Utilisation PEAP MS-CHAPV2

Pourquoi :

Pour avoir l'authentification machine et utilisateur
Utilisateur authentifié par son mot de passe / login AD
Pas de clé à installer sur les postes

Mise en oeuvre :

Le point d'accès est un WRT54GS V4 avec firmware dd-wrt 0,23

Coté serveur :

Sur un contrôleur de domaine, installer :
- IIS
- Service d'authentification internet
- Certificat
- Configurer le routage et accès distant (pour utiliser DHCP sur les postes en wifi)

Résultat :

L'authentification par couple login mot de passe fonctionne, il y a descente des profils et exécution des scripts de connexion.

Les GPO machines et utilisateurs sont prises en compte à condition d'ajouter la clé suivante dans la base de registre :

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters

Clé de type REG_DWORD : DisableDHCPMediaSense
Mettre la valeur 1

Le processus de BOOT est alors beaucoup plus long, mais tous les paramètres machine sont correctement installés.

Ce mode de connexion wifi est vulnérable aux attaques avec des couples mot de passe / login donc dans les paramètres de sécurité, désactiver les comptes après 5 tentatives infructueuses d'ouverture de session pendant 5 min par exemple. De plus refuser le wifi aux utilisateurs ayant des privilèges administrateur sur le domaine.

Important : toutes les affirmations de ce document doivent être complétées par : "pour autant que je sache"

PEAP MS CHPA-V2

Ici, le client s'assure de l'identité du serveur radius par un certificat sur celui-ci.
Par contre, tout utilisateur capable de fournir un couple login / mot de passe, validé par radius, sera accepté sur le réseau.
Cela implique, qu'il est prudent de limiter les comptes acceptés par radius, en particulier, les administrateurs du domaine ne devraient pas utiliser une station en wifi pour administrer le réseau.
Le serveur radius communique avec le point d'accès grâce à l'adresse IP de celui et une clé partagée qui doit être robuste.
Il est important de configurer les clients afin qu'ils refusent la connexion à un serveur radius qui n'a pas de certificat, ceci afin d'éviter qu'un pirate tente de se faire passer pour un point d'accès et intercepte toutes les

communications du client.

Le mécanisme d'ouverture de session est sûr, les échanges sont cryptés et ne sont pas analysables (19/12/2006) ensuite, la session est cryptée en WPA-AES ou bien WPA-TKIP qui est un peu moins robuste mais toujours considéré comme non cassable. On peut mixer les deux (TKIP+AES)

Pour améliorer la sécruité de l'ensemble, j'ai imposé la signature SMB sur les clients wifi.
(je ne suis pas certain du grand interet de la chose...)

EAP-TLS

L'EAP-TLS demande l'installation de certificats sur la machine, pour identifier la machine et pour l'utilisateur. C'est un peu lourd à gérer par contre, c'est très sûr.

WPA – PSK
Demande l'installation de clés partagées entre le point d'accès et les stations, si la clé du point d'accès est compromise, il faut repasser sur toutes les stations. On ne peut pas filtrer les utilisateurs qui se connectent en wifi.
Deux cryptages sont proposés :

- TKIP, compatible avec le matériel utilisant le cryptage WEP
- AES plus performant

Parfois on a l'option TKIP+AES sur le point d'accès ce qui donne la possibilité d'utiliser des clients avec les deux types de cryptage

Installation de l'autorité racine

Pour initier une ouverture de compte , il faut une communication sécurisée, un tunnel crypté. Pour cela le protocole PEAP – MS CHAP V2 demande un certificat serveur qui sera validé au niveau du client (on valide l'autorité de certification).

L'installation de l'autorité racine est parfaitement détaillée sur ce lien :

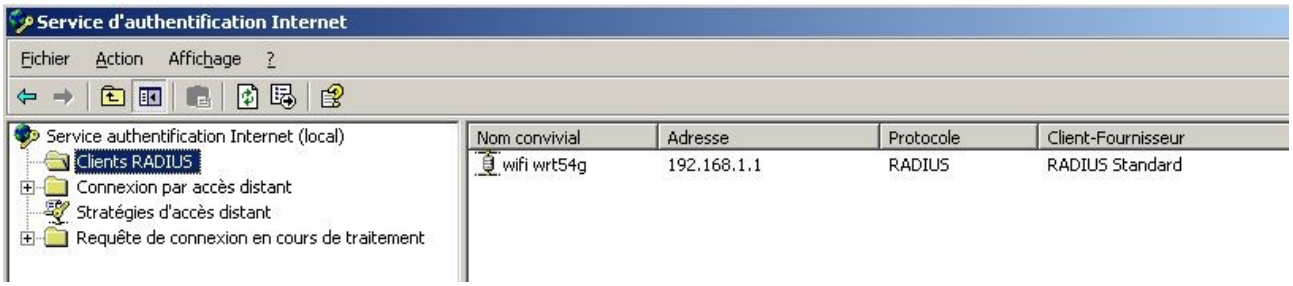
http://www.laboratoire-microsoft.org/articles/network/wpa/3/

Installation d'IAS

Le serveur radius, est un des services proposé par IAS, il faut donc installer ce service. L'installation se fait par : ajout / suppression de programmes => Ajouter supprimer des composants Windows => Services de mise en réseau => Service d'authentification Internet.

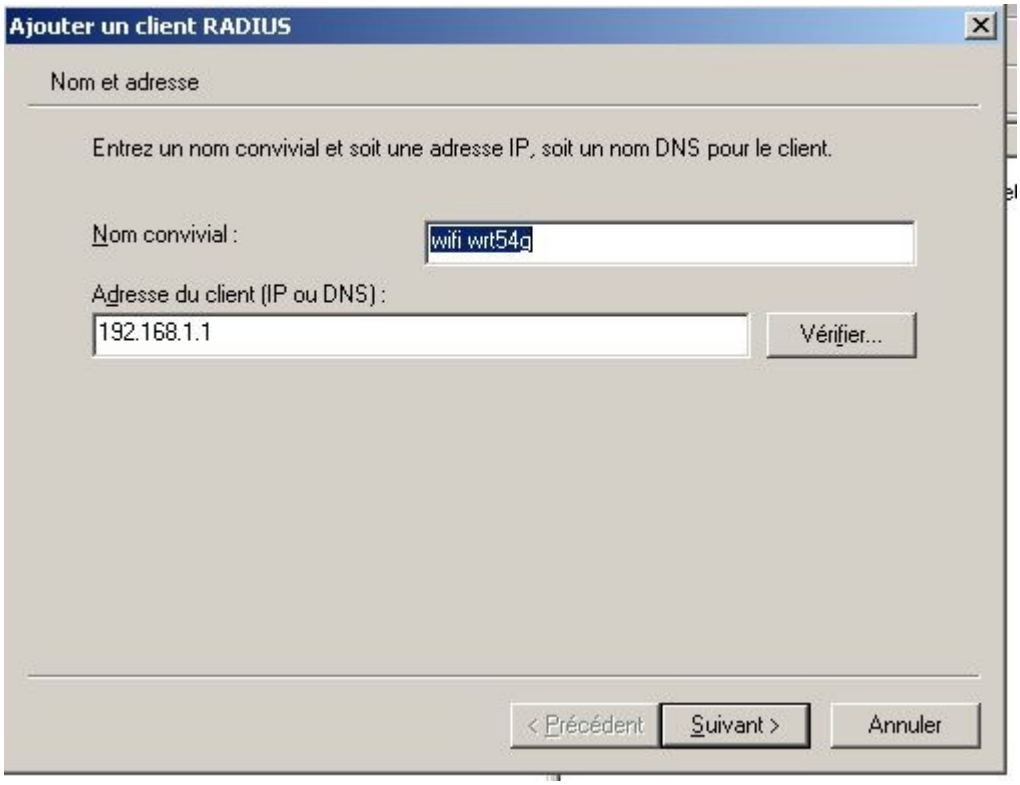
Lancer la console services et authentification internet

Ajout du client
Il y a autant de clients que de points d'accès, *y penser lorsque l'on nomme son client*.

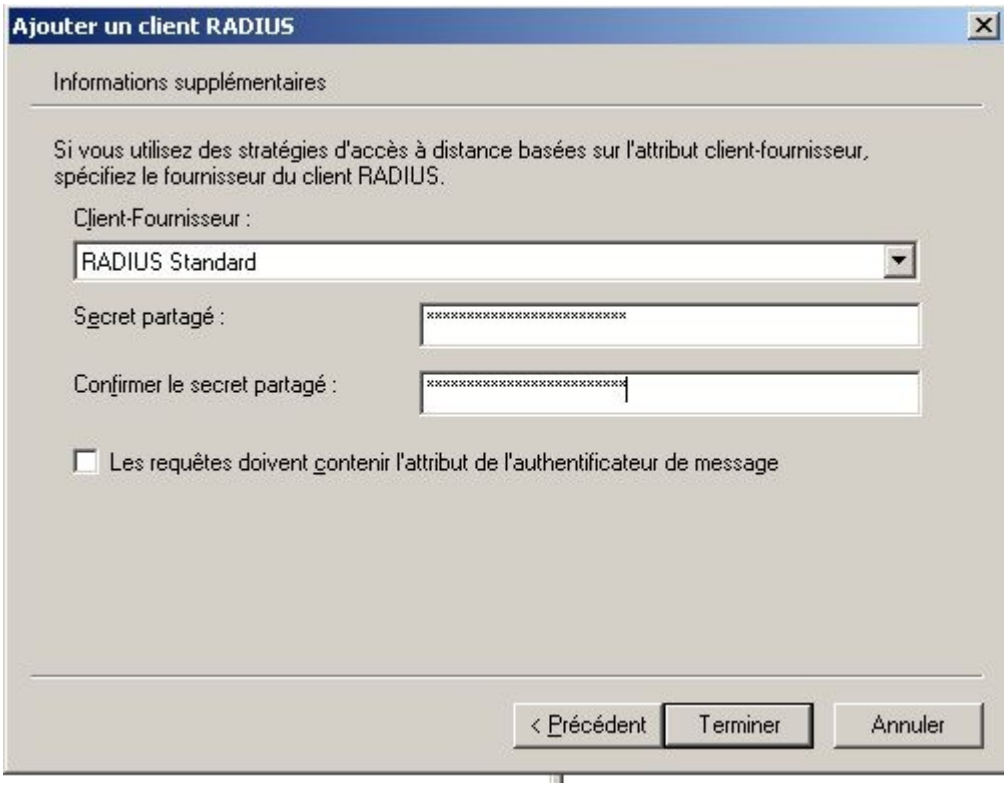


Adresse IP du point d'accès ou son nom, s'il est enregistré dans DNS, le bouton « vérifier » permet de faire une résolution DNS.

Nom convivial : Nom qui apparaîtra dans la console IAS

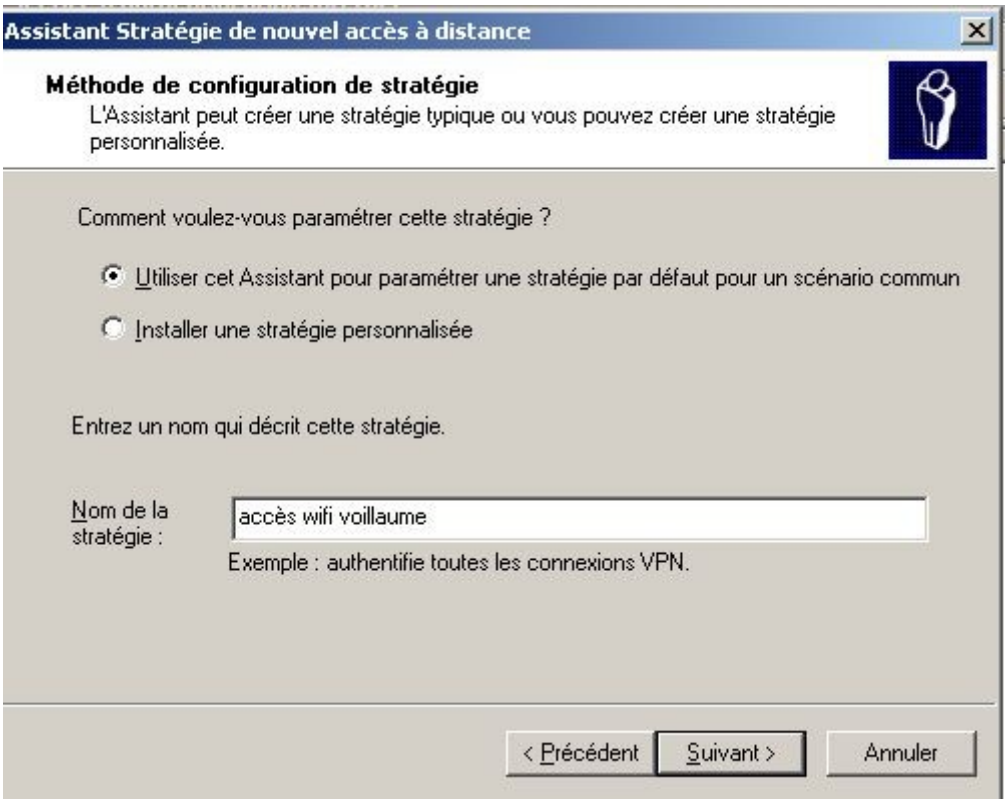


Le secret est partagé entre le point d'accès et le serveur Radius, **il doit être robuste**.

