

TUTORIEL RADIUS

Dans ce tutoriel nous allons voir, comment mettre en place une borne wifi avec un protocole RADIUS. Pour cela, vous aurez besoin :

- d'un serveur Windows 2012
- d'un Active Directory
- d'une borne wifi (D-Link dans notre cas).

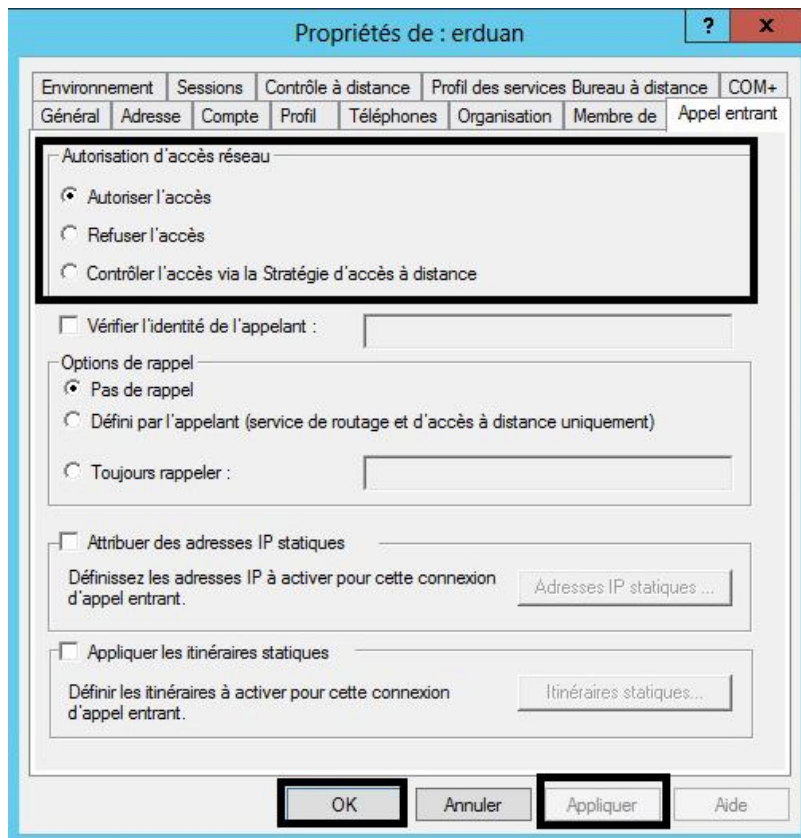
I. Qu'est-ce que RADIUS ?

RADIUS (Remote Authentication Dial-In User Service) est un protocole client-serveur permettant de centraliser des données d'authentification. Le protocole RADIUS permet de faire la liaison entre des besoins d'identification et une base d'utilisateurs en assurant le transport des données d'authentification de façon normalisée.

L'opération d'authentification est initiée par un client du service RADIUS, qui peut être un boîtier d'accès distant (NAS : Network Access Server), un point d'accès réseau sans fil, un pare-feu (firewall), un commutateur, un autre serveur. Le serveur la traite en accédant si nécessaire à une base externe : base de données SQL, annuaire LDAP, comptes d'utilisateur de machine ou de domaine ; un serveur Radius dispose pour cela d'un certain nombre d'interfaces ou méthodes.

II. Création d'un groupe et d'utilisateur

Pour commencer il faut créer un groupe de travail dans l'active directory et un utilisateur. Lorsque l'utilisateur est créé il faut faire un clic droit, propriété sur l'utilisateur et accorder l'accès au réseau, de cette façon :



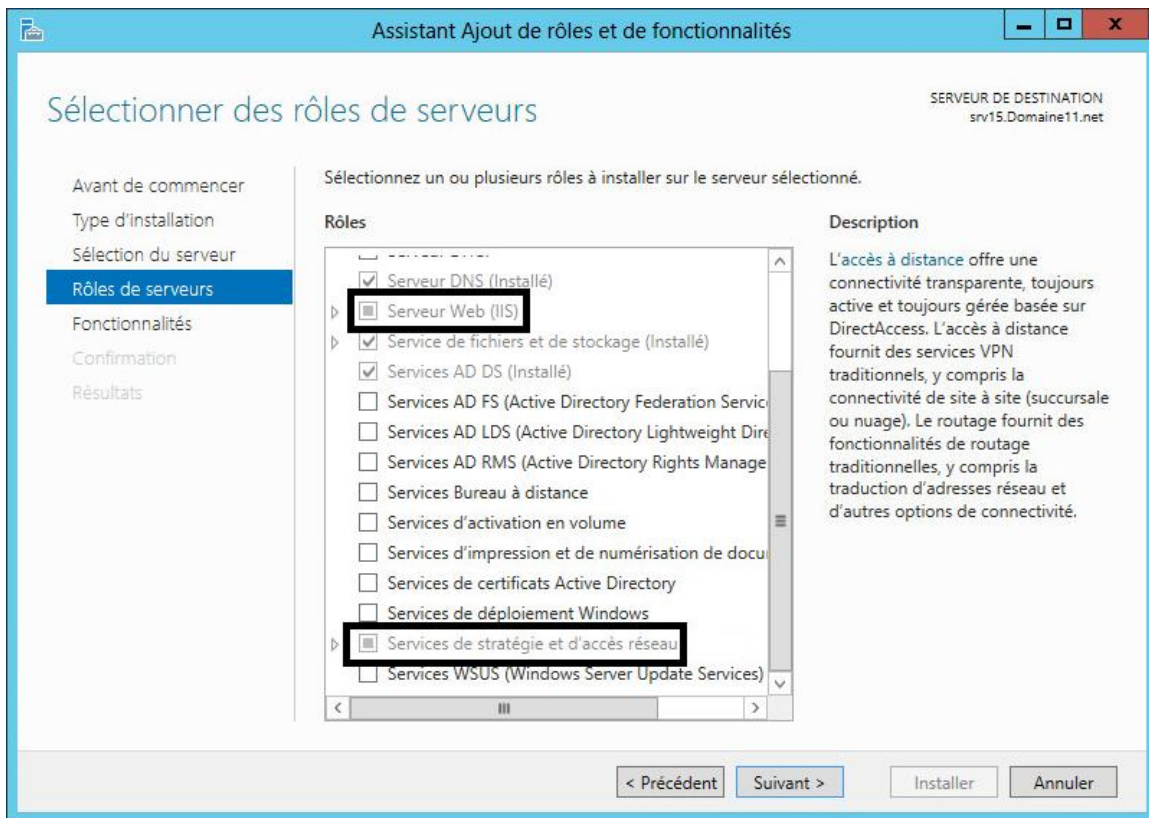
III. Mise en place du serveur RADIUS

Network Policy Server (NPS) peut être utilisé comme serveur RADIUS afin d'effectuer l'authentification, l'autorisation et la gestion des clients RADIUS.

