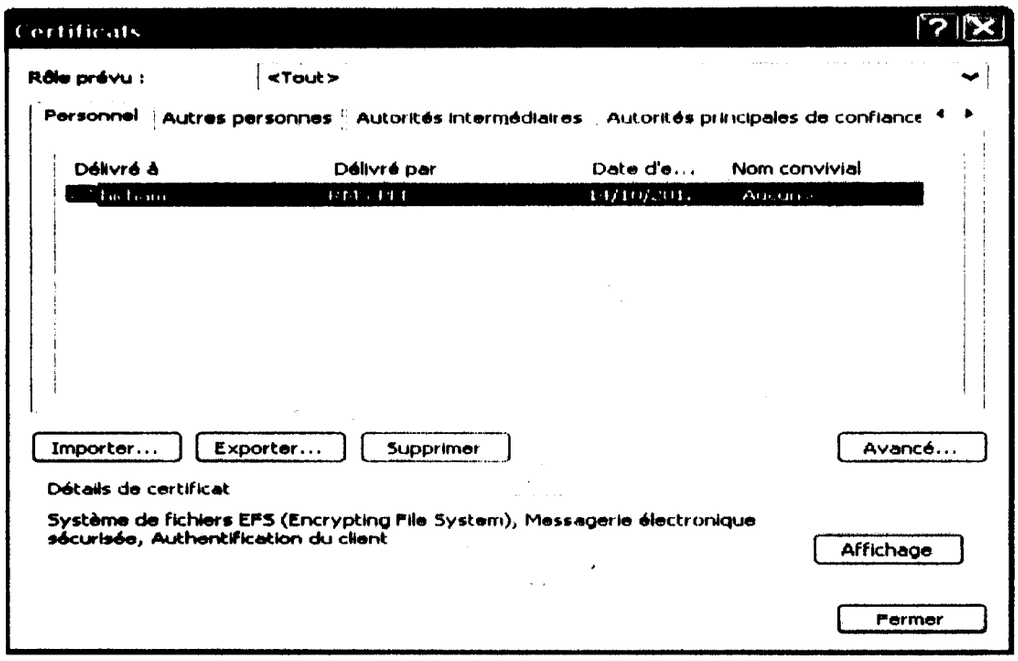


Appuyant sur **Contenu** puis **Certificats**

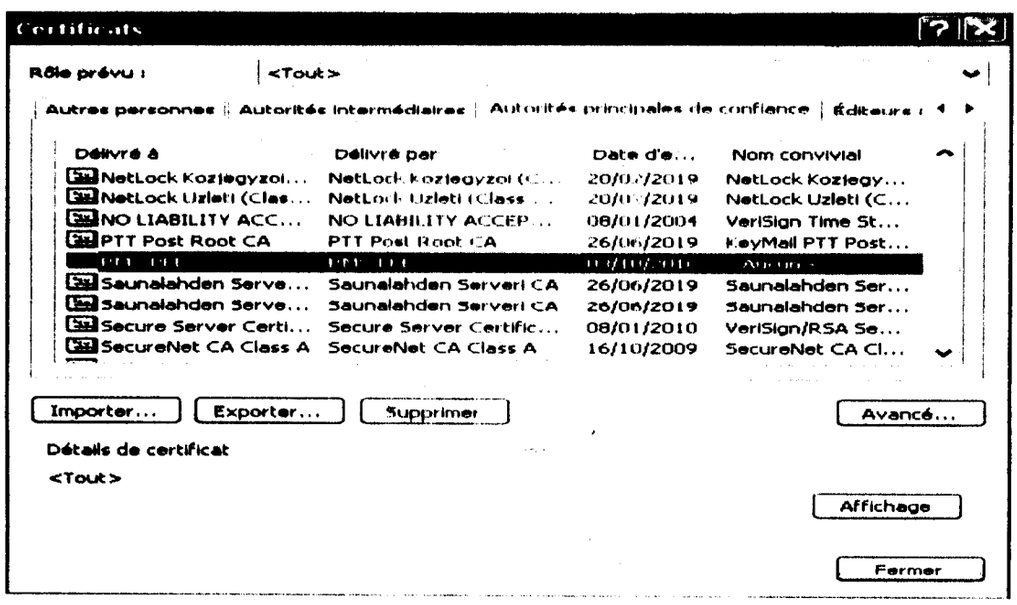


Cliquons sur **personnel**

Le voila notre certificat est bien installer pour l'utilisateur **hicham.**

