TP N°3 Réseaux 2A

Mise en place d'un client/serveur VPN sous Windows XP

Module TR-C8

1. Objectif

Le VPN repose sur un protocole de tunnelisation permettant la connexion sécurisée sur un réseau distant via une connexion WAN. De nombreuses entreprises utilisent le VPN pour connecter des utilisateurs distants, via Internet , pour leur permettre d'accéder aux ressources de l'entreprise comme par exemple un serveur d'applications.

Il est important pour les connexions VPN d'assurer la confidentialité des données échangées. En effet, on rappelle qu'Internet est utilisé comme support de transmission, donc il y a toujours un risque d'interception des données. La connexion entre client et serveur ne s'établit que si le cryptage des données est activé, auquel cas, la connexion est refusée. Ainsi, une identification des utilisateurs, un cryptage des données et la gestion d'adressage sont largement suffisants dans ce type de cas. Le protocole le plus approprié est donc PPTP.

Pour le protocole PPTP trois mécanismes sont mis en place : *l'authentification de l'utilisateur*, *la gestion de l'adressage* et *le cryptage des données*.

L'authentification de l'utilisateur se fait généralement avec un login et un mot de passe. En PPTP, cette authentification est gérée par le protocole « MS CHAP V2 » *(Microsoft Challenge Handshake Authentification Protocole)*. Le fonctionnement peut se résumer par ces étapes :

1. Le serveur demande au client de s'identifier. Pour cela il envoie un identifiant de session et une chaîne aléatoire.
2. Le client renvoie son nom, une chaîne aléatoire complémentaire à celle envoyée par le serveur, son mot de passe, son identifiant de session et un cryptage de la chaîne envoyée par le serveur.
3. Le serveur répond et accorde la connexion en fonction des éléments précédemment cités.
4. Le client utilise la connexion si la réponse d'authentification est correcte.

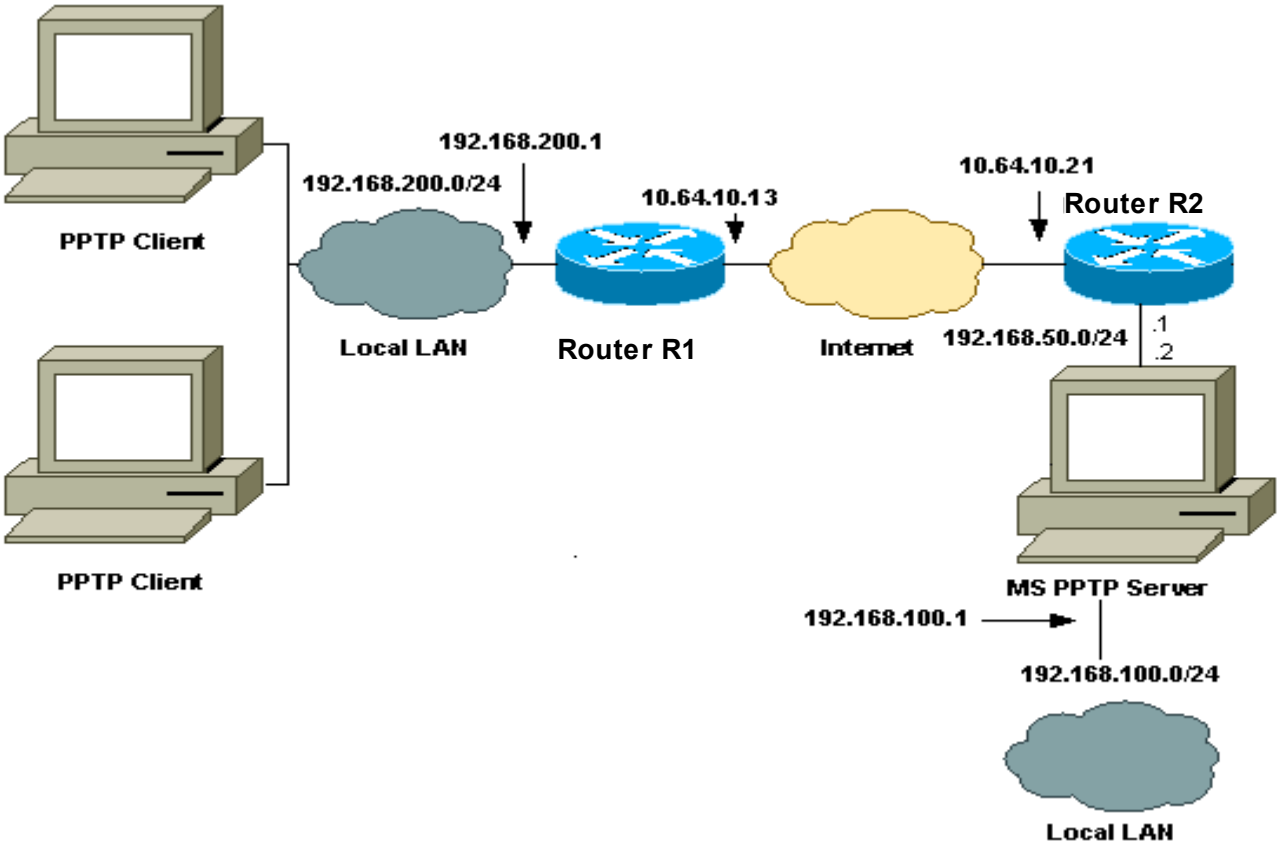
Le cryptage est assuré par le protocole MPPE *(Microsoft Point-to-Point Encryption)* . Ce

