Objet :	**WIFI sécurisé en entreprise (sur un Active Directory 2008)**	Date : Version :	**02/05/2012 2.0**

Objectif de ce document : montrer *comment un point d'accès Wifi peut être mis en œuvre sur un active directory 2008, avec une authentification sécurisée qui s'appuie sur les comptes utilisateurs de l'AD.*
Les postes W7 ou XP se connectent alors de manière transparente avec leur login et mot de passe Windows (si le portable appartient au domaine Windows, sinon cela marche aussi)

0 - Théories et principes divers sélectionnés

Quelques normes :

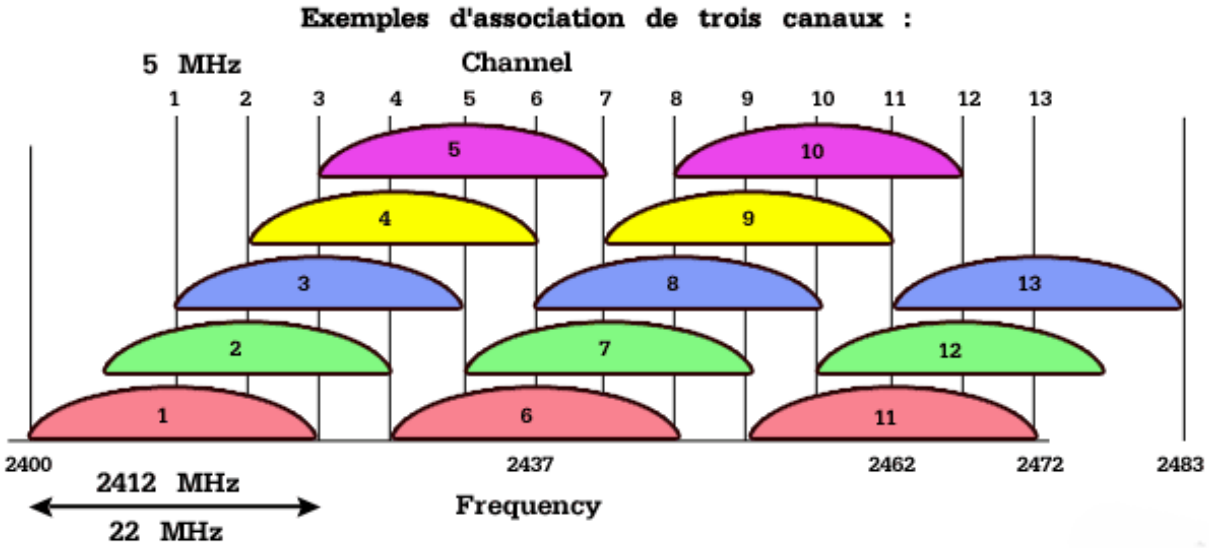
802.11 : ensemble de normes qui couvre les connexions à un réseau local sans-fils (appelé WLAN) dont

- 802.11b : norme Wifi avec débit maximum à 11 Mb/s
- 802.11g : norme Wifi avec débit maximum à 54 Mb/s
- 802.11n : norme Wifi prévue pour 2008 avec débit maximum à 540 Mb/s

Ces normes permettent une connexion sans fil sur une couverture théorique de 25 m à 125m , selon les conditions physiques des bâtiments. Les débits annoncés sont maximales, et dépendent également de la distance ainsi que du nombre de clients connectés sur le point d'accès Wifi.

Ondes & signaux :

Le Wifi fonctionne sur la bande de fréquence des 2.4 Ghz sur 13 canaux (pour l'Europe). Chaque canal correspond à une fréquence différente (canal 1 = 2.412 Ghz, canal 13 = 2.472 Ghz).
Si plusieurs point d'accès Wifi sont installés dans votre entreprise, assurez-vous que les canaux utilisés ne se recouvrent pas ; cela revient à laisser 3 canaux vides entre 2 points d'accès. Par exemple : canaux 1, 5, 9, 13 voire un espacement plus large en 802.11b : 1, 6, 11



Modes de connexion :

Il existe deux manières d'utiliser un réseau WIFI :

- réseau **AdHoc** : lorsque deux ordinateurs équipés de cartes Wifi se connectent l'un à l'autre
- réseau **Infrastructure** : lorsqu'un ou plusieurs ordinateurs se connectent à un point d'accès (qui centralise les connexions). Ce point d'accès est l'équipement qui fournira l'accès au réseau local de l'entreprise. C'est cette dernière forme de connexion qui nous intéresse.

Authentifications & Cryptages :

Comme toujours quand une technologie novatrice sort : les soucis de confidentialité ou de protection sont quasi-inexistant sur les premiers points d'accès Wifi tant au point de vue de l'authentification que sur celui du cryptage. N'importe qui pouvait alors se connecter à un point d'accès, puis accéder aux ressources réseau via le Point d'Accès, il était également

facile de capturer les paquets transmis en Wifi et de les lire (ceux-ci circulant en clair).

Une première protection illusoire a été proposée pour le cryptage des données : WEP. Encore trop répandue, cette solution WEP est à proscrire… Tous les outils existent sur internet pour capturer un trafic Wifi, et le décoder. Le plus dur étant de trouver la carte Wifi compatible.

La seconde protection : WPA (chiffrement basé sur RC4) mais qui a déjà fait l'objet de vulnérabilités démontrées et plus récemment WPA2 normalisé qui reste encore « sûr » lorsqu'il est employé avec le chiffrage AES.

En plus des différents cryptages possibles ci-dessus, nous aurons 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.

Dans notre cas : c'est **WPA2** et **PEAP** qui seront utilisés afin d'assurer un minimum de protection sur l'authentification des utilisateurs sur le point d'accès et de réduire les possibilités de décryptage des données circulant entre le PA et le client.

Dernières remarques avant de démarrer : les explications fournies ici ne tiennent pas compte d'un renforcement possible du niveau de sécurité par utilisation de VLAN, authentification MAC (pourquoi pas), accès en DMZ via un parefeu, la sécurisation via GPO des stratégies réseau, la mise en Quarantaine des postes distants,…

L'environnement décrit pour la connexion Wifi nécessite (nécessitera) les équipements suivants :

- ActiveDirectory 2008 (déjà configuré)
- Serveur DHCP (pour ce cas d'école, on fera en sorte que ce soit ce serveur DHCP qui configure l'IP des postes Wifi client)
- Une autorité de certification (soit en mode Entreprise, soit en mode Autonome)

- Point d'accès Wifi supportant **WPA2 avec Radius** et cryptage **AES** . Ce point d'accès doit connaître l'adresse IP du serveur Radius Windows 2008 ainsi que la presharedkey ce dernier.