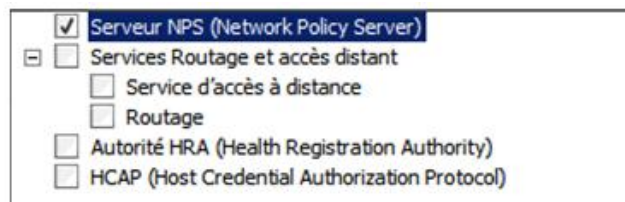
NPS utilise un domaine AD DS pour l'authentification des informations d'identification utilisateur des messages de demande d'accès RADIUS entrants.

Il est nécessaire d'installer le rôle IIS afin d'obtenir un certificat pour que le serveur puisse répondre au requête RADIUS, nous allons donc installer le rôle Services de Stratégie d'Accès Réseau et IIS.

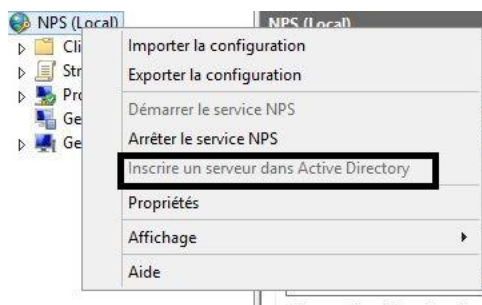
Dans « Gérer » choisissez « Ajouter des rôles et fonctionnalité » et sélectionnez les rôles correspondant :



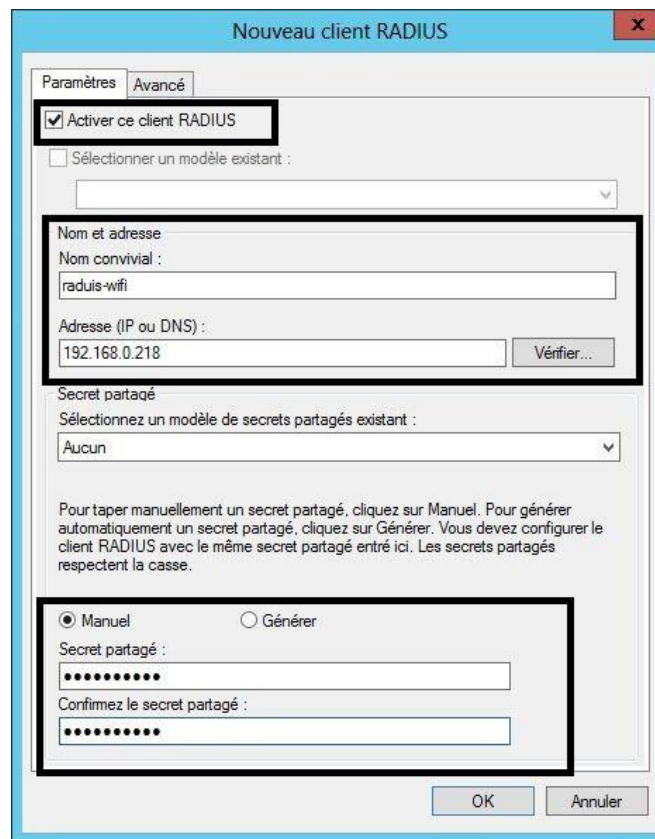
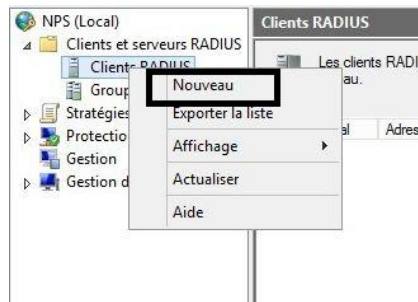
Pour les services de Rôle IIS laissez tous par défaut, du moins pour la présentation actuel, si vous avez besoin d'autres services sélectionnez les, le certificat dans le rôle IIS est intégré de base, c'est une fonctionnalité obligatoire. Pour le NPS sélectionnez « Serveur NPS»



Maintenant que le serveur NPS est installé, rendez-vous sur l'interface de ce serveur et joignez-le à l'Active Directory :

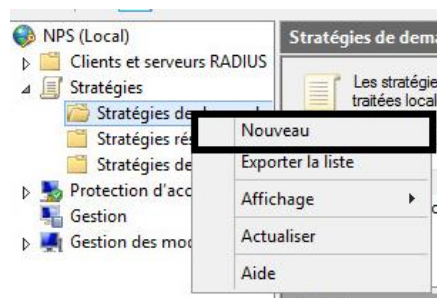


Crée un nouveau client RADIUS et saisir les informations nécessaires : nom convivial, adresse IP du serveur et le secret partagé :



Puis valider en cliquant sur OK.

Ensuite, vous devez créer une stratégie de demande de connexion :



Donnez un nom à la stratégie (« wifi » dans notre cas) :

Nouvelle stratégie de demande de connexion

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

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

Nom de la stratégie :

wifi

Méthode de connexion réseau

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

Type de serveur d'accès réseau :

Non spécifié

Spécifique au fournisseur :

10

Précédent Suivant Terminer Annuler

Vous devez rajouter des conditions : - le nom d'utilisateur (Erduan dans notre cas)
- le type de port (sans fil)

Sélectionner une condition

Sélectionnez une condition, puis cliquez sur Ajouter.

