Objet :	**WIFI sécurisé en entreprise (sur un active directory 2003)**	Date :	**26/12/2007**
		Version :	**1.0**

0 - Théories et principes divers sélectionnés

Quelques normes :

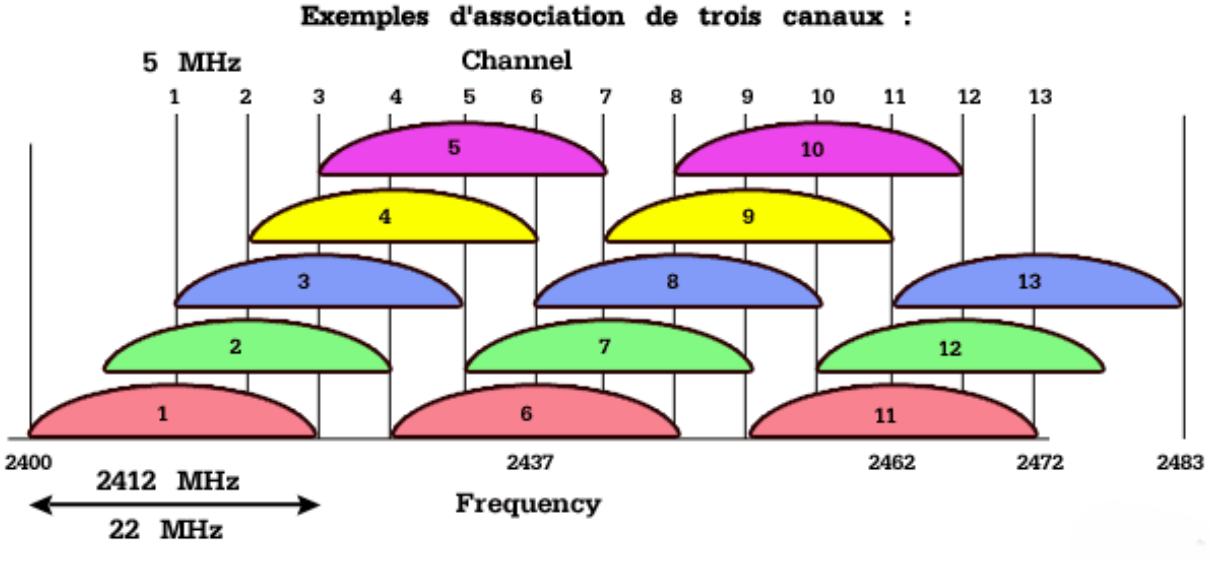
802.11 : ensemble de normes qui couvre les connexions à un réseau local sans-fils (appelé WLAN) dont

- 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) et plus récemment WPA2 (chiffrement basé sur AES) , normalisé.

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 réelle 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,…

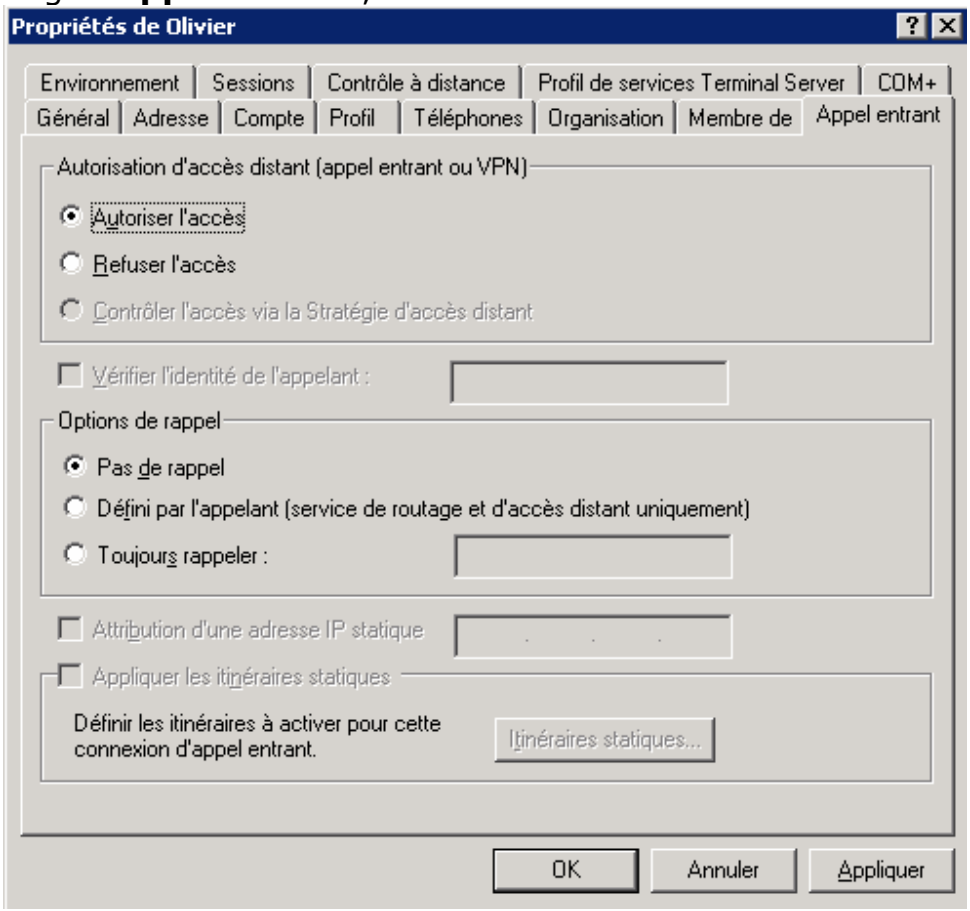
L'environnement décrit pour la connexion Wifi nécessite (nécessitera) les équipements suivants :