- Un poste avec carte Wifi

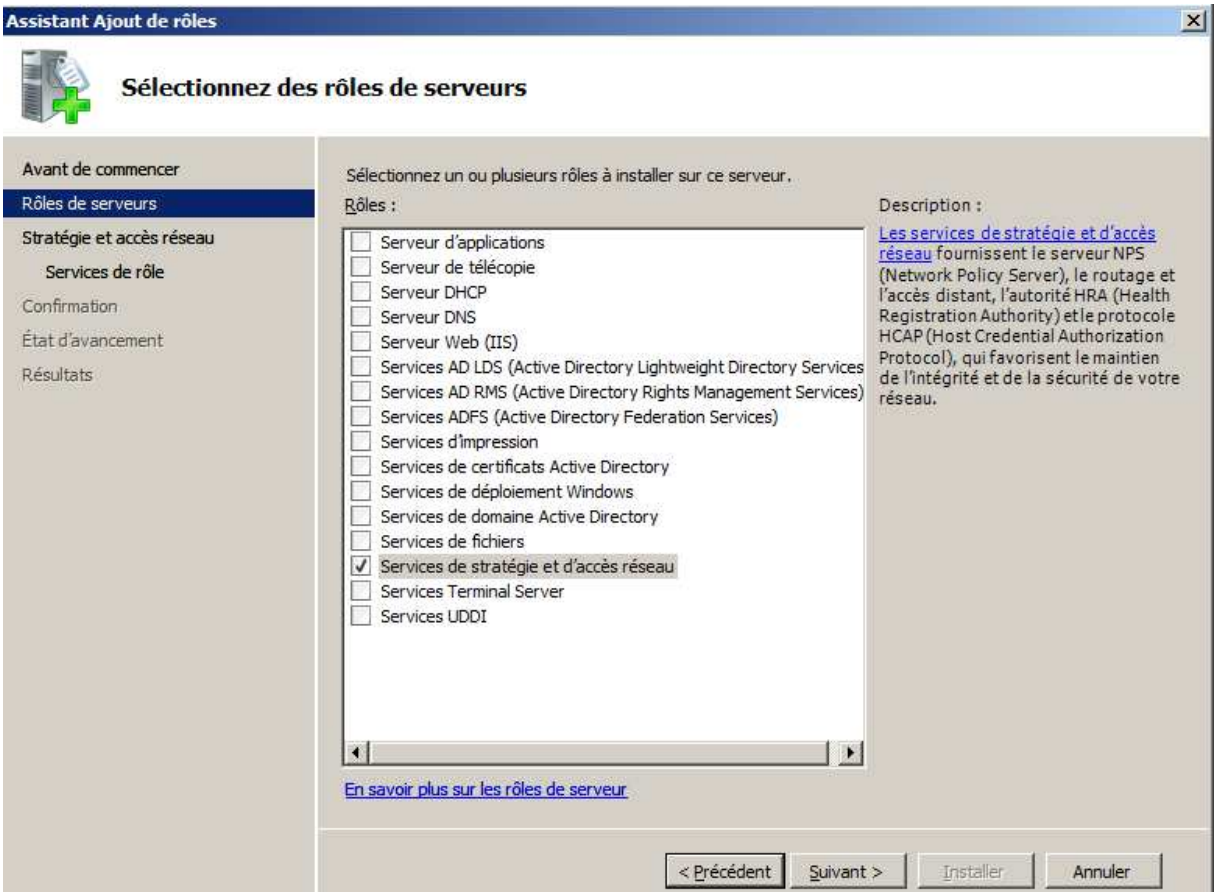
1 – Préparation de l'environnement Windows – ActiveDirectory

Les utilisateurs qui pourront se connecter via Wifi devront faire partie d'un groupe *global* d'utilisateur définit (par exemple : WIFI-LAN) et seul les membres de ce groupe pourront s'authentifier sur les PA Wifi.

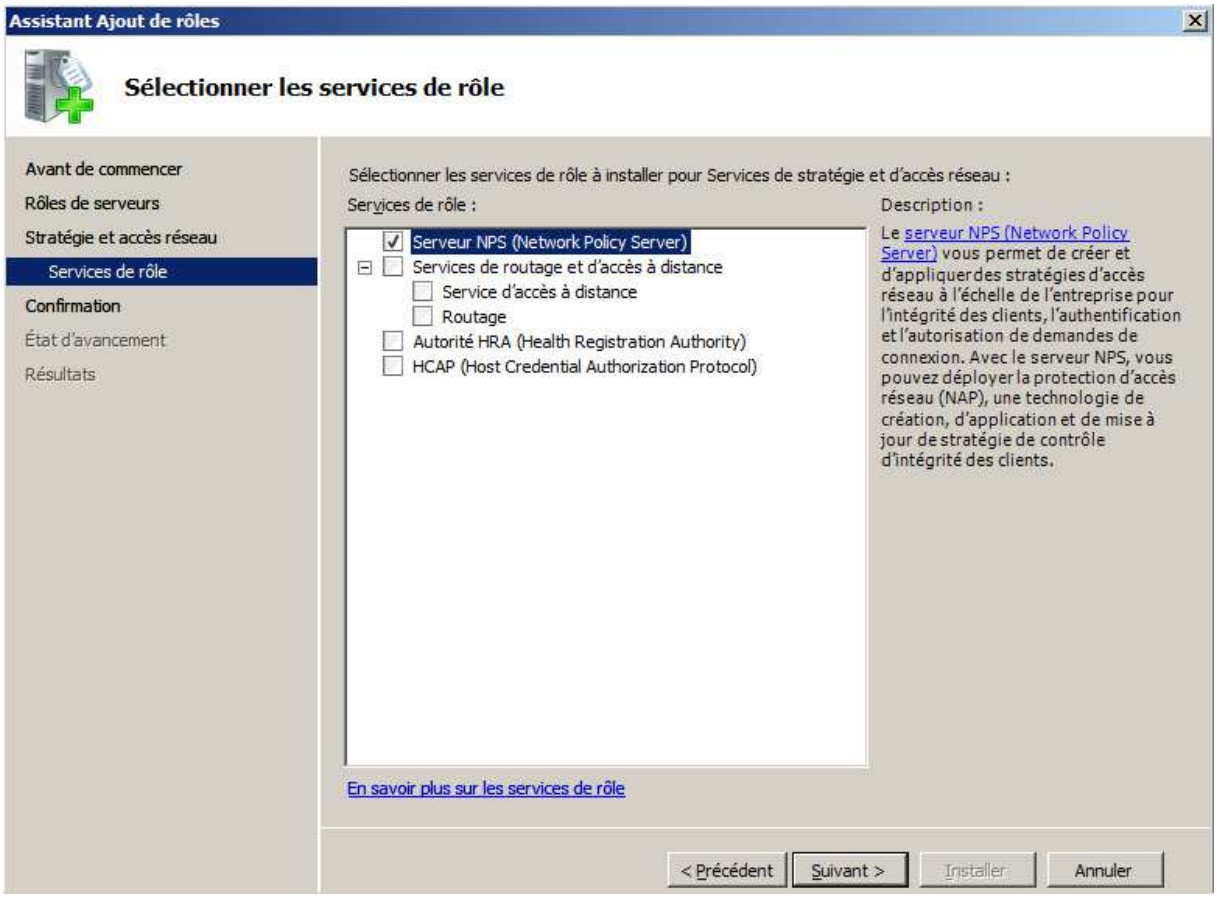
2 – Installation du serveur Radius

Sur le serveur, ajoutez le rôle Radius sous Windows 2008 qui se nomme Network Policy Server , NPS qui remplace l'IAS de Windows 2003.