HCAP

Groupes d'emplacements
La condition Groupes d'emplacements HCAP spécifie les groupes d'emplacements HCAP (Host Credential Authorization Protocol) nécessaires pour correspondre à cette stratégie. Le protocole HCAP sert à la communication entre le serveur NPS et des serveurs NAS tiers. Consultez la documentation de votre serveur NAS avant d'utiliser cette condition.

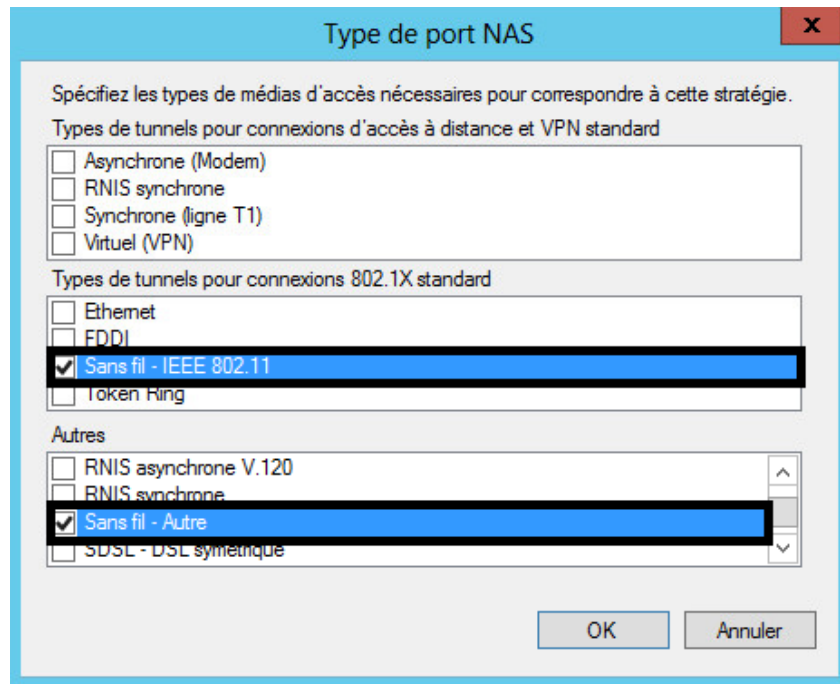
Nom d'utilisateur
Nom d'utilisateur employé par le client d'accès à distance dans le message RADIUS. Cet attribut est une chaîne de caractères qui contient généralement un nom de domaine et un nom de compte d'utilisateur.

Propriétés de la connexion

Adresse IPv4 du client d'accès
La condition d'adresse IPv4 du client d'accès spécifie l'adresse IPv4 du client d'accès qui demande l'accès à partir du client RADIUS.

Ajouter... Annuler

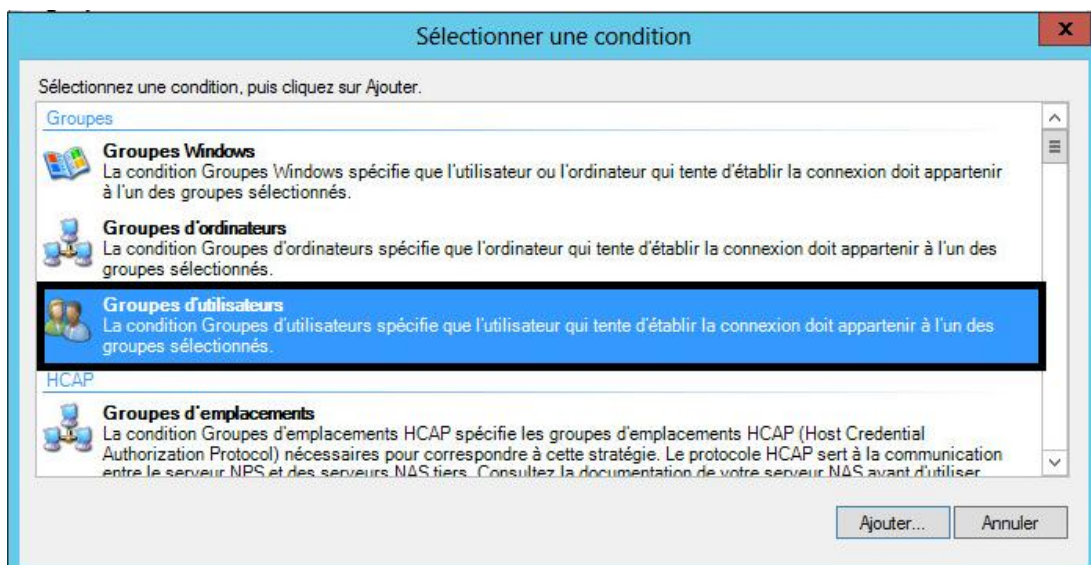
Veillez cocher ces cases pour le type de port NAS :



Puis laisser les autres paramètres par défaut et « Suivant ».

Il faut à présent créer une stratégie de réseau possédant le même nom que la stratégie précédemment créée (« wifi » dans notre cas) et rajouter les conditions suivantes :

- les groupes d'utilisateurs (bts dans notre cas)
- le type de port (avec les mêmes types de port qu'au dessus)



Puis, il faut bien évidemment accordé l'accès :

