

V.P.N. sous Win XP

Table des matières

V.P.N. sous Win XP.....	1
Introduction aux Réseaux Privés Virtuels.....	1
Royaume : « realm ».....	3
Qui fait une demande de « realm » ?.....	3
Quels sont les « realms » actifs ?.....	3
Obtenir un certificat, des droits.....	4
Rencontrer son correspondant réseau/wifi.....	4
Délivrance du certificat.....	4
Droits.....	4
Les serveurs VPN en usage à l'UFC.....	4
Création de la connexion réseau V.P.N. sous windows XP.....	5
Importation du certificat.....	20
Complément de configuration pour le navigateur Internet Explorer 7.....	31

Introduction aux Réseaux Privés Virtuels

L'objectif d'un VPN est simple. Il s'agit de sécuriser des échanges de données en utilisant comme support un réseau non sécurisé comme par exemple le réseau Internet. Un VPN est également un bon candidat pour la sécurisation de flux informatiques à travers un réseau WIFI.

Définition d'un VPN (Virtual Private Network) :

Décomposons l'expression VPN.

Network : un réseau est constitué de plusieurs machines qui peuvent communiquer entre elles d'une façon ou d'une autre. Ces machines peuvent être dans un même endroit physiquement ou dispersées, et les méthodes de communication sont diverses.

Private : privé veut dire que les communications entre deux ou plusieurs machines sont secrètes et donc inaccessibles pour une machine ne participant pas à la communication privée.

Virtual : dans le concept de virtuel, nous retiendrons l'émulation d'une fonction d'un objet qui n'est pas vraiment là. Un réseau virtuel n'est pas un réseau physique, mais émuler pour faire croire à un réseau physique.

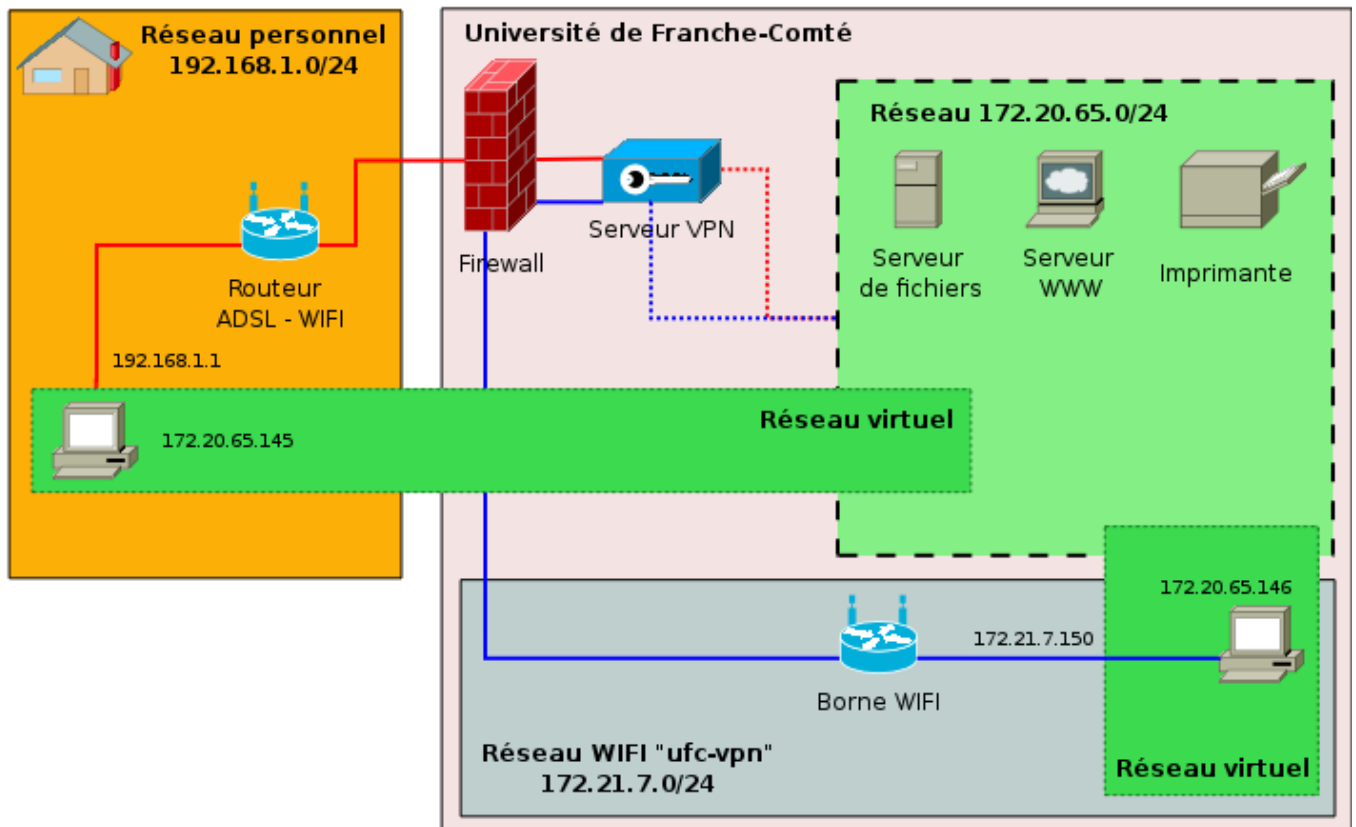
Un réseau privé virtuel est donc l'association de ces trois concepts. Une fois en place, il vous offre la possibilité d'utiliser un réseau public non sécurisé pour créer un réseau privé (données cryptées) et y faire circuler des données.

Quelques explications :

En général, les RPV permettent à des utilisateurs de se servir de leur connexion Internet de type ADSL pour accéder à leur réseau professionnel de manière transparente. Un fois connecté, l'utilisateur peut atteindre les ressources (espaces disques, imprimantes, etc) fournies par ce réseau.

Dans le schéma ci-dessous, nous voyons un utilisateur travaillant depuis son ordinateur personnel. Il emprunte donc son accès Internet personnel pour se connecter à travers un VPN à son réseau universitaire. Les traits rouges montrent les liens physiques réels. La zone « Réseau virtuel » montre le réseau virtuel mis en place entre son domicile et le réseau interne après l'établissement de la connexion.

Une autre connexion est établie entre un poste utilisant le réseau WIFI universitaire. L'utilisation du réseau WIFI "ufc-vpn" permet de créer un réseau virtuel entre ce poste nomade et un réseau interne. Tout comme le premier exemple, le poste fait partie du réseau interne et peut user de toutes les ressources mises à sa disposition.



Quelles possibilités pour le VPN ?

Concrètement, que pourra faire l'utilisateur accédant au réseau de l'UFC en utilisant le VPN ?

Tout simplement, exactement ce qu'il peut faire sur son PC lorsque celui-ci est branché physiquement au réseau lorsqu'il est au bureau, par exemple récupérer ses courriers électroniques sur le serveur de messagerie, consulter des sites Intranet (ceux qui ne sont pas accessibles depuis l'extérieur de l'UFC), accéder à ses fichiers sur les serveurs de fichiers, etc. Tout ceci via Internet et de façon sécurisée.

La sécurité du VPN mise en place à l'UFC dépend de trois éléments :

- l'authentification machine ;
- le cryptage des données ;
- l'authentification de l'utilisateur.

L'authentification machine : les deux machines s'assurent mutuellement qu'elles ont les droits pour communiquer entre elles (vérification du certificat).

Le cryptage des données s'effectue par l'échange de clefs.

L'authentification de l'utilisateur est faite à travers l'annuaire LDAP de l'UFC ou d'un serveur d'authentification cascadié (laboratoires, UFR ...).

Parmi les termes fréquemment employés, nous retrouverons « realm », « certificat ».

Royaume : « realm »

Un « royaume » (« realm » dans le monde de Radius) est, d'une manière plus restrictive pour le projet VPN de l'UFC, l'association d'un nom vis à vis d'un réseau de l'UFC.

Lors d'une connexion VPN, vous indiquerez le « realm » auquel vous voulez rattacher votre session VPN.

Par exemple, si je crée une session VPN avec l'identifiant « monNom@lifc-edu » et que je suis autorisé à me connecter sur le « realm » « @lifc-edu », ma machine obtiendra une adresse IP du réseau « lifc-edu », c'est-à-dire, une adresse dans le réseau 172.20.128.0/24.

Qui fait une demande de « realm » ?

Les demandes de « realms » seront effectuées par les correspondants réseaux de l'UFC. Le CRI étudiera avec eux les besoins et créera si nécessaire le « realm » proposé.

La création d'un « realm » est une opération lourde et ne se justifie que pour des besoins importants.

Quels sont les « realms » actifs ?

Pour l'ensemble des personnels et étudiants de l'Université de Franche-Comté, il existe un « realm » par défaut « @ufc » qui donne accès à un réseau interne de l'UFC, comme le faisait le service du PPP.

Pour les laboratoires, des royaumes spécifiques sont créés, en voici quelques exemples :

à Besançon :

- « @lifc-edu » sur le réseau 172.20.128.0/24 (vlan 7)
- « @lifc-lab » sur le réseau 172.20.65.0/24 (vlan 9)
- « @femto-st » sur le réseau 172.20.208.64/26 (vlan 44)

à Belfort :

- « @iutm »

Obtenir un certificat, des droits

L'utilisation du VPN n'est pas anonyme, ni anodine. Ce service vous permet de vous connecter dans l'un des réseaux de l'Université de Franche-Comté depuis n'importe quel réseau extérieur ayant la possibilité de créer un VPN IPSEC (protocole ESP).

Cette connexion doit s'établir sans problème depuis chez vous ou depuis un accès WiFi (SSID ufc-vpn) de l'UFC.

Vos droits s'acquièrent en deux phases :

- 1) récupérer un certificat pour accéder à la machine VPN ;
- 2) obtenir des droits sur un « realm ».

Rencontrer son correspondant réseau/wifi

Il est impératif que votre demande de certificat passe par le correspondant informatique de votre laboratoire ou de votre UFR, car il nous faut des renseignements sur votre identité et la machine pour laquelle le certificat sera délivré (PC windows/linux, MacOS).

Délivrance du certificat

Le certificat est généré par le CRI qui le fournira directement à l'utilisateur ou au correspondant réseau. Ce certificat de machine permet ensuite à la machine sur lequel il est installé, de se connecter et surtout d'être reconnu par le serveur VPN comme une machine valide.

Vous pouvez installer un même certificat sur plusieurs machines, mais une seule à la fois pourra effectuer une connexion sur le serveur VPN. Si vous avez des besoins multiples, il faudra demander plusieurs certificats.

Droits

Les droits sont attribués par le correspondant réseau qui est en charge des « realms » qui lui sont confiés. Le CRI pourra aussi vous attribuer des droits, mais ne le fera que sur le « realm » générique « @ufc ».

Les serveurs VPN en usage à l'UFC

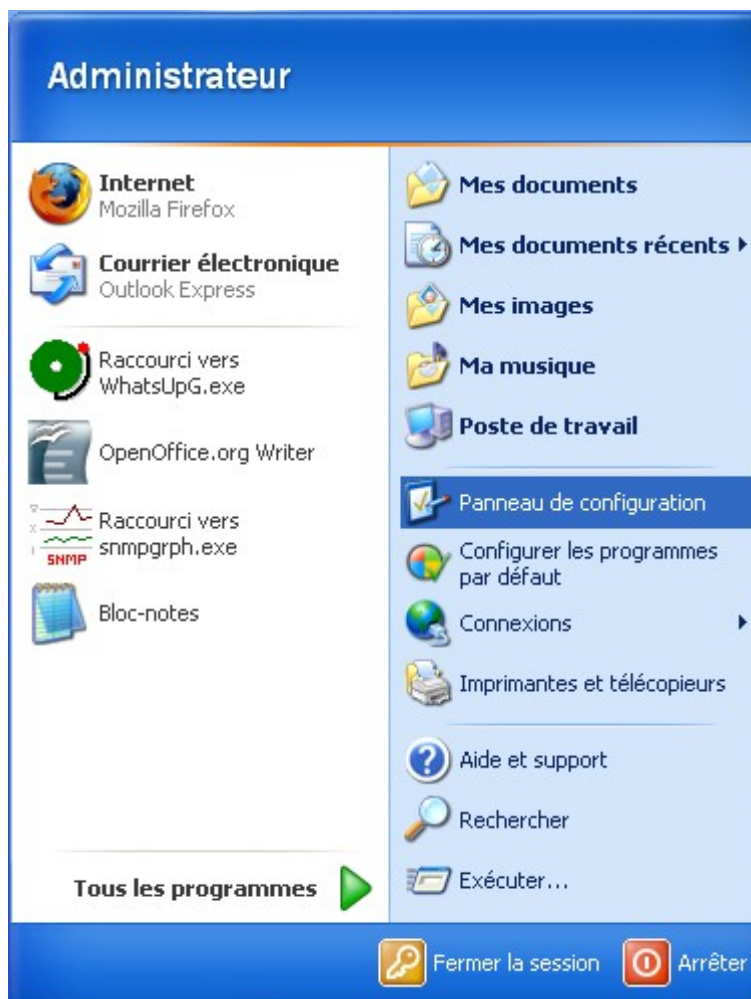
- | | | | |
|-----------------------------|----------|---------------|-----------------------------|
| • le serveur de test | test-vpn | 194.57.91.251 | actif jusqu'à fin juin 2008 |
| • le serveur de Besançon | vpn1 | 194.57.91.250 | actif début juin 2008 |
| • le serveur de Montbéliard | vpn2 | 194.57.89.97 | actif début juin 2008 |
| • le serveur de Belfort | vpn3 | 194.57.89.105 | actif début juin 2008 |

