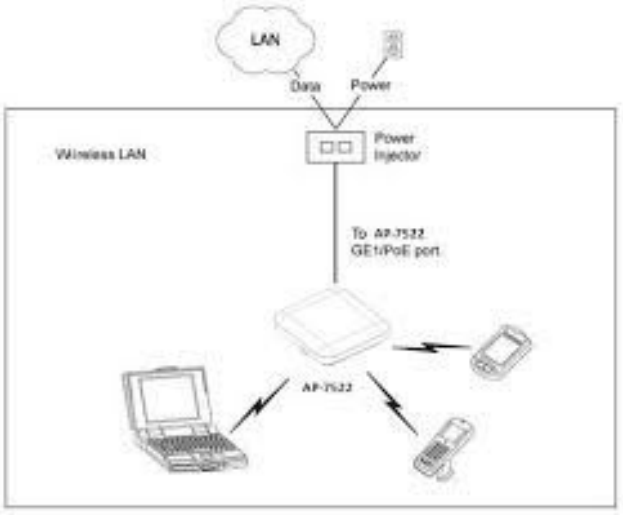
MISSION N° 2 - Configuration et installation d'un point d'accès relié à un serveur Radius

Partie 1 - Configuration du point d'accès wifi

Il m'a été demandé de configurer deux points d'accès wifi afin d'étendre sa portée car certains zones de l'entreprise n'était pas couverte par le réseau.

N'ayant jamais configuré de PA avant, j'ai dû m'informer sur le sujet au préalable, comment le brancher correctement, accéder à la page de configuration etc… sur internet.



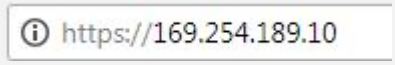
Une fois l'appareil bien branché, c'est à dire le PA relié à un Power Injector lui même relié au réseau par la box et relié à une prise d'alimentation, il fallait me connecter à l'interface.

L’appareil possédant une adresse ip de base étant : 169.254.189.10, il me fallait pouvoir communiquer avec, or, en effectuant la commande “ping 169.254.189.10”, mon ordinateur (10.1.42.56) et l’appareil ne communiquaient pas car ils n’étaient pas sur le même réseau.

```
Envoi d’une requête ’Ping’  169.254.189.10 avec 32 octets de données :
Délai d’attente de la demande dépassé.
```

Une fois le problème décelé, j’ai du, à l’aide des droits administrateur, changer ma configuration ip en “169.254.189.11” afin de pouvoir me connecter à sa page d’interface.

Une fois l’adresse ip changé, le ping étant bon, je puis me connecter au point d’accès en tapant simplement son adresse ip dans la barre url d’un navigateur :

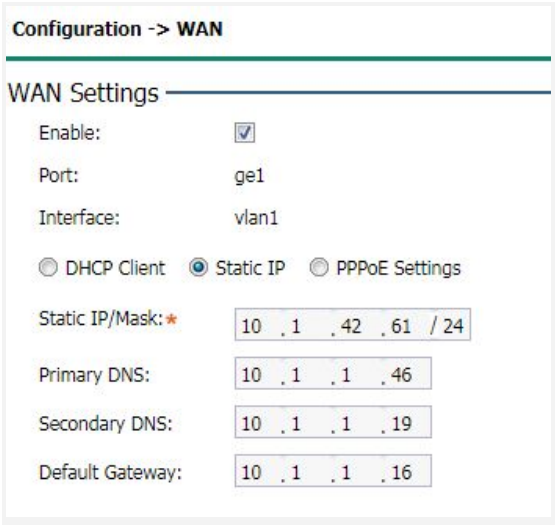


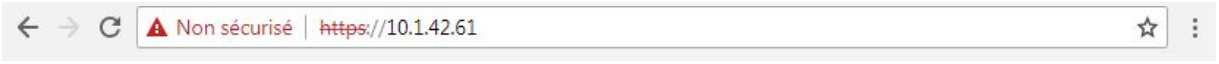
Cette manipulation m’a donc amené sur la première page, où des identifiants étaient demandés.

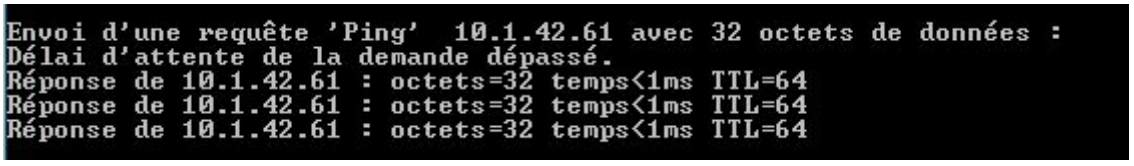
J’ai du me connecter avec les identifiants login “admin” mot de passe “admin” afin d'accéder à l’interface du point d’accès.

Etant donné que tout le monde sur le réseau pouvait accéder à cette page, la première chose à faire étant connecté était de immediatement modifier le mot de passe dans le but de sécuriser l’accès.