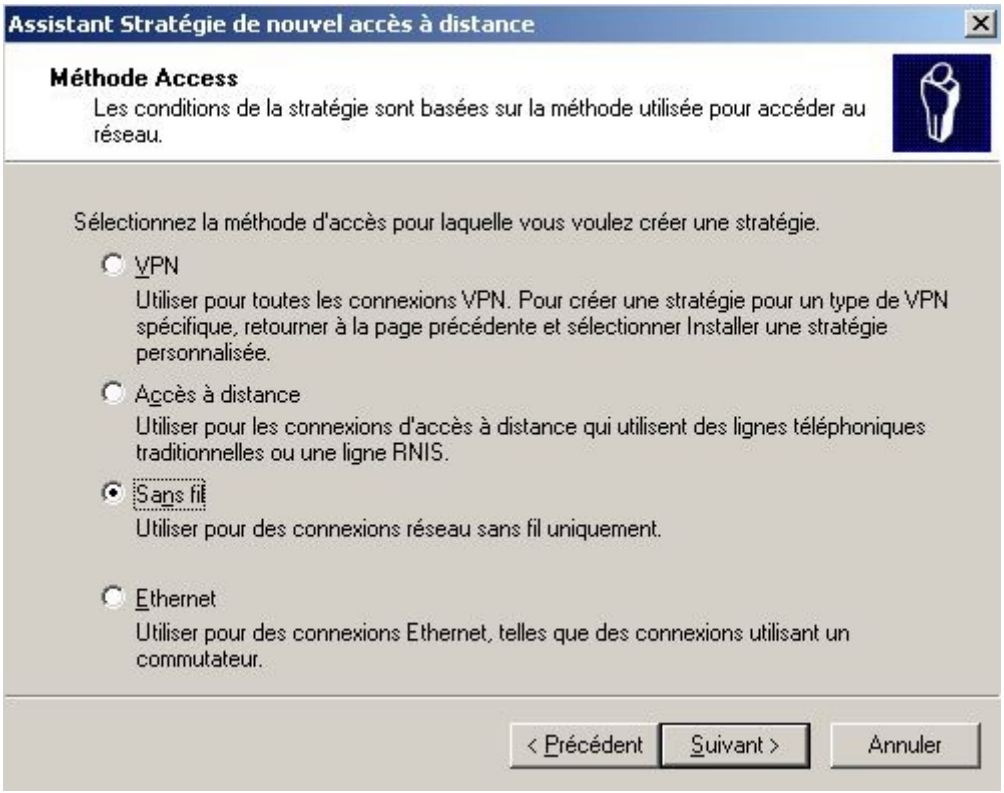


Que dire de la case à cocher ?

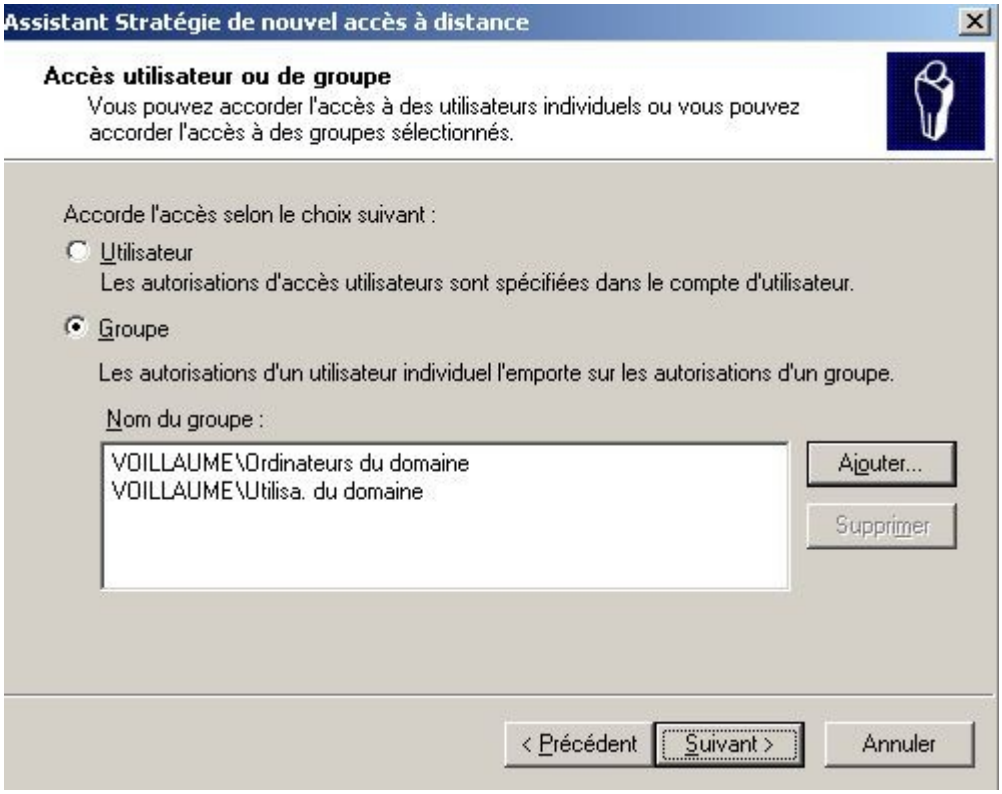
Ensuite, l'assistant nous propose de paramétrer une stratégie RADIUS



On utilise l'assistant et on donne un nom à cette stratégie, c'est le nom qui apparaîtra dans la console IAS.



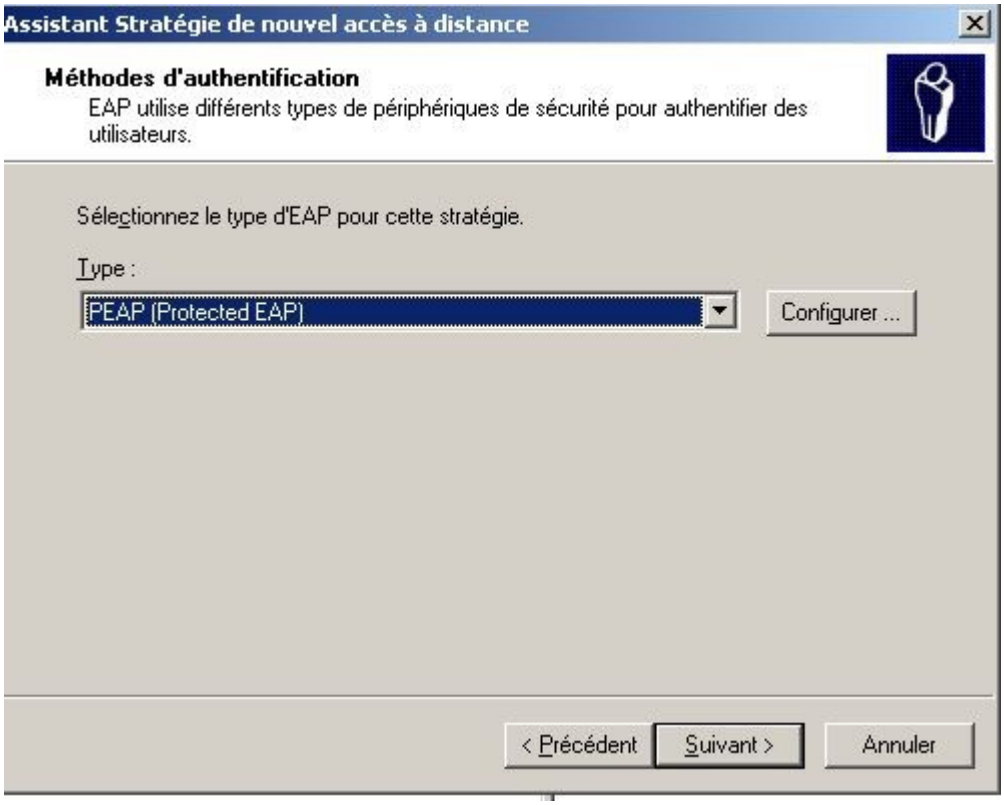
C'est une stratégie pour du sans-fil



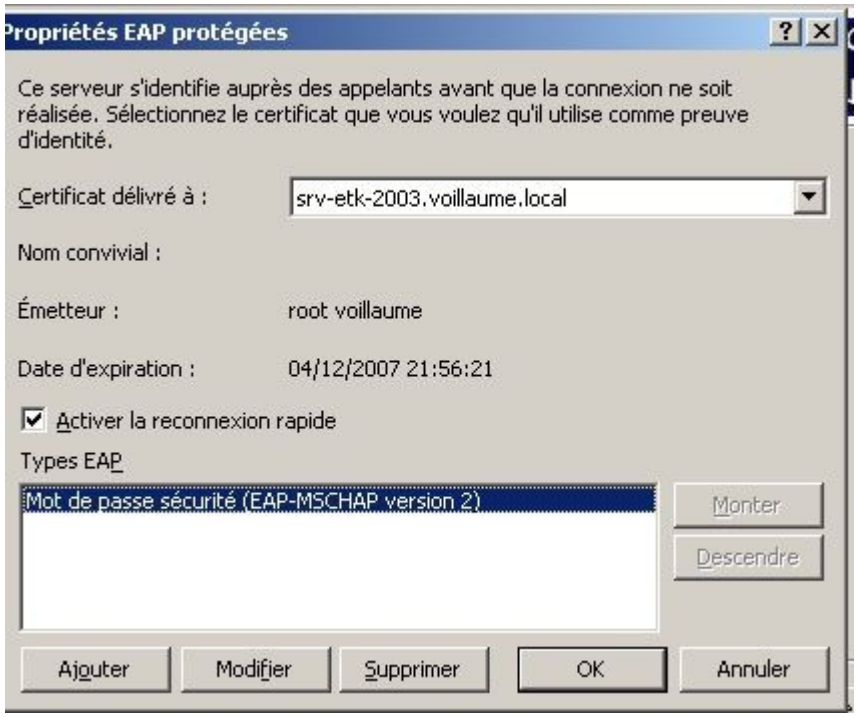
Je pense qu'il faut mettre les ordinateurs du domaine afin que le réseau soit monté avant l'ouverture de session. L'ordinateur s'authentifie à radius et peut donc exécuter la partie machine des gpo (scripts, sécurité, etc.) j'y reviendrai.

Attention, le protocole est vulnérable à une attaque sur dictionnaire de mot de passe ou une attaque en brute. Le réseau étant accessible d'un point extérieur, on peut essayer de se connecter avec des couples login / mot de passe.
Je pense qu'il est préférable de ne laisser l'accès qu'aux profs et élèves voir restreindre en fonction des classes.
Les administrateurs du domaine, ne devraient pas pouvoir accéder au réseau via le wifi

Il est également possible de créer un groupe Wifi, dans lequel on mettra les ordinateurs et les utilisateurs autorisés à utiliser le wifi.

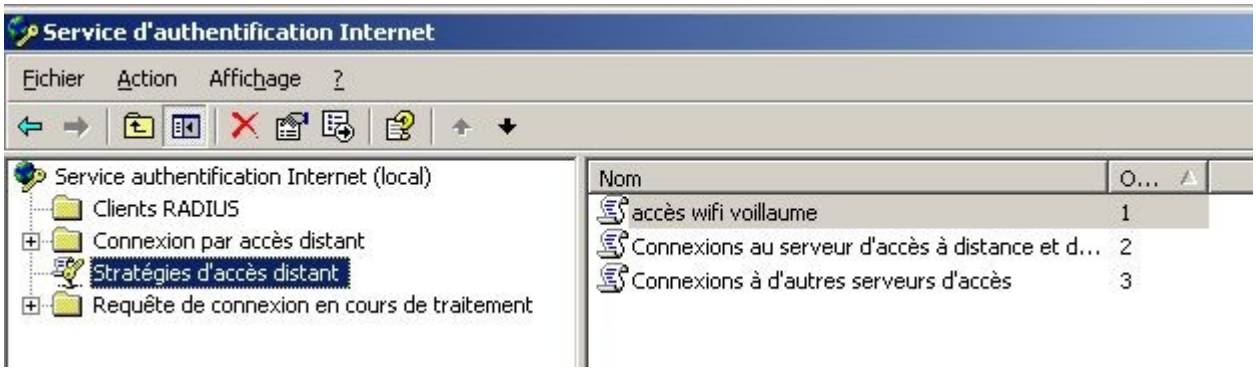


Ici on choisi **PEAP** et on configure



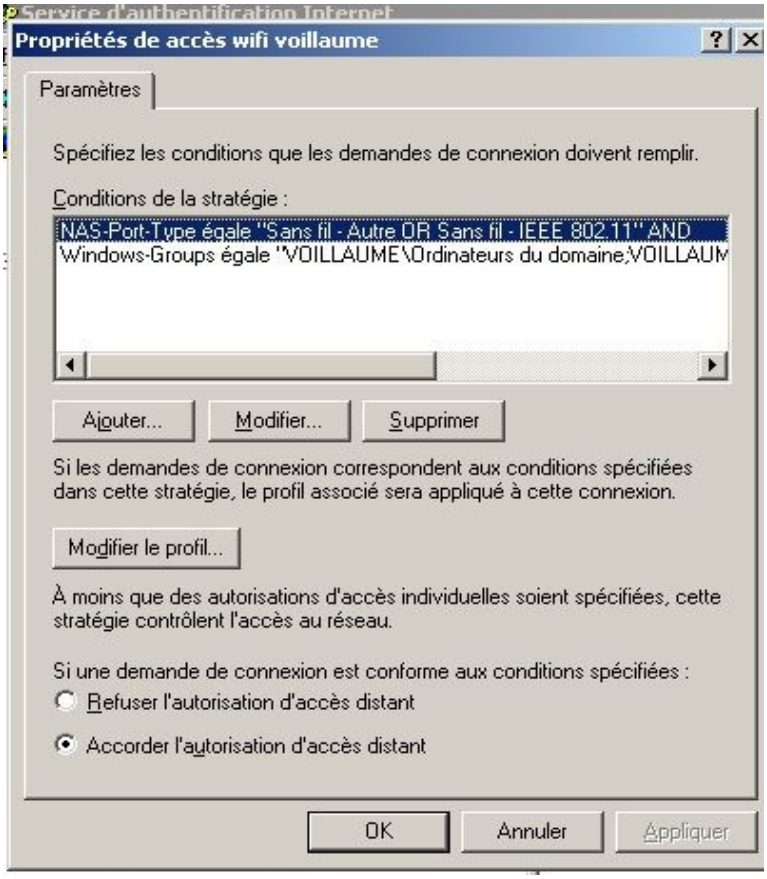
Il faut indiquer ici qui est l'autorité qui détient le certificat

On clique sur OK.