- ActiveDirectory 2003 (déjà configuré)
- Serveur DHCP (déjà configuré)
- Serveur Radius 2003
- Point d'accès Wifi supportant WPA2 et PEAP (dans l'exemple ci-dessous, un produit d'entrée de gamme Netgear WG302 est utilisé)
- Un poste avec carte Wifi

1 – Préparation de l'environnement Windows – ActiveDirectory

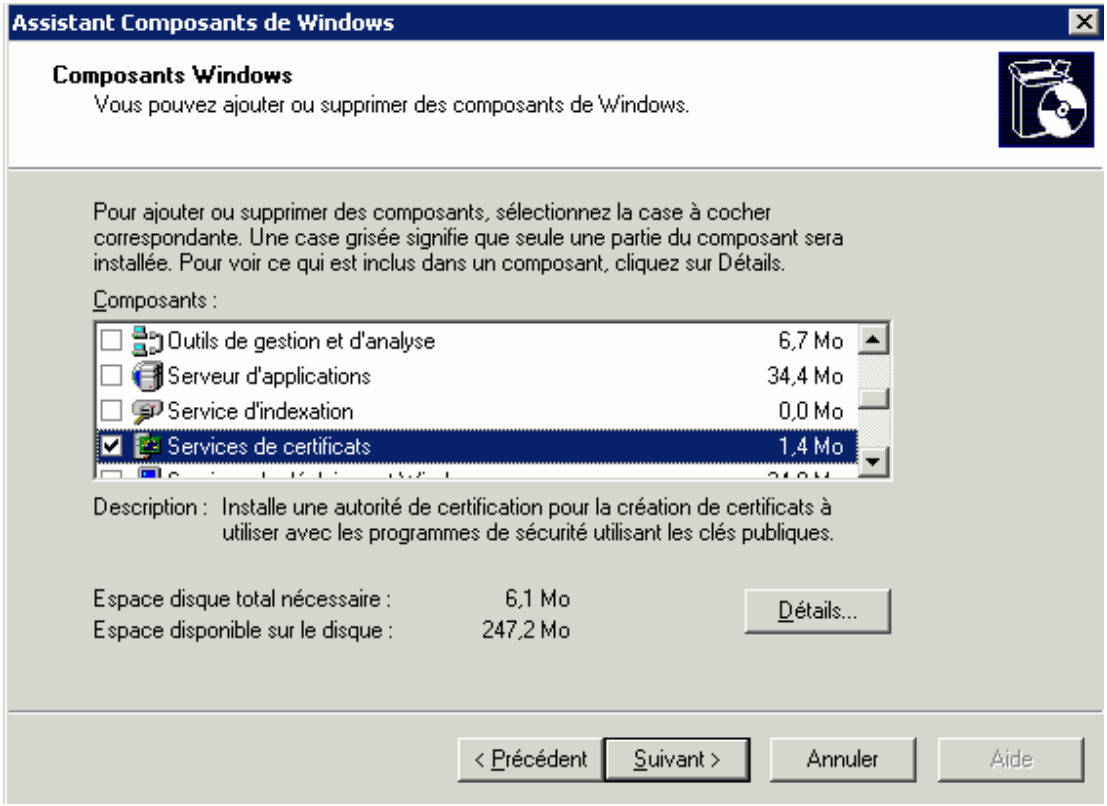
Les utilisateurs qui pourront se connecter via Wifi devront faire partie d'un groupe *global* d'utilisateur définit (par exemple : WIFI-LAN) et seul les membres de ce groupe pourront s'authentifier sur les PA Wifi.