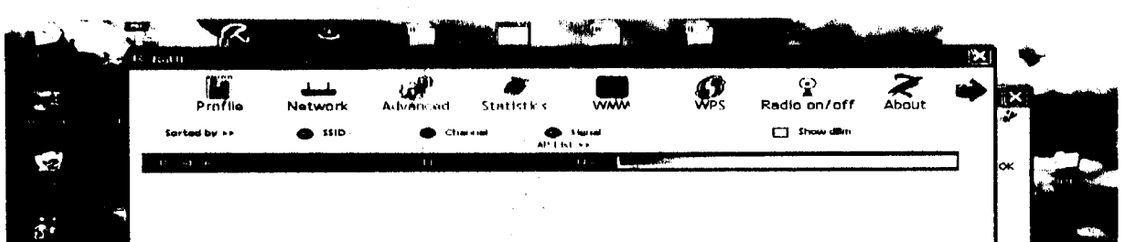


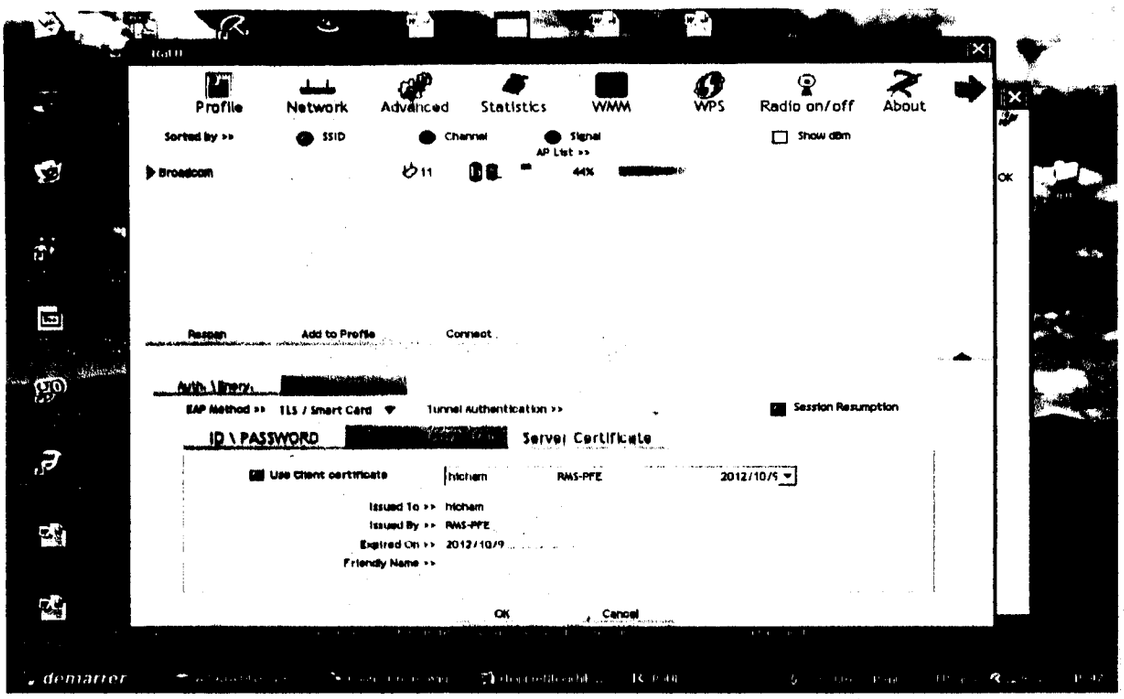
Nous avons vérifié également que le serveur de certificat était présent dans la liste des **Autorités principale de confiance**