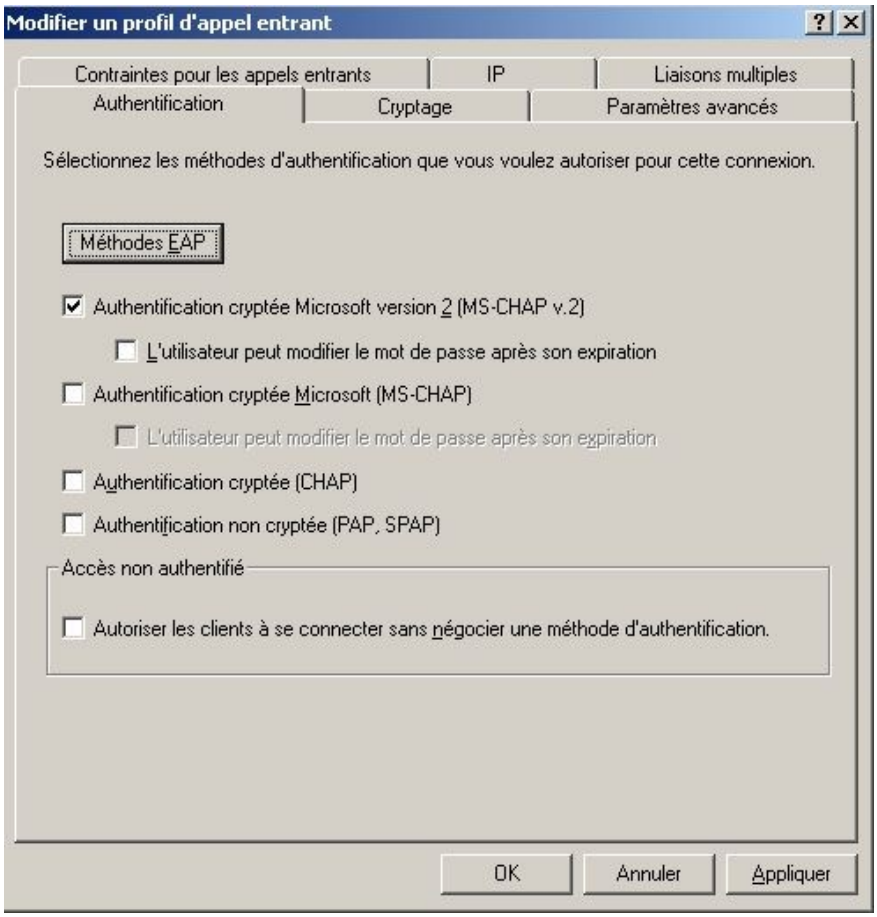


Les stratégies sont examinées les unes après les autres, dès qu'un accès est autorisé, on arrête. Sinon, on examine la stratégie suivante. Il faut donc laisser ces deux stratégies qui in fine bloquent l'accès au réseau sans fil.

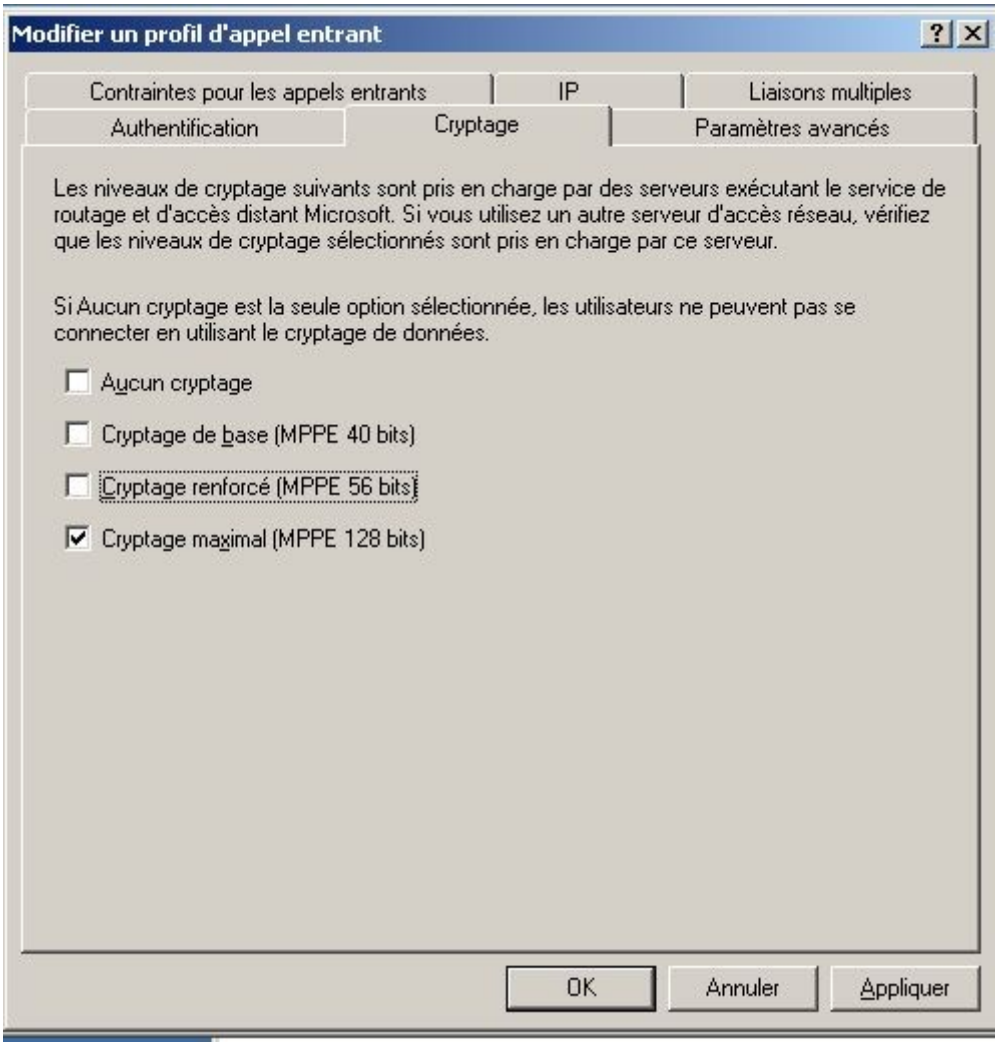
On va ensuite dans propriétés de la stratégie, pour configurer deux ou trois petites choses :



et l'on clique sur modifier le profil

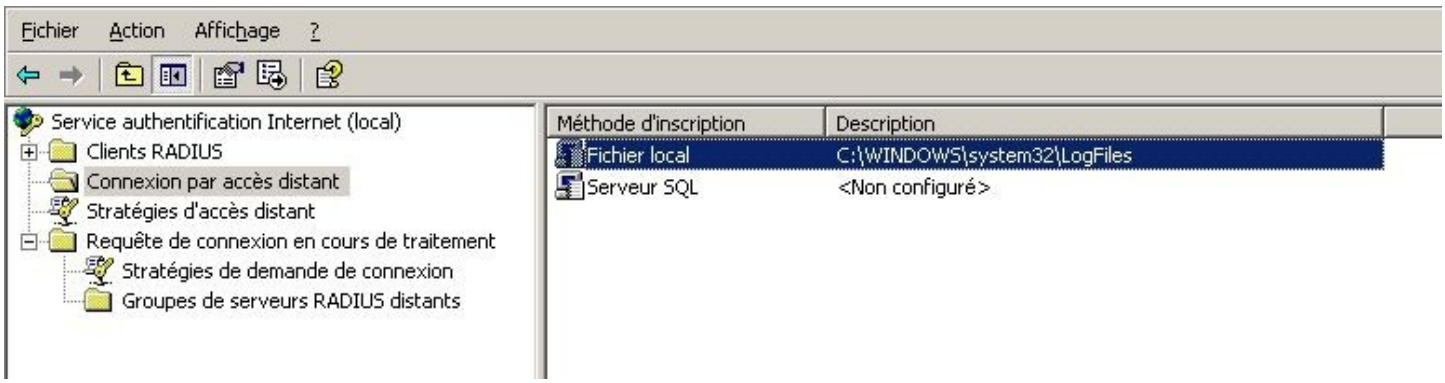


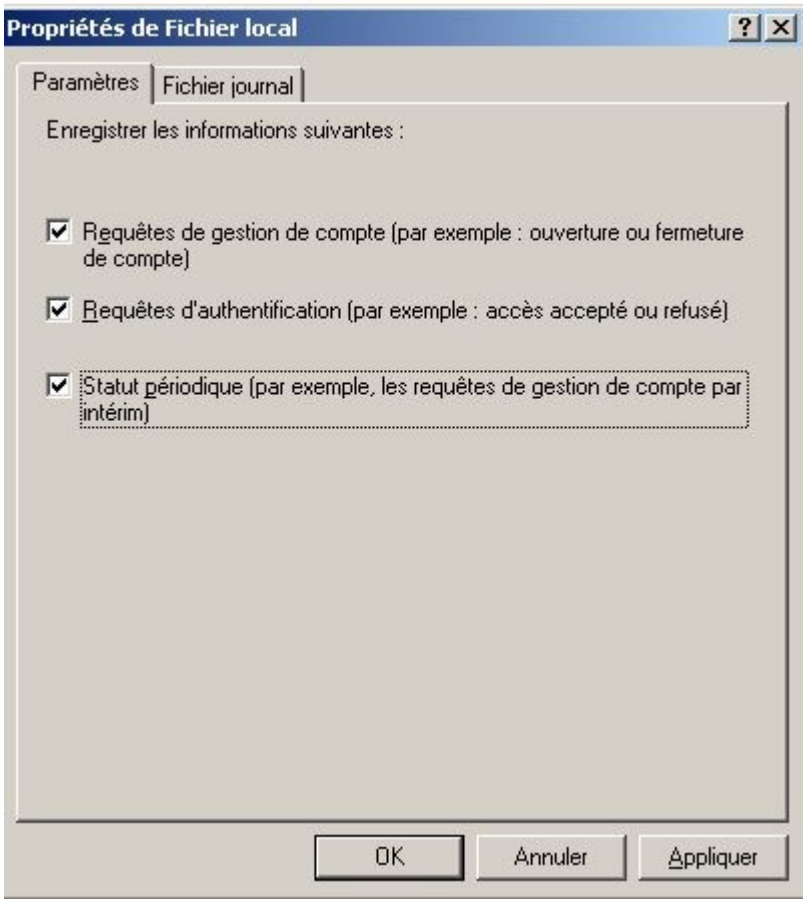
Que dire de : "l'utilisateur peut modifier le mot de passe après expiration" ?

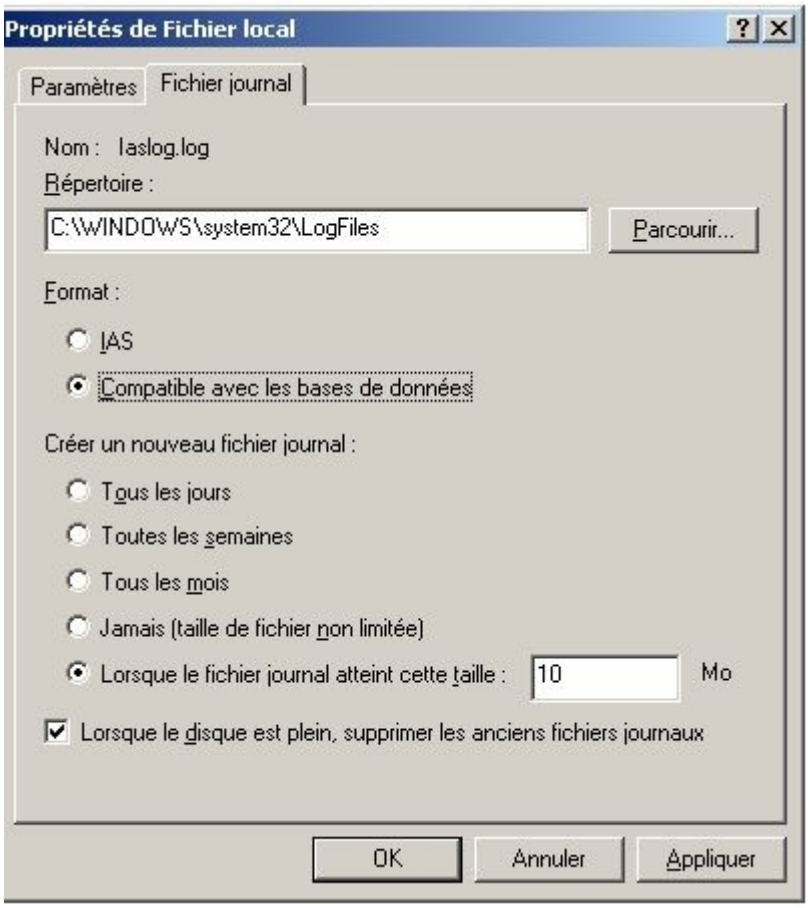


Dans l'onglet cryptage, je n'ai laissé que 128 bits, ce qui doit imposer une version de IE avec le cryptage 128 bits.
Dans un premier temps, j'avais tout laissé afin de ne pas avoir une source de blocage ici.

Enfin, ne pas oublier les logs (sinon Fabrice va me tuer !)

