2014-2016

Projet Personnel Encadré

BTS Services Informatiques aux Organisations

Baptiste Lionel

Table des matières

Table des figures

BTS SIO Service Informatiques aux Organisations Session 2014-2016	
BAPTISTE Lionel Option : SISR	Année 2014-2015 Activité professionnelle N°7
NATURE DE L'ACTIVITE : 7. Mise en place de Wifi d'entreprise via AD, DNS, DHCP, NPS	
COMPETENCES MISES EN ŒUVRE POUR CETTE ACTIVITE PROFESSIONNELLE	
Situation obligatoire	«Installation d'un autre système d'exploitation sur mon ordinateur quotidien.»
Matériel	Logiciel VirtualBox, Image .iso Windows 7
Durée de réalisation	Environ 1 heure

1. Contexte

Dans ce projet, je décide de mettre en place une connexion Wifi d'entreprise sécurisée. Deux solutions s'offrent à moi pour mener à bien ce projet :

2. Solution envisageable

Un réseau de hot spot :

Un réseau hot spot est totalement distinct de celui de l'entreprise. Il est généralement constitué d'un réseau de bornes Wi-Fi connectées à une application spécialisée (Bluesocket, Nomadix, etc.) ou à un serveur dédié équipé d'un logiciel de gestion des hot spots (Ucopia, Netinary, etc.).

Cet équipement se charge d'authentifier les utilisateurs sans aucun lien avec le référentiel de l'entreprise. Il ne présume par ailleurs d'aucun type d'adressage et s'adapte à ce que lui envoie le client dès la connexion à la borne, au niveau 2 de la couche réseau. À ce stade, le client est sur un portail web captif et l'utilisateur ne peut que saisir un identifiant. Il s'agit généralement du couple "login/mot de passe "défini sur l'équipement lui-même ou éventuellement stocké dans l'annuaire LDAP de l'entreprise, dans un profil visiteur par exemple.

Une fois authentifié, l'accès est ouvert vers internet et la connexion entre le client et la borne est généralement chiffrée grâce au standard de sécurité WPA (dont la clé est fournie via le protocole 802.1x), ou grâce à du WEP dynamique pour les clients qui ne supporteraient pas le WPA. Selon les équipements, il est également possible de définir des niveaux de qualité de service, par exemple, pour ces connexions.

Un serveur NPS / Radius :

Cela doit offrir un accès complet au système d'information de l'entreprise : un choix plus risqué. En contrepartie les utilisateurs sont connus et la configuration des clients mieux maîtrisée, permettant une plus grande souplesse dans l'authentification et la sécurité.

L'architecture est toutefois plus complexe : les bornes doivent relayer l'authentification des clients au mécanisme existant de l'entreprise, généralement un annuaire LDAP ou Active Directory. Hélas, en matière d'authentification, les bornes Wi-Fi ne comprennent nativement que le protocole 802.1x, qui lui-même ne parle qu'aux serveurs Radius.

3. Solution retenue

L'élément essentiel est de déterminer à qui va servir le Wi-Fi, étant donné que ce sont les utilisateurs de mon précédent projet qui portait sur l'installation d'un serveur de domaine avec Active Directory, DHCP et DNS sous Windows Serveur 2012, je décide de mettre en place une serveur NPS, Network Policy Server. Il aura pour but de d'authentifier les utilisateurs via le login et password des utilisateurs de l'AD.

4. Prérequis

Pour mettre en place ce projet, je vais avoir besoin de ma machine virtuelle sous Windows Serveur 2012 ainsi que d'une machine sous Windows 7 sur mon domaine et muni d'un adaptateur Wifi.

Mon serveur de domaine étant déjà configuré en fonction du contexte M2L, je n'ai juste à y installer mes nouveaux services et les configurer.

Il sera nécessaire d'avoir un point d'accès Wifi compatible avec un serveur Radius et le protocole 802.1x. Pour ça je vais utiliser l'AP « Linksys by cisco ; WRT54GL ».
Attention pour que la borne soit compatible il faut qu'elle ait un firmware de cette distribution dd-wrt.com que j'aurais au préalable flashé.

Je récupère donc les configurations machines de mon précédent projet qui sont les suivantes :

A) Configuration des machines hôtes

Ordinateur fixe :

- Système d'exploitation : Windows 7 64 bits
- Mémoire vive : 16Go
- Disque dur : 1To
- Processeur : Intel Core i5-4690 CPU @3.50GHz-3.50GHz

Ordinateur fixe :

- Système d'exploitation : Windows 7 64 bits
- Mémoire vive : 8Go
- Disque dur : 1To
- Processeur : Intel Core i7-4510U CPU @2.00GHz – 2.60GHz

B) Configuration des machines virtuelles

Ordinateur fixe :

Machine Virtuelle 1 :

- Nom : WIN2012-M2L
- Système d'exploitation : Windows serveur 2012 R2
- Processeur : Intel Core i5-4690 CPU @3.50GHz-3.50GHz
- Mémoire vive : 3Go
- Disque dur : 25Go
- Nombre d'interface : 1
- Mode accès réseau : Accès par pont

Machine Virtuelle 2 :

- Nom : IPCOP
- Système d'exploitation : IPCop-2.1.8
- Processeur : Intel Core i5-4690 CPU @3.50GHz-3.50GHz
- Mémoire vive : 1Go
- Disque dur : 8Go
- Nombre d'interface : 2
- Mode accès réseau :
  - Interface 1 : Réseau privé hôte
  - Interface 2 : Accès par pont

Ordinateur portable :

Machine Virtuelle Cliente :

- Nom : Windows7
- Système d'exploitation : Windows 7 Professionnel SP1
- Processeur : Intel Core i7-4510U CPU @2.00GHz – 2.60GHz
- Mémoire vive : 4Go
- Disque dur : 35Go
- Nombre d'interface :
- Mode d'accès réseau : Accès par pont

5. Les étapes à suivre

Je commence par redémarrer mon serveur Windows Serveur 2012 R2 sur mon ordinateur fixe par le biais de VM VirtualBox.

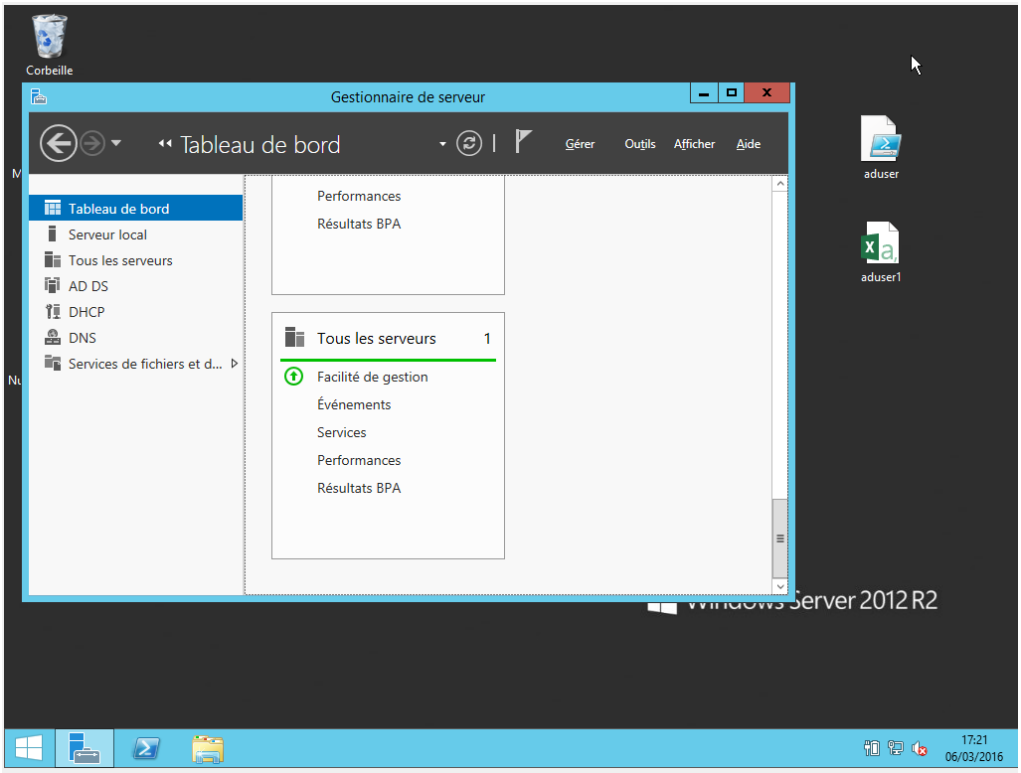

Figure 1 : Serveur 2012 M2L

Afin de mettre en œuvre le serveur d'authentification il est nécessaire d'avoir les services suivants :

- Autorité de certification (certificat serveur)

- Serveur Radius (NPS)

a) Installation et configuration du rôle Services de certificats Active Directory

Donc pour ça je fais « **Gérer »**, je clique sur « **ajouter des rôles et fonctionnalités** », je choisis l'« **Installation basée sur un rôle ou une fonctionnalité** » et je fais suivant.
J'ajoute ensuite le rôle « **Services de certificats Active directory** ».

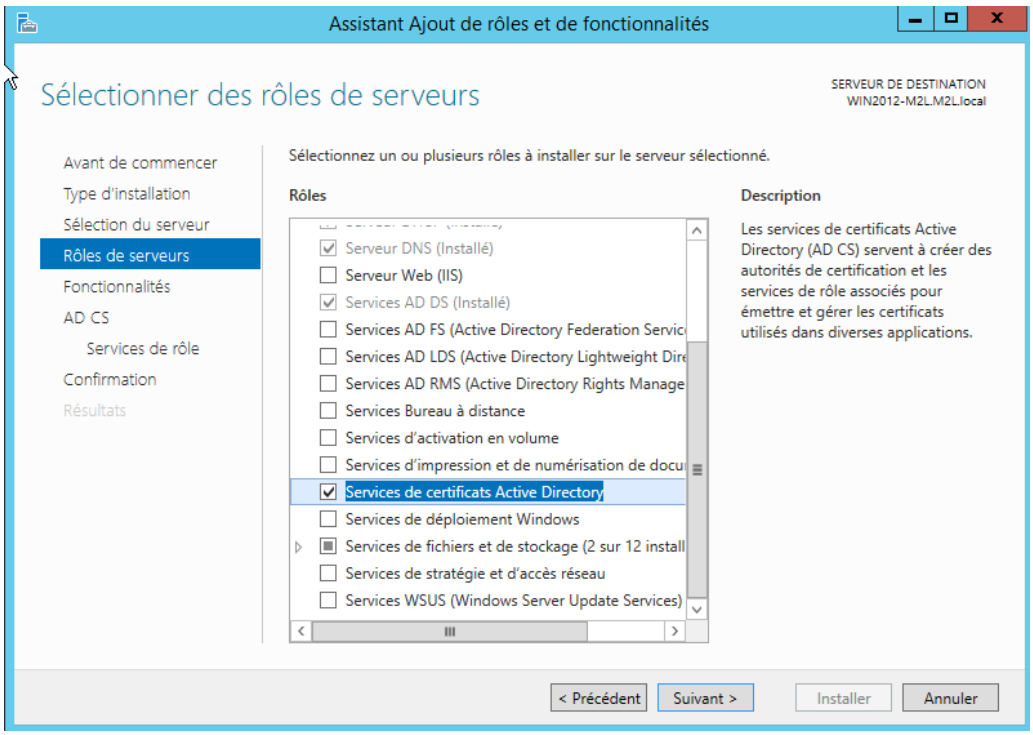

Figure 2 : Ajout du rôle Services de certificats Active Directory

Je laisse les valeurs par défaut et je fais Installer.