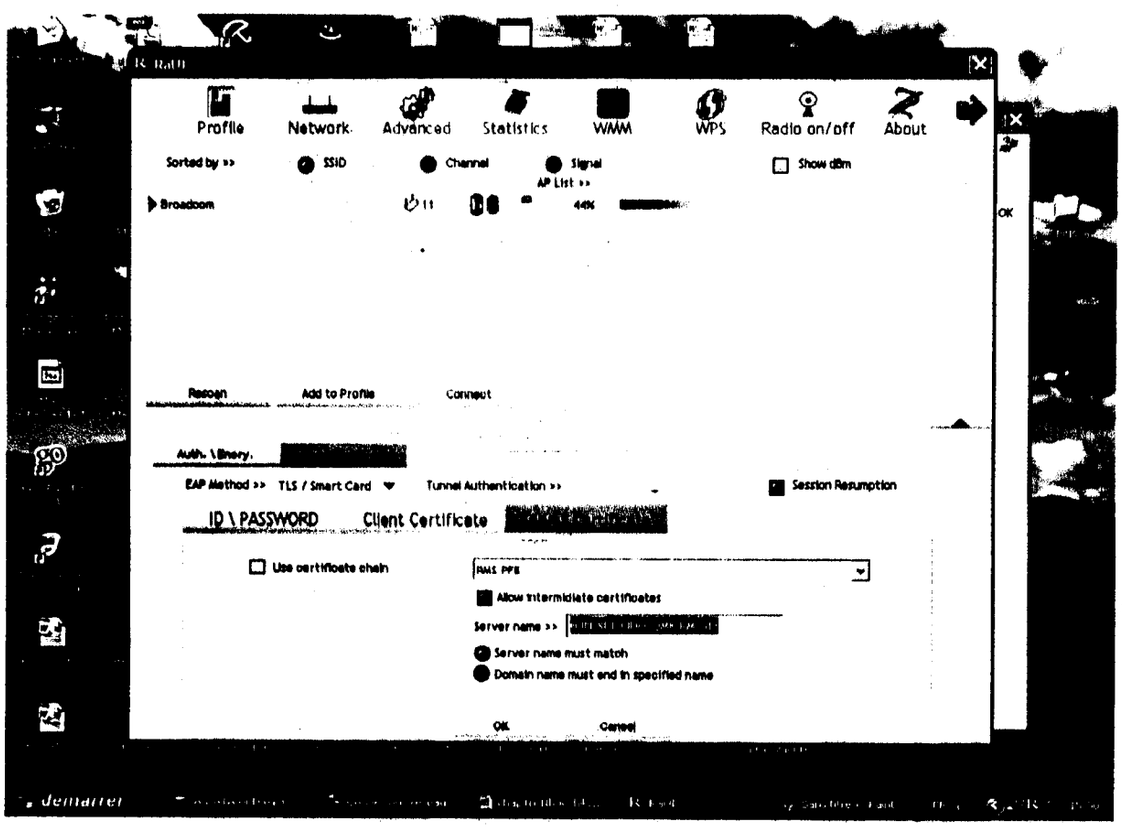


Maintenant l'installation de notre certificat est bien terminée.