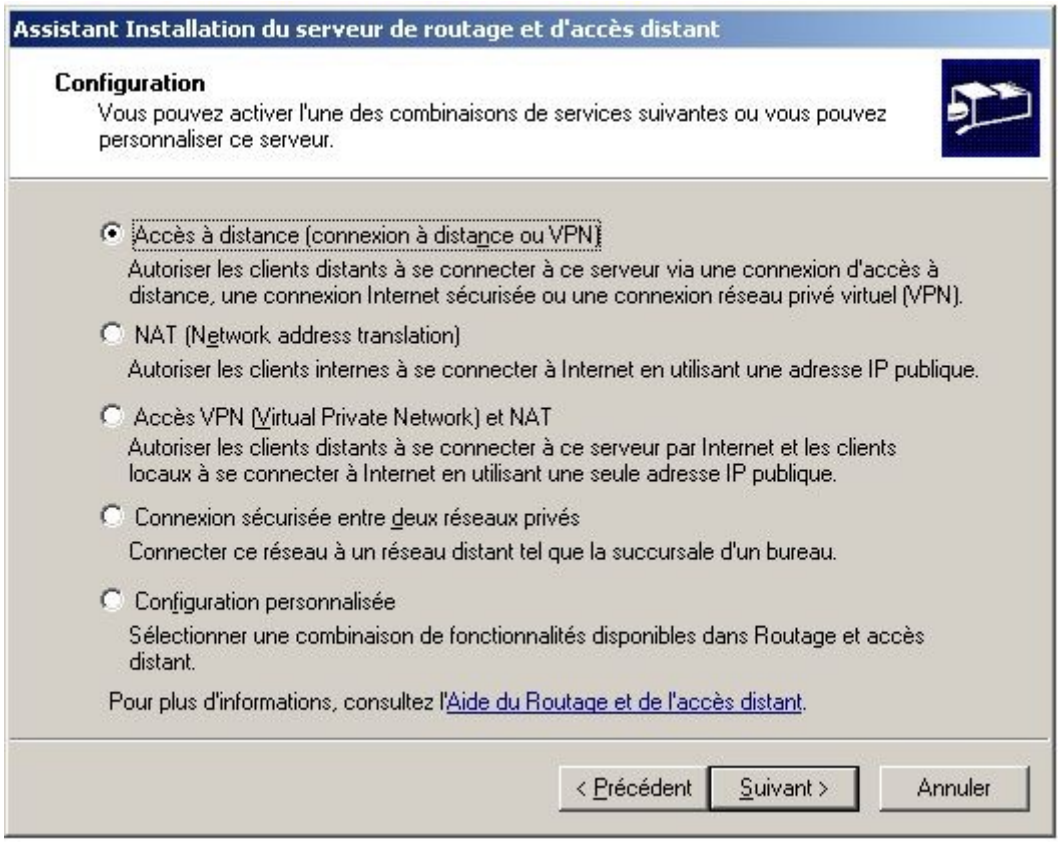


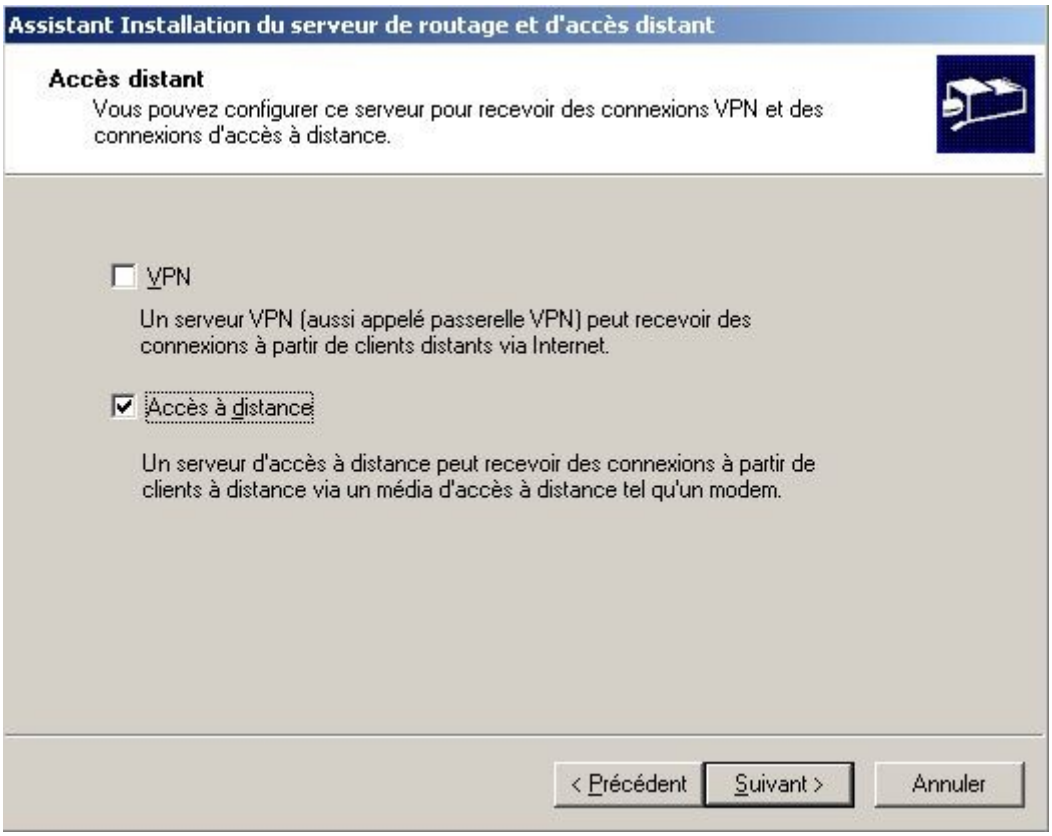


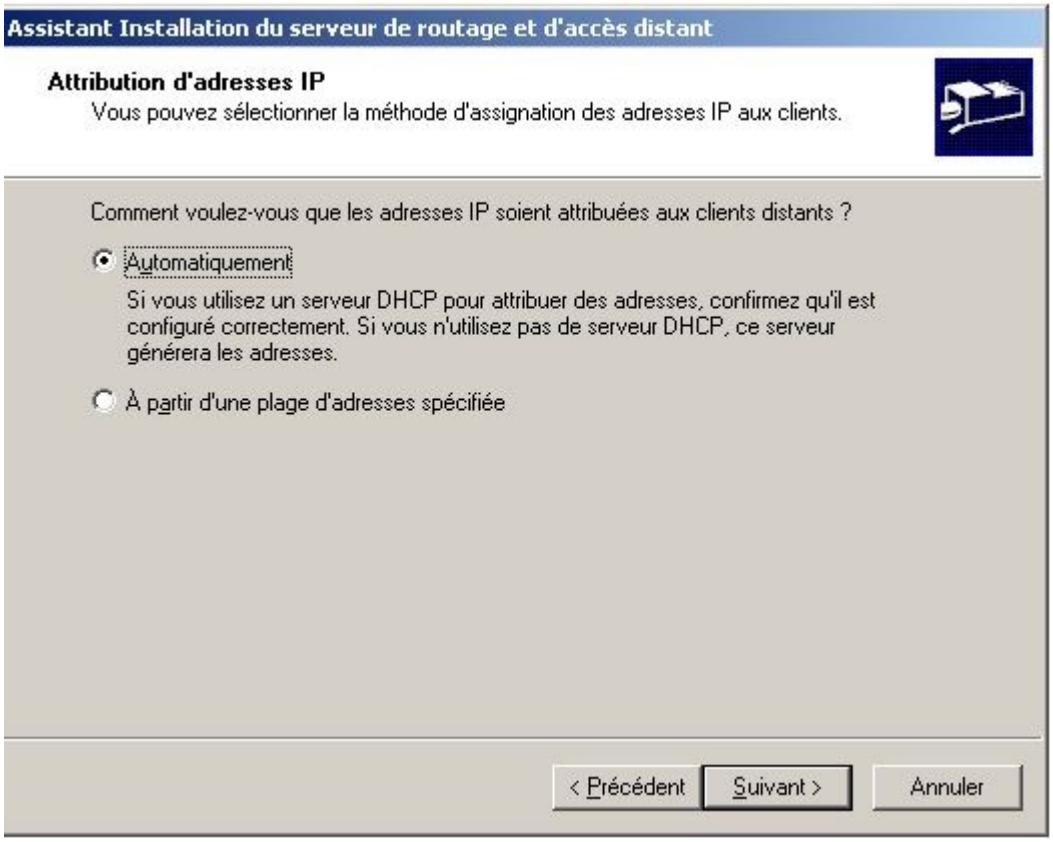

Propriétés de Fichier local
Paramètres
Fichier journal
Nom : Iaslog.log
Répertoire :
C:\WINDOWS\system32\LogFiles
Parcourir...
Format :
IAS
Compatible avec les bases de données
Créer un nouveau fichier journal :
Tous les jours
Toutes les semaines
Tous les mois
Jamais (taille de fichier non limitée)
Lorsque le fichier journal atteint cette taille :
10
Mo
Lorsque le disque est plein, supprimer les anciens fichiers journaux
OK
Annuler
Appliquer

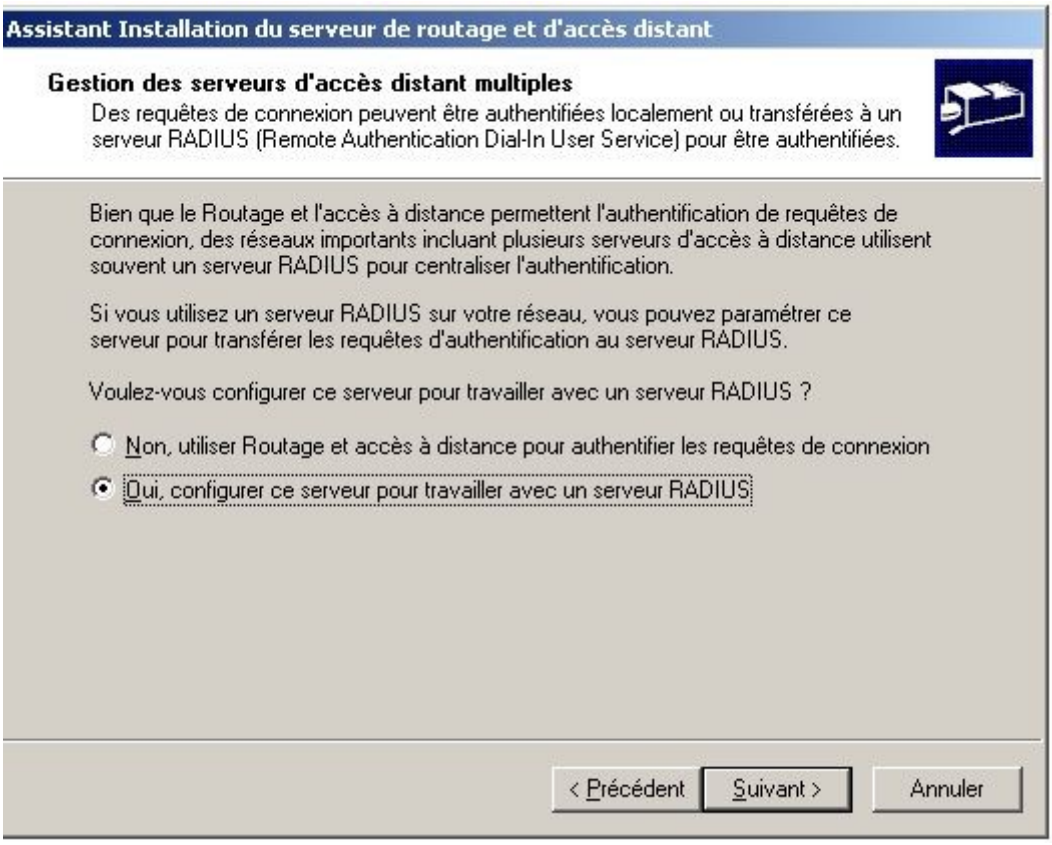
Si l'on veut utiliser DHCP pour ses clients sans fil, il faudra configurer le routage et accès distant.

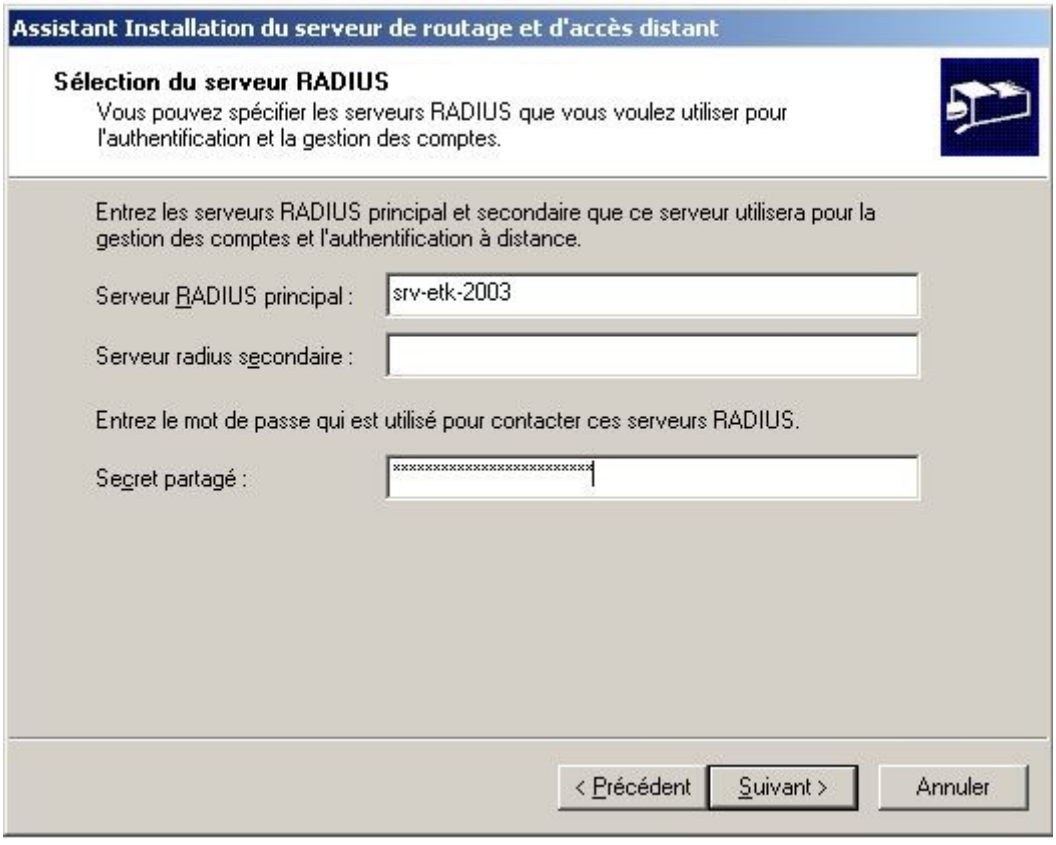
Lancer routage et accès distant dans outils d'administration.