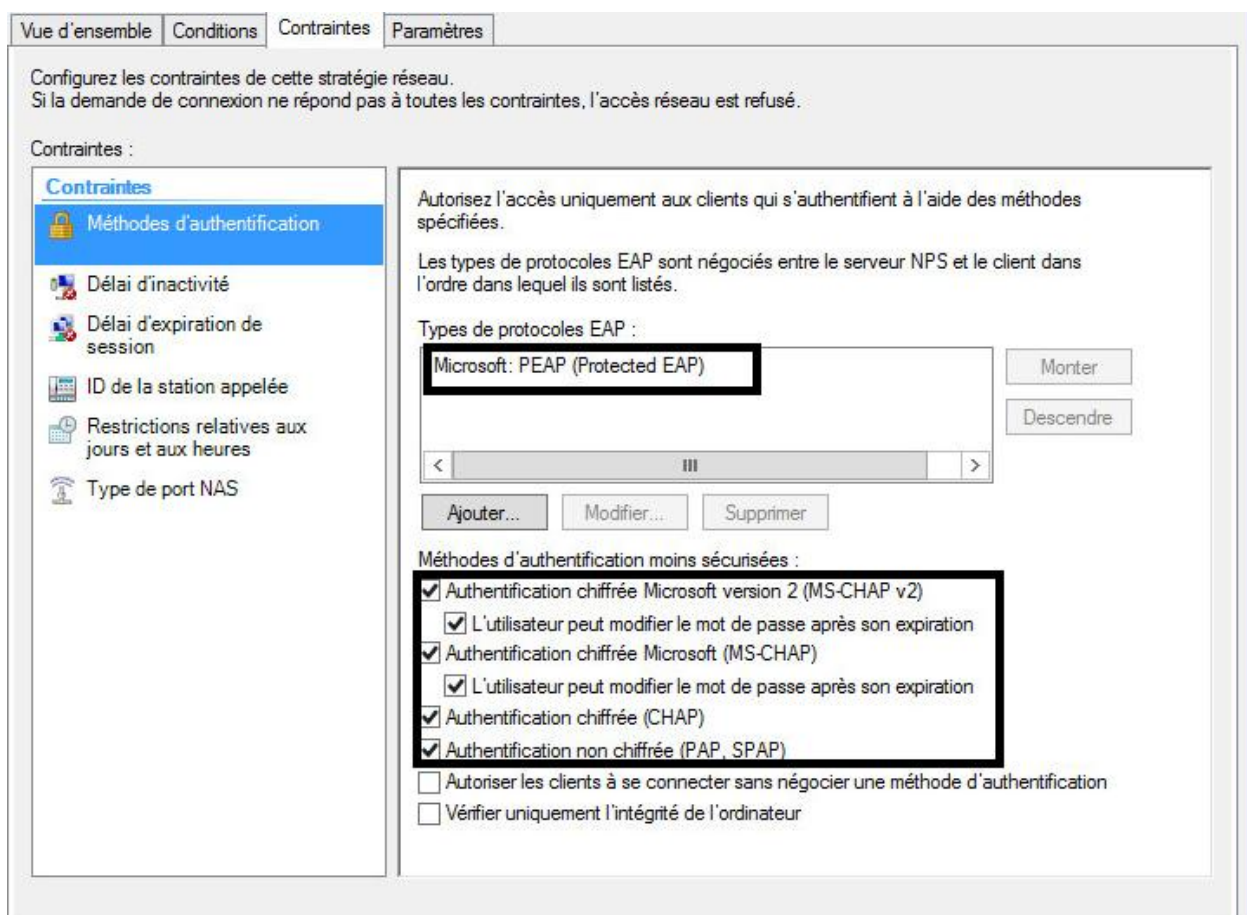


Spécifier l'autorisation d'accès

Effectuez la configuration nécessaire pour accorder ou refuser l'accès réseau si la demande de connexion correspond à cette stratégie.

Accès accordé
Accordez l'accès si les tentatives de connexion des clients répondent aux conditions de cette stratégie.

Concernant les méthodes d'authentification, il faut ajouter le protocole EAP et cocher les cases suivantes :



Vue d'ensemble Conditions Contraintes Paramètres

Configurez les contraintes de cette stratégie réseau.
Si la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé.

Contraintes :

Contraintes

- Méthodes d'authentification
- Délai d'inactivité
- Délai d'expiration de session
- ID de la station appelée
- Restrictions relatives aux jours et aux heures
- Type de port NAS

Autorisez l'accès uniquement aux clients qui s'authentifient à l'aide des méthodes spécifiées.

Les types de protocoles EAP sont négociés entre le serveur NPS et le client dans l'ordre dans lequel ils sont listés.

Types de protocoles EAP :

Microsoft: PEAP (Protected EAP) [Monter] [Descendre]

[Ajouter...] [Modifier...] [Supprimer]

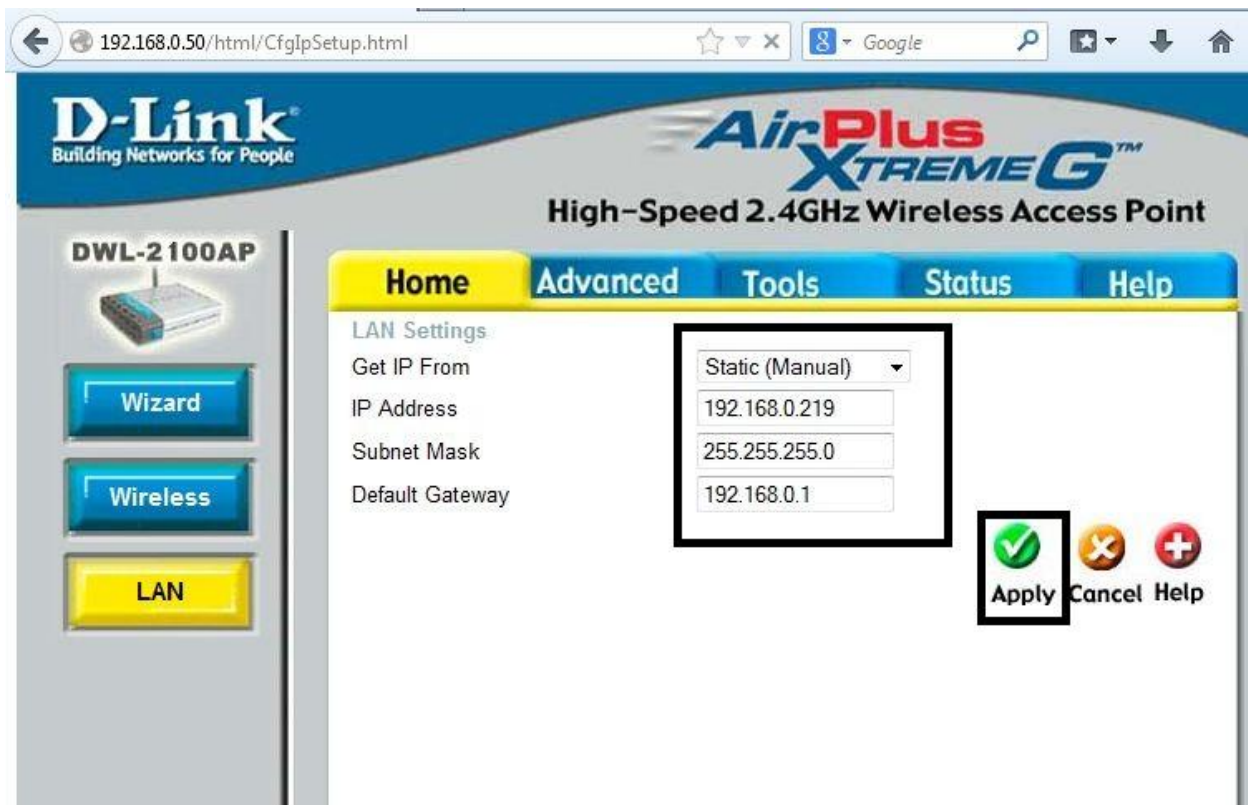
Méthodes d'authentification moins sécurisées :