Création de la connexion réseau V.P.N. sous windows XP

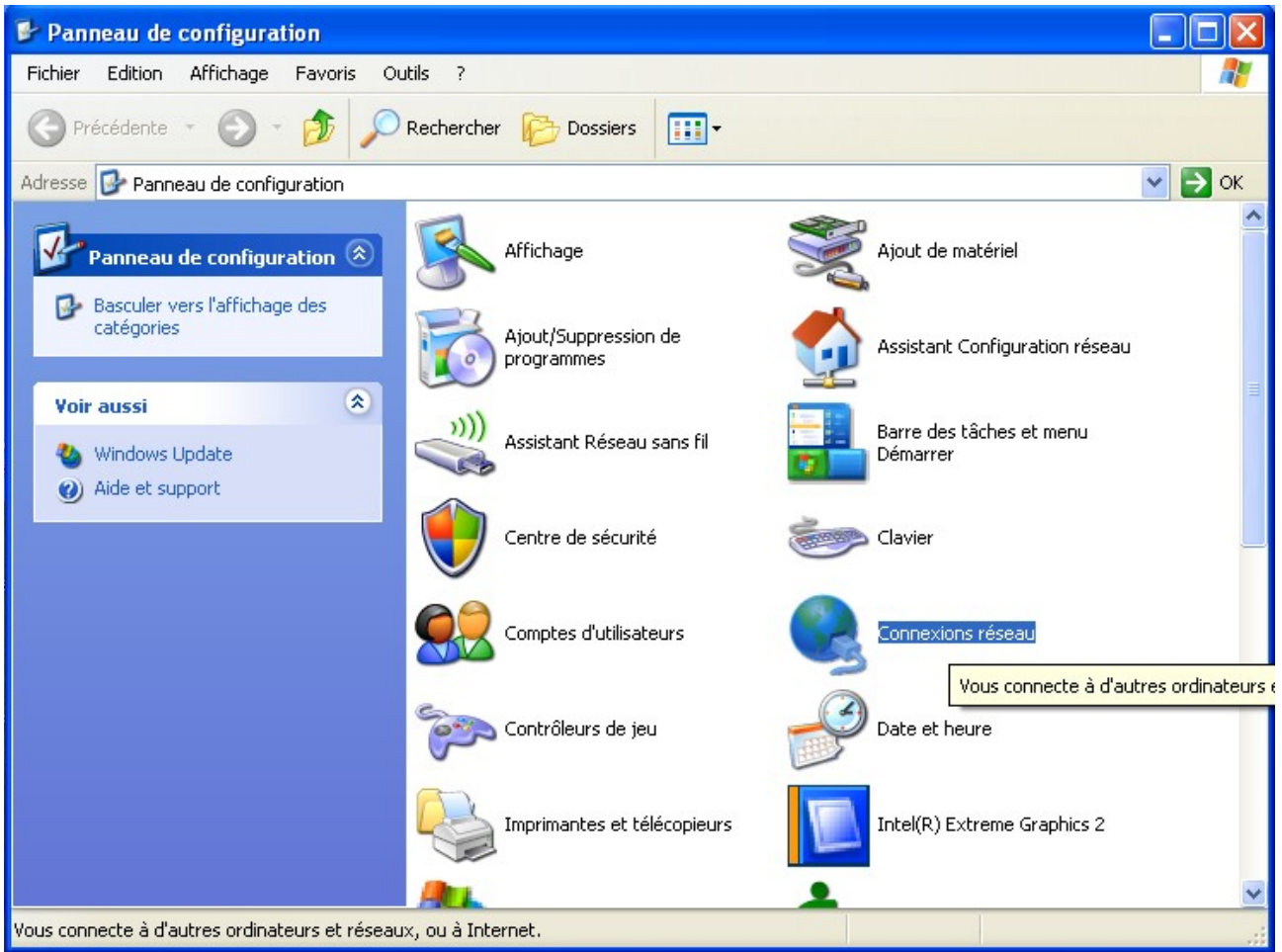
Attention, pour que votre connexion fonctionne, **il faut impérativement que vous ayez reçu votre certificat.**

Pour cela, veuillez suivre la procédure de remise des certificats comme indiquée page précédente et le chapitre Importation du certificat page 20 pour sa mise en place.

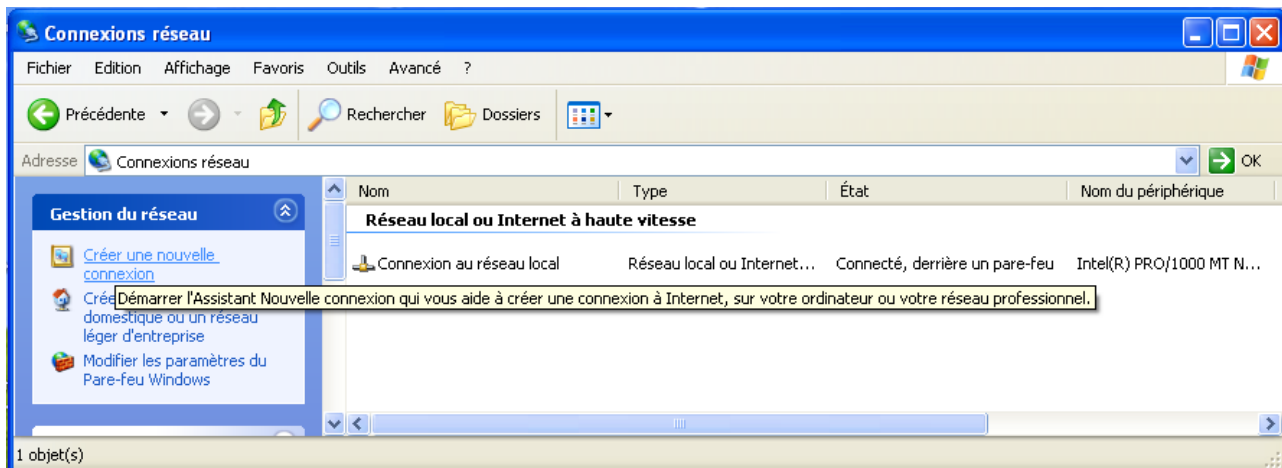
- Ouvrir le panneau de configuration



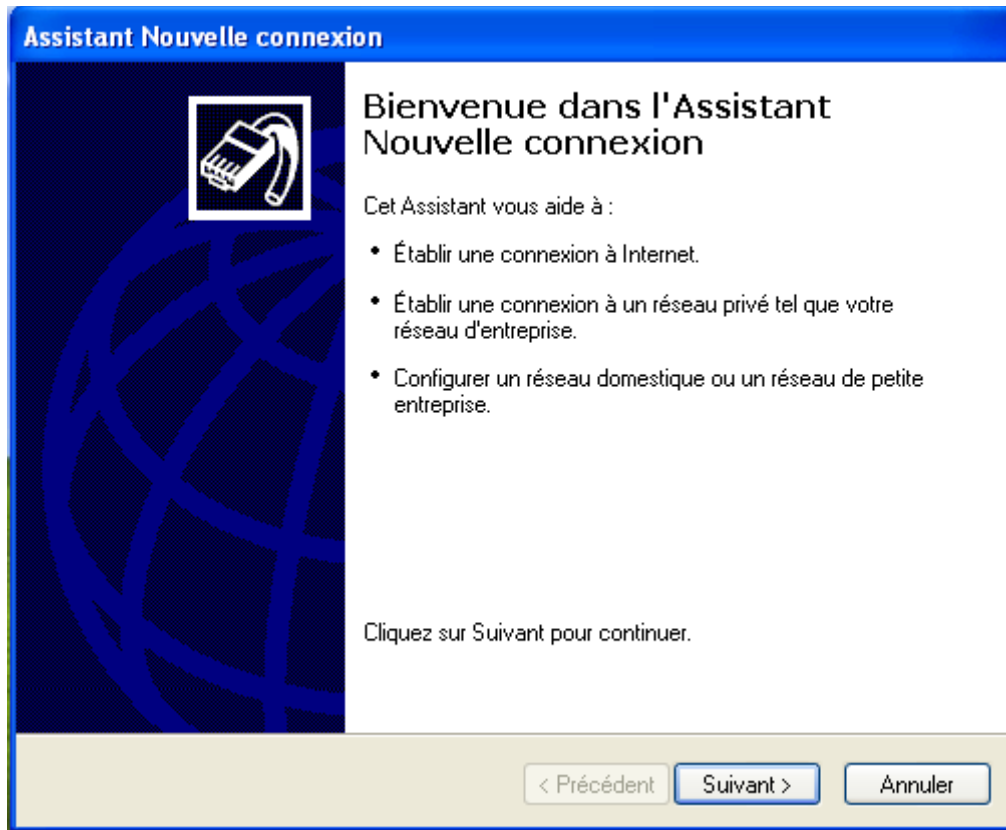
- Aller dans les « **Connexions réseaux** » du panneau de configuration



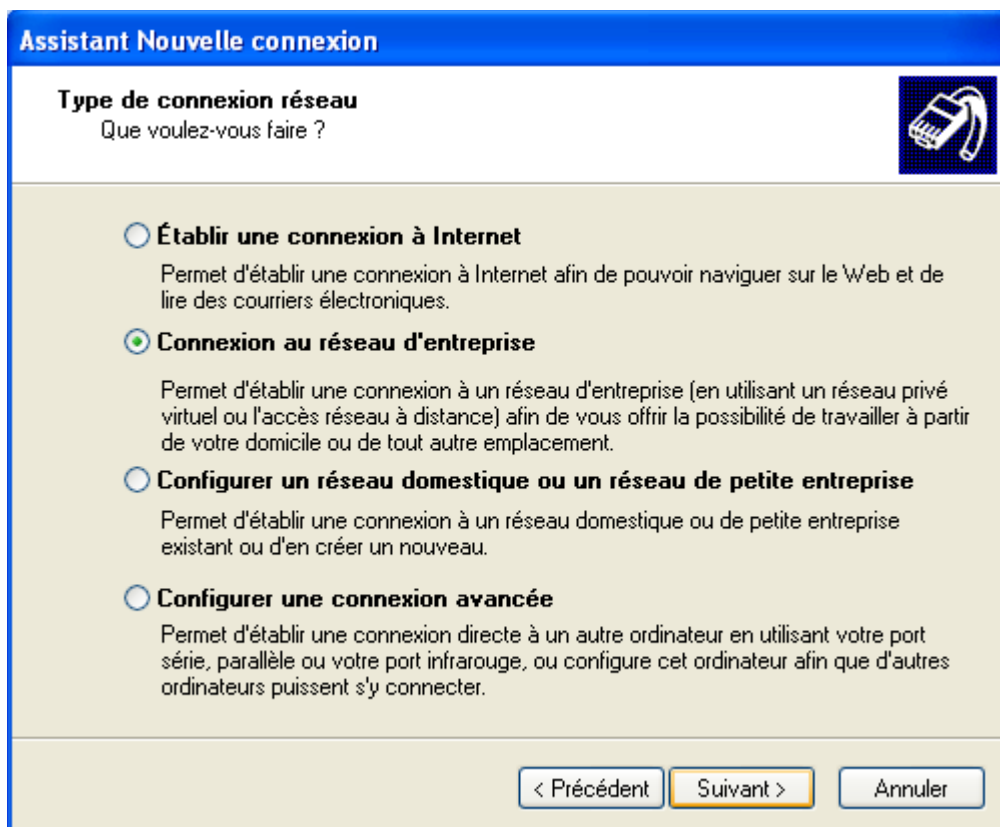
- Cliquer sur « **Créer une nouvelle connexion** » pour lancer l'assistant Nouvelle connexion.