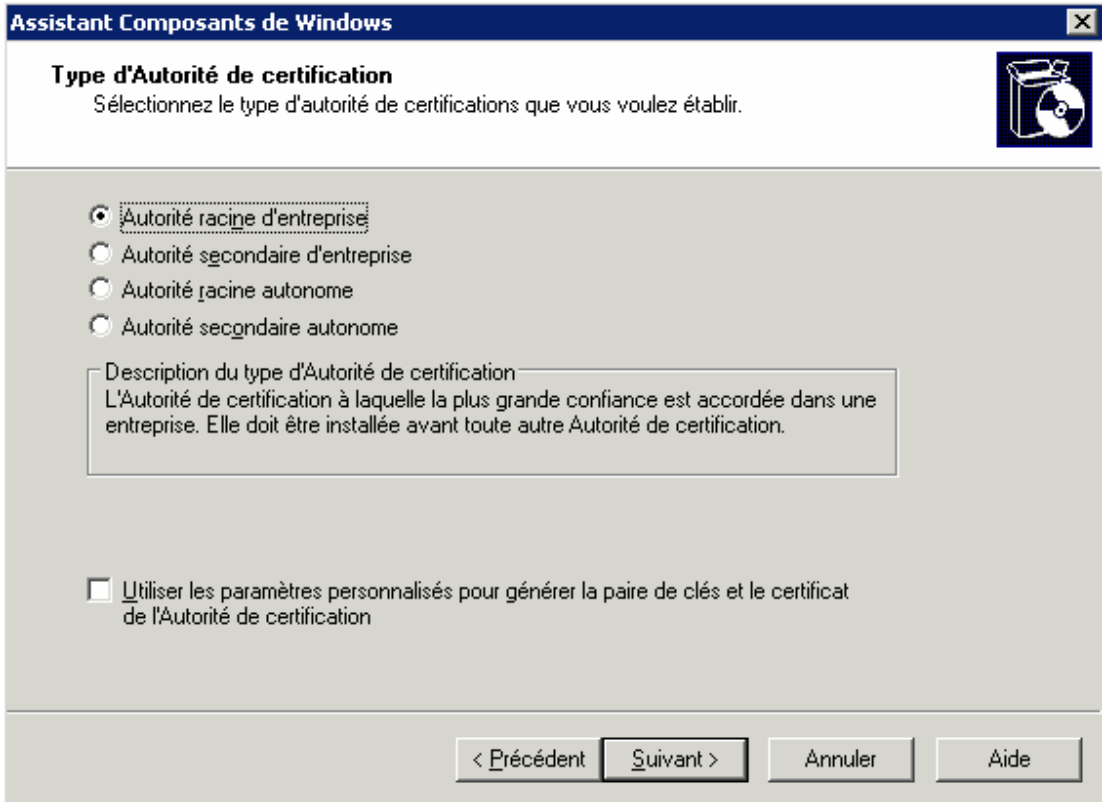
Chaque Utilisateur Active Directory qui se connectera en Wifi doit avoir également l'autorisation sur l'accès distant : Propriété de l 'utilisateur, onglet **Appel entrant**, sélectionner **Autoriser l'accès**.

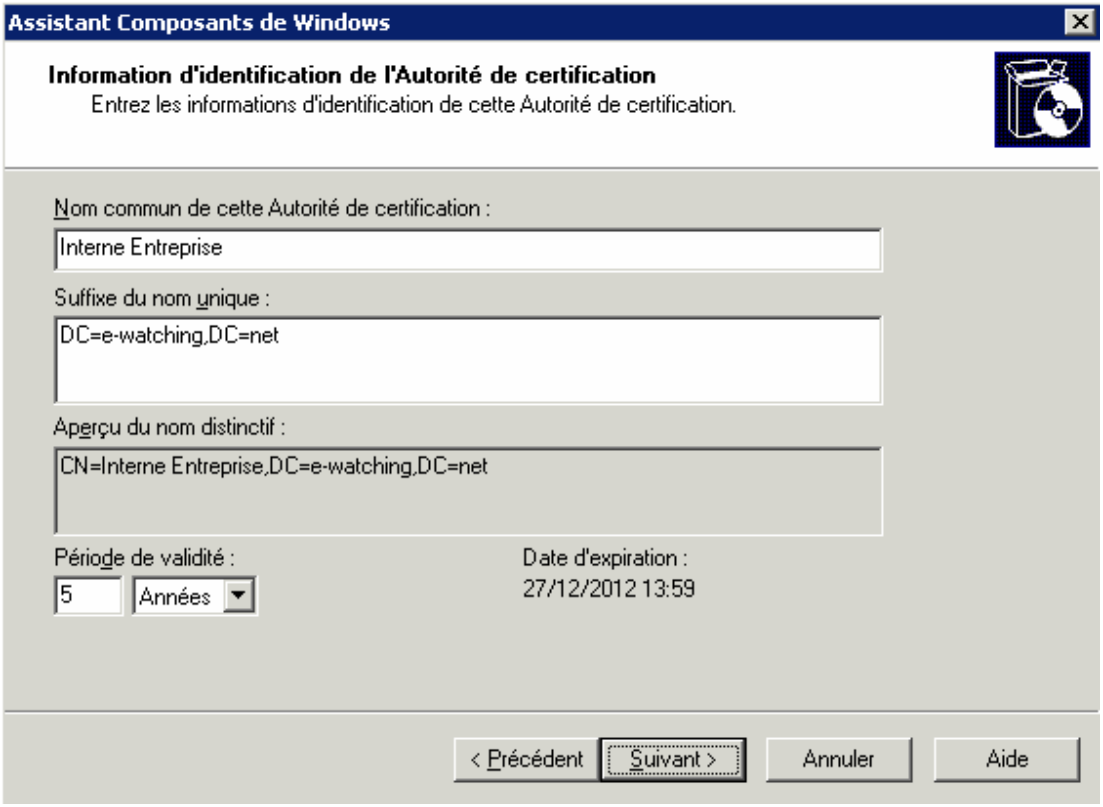


2 – Mise en place d'une autorité de certificat

Il est préférable d'avoir un service IIS/ASP installé sur le serveur sur lequel vous installerez l'autorité de certificat. Dans l'exemple « à vocation pédagogique » ci-dessous, nous supposons que l'autorité de certification est la première de l'AD.
Dans tous les cas, l'installation est des plus simples et la configuration quasi nulle ; au moins en ce qui concerne la mise à disposition d'une autorité de certification pour PEAP .