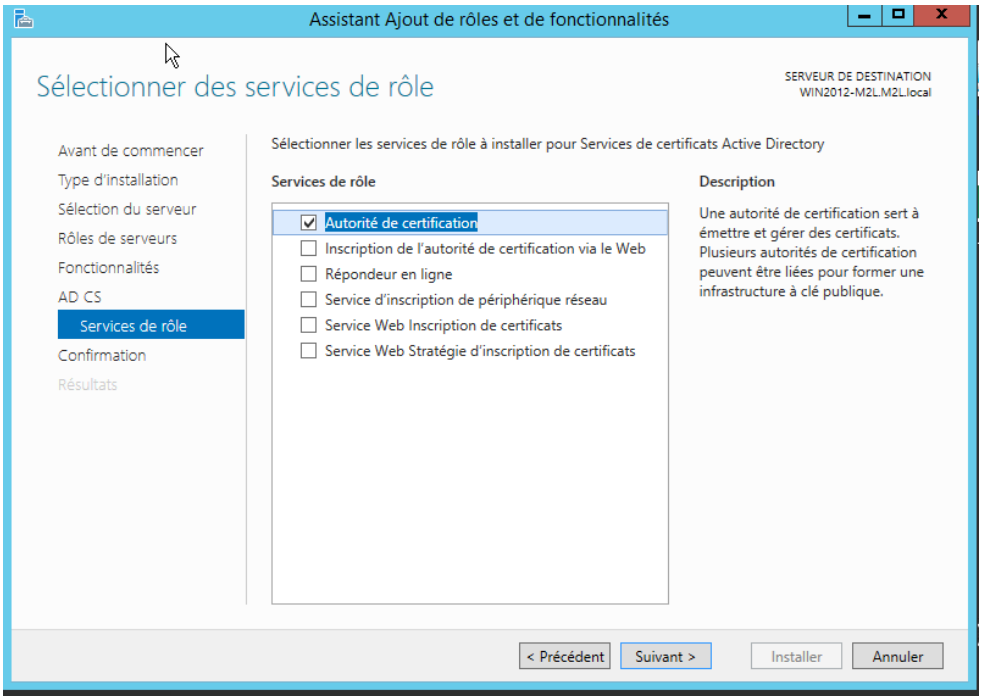

Figure 3 : Autorité de certification

Je choisis maintenant de configurer les services de certificats.

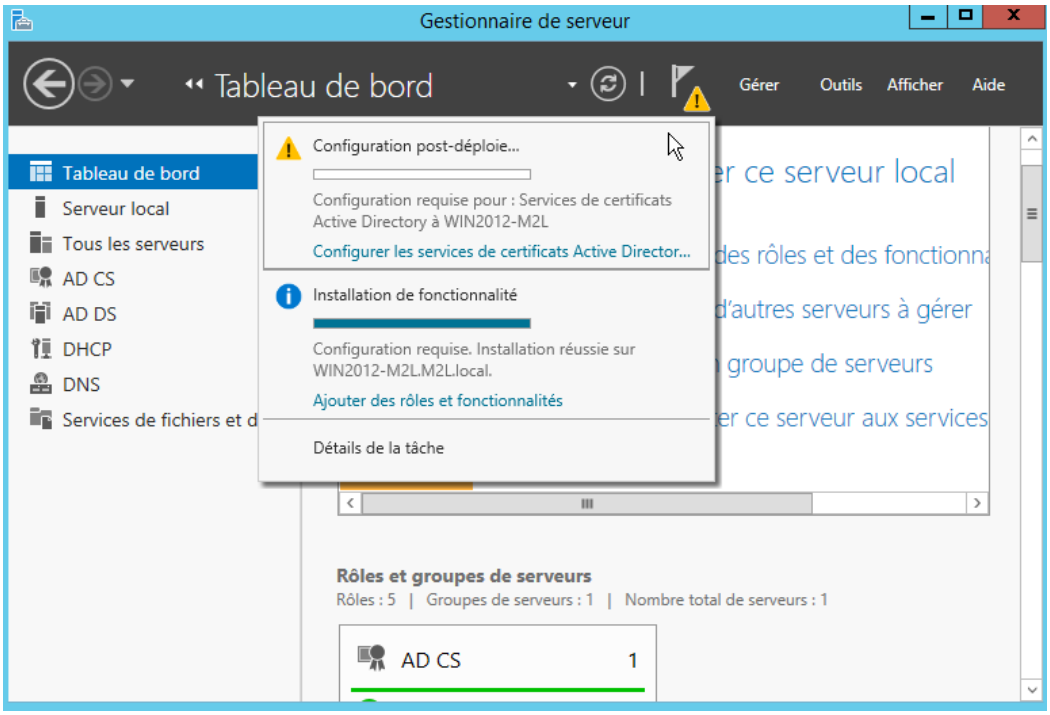

Figure 4 : Configuration des services de certificats

Ici je choisis « **Autorité de certification d'entreprise** ».

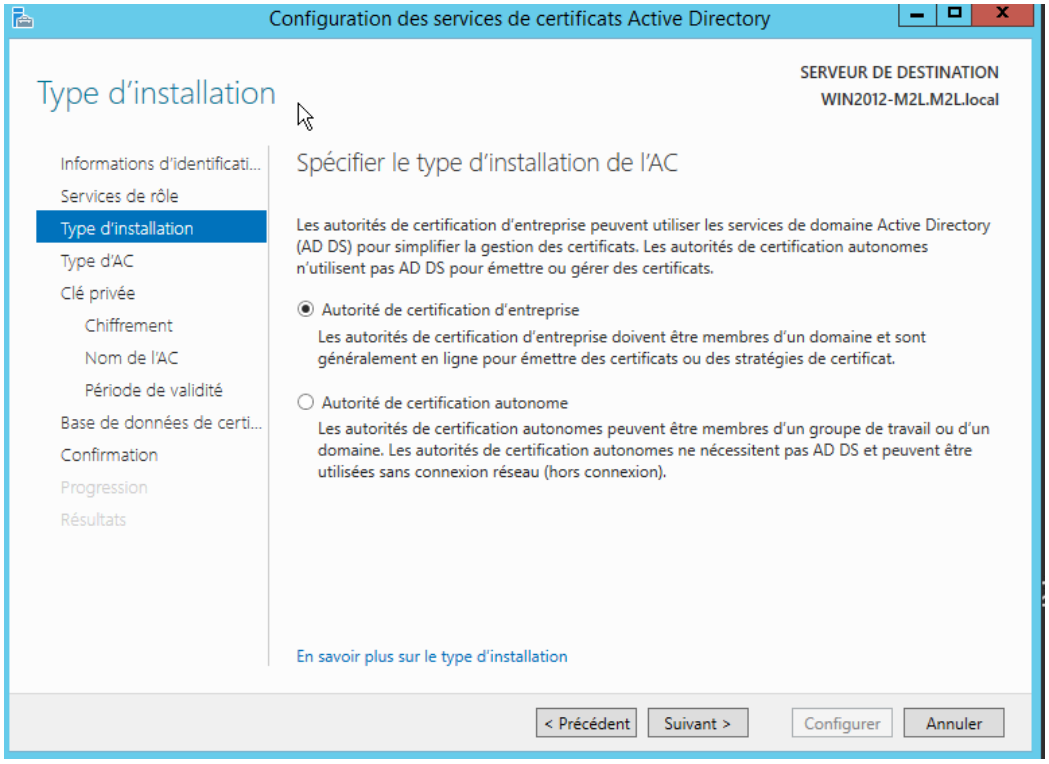

Figure 5 : Autorité de certification d'entreprise

Je laisse les valeurs par défaut et je fais suivant, ensuite je choisis l'algorithme « SHA1 ». Puis je fais suivant.

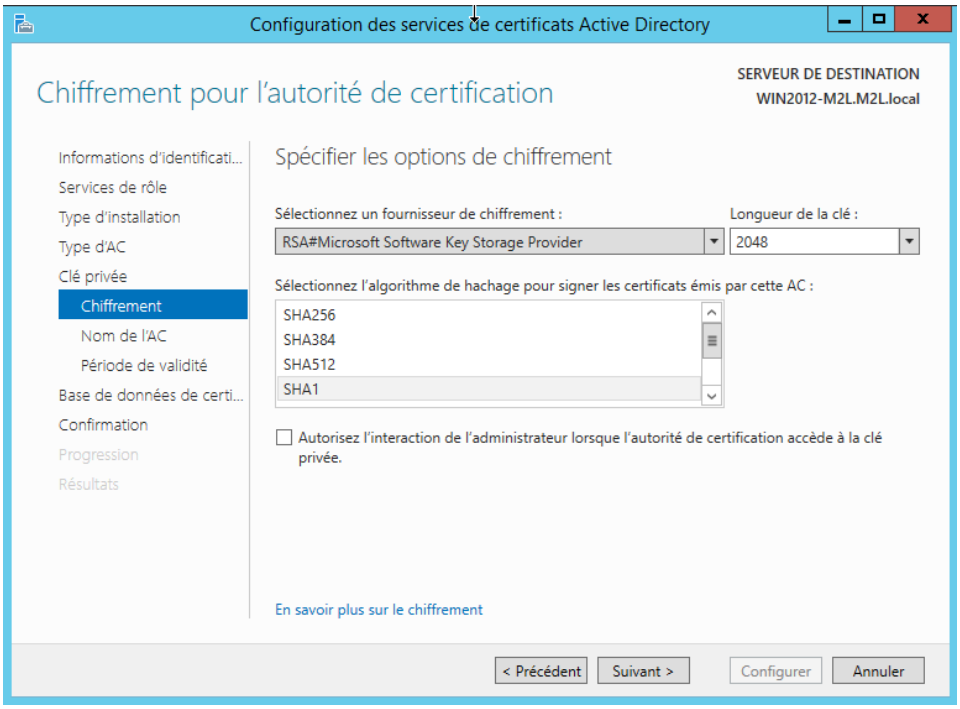

Figure 6 : Choix de l'algorithme de chiffrement

Je nomme l'Autorité de Certification.