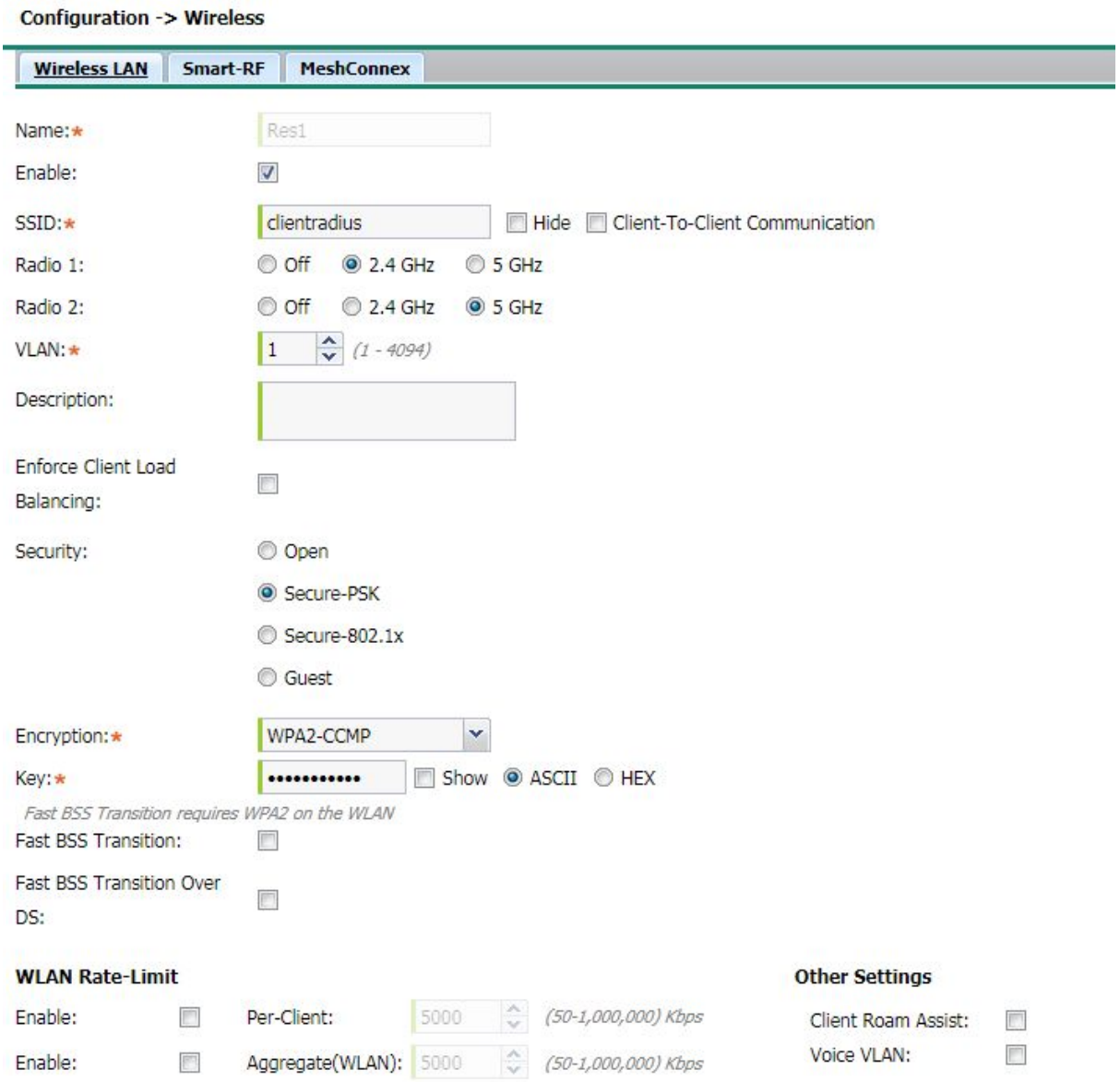
Ainsi, j'ai changé l'adresse ip du point d'accès en "10.1.42.61" afin de pouvoir revenir sur ma configuration de base et pouvoir m'y connecter. Ainsi, le ping passait, on pouvait donc s'y connecter encore une fois en tapant l'adresse ip dans la barre de recherche de son navigateur.







Une fois le mot de passe modifié et l'adresse ip attribué, le but est de créer un réseau, un SSID, un VLAN, un type de sécurité et une fréquence sur laquelle diffuser comme montré ci-dessous :



Ainsi, pour notre point d'accès, le SSID est "clientradius", c'est donc ainsi qu'il sera identifié comme réseau sans fil, il diffuse sur du 2.4 GHz et du 5 GHz, est attribué au VLAN n°1 et a pour type de sécurité du PSK en WPA2-CCMP avec la clef cryptée en ASCII.

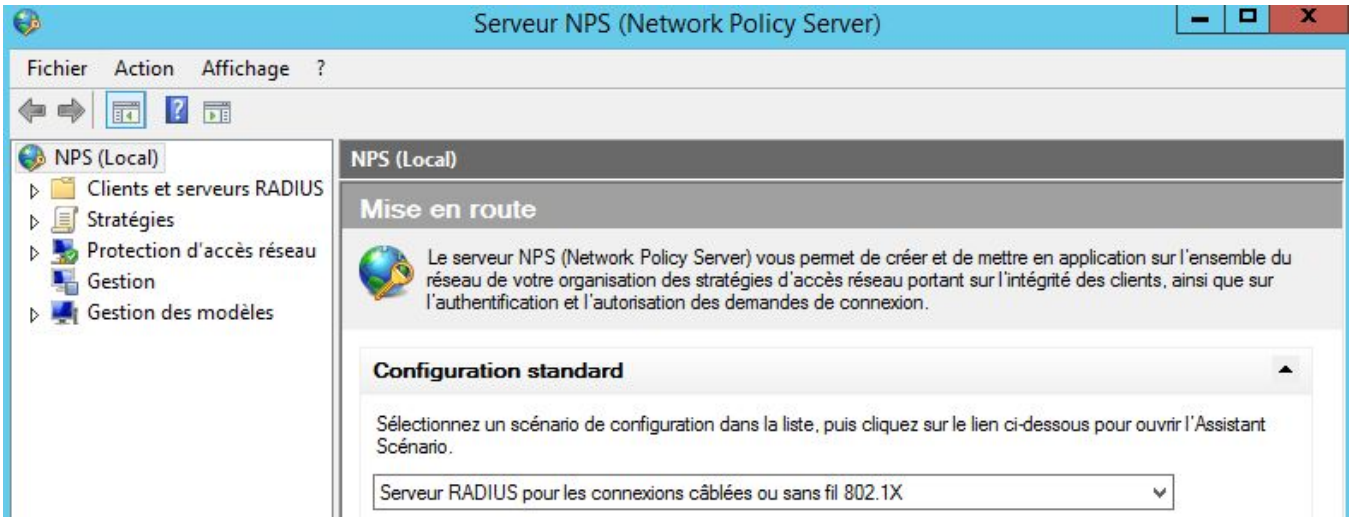
J'ai mis ces paramètres de sécurité pour tester l'appareil dans un premier temps et un ordinateur portable ou un téléphone pouvait s'y connecter.