protocole chiffre les données avec l'algorithme RSA/RC4.

La gestion de l'adressage peut se faire de deux manières. Le plus couramment, le serveur VPN attribue une adresse IP au client VPN selon une plage d'adresses définies. Cette technique permet de définir un nombre restreint de clients VPN sur le réseau. Un serveur DHCP peut aussi attribuer de manière automatique une adresse qui sera sous la forme 169.254.X.X .

2. Créer un serveur VPN :

Nous allons maintenant configurer une machine sous Windows XP Pro de notre réseau local pour accepter des connexions VPN. Voici la topologie d'étude:

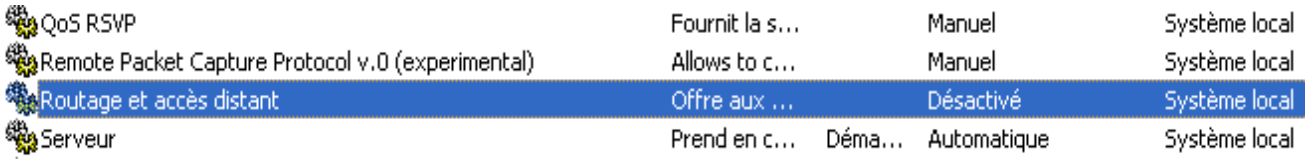


Pour mettre en place notre liaison VPN, il faut tout d'abord activer le service RAS (Routage et accès distant). Par défaut, celui-ci n'est pas démarré.

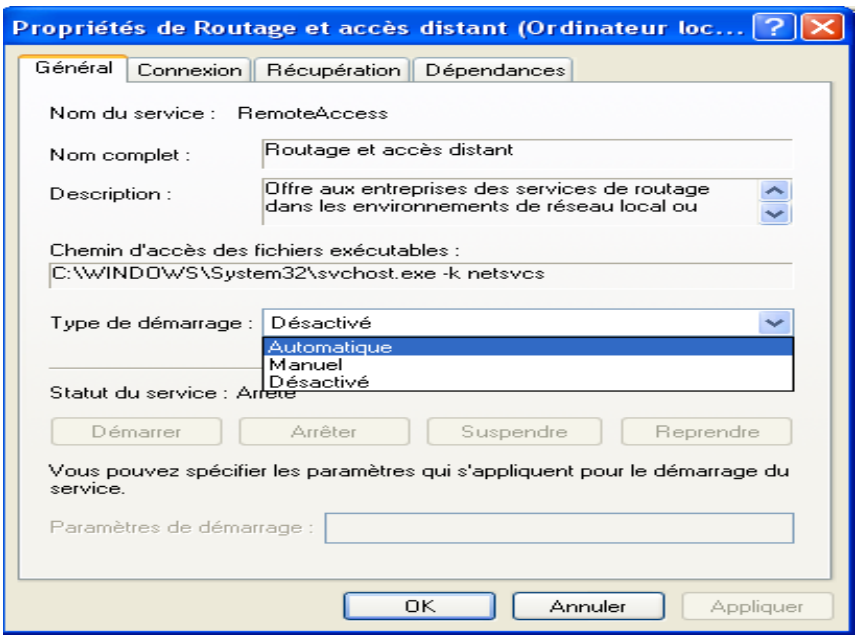
Démarrage du Routage et accès distant:

1. Dans Panneau de Configuration, sélectionner l'onglet Outils d'administration.

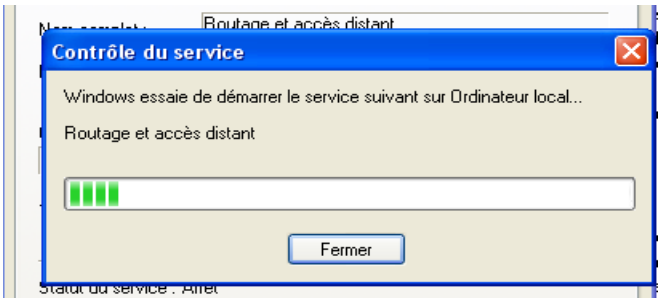
2. Sélectionner l'icône Service.
3. Chercher la ligne « Routage et accès distant ».



4. Faites un clique droit puis « Propriétés ». Vous arrivez dans une boîte de dialogue. Dans le champ « Type de démarrage », choisissez « **Automatique** ».



5. Cliquez sur « Démarrer » pour lancer le service.



<u>Paramétrage de la connexion VPN</u> :

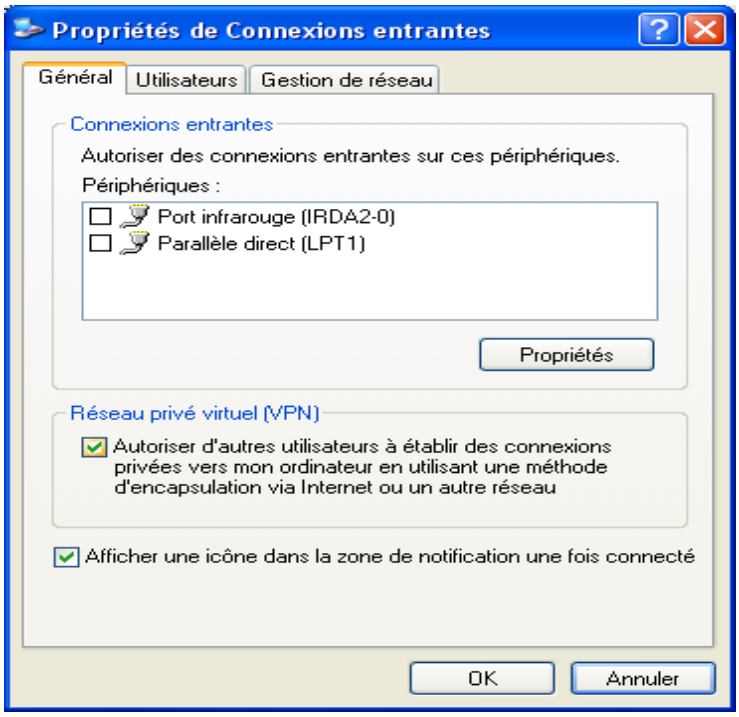
6. Rendez-vous dans « Connexions réseaux et accès

distants » toujours dans la Panneau de configuration.