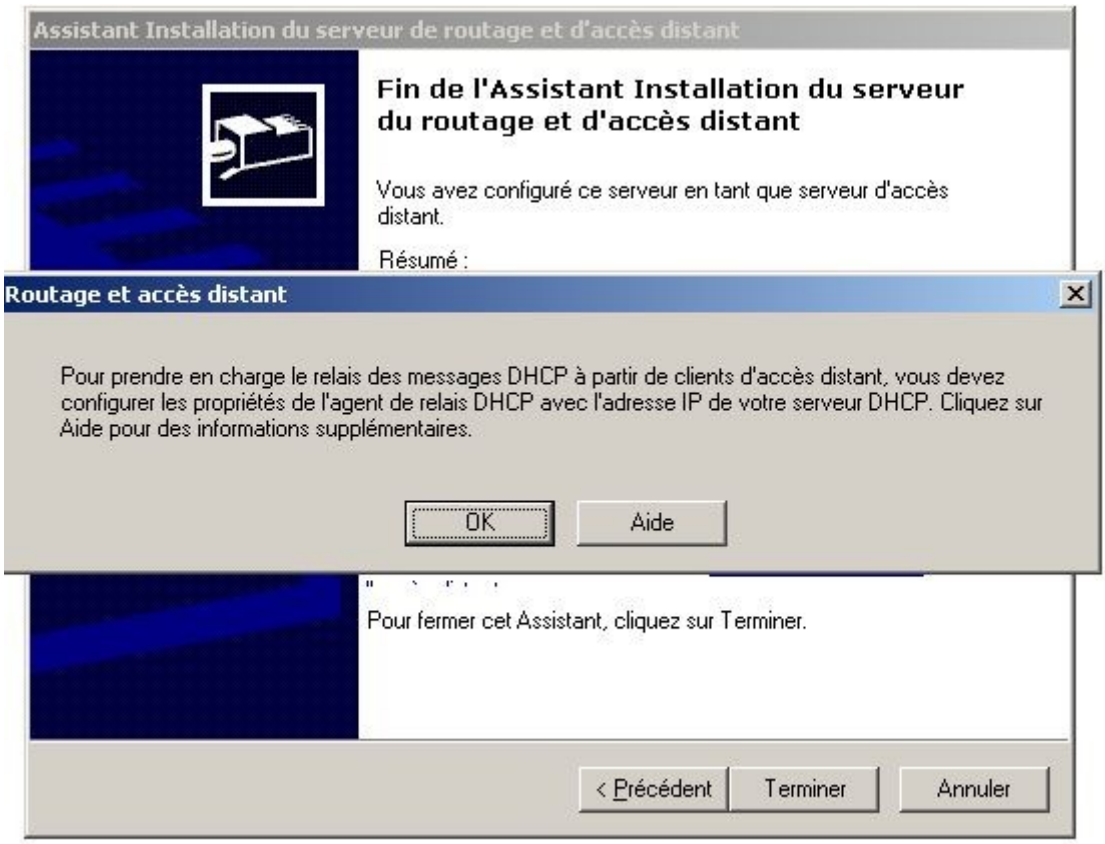

Assistant Installation du serveur de routage et d'accès distant
Accès distant
Vous pouvez configurer ce serveur pour recevoir des connexions VPN et des connexions d'accès à distance.
VPN
Un serveur VPN (aussi appelé passerelle VPN) peut recevoir des connexions à partir de clients distants via Internet.
Accès à distance
Un serveur d'accès à distance peut recevoir des connexions à partir de clients à distance via un média d'accès à distance tel qu'un modem.
< Précédent
Suivant >
Annuler


Assistant Installation du serveur de routage et d'accès distant
Attribution d'adresses IP
Vous pouvez sélectionner la méthode d'assignation des adresses IP aux clients.
Comment voulez-vous que les adresses IP soient attribuées aux clients distants ?
Automatiquement
Si vous utilisez un serveur DHCP pour attribuer des adresses, confirmez qu'il est configuré correctement. Si vous n'utilisez pas de serveur DHCP, ce serveur générera les adresses.
À partir d'une plage d'adresses spécifiée
< Précédent
Suivant >
Annuler



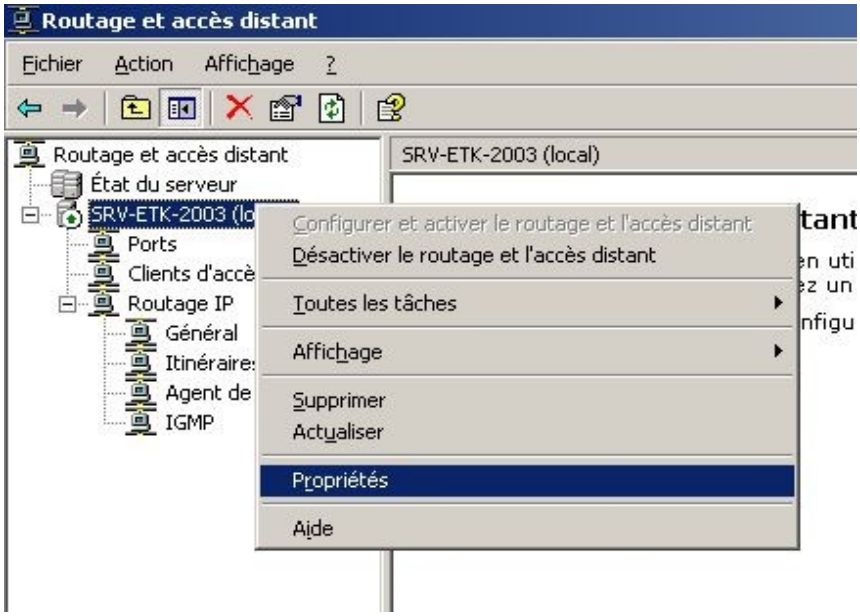


On peut installer un serveur radius secondaire, mais je ne sais pas comment indiquer à mon point d'accès un deuxième radius...

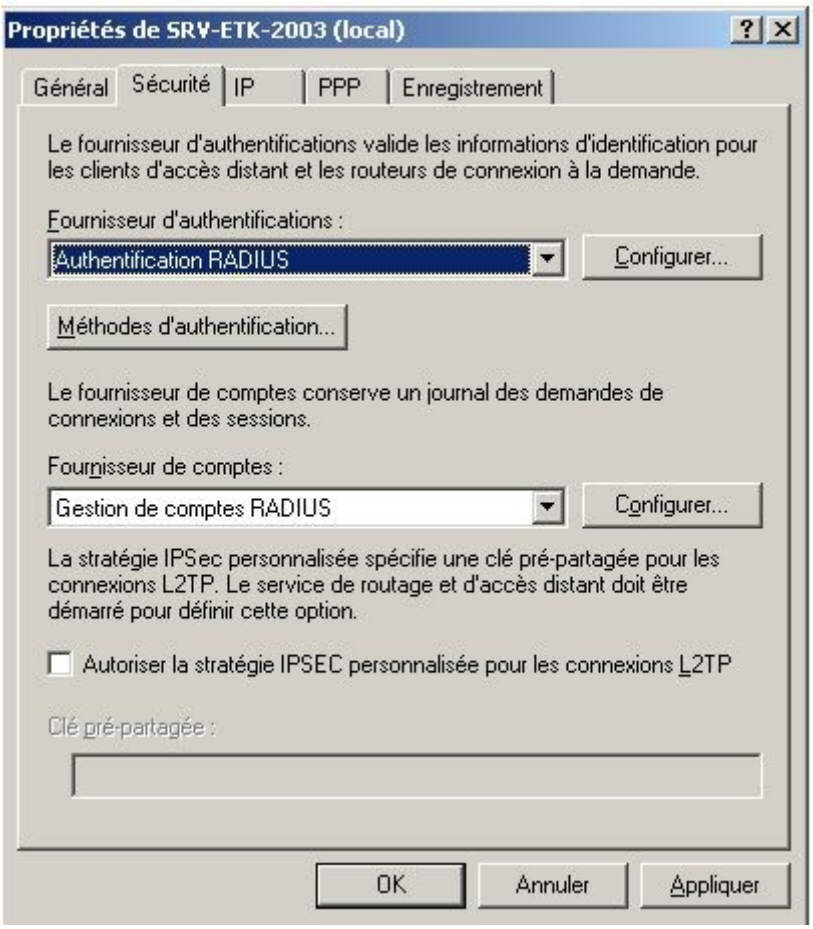


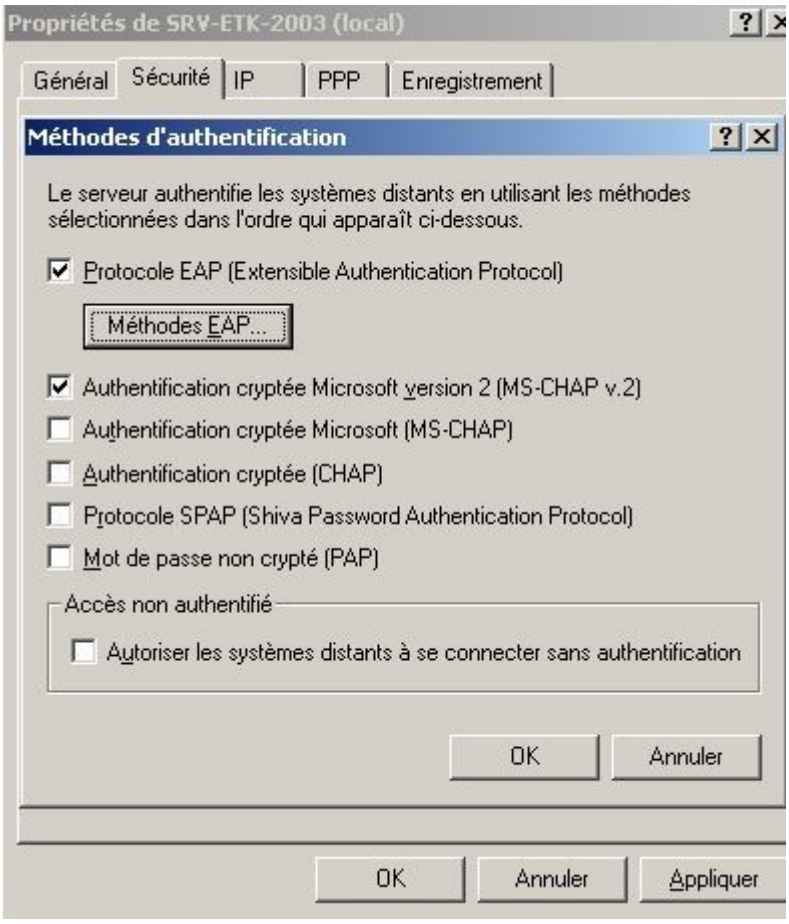
Le service prend en charge, le relais DHCP.