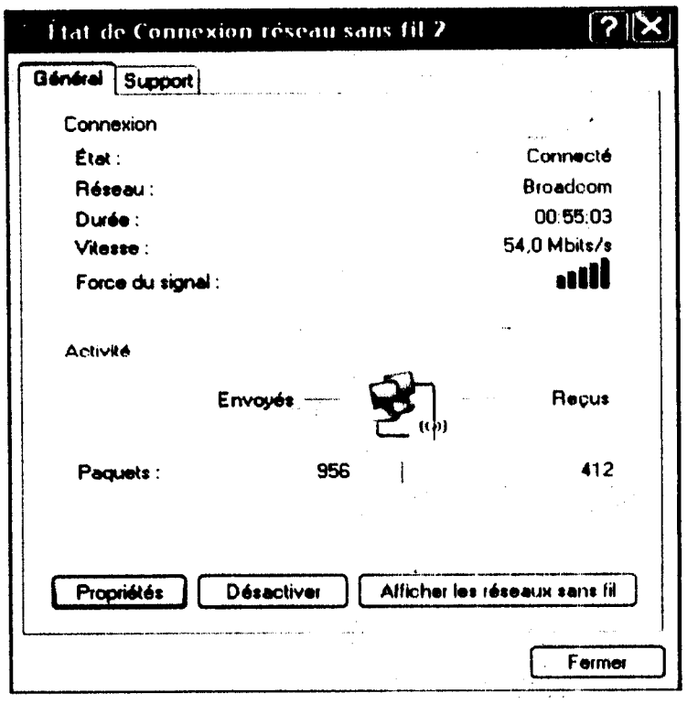
III.8 Test de sécurité et Partage des fichiers



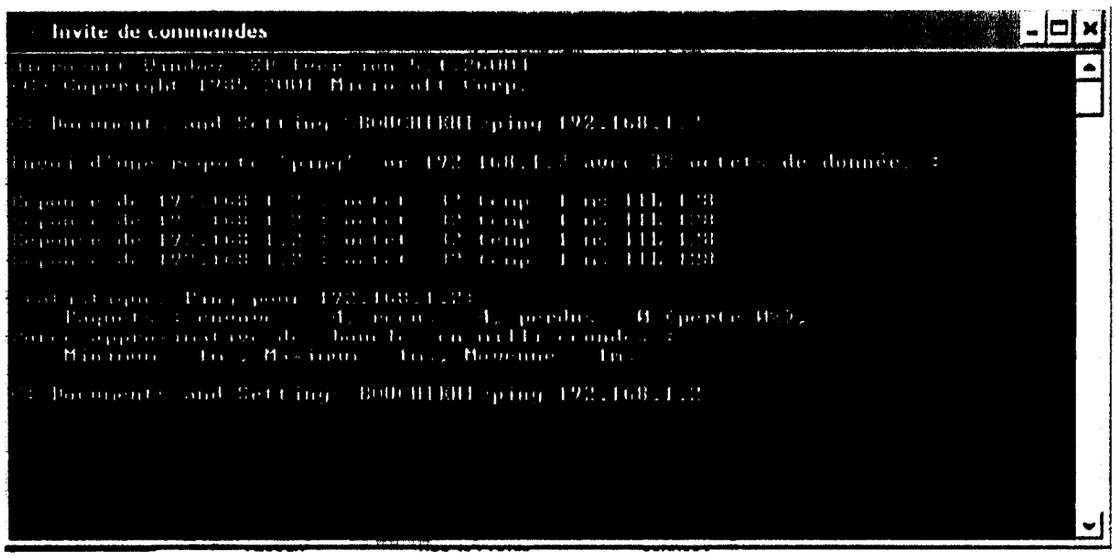

Profile
Network
Advanced
Statistics
WMM
WPS
Radio on/off
About
Sorted by >>
SSID
Channel
Signal
Show dBm
AP List >>
Broadcom
11
44%
OK
Rescan
Add to Profile
Connect
Auth. \ Encry.
EAP Method >>
TLS / Smart Card
Tunnel Authentication >>
Session Resumption
ID \ PASSWORD
Server| Certificate
Use Client certificate
hicham
RMS-PFE
2012/10/9
Issued To >> hicham
Issued By >> RMS-PFE
Expired On >> 2012/10/9
Friendly Name >>
OK
Cancel
démarrer