Sélectionnez **Services de stratégie et d'accès réseau**



puis cochez **Serveur NPS**

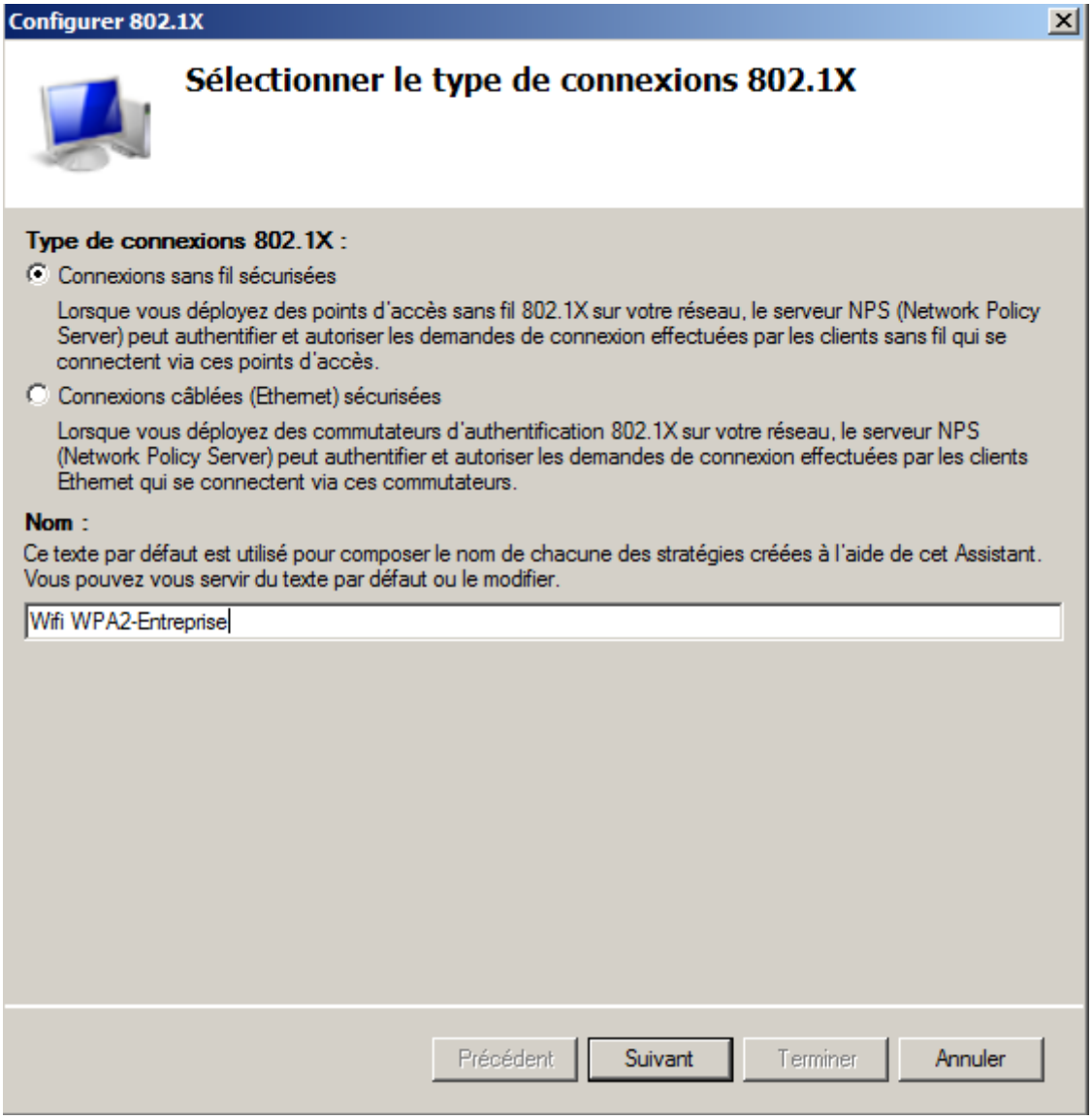


Pas de redémarrage nécessaire.
Une nouvelle icône est ajoutée dans les outils d'administration :

3 – Configuration du Serveur Radius

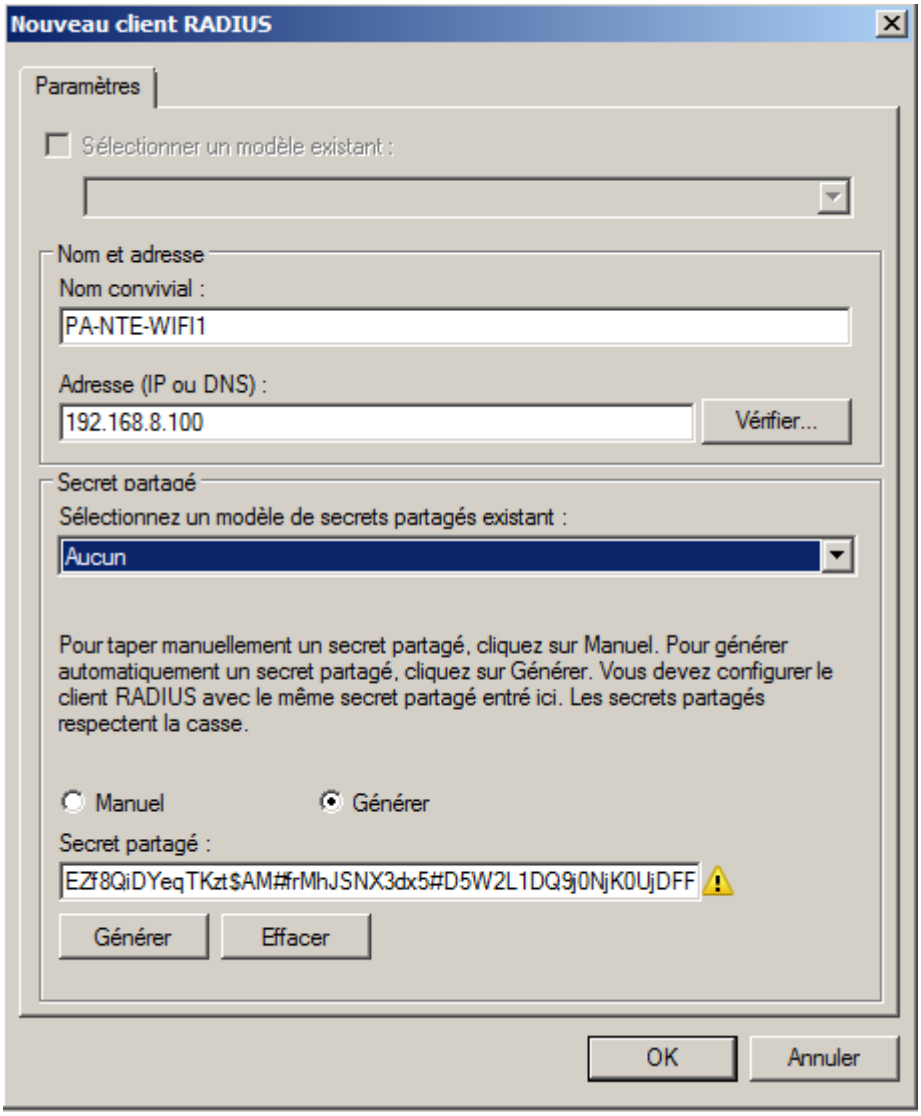
Dans l'interface d'administration, commencez par sélectionner « Serveur RADIUS pour les connexions sans fil ou 802.1X ».

Cliquez ensuite sur « Configurer 802.1X »



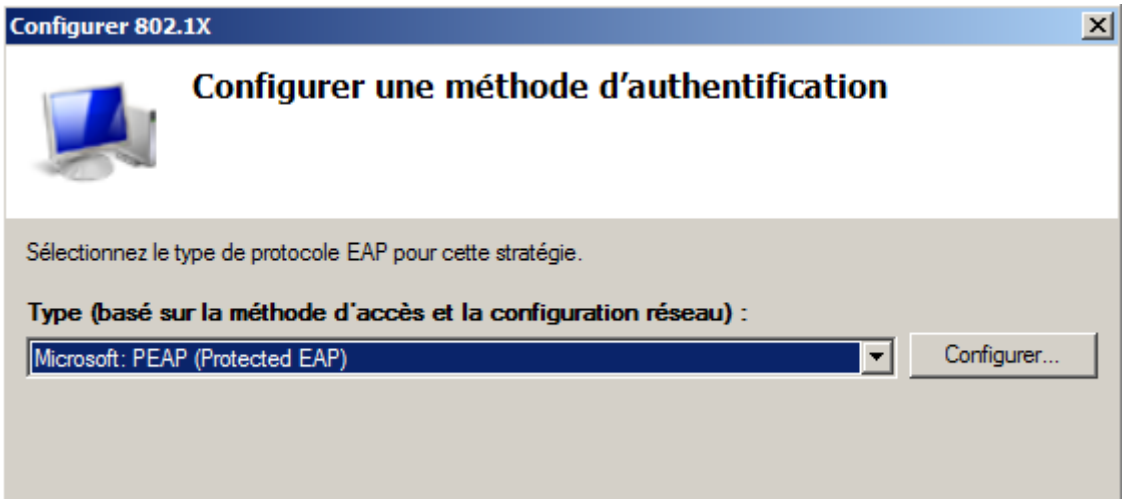
Sélectionnez Connexions sans fil sécurisées et donnez lui un nom.