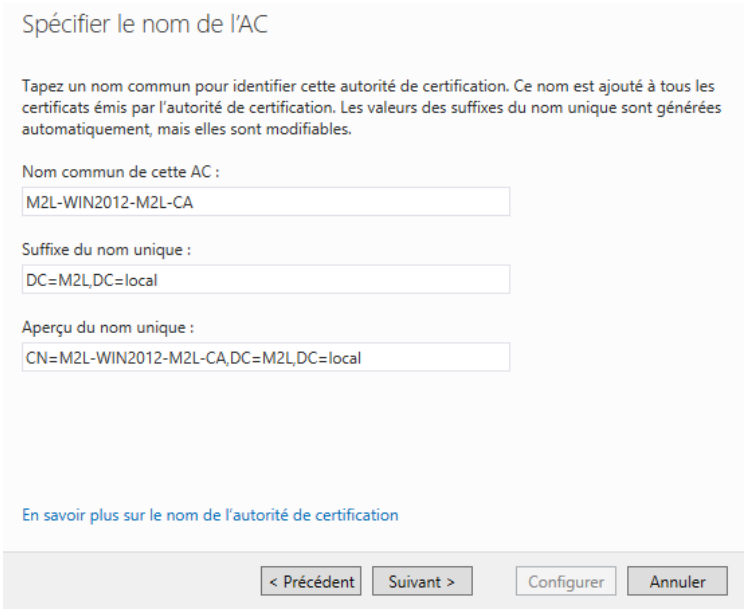

Figure 7 : Nom de l'AC

Je laisse ensuite la période de validité à 5 année.
Et j'indique les emplacements de la base de données de certificats ainsi que le journal de la base.

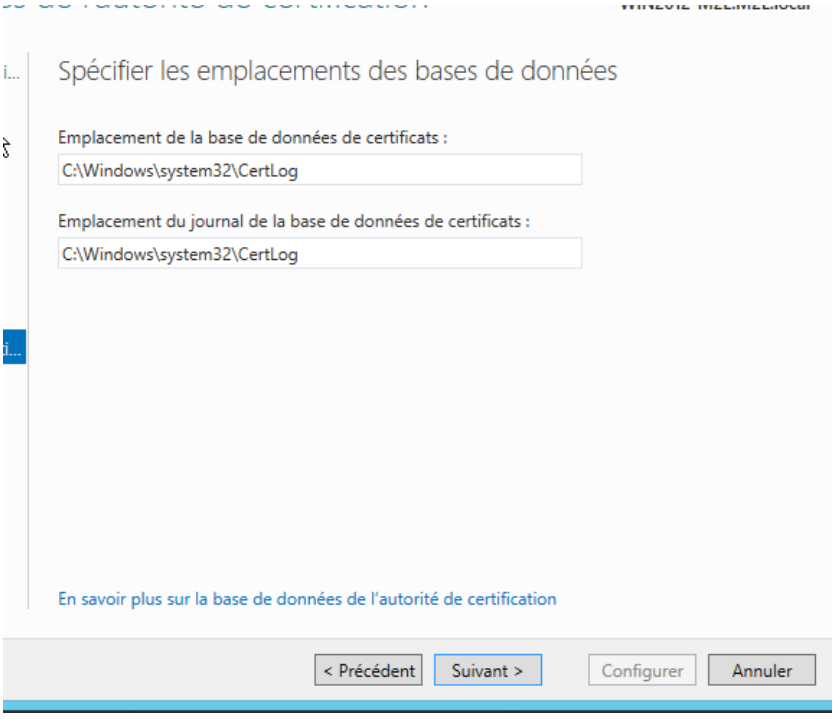

Figure 8 : Emplacement des bases de données

Il ne me reste plus qu'à faire Configurer pour finaliser la configuration.

Mon Autorité de certification est maintenant configurer et fonctionnelle

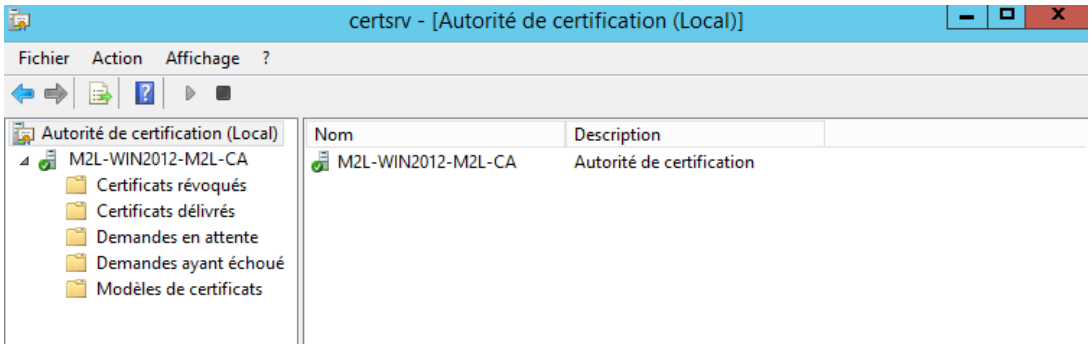

Figure 9 : Autorité de certification fonctionnelle

b) Installation et configuration du Services de stratégie et d'accès réseau

Maintenant je vais procéder à l'installation du Services de stratégie et d'accès réseau qui corresponds au serveur NPS.

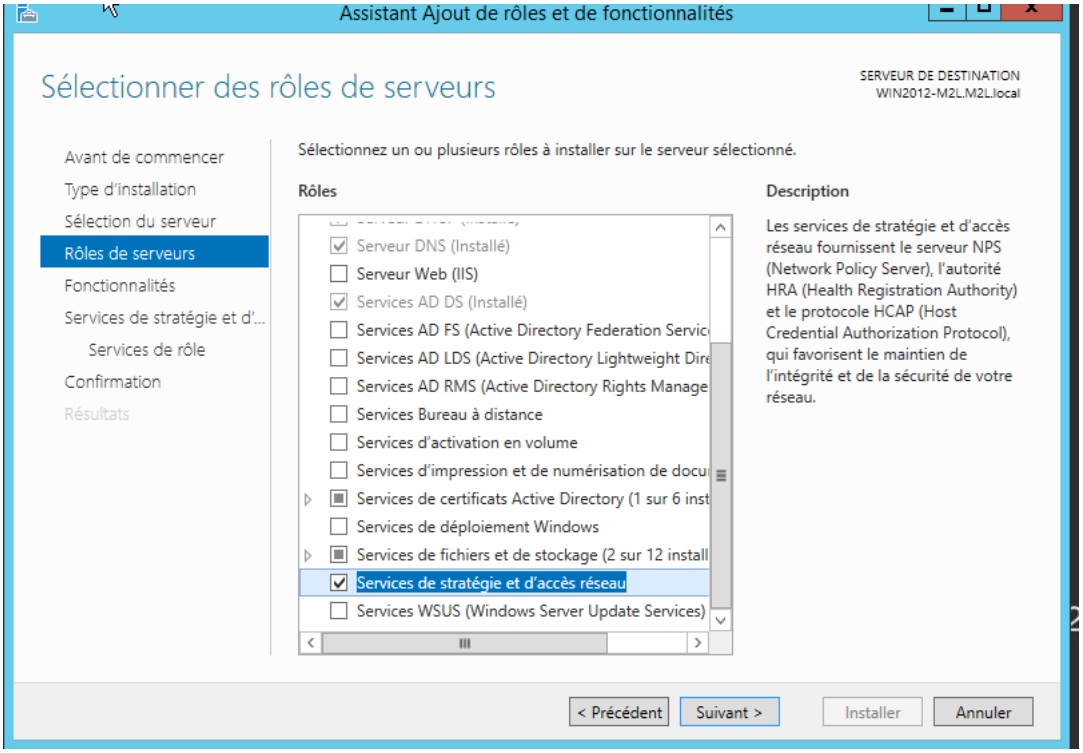

Figure 10 : Ajout des Services de stratégies d'accès réseau

Avant d'instaurer un nouveau client radius je vais réserver une adresse dans mon serveur DHCP, je vais la dédier à mon futur point d'accès Wifi.

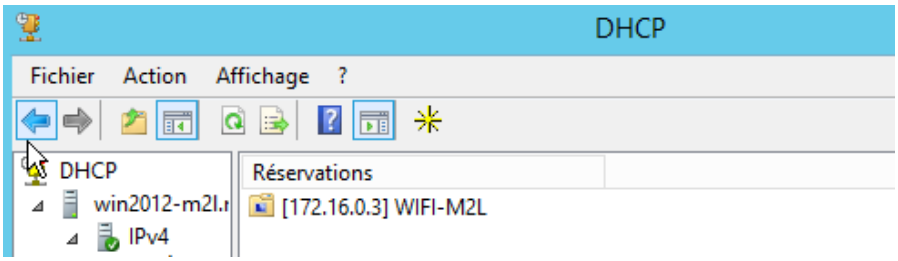

Figure 11 : Réservation IP dans le serveur DHCP

J'ouvre maintenant mon serveur NPS pour passer à la configuration, pour ça je l'ouvre par le biais du Gestionnaire de serveur.