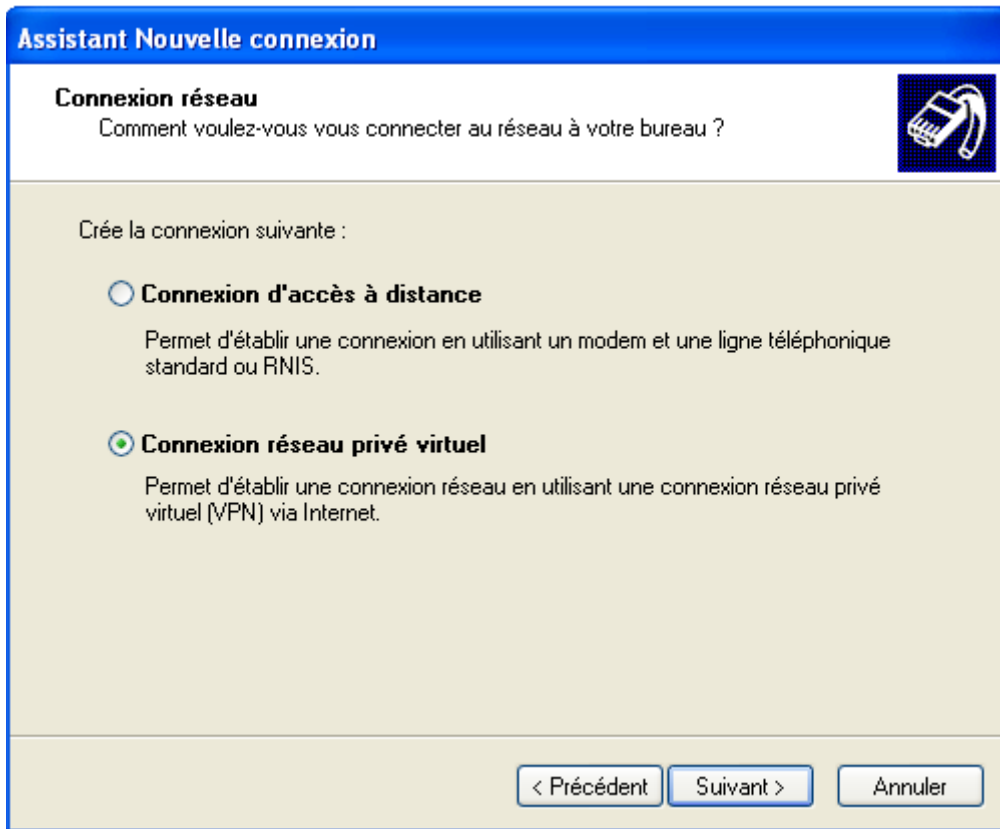
- L'assistant Nouvelle Connexion s'ouvre, cliquer sur « **Suivant** »



- Choisir « **Connexion au réseau d'entreprise** » puis « **Suivant** »



- Choisir « **Connexion réseau privé virtuel** » puis « **Suivant** »



- Donner le nom de cette nouvelle connexion VPN en tant que « **Nom de la société** » puis « **Suivant** »

Assistant Nouvelle connexion

Nom de la connexion
Spécifiez un nom pour cette connexion à votre lieu de travail.

Entrez un nom pour cette connexion dans la case suivante.

Nom de la société

UFC-VPN

Par exemple, vous pouvez entrer le nom de votre lieu de travail ou le nom du serveur auquel vous allez vous connecter.

< Précédent Suivant > Annuler

- Choisir « **Ne pas établir la connexion initiale** » puis « **Suivant** »
- Entrer ensuite le **nom ou l'IP** du serveur VPN auquel vous voulez vous connecter (voir la rubrique ci-dessus "Les serveurs VPN en usage à l'UFC") puis « **Suivant** »

Assistant Nouvelle connexion

Sélection de serveur VPN
Quel est le nom ou l'adresse du serveur VPN ?

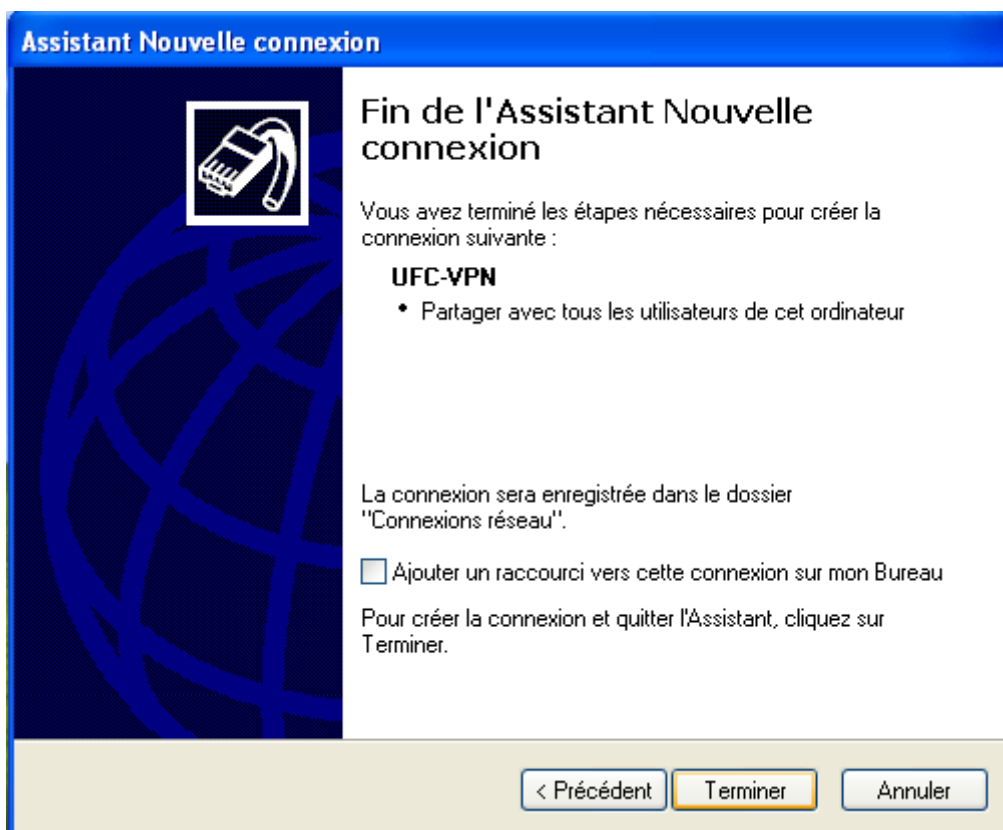
Entrez le nom d'hôte ou l'adresse IP (Internet Protocol) de l'ordinateur auquel vous voulez vous connecter.

Nom d'hôte ou adresse IP (par exemple, microsoft.com ou 157.54.0.1) :

|

< Précédent Suivant > Annuler

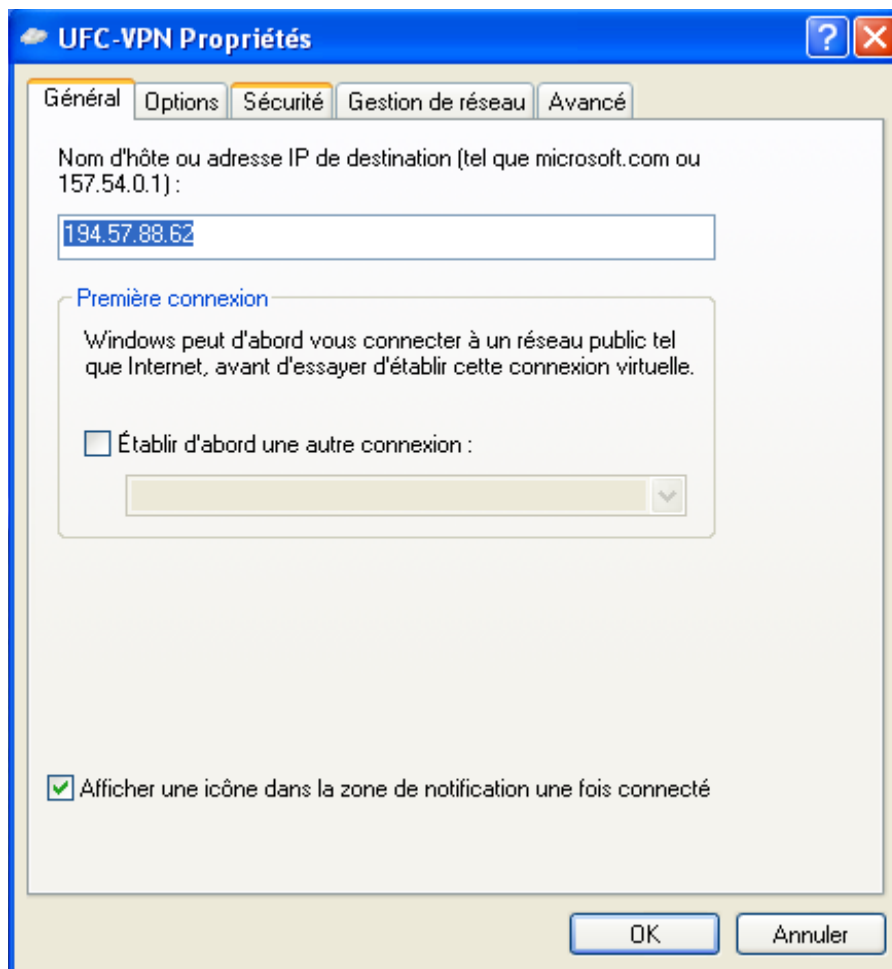
- Fermer l'assistant Nouvelle connexion avec le bouton **Terminer**



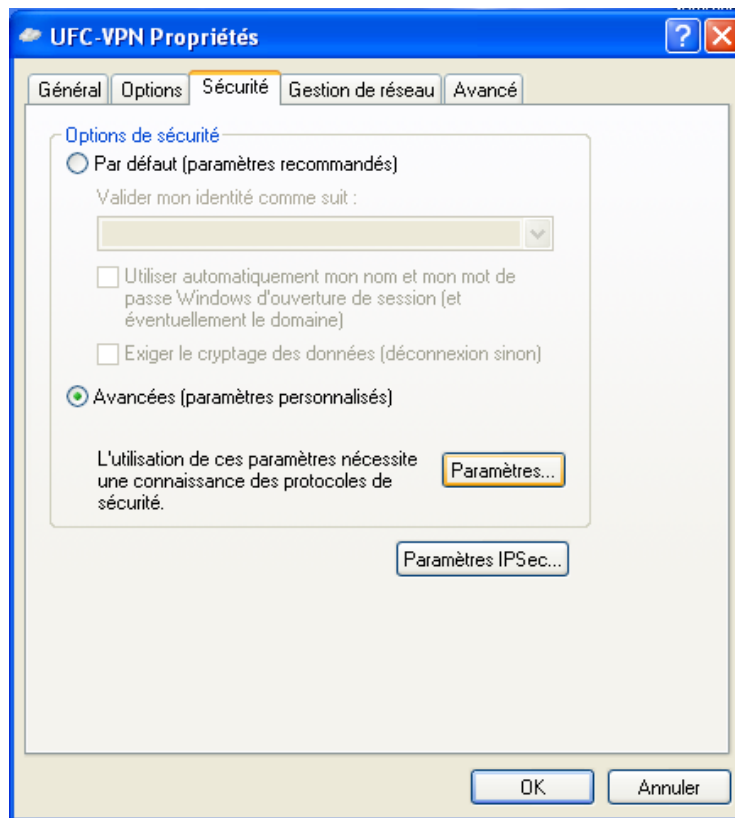
- Une fenêtre apparaît alors pour vous permettre de vous connectez.



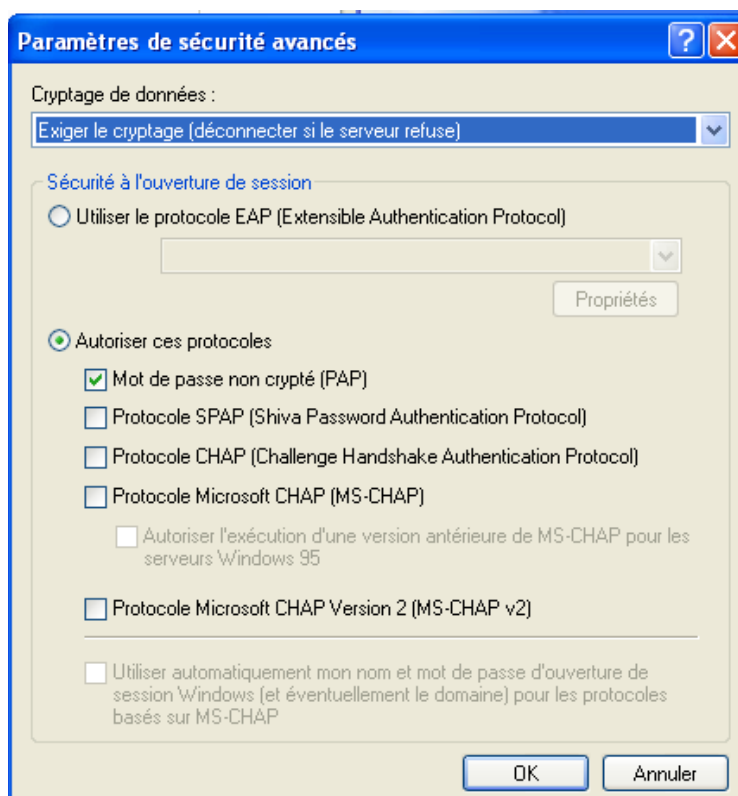
- Cliquer sur « **Propriétés** »



- Cliquer sur l'onglet « **Sécurité** » :
- choisir l'Option de sécurité « **Avancées** (paramètres personnalisés) »
- cliquer sur « **Paramètres...** »