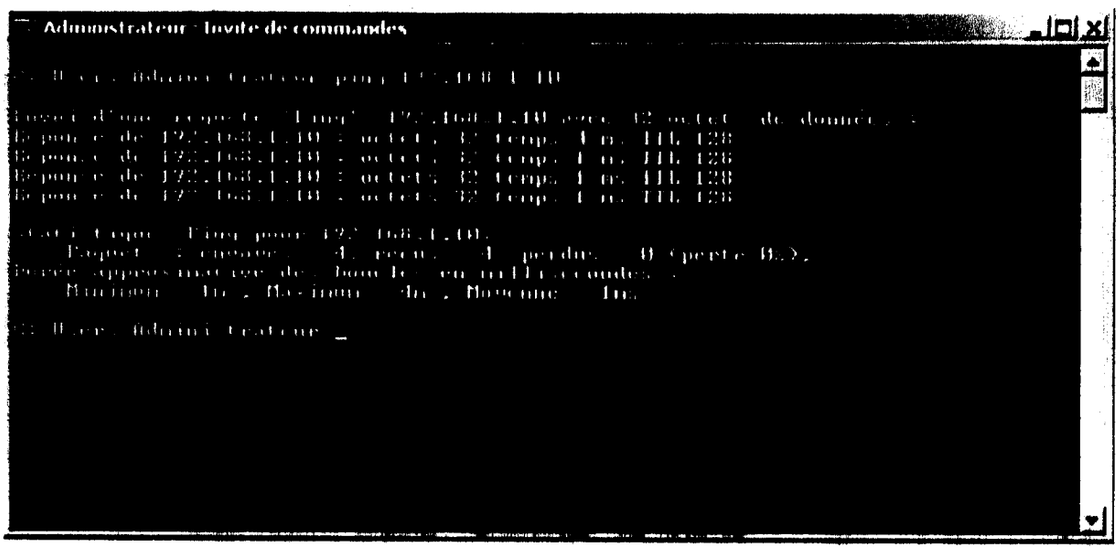

Profile
Network
Advanced
Statistics
WMM
WPS
Radio on/off
About
Sorted by >>
SSID
Channel
Signal
Show dBm
AP List >>
Broadcom
11
44%
OK
Rescan
Add to Profile
Connect
Auth. \ Encry.
EAP Method >>
TLS / Smart Card
Tunnel Authentication >>
Session Resumption
ID \ PASSWORD
Client Certificate
Use certificate chain
RMS PFE
Allow intermidiate certificates
Server name >>
Server name must match
Domain name must end in specified name
OK
Cancel
démarrer