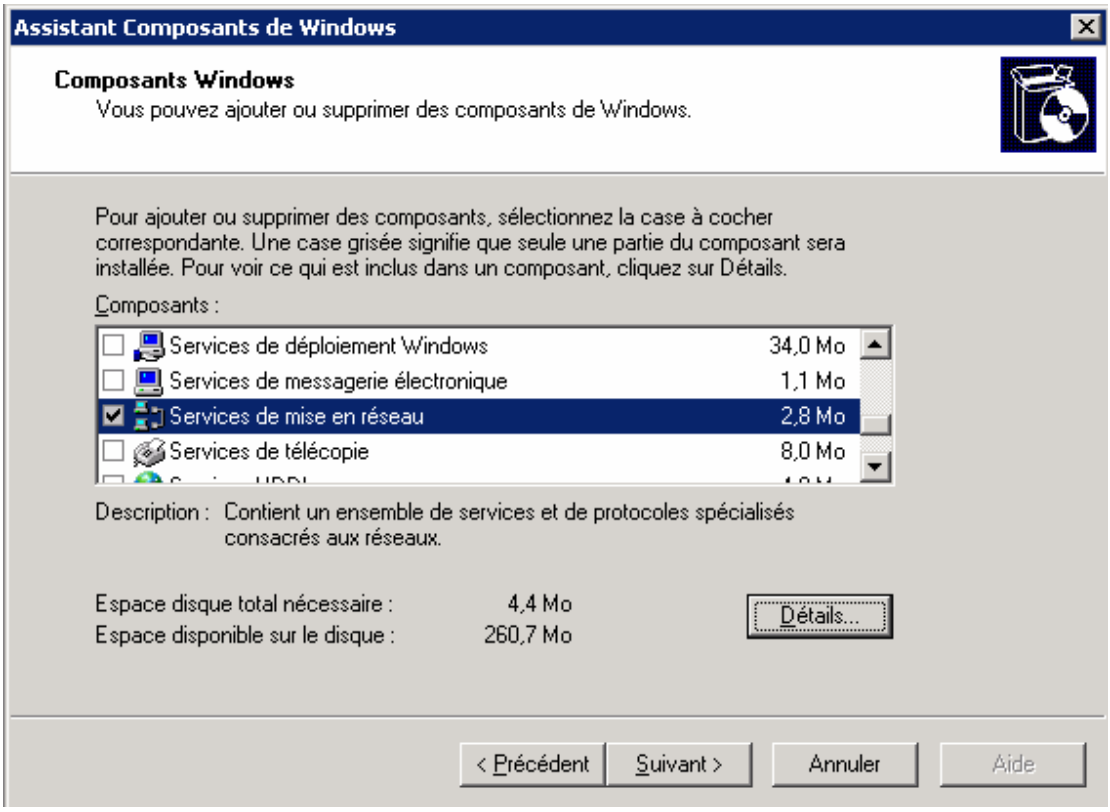

Assistant Composants de Windows
Composants Windows
Vous pouvez ajouter ou supprimer des composants de Windows.
Pour ajouter ou supprimer des composants, sélectionnez la case à cocher correspondante. Une case grisée signifie que seule une partie du composant sera installée. Pour voir ce qui est inclus dans un composant, cliquez sur Détails.
Composants :
Outils de gestion et d'analyse 6,7 Mo
Serveur d'applications 34,4 Mo
Service d'indexation 0,0 Mo
Services de certificats 1,4 Mo
Description : Installe une autorité de certification pour la création de certificats à utiliser avec les programmes de sécurité utilisant les clés publiques.
Espace disque total nécessaire : 6,1 Mo
Espace disponible sur le disque : 247,2 Mo
Détails...
< Précédent
Suivant >
Annuler
Aide


Assistant Composants de Windows
Type d'Autorité de certification
Sélectionnez le type d'autorité de certifications que vous voulez établir.
Autorité racine d'entreprise
Autorité secondaire d'entreprise
Autorité racine autonome
Autorité secondaire autonome
Description du type d'Autorité de certification
L'Autorité de certification à laquelle la plus grande confiance est accordée dans une entreprise. Elle doit être installée avant toute autre Autorité de certification.
Utiliser les paramètres personnalisés pour générer la paire de clés et le certificat de l'Autorité de certification
< Précédent
Suivant >
Annuler
Aide