- Authentification chiffrée Microsoft version 2 (MS-CHAP v2)
 - L'utilisateur peut modifier le mot de passe après son expiration
- Authentification chiffrée Microsoft (MS-CHAP)
 - L'utilisateur peut modifier le mot de passe après son expiration
- Authentification chiffrée (CHAP)
- Authentification non chiffrée (PAP, SPAP)
- Autoriser les clients à se connecter sans négocier une méthode d'authentification
- Vérifier uniquement l'intégrité de l'ordinateur

Vous devez laisser les paramètres suivants par défaut, et valider la stratégie.

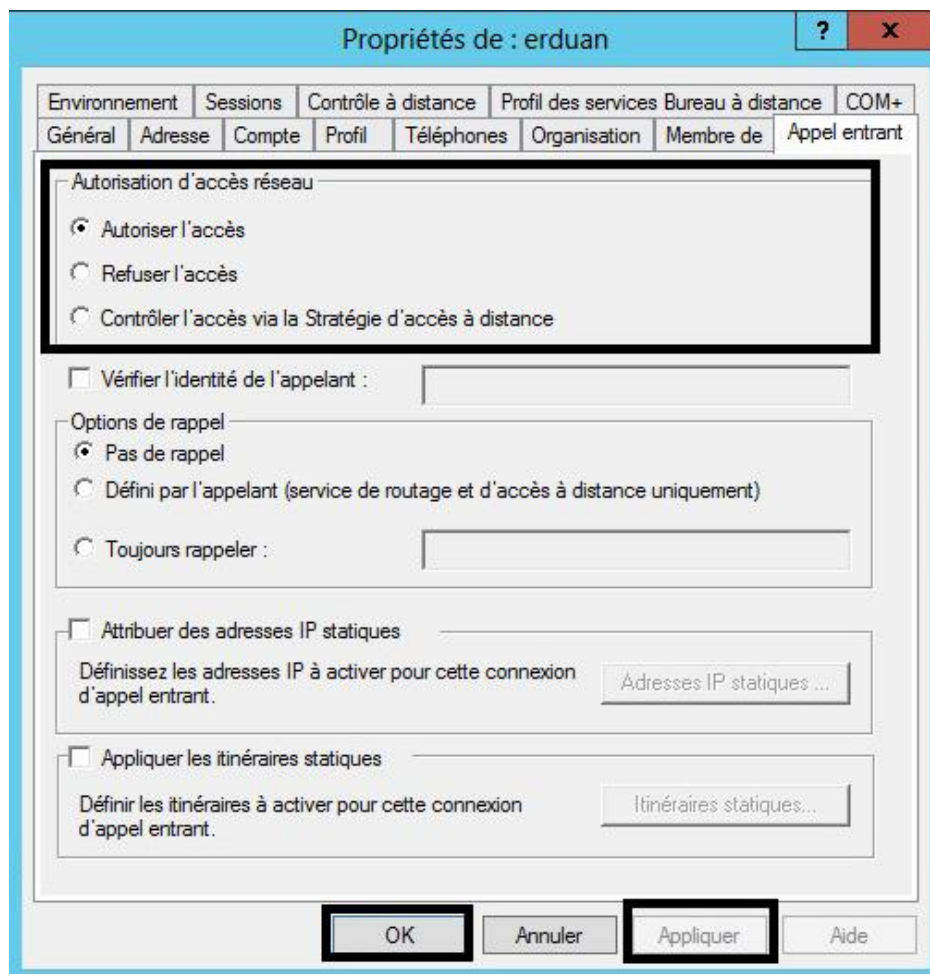
IV. Configuration de la borne wifi

Maintenant que le serveur RADIUS est configuré sur le Windows SERVER 2012, il est nécessaire de configurer la borne wifi. Ouvrez votre navigateur et entré l'adresse IP de la borne (dans notre l'adresse IP par défaut est 192.168.0.50). Vous devez vous rendre dans le menu du LAN à gauche et modifier l'IP de la borne :



