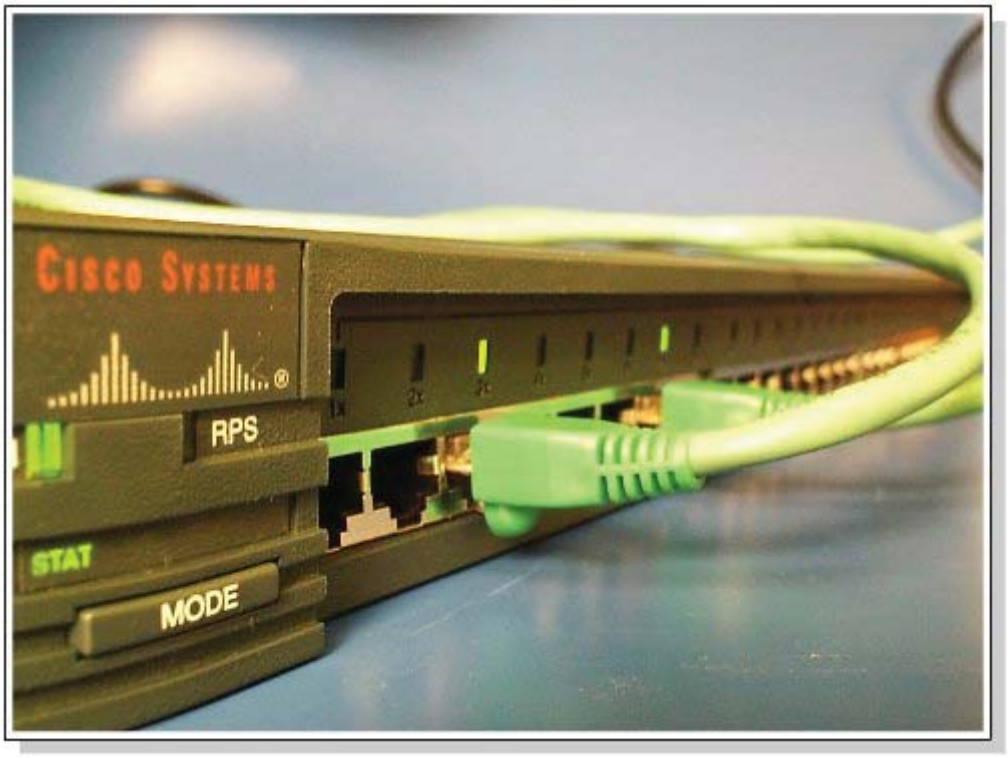
TP : Réseau embarqué sécurisé



TP Mise en place d'un LAN

1) Objectifs

L'étudiant devra être capable :

-D'identifier les différents matériels dans le réseau (routeur, switch, hub, PC, etc....)

-De câbler les différents matériels suivant une architecture réseau

-De configurer les routeurs face aux exigences de sécurité et de configuration

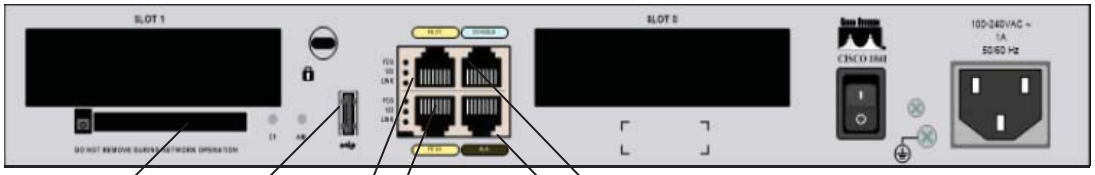
- De vérifier par des tests élémentaires la conformité de l'architecture du réseau local

2) Pré-requis

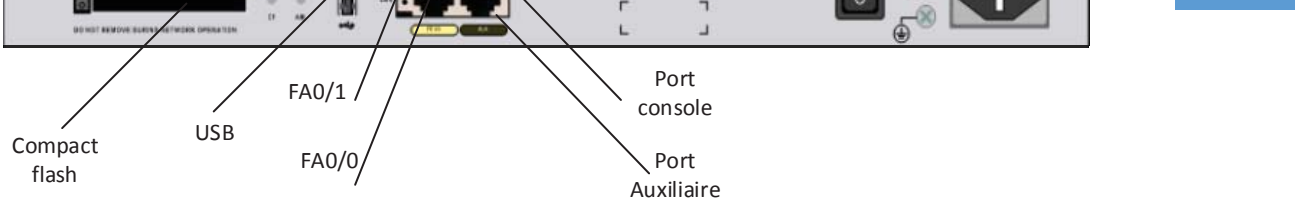
Cours sur les réseaux à technologie TCP-IP et le chiffrement.

3) Les routeurs CISCO











WAN G-SHDSL



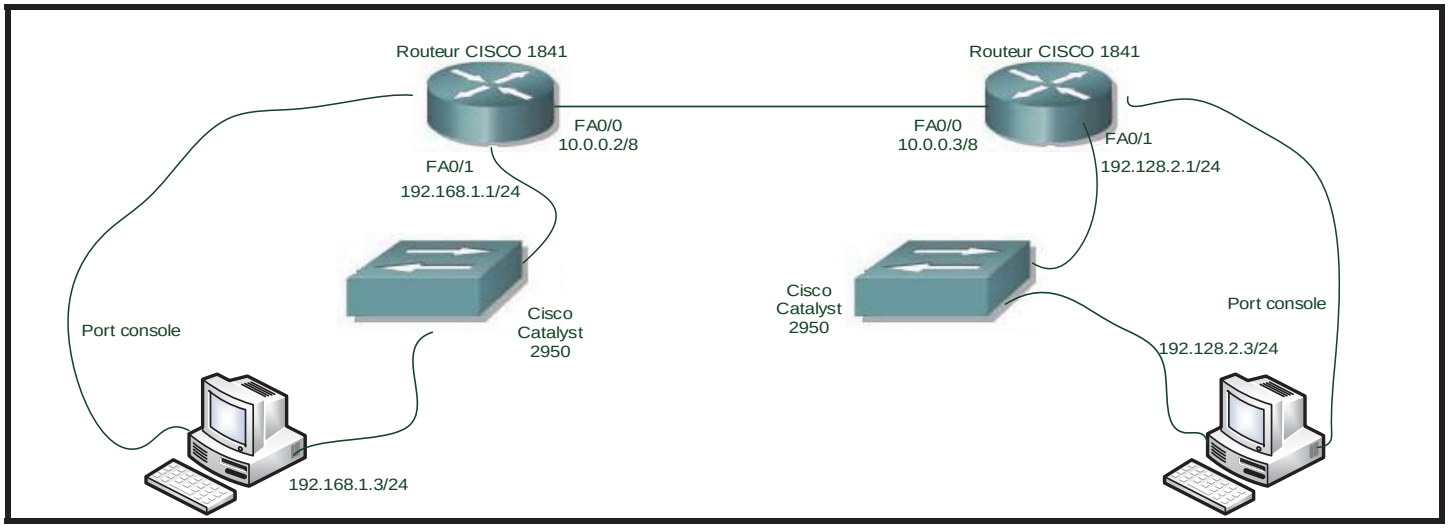
WIC-1T WAN serial 1 port



WIC-2T WAN serial 2 ports

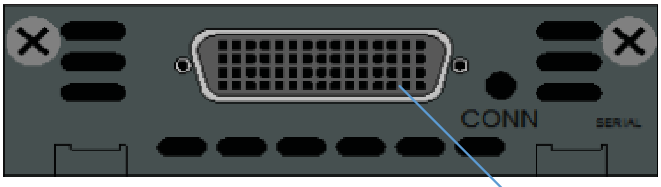
4) Configuration de deux routeurs

4.1) Réalisez le montage suivant :



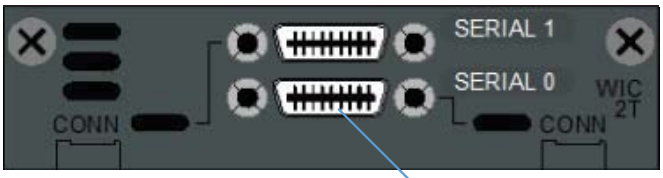
4.2) En vous aidant du dossier annexe, configurez les routeurs afin de respecter l'architecture réseau précédente (on utilisera un routage statique).
La liaison entre les deux routeurs sera du type fast Ethernet
4.2.3) Vérifiez si les 2 machines se voient et interprétez le paramètre TTL
4.2.4) Supprimez le routage statique et mettez en place un routage dynamique du type RIP.
4.2.5) Vérifiez si les 2 machines se voient et interprétez le paramètre TTL

Il est possible d'utiliser des liaisons séries du type WAN. Dans ce cas précis les routeurs disposent de carte WIC (WAN Interface communication). Les deux routeurs dont on dispose possèdent deux modèles de cartes WIC :
La WIC-1T qui dispose d'une interface série
La WIC-2T qui dispose deux interfaces séries



WIC-1T

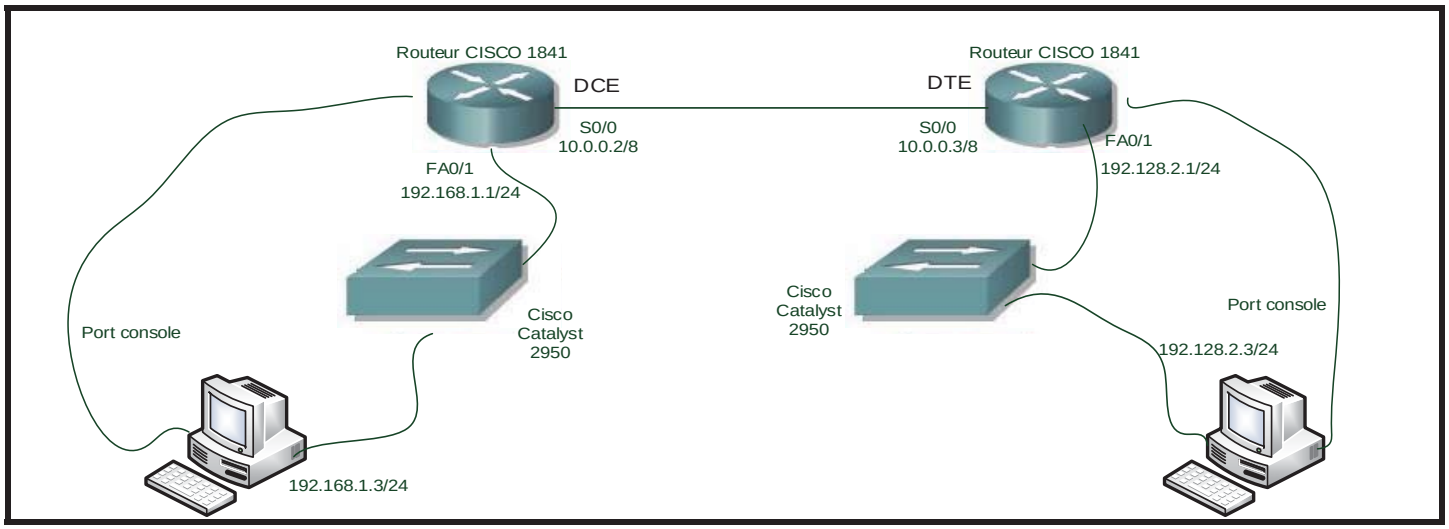
DB60



WIC-2T

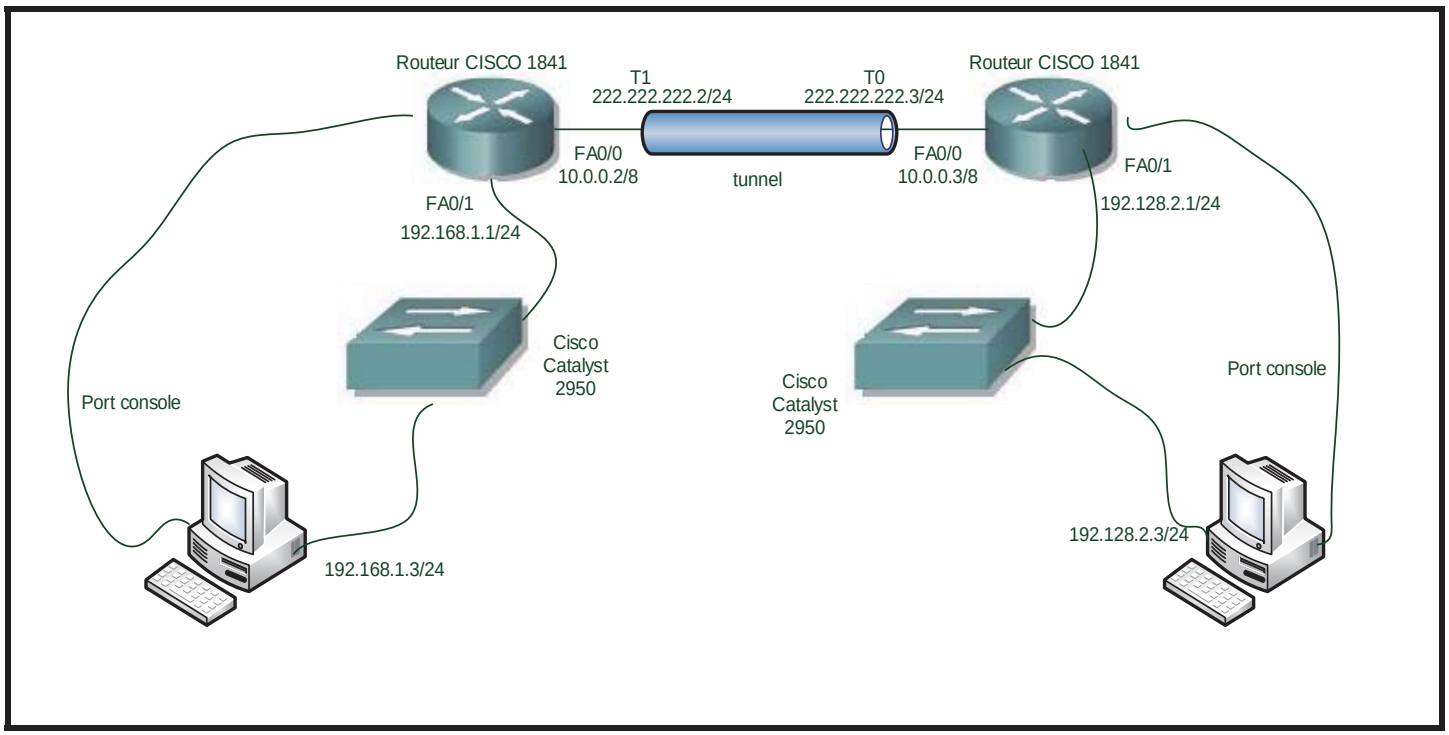
Smart serial

4.2.6) Si le routeur dispose d'une interface série, vérifiez le type de protocole série par défaut utilisé par le routeur.
Router#sh int S0



4.2.7) Réalisez le câblage ci-dessus, paramétrez et configurez afin d'assurer cette interface série du type WAN

Afin de sécuriser l'information qui circule entre les 2 routeurs on souhaite mettre en place un tunnel.



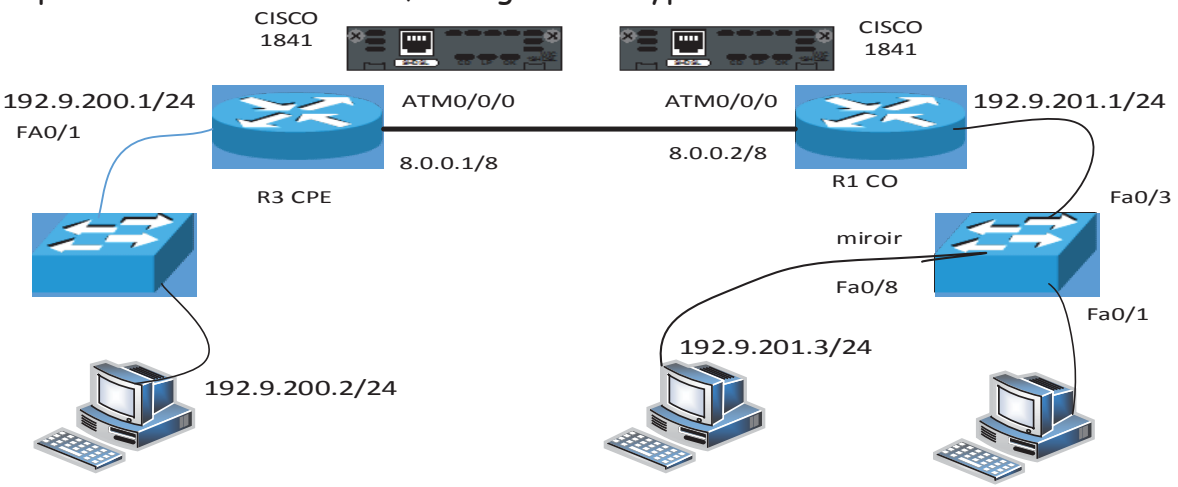
4.3) Mise en place d'un tunnel

4.3.1) en vous aidant du dossier annexe, configurez les routeurs afin de réaliser le tunnel précédent entre les 2 routeurs.

4.3.2) Vérifiez si les 2 machines se voient.

4.4) Mise en place d'une liaison du type HDSL-ATM

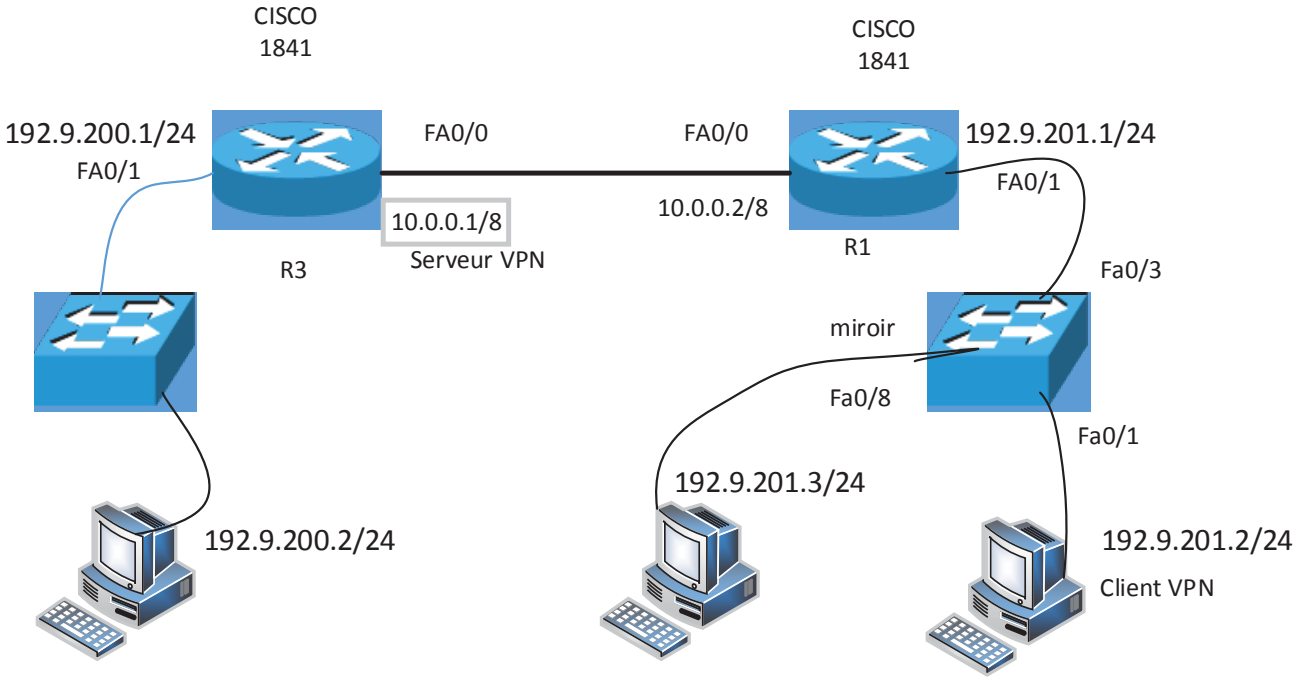
Dans ce cas de figure la liaison WAN entre les 2 routeurs est du type SDSL (voir dossier annexe).
En vous inspirant du dossier annexe, configurez ce type de liaison entre les deux routeurs



4.5) mise en place d'une liaison sécurisée entre un client et un serveur VPN

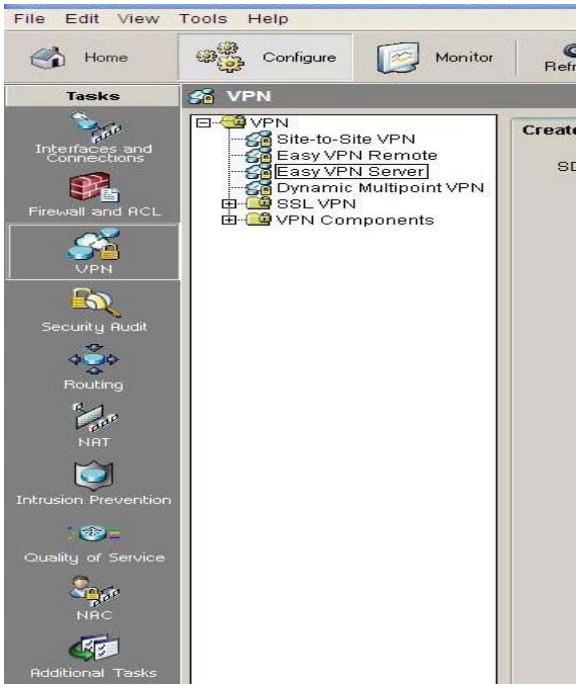
Les routeurs CISCO1841 disposent d'un module cryptographique matériel afin de mettre en place des liaisons sécurisées entre des systèmes informatiques. La première solution est de créer une sécurisation entre un client VPN et un serveur VPN.

Le serveur VPN est implanté dans le routeur R3 et sera appelé par un poste client VPN.

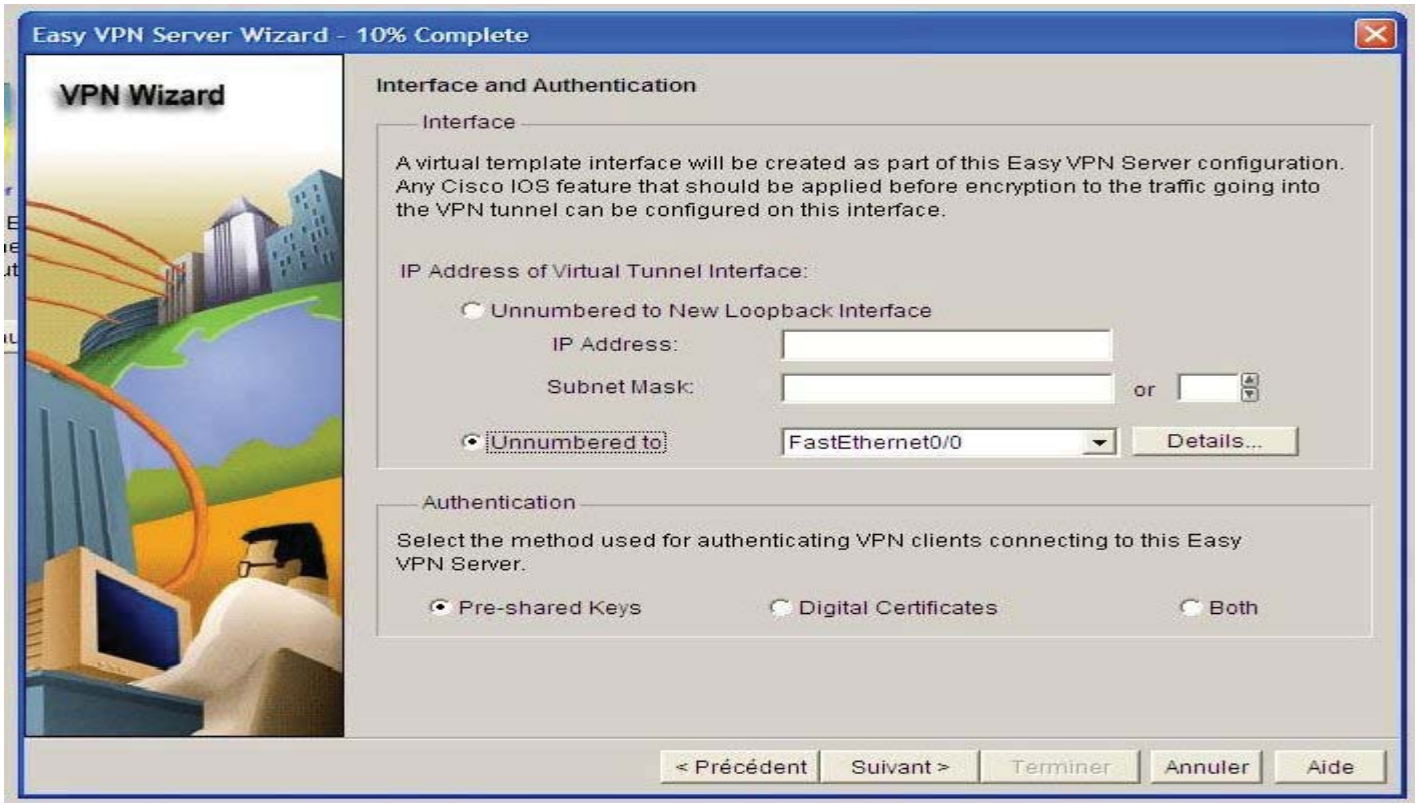


4.5.1) Mettre en place les différentes liaisons non sécurisées et vérifiez si les différents postes informatiques se voient sur le réseau.

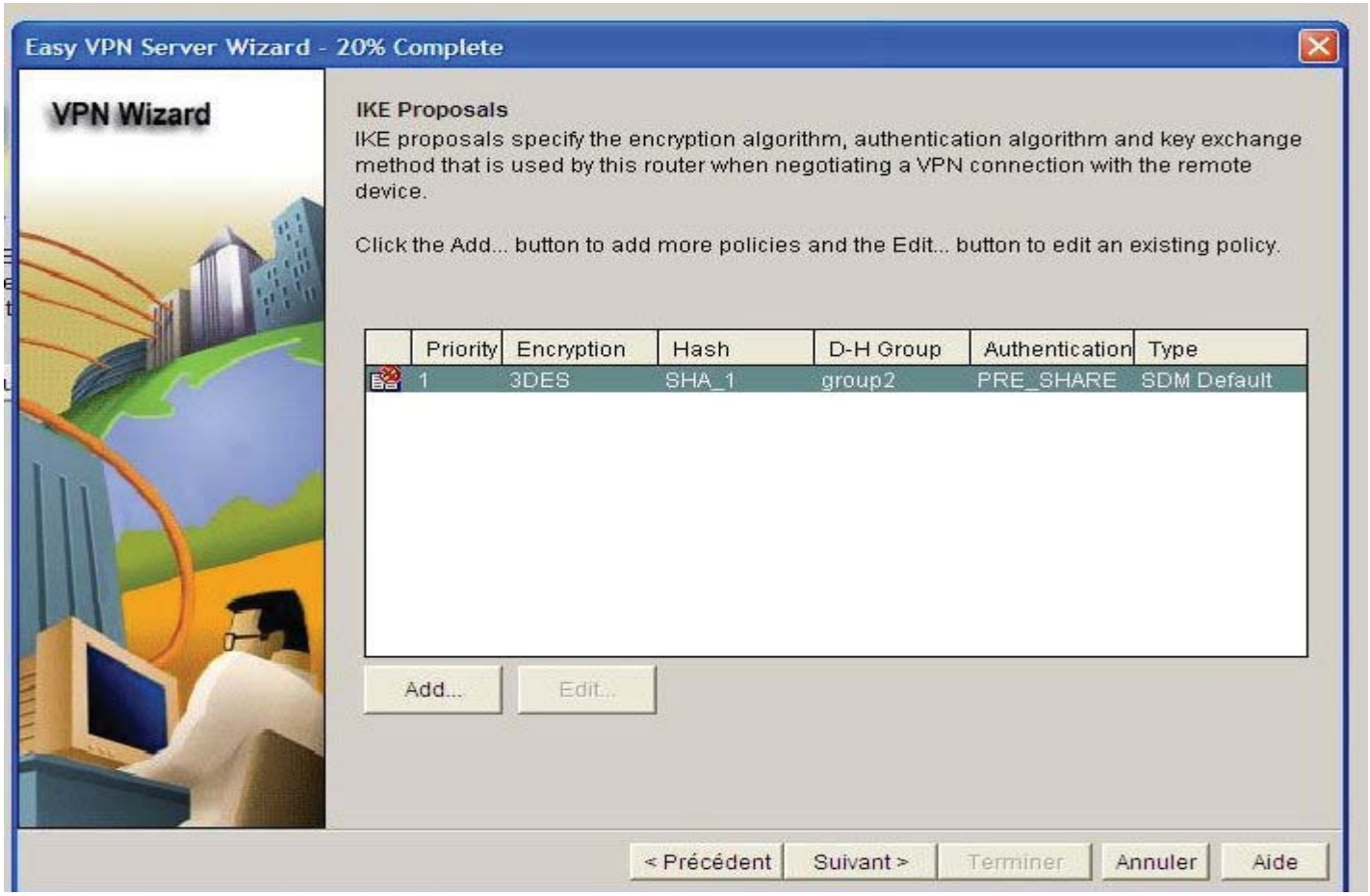
4.5.2) Suivre la démarche suivante pour mettre en place une liaison sécurisée entre le client VPN et le serveur VPN.
Grace à un client WEB (internet explorer), tapez l'adresse IP du serveur VPN afin de faire apparaitre la page de configuration.
Cliquez sur configure et sur VPN. La page suivante apparait :



Choisir Easy VPN Server, puis sélectionnez l'interface sur laquelle le serveur VPN reçoit les connexions des clients.



Choisir des clés pré-partagés et non un certificat digital pour la mise en place des éléments cryptographiques.
La fenêtre suivante nous donne la configuration de IKE (internet key echange) qui permet de mettre en place les protocoles pour l'échange des clés lors de l'ouverture du tunnel



Gardez la configuration par défaut :

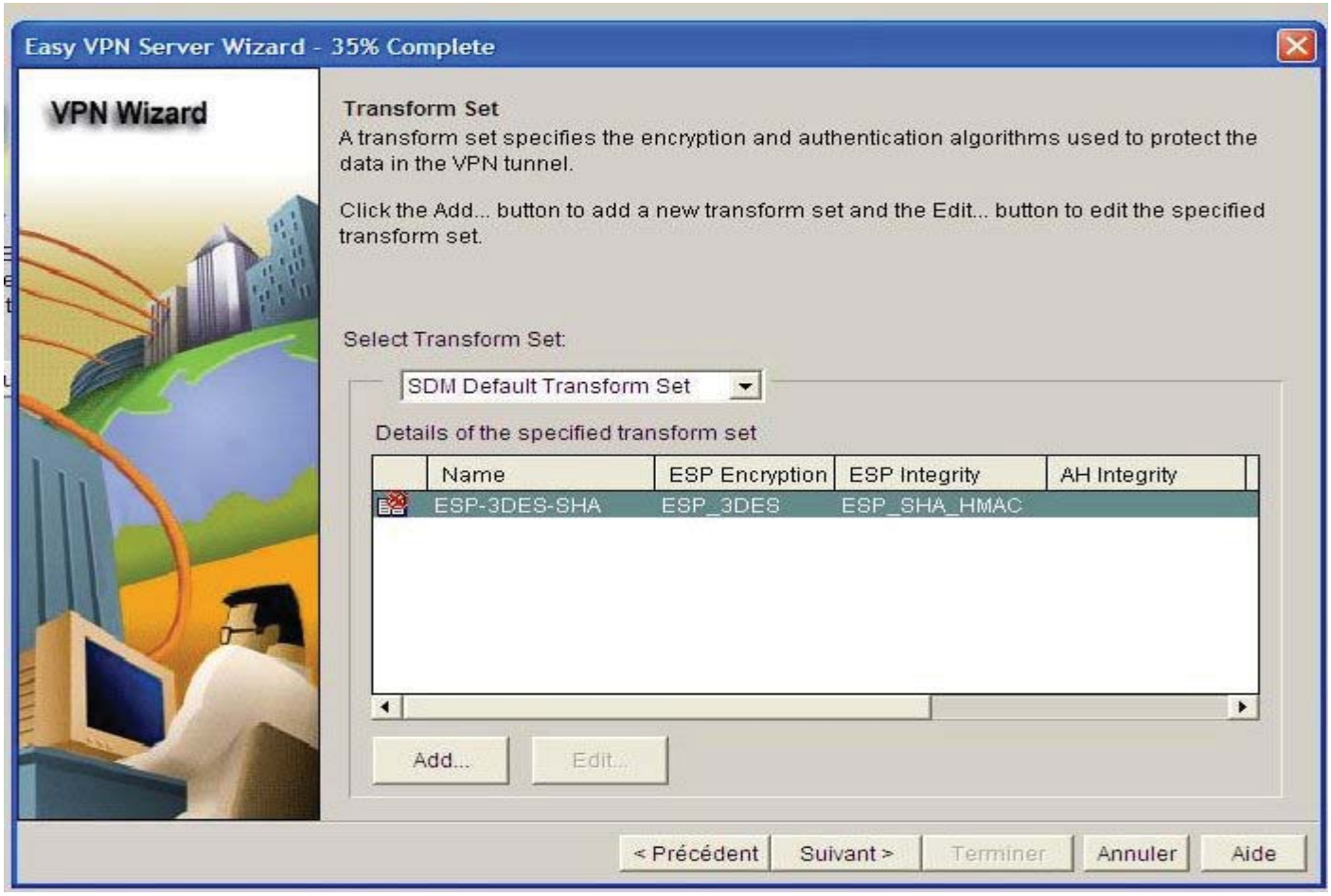
- ✓ L'échange de clé s'effectue grâce à un protocole diffie heffman groupe 2
- ✓ Une signature du message du type SHA version 1
- ✓ un chiffrement du type 3DES grâce aux clés pré-partagées

4.5.1) Le chiffrement est-il symétrique ou asymétrique ?

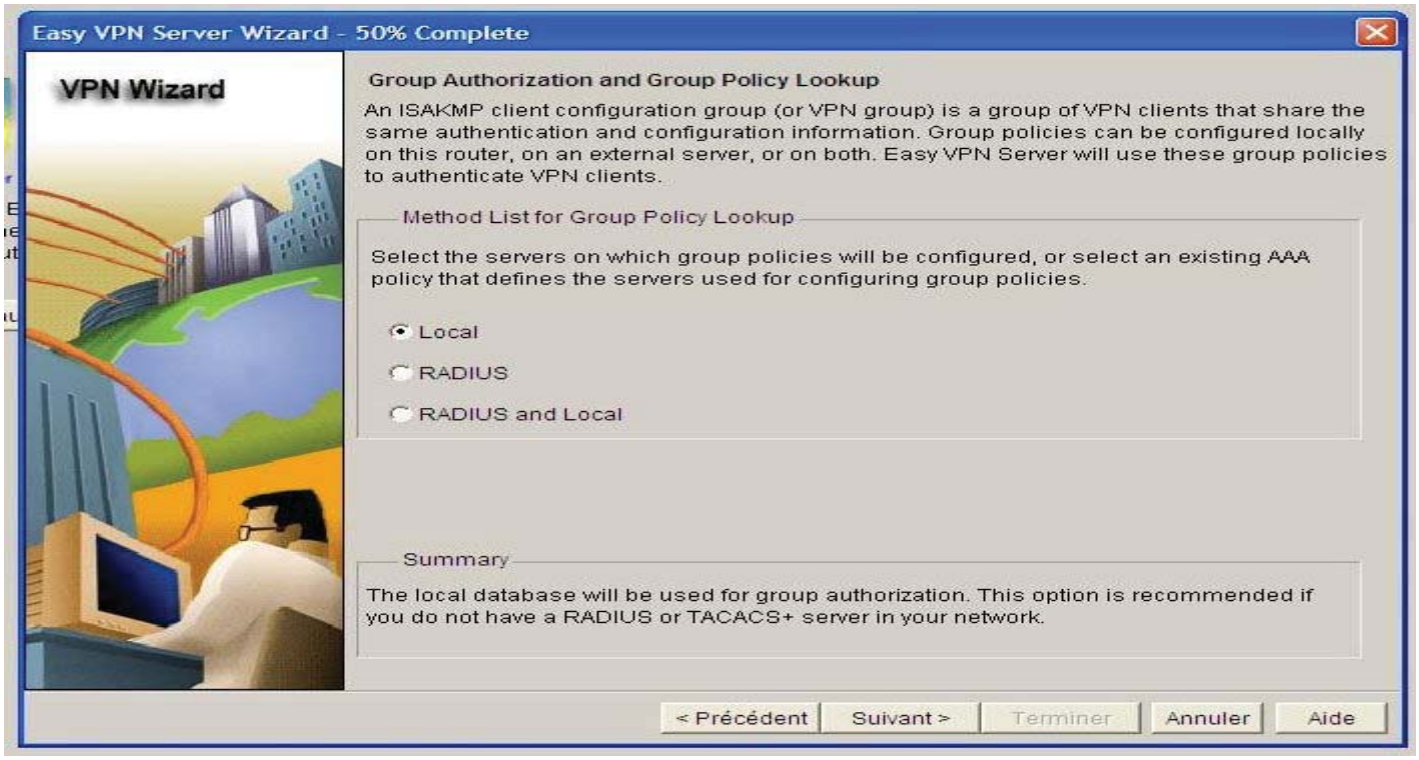
La page suivante transform set permet de configurer la façon dans les données vont être transformés et chiffrées dans le tunnel. On choisira la configuration suivante :

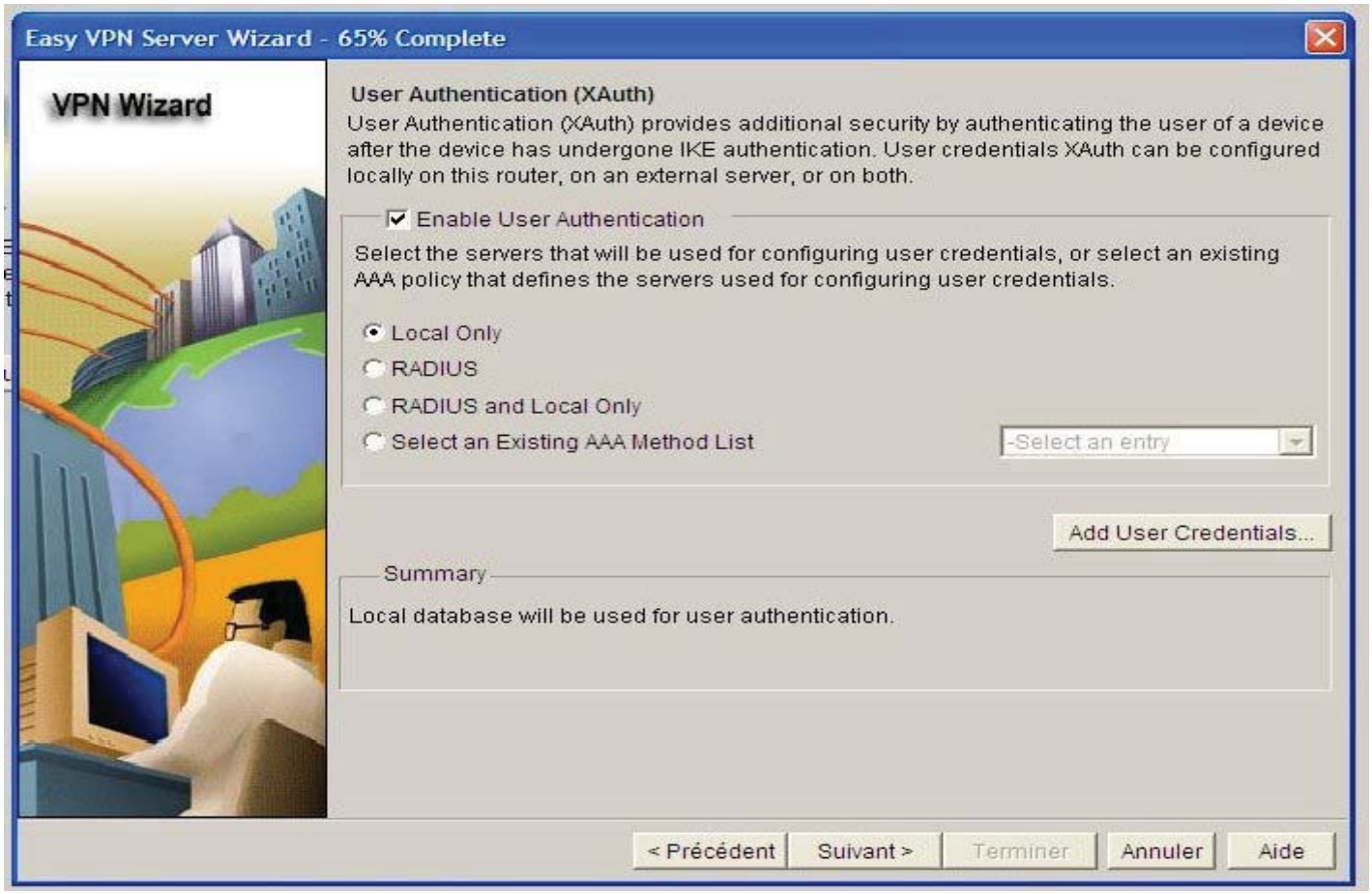
- ✓ un chiffrement symétrique du type ESP_3DES
- ✓ Une signature du type ESP_SHA_HMAC

4.5.2) Que permet d'assurer la signature ?

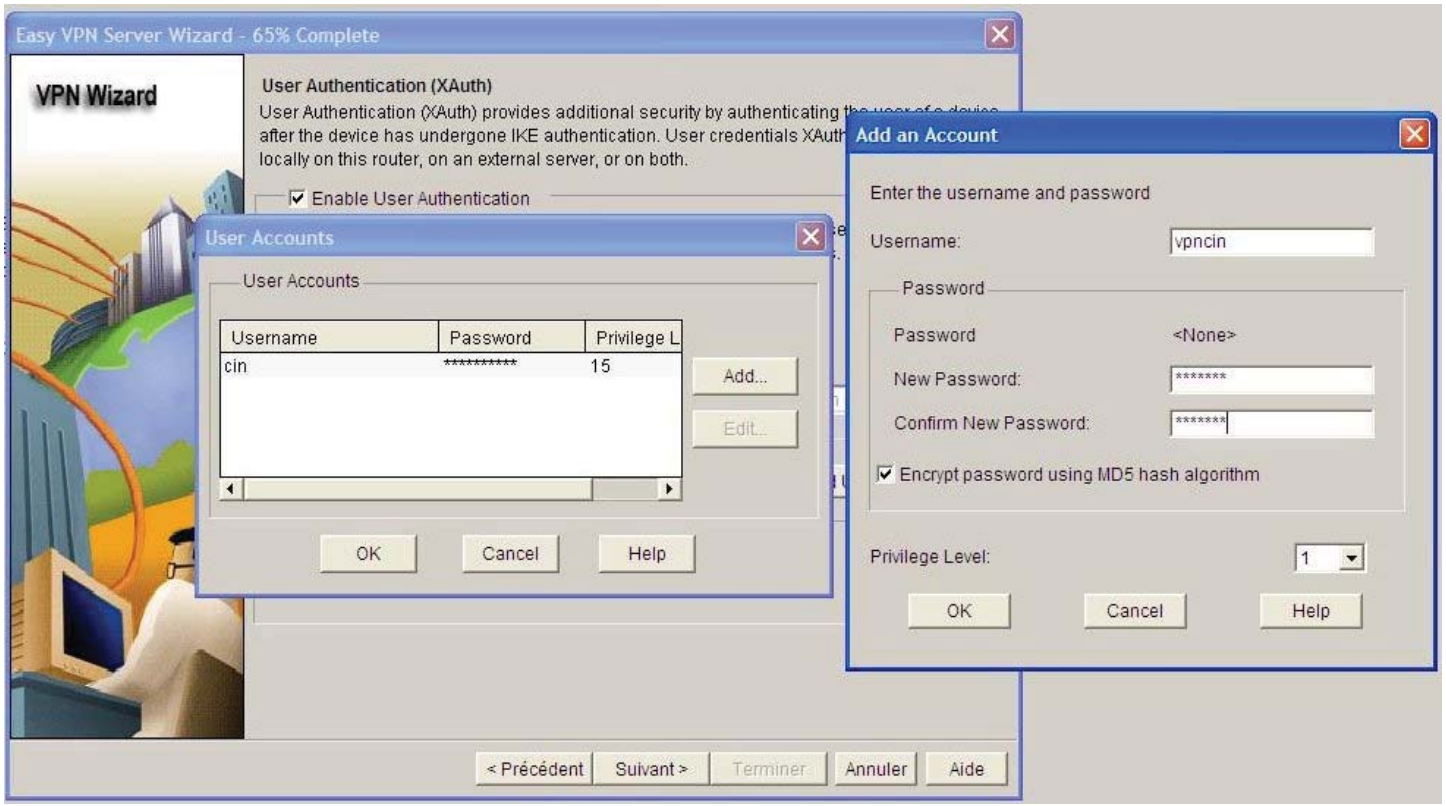


On va par la suite configurer un groupe de clients qui vont se connecter sur le serveur VPN

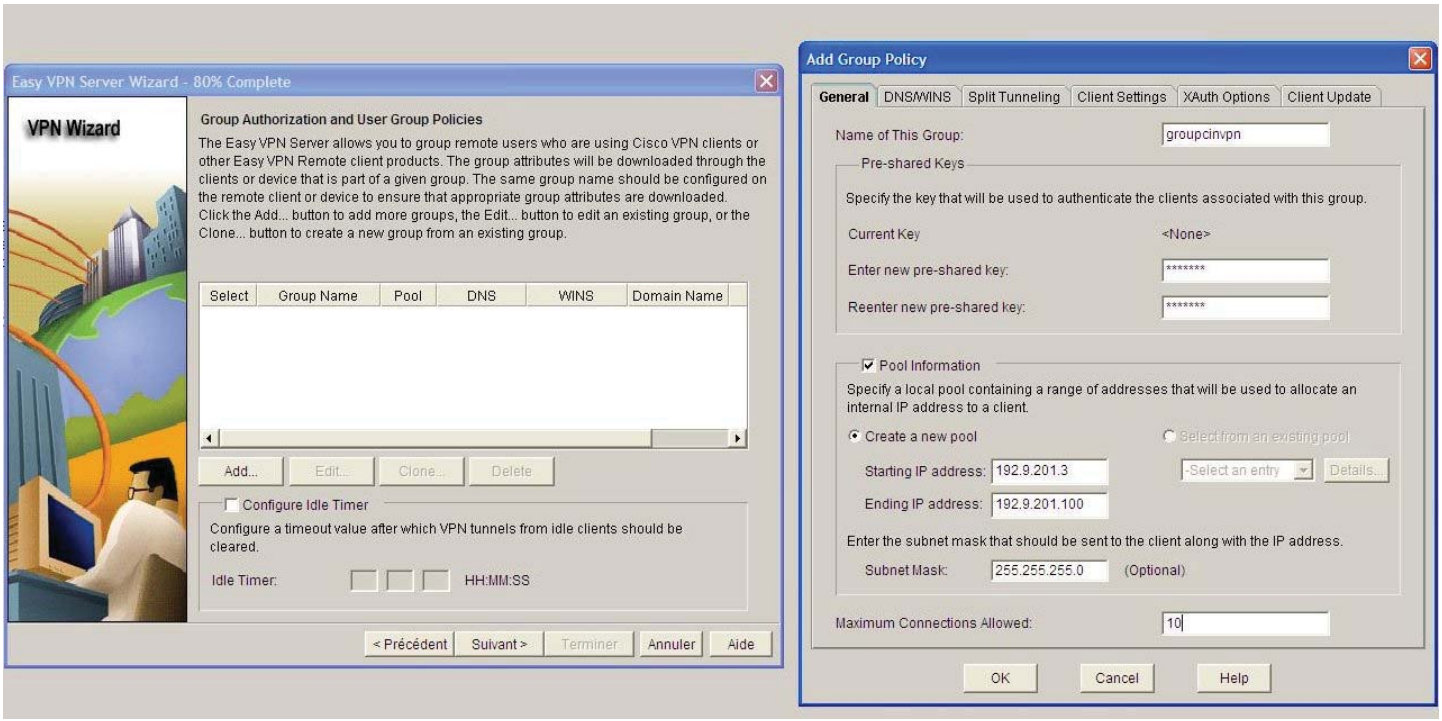


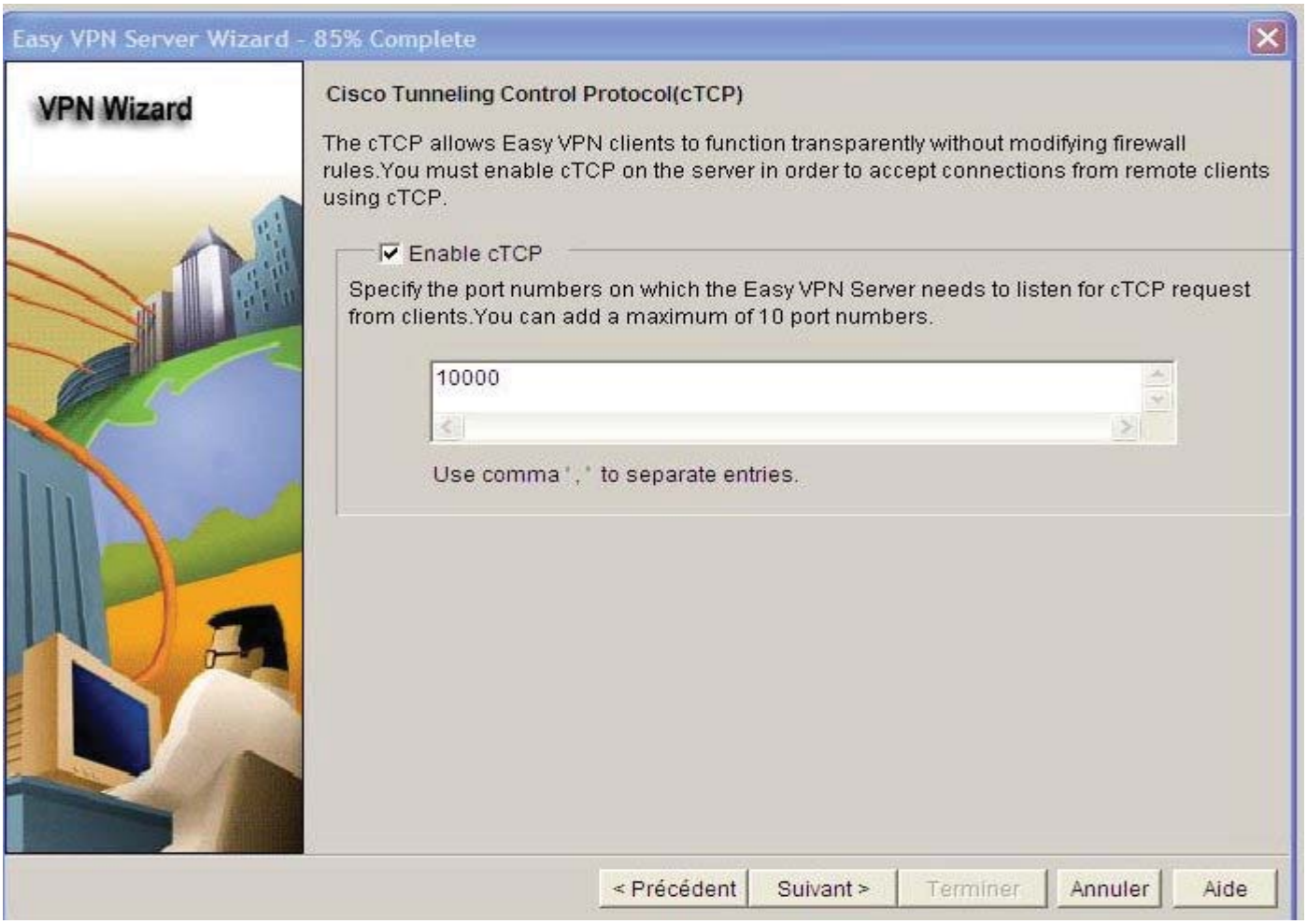


Cliquez sur add user puis sur add (username vpncin password cisco1*)



Créez un compte pour un groupe d'utilisateurs groupcinvpn ayant pour mot de passe password cisco1*





Gardez le port d'écoute TCP pour les clients qui se connectent