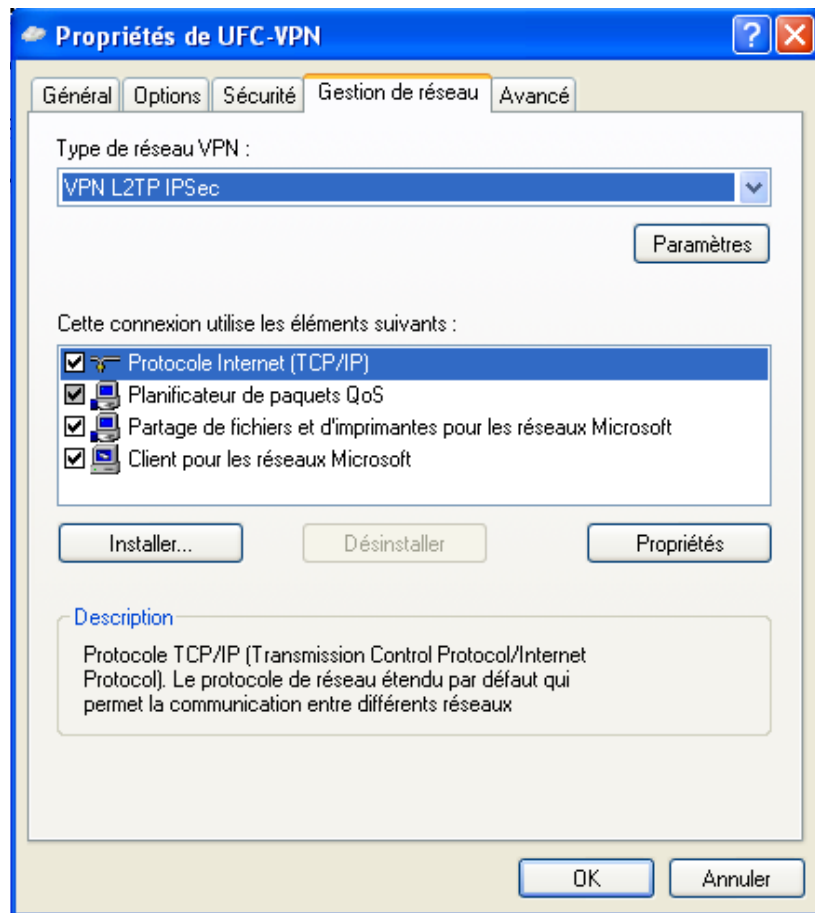
- sélectionner « **Exiger le cryptage (déconnecter si le serveur refuse)** » dans la liste.
- cocher « **Mot de passe non crypté (PAP)** » : l2tp ne supporte que PAP et CHAP
- si votre système le réclame, cochez « **Protocole Microsoft CHAP Version 2 (MS-CHAP v2)** »
- décocher tous les autres protocoles



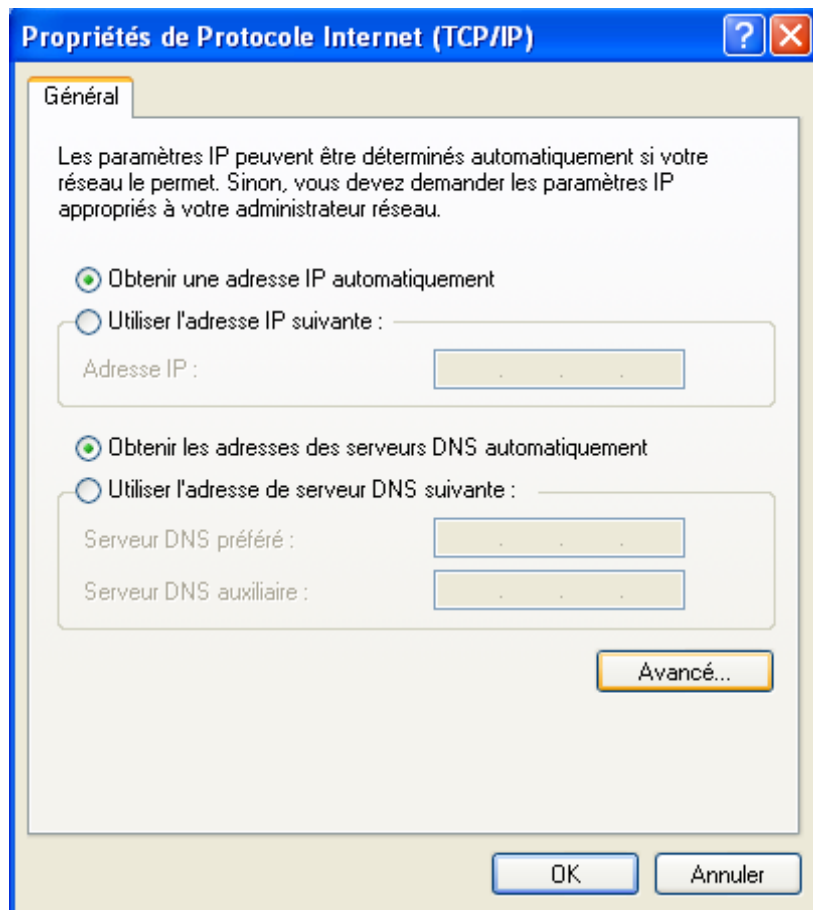
- puis cliquer sur le bouton **OK**

Si un message d'information apparaît vous demandant si vous voulez conserver ces paramètres, répondez « **OUI** »

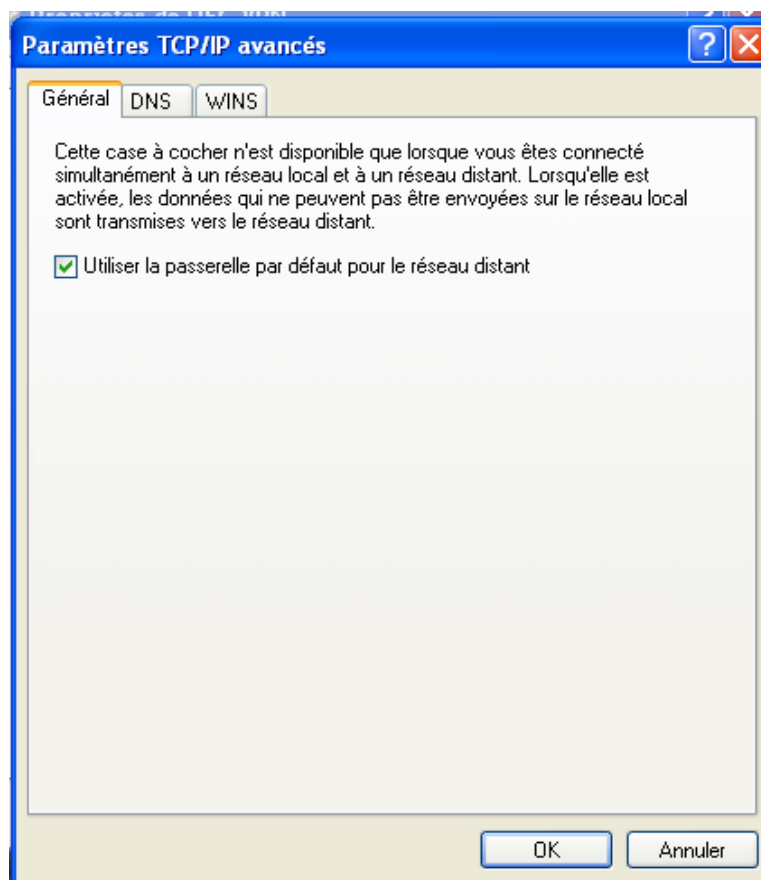
- Cliquer sur l'onglet « **Gestion du réseau** » et choisir dans le Type de réseau VPN « **VPN L2TP IPSec** »
- Cliquer sur **Protocole Internet (TCP/IP)** puis le bouton « **Propriétés** »



- Cliquer sur le bouton « **Avancé...** »



- Cochez la case « **Utiliser la passerelle par défaut pour le réseau distant** »



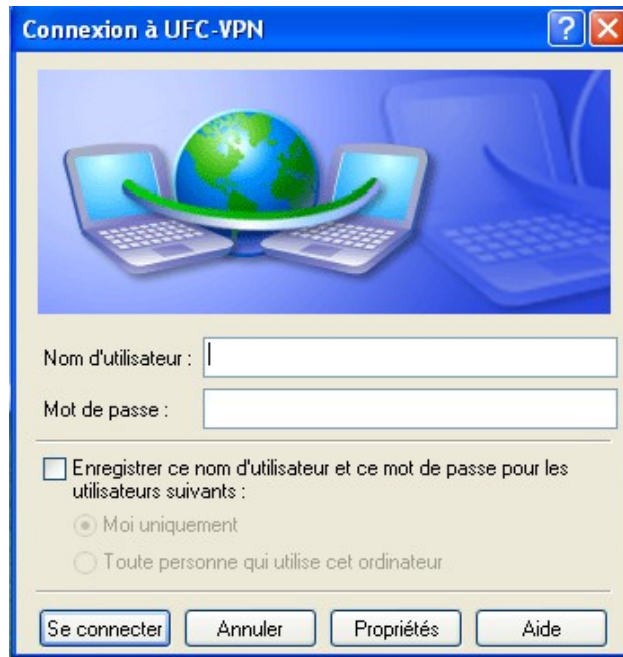
- Cliquer sur le bouton **OK** pour fermer la fenêtre des paramètres TCP/IP
- Cliquer sur le bouton **OK** pour fermer la fenêtre des Propriétés de Protocole Internet

- Cliquer sur le bouton **OK** pour fermer la fenêtre des Propriétés de la connexion VPN que vous avez créé.
- Entrer votre **nom d'utilisateur** et votre **mot de passe** (pour la connexion au serveur L2TP) et cocher « **Enregistrer ce nom d'utilisateur...** » (si vous ne voulez pas avoir à les retaper à chaque fois).

N.B. : Le **Nom d'utilisateur** correspondant à votre [login_ldap@votre_realm](#)

Exemple : jdupont@ufc pour J. Dupont qui souhaite se connecter sur le realm générique de l'université.

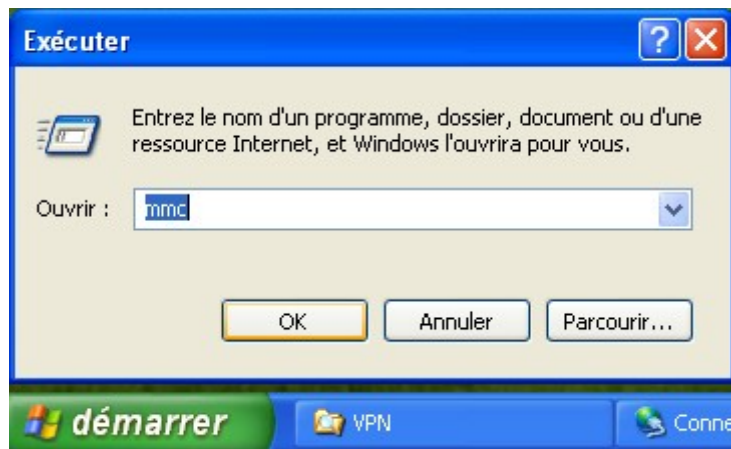
Le **Mot de passe** est celui stocké dans LDAP, que vous utilisez pour l'ENT ou votre messagerie.



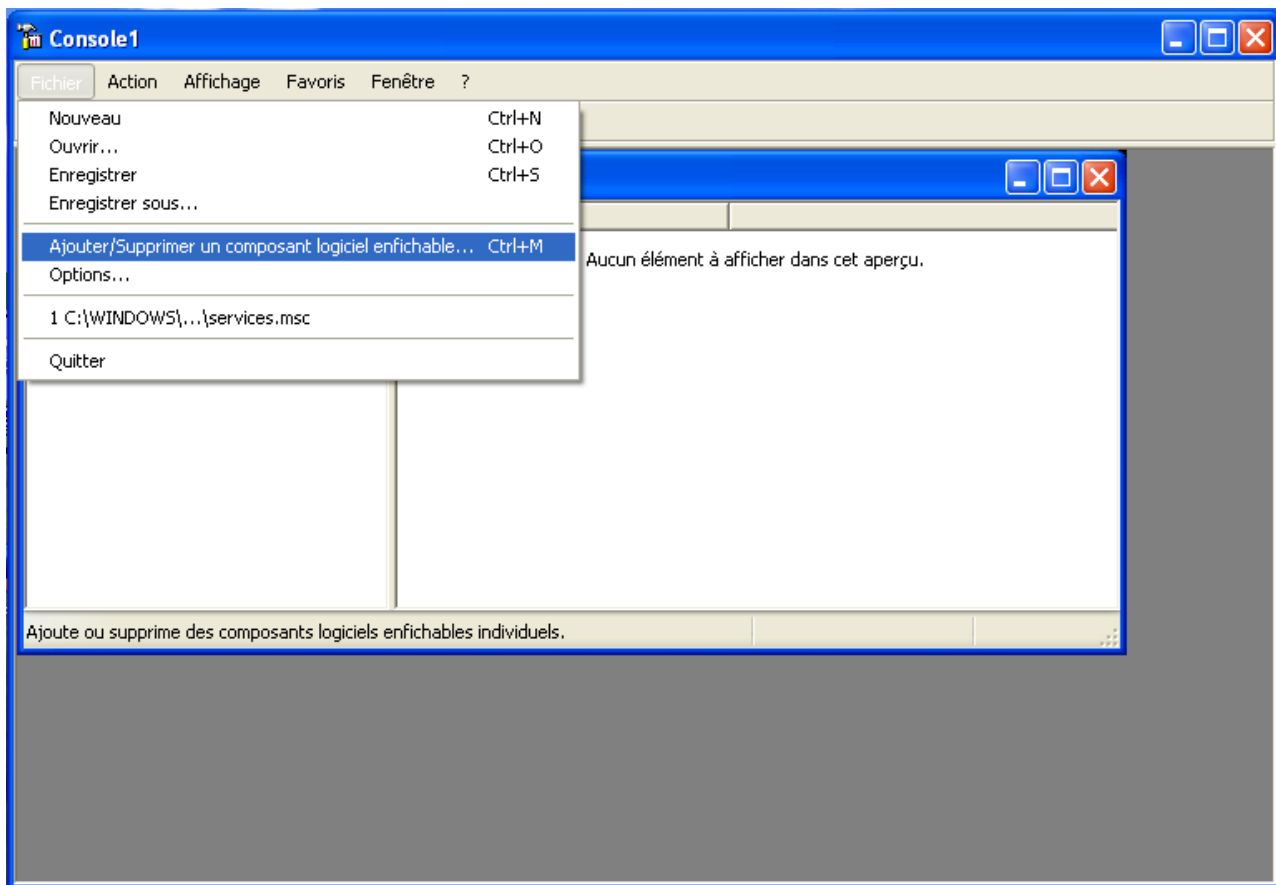
Cliquer enfin sur « **Se connecter** »