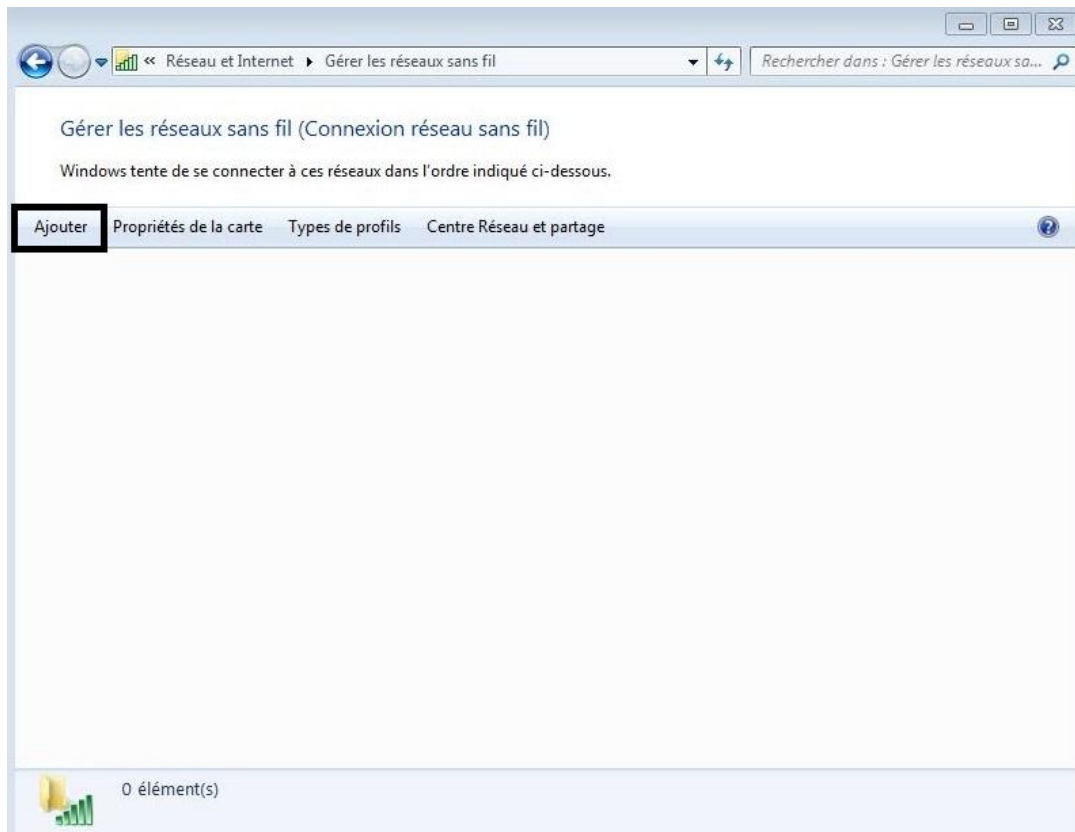
Puis, vous devez aller dans le menu Wireless à gauche et modifier les informations de façon à obtenir ce type de configuration :

- Authentication: WP2-EAP
- RADIUS Server : l'adresse IP du serveur (192.168.0.161 dans notre cas)
- RADIUS Port : port par défaut (1812)
- RADIUS Secret : le secret partagé crée dans le serveur NPS