Partie 2 - Installation d'un serveur Radius

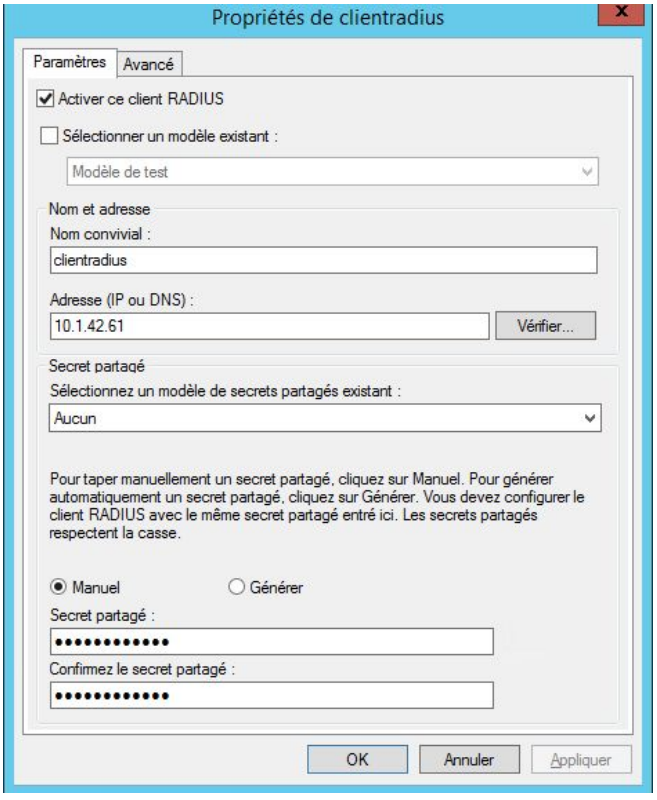
Il m'a ensuite été demandé d'installer un serveur Radius afin de sécuriser l'accès wifi au point d'accès. Ainsi, pour s'y connecter, il faut être membre du domaine dans lequel il sera inscrit et connaître l'identifiant et le mot de passe de son compte Active Directory.

On m'a fournit un serveur Windows 2012R2 (10.1.42.42) sur lequel j'avais les droits admin et le point d'accès.

La première étape fût d'installer un serveur NPS :

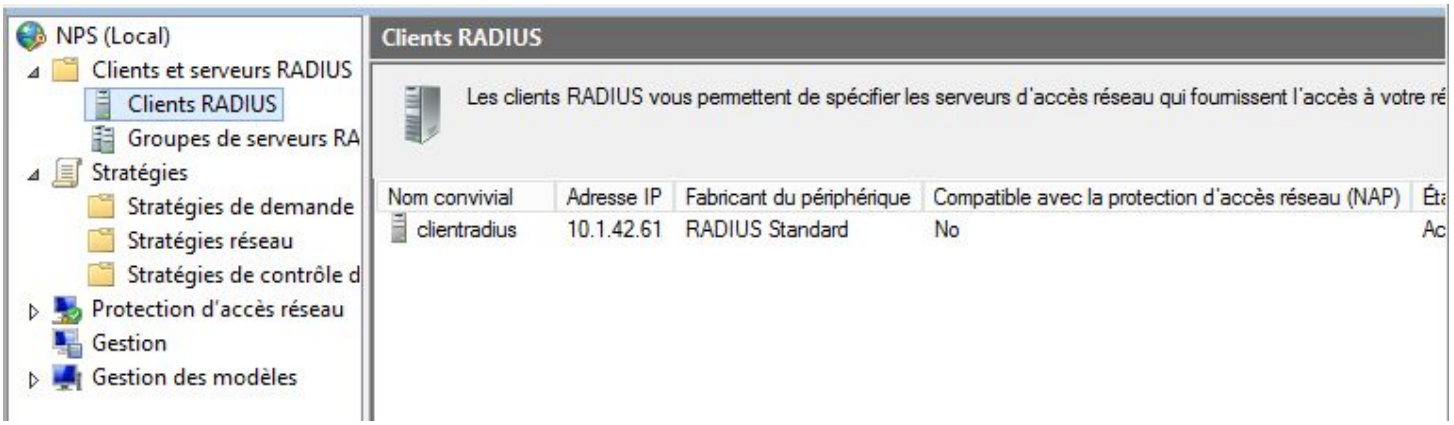


Une fois ce serveur installé, comme on peut le voir sur le côté gauche, il fallait créer un client Radius. Ce client représentera donc le point d'accès.



Ainsi, on lui donne un nom, une adresse ip (qui sera donc celle du point d'accès et dont on peut vérifier l'appartenance au réseau et à l'AD) puis on choisit un secret qui sera partagé entre le serveur NPS et le point d'accès pour crypter les échanges.