Importation du certificat

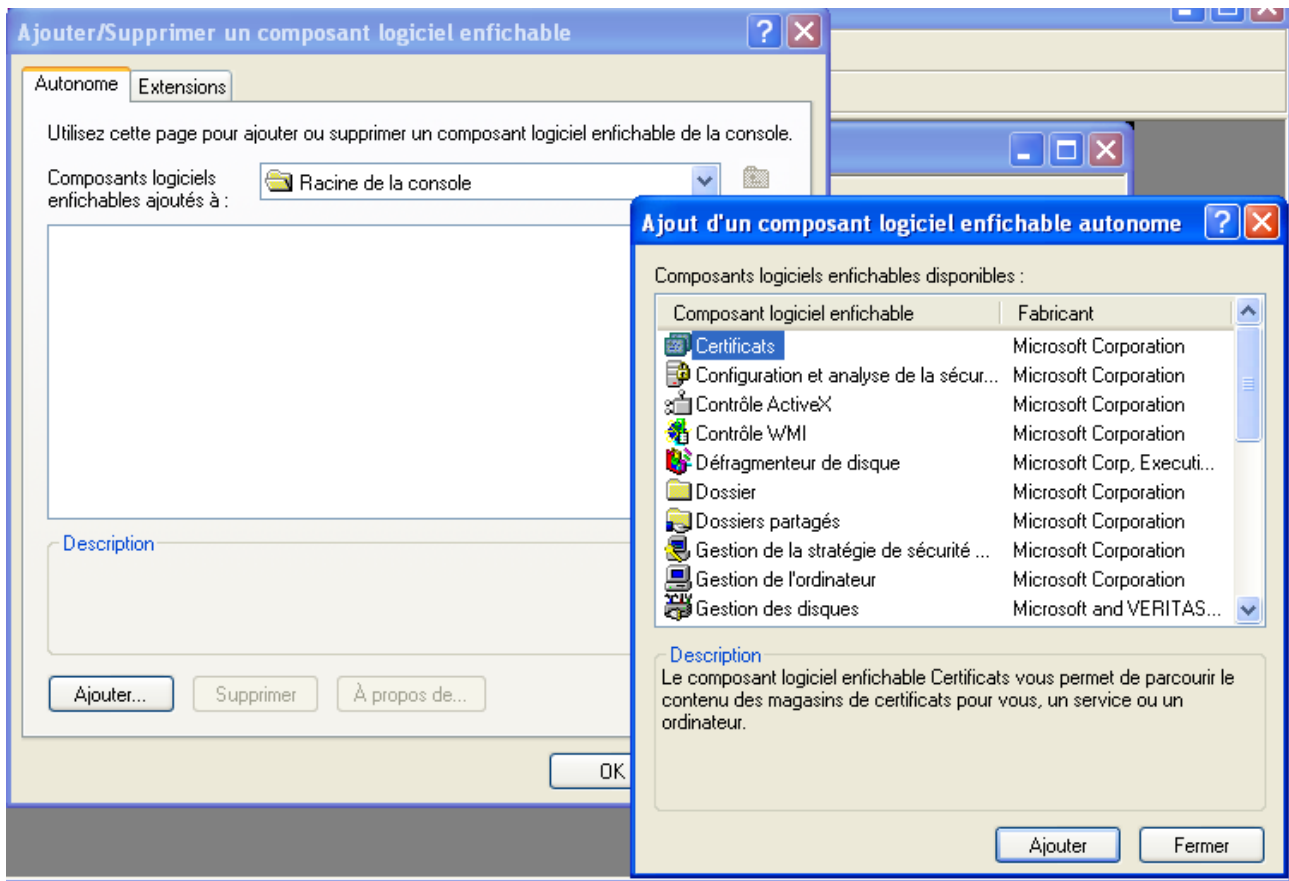
- Ouvrir une console Microsoft en cliquant sur démarrer puis exécuter
- Dans le champ « Ouvrir » taper **mmc** et cliquer sur le bouton **OK**



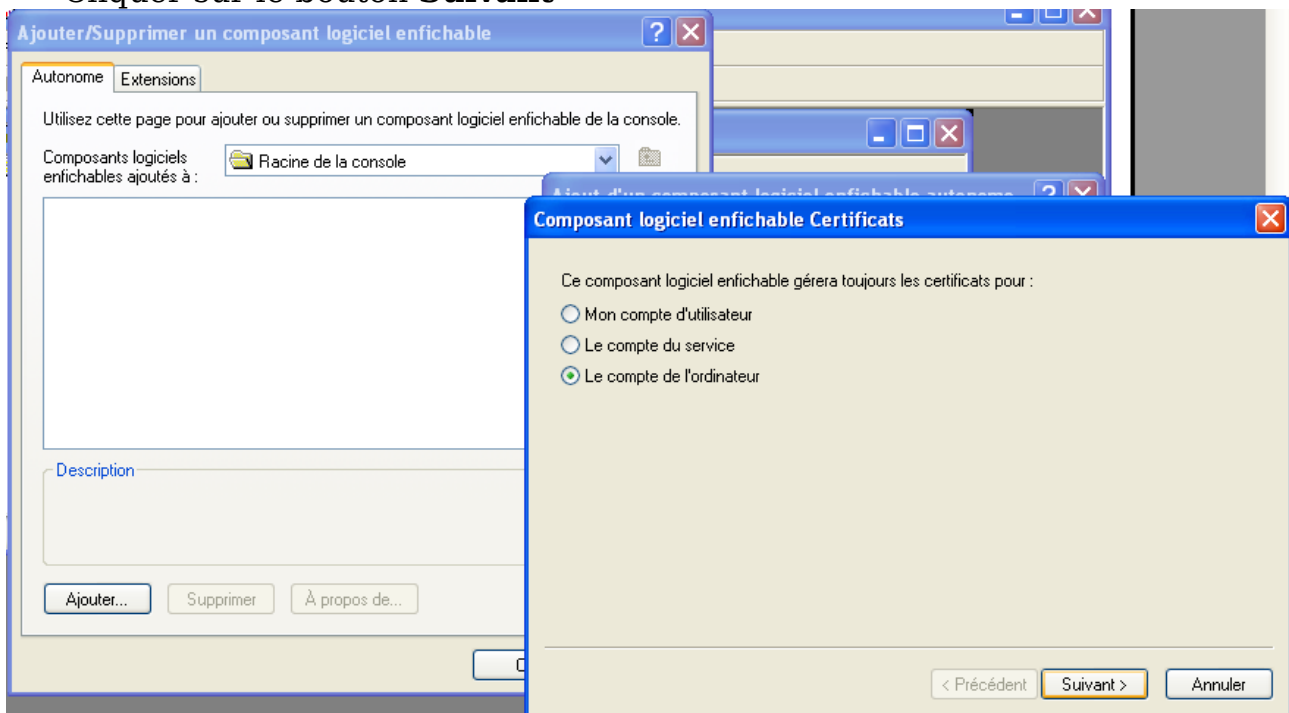
- Dans le menu Fichier, choisir **Ajouter/Supprimer un composant logiciel enfichable**



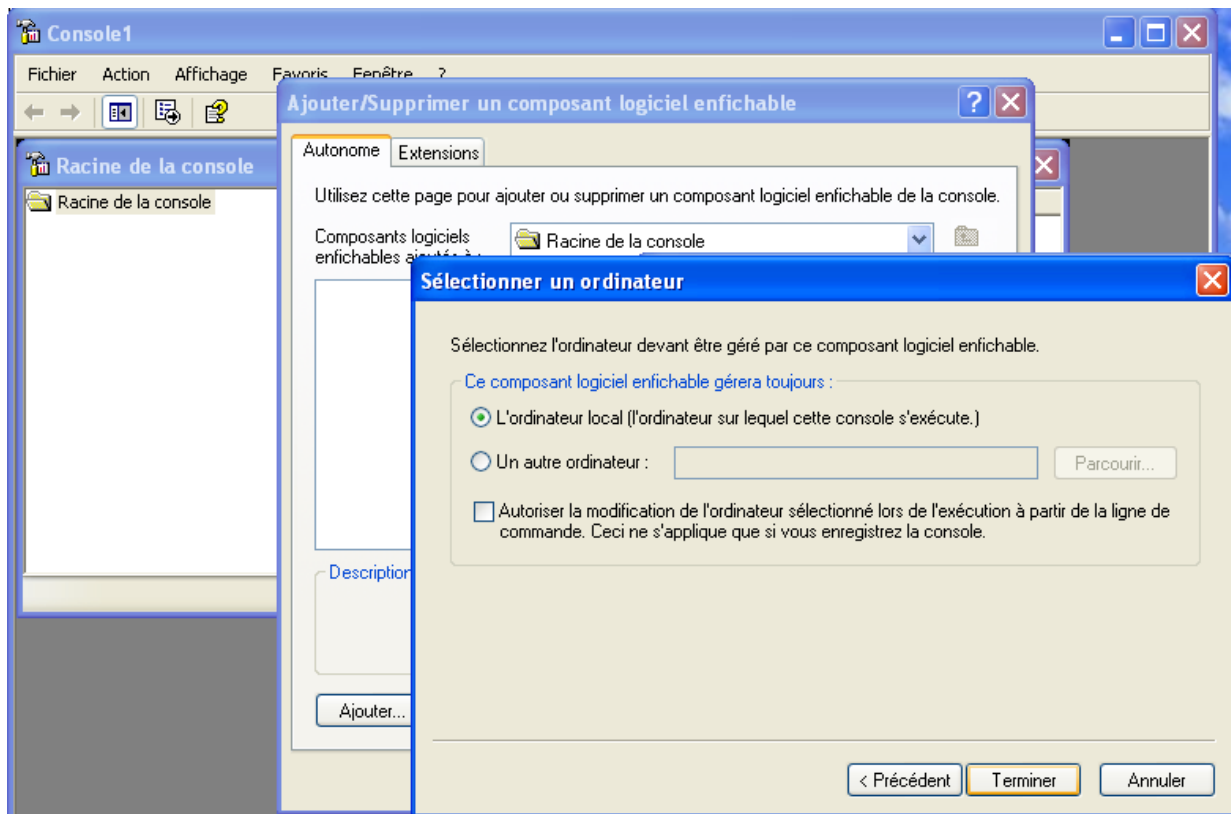
- Cliquer sur le bouton « **Ajouter** » en bas de la fenêtre puis choisir le composant **Certificats** dans la nouvelle fenêtre qui s'est ouverte
- Cliquer de nouveau sur le bouton « **Ajouter** » en bas de cette nouvelle fenêtre



- Choisir le bouton radio « **Le compte de l'ordinateur** »
- Cliquer sur le bouton **Suivant**