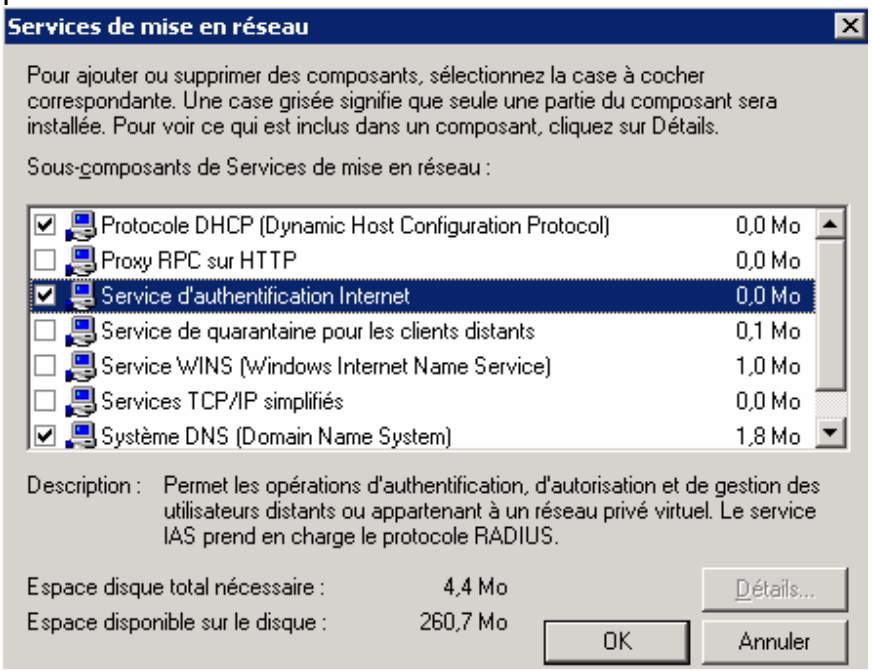


2 – Installation du serveur Radius

Sur le serveur, aller dans Ajout/Suppression de programmes – Ajouter/Supprimer des composants Windows
Sélectionnez **Services de mise en réseau**



puis allez sur **Détails**



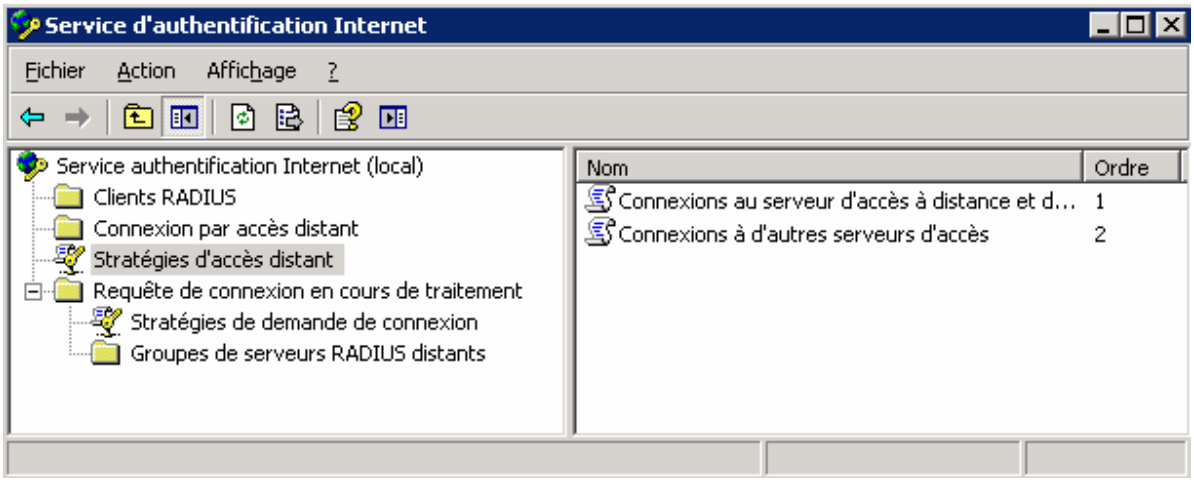
Cochez **Services d'authentification Internet**, puis validez jusque **Terminer**

Pas de redémarrage nécessaire.