Voila l état de notre réseau sans fil

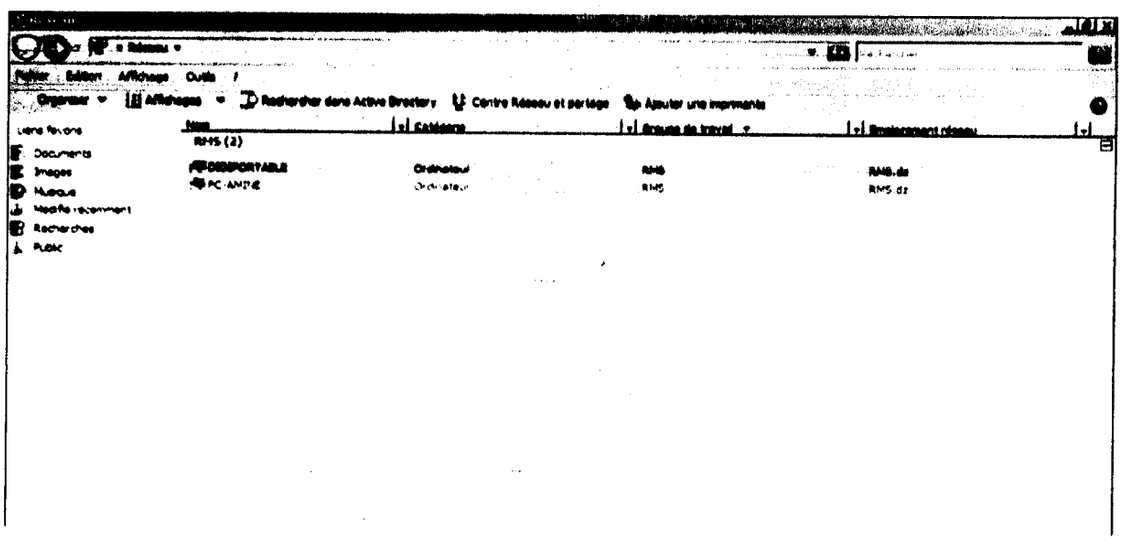


Une fois l'utilisateur hicham connecté, il a accédé aux ressources partagées du serveur comme on peut le voir ci-dessous et bien entendu les **ping** vers le routeur et le serveur ont réussi, indiquant la connexion effective de hicham. On a ensuite essayé de pénétrer le réseau avec un utilisateur non autorisé et ça a échoué comme escompté, ce qui indique qu'on a effectivement et efficacement sécurisé notre réseau test.





Voila le Partage des fichiers



Conclusion

En résumé, on pense avoir réussi à sécuriser notre réseau Wi-Fi, puisqu'on a fait plusieurs essais pour connecter des utilisateurs non autorisés, sans succès. Même des utilisateurs ayant connaissance du SSID, ne peuvent pas y accéder, puisque leur authentification par certificat qu'ils ne possèdent pas, a échoué.

Conclusion générale

Malgré des problèmes de sécurité intrinsèques, les réseaux sans fil continuent et continueront surement à se développer, surtout avec l'arrivée récente du wifi mesh en tant que MAN. Il est donc important de bien connaître les problèmes liés à la mise en place de ce type de réseaux afin d'en limiter les effets néfastes et d'être prêt à toutes les éventualités. Il est également important de déterminer le niveau de sécurité souhaité afin de mettre en place une solution en adéquation avec ce choix.

Malgré le peu de recul sur la norme IEEE 802.11i, celle-ci est vouée à s'imposer comme la norme unificatrice en matière de sécurité. Donc notre choix de sécuriser notre réseau test avec la méthode WPA2 qui allie le serveur RADIUS, le protocole 802.1x et l'EAP-TLS, nous permet d'utiliser et de marier les méthodes les plus sures connues à ce jour dans le domaine de la sécurité.

Le test effectué a été probant et même si le SSID est diffusé en clair, un utilisateur ne possédant pas les certificats adéquats et n'étant pas enregistré sur le serveur ne pourra en aucun cas se connecter et accéder aux ressources du réseau sans fil ou filaire.

LISTE DES FIGURES

REFERENCES BIBLIOGRAPHIQUES

[1] http://fdigallo.online.fr/cours/reseaux.pdf

[2] http://www. urec. enrs. fr/IMG/pdf/cours. postes-clients, pdf

[3] http://www.securiteinfo.com/cryptographie/symetrique-iphone.shtml

[4] http://fr.wikipedia.org/wiki

[18] http://wiki.caensansfil.org/index.php

[6] http://www.commentcamarche.net

[7] http://tuncert.ansi.tn/publish/docs/guides/guideauthentification802.lx.pdf

[8] http://wapiti.telecomlille 1. eu/commun/ens/peda/bptions/ST/RIO/pub/exposes

LISTE DES ABREVIATIONS

"A"

AAA: Authentication Authorization Accounting

ACK: Acknowledgement

AD CS: Active Directory Certificate Services

ADSL: Asymetric Digital Subscriber Line

AES: Advanced Encryption Standard

AKA: Authentification and Key Agreement

AP: Access Point

ART: Autorité de Régulation des Télécommunications

ATM: Asynchrous Transfer Mode

"B"