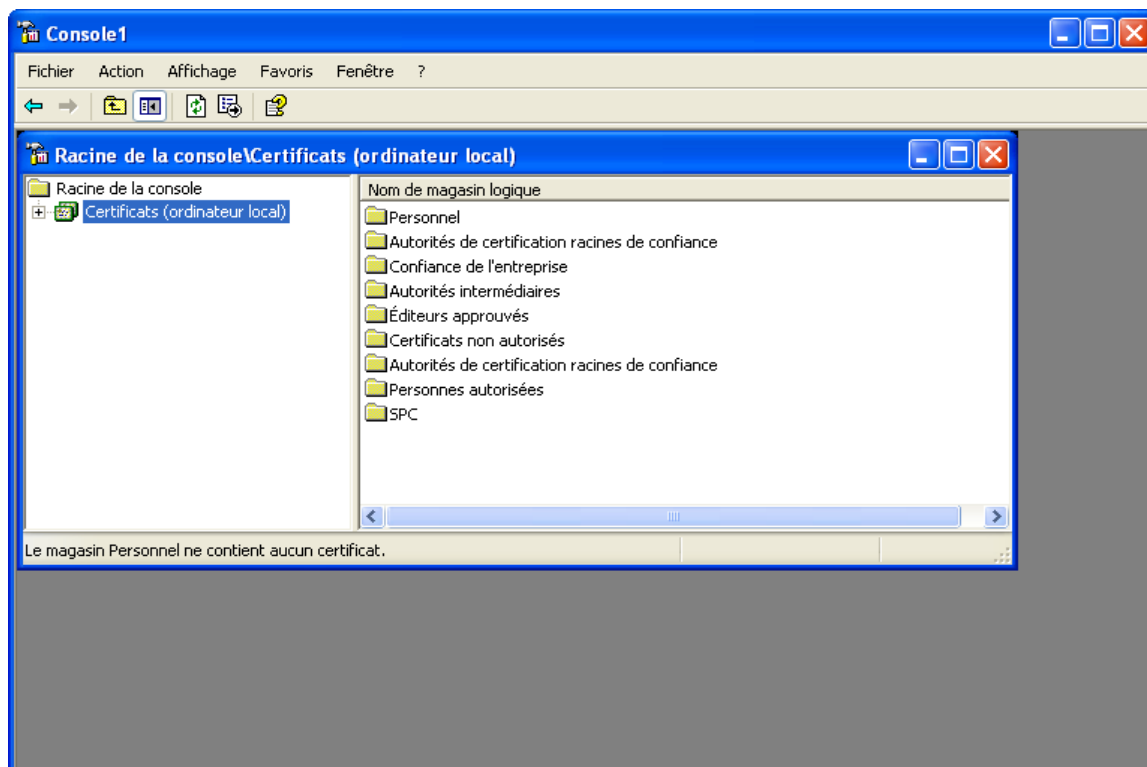


- Choisir le bouton radio « **L'ordinateur local** »
- Cliquer sur le bouton **Terminer**

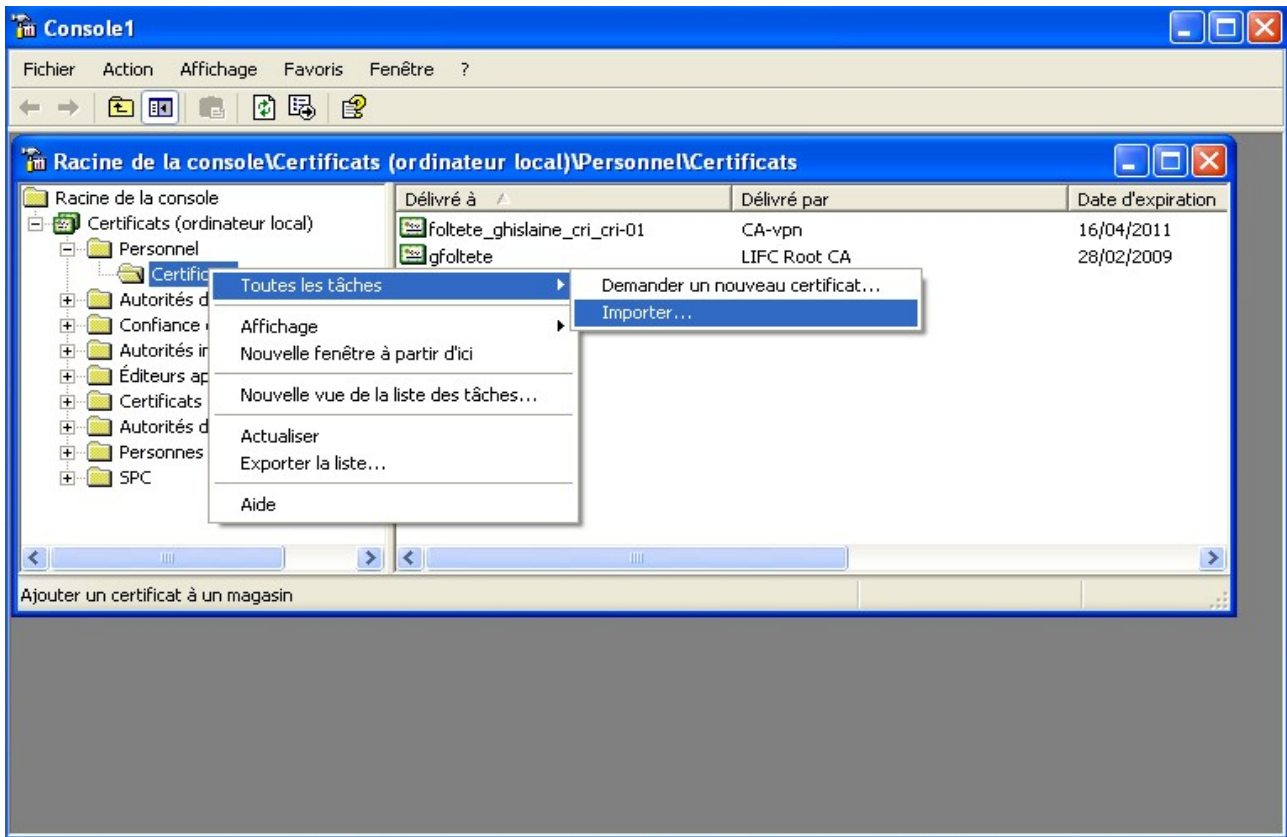


- Fermer la fenêtre « Ajout d'un composant enfichable autonome » en appuyant sur « **Fermer** »
- Fermer la fenêtre « Ajouter/Supprimer un composant enfichable » en appuyant sur « **Ok** »

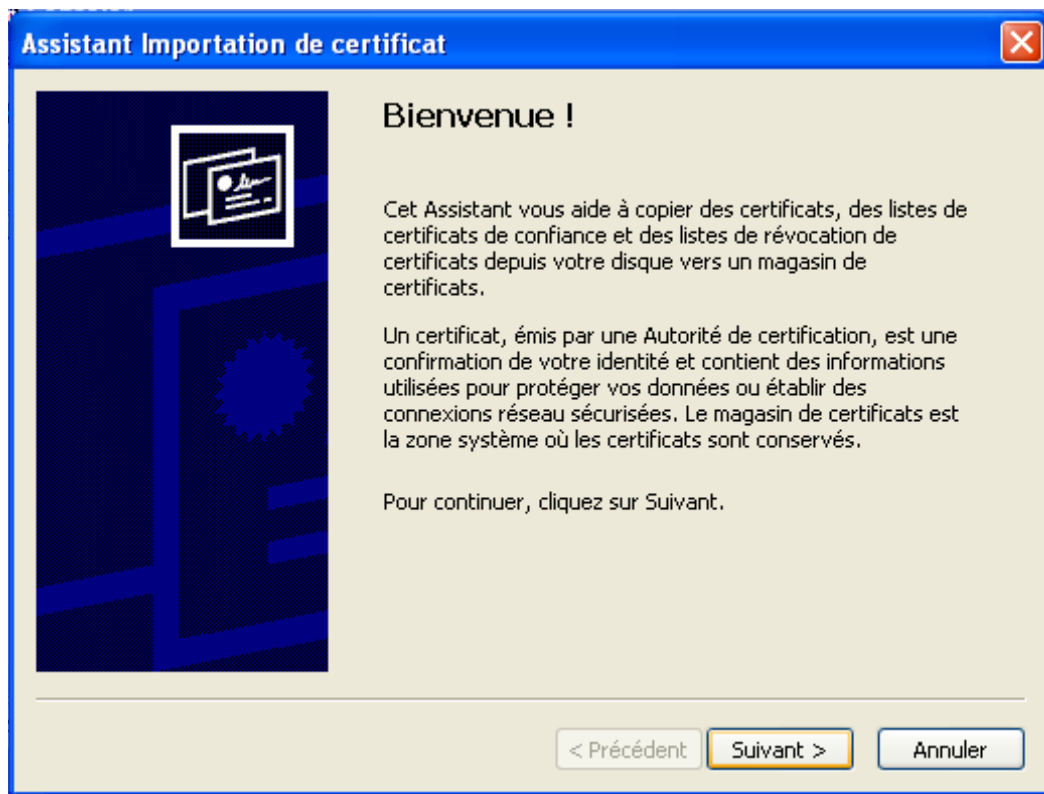
Dérouler l'arborescence des certificats en cliquant sur l'icône + placée devant « **Certificats (ordinateur local)** »



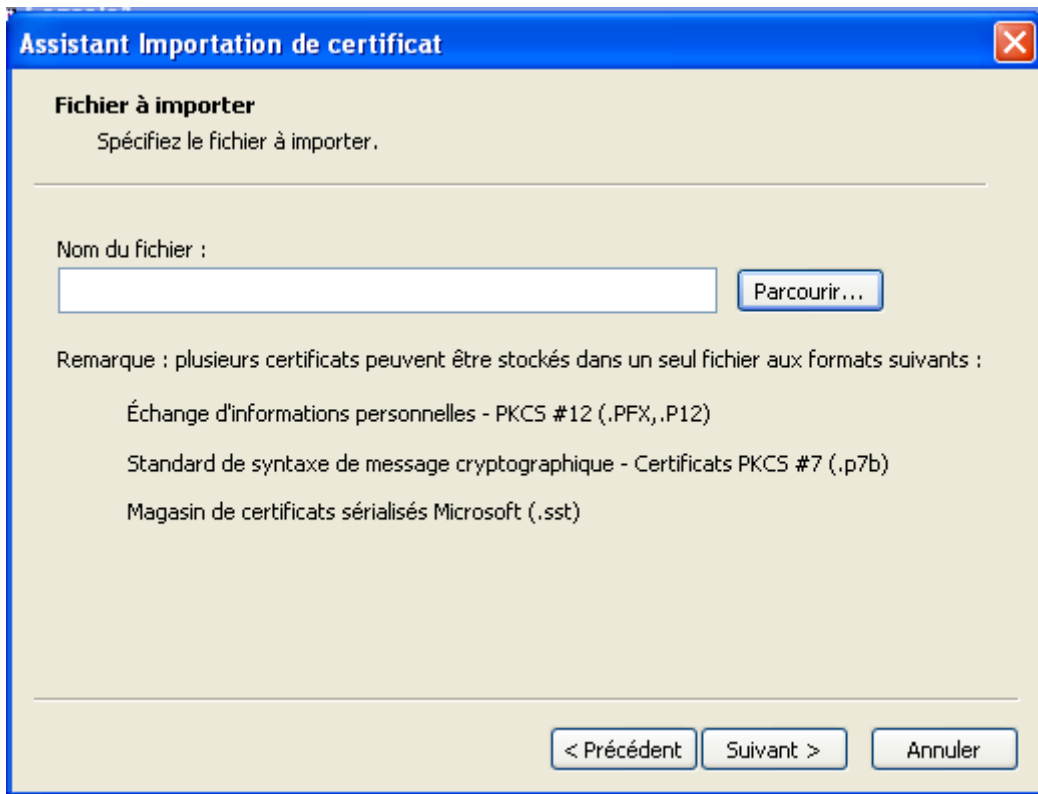
- Effectuer un clic droit sur « **Personnel** »
- Choisir « **Toutes les tâches** » puis « **Importer** »



L'assistant d'importation de certificat s'ouvre.