L'étape suivante consiste à déclarer un client RADIUS qui sera autorisé à s'authentifier via NPS. Ce client RADIUS sera la borne Wifi.

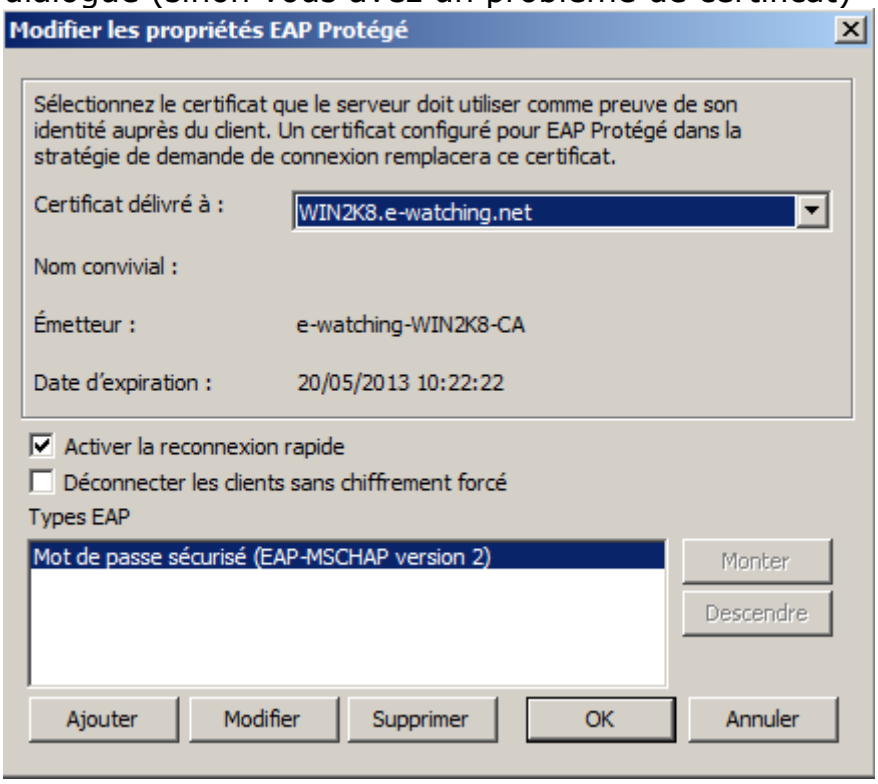


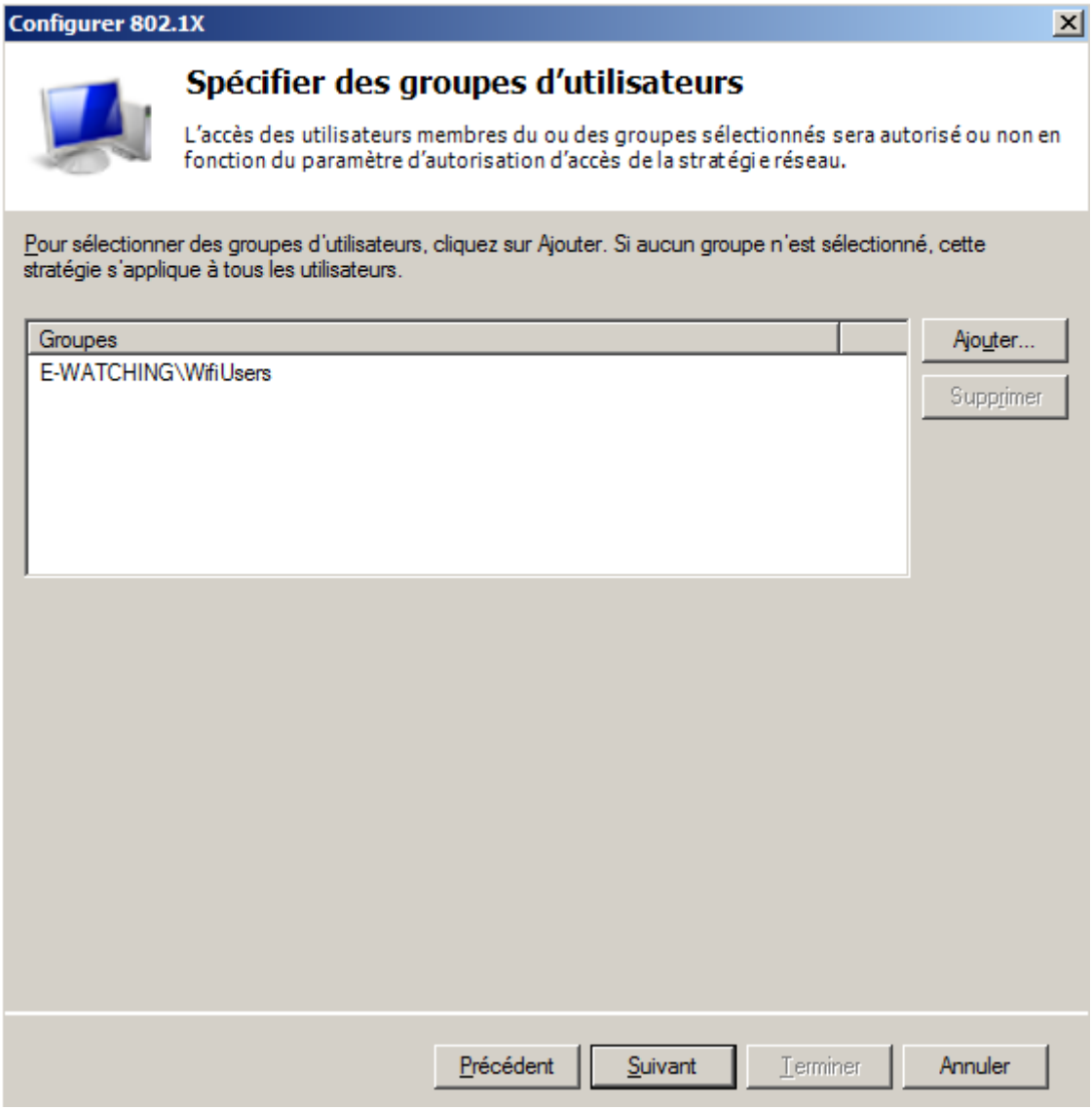
Renseignez son nom, @ip (ou fqdn si le DNS est renseigné), puis spécifiez-lui un secret partagé (manuellement ou automatiquement).

- Spécifiez ensuite la méthode d'authentification par Microsoft PEAP.