BLR: Boucle Locale Radio

BPSK: Binary Phase-Shift Keying

BSS: Basic Service Set

BTS: Base Transceiver Station

"C"

CA: Certification Authority

CBC: Cipher Block Chaining

CCA: Clear Channel Assessment

CD: Compact Disc

CDC: Control Data Corporation

CEPT: Conférence Européenne des administrations des Postes et Télécommunications

CFB: Cipher Feed Back

CHAP: Challenge-Handshake Authentication Protocol

CRC: Cyclic Redundancy Check

CSMA/CA: Carrier Sense Multiple Access with Collision Avoidance

CSMA/CD: Carrier Sense Multiple Access with Collision Detection

CTS: Clear To Send

"D"

DGF: Distributed Coordination Function

DCS: Digital Communication System

DEA: Data Encryption Algorithm

LISTE DES ABREVIATIONS

DECT: Digital Enhanced Cordless Telephone

DES: Data Encryption Standard

DHCP: Dynamic Host Configuration Protocol

DIFS: Distributed Inter Frame Space

DN: Distinguished Name

DNS: Domain Name System

DS: Distribution Service

DSA: Digital Signature Algorithm

DSL: Digital Signature Algorithm

DSSS: Direct Sequence Spread Spectrum

"E"

EAP: Exetensible Authentication Protocol

EAPOL: EAP Over LAN

ECB: Electronic Code Book

ESS: Extended Service Set

ETSI: European Telecommunications Standard Institute

"F"

FAST: Flexible Authentication via Secure Tunneling

FCC: Federal Communications Commission

FDD: Frequency Division Duplexing

FDDI: Fiber Distributed Data Interface

FHSS: Frequency Hopping Spread Spectrum

FIPS: Federal Information Processing Standards

"G"

GPRS: General Packet Radio Service

GPS: Global Positioning System

GSM: Global System for Mobile Communication

GUI: Graphical User Interface

"H"

HiperLAN2: High Performance Radio LAN 2.0

LISTE DES ABREVIATIONS

"I"

IAS: Internet Authentication Service

IBM: International Business Machines

IBSS: Independent Basic Service Set

ICV: Integrity Check Value

IEEE: Institute of Electrical and Electronic Engineers

IIS: Internet Information Server

IP: Internet Protocol

IR: Infra Rouge

IrDA: Infrared Data Association

ISM: Industrial Scientific and Medical

ISO: International Standard Organization

"L"

LAN: Local Area Network

LEAP: Lightweight EAP

LLC: Logical Link Control

LOS: Line Of Sight

LTE: Long Term Evolution

"M"

MAC: Medium Access Control

MAN: Metropolitan Area Network

MD5: Message Digest 5

MIC: Message Integrity Code

MIMO: Multiple Input Multiple Output

MIT: Massachusetts Institute of Technology

MKK: Mensa-kentei Kyokai

MMS: Multimedia Messaging Service

MS: Mobile Station

"N"

NAP: Network Access Protection

NAS: Network Access Server

NIC: network Interface Controller

LISTE DES ABREVIATIONS

NIST: National Institute of Standards and Technology

NLOS: Non Line Of Sight

NPS: Network Policy Server

"O"

OFB: Output Feed Back

OFDM: Orthogonal Frequency Division Multiplex

OLSR: Optimized Link State Routing

OMS: Organisation mondiale de la santé

OSI: Open Systems Interconnection

"P"

PAP: Password Authentication Protocol

PC: Personal Computer

PCF: Point Coordination Function

PCI: Peripheral Component Interconnect

PCMCIA: Personal Computer Memory Card International Association

PCS: Personal Communications Service

PDA: Personal Data Assistant

PEAP: Protected EAP

PKI: Public Key Infrastructure

PLCP: Physical Layer Convergence Protocol

PLW: PSDU Length Word

PMD: Physical Medium Dependent

PMK: Pairwise Master Key

PMKID: Pairwise Master Key Identifier

PPM: Pulse Position Modulation

PSK: Pre-Shared Key

"Q"