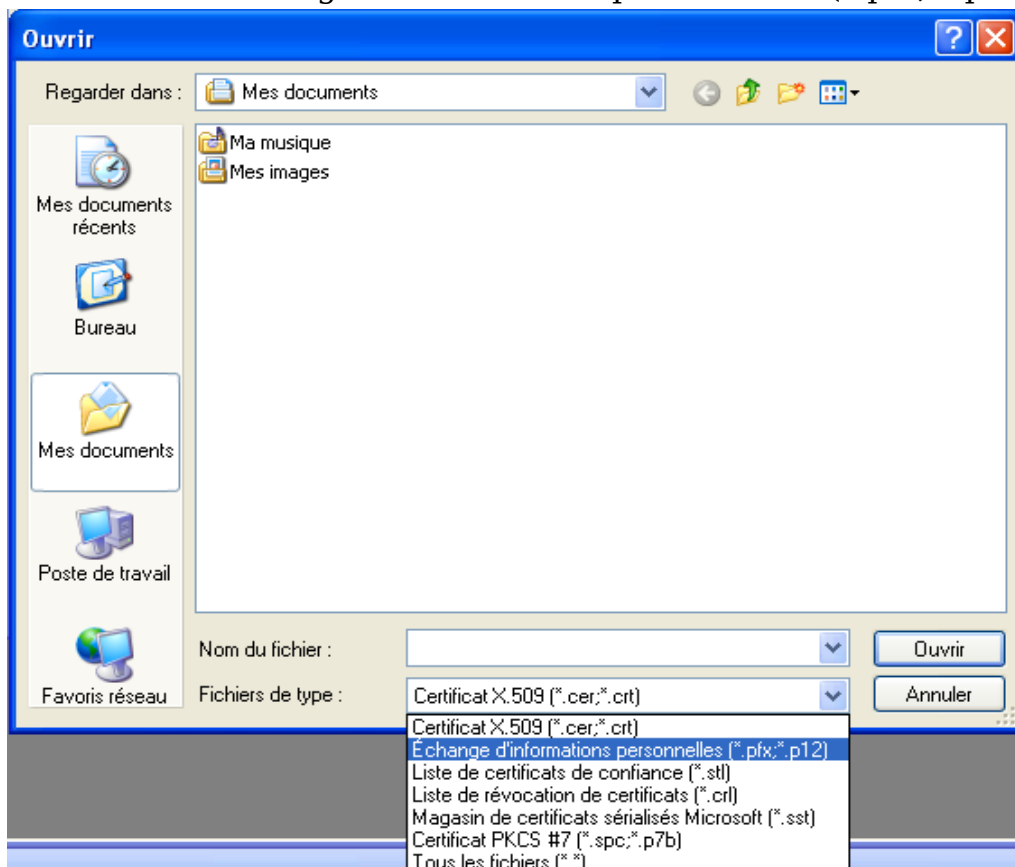


- Avec le bouton « **Parcourir** » rechercher votre fichier contenant le certificat xxxx.p12 qui vous a été remis

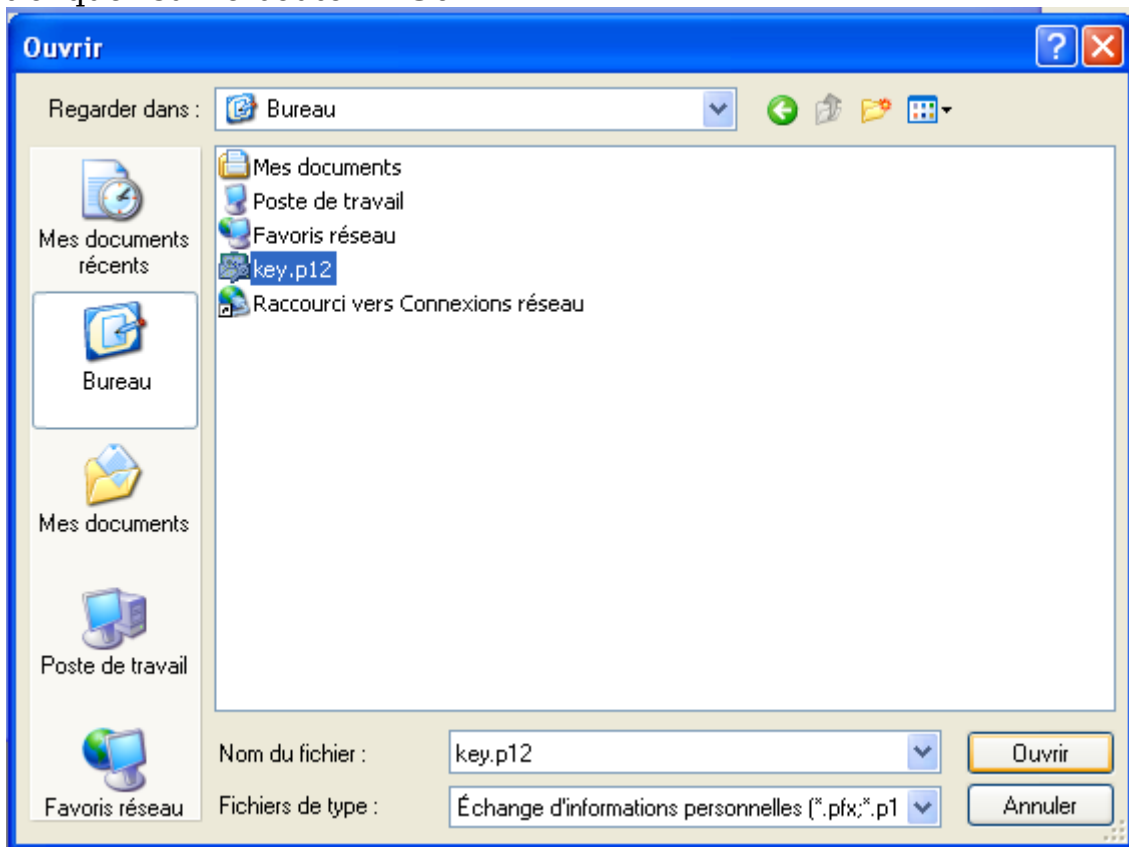


Lorsque vous êtes atteint le dossier contenant le certificat, s'il n'apparaît pas,

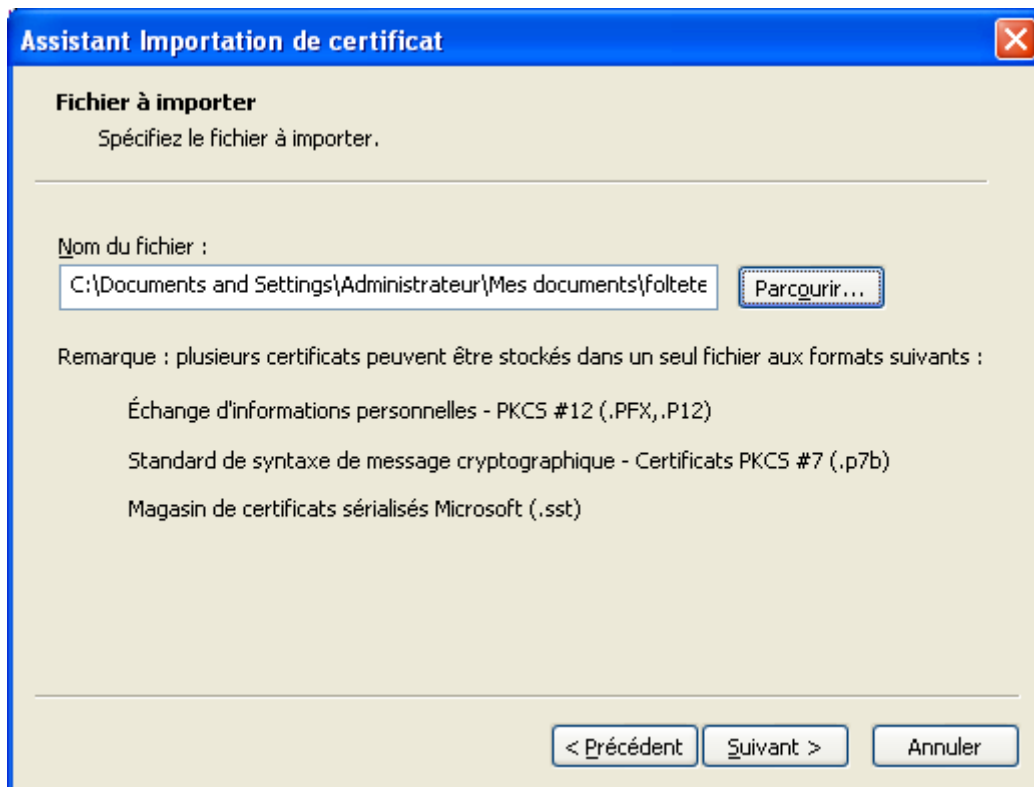
- sélectionner le type de fichier en déroulant la liste « Fichiers de type »
- et choisissez « Échange d'informations personnelles (*.pfx; *.p12) »



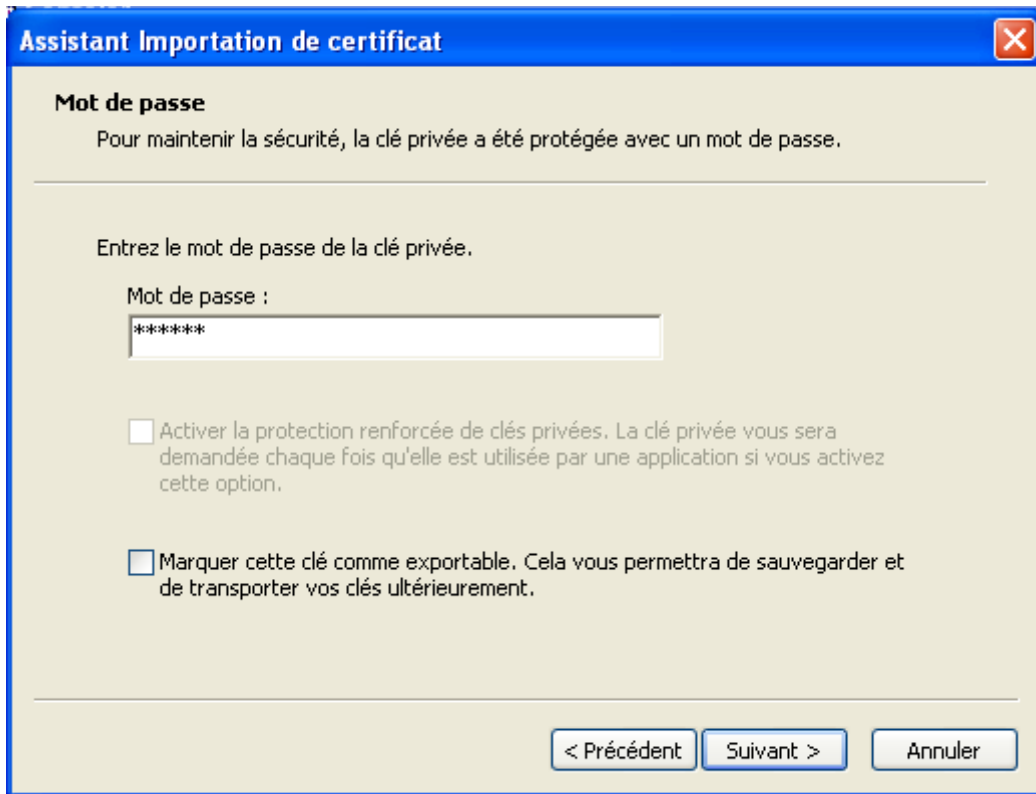
- sélectionner le fichier
- et cliquer sur le bouton « **Ouvrir** »



- Cliquer sur le bouton « **Suivant** »



- Taper le mot de passe qui vous a été remis avec le certificat



Assistant Importation de certificat

Mot de passe
Pour maintenir la sécurité, la clé privée a été protégée avec un mot de passe.

Entrez le mot de passe de la clé privée.

Mot de passe :

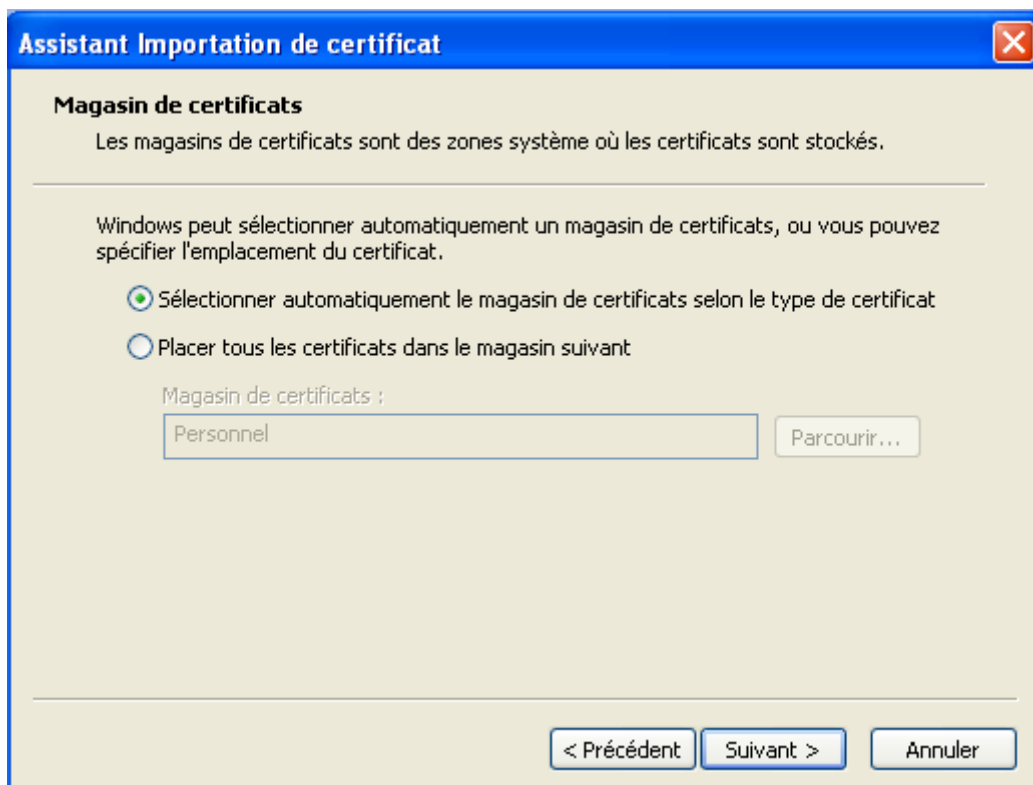
Activer la protection renforcée de clés privées. La clé privée vous sera demandée chaque fois qu'elle est utilisée par une application si vous activez cette option.

Marquer cette clé comme exportable. Cela vous permettra de sauvegarder et de transporter vos clés ultérieurement.