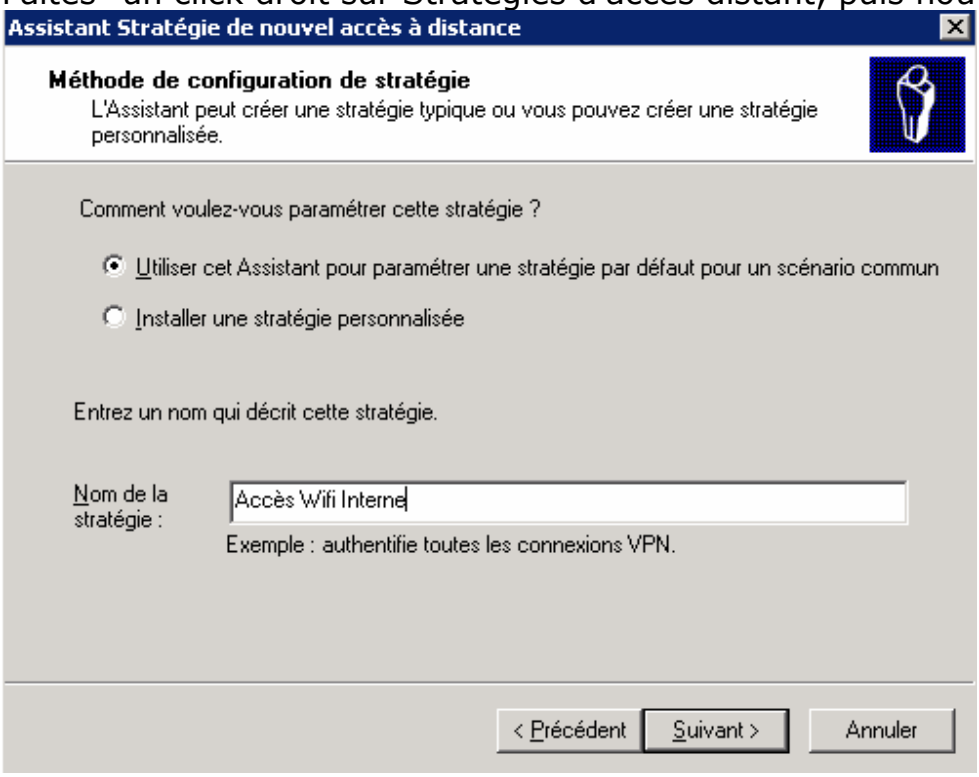
Une nouvelle icône est ajoutée dans les outils d'administration :

3 – Configuration du Serveur Radius

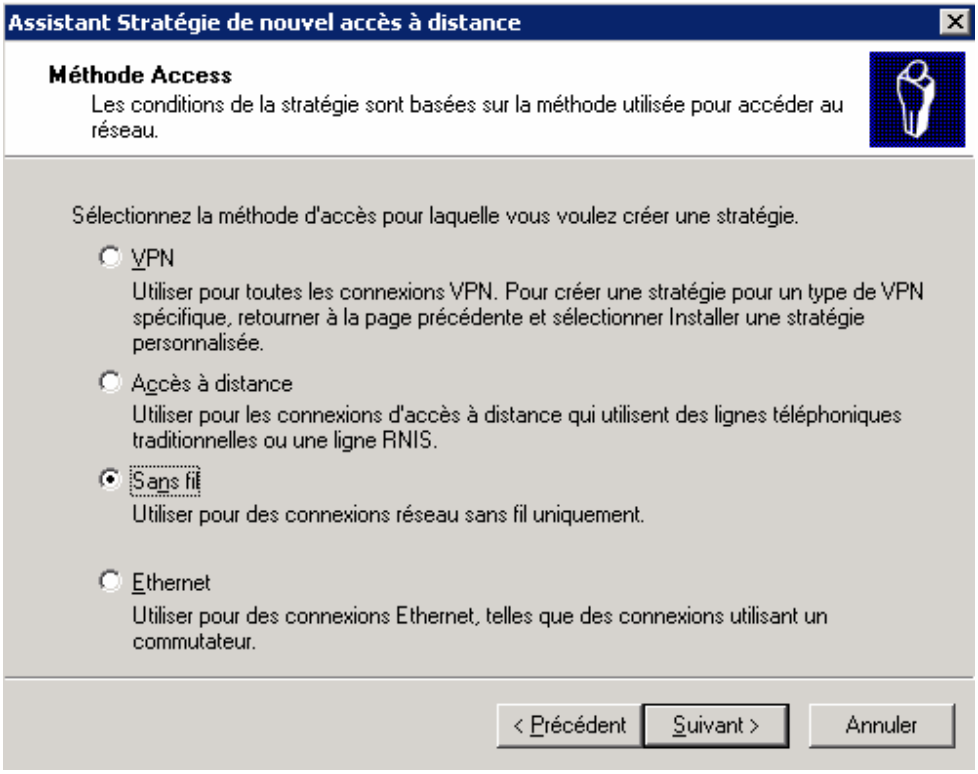
Nous devons maintenant configurer le service authentification Internet (service Radius) afin de lui préciser quels utilisateurs pourront s'authentifier via Radius, mais aussi quels équipements réseaux auront le droit de transmettre les requêtes d'authentification à ce serveur Radius.