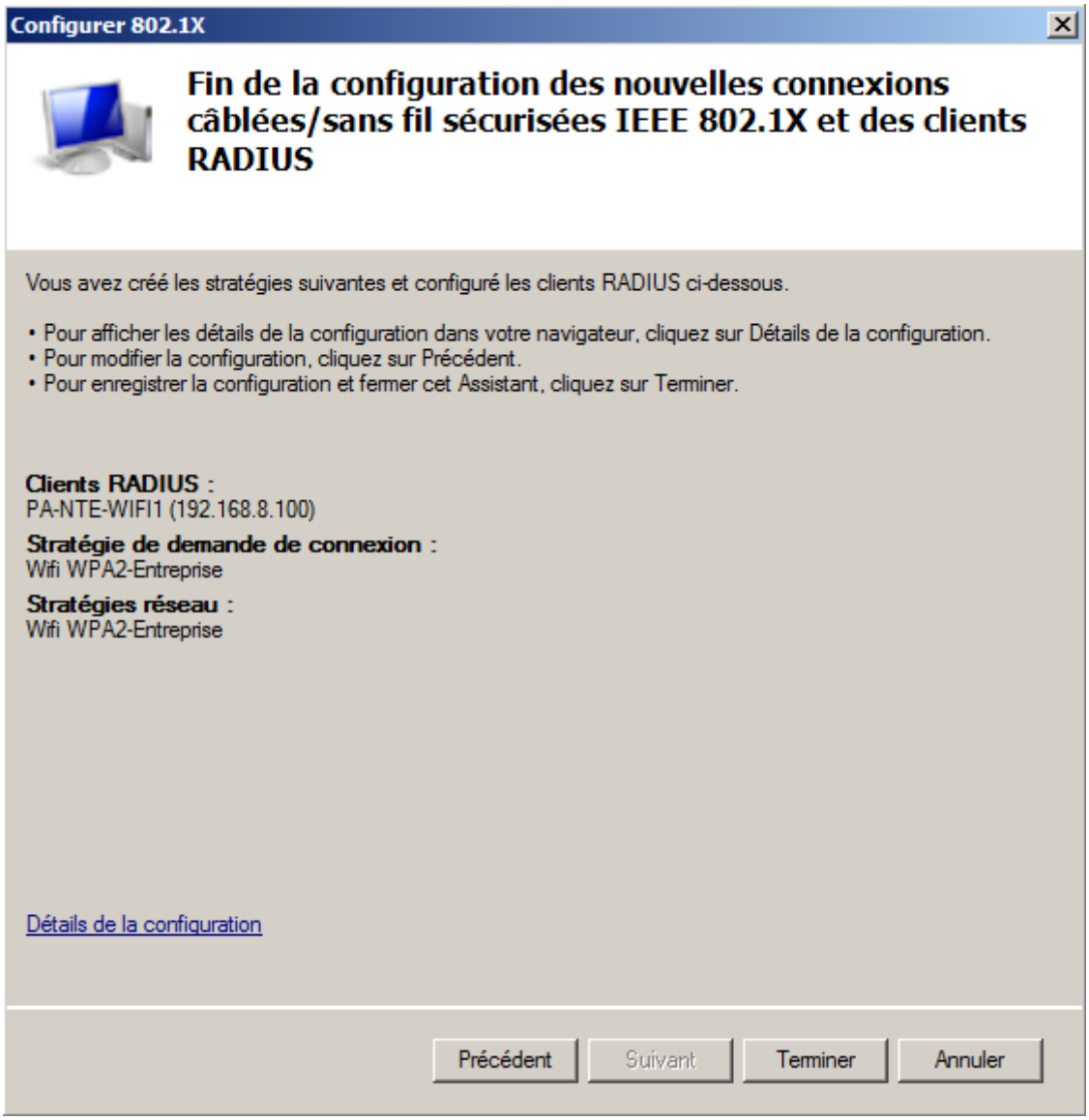


Si vous cliquez sur « configurer », vous devez obtenir cette boite de dialogue (sinon vous avez un problème de certificat)

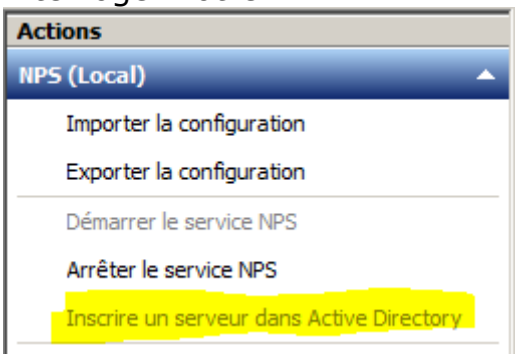




- Ajoutez ensuite le groupe des utilisateurs qui seront autorisés à s'authentifier.

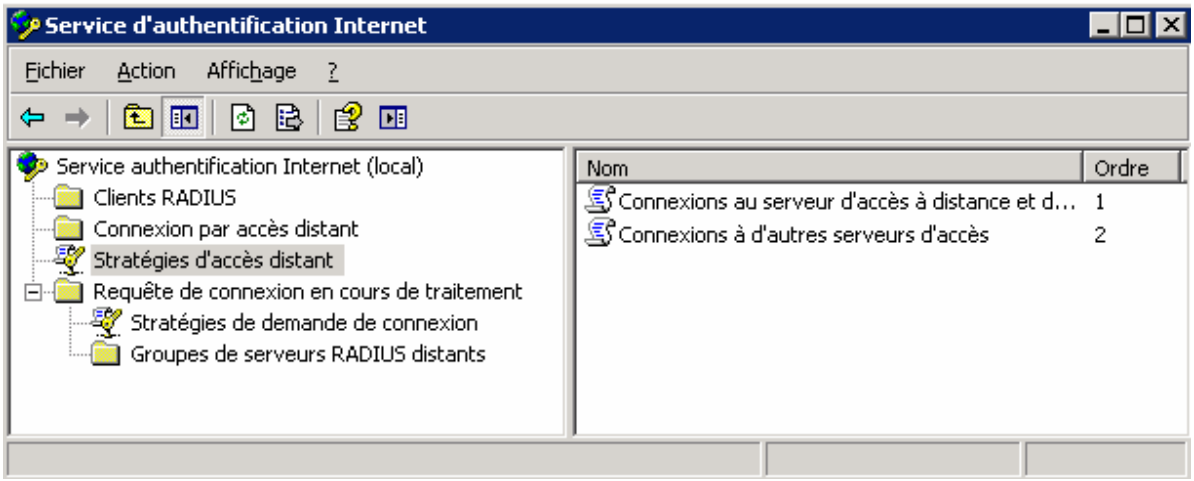


En fin de configuration, n'ommetez pas d'autoriser votre serveur NPS à interroger votre AD :

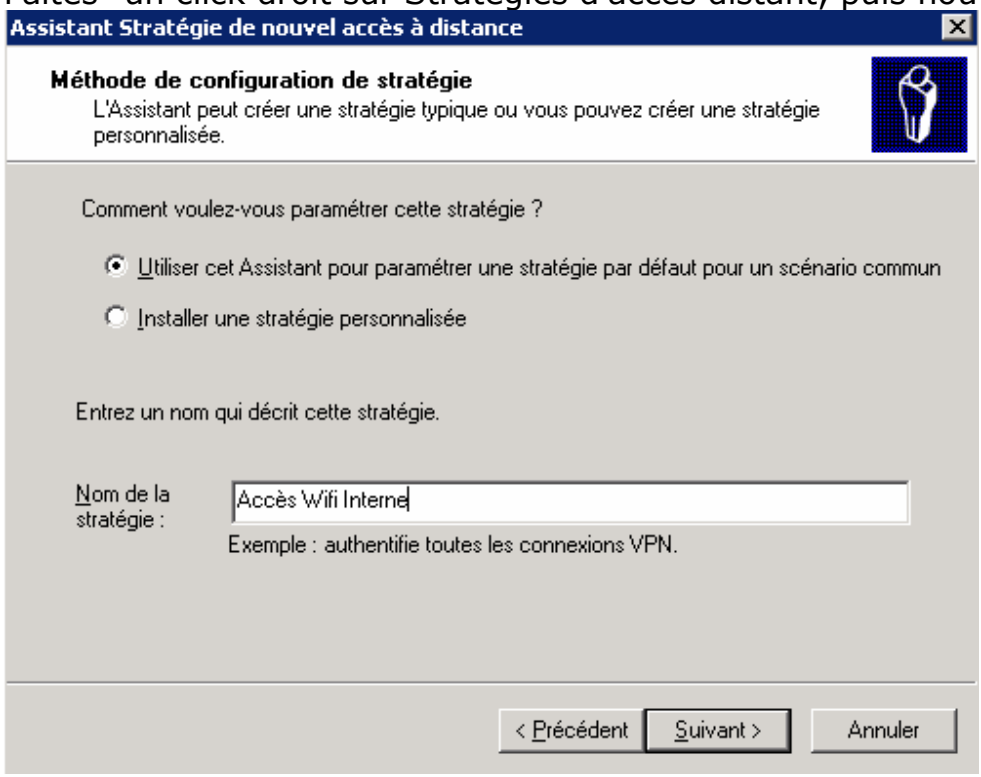


Nous allons maintenant configurer les stratégies de demande de connexion via le serveur NPS :

