Installation VPN Windows 2003 serveur

1. Utilité d'un VPN au sein de Tissea SARL

1.1. Présentation

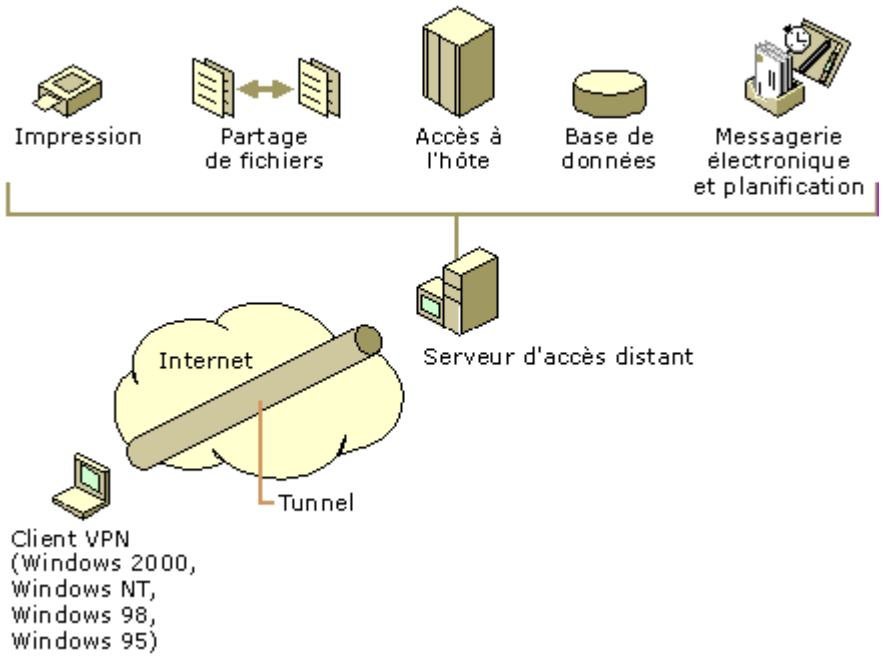
Un réseau privé virtuel (VPN) est un moyen pour se connecter à un réseau privé par le biais d'un réseau public qu'est Internet. Il allie les avantages d'une connexion à distance avec un serveur d'accès distant à la facilité et à la commodité d'une connexion Internet

La solution d'installer un serveur VPN au sein de Tissea SARL permettrait que les sites distants puissent accéder au réseau de manière transparente et sécurisée. Donc, il fallait établir un lien entre ces sites afin qu'ils puissent regrouper et partager leurs ressources de documents afin d'augmenter leur productivité.

1.2. Communication entre les sites

Avant l'apparition du VPN dans l'entreprise, pour relier ces plusieurs réseaux physiques, il y'avait une ligne spécialisée qui réalisait un WAN entre ces réseaux depuis un moment. L'utilité principale du VPN était de permettre à une machine distante d'un réseau (Marrakech par exemple) d'y accéder, par l'intermédiaire d'Internet, et tout cela en assurant une sécurité des données échangées. Ceci étant établi, Une fois connecté à Internet, l'utilisateur peut créer un VPN entre sa machine et le réseau éloigné.

Voici en image une illustration concrète :



2. Composants d'un serveur VPN

2.1. Explications

Dans Windows 2003, le protocole de réseau privé virtuel est constitué des composants suivants :

1 serveur VPN, 1(n) client(s) VPN, 1 connexion VPN (ceci est la partie de la connexion où les données sont cryptées) et du tunnel (la partie de la connexion où les données sont encapsulées).

La tunnellisation est effectuée grâce à l'un des protocoles de tunnellisation inclus dans Windows 2003 (existant déjà sous 2000), qui sont tous les deux installés avec le service Routage et accès distant, ou service appelé "RRAS" (Routing and Remote Access). Les deux protocoles principaux de tunnellisation inclus avec Windows 2003 sont :

- **PPTP** (Point-to-Point Tunneling Protocol) qui assure le cryptage des données à l'aide du Cryptage point à point Microsoft Corporation.

- **L2TP** (Layer Two Tunneling Protocol) qui lui assure le cryptage, l'authentification et l'intégrité des données à l'aide du protocole IPSec.

Notons cependant qu'il est recommandé que votre connexion à Internet utilise une ligne spécialisée de type T(n) fractionnel ou à relais de trames. La carte WAN doit être configurée avec l'adresse IP et le masque de sous-réseau attribués à votre domaine ou fournis par un provider, ainsi qu'avec la passerelle par défaut du routeur ISP.

2.2. Différences entre PPTP et L2TP/IPSec

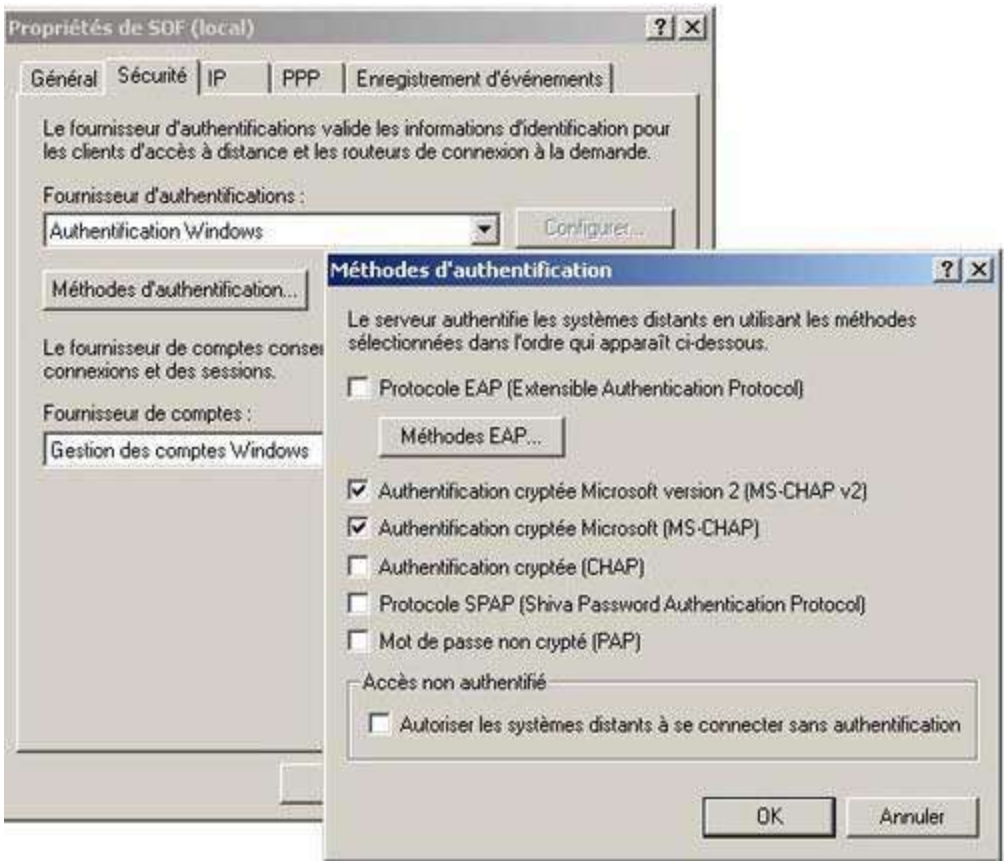
Nous venons de voir que Windows 2003 supporte deux protocoles VPN qui sont les suivants:
- Le protocole **PPTP** (point to point tunneling protocol)

- Le protocole **L2TP** (layer 2 tunneling protocol).

Le protocole **PPTP** utilise la méthode de chiffrement **MPPE** (Microsoft Point to point encryption) tandis que L2TP est basé sur **IPSec**. Cependant, pour avoir une communication chiffrée avec le protocole PPTP il est nécessaire d'avoir utilisé l'une des méthodes suivantes d'authentification:

- **MS-CHAP v1 ou v2**

- **EAP/TLS** pour les cartes à puces.
(IPSec ne requiert aucune méthode d'authentification particulière)



La méthode MPPE permet de chiffrer sur 40,56 et 128 bits; pour pouvoir utiliser le cryptage sur 128 bits il était nécessaire d'avoir installer le High encryption pack (inclus dans le service pack3) et d'installer un patch correcteur pour les versions 95 et 98 de Windows mais avec Windows 2003 cela est résolu.

Voici un tableau des principales caractéristiques des protocoles **PPTP** et **L2TP**

Caractéristiques	PPTP	L2TP
Compression d'en-tête	Non	Oui
Authentification du tunnel	Non	Oui
Cryptage intégré	Oui	Non
Transmission sur des réseaux basés sur IP	Oui	Oui
Transmet sur des réseaux basés sur UDP, Frame Relay, X.25 ou ATM	Non	Oui

3. Installation sur Windows 2003 serveur

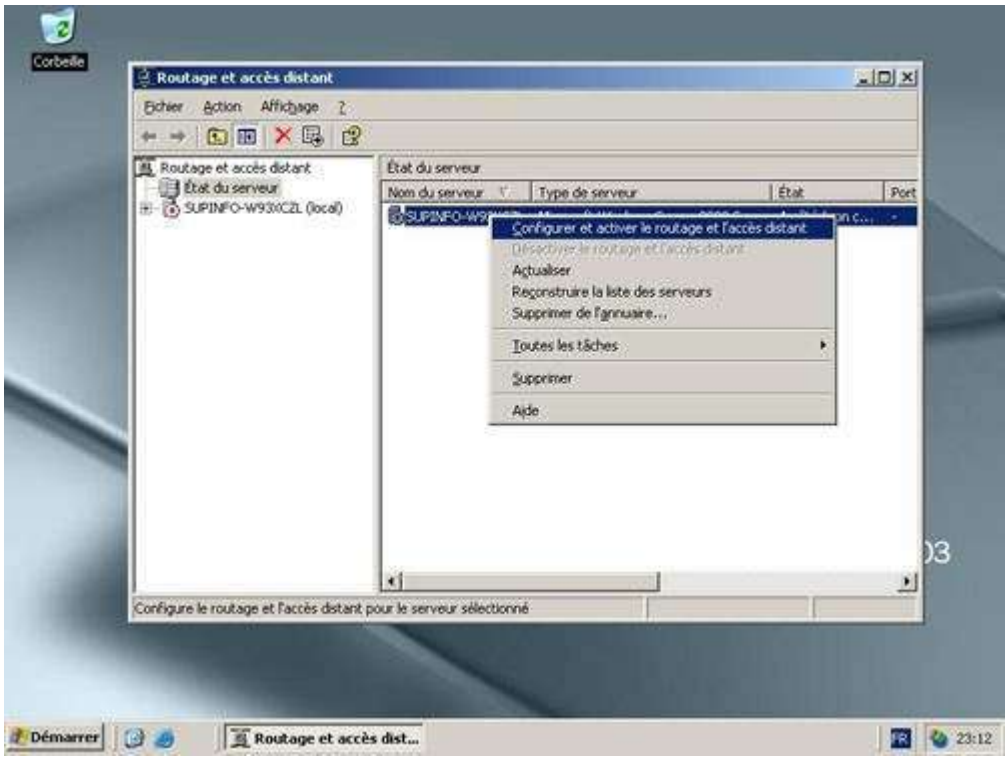
3.1. Installation et activation du vpn

Pour installer et activer un serveur VPN sur Windows 2003 serveur, procédez comme suit :

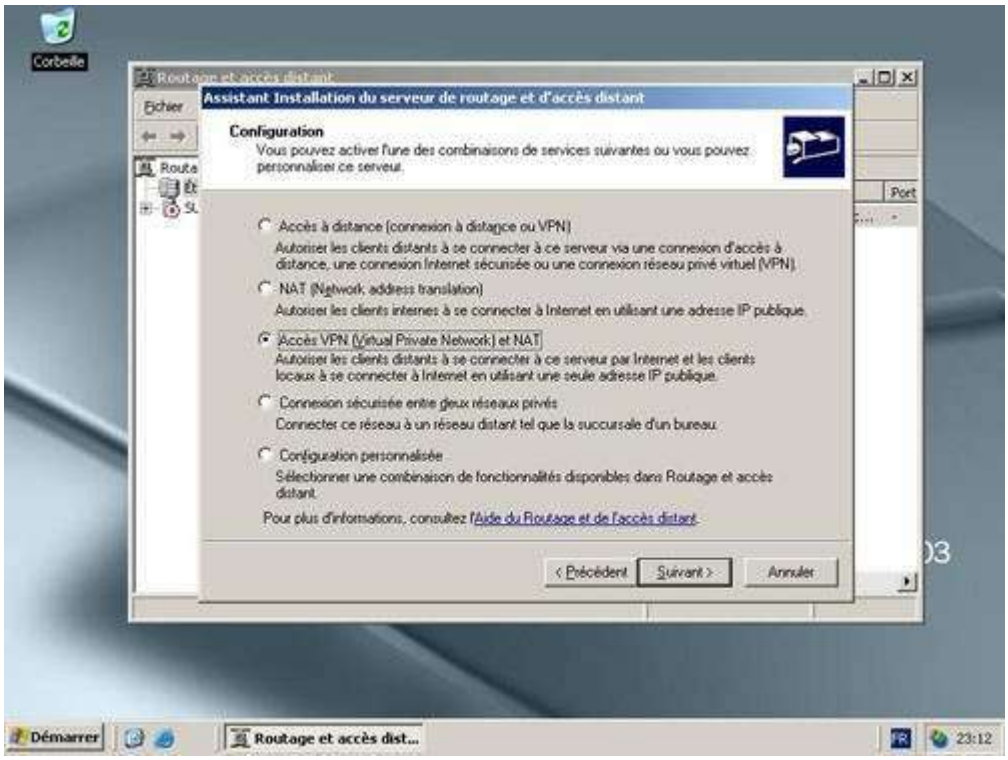
1) Tout d'abord, sur l'unité possédant VPN Microsoft Windows 2003, confirmez que la connexion à Internet et la connexion à votre réseau local d'entreprise (LAN) sont toutes les deux correctement configurées, ceci est important pour les étapes suivantes:

2) Cliquez sur Démarrer, pointez sur Outils d'administration, puis cliquez sur Routage et accès distant.

3) Cliquez sur le nom du serveur dans l'arborescence, puis sur Configurer et activer le service Routage et accès distant dans le menu Action. Cliquez sur Suivant.



4) Dans la boîte de dialogue Configurations communes, cliquez sur Réseau privé virtuel (serveur VPN), puis sur Suivant.



5) Dans la boîte de dialogue Protocoles du client distant, confirmez que TCP/IP est inclus dans la liste ; cliquez sur Oui, tous les protocoles disponibles sont dans cette liste, puis sur Suivant.

6) Dans la boîte de dialogue Connexion Internet, sélectionnez la connexion Internet utilisée pour vous connecter à Internet, puis cliquez sur Suivant.

7) Dans la boîte de dialogue Attribution d'adresses IP, sélectionnez Automatiquement afin d'utiliser le serveur DHCP de votre sous-réseau pour attribuer des adresses IP aux clients d'accès distant et au serveur.

8) Dans la boîte de dialogue Gestion de serveurs d'accès distant multiples, confirmez que la case à cocher Non, je ne veux pas configurer ce serveur pour utiliser RADIUS maintenant est activée.

9) Cliquez sur Suivant, puis sur Terminer.

10) Cliquez avec le bouton droit sur le nœud Ports, puis cliquez sur Propriétés.

11) Dans la boîte de dialogue Propriétés des ports, cliquez sur le périphérique Miniport WAN (PPTP), puis sur Configurer.

12) Dans la boîte de dialogue Configurer le périphérique - Miniport WAN (PPTP), cette possibilité s'offre à vous :

NB: Si vous ne voulez pas prendre en charge un VPN d'accès utilisateur distant direct aux modems installés sur le serveur, désactivez la case à cocher Connexions de routage de numérotation à la demande (entrantes et sortantes).

13) Tapez le nombre maximum de connexions PPTP simultanées que vous voulez autoriser dans la zone de texte Nombre maximum de ports. (Ce nombre peut dépendre du nombre d'adresses IP disponibles.)

14) Répétez les étapes 11 à 13 pour le périphérique L2TP, puis cliquez sur OK.

3.2 Configuration du serveur VPN

Configuration du serveur d'accès distant en tant que routeur
Pour que notre serveur d'accès distant puisse acheminer le trafic correctement sur votre réseau, vous devez le configurer en tant que routeur avec soit des itinéraires statiques, soit des protocoles de routage, de façon à ce que tous les sites sur l'intranet soient joignables à partir du même serveur d'accès distant.

Pour configurer le serveur en tant que routeur :

1) tout d'abord, cliquez sur Démarrer, pointez sur Outils d'administration, puis cliquez sur Routage et accès distant.

2) Cliquez avec le bouton droit sur le nom du serveur, puis cliquez sur Propriétés.

3) Dans l'onglet Général, sélectionnez Activer cet ordinateur en tant que routeur.

4) Sélectionnez Routage pour réseaux locaux uniquement ou Routage réseau local et de numérotation à la demande. Cliquez pour finir sur "OK" pour fermer la boîte de dialogue Propriétés.

3.3 Configuration des ports PPTP

Confirmez le nombre de ports PPTP dont vous avez besoin. Pour vérifier le nombre de ports ou pour ajouter des ports, procédez comme suit :

1) Cliquez sur Démarrer, pointez sur Outils d'administration, puis cliquez sur Routage et accès distant.

2) Dans l'arborescence de la console, développez Routage et accès distant, développez le nom du serveur, puis cliquez sur Ports.

3) Cliquez avec le bouton droit sur Ports, puis cliquez sur Propriétés.

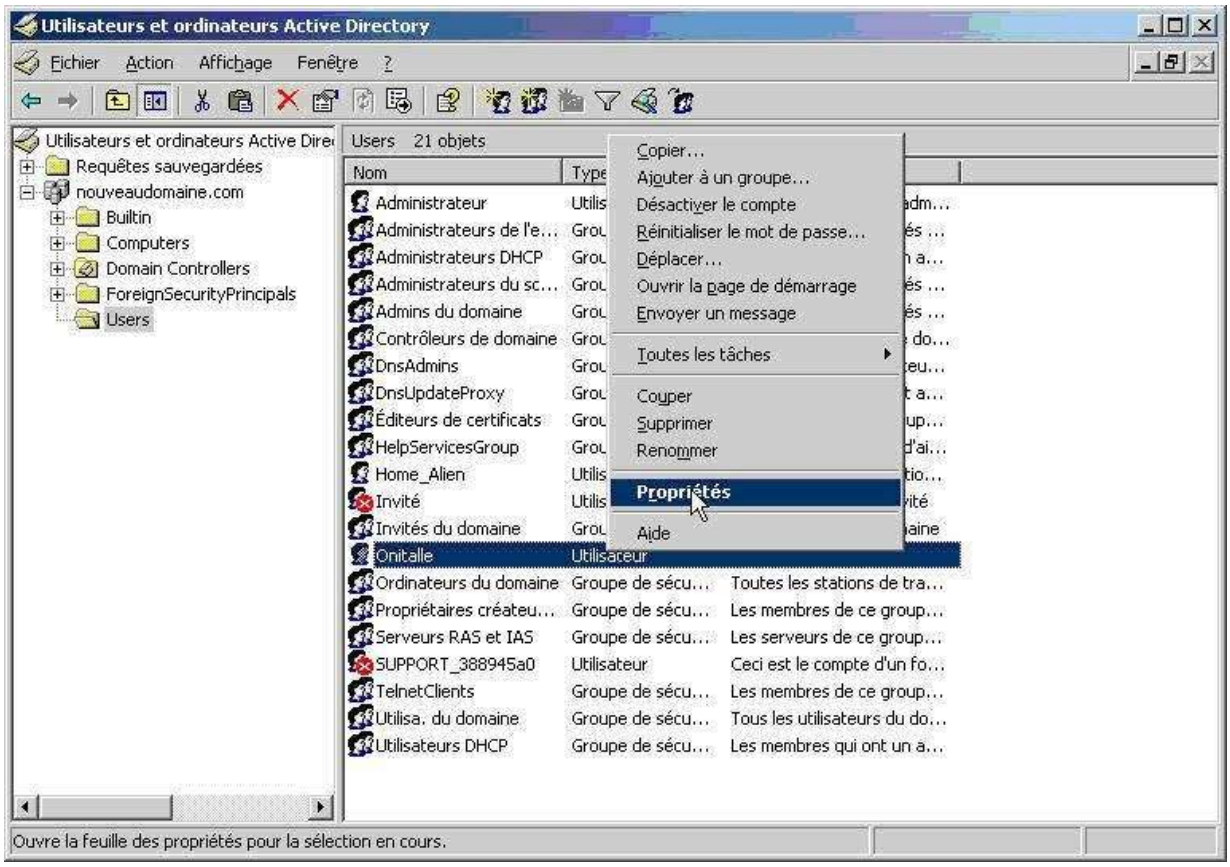
4) Dans la boîte de dialogue Propriétés des ports, cliquez sur Mini port WAN (PPTP), puis sur Configurer.

5) Dans la boîte de dialogue Configurer le périphérique, sélectionnez le nombre maximum de ports pour le périphérique, puis sélectionnez les options permettant de spécifier si le périphérique accepte les connexions entrantes uniquement ou à la fois les connexions entrantes et sortantes.

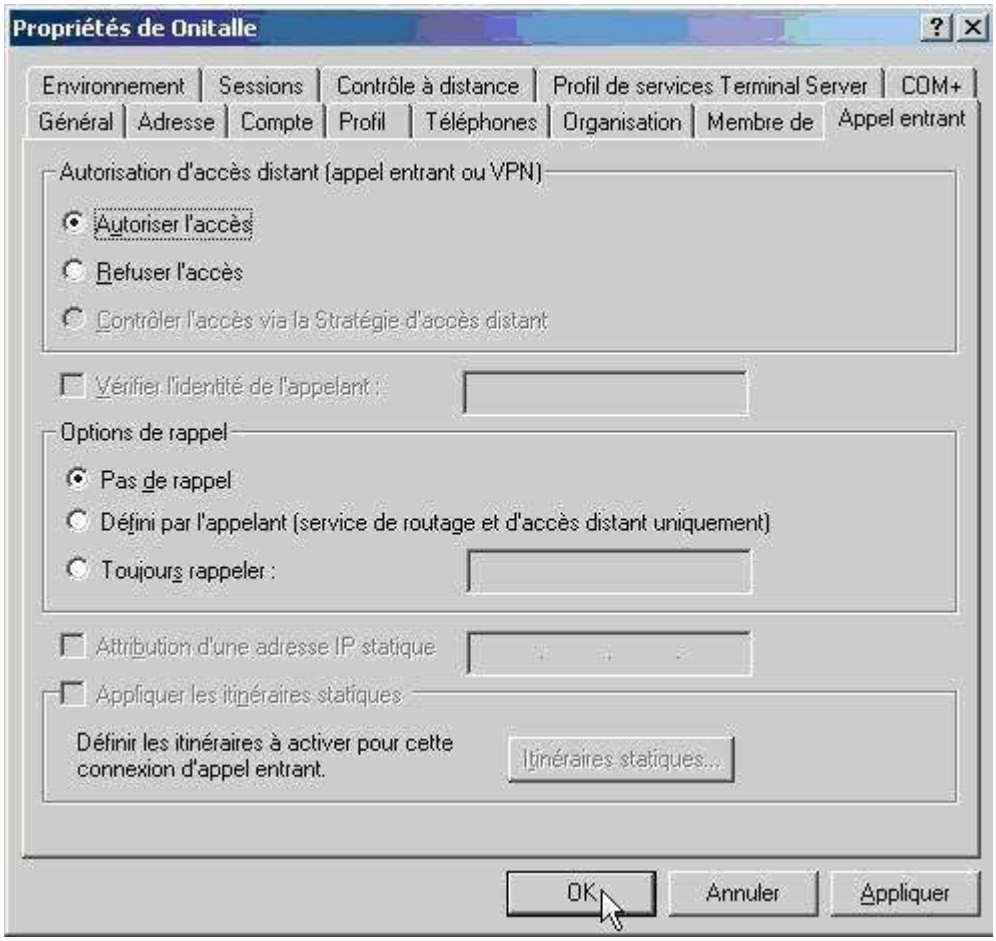
Comment autoriser un utilisateur à se connecter à un serveur VPN installé sur une plate forme Windows 2003 Server ?

1- Cliquez sur **Démarrer \Outils d'administration\Utilisateurs et ordinateurs** ou éxecuter : **DSA.MSC**

2- Sélectionnez l'utilisateur désiré, afficher le menu contextuel avec le bouton droit, sélectionnez **Propriétés**.



3- Dans l'onglet **Appel entrant**, cocher la case **Autoriser l'accès**.



L'utilisateur est en mesure de se connecter au VPN.

3.4 Gestion des adresses et des serveurs de noms

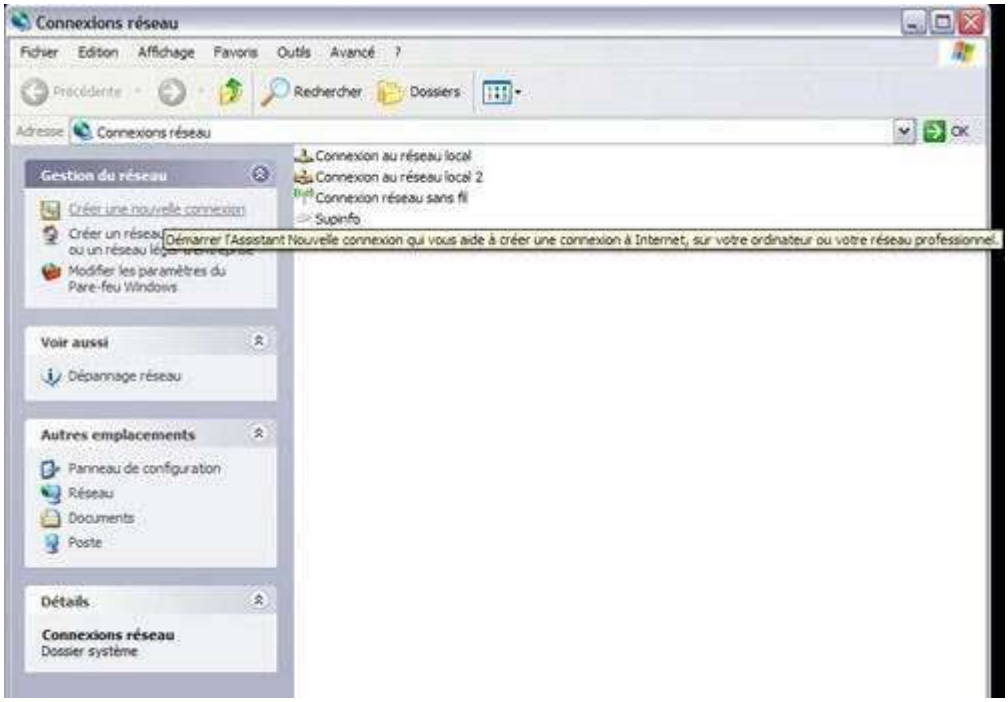
Le serveur VPN doit avoir des adresses IP à disposition, en effet il doit les attribuer à l'interface virtuelle du serveur VPN et aux clients VPN au cours de la phase de négociation IPCP (IP Control Protocol) du processus de connexion. L'adresse IP attribuée au client VPN est attribuée à l'interface virtuelle du client VPN.

Pour les serveurs VPN Windows 2003, les adresses IP attribuées aux clients VPN sont obtenues par adressage DHCP par défaut. Vous pouvez également configurer un groupe d'adresses IP statiques. Le serveur VPN doit également être configuré avec des serveurs de résolution de noms (généralement des adresses de serveurs DNS et WINS) à attribuer au client VPN au cours de cette négociation IPCP.

4. Connexion vpn d'un client 2000/XP

4.1. Création de la connexion du client

Dans les paramètres de connexion réseau, cliquez sur créer une nouvelle connexion :



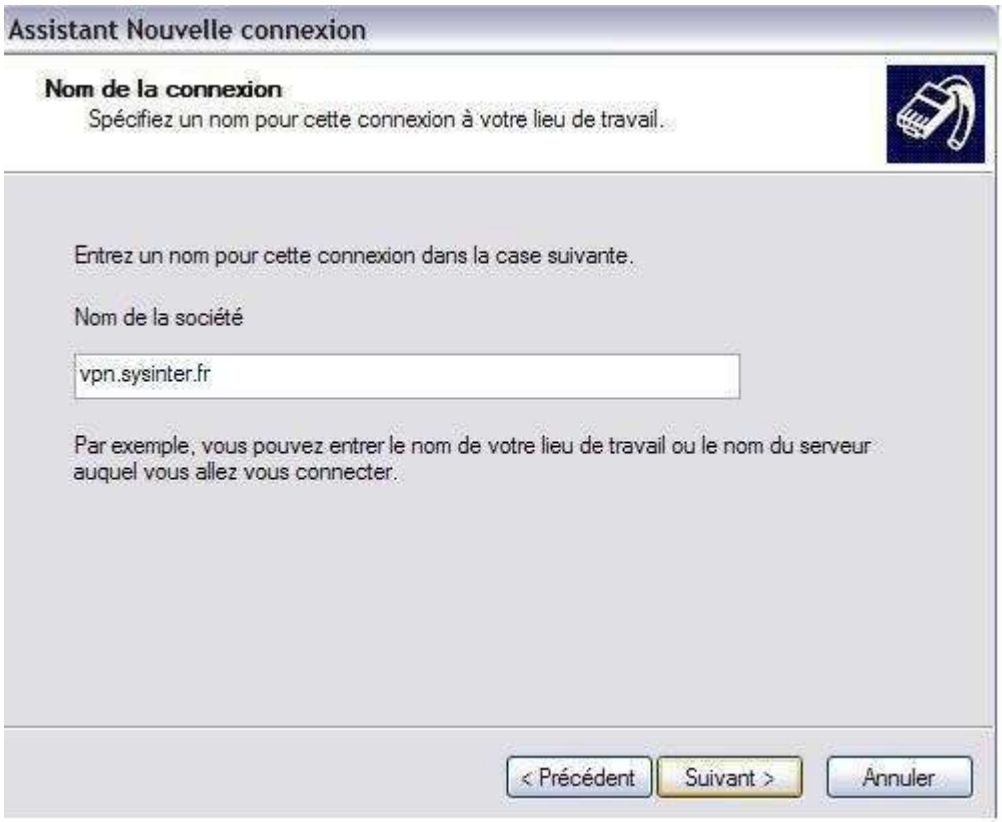
Cliquez ensuite sur suivant lors de l'apparition de la fenêtre.

Ensuite il vous sera demandé le type de connexion à choisir :

Ensuite, après avoir cliqué sur suivant, choisissez connexion VPN:

Après avoir valider ce choix, Entrez le nom de l'entreprise :

Saisissez ensuite l'adresse ou le nom du VPN :

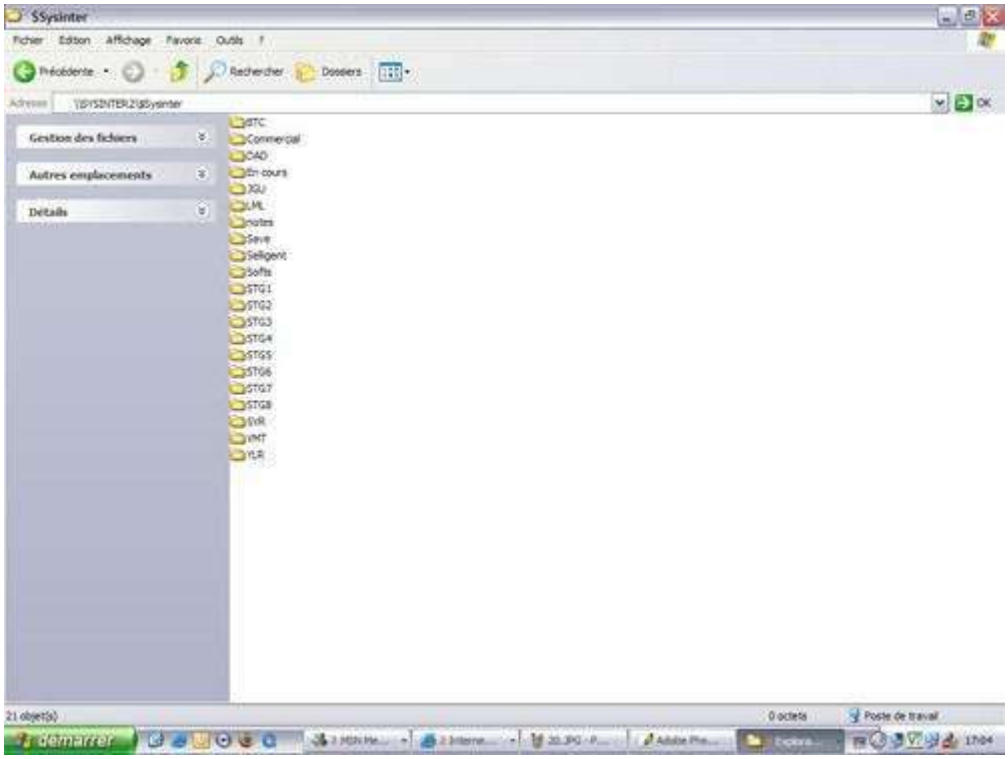


Cliquez sur suivant, puis valider la création de la connexion, un raccourci peut être fait sur le bureau pour que les utilisateurs "delta" puissent se connecter facilement.

4.2. Connexion du client une fois configuré

Cliquez sur le raccourci propre à la connexion, saisissez votre nom d'utilisateur ainsi que le mot de pas et le domaine fournit par votre administrateur Réseau et cliquez sur "se connecter":

Vous avez à présent au réseau de votre entreprise :



Conclusion

Pour une entreprise, le choix de mettre en place un VPN pour les sites et postes distants peut être très utile.

En effet d'un coût faible par rapports aux atouts que cela peut apporter, le VPN se présente comme une solution complète et fiable pour relier des réseaux distants entre eux. De nos jours, les performances et les capacités des accès Internet que ce soit pour l'usage domestique ou professionnel permettent d'utiliser cette technologie sans contraintes.

Pour le client, l'utilisation est très simple et l'utilisateur peut travailler de chez lui tout en enregistrant ses données sur le serveur habituel de son entreprise par exemple et pour les responsables de l'installation, mis à part des mises à jour de configuration, il y'a peu de maintenance.

Les réseaux VPN sont donc des solutions peu coûteuses comparées au prix de lignes dédiées et sécurisées permettant l’accès à un réseau d’entreprise.