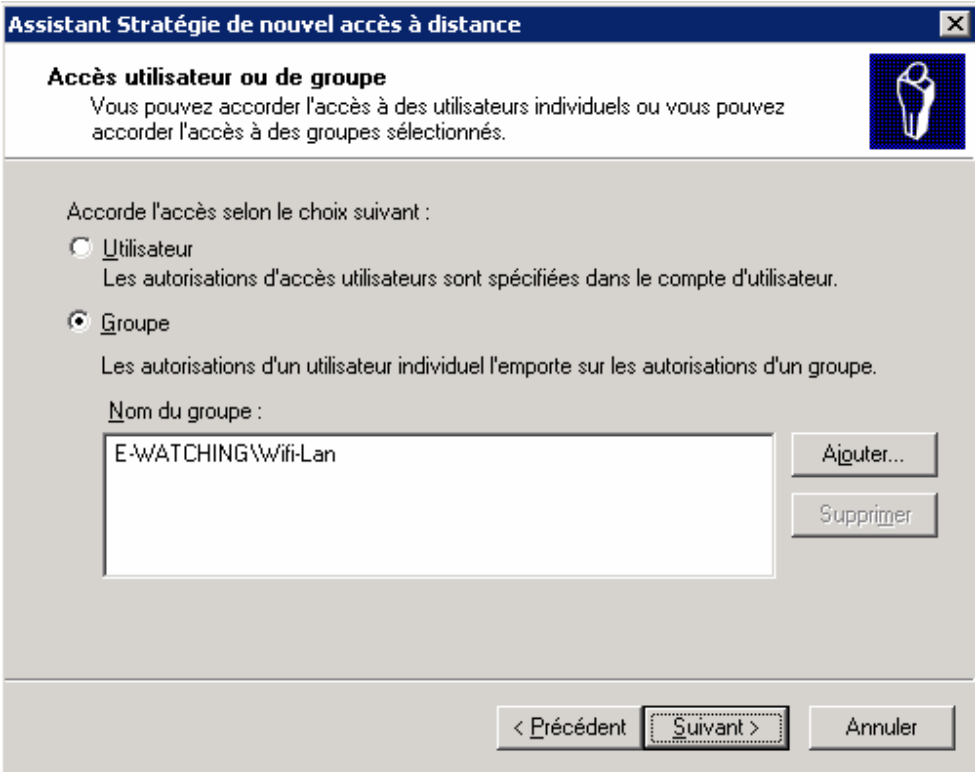
Faites- un click droit sur Stratégies d'accès distant, puis nouvelle stratégie



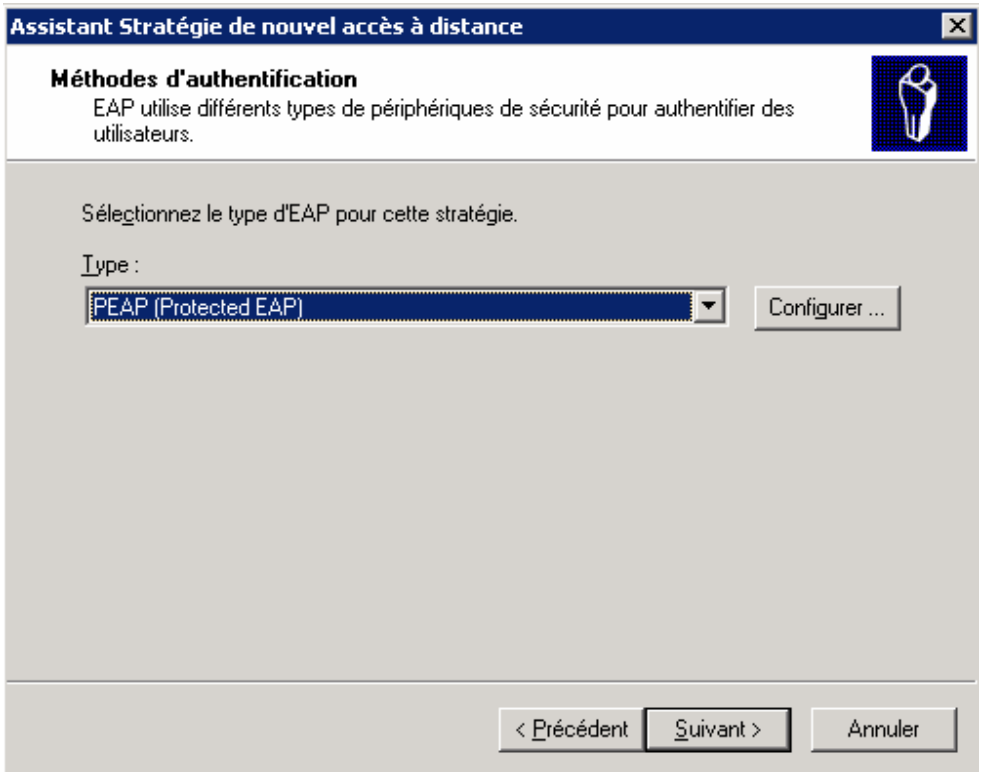
Donnez-lui un nom explicite et précisez que c'est une stratégie pourun scénario commun