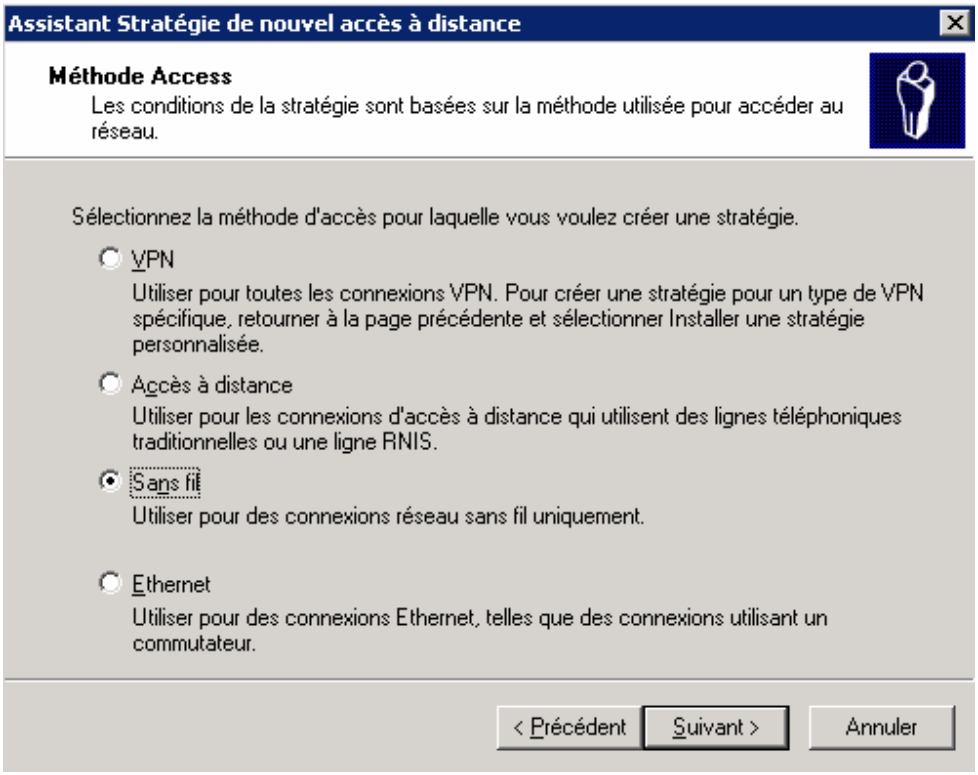
Nous devons maintenant configurer le service authentification Internet (service Radius) afin de lui préciser quels utilisateurs pourront s'authentifier via Radius, mais aussi quels équipements réseaux auront le droit de transmettre les requêtes d'authentification à ce serveur Radius.



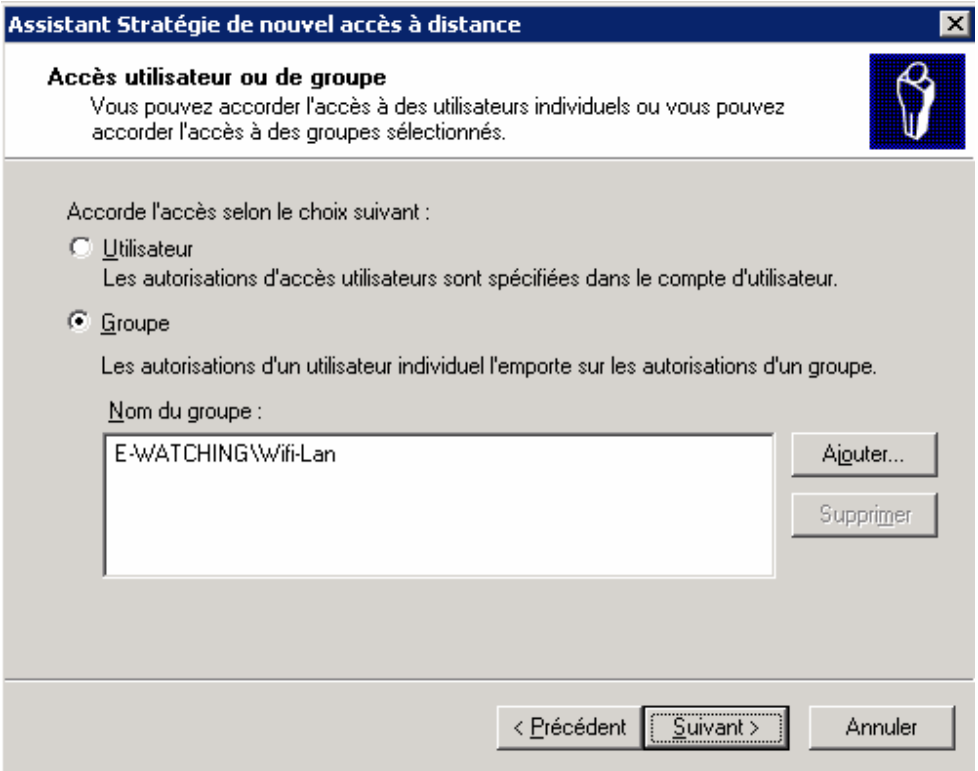
Faites- un click droit sur Stratégies d'accès distant, puis nouvelle stratégie



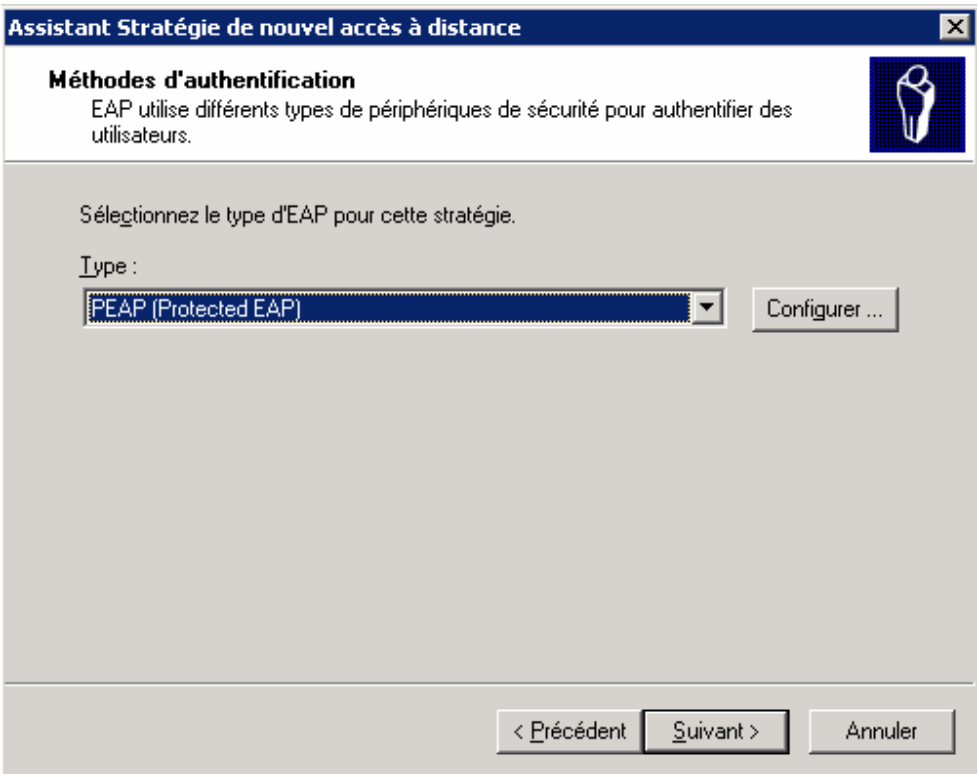
Donnez-lui un nom explicite et précisez que c'est une stratégie pourun scénario commun