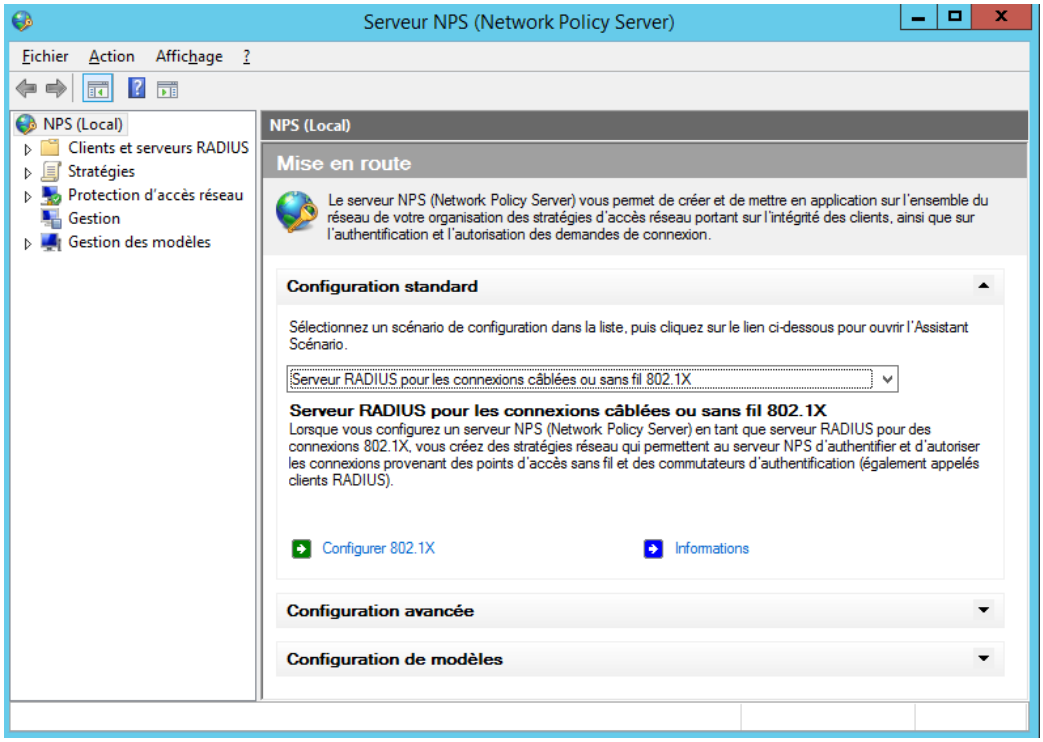

Figure 12 : Configuration 802.1X

Je choisis **Configurer 802.1X**, puis je sélectionne Connexions sans fil sécurisées et je renomme le type de connexion.

Figure 13 : Connexions sans fil sécurisées

Ensuite j'ajoute un nouveau client Radius qui est donc ma borne, je configure donc le Nom, l'adresse IP ainsi que le code secret partagé (ce code je devrais aussi le mettre dans la configuration de ma borne).

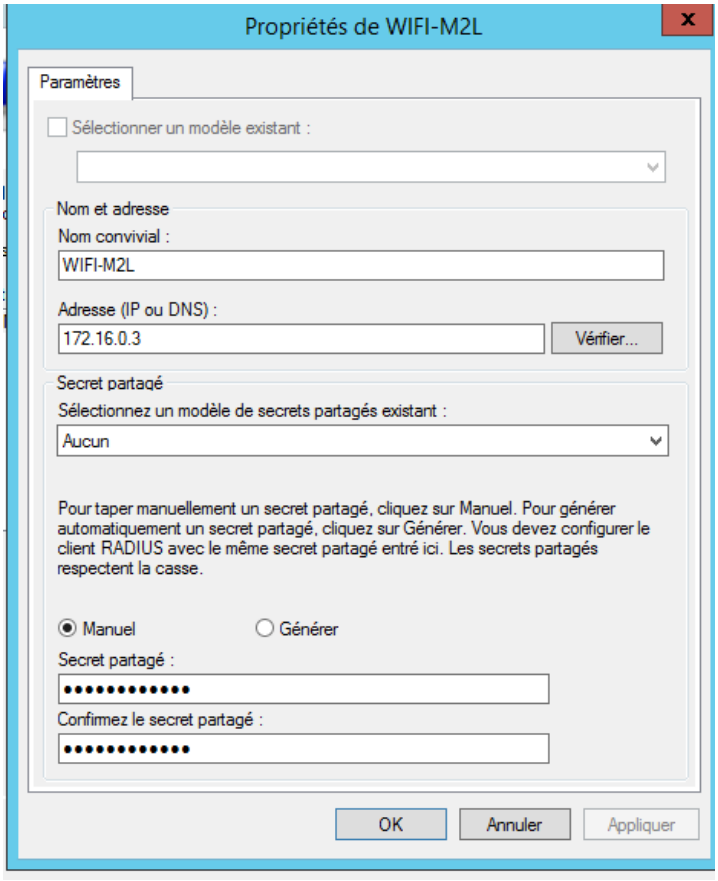

Figure 14 : Ajout d'un client Radius

Ensuite je choisis le type de protocole **EAP** pour cette stratégie, je sélectionne Microsoft : **PEAP**, et je le configure avec mon nouveau certificat.

J'ai besoin d'un mécanisme d'authentification de l'utilisateur qui souhaite se connecter au réseau. **EAP** (ou plus précisément Protected EAP) est le protocole idéal dans notre cas : il permet au point d'accès d'interroger un serveur d'identification (Radius) avant d'autoriser l'utilisateur à accéder aux ressources réseau de l'entreprise. Le serveur Radius, lui se chargera d'interroger l'Active Directory pour savoir si les informations d'authentification (login + password) sont valides ou pas : si oui, le serveur Radius donnera conformation au Point d'accès Wifi. La version de **PEAP** utilisée fait appel à un mécanisme d'authentification **MSCHAPv2** : le nom réel de la solution sera donc **PEAP-EAP-MSCHAPv2** où l'authentification est faite par login/password. **PEAP-EAP-TLS** fait référence à un mécanisme d'authentification renforcé basé sur des certificats. (D'où l'installation d'un nouveau certificat).

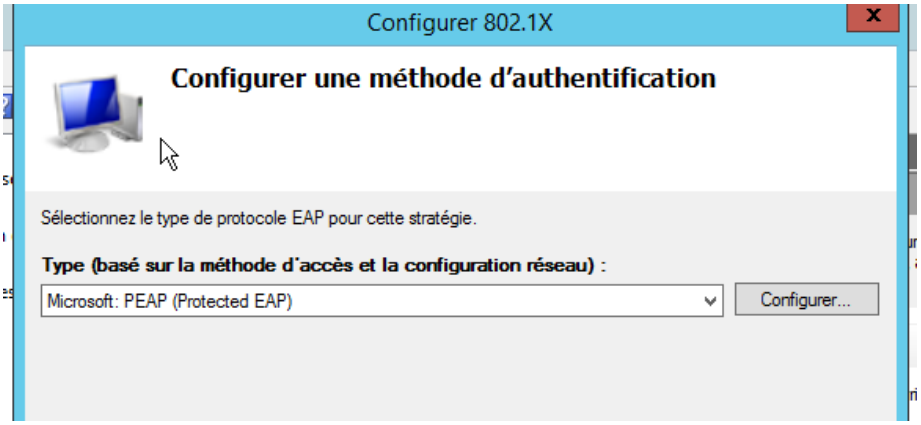

Figure 15 : Configuration du type de protocole EAP pour la stratégie

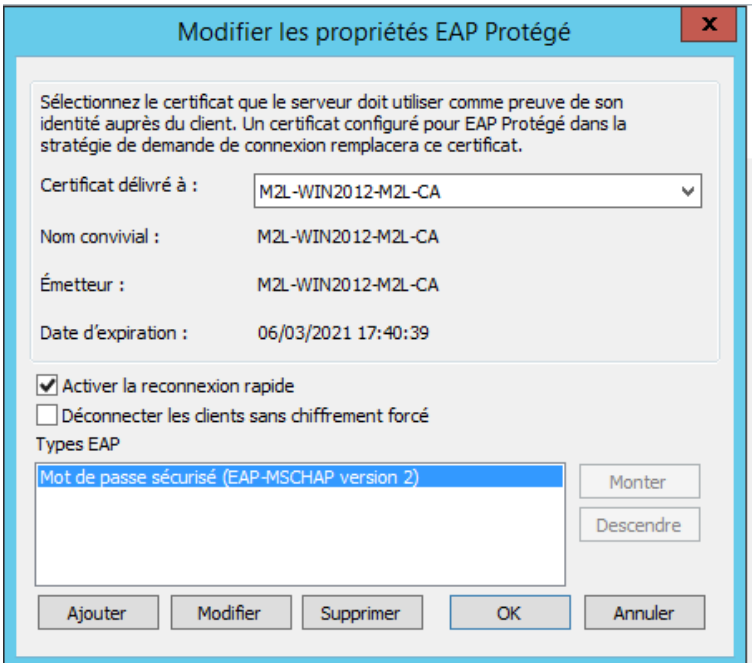

Figure 16 : Sélection du certificat

Maintenant je spécifie le groupe d'utilisateurs qui aura accès à cette stratégie, ce groupe d'utilisateurs je l'ai au préalablement crée dans mon AD.

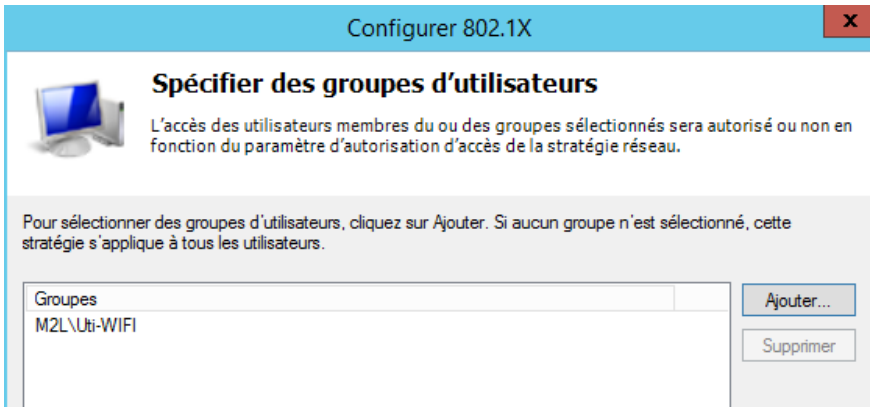

Figure 17 : Groupe pour la stratégie

La configuration du nouveau client Radius est fini ainsi que sa stratégie d'accès. Mais il ne faut pas oublier d'inscrire le serveur dans l'AD.