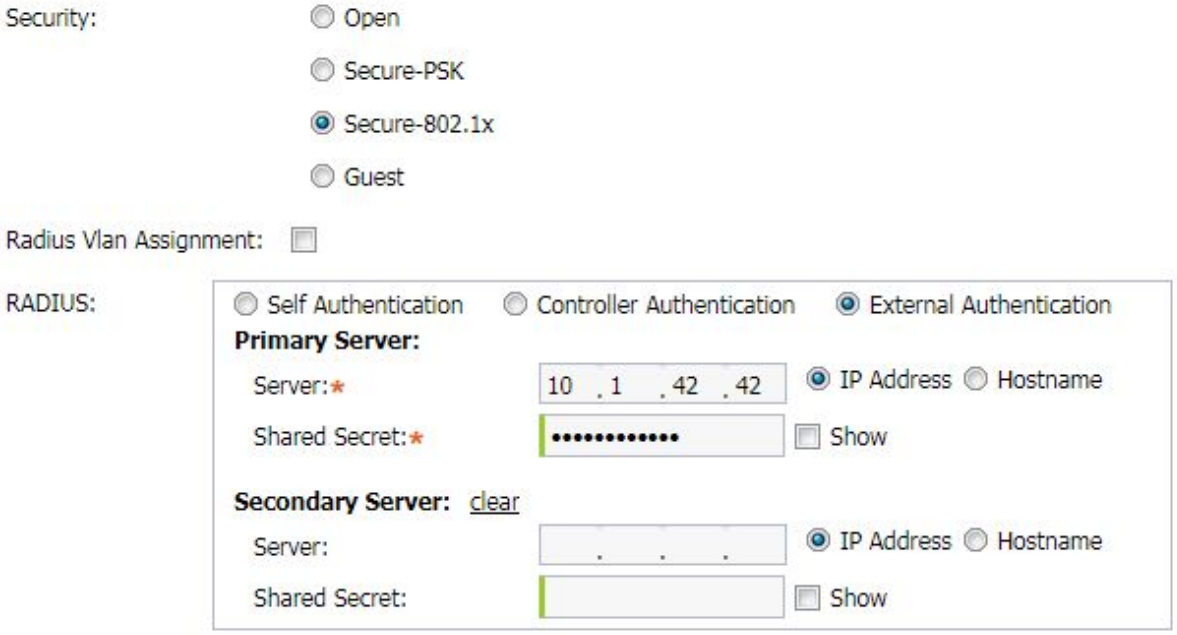
Le client Radius est alors créé :



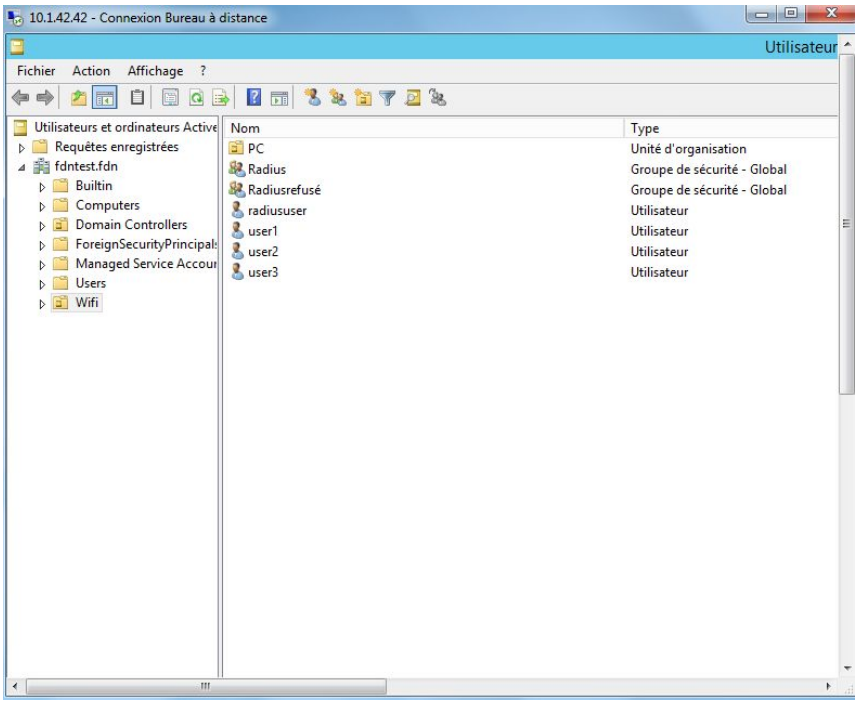
La prochaine étape est de retourner sur le point d'accès et changer le type de sécurité en 802.1x qui est un standard lié à la sécurité des accès informatique; il permet de contrôler l'accès aux équipements d'infrastructure réseau.

Ainsi, sur la page du point d'accès, il fallait modifier le type de sécurité en 802.1x et y assigner un serveur Radius. Il faut également le mettre en mode "Authentification externe" car le point d'accès possède un serveur Radius intégré mais nous n'allons pas l'utiliser.

Il faut donc mettre comme adresse ip du serveur Radius celle du serveur W2012R2 soit 10.1.42.42 et en secret partagé le secret rentré lors de la configuration du client Radius.



Une fois cette manipulation réalisé, il me fallait installer un serveur Active Directory pour pouvoir faire la connexion entre le serveur Radius et l'annuaire d'authentification.



Ensuite, il fallait lancer l'outils "Utilisateur et Ordinateurs Active Directory" et créer un groupe ensemble "Wifi" dans lequel on y mettra deux groupes :

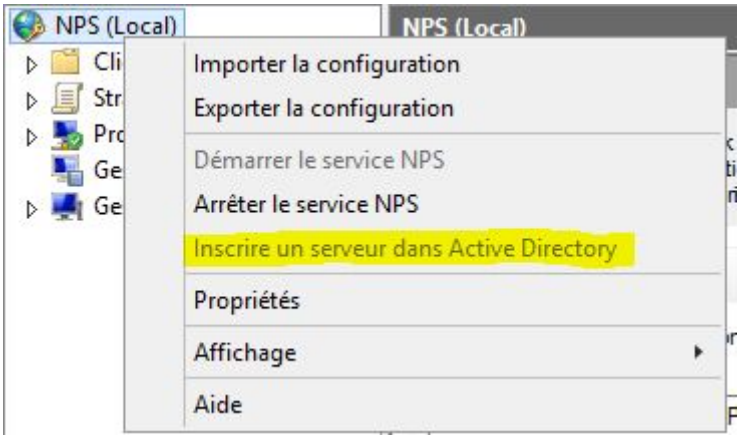
- Radius
- Radiusrefusé

Il faut ensuite créer des utilisateurs, ici :