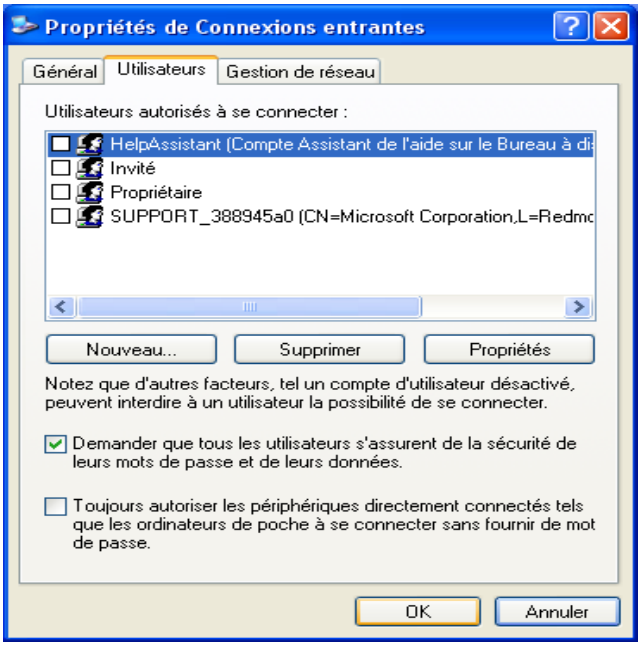
7. Double cliquez sur la nouvelle connexion entrante 

(XP) ou clique droit puis Propriétés.

8. Dans l'onglet Général, veillez à ce que les cases « Autoriser d'autres utilisateurs à établir des connexions privées vers mon ordinateur en utilisant une méthode d'encapsulation via Internet ou un autre réseau » et « Afficher une icône dans la zone de notification une fois connecté » soient cochées.



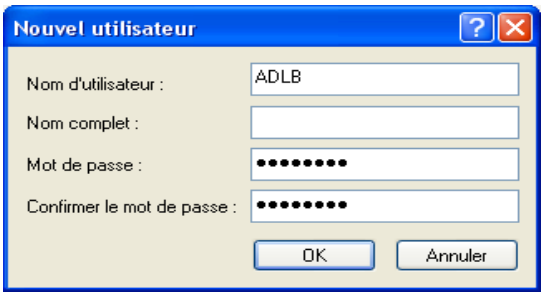
La première autorise les connexions VPN, la deuxième informera par une icône que la connexion VPN est établie.



9. Dans l'onglet Utilisateurs, cocher la case « Demander que tous les utilisateurs s'assurent de la sécurité de leurs mots de passe et de leurs données ». Cette option permettra de crypter en MSCHAP les mots de passe.

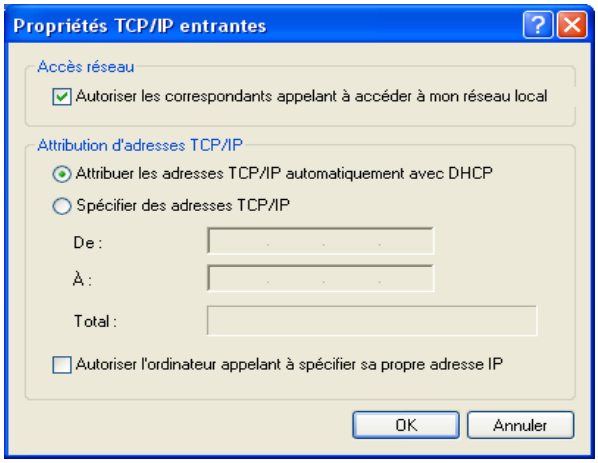
10. Pour les utilisateurs, il est préférable de créer un nouveau profil. Pour cela cliquez sur « Nouveau ».

11. Donnez un nom d'utilisateur et un mot de passe avec de préférences des caractères numériques et alphabétique (minuscule et majuscule) ainsi que des caractères du type " :", "/"où "% ". Cliquez sur « OK » pour confirmer.



12a. Passons au dernier Onglet « Gestion du Réseau ». Placez vous sur « Protocole Internet TCP/IP » et cliquez sur « Propriétés ». Une nouvelle fenêtre s'ouvre (Propriétés TCP/IP entrantes). Cochez la case "Autoriser les appelants à accéder à mon réseau local". Cette option permet aux personnes connectées d'accéder à un autre poste sur votre réseau local.