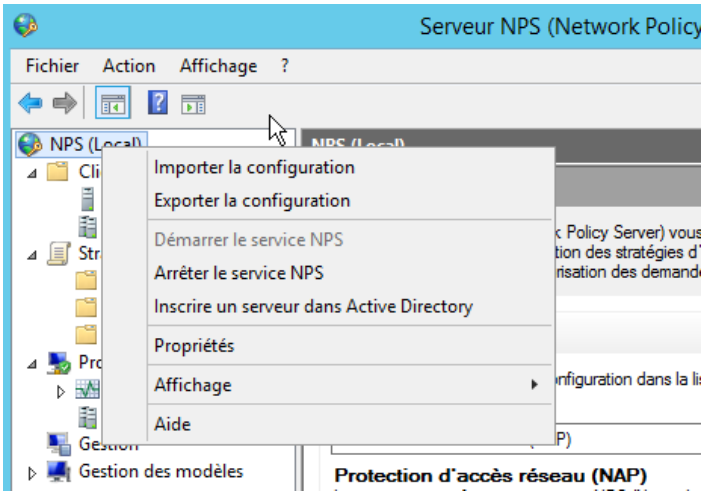

Figure 18 : Inscription d'un serveur dans l'AD

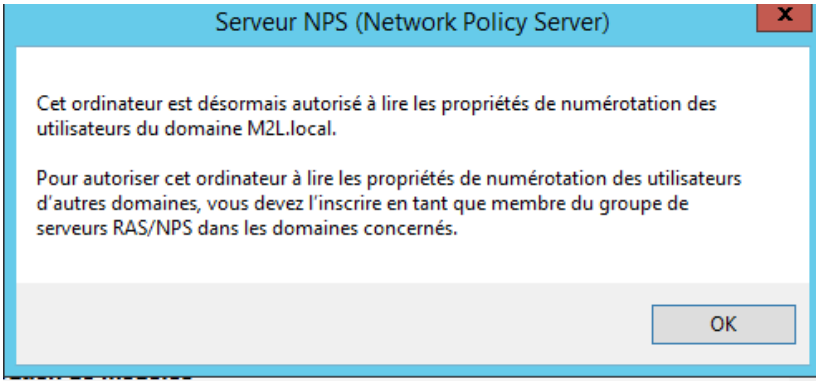

Figure 19 : Inscription du serveur dans l'AD

Afin d'avoir un suivi des tentatives de connexions, je configure le serveur pour qu'il me génère un fichier texte. Pour ça il faut aller dans « **Gestion** », et cliquer sur « **Configurer la gestion des comptes** ».

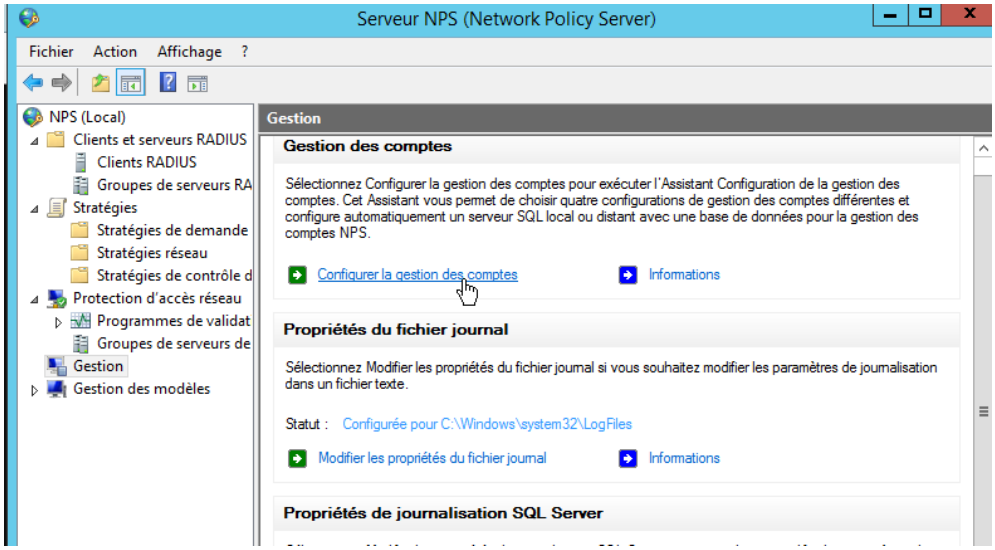

Figure 20 : Configurer la gestion des comptes

Je sélectionne donc « **Enregistrer les données dans un fichier texte sur l'ordinateur local.** »

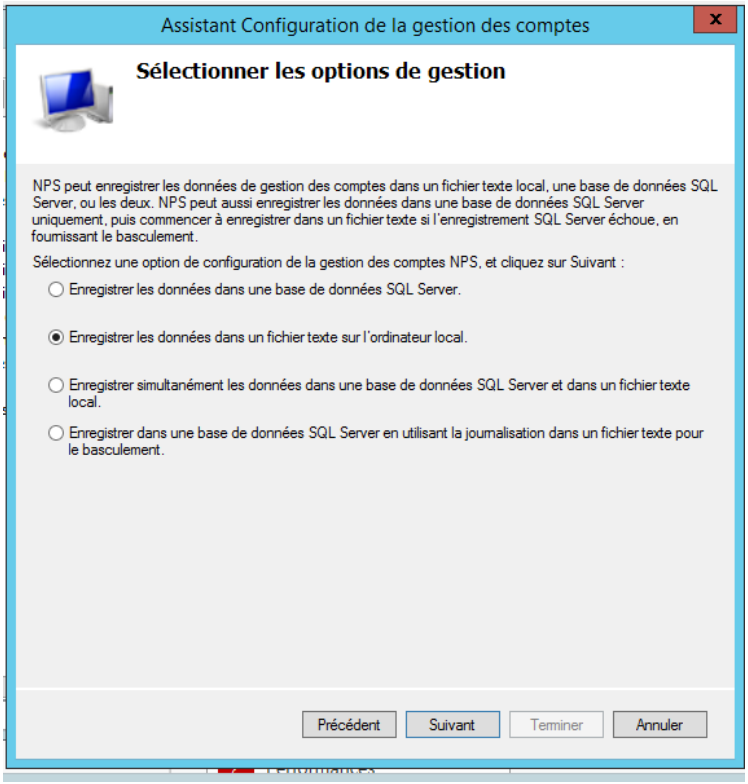

Figure 21 : Enregistrement des données sur le PC

Maintenant il me faut tout cocher afin d'après des fichiers Logs lisible et je choisis le chemin où je veux le créer.

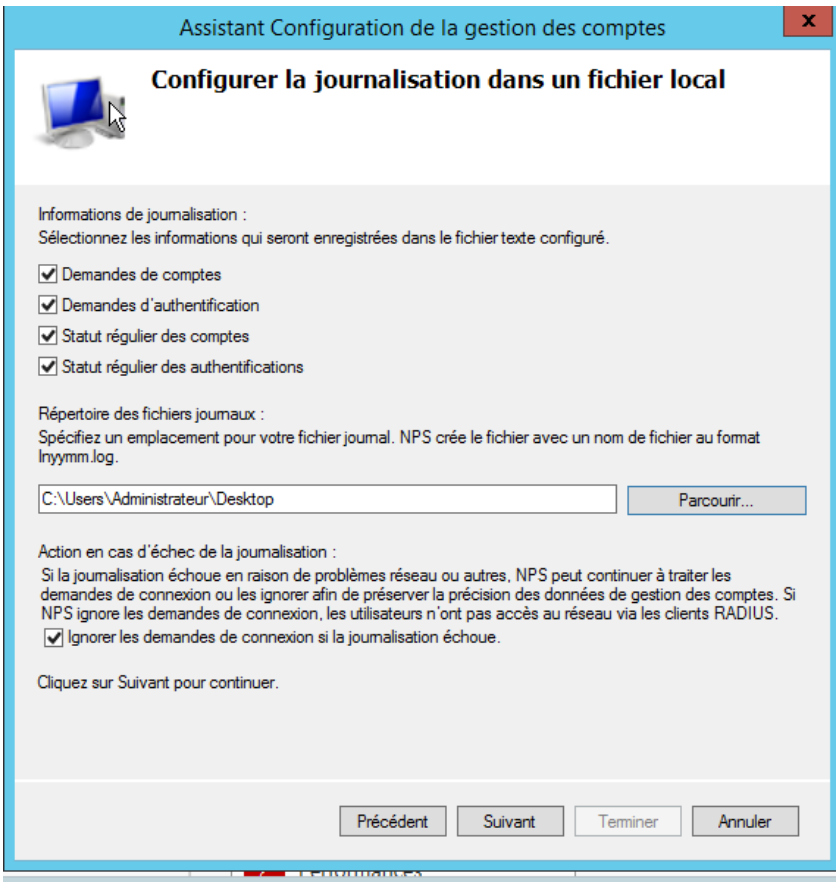

Figure 22 : Journalisation dans un fichier local

c) Configuration des propriétés des utilisateurs de l'Active Directory

Ensuite pour chaque utilisateur dont je veux donner l'accès au Wifi, il faut que je modifie quelques paramètres dans les propriétés comme :

Dans l'onglet Appel entrant, il faut Autoriser l'accès réseau.

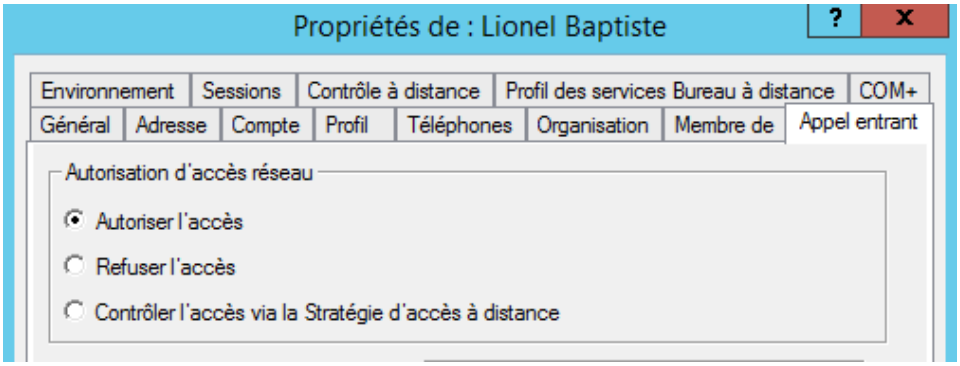

Figure 23 : Appel entrant

L'ajouter au groupe Uti-WIFI.

Figure 24 : Ajout dans le groupe Uti-WIFI

d) Mise en place d'une stratégie de groupe

Afin que les utilisateurs de la Maison des Ligues n'est pas besoin de configurer ses paramètres Wifi, je décide de créer une GPO afin que la configuration soit automatique à l'ouverture de leur session.

Pour ça j'ouvre la console de Gestion de stratégie de groupe et je crée un nouvel objet GPO que je renomme Stratégie WIFI 802.1X.