- User1
- User2
- User3

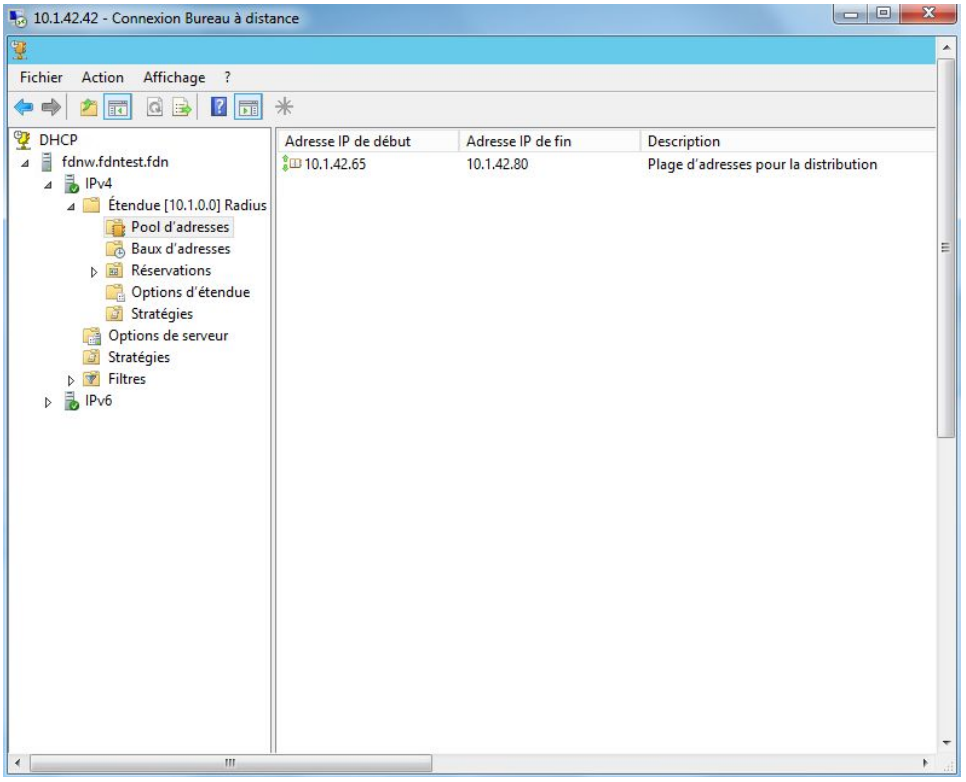
Ces groupes et ces utilisateurs m'ont permis de faire des test.

Enfin, il suffit d'inscrire le serveur Radius dans l'annuaire Active Directory :



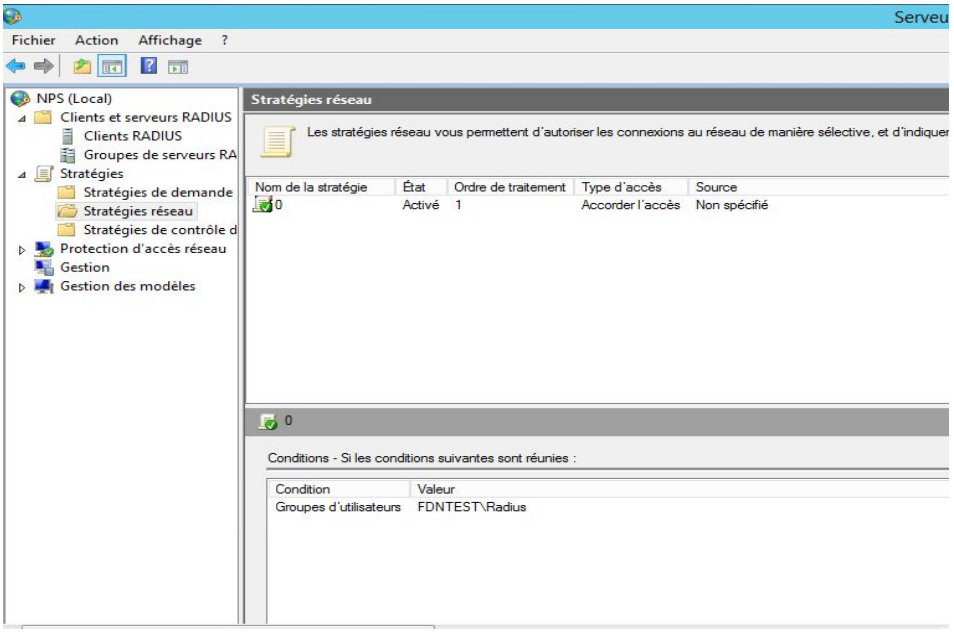
De ce fait, le serveur Radius peut communiquer avec l'AD et lui demander si l'identifiant et le mot de passe qu'il a reçu correspond ou non à un utilisateurs du domaine.

