Exemple de configuration de routeur Cisco en tant que serveur VPN distant à l'aide de SDM

Contenu

Introduction

Ce document décrit comment utiliser Cisco Security Device Manager (SDM) pour configurer le routeur Cisco en tant que serveur Easy VPN. Cisco SDM vous permet de configurer votre routeur comme un serveur VPN pour le Client VPN Cisco à l'aide d'une interface de gestion basée sur le Web facile à utiliser. Une fois que la configuration du routeur Cisco est terminée, elle peut être vérifiée à l'aide du Client VPN Cisco.

Conditions préalables

Conditions requises

Ce document suppose que le routeur Cisco est complètement opérationnel et configuré pour permettre au Cisco SDM d'apporter des modifications de configuration.

Remarque: Référez-vous à Permettre l'accès HTTPS pour SDM afin de permettre au routeur d'être configuré par SDM.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeur Cisco 3640 avec logiciel Cisco IOS® version 12.3(14T)
- Security Device Manager v2.31
- Client VPN Cisco v4.8

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

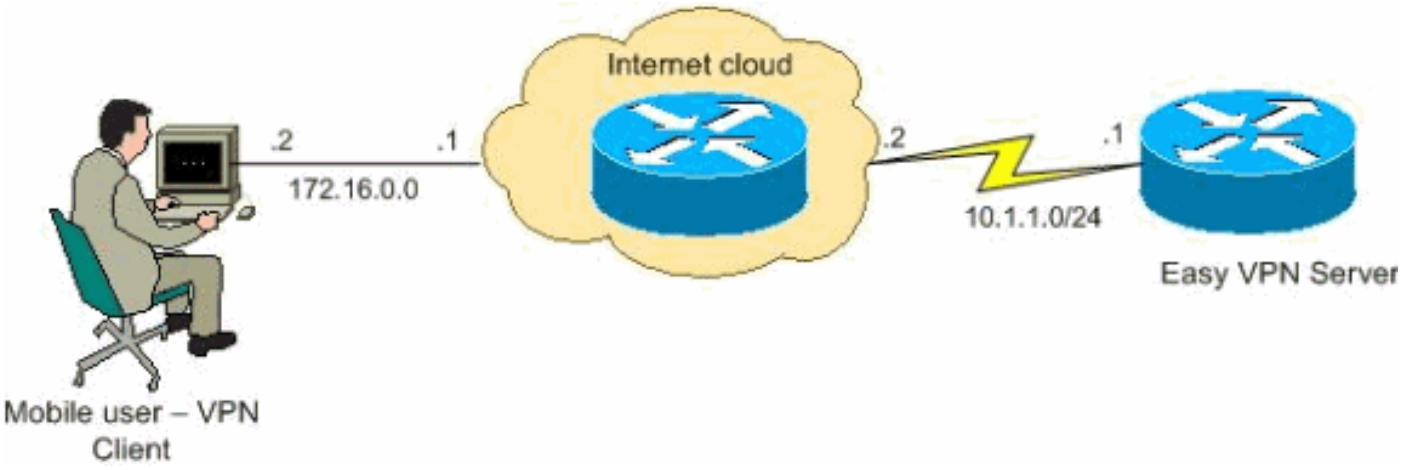
Configurez

Dans cette section vous sont présentées les informations pour configurer la fonction serveur Easy VPN qui permet à un utilisateur final distant de communiquer à l'aide de IPsec avec n'importe quelle passerelle Cisco IOS® VPN.

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

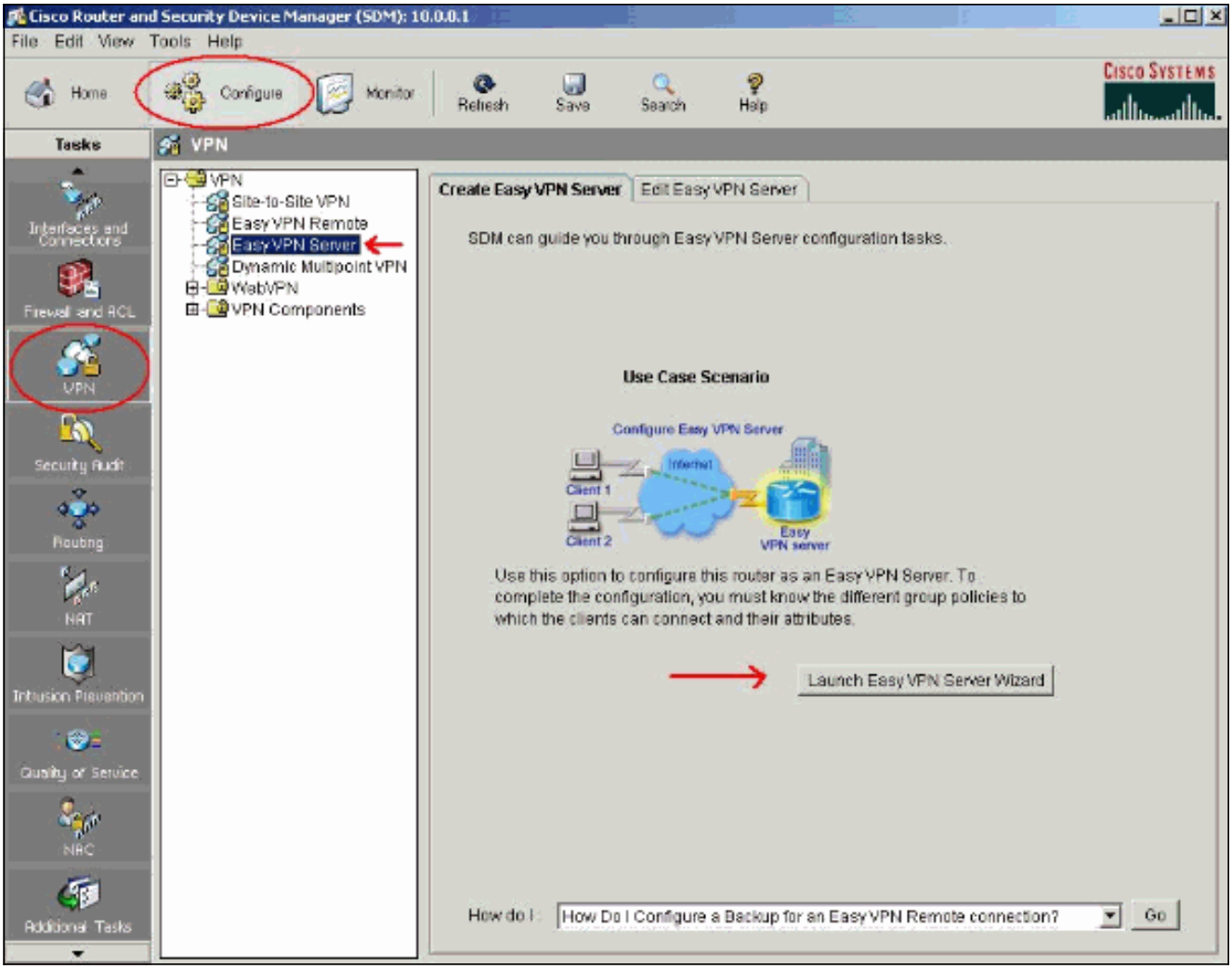
Ce document utilise la configuration réseau suivante :



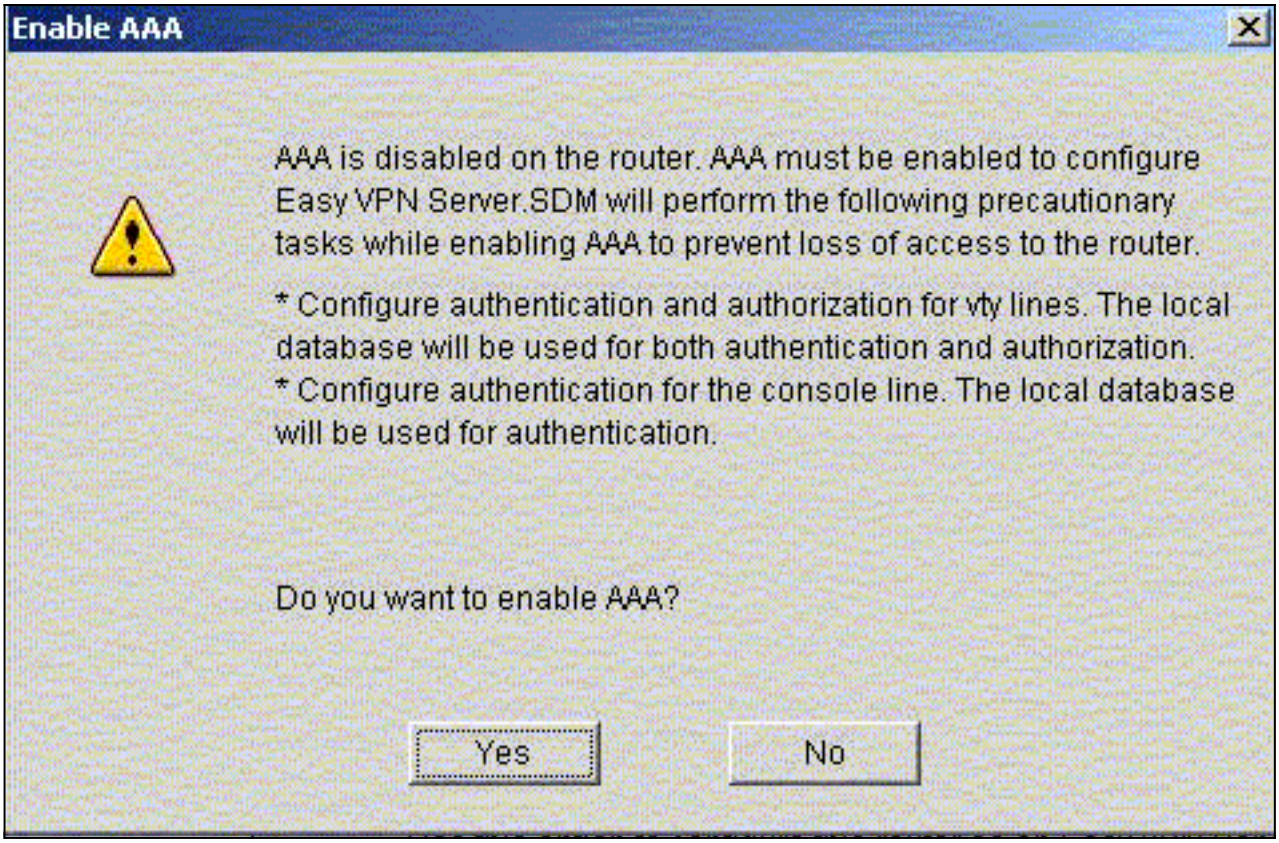
Procédure de configuration

Complétez ces étapes afin de configurer le routeur Cisco comme un serveur VPN distant à l'aide de SDM :

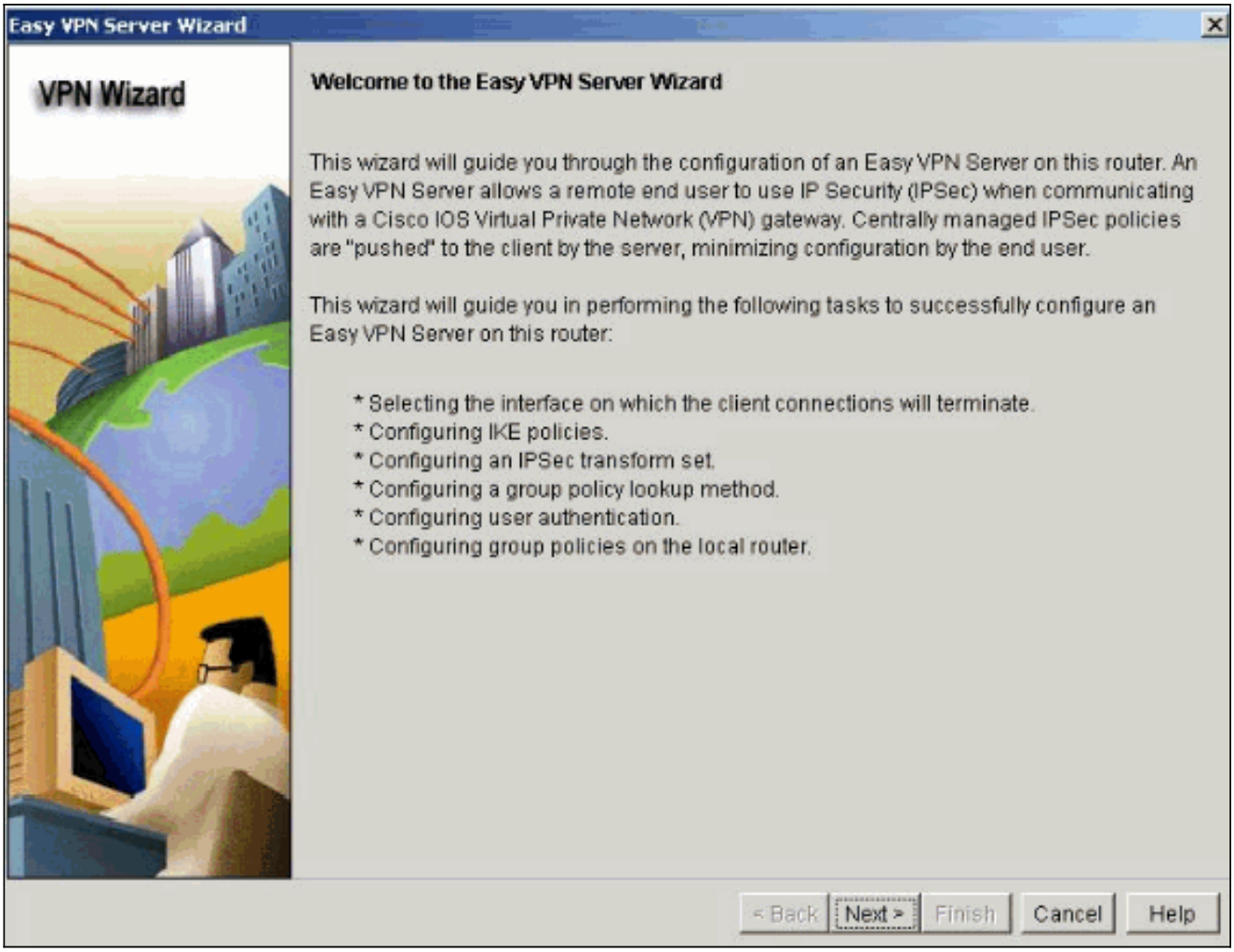
1. Sélectionnez **Configure > VPN > Easy VPN Server** dans la fenêtre d'accueil et cliquez sur **Launch Easy VPN Server Wizard**.



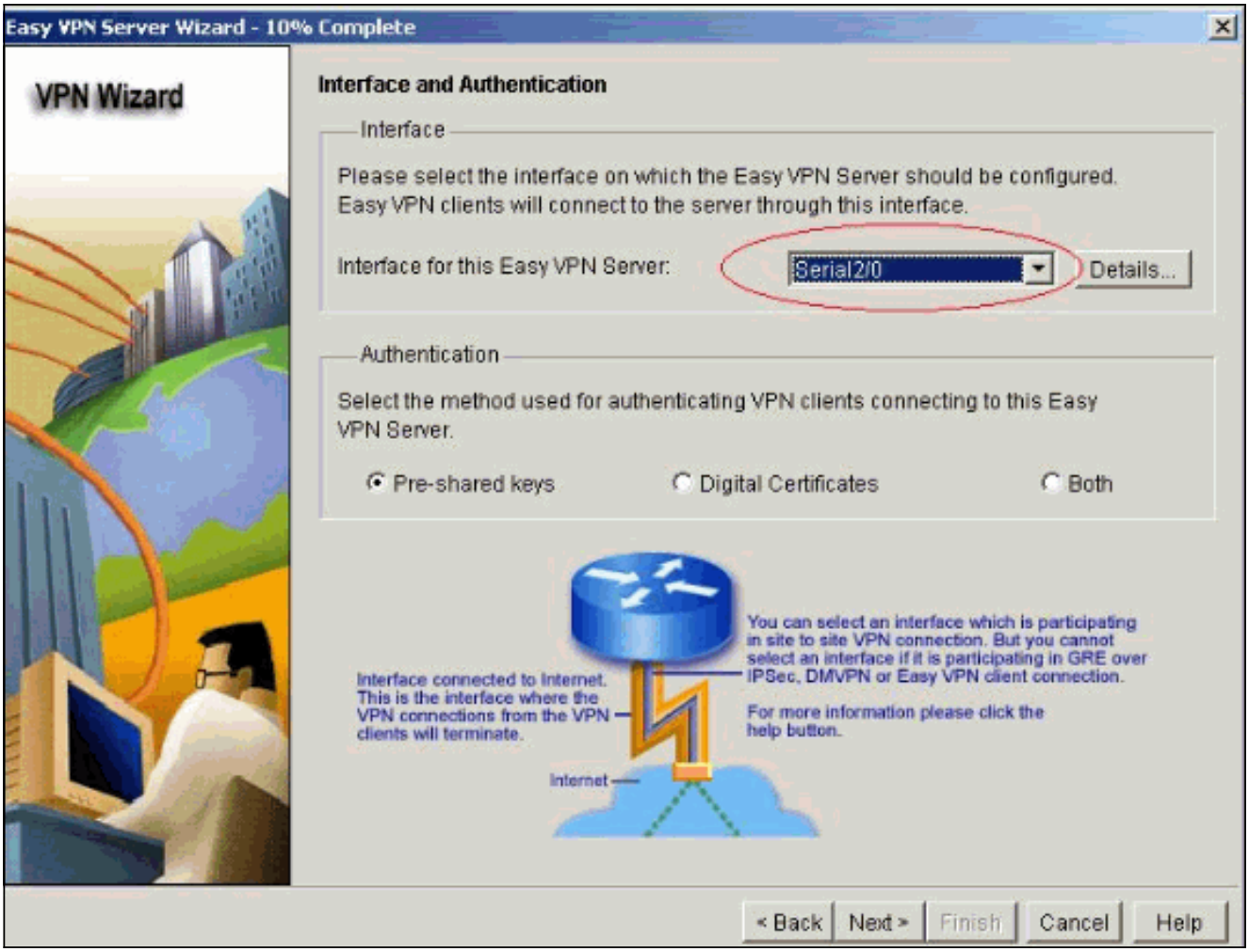
2. AAA doit être activé sur le routeur avant que la configuration du serveur Easy VPN ne démarre. Cliquez sur **Yes** pour poursuivre la configuration.Le message « AAA has been successfully enabled on the router » (activation AAA réussie sur le routeur) s'affiche. Cliquez sur **OK** pour commencer la configuration du serveur Easy VPN.



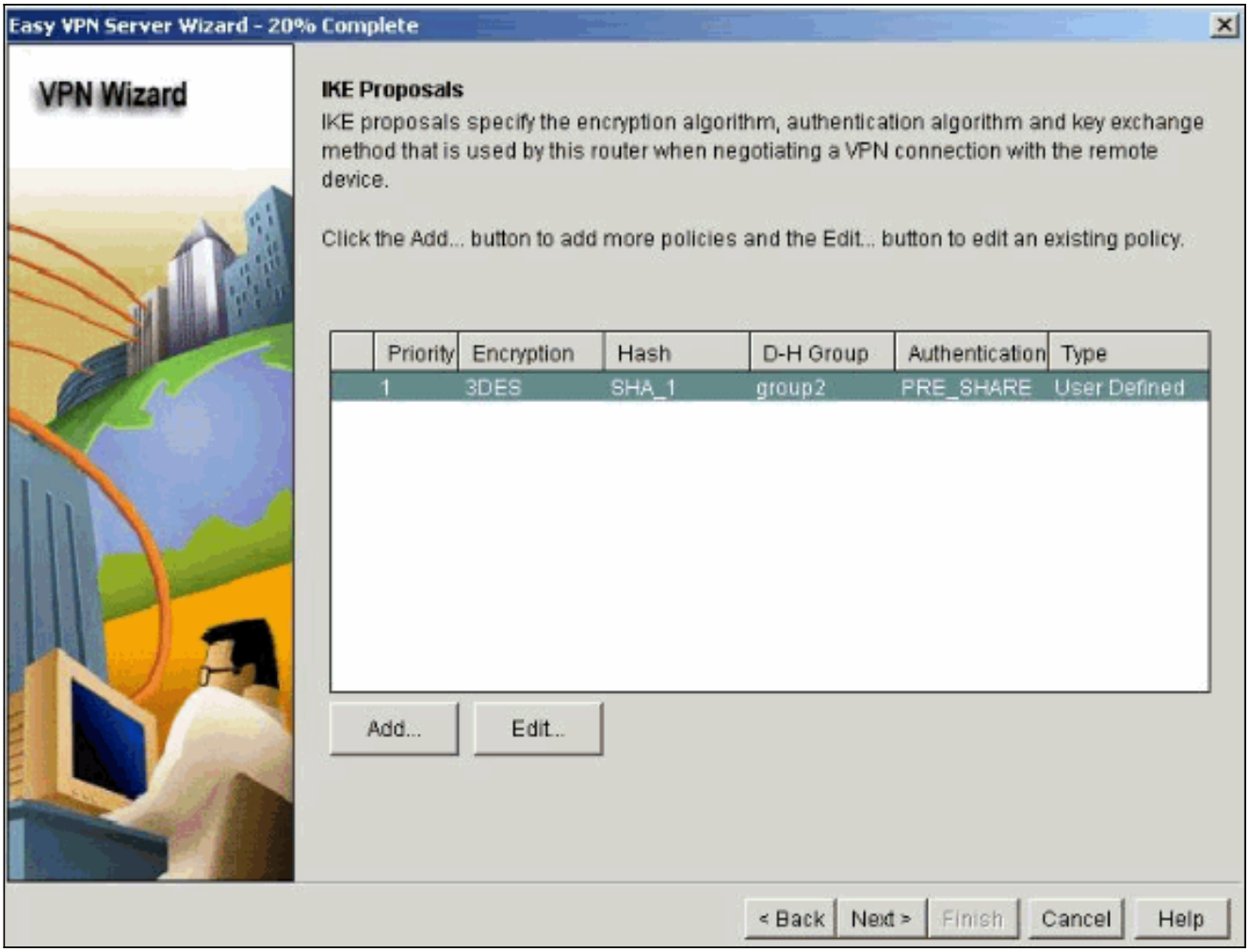
3. Cliquez sur **Next to** pour démarrer l'assistant Easy VPN Server.



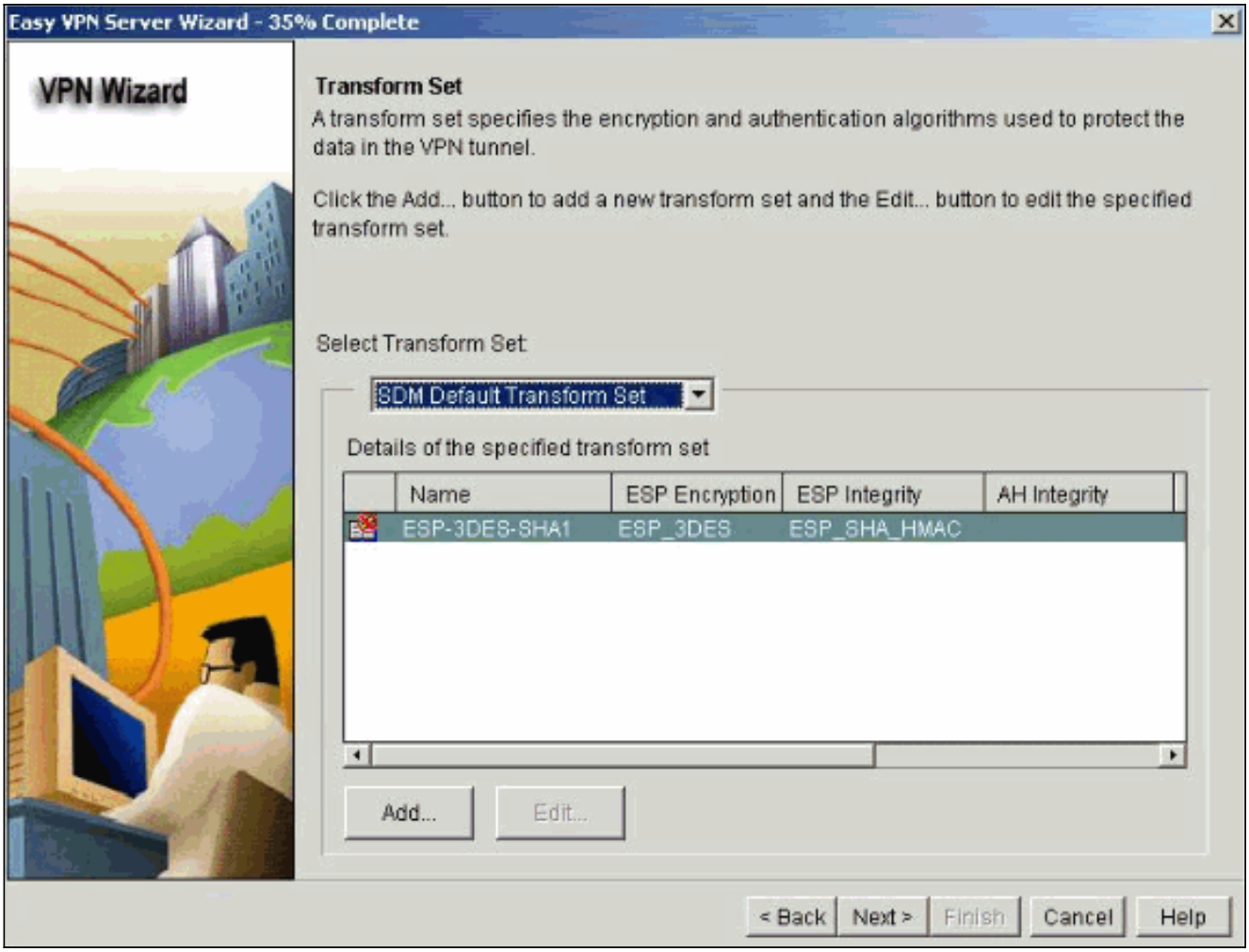
4. Sélectionnez l'interface sur laquelle les connexions du client se terminent et le type d'authentification.



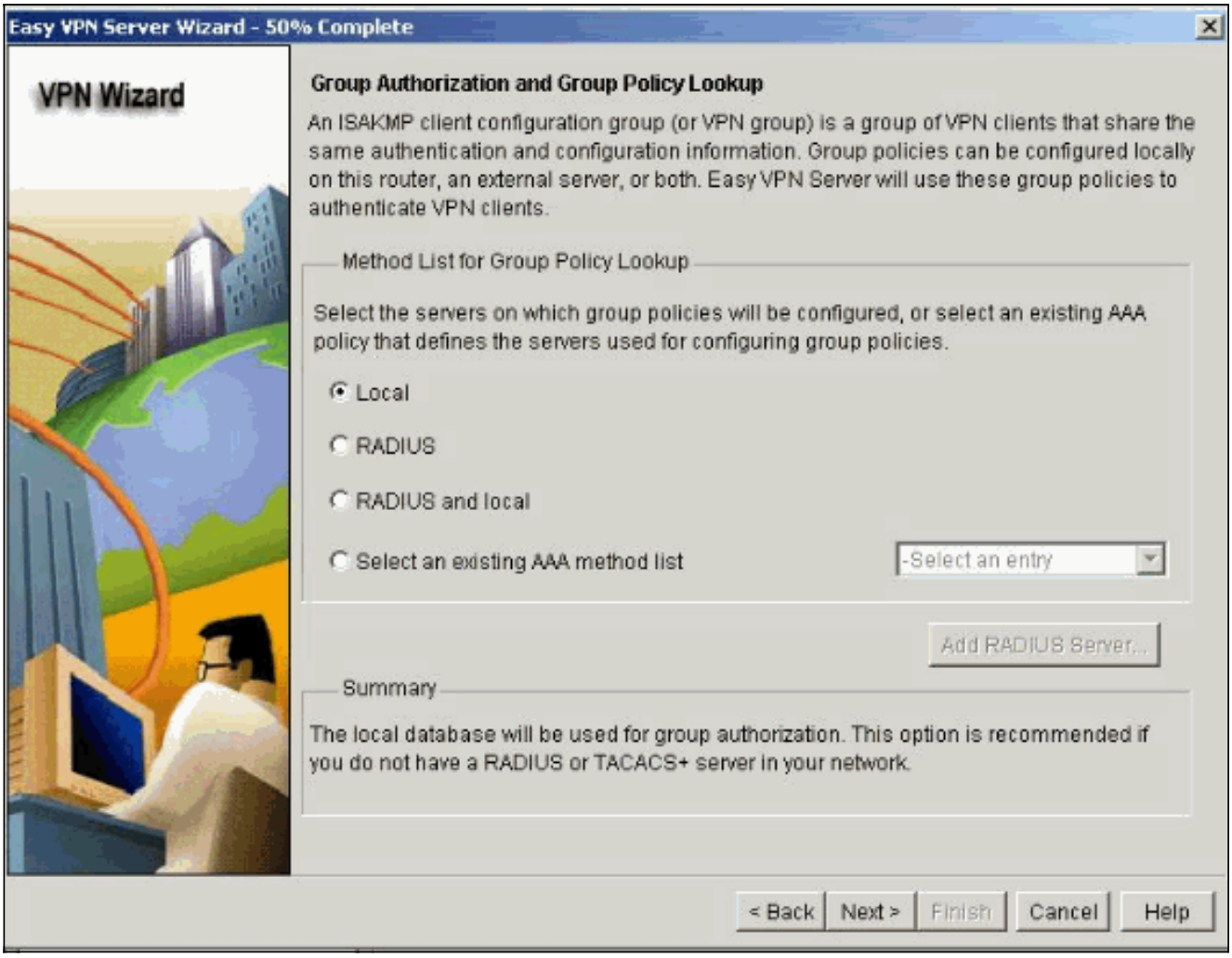
5. Cliquez sur **Next to** pour configurer les stratégies d'Échange de clés Internet (IKE) et utilisez le bouton **Add** pour créer la nouvelle stratégie.Les configurations des deux côtés du tunnel doivent correspondre exactement. Cependant, le Client VPN Cisco sélectionne automatiquement la configuration appropriée pour lui-même. Par conséquent, aucun configuration d´IKE n'est nécessaire sur le PC
Client.



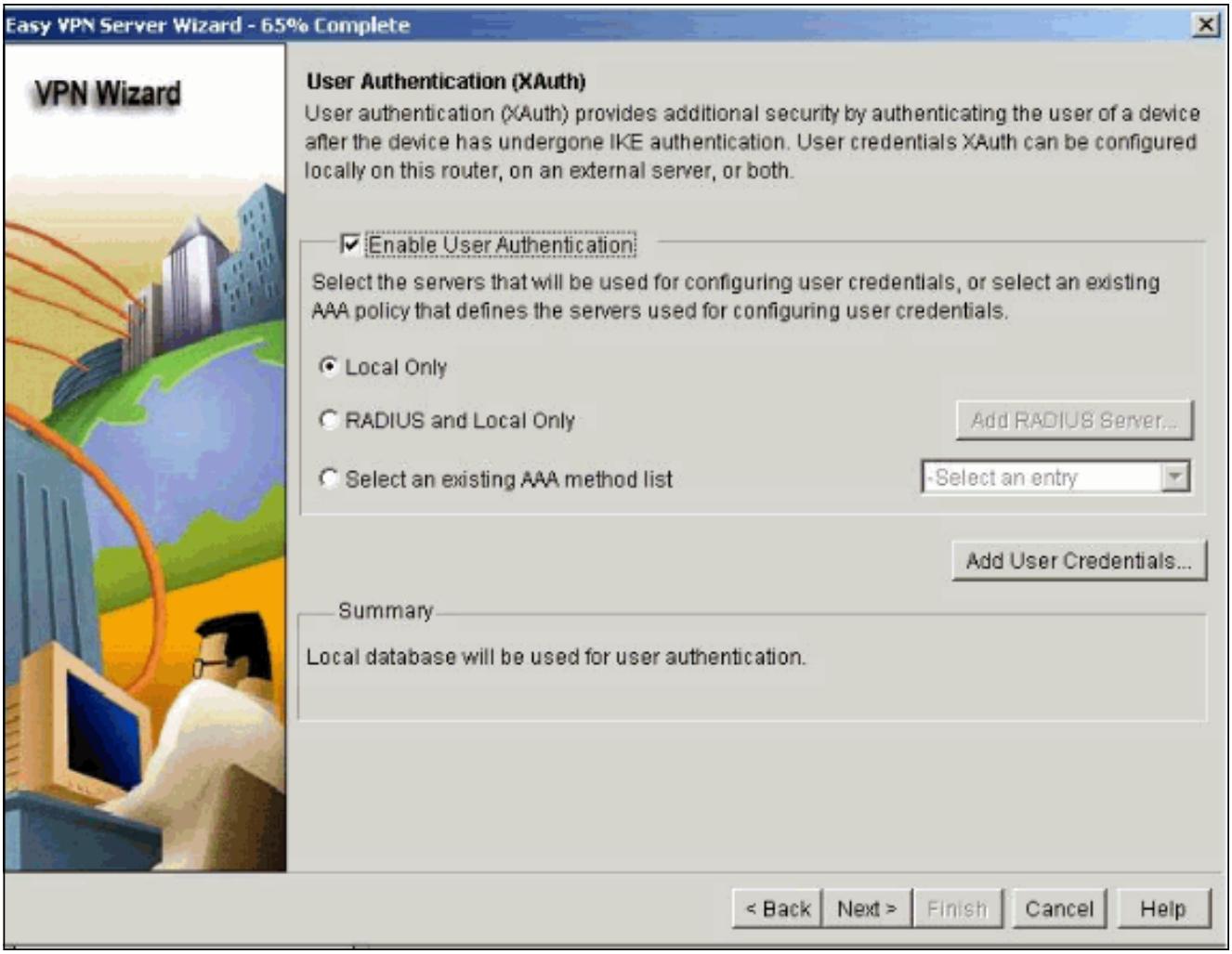
6. Cliquez sur **Next** pour choisir le jeu de transformations par défaut ou pour ajouter le nouveau jeu de transformations pour spécifier l'algorithme de cryptage et d'authentification. Dans ce cas, le jeu de transformations par défaut est
utilisé.



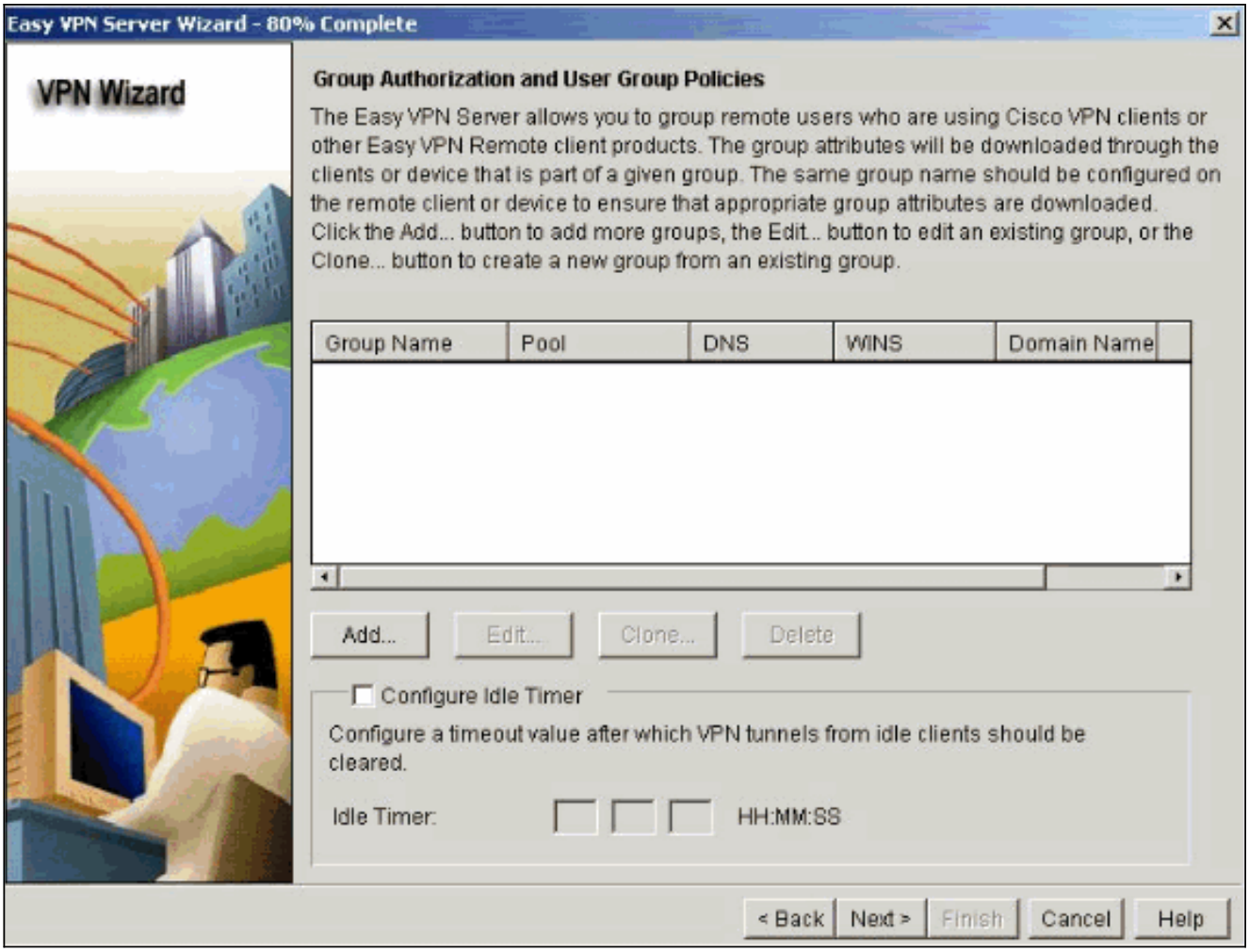
7. Cliquez sur **Next** pour créer une nouvelle liste de méthodes de réseau d'autorisation AAA (authentification, autorisation et traçabilité) pour la recherche de stratégie de groupe ou pour choisir une liste de méthodes de réseau existant utilisée pour l'autorisation de groupe.



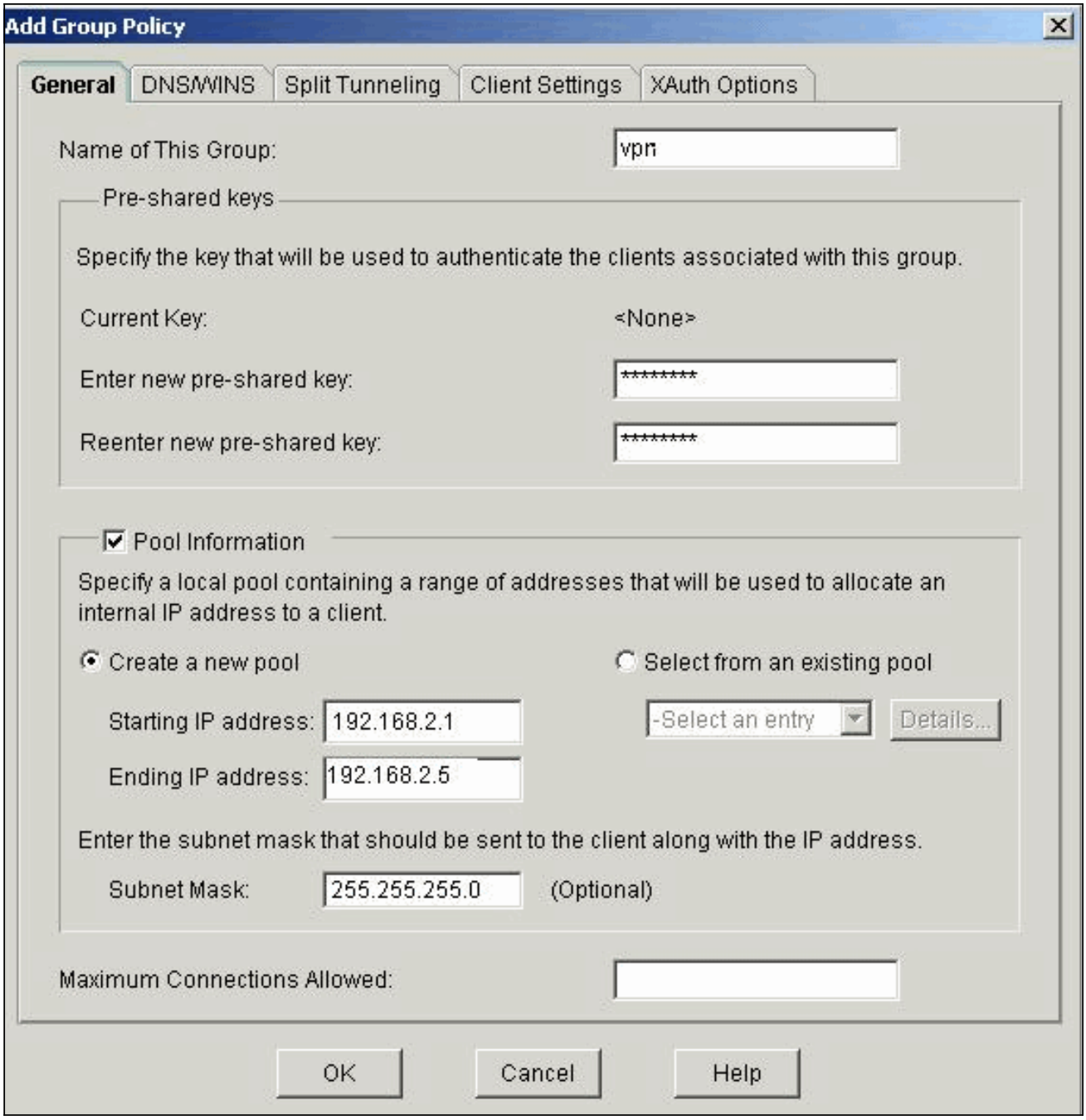
8. Configurez l'authentification des utilisateurs sur le serveur Easy VPN.Vous pouvez enregistrer les détails d'authentification des utilisateurs sur un serveur externe tel qu'un serveur RADIUS ou une base de données locale ou sur chacun des deux. Une liste de méthodes d'authentification de connexion AAA est utilisée pour décider de l'ordre dans lequel les détails d'authentification des utilisateurs devraient être recherchés.



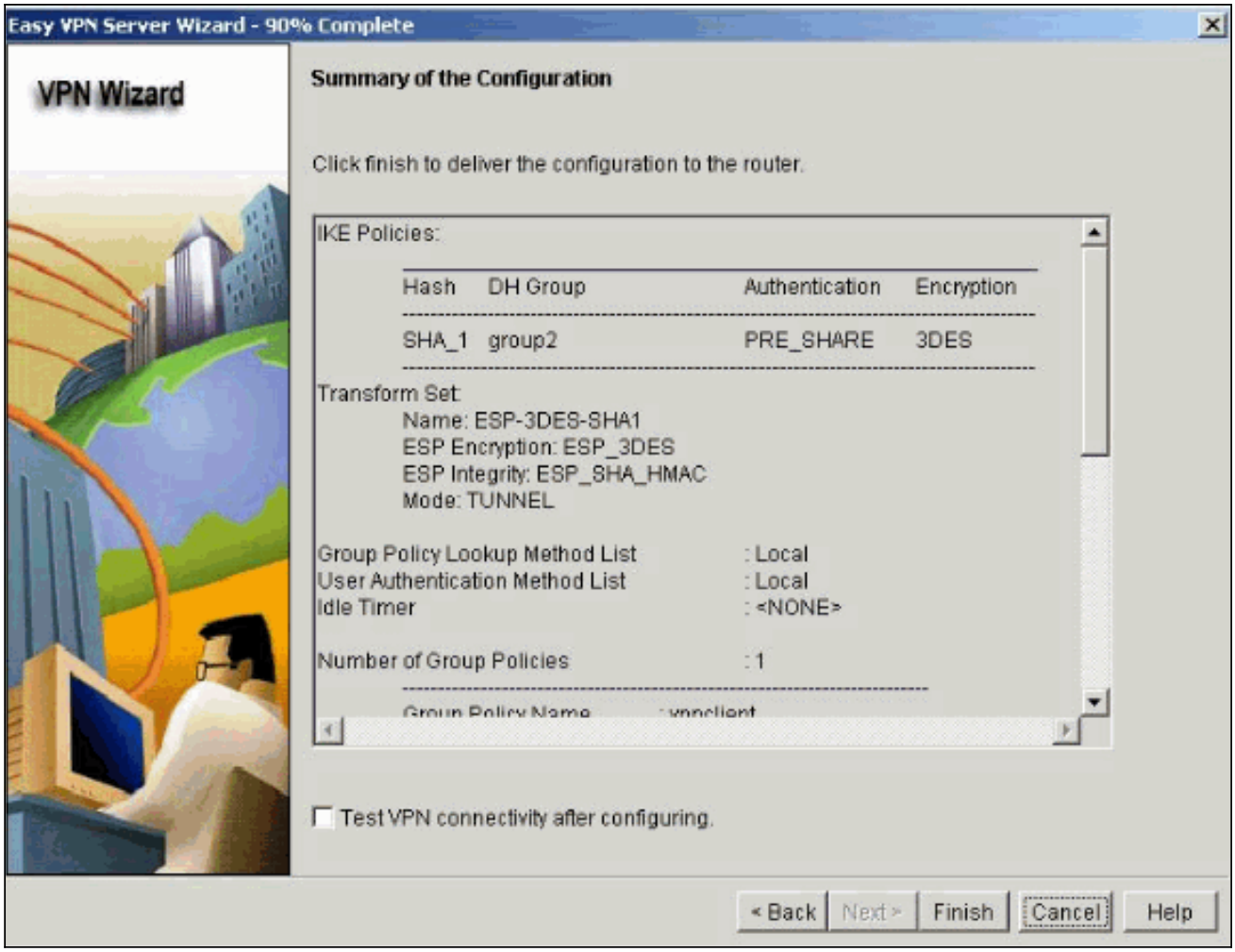
9. Cette fenêtre vous permet d'ajouter, de modifier, de cloner ou de supprimer les stratégies de groupe d'utilisateurs sur la base de données
locale.



10. Écrivez un nom pour le nom du groupe tunnel. Fournissez la clé pré-partagée utilisée pour les informations d'authentification.Créez un nouveau pool ou sélectionnez un pool existant utilisé pour allouer les adresses IP aux clients
VPN.

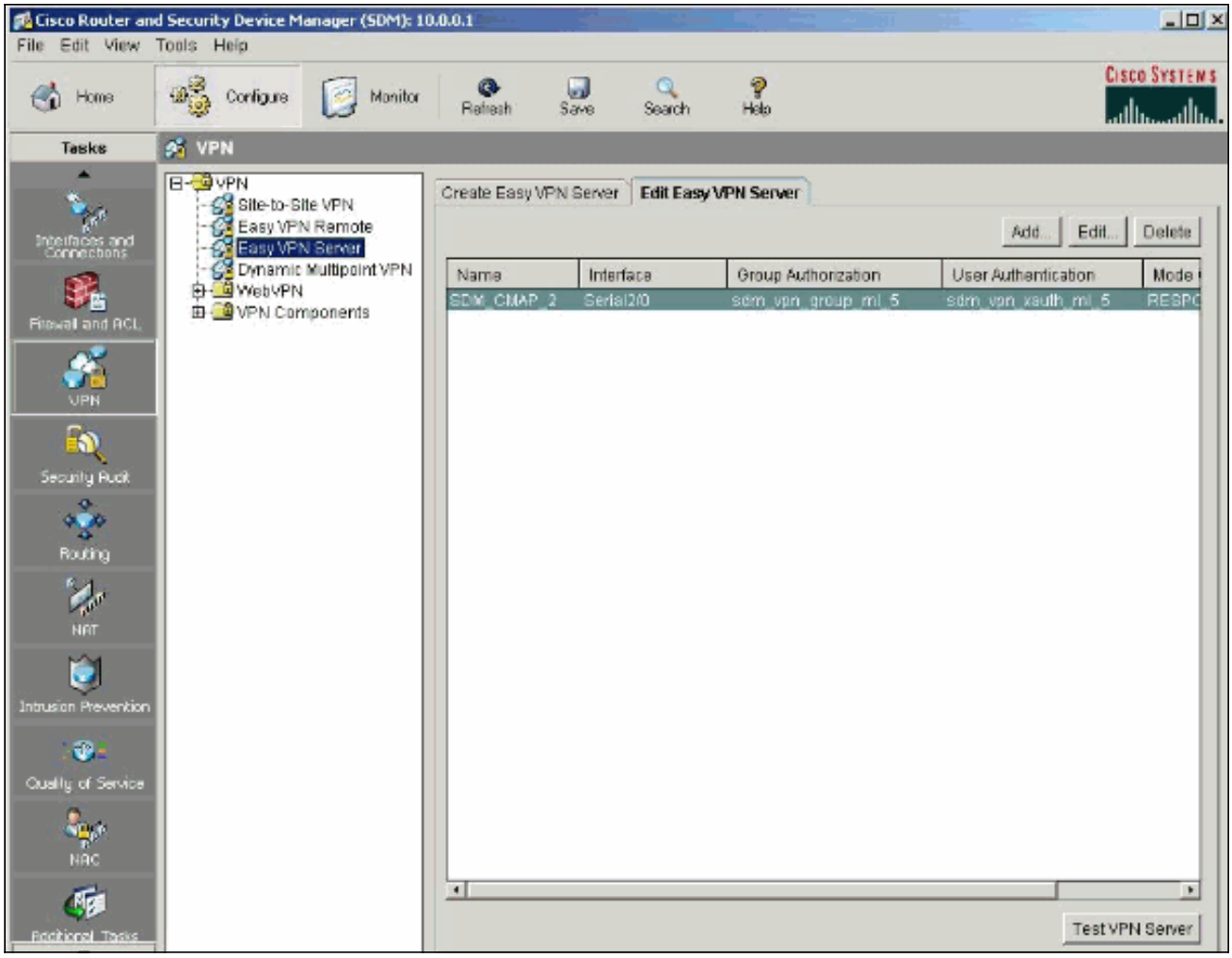


11. Cette fenêtre montre un résumé des actions que vous avez prises. Cliquez sur **Finish** si vous êtes satisfait de votre configuration.



12. Le SDM envoie la configuration au routeur pour mettre à jour la configuration en cours. Cliquez sur **OK** pour terminer.

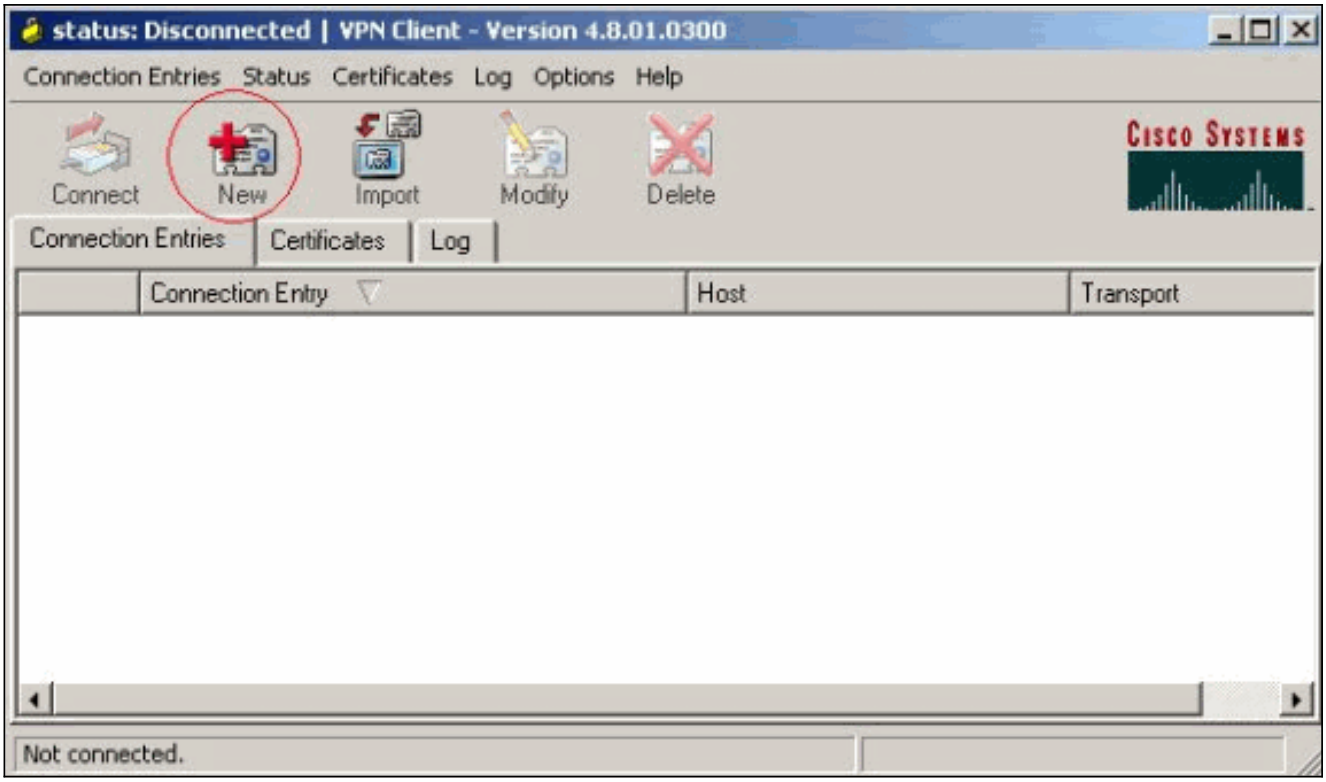
13. Une fois terminé, vous pouvez changer et modifier les modifications de la configuration, si nécessaire.



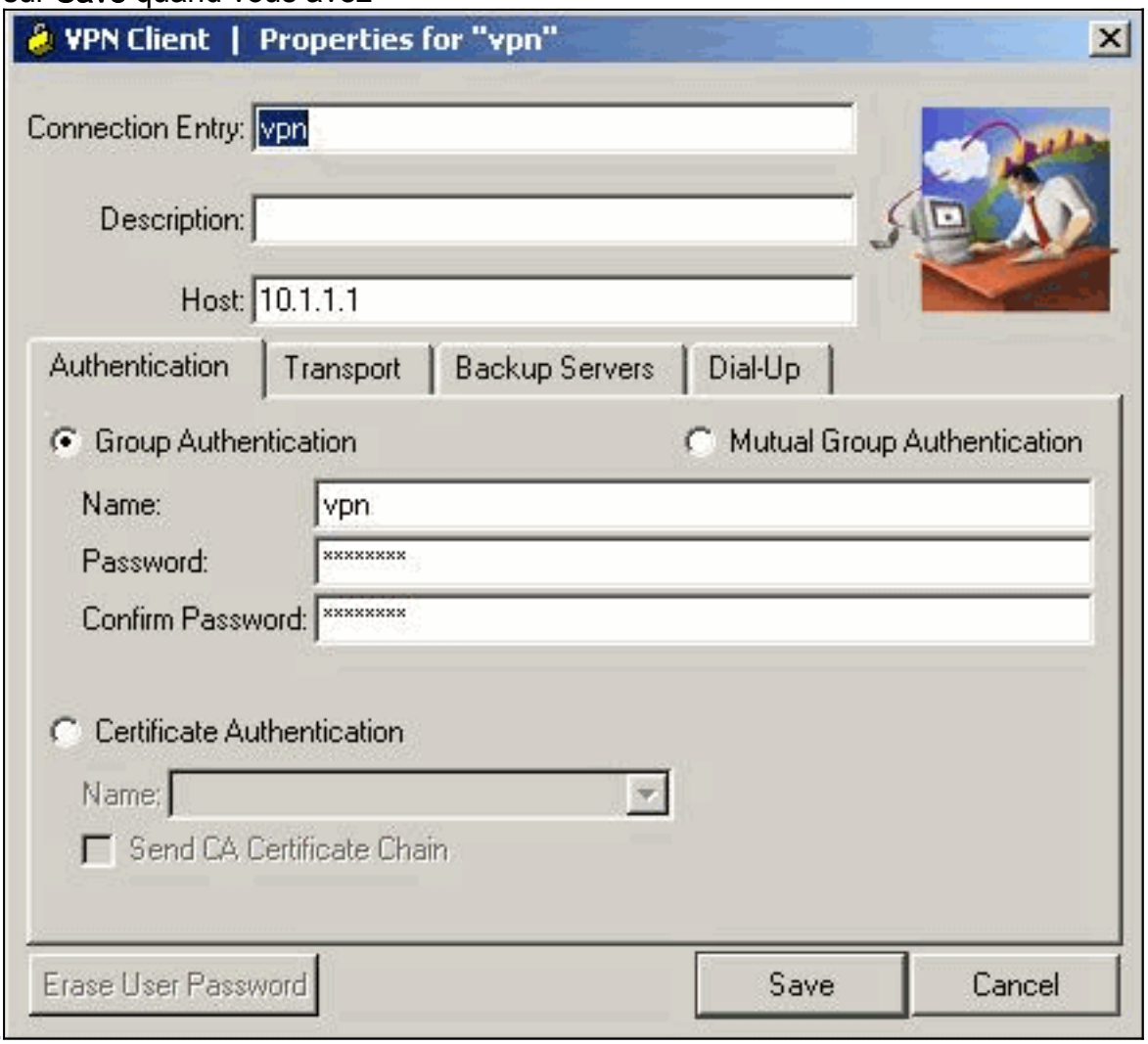
Vérifiez

Essayez de vous connecter au routeur Cisco à l'aide de Client VPN Cisco afin de vérifier que le routeur Cisco est correctement configuré.

1. Sélectionnez **Connection Entries > New**.

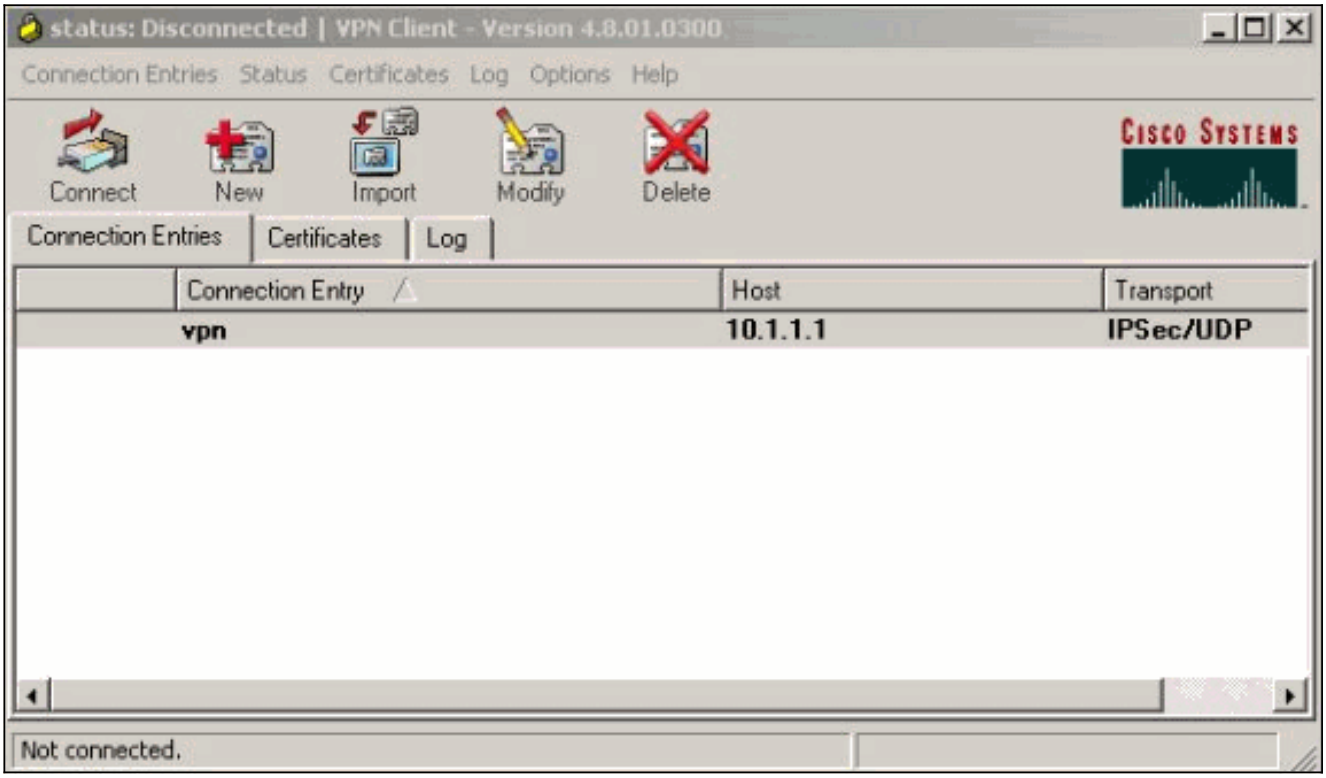


2. Complétez les détails de votre nouvelle connexion.Le champ Host doit contenir l'adresse IP ou le nom d'hôte du point d'extrémité du tunnel du serveur Easy VPN (routeur Cisco). Les informations d'authentification de groupe doivent correspondre à celles utilisées à l'étape 9. Cliquez sur **Save** quand vous avez terminé.