Précisez la méthode d'accès : Sans-fil



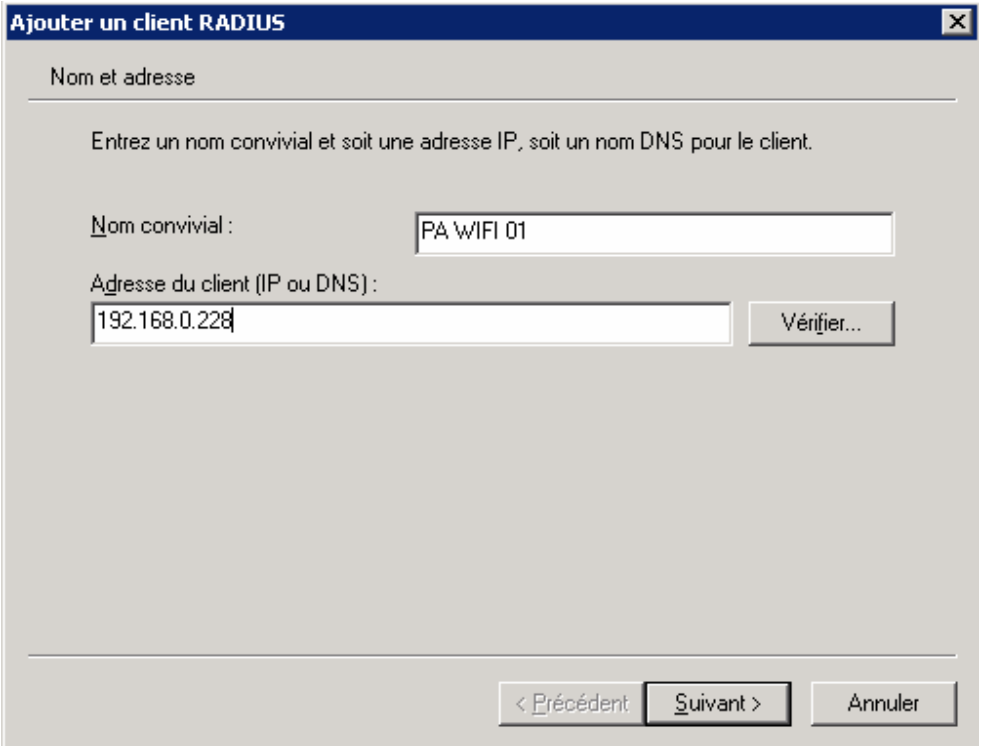
Indiquez quel groupe pourra utiliser cette stratégie (dans notre cas, le groupe Wifi)



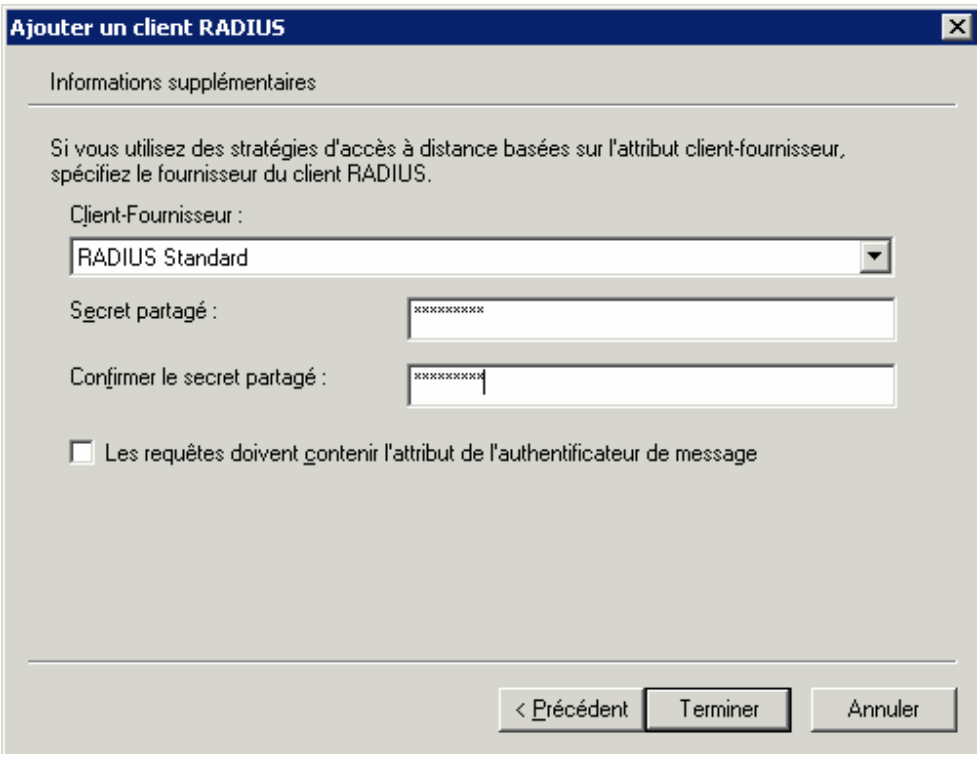
Choisissez la méthode d'authentification PEAP

➔ Nous devons ensuite déclarer un « client Radius », ce client désignera le point d'accès Wifi autorisé à interroger le serveur Radius

Avec l'outils d'administration Radius, allez dans le dossier Client Radius, click droit, nouveau client Radius



Nommez ce point d'accès, et renseignez l'adresse IP de ce point d'accès



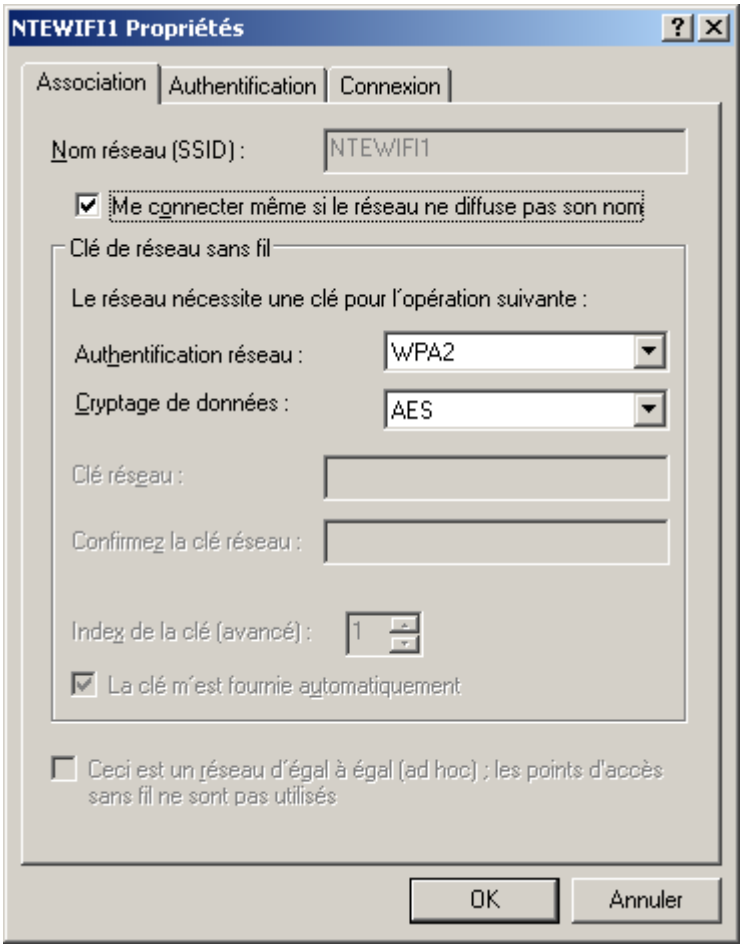
Sélectionnez le client-fournisseur Radius Standard et définissez un secret partagé suffisamment **long et complexe**.