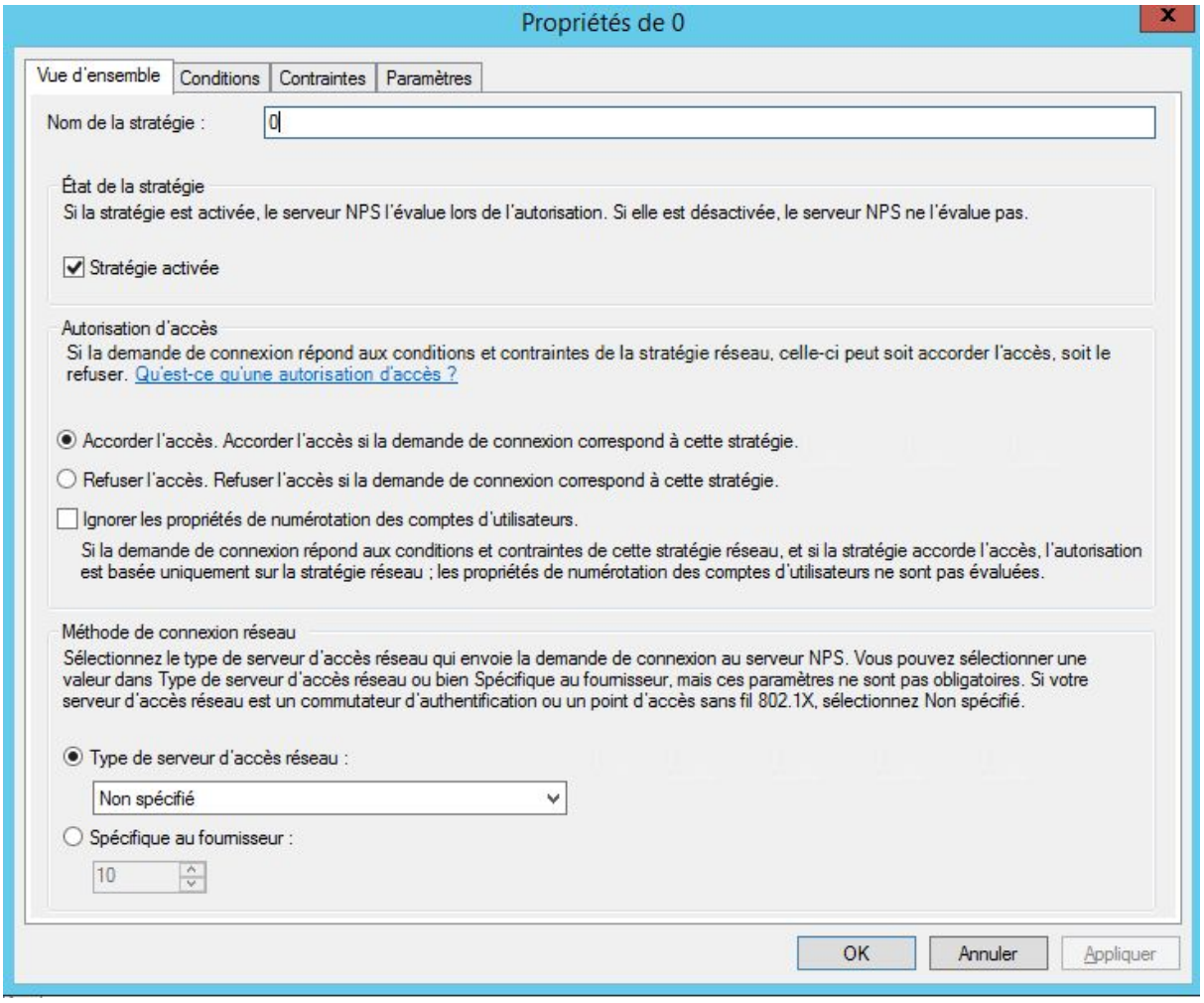
Ensuite, j'ai du installer un serveur DHCP afin que les utilisateurs qui se connectent au point d'accès reçoivent une adresse ip.



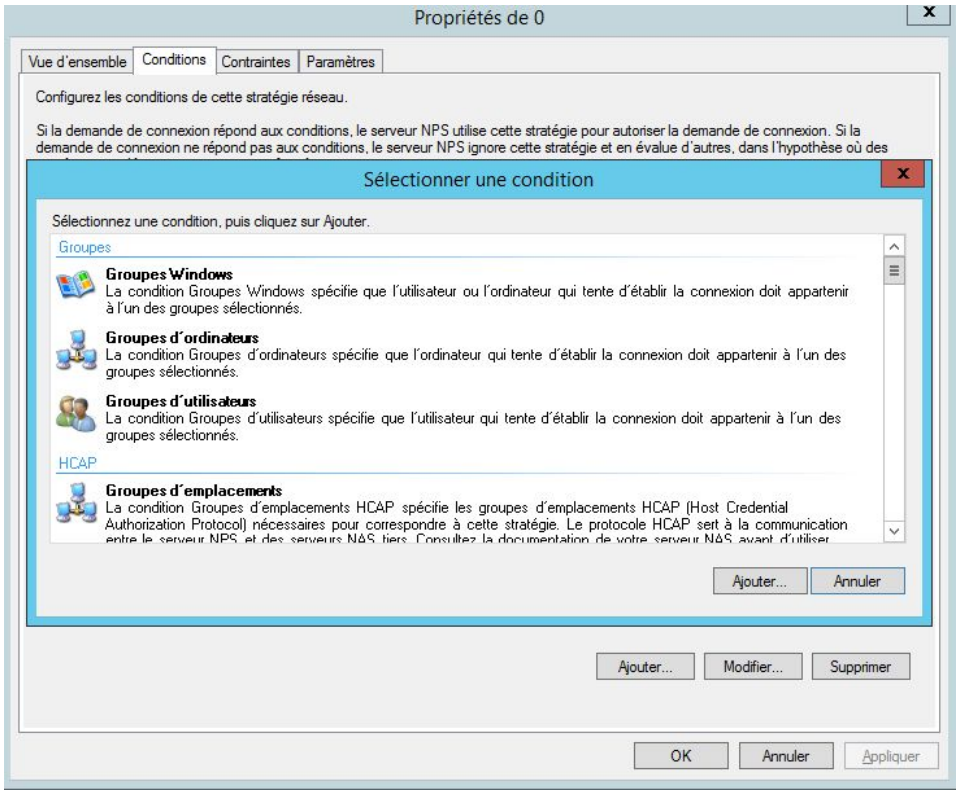
Après l'avoir installé, j'ai ainsi créer une étendue réservée au serveur Radius, ainsi, chaque appareil qui se connectera au point d'accès recevera une adresse ip entre "10.1.42.65" et "10.1.42.80".

Maintenant que tous les composants était prêt, j'ai du configurer une stratégie Radius, qui ressemble au filtrage mac/ip.