À partir d'ici, la gestion de l'adressage peut se faire de deux manières. Le plus couramment, le serveur VPN attribue une adresse IP au client VPN selon une plage d'adresses définies. Cette technique permet de définir un nombre restreint de client VPN sur le réseau:



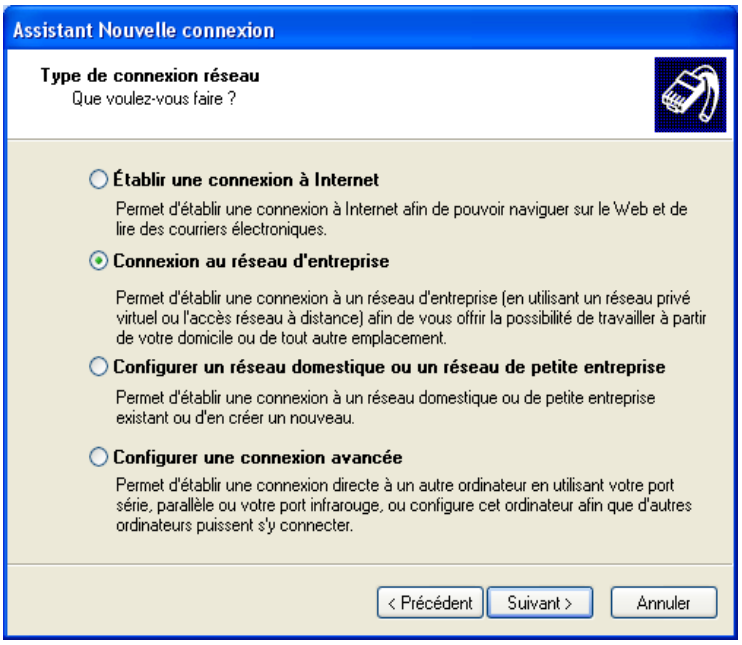
12b. On souhaite définir un adressage afin de mieux gérer les connexions. Dans ce cas, vous définissez une plage d'adresse non utilisée dans votre réseau local. Dans l'exemple, 3 adresses seront disponibles. La première sera attribuée au serveur, et le reste aux différents clients.

13. Cliquez sur OK pour valider. La partie de configuration du Serveur est maintenant terminée.

3. Créer un client VPN :

Maintenant il faut configurer le client VPN. Encore ici, 2 possibilités: (1) Soit le réseau possède une IP fixe pour Internet et celui-ci est toujours accessible, (2) Soit il possède une IP dynamique fournie par son FAI et là il faut associer ces adresses IP changeantes à un nom de domaine fixe (création d'un compte DynDNS).

1. Sur le poste qui va se connecter au serveur VPN, allez dans Panneau de Configuration et double-cliquez sur « Connexions réseaux et accès distants ».



2. Cliquez sur "créer une nouvelle connexion". Sélectionner ensuite « Connexion au réseau d'entreprise » puis cliquez sur Suivant
Sélectionnez « Connexion réseau privé virtuel » et faites « Suivant ».

Rentrer le nom pour la connexion et faites « Suivant ».
Enfin entrer l'adresse IP fixe du serveur ou le nom de domaine dans le cas d'un dynDNS dans le champ"Nom d'hôte ou adresse IP" et faites « Suivant », puis « Terminer ».

3. Une nouvelle interface apparaît alors dans "Connexions réseaux et accès à distance" sous le nom de votre connexion.

4. Faites un Clique-droit dessus puis « Propriétés ». Une nouvelle interface se lance.

5. Avant de se connecter au serveur il est indispensable de procéder à quelques réglages en cliquant sur le bouton « Propriétés ». Dans l'onglet Gestion de réseau sélectionnez le protocole PPTP dans la liste. Sélectionnez le protocole TCP/IP et cliquez sur propriétés:

La fenêtre qui s'affiche permet de définir l'adresse IP que la machine cliente aura lors de l'accès au serveur VPN. Saisissez le nom d'utilisateur et le mot de passe configurés dans la partie Serveur VPN et cliquez sur « Se Connecter ».

La connexion s'établit après les phases de vérification et d'authentification de l'utilisateur. La connexion entre le serveur et le client VPN est maintenant établie. Une icône de notification apparaît en bas à droite, à côté de l'horloge.