QAM: Quadrature Amplitude Modulation

QoS: Quality of Service

QPSK: Quadrature Phase Shift Keying

"R"

RADIUS: Remote Authetification Dial-In-User Service

RC4: Rivest Cipher 4

RCA: Radio Corporation of America

RFC: Request for Comments

RLE: Réseau Local d'Entreprise

RODC: Read Only Domain Controller

RPV: Réseau Privé Virtuel

RSA: Rivest Shamir Adleman

RTS: Request To Send

"S"

SAM: Security Accounts Manager

SFD: Start Frame Delimiter

SIM: Subscriber Identity Module

SKE: Shared Key Exchange

SMS: Short Message Mobile

SNMP: Simple Network Management Protocol

SQL: Structured Query Language

SSID: Service Set Identity

SSL: Secure Socket Lover

"T"

TACACS: Terminal Access Control Access Control System

TCP: Transmission Control Protocol

TDD: Time-Division Duplex

TKTP: Temporal Key Integrity Protocol

TLS: Transport Layer Security

TTLS: Tunneled Transport Layer Security

"U"

UIT: Union International des Telecommunications

UMTS: Universel Mobile Télécommunications System

U-NII: Unlicensed-National Information Infrastructure

USB: Universal Serial Bus

LISTE DES ABREVIATIONS

USIM: Universal Subscriber Identity Module

"V"

VLAN: Virtual Local Area Network

VPN: Virtual Private Network

"W"

WAP: Wireless Application Protocol

WDS: Wireless Distribution System

WECA: Wireless Ethernet Compatibility Alliance

WEP: Wired Equivalent Privacy

WI-FI: Wireless-Fidelity

WIMAX: Worldwide Interoperability for Microwave Access

WLAN: Wireless Local Area Network

WMAN: Wireless Metropolitan Area Network

WPA: Wi-Fi Protected Access

WPAN: Wireless Personal Area Network

WWAN: Wireless Wide Area Network

Abstract

Note that in recent years a remarkable growth rate of uses of wireless networks, parallel growth of piracy equipped easy to find a simple search in the net, wireless networks vulnerable to numerous attacks on all with the existing competition between companies today, so security is an essential point for deploying a network, such a study will be very interesting.

<<Using RADIUS in Windows Server 2008 to secure a wireless network 802.11>> the end of our proposed study aims to define the different types of attacks with possible solutions to offer a satisfactory safety , was chosen the establishment of a secure WIFI in the RADIUS authentication server for Microsoft Windows server 2008. This study allows the administrator to choose a security strategy that best fits are possible for the network. It cited all the steps to deploy when the method to chose.

تلخيص

نعلم أنه في السنوات الأخيرة معدل النمو الملحوظ لاستخدام الشبكات اللاسلكية، في موازاة نمو القرصنة و من السهل العثور على بحث بسيط على الإنترنت، و شبكات اللاسلكية عرضة للهجوم لارتفاع المنافسة القائمة بين الشركات حاليا، وتامينها هو النقطة الأساسية لنشر الشبكة بحيث مثل هذه الدراسة سوف تكون مثيرة جدا للاهتمام. { استعمال الـ"RADIUS" في"Windows Server 2008" لتأمين شبكة اتصال لاسلكية 802.11} انه مشروع نهاية دراستنا المقترح الذي يهدف إلى تحديد أنواع مختلفة من الهجمات مع الحلول الممكنة لتقديم سلامة مرضية، وقد قمنا باختيار"WIFI" لتامينه في خادم المصادقة "RADIUS" تحت نظام التشغيل "Windows Server 2008". هذه الدراسة تسمح للمسؤول اختيار إستراتيجية الأمن التي تتناسب مع الشبكة. ولقد ذكرنا كل الخطوات التي تظهر الطريقة التي قمنا باختيارها.