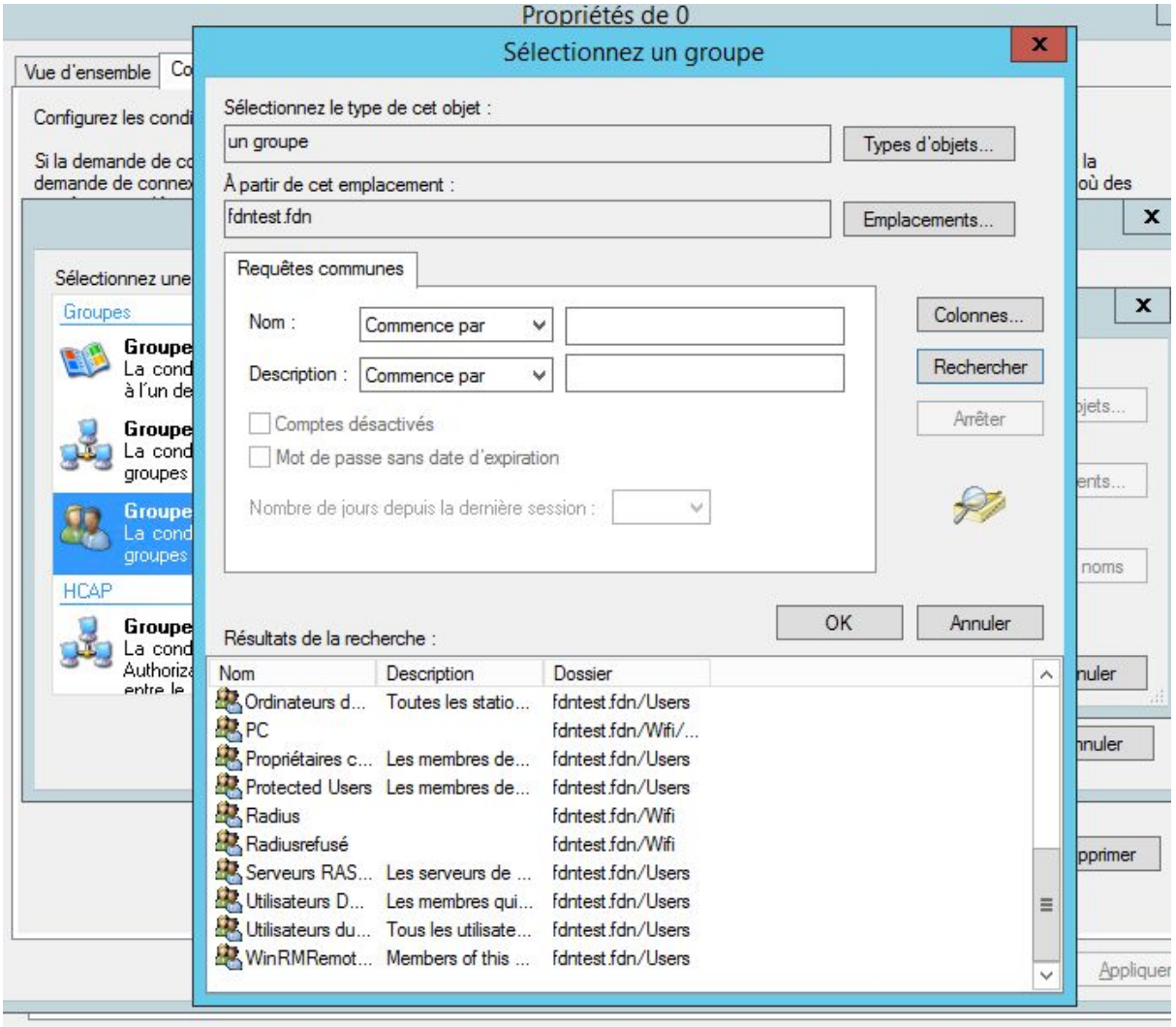


On y choisit donc un nom pour la stratégie, le fait d'accorder ou de refuser l'accès.



On y choisit ensuite le type de filtrage, les principaux modes de filtrage sont donc "Groupe Windows", "Groupes d'ordinateurs" et 'Groupes d'utilisateurs".

Ici, on choisira Groupes Windows, qui est un mélange des deux autres, ainsi l'authentification se fera par l'ordinateur et par les identifiants.



On y choisit ensuite quels groupes ou quels utilisateurs à intégrer dans la règle. Evidemment, il faut que ces derniers soient inscrits dans le domaine.

Après avoir fini l'installation de ces composants, j'ai décidé de faire des tests avec l'ordinateur portable. Ainsi, en mettant l'ordinateur portable sur le domaine concerné et en se connectant à la session avec "User1", la connexion au PA m'était refusé sans même une demande d'authentification avec un message "Windows n'a pas pu se connecter au réseau".

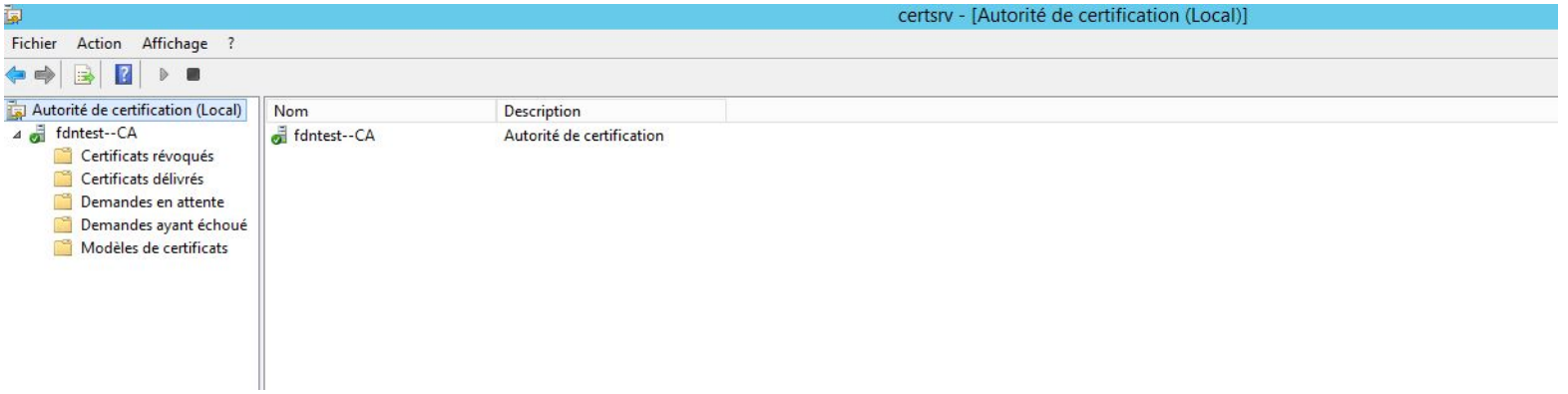
Ne sachant pas comment résoudre ce problème, je me tourne vers mon maître de stage qui me conseille de regarder les log d'erreurs du point d'accès (voir annexe)