Je vais ensuite dans propriétés

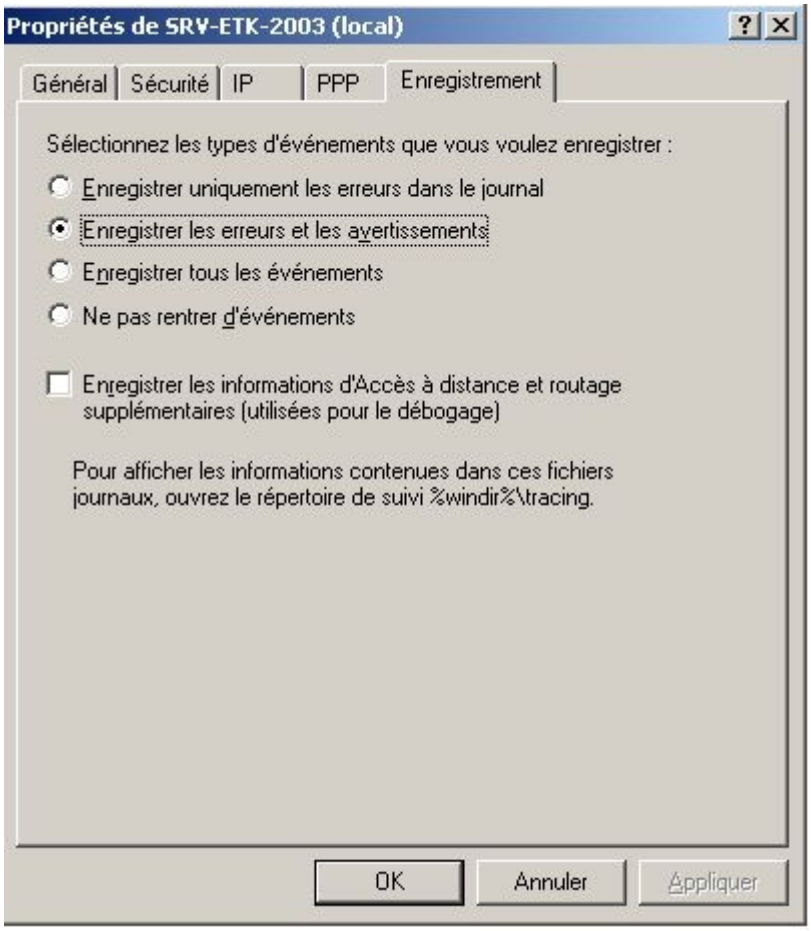


Pour configurer la sécurité :





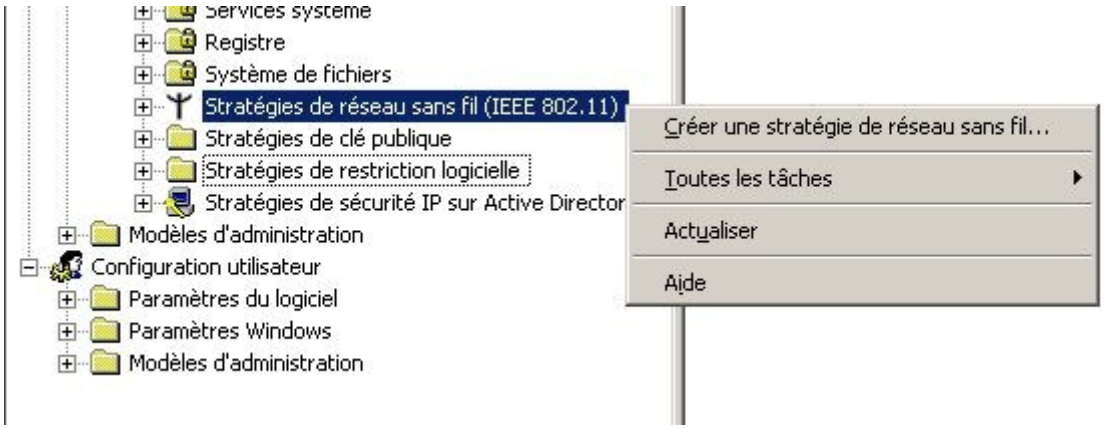
Finalement, pour le débogage. Noter que le suivi se trouve dans %WINDIR%\TRACING

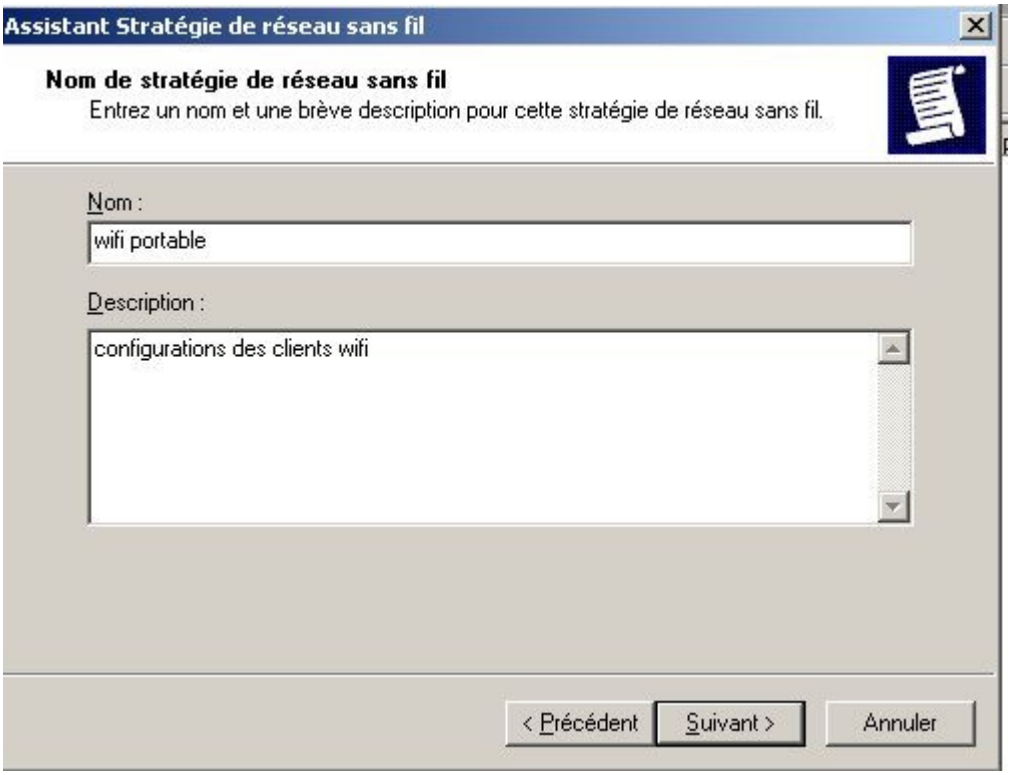


Configuration des clients (portables par exemple)

La configuration peut se faire au niveau des stratégies, ou directement sur chacun des portables. Si l'on configure au niveau des stratégies avec une OU qui contient les portables par exemple il y aura juste à brancher une fois le portable sur le réseau avec un cordon réseau, pour qu'il prenne sa stratégie et c'est tout !

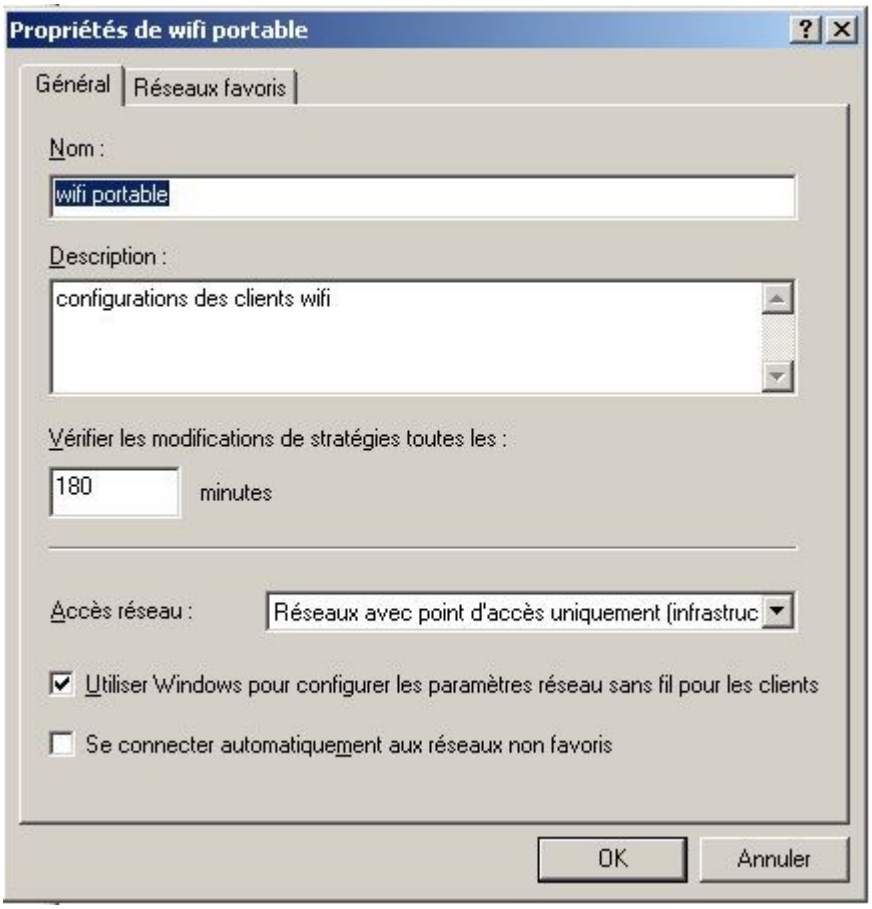
Configuration au niveau stratégies



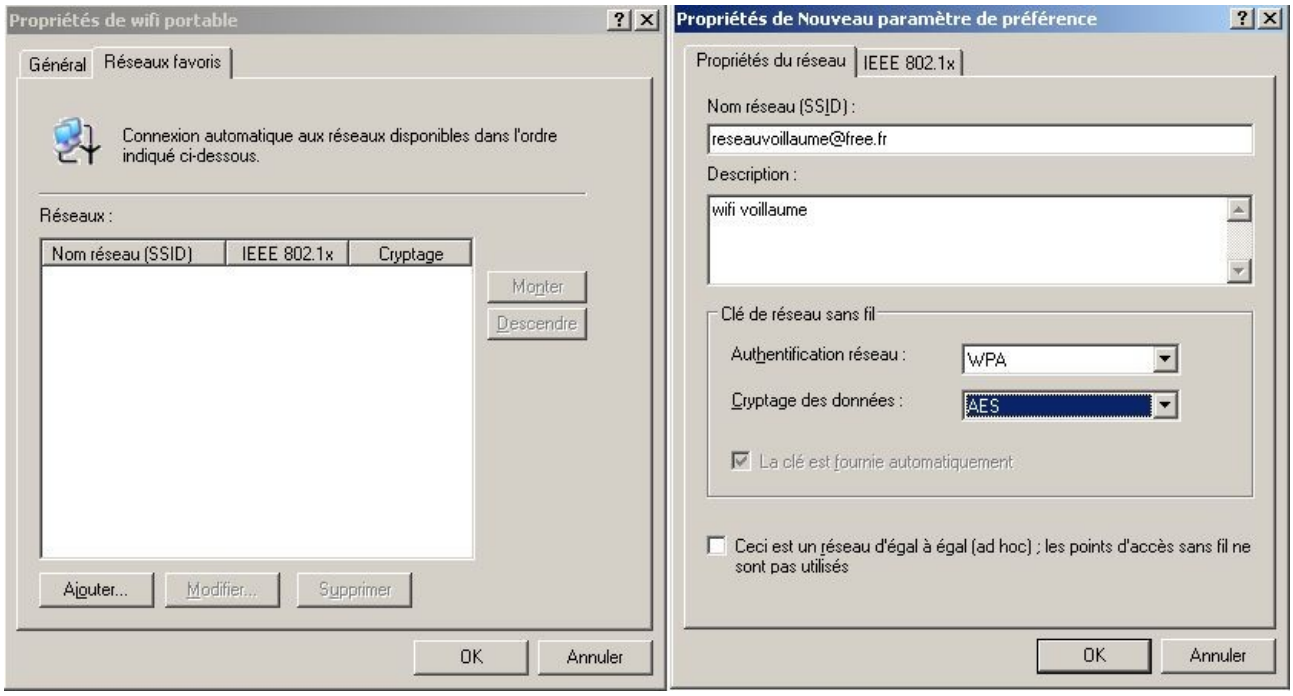


On donne ici le nom de la stratégie.

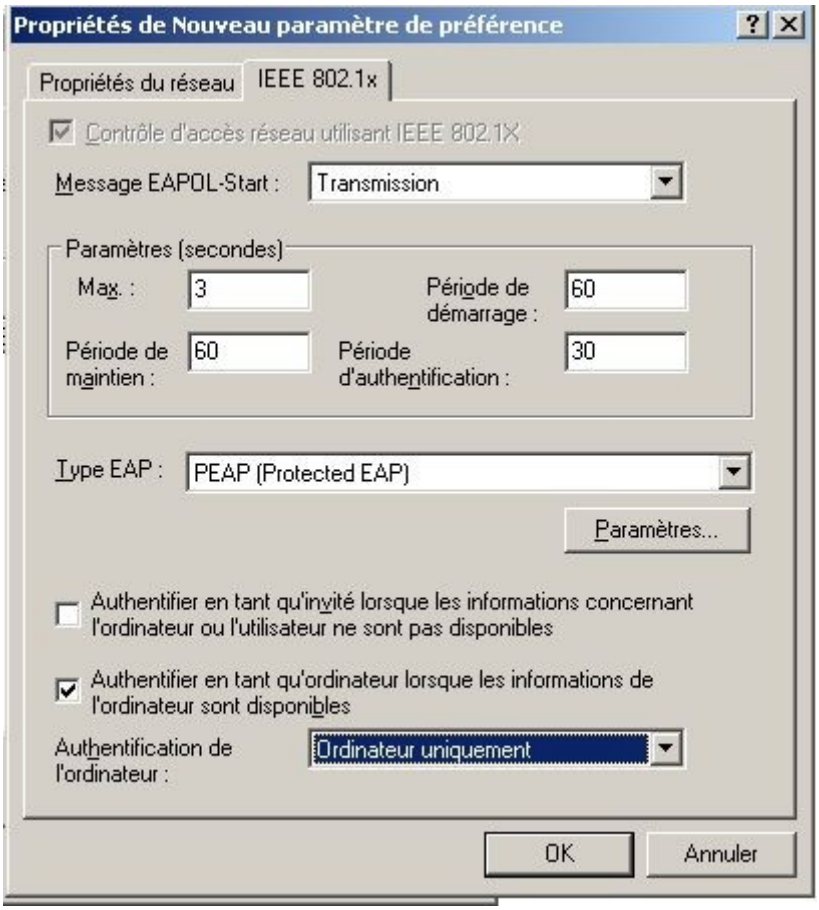
À la fin de la création de la stratégie, on nous propose de la configurer.