< Précédent Suivant > Annuler

Cliquer sur le bouton « **Suivant** »

Choisir le bouton-radio « **Sélectionner automatiquement le magasin selon le type de certificat** »



Assistant Importation de certificat

Magasin de certificats
Les magasins de certificats sont des zones système où les certificats sont stockés.

Windows peut sélectionner automatiquement un magasin de certificats, ou vous pouvez spécifier l'emplacement du certificat.

Sélectionner automatiquement le magasin de certificats selon le type de certificat

Placer tous les certificats dans le magasin suivant

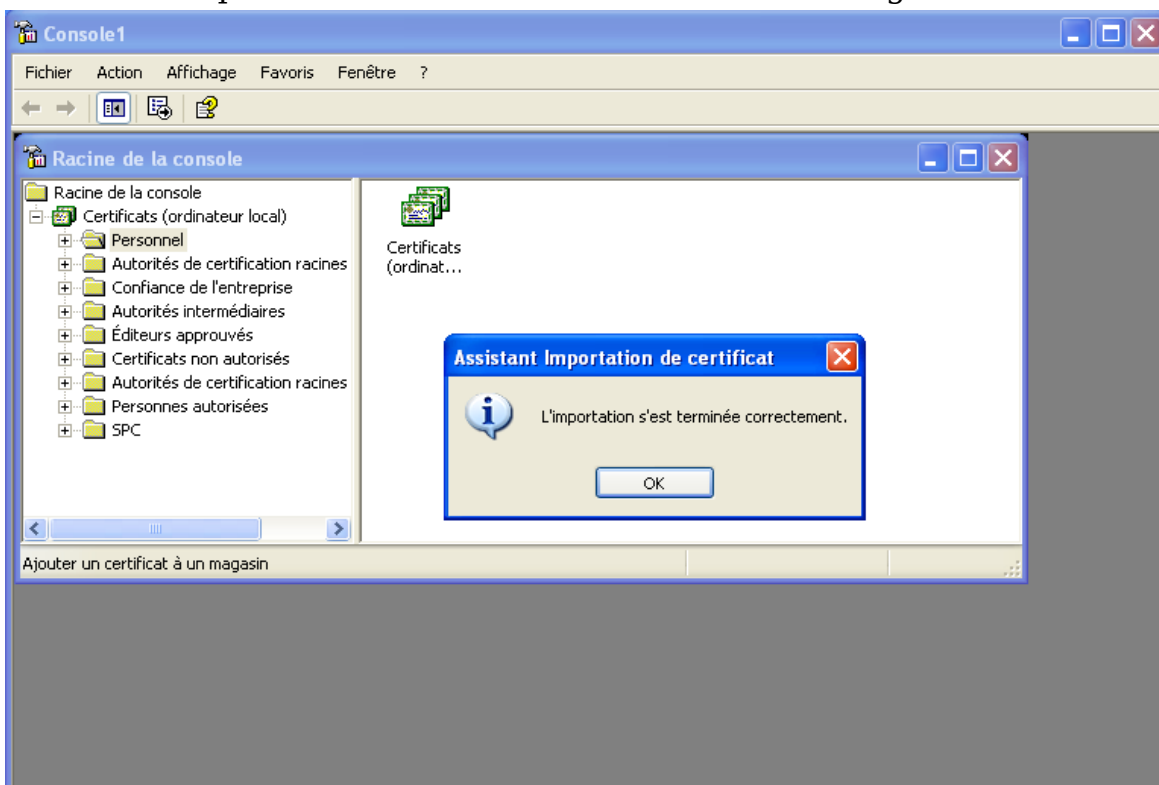
Magasin de certificats :
Personnel Parcourir...

< Précédent Suivant > Annuler

Cliquer sur le bouton « **Terminer** »



L'assistant d'importation se ferme en affichant un message



Fermer toutes les fenêtres.

Vous pouvez maintenant vous connecter en VPN dans votre réseau.

Rappel : pour ouvrir votre connexion VPN

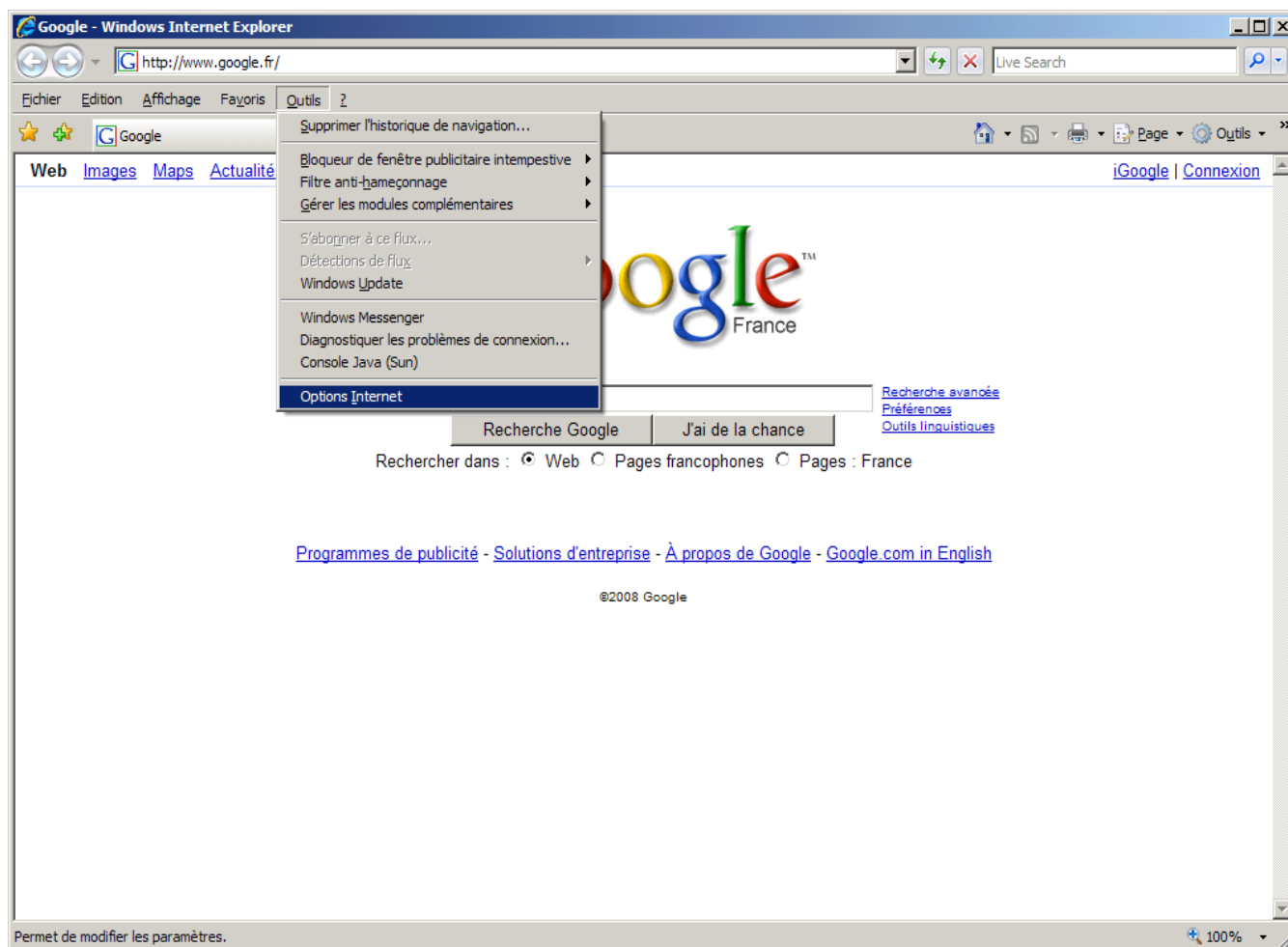
- allez dans Panneau de configuration
- choisir Connexions Réseau
- effectuer un clic droit sur votre connexion VPN
- et choisir Se connecter

Complément de configuration pour le navigateur Internet Explorer 7

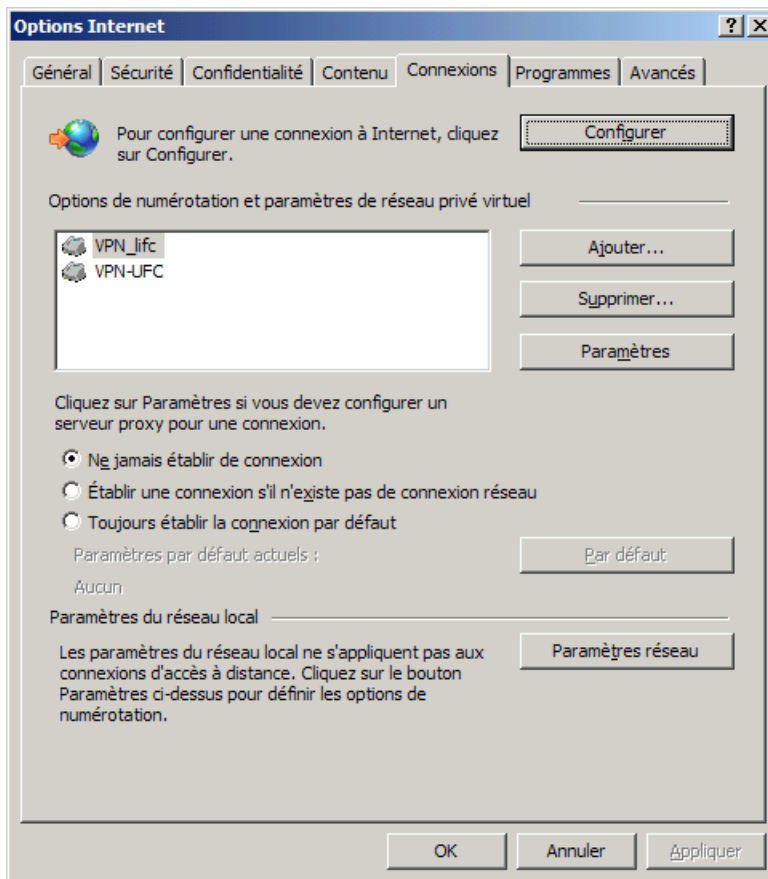
Si vous utilisez Internet Explorer 7, il faut configurer la connexion VPN dans le navigateur pour qu'elle utilise le proxy de l'université.

Cette configuration complémentaire est inutile avec Firefox ou Opéra.

Dans votre navigateur IE 7, cliquer sur le bouton « **Outils** » et choisissez « **Options Internet** »

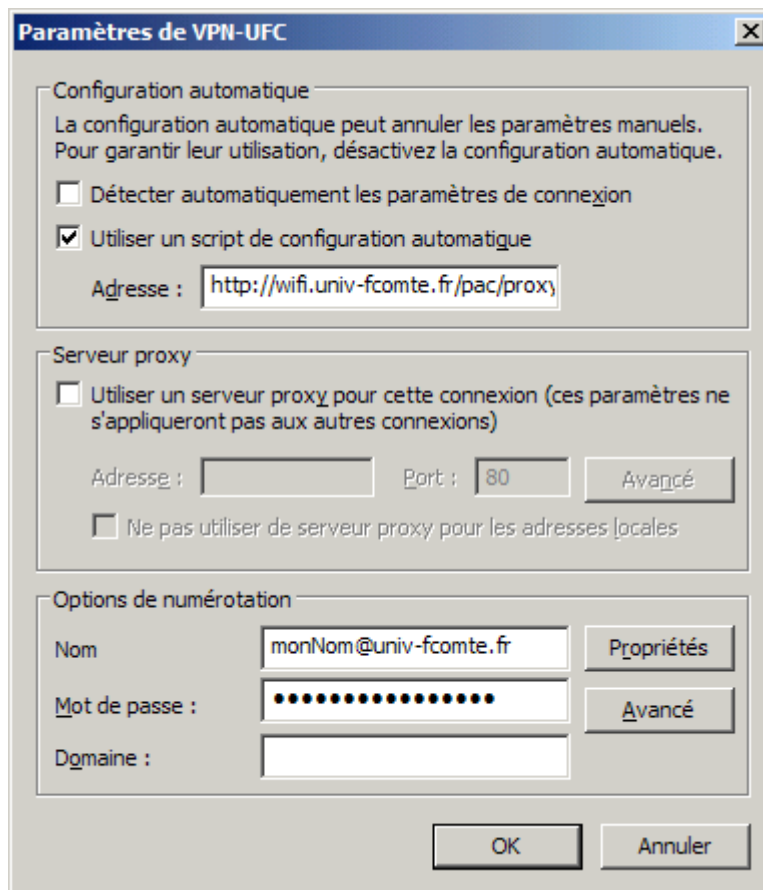


Cliquer sur l'onglet « **Connexions** »



Sélectionner la connexion VPN que vous souhaitez configurer, par exemple VPN-UFC et cliquer sur le bouton « **Paramètres** »

Cochez l'option « **Utilisez un script de configuration automatique** » et remplissez **Adresse** comme suit : <http://wifi.univ-fcomte.fr/par/proxy.pac>



Fermez la fenêtre en cliquant sur le bouton « **OK** ».