Précisez la méthode d'accès : Sans-fil



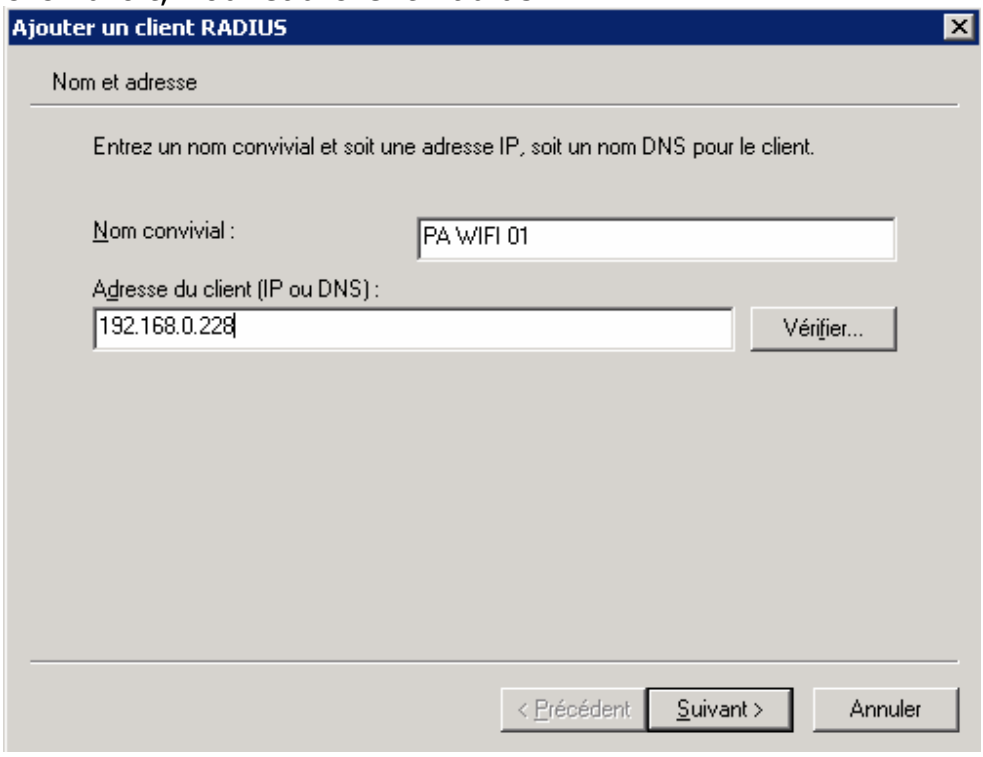
Indiquez quel groupe pourra utiliser cette stratégie (dans notre cas, le groupe Wifi)



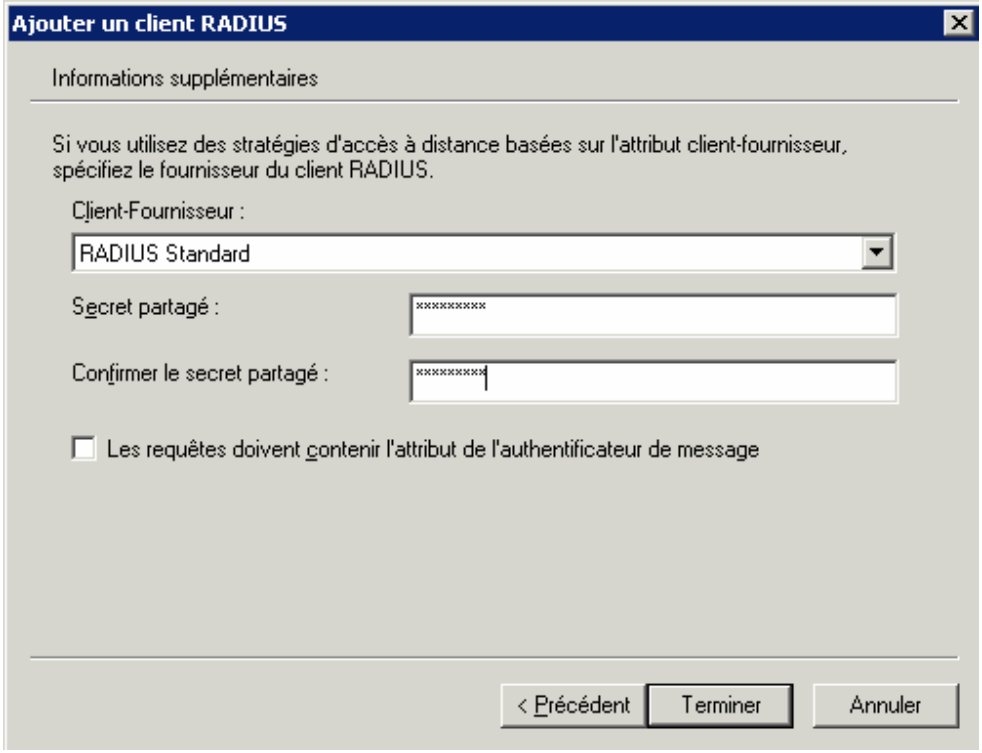
Choisissez la méthode d'authentification PEAP

➔ 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 + SP2)

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'authentificaiton PEAP & MS-CHAP v2. Vous devez alors avoir la possibilité d'associer votre login (domaine\login) + password à la conneixon 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).
Dès que la connexion est établie, le poste recevra une adresse IP (+ DNS + passerelle +…) si un serveur DHCP se trouve configuré sur le LAN.

5- Améliorations ?

Une faiblesse toutefois à toutes ces explications : n'importe quel PC peut se connecter au LAN de l'entreprise à la seule condition de connaître le login (+ password) d'un utilisateur qui se trouve dans le groupe global Wifi. C'est un peu à l'image d'un anonyme qui vient brancher son PC sur

une fiche Ethernet du LAN de l'entreprise, sauf qu'en plus dans le cas du Wifi l'individu n'est pas nécessairement présent dans le bâtiment.