On ajoute un réseau wifi



Et on configure le 802.1x

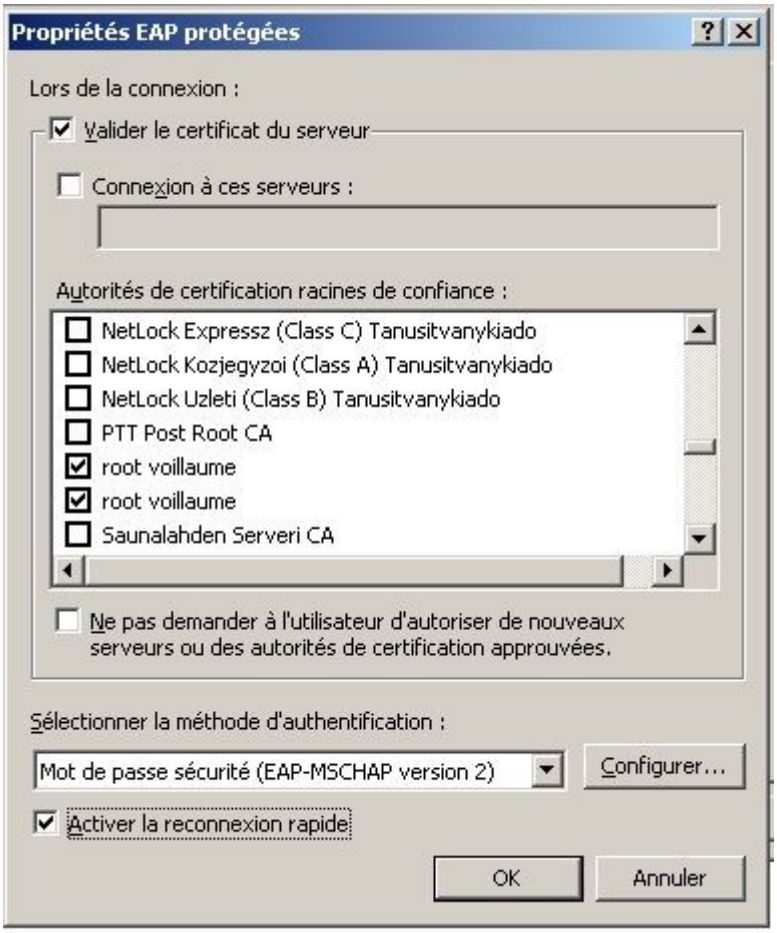


Ici je suis un peu paumé je me contente de choisir type PEAP et d'aller dans paramètres

Que dire du message EAPOL-START ?

Que dire des trois options pour l'authentification de l'ordinateur ?

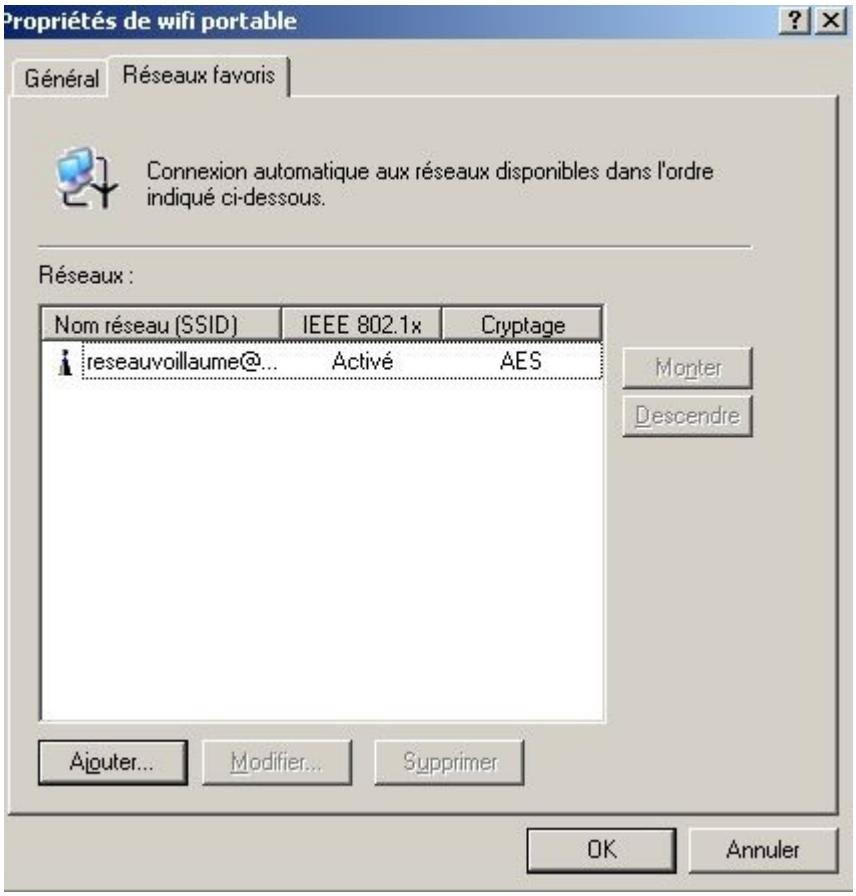
Ici, on valide l'autorité de certification :



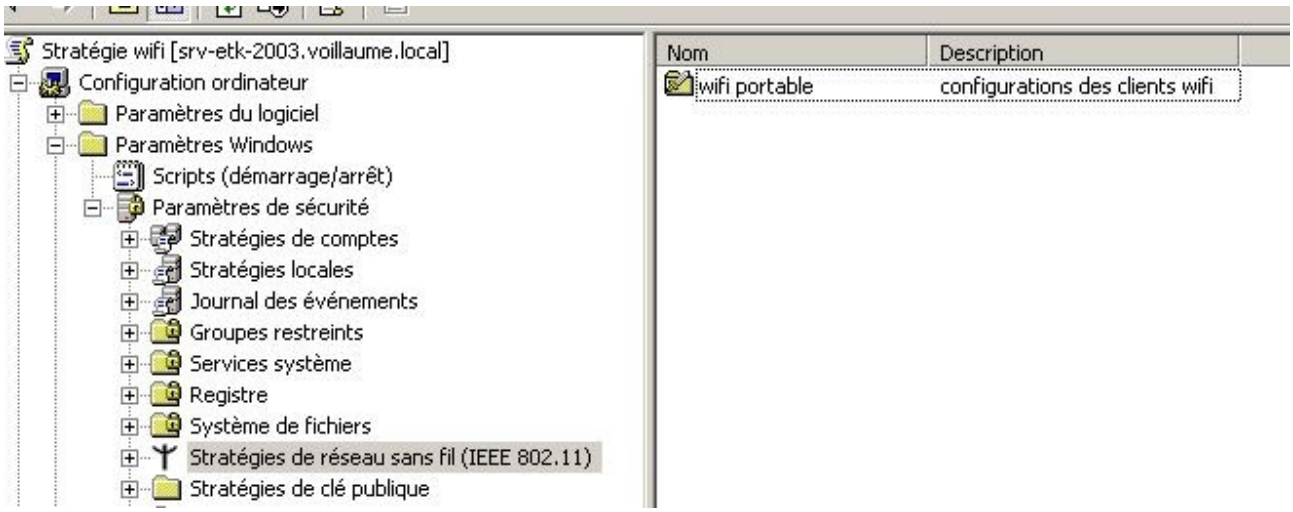
Pourquoi deux certificats / serveurs ici ?

On active la reconnexion rapide (pour un changement de point d'accès, je crois).

On vérifie que dans *configurer*, la case est bien cochée



Toutes les options présentes ici ne se retrouvent pas dans la configuration réseau de l'ordinateur ?

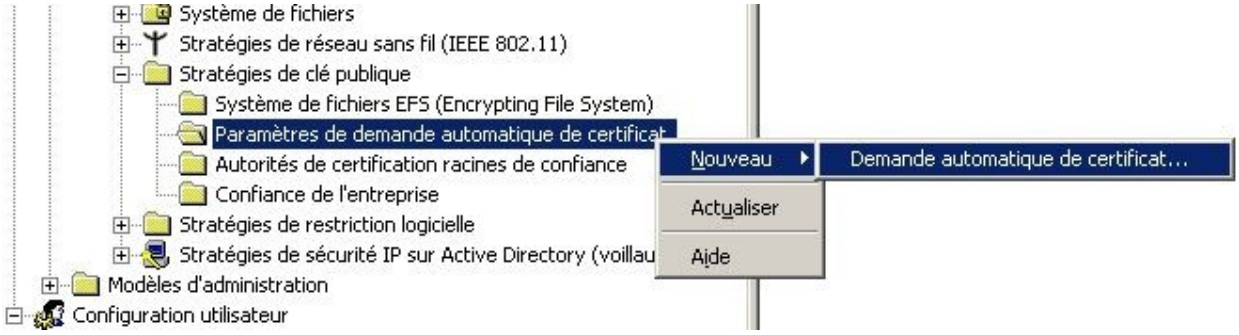


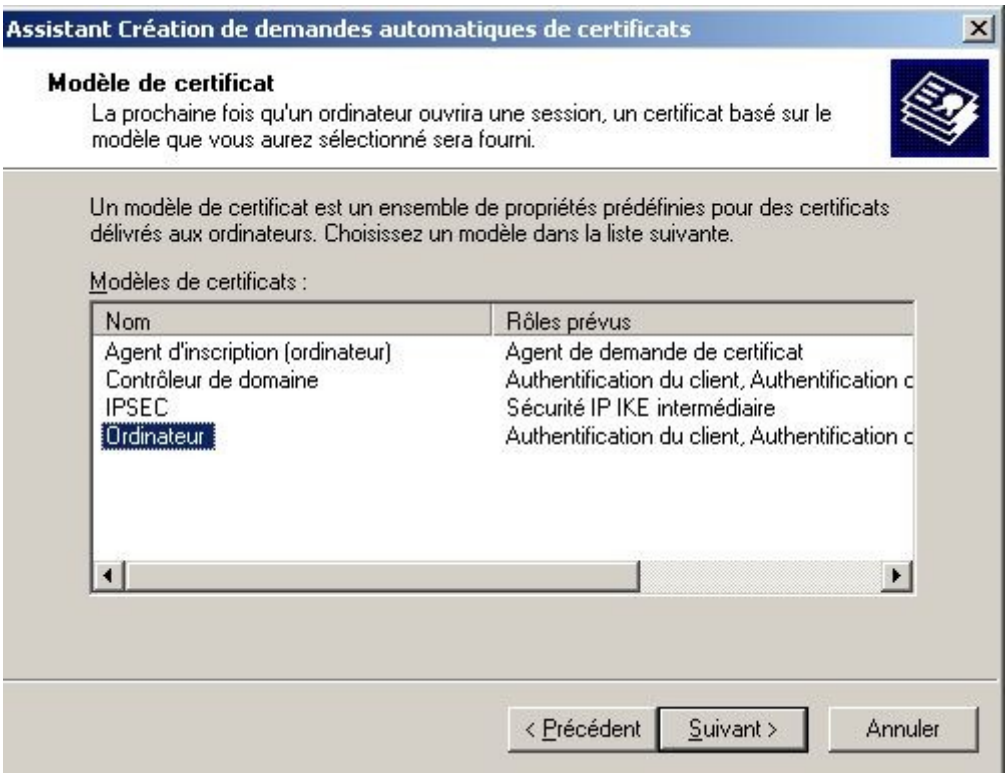
Cette partie n'est pas nécessaire dans le cadre d'une authentification MS-CHAP V2

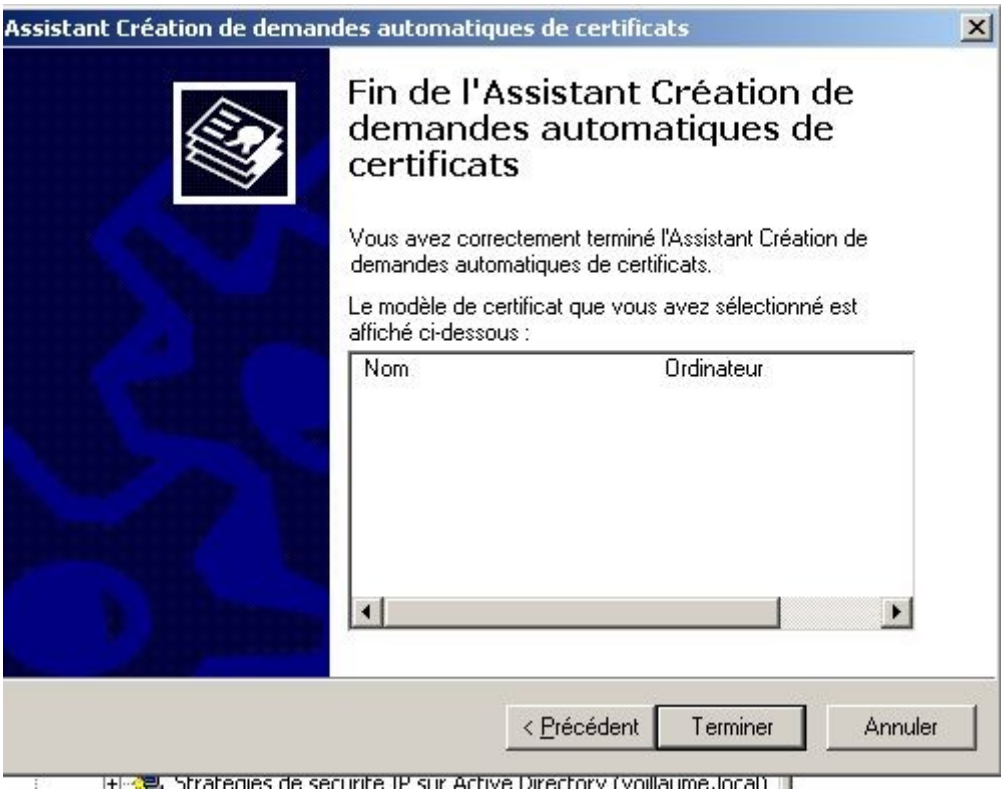
Par contre, elle peut être utilisée en EAP TLS que je n'ai pas testé

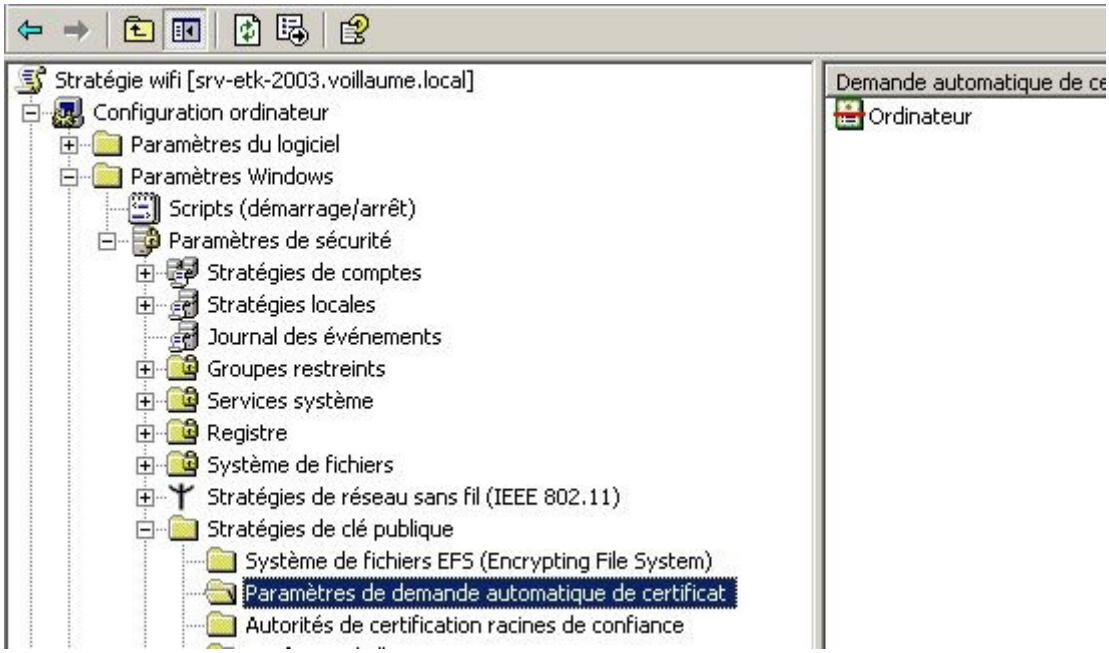
Configuration de l'inscription automatique des certificats ordinateurs

Elle permet d'installer un certificat machine automatiquement.