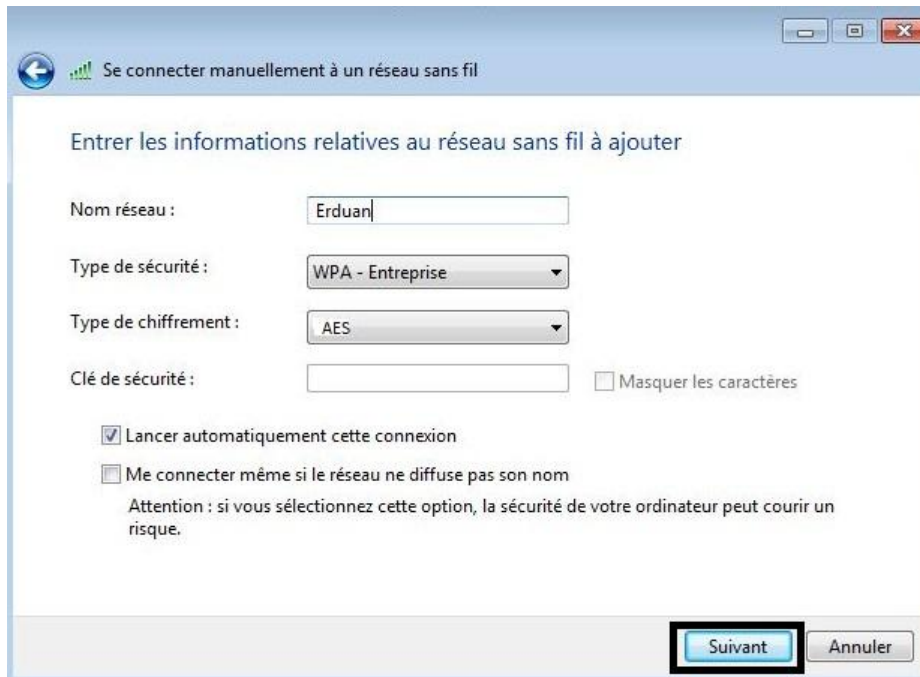


V. Joindre le réseau WIFI

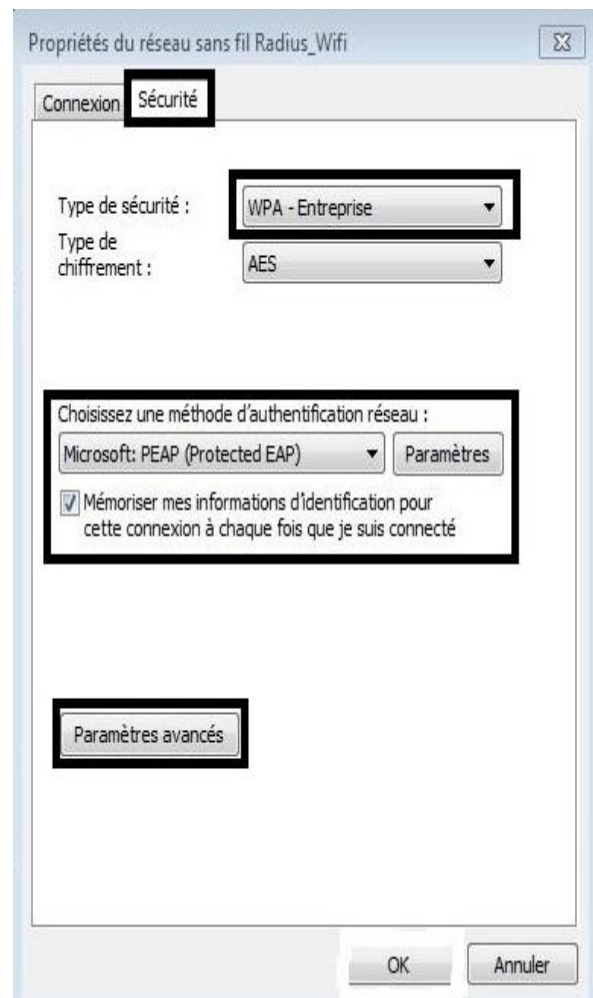
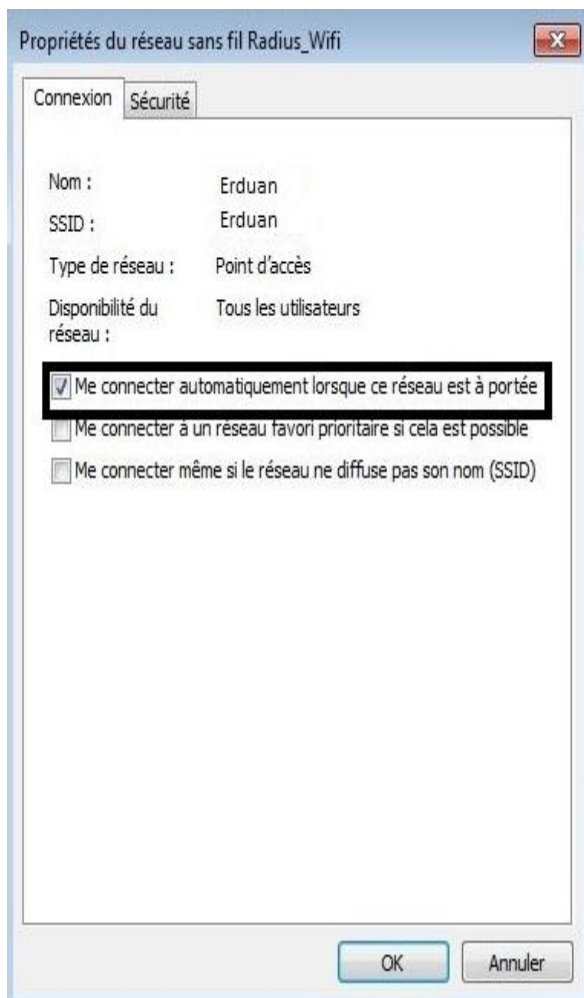
Pour pouvoir joindre le réseau wifi, il est nécessaire de faire quelques modifications. Allez dans Panneau de configuration, puis Réseau et Internet, Gérer les réseaux sans fil et cliquer sur Ajouter (pour ajouter un réseau sans fil) :



Puis Créer un profil réseau manuellement et entrez les informations nécessaires (nom réseau, type de sécurité, type de chiffrement et la clé de sécurité).

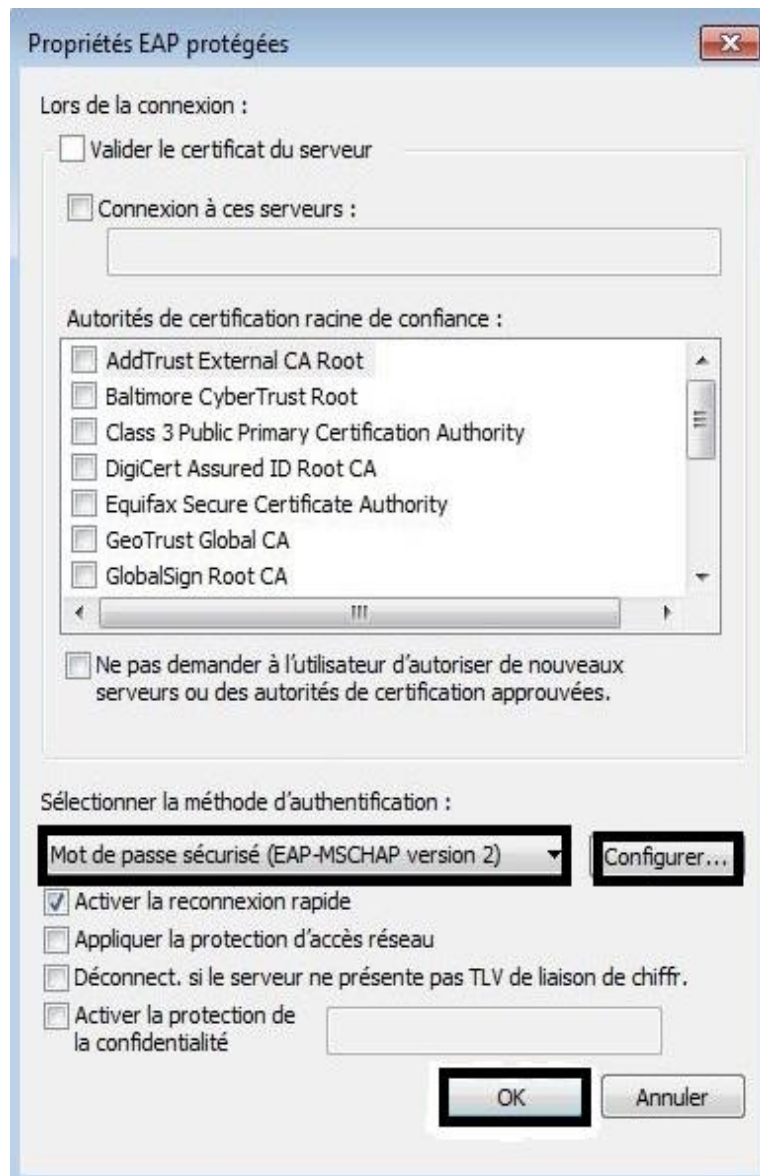


Lorsque les informations sont entrées, il est nécessaire de modifier les paramètres de connexion :



Dans l'onglet Sécurité de la fenêtre « Propriétés du réseau sans fil ... », vous devez vous rendre dans Paramètres (pour la méthode d'authentification réseau).