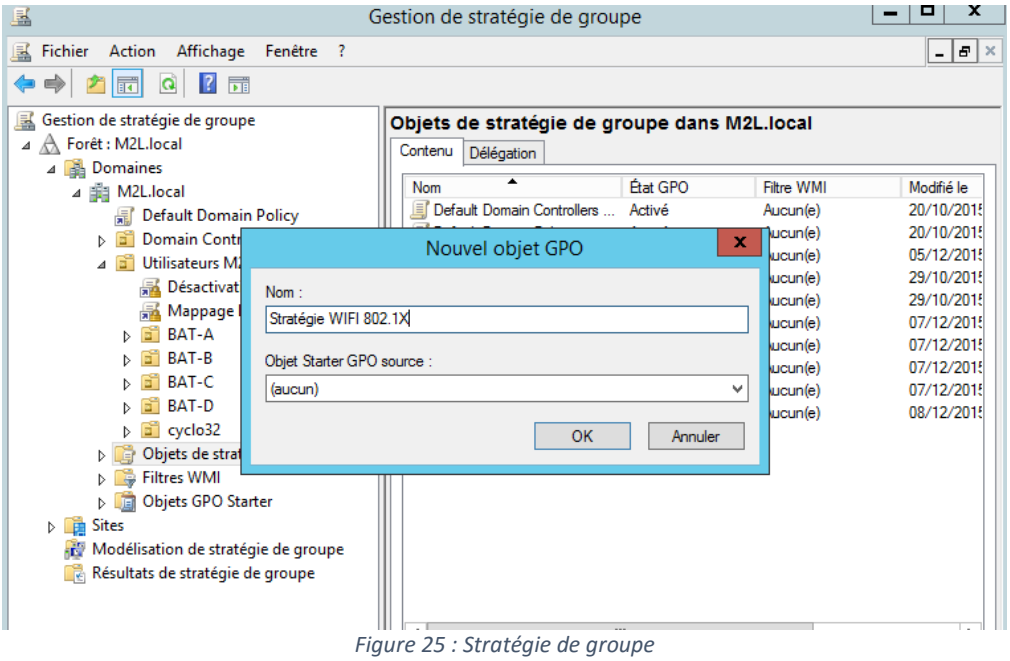

Figure 25 : Stratégie de groupe

Je fais bouton droit de la souris sur « **Stratégie WIFI 802.1X** », je clique sur le bouton droit « **Modifier** » et je développe « **Configuration ordinateur** » → « **Stratégies** » → « **Paramètres Windows** » → « **Paramètres de sécurité** » → Clique sur « **Stratégies de réseau sans fil** (IEEE802.11) » → « **Créer une stratégie de réseau sans fil pour Windows Vista et versions ultérieures** »

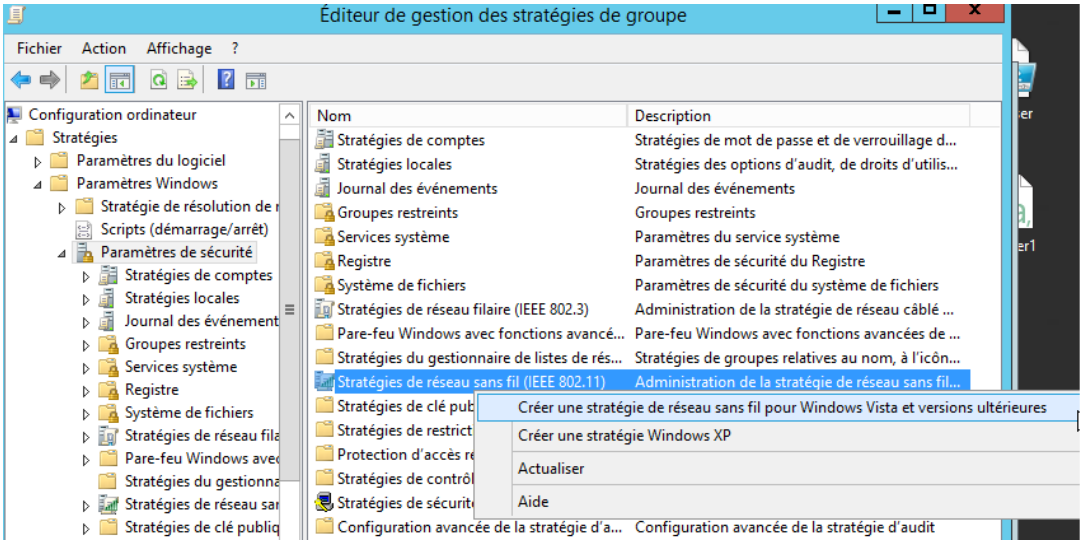

Figure 26 : Stratégie de réseau sans fil

Je crée dans un premier temps une stratégie pour les postes informatiques sous Windows vista et plus récent.
J'ajoute donc un nom à ce profil et je l'attribue à mon SSID.

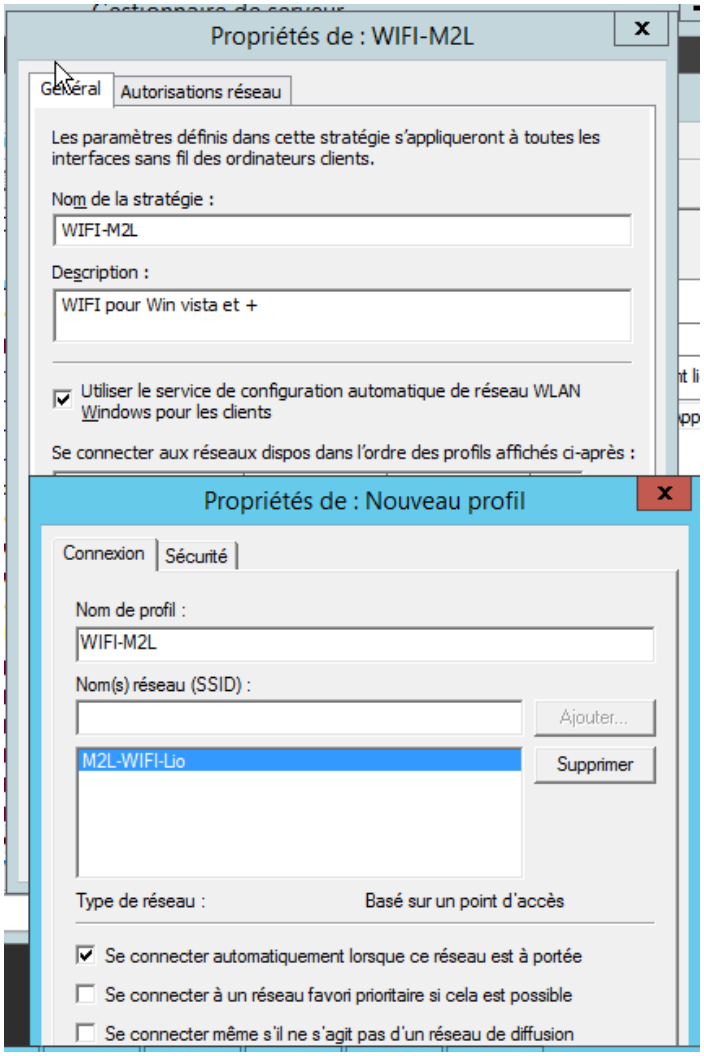

Figure 27 : Configuration de la stratégie de réseau sans fil

Ensuite je vais dans l'onglet Sécurité, pour initialiser l'Authentification « WPA2-Entreprise » et le chiffrement « AES », je sélectionne la méthode d'authentification précédemment choisie « PEAP » ainsi que le mode d'authentification « Utilisateur ou ordinateur »

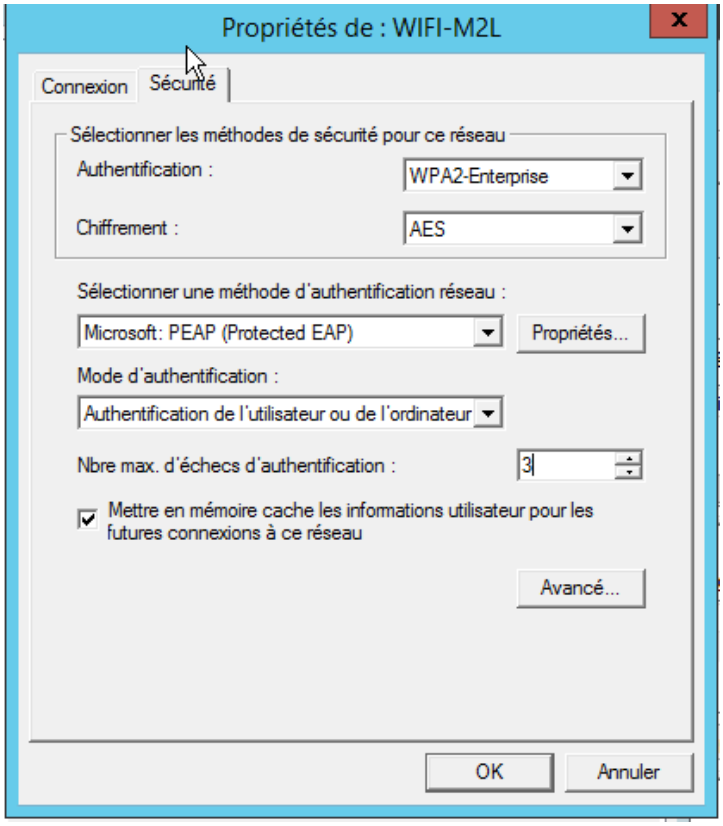

Figure 28 : Sécurité de la stratégie

Maintenant dans l'onglet Autorisations réseau, je décoche toutes les cases sauf « Autoriser l'utilisateur à afficher les réseaux refusés » et « Autoriser tout le monde à créer tous les profils utilisateur ».