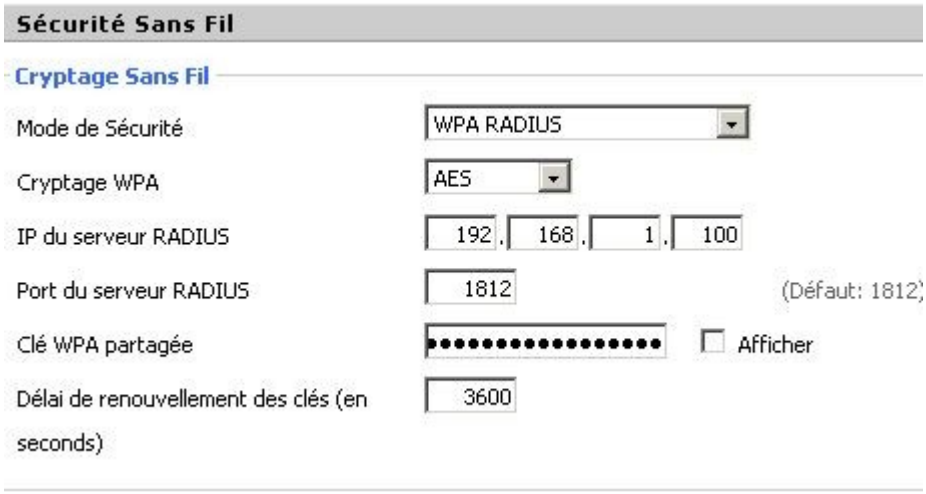



Assistant Création de demandes automatiques de certificats
Fin de l'Assistant Création de demandes automatiques de certificats
Vous avez correctement terminé l'Assistant Création de demandes automatiques de certificats.
Le modèle de certificat que vous avez sélectionné est affiché ci-dessous :
Nom
Ordinateur
< Précédent
Terminer
Annuler


Stratégie wifi [srv-etk-2003.voillaume.local]
Configuration ordinateur
Paramètres du logiciel
Paramètres Windows
Scripts (démarrage/arrêt)
Paramètres de sécurité
Stratégies de comptes
Stratégies locales
Journal des événements
Groupes restreints
Services système
Registre
Système de fichiers
Stratégies de réseau sans fil (IEEE 802.11)
Stratégies de clé publique
Système de fichiers EFS (Encrypting File System)
Paramètres de demande automatique de certificat
Autorités de certification racines de confiance
Demande automatique de ce
Ordinateur

Configuration du point d'accès :

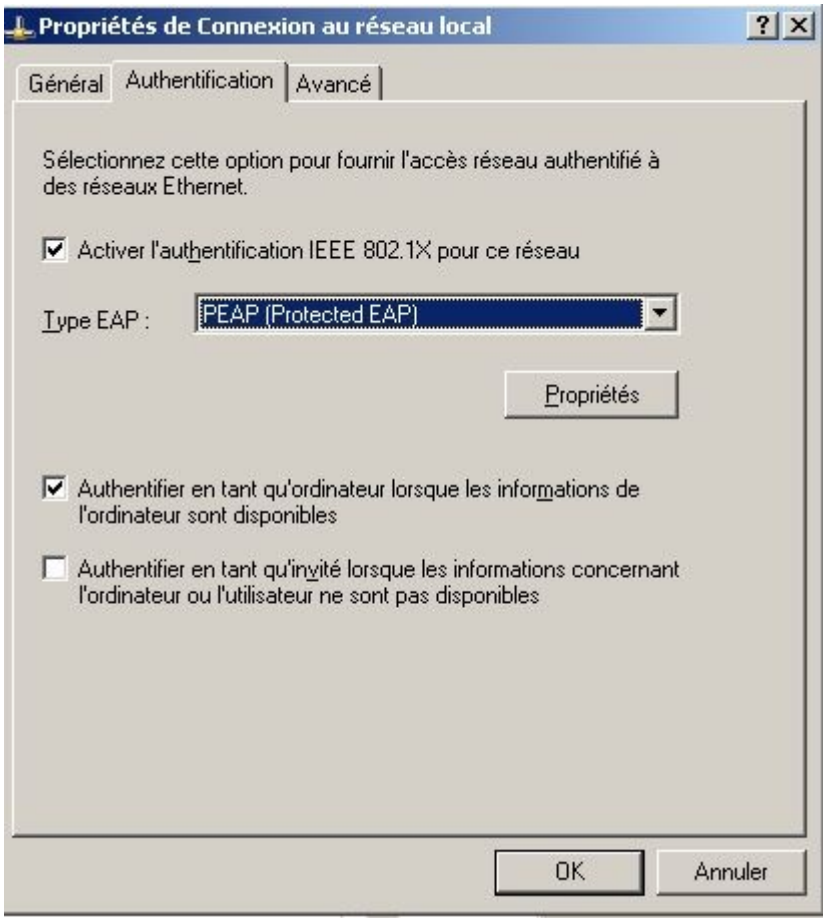
Pas grand chose à mettre sur le point d'accès, la clé partagée avec le serveur radius. L'adresse IP du serveur radius (le serveur avec IAS IIS, etc.) Le port donné ici est celui par défaut de Windows 2003

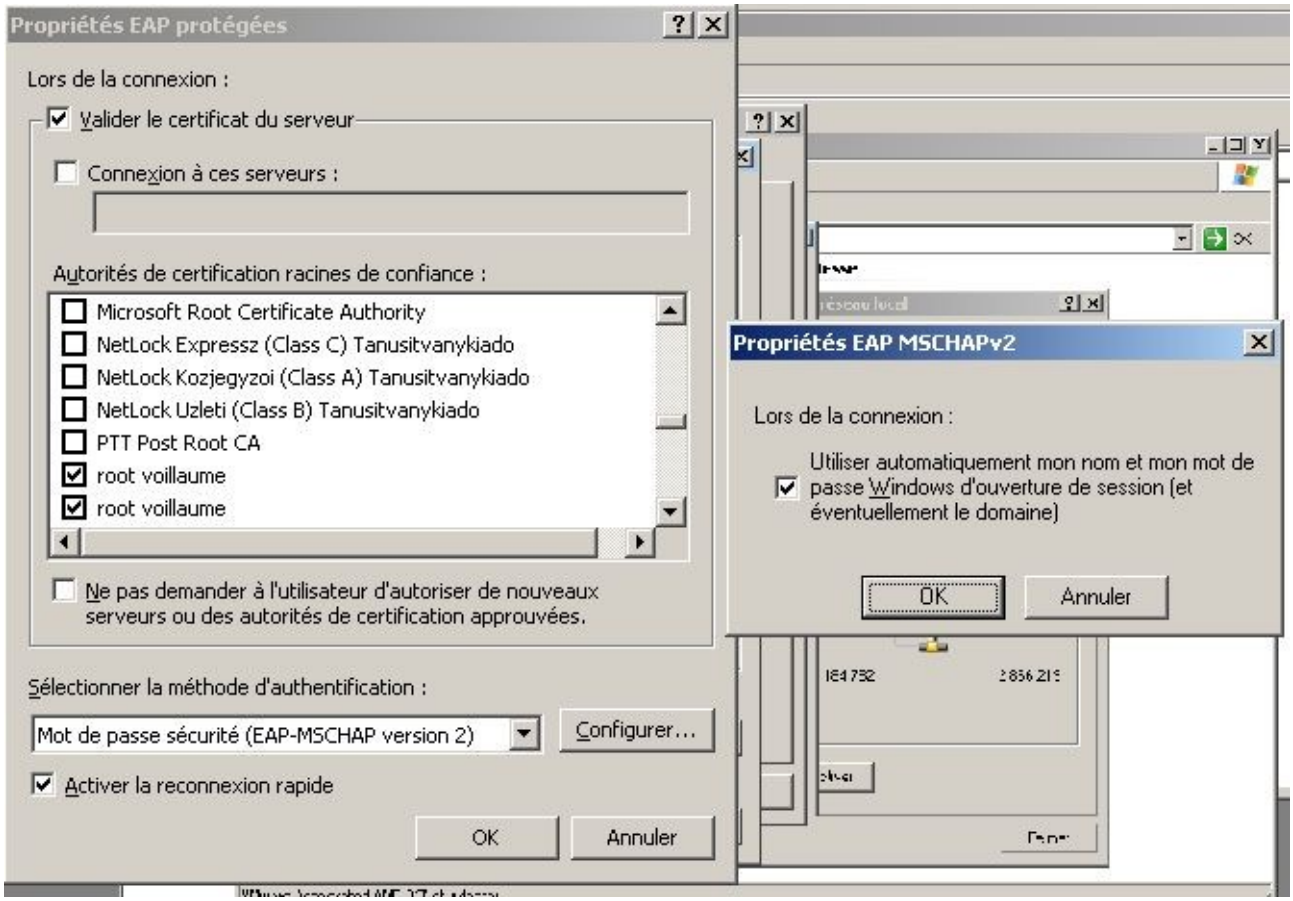


192,168,1,10 = IP serveur ETK hébergeant IAS, certificats, AD

Configuration du client à la main (sans passer par les GPO)

Pour vérifier que ç marche pour le premier portable.




Propriétés EAP protégées
Lors de la connexion :
Valider le certificat du serveur
Connexion à ces serveurs :
Autorités de certification racines de confiance :
Microsoft Root Certificate Authority
NetLock Expressz (Class C) Tanusitvanykiado
NetLock Kozjegyzoi (Class A) Tanusitvanykiado
NetLock Uzleti (Class B) Tanusitvanykiado
PTT Post Root CA
root voillaume
root voillaume
Ne pas demander à l'utilisateur d'autoriser de nouveaux serveurs ou des autorités de certification approuvées.
Sélectionner la méthode d'authentification :
Mot de passe sécurité (EAP-MSCHAP version 2)
Configurer...
Activer la reconnexion rapide
OK
Annuler
Propriétés EAP MSCHAPv2
Lors de la connexion :
Utiliser automatiquement mon nom et mon mot de passe Windows d'ouverture de session (et éventuellement le domaine)
OK
Annuler

Gestion du sans-fil par stratégies de groupe :

On a ici plusieurs options pour traiter les stratégies :

La détection d'une liaison lente de stratégie de groupe annule une partie des éléments des stratégies

Le seuil est à 500 Kbps soit 0,5 Mbps ce qui sur un point d'accès 54 Mbps ne devrait pas poser de problème.

On peut agir de deux façons pour modifier cela
- le seuil de détection de liaison (ou tout simplement désactiver la détection de liaison lente
- la prise en compte ou non des parties de stratégie en cas de liaison lente

Les paramètres de sécurité ne peuvent pas être désactivés

Ce tableau indique si la partie de stratégie est prise en compte en :

Liaison lente : si la liaison lente était détectée

peut être forcé : on peut les GPO, forcer l'application de ces parties de GPO même si une liaison lente est détectée

Arrière-plan : partie des GPO régulièrement mises à jour
(via GPO) : contrôlable via GPO

Paramètre	(liaison lente) (peut être forcé)	Arrière-plan par défaut (via GPO)
Maintenance d'IE	(Non) (Oui)	OUI
Installation logicielle	(NON) (NON)	Non (NON)
redirection de dossier	(NON) (NON)	Non (NON)
scripts	(NON) (OUI)	Oui
sécurité IP	Non (OUI)	
stratégie sans fil	Non (OUI)	OUI
Récupération EFS		
Quotas de disque		OUI
Paramètre machine	Non (OUI)	OUI

Quelques liens :

http://www.microsoft.com/windows2000/fr/server/help/default.asp?url=/windows2000/fr/server/help/sag_RASS_MSCHAPv2.htm

http://www.schneier.com/paper-pptpv2-fr.html

http://www.informit.com/guides/content.asp?g=security&seqNum=72&rl=1

http://phares.ac-rennes.fr/_fichiers_/seriaE/admin/Telech/WiFi_PresentationDAIP.pdf