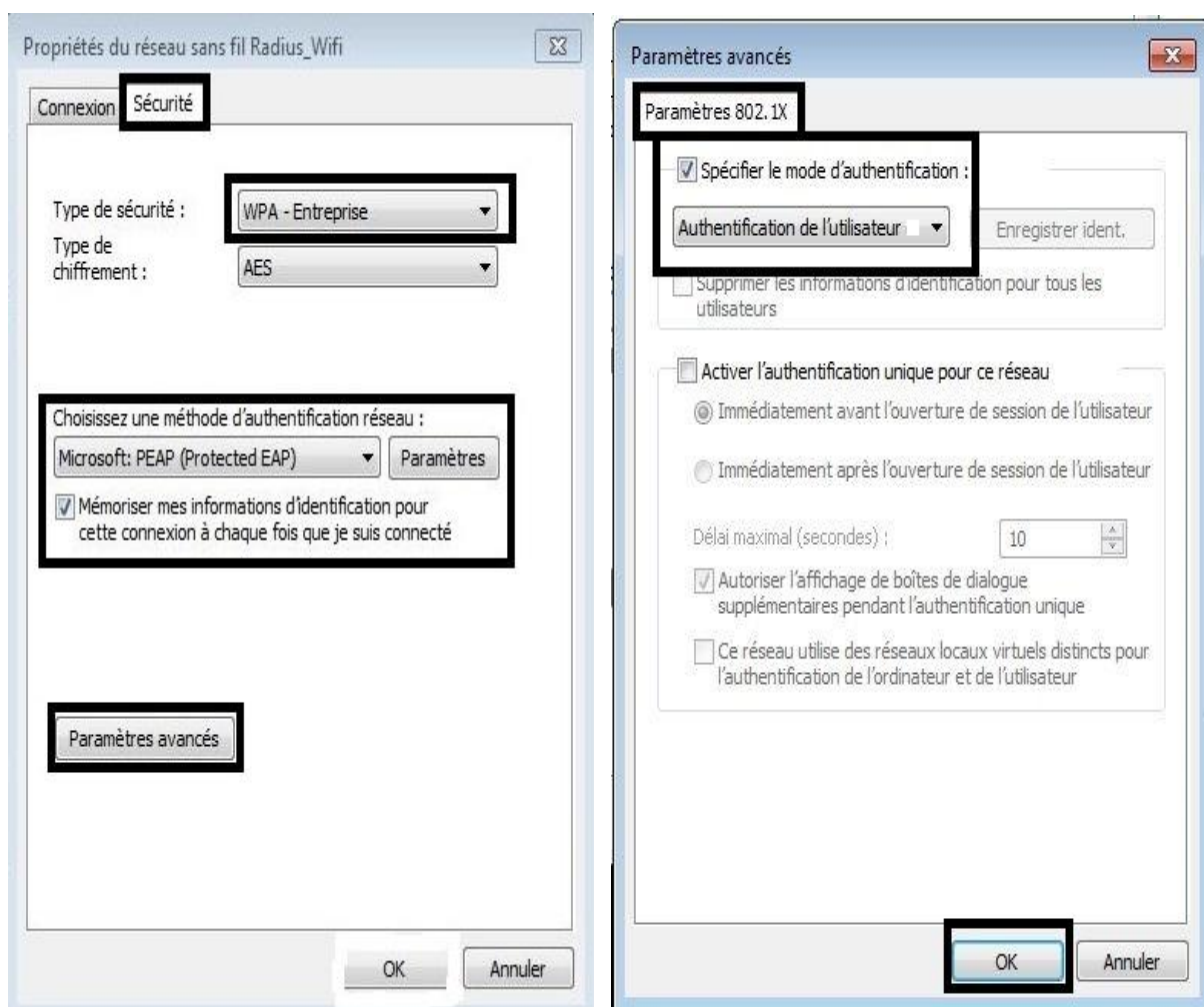
Une nouvelle fenêtre fait son apparition, vous devez alors décocher la case « Valider le certificat du serveur » (cocher par défaut) et sélectionner la méthode d'authentification : Mot de passe sécurisé (EAP-MSCHAP version 2) :



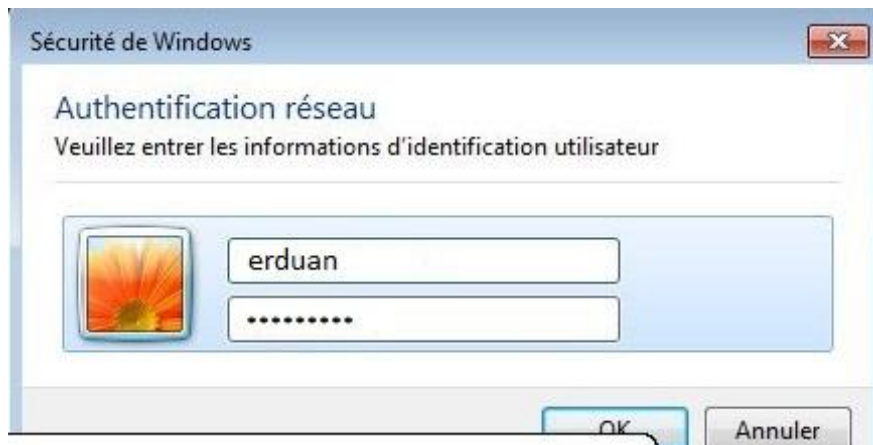
Ensuite cliquer sur Configurer et décocher la case « Utiliser automatiquement mon nom et mon mot de passe Windows ... » puis OK et enfin revenez sur la fenêtre « Propriétés du réseau sans fil ... » :



Rendez vous maintenant dans « Paramètres avancés », une nouvelle fenêtre s'ouvre, cocher « Spécifier le mode d'authentification » et choisissez « Authentification de l'utilisateur » :



Enfin Windows vous demande une authentification, c'est à ce moment qu'il faut entrer les données de l'utilisateur créé auparavant (l'utilisateur erduan dans notre cas) :



Vous êtes désormais connecter à la borne wifi Erduan avec le protocole RADIUS :