J'y découvre alors trois erreurs :

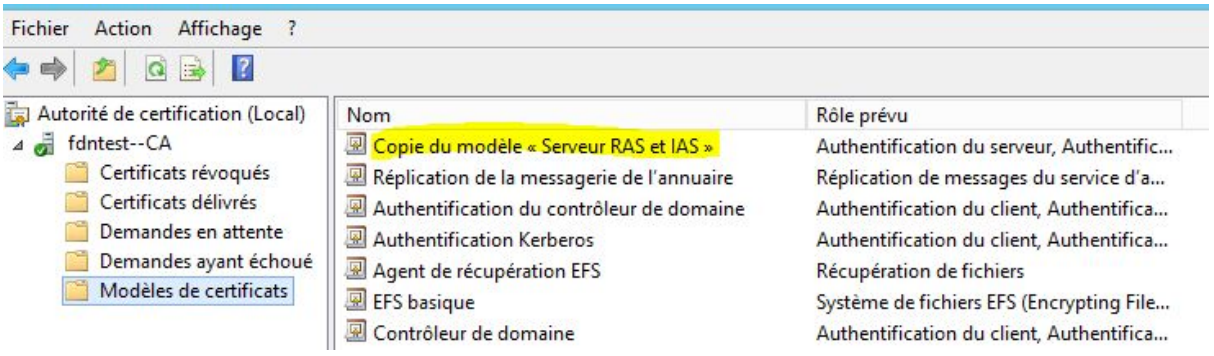
- Erreur n°8
- Erreur n°23
- Erreur n°1

En me renseignant sur internet, je découvre que ce problème interviendrait entre le PA et le serveur Radius et que la solution tournerait autour des certificats windows.

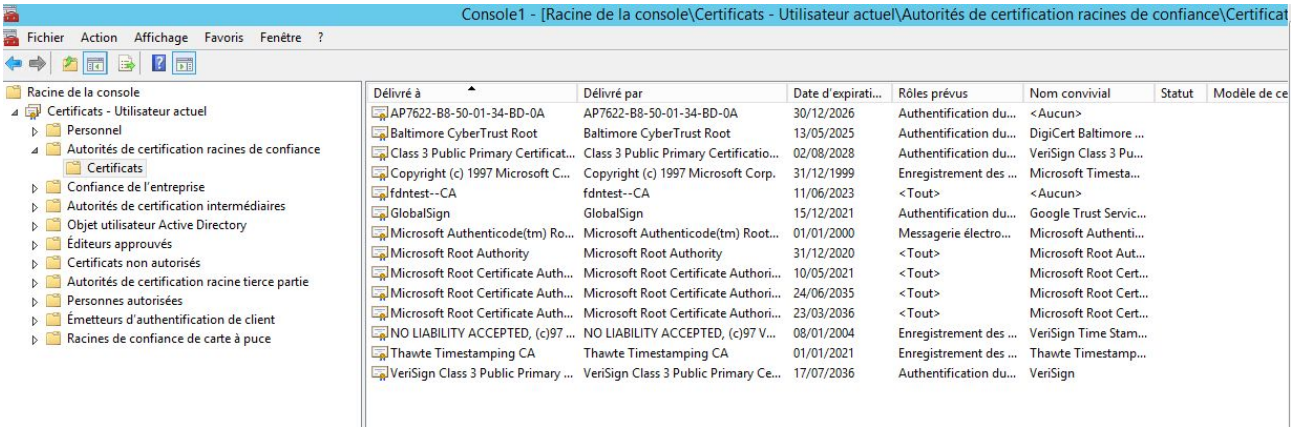
Alors, j'ai créer une Autorité de Certification :



Puis j'ai créer un certificat depuis le modèle de certificat "Serveur RAS et IAS".



Enfin, j'ai appliqué ce certificat dans les "Autorités de certifications racines de confiance" afin qu'il soit reconnu par tous les composants du serveur. Il faut ensuite l'exporter, ce qui nous donne un .exe et l'installer sur chaque poste désirant se connecter au point d'accès.



Une fois le certificat installé sur l'ordinateur, ou même sur mon téléphone, il suffit de rentrer des identifiants dont on a accordé l'accès lors de la stratégie pour se connecter au réseau.

Ainsi, une fois le certificat installé, le serveur Radius est opérationnel.

Mails échangés avec le responsable informatique :

Aziz TALBO <atalbo@furet.com>
À moi

Bonjour Denis,

J'espère tout va bien pour toi ?

J'ai un petit problème avec le serveur 2012, je ne me rappel plus du mot de passe ?
Et je ne veux pas le réinstaller avant de revoir ce que tu as fait.
Tu peux me l'envoyer ?

Merci

Denis ARDOUIN <denis.ardouin.avron@gmail.com>
À DEV

Bonjour Monsieur TALBO,

Pour ma part je vais bien, j'espère que vous et tout le service également.

De ce que je me souviens, le mot de passe est soit 123fdn / fdn123 soit Denis11.

Si ce n'est pas ça, veuillez m'excuser mais je n'arrive pas à m'en rappeler.

Cordialement, Denis ARDOUIN.

Aziz TALBO <atalbo@furet.com>
À moi

Merci Denis,

J'ai trouvé par contre c'est celui du boitier Wifi que je n'arrive pas à trouver.

Cdt,