Ce secret partagé (ou mot de passe) sera ensuite renseigné sur le Point d'accès Wifi.

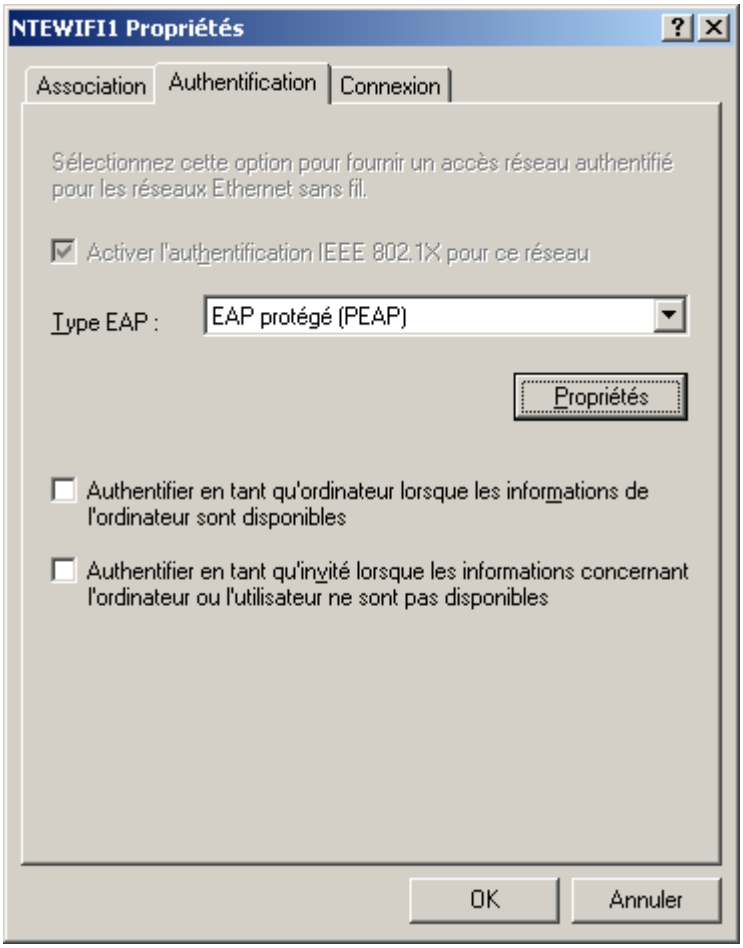
4 – Configuration de la connexion Client (Xp ou W7)

Le réseau Wifi configuré sur le point d'accès doit être visible depuis le client Wifi (cf nom de réseau SSID utilisé sur la PA)
La connexion Wifi doit être de type WPA-Entreprise, avec méthode d'authentification PEAP & MS-CHAP v2. Vous devez alors avoir la possibilité d'associer votre login (domaine\login) + password à la connexion Wifi ou même d'utiliser les informations d'authentification déjà saisies pour l'ouverture de session Windows (si le PC fait partie du domaine Windows visé).
Attention, sur un ordinateur qui ne fait partie du domaine AD, vous devez au préalable exporter l'autorité de certification du controleur AD ou du serveur Windows à partir duquel vous avez généré le certificat, puis l'inscrire sur le portable (via la MMC+ composants Certificats).
Dès que la connexion est établie, le poste recevra une adresse IP (+ DNS + passerelle +…) si un serveur DHCP se trouve configuré sur le LAN.

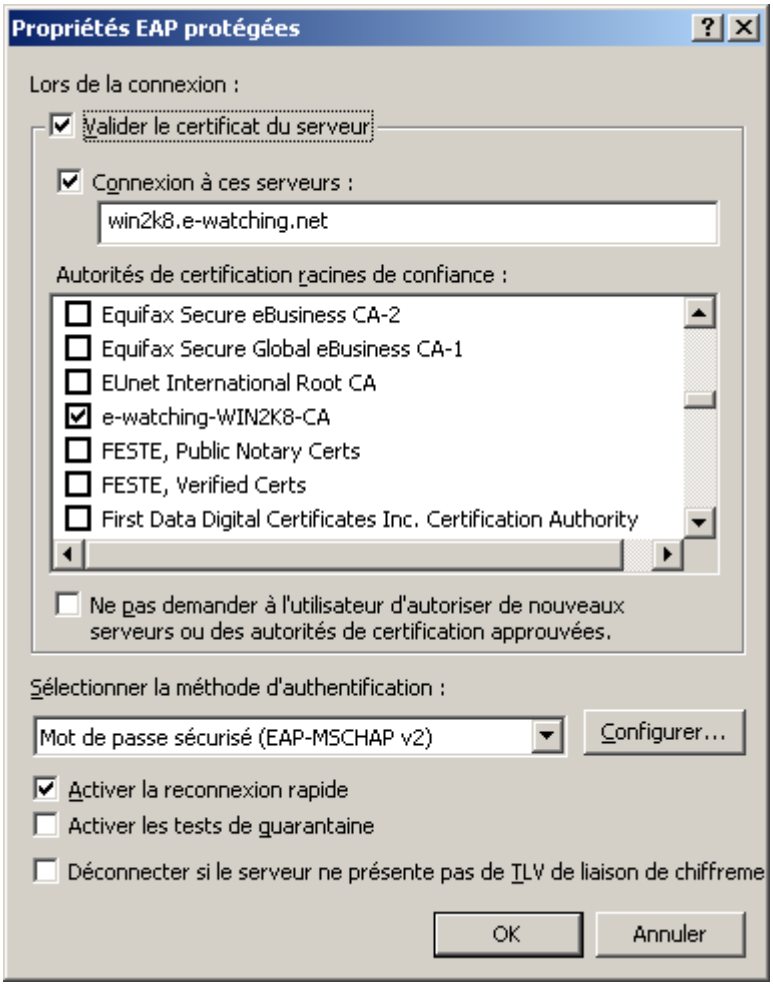
Exemple de configuration sous Windows XP (+SP2 minimum)
Propriété de la connexion Wifi



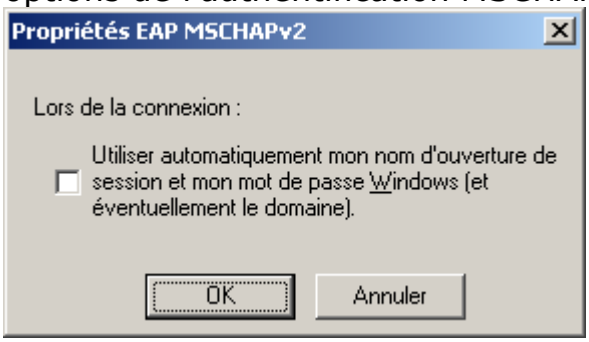
Onglet Authentification



Propriétés PEAP (cette copie d'écran indique le choix du certificat émis par votre serveur AD ou NPS).



Si vous êtes sur un portable hors domaine, alors allez aussi dans les options de l'authentification MSCHAP



Afin de ne pas utiliser le login/password du poste local pour s'authentifier sur un serveur distant qui ne reconnaitra pas votre login.