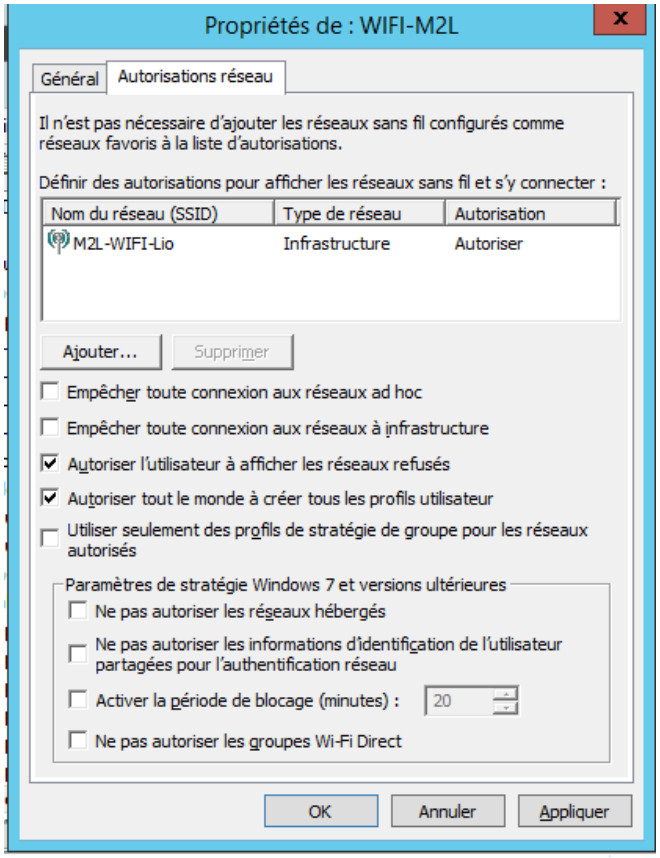

Figure 29 : Autorisation de la stratégie

A présent je refais clique droit et je crée une stratégie Windows XP de la même manière que pour vista et plus récent.

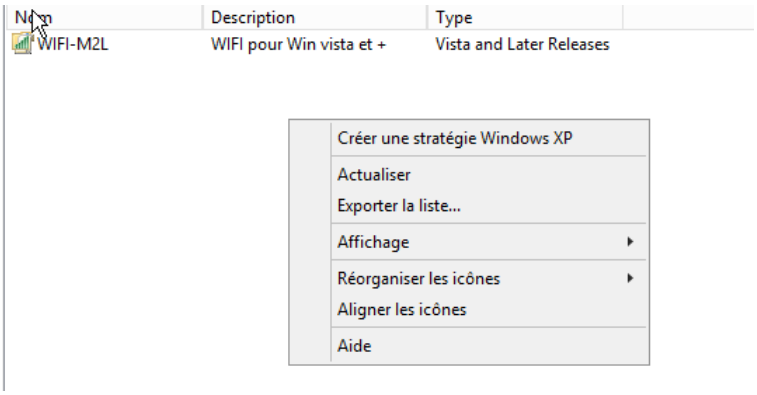

Figure 30 : Création d'une stratégie Win XP

Voilà ma GPO finit d’être paramétrée.

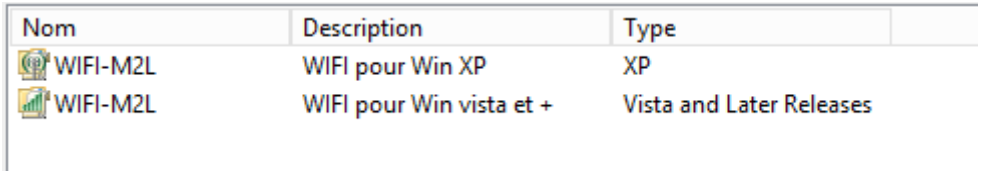

Figure 31 : Les deux stratégies d'accès réseau

Je peux donc l'appliquer à tous les Utilisateurs M2L.

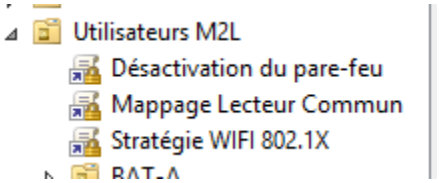

Figure 32 : Ma nouvelle GPO Active

e) Configuration du point d'accès Wifi WRT54GL

Pour finaliser l'installation de mon Wifi d'entreprise, il ne me reste plus qu'à configurer mon AP.
Pour ça je me connecte à celle-ci par le biais d'un navigateur Web en tapant son adresse IP.

Je désactive tout type de connexion WAN, je change le nom du routeur en « WIFI-M2L » et j'ajoute aussi le nom de mon domaine qui est celui du contexte M2L et de mon précédent projet « M2L.local ».

Je rentre les paramètre IP du routeur Wifi :

AdresseIP	172.16.0.3	*Adresse réserver dans mon DHCP*
Masque	255.255.0.0	
Passerelle	172.16.0.254	*Adresse de passerelle de mon serveur (Interface Ipcop du précédent projet)*
DNS local	172.16.0.1	*Adresse DNS de mon serveur M2L.local*

Enfin je paramètre le « Relay DHCP » afin que le routeur Wifi, demande à mon serveur DHCP de distribuer des adresses IP aux utilisateurs du Wifi.

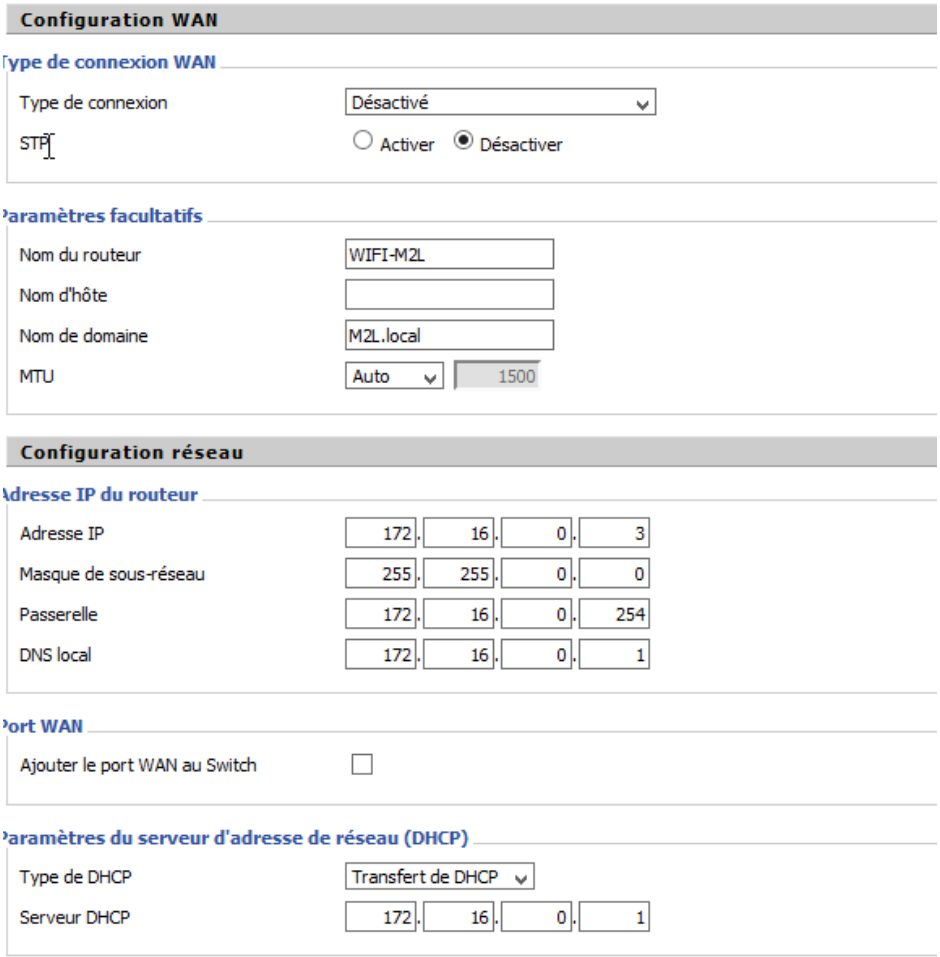

Figure 33 : Configuration réseau + relay DHCP

A présent je configure le réseau Wifi de celui-ci, je choisis donc le SSID en fonction de celui que j'ai initialiser lors de la configuration de ma GPO, soit « M2L-WIFI-Lio ».

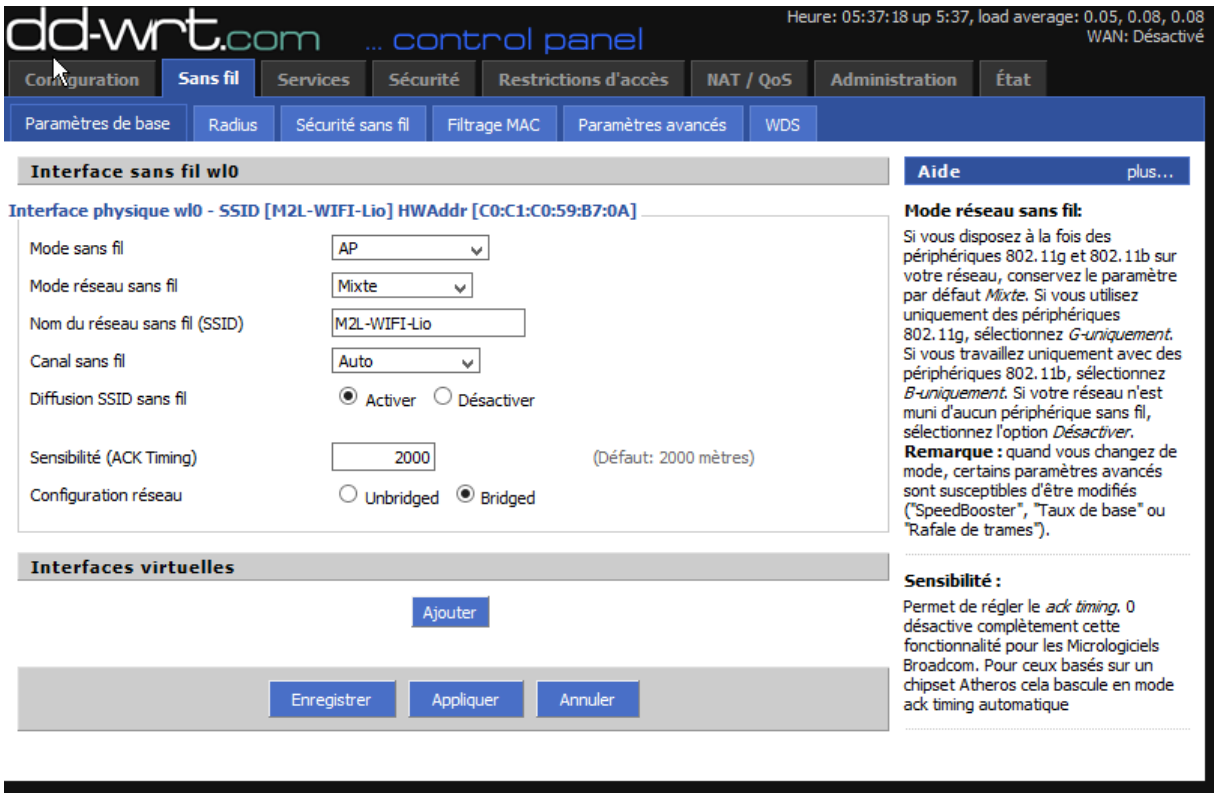

Figure 34 : Configuration WIFI de base

Ensuite je configure le serveur Radius « Remote Authentification Dial-In User Service ».
Je l'active, j'insère l'adresse de mon serveur Radius qui est donc celle de mon serveur de domaine, j'attribue le port du serveur, qui est par défaut « 1812 ».
Je choisis le format du mot de passe qui est la clé partagée précédemment initialiser à la création du client radius sur le serveur NPS. Puis j'enregistre la configuration.

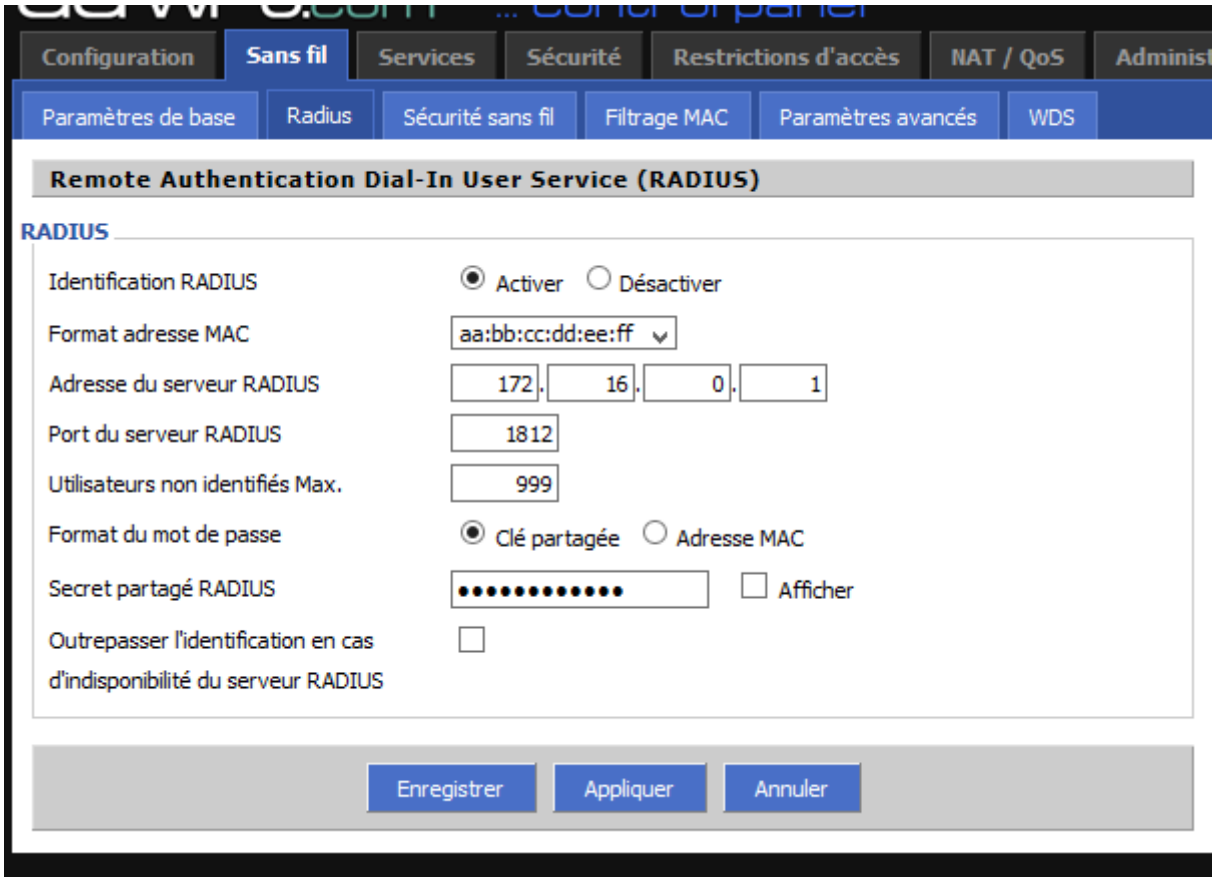

Figure 35 : Configuration Radius

Et pour finir je vais dans l'onglet « **Sécurité sans fil** », je sélectionne le mode de sécurité « **WPA2-Entreprise** », cryptage WPA « **AES** », l'adresse de mon serveur Radius, le port par défaut du serveur Radius et encore une fois la clé partagée. Puis j'enregistre.

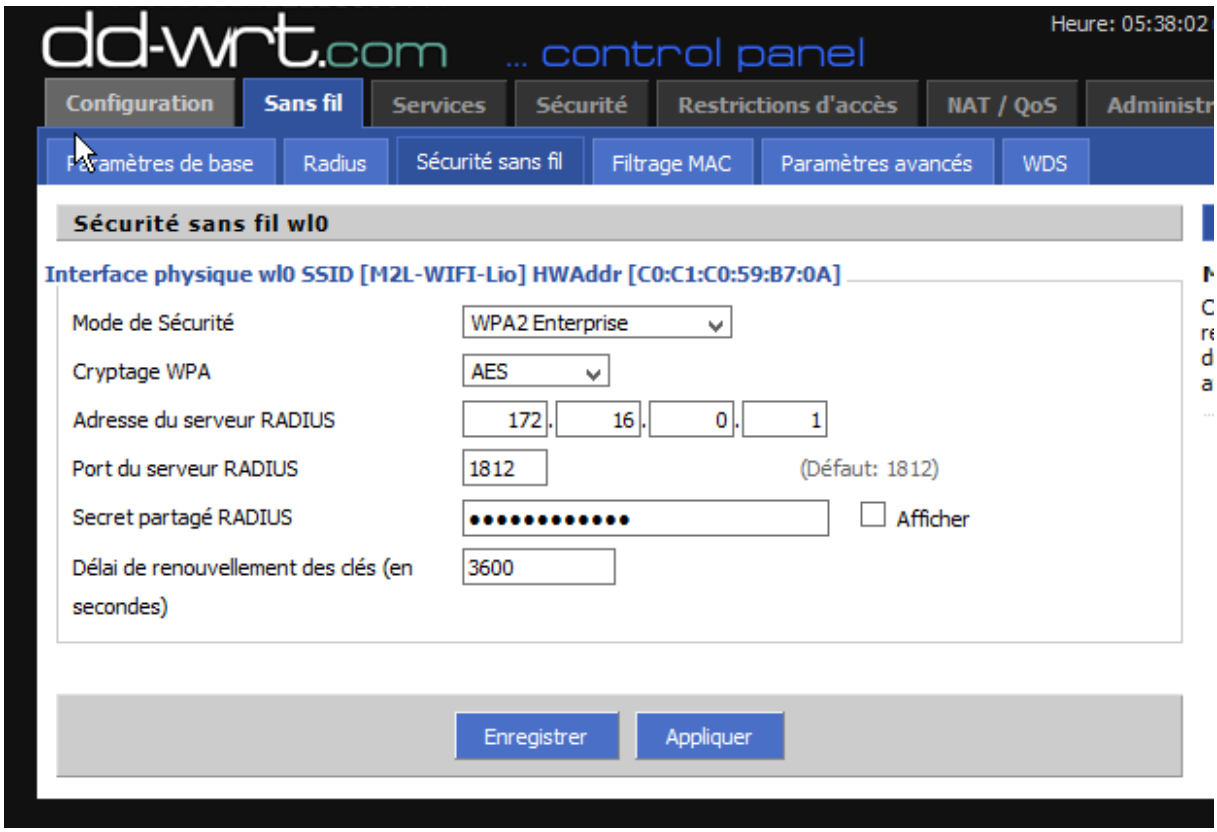

Figure 36 : Configuration de la sécurité sans fil

6. Conclusion

a. Condition initiale

Initialement, j'avais qu'un seul système d'exploitation de disponible sur ma machine de tous les jours, je n'avais donc pas de machine TEST, ni même répondu aux attentes du professeur.

b. Condition finale

Cette opération m'a permis d'avoir deux systèmes d'exploitation sur ma machine de tous les jours. Je peux donc effectuer tous les tests que je désire comme des modifications de la base de registre, des installations de logiciels pas dangereux et tout cela sans risquer d'endommager la machine hôte.

c. Durée de l'activité

Pour cette activité j'ai mis environ 1 heure à la réaliser, ce fût un peu long dû au fait qu'il faut installer le deuxième OS exactement comme sur un ordinateur physique. Le temps d'installation a été le plus long de l'activité.

d. Solution envisagée

Par la suite, si je souhaite faire évolué ma machine virtuelle je peux le faire par le biais de la configuration en augmentant la capacité du disque dur virtuel ou encore des capacités de mémoire vives.

La situation professionnelle est basée sur le contexte de la Maison des Ligues de Lorraine, comme pour le précédent projet. D'ailleurs je me suis servi de mon premier projet pour effectuer celui-ci. Il m'a été demandé de créer un Wifi d'entreprise sécurisé, après l'étude de plusieurs solutions, j'ai opté pour sécuriser mon Wifi, d'utiliser un serveur NPS avec authentification PEAP. Cela me permet d'être dans la continuité de mon projet 1 car cette méthode d'authentification utilise les comptes utilisateurs de l'Active directory ainsi que le serveur DHCP et DNS de mon contrôleur de domaine. L'infrastructure réseau existante ne disposait pas de WIFI. J'ai donc mis en place un serveur de domaine «M2L » avec Active Directory, DNS, DHCP et NPS. J'ai utilisé une GPO pour automatiser les paramètres d'authentification sur le SSID M2L-WIFI-Lio. Grâce à cette GPO, l'utilisateur n'a rien à faire pour accéder au Wifi d'entreprise, la GPO fait le lien avec son login et password de l'AD afin d'authentifier l'utilisateur au serveur NPS.

Maintenant La Maison des Ligues dispose d'un accès internet sécurisé via un pare-feu ainsi d'un serveur de domaine disposant d'un Active Directory, DHCP, DNS, NPS et d'une connexion WIFI sécuriser au maximum. Chaque bâtiment dispose d'un répertoire dédié, ainsi qu'un répertoire commun.

Grâce à ce type d'authentification, les utilisateurs équipés de smartphone, pourront se connecter au réseau Wifi d'entreprise par le biais de leur identifiant/mot de passe de l'AD (celui qu'ils utilisent pour ouvrir l'un session).