4. Configuration des routers R1 et R2 :

- Sur les deux routers R1 et R2, il faut configurer la translation d'adresses NAT-PT.

Exemple de configuration de NAT-PT sur R1

```
interface FastEthernet0/0
ip address 10.64.10.13 255.255.255.0
   !--- Defines the interface as external for NAT.
      ip nat outside

interface FastEthernet0/1
ip address 192.168.200.1 255.255.255.0
   !--- Defines the interface as internal for NAT.
      ip nat inside
```

```
!--- Indicates that any packets received on the inside interface permitted
!--- by access list 101 share one public IP address (the address on Fa0/0).

ip nat inside source list 101 interface FastEthernet0/0 overload
ip route 0.0.0.0 0.0.0.0 10.64.10.21
access-list 101 permit ip any any
```

- Sur le routeur R2, il faut rediriger les connexions VPN (port 1723, protocole PPTP) vers le serveur qui traitera les demandes de connexions. Cette redirection de port (PAT) se fait en fournissant:
  1. l'adresse IP locale de la machine sur laquelle on souhaite rediriger un port, 192.168.50.2 dans notre cas.
  2. Protocole de couche 4 (TCP, UDP).
  3. Le numéro de port. Le port utilisé par le protocole VPN PPTP sous Windows XP Pro est le 1723.

Exemple de configuration de redirection de port sur R2

```
!--- Static port translation for the Microsoft PPTP server on TCP port 1723
!--- share one public IP address (the address on Fa0/0).

ip nat inside source static tcp 192.168.50.2 1723 interface FastEthernet0/0 1723
```

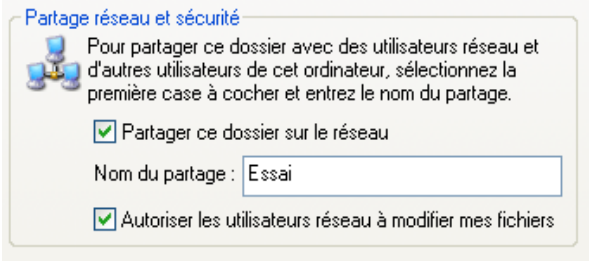
5. Accès au Serveur :

L'intérêt de la mise en place de connexions VPN est l'accès aux ressources pour des personnes se situant sur des sites distants. On se propose d'accéder à un dossier partagé sur le serveur VPN:

Partage du dossier sur le Serveur:

1. Quel que soit l'endroit où se trouve le dossier, faites un clique droit puis « Propriétés ». Aller dans l'onglet « Partage ».

2. Cochez la case « Partager ce dossier sur le réseau ». Vous pouvez donner un nom à ce partage. Cochez si vous le souhaitez « Autoriser les utilisateurs réseau à modifier mes fichiers ».



3. Cliquez sur « Appliquer » puis sur « Ok » pour valider. Une main doit apparaître sous le dossier signifiant ainsi que le dossier est bien partagé.

Accès aux dossiers partagés par le client:

Pour pouvoir accéder au dossier précédemment partagé par le serveur, suivez les étapes suivantes :

Attention:
Il faut posséder un accès réseau (dans notre cas, notre liaison VPN) et d'une autorisation de connexion sur le serveur pour réaliser la suite des manipulations !

4. Dans Panneau de Configuration, double-cliquez sur « Connexions réseaux et accès distants ». Cliquez sur Favoris Réseaux sur la gauche. Cliquez ensuite sur « Ajouter un favori réseau ». Une fenêtre « Assistant Ajout d'un favori réseau » s'ouvre.

5. Cliquez sur « Suivant ». Sélectionner « Choisissez un autre emplacement réseau. Spécifiez l'adresse d'un emplacement réseau. Cliquez ensuite sur « Suivant ». Entrez l'adresse réseau de l'emplacement du dossier. La syntaxe est « \\serveur\Essai » ou serveur est l'adresse IP ou le nom de domaine du serveur et Essai le dossier partagé. Dans le cas où le dossier partagé serait sur un poste quelconque, on réalise la même opération:Adresse = \\Adresse-IP-du-Poste\Nom-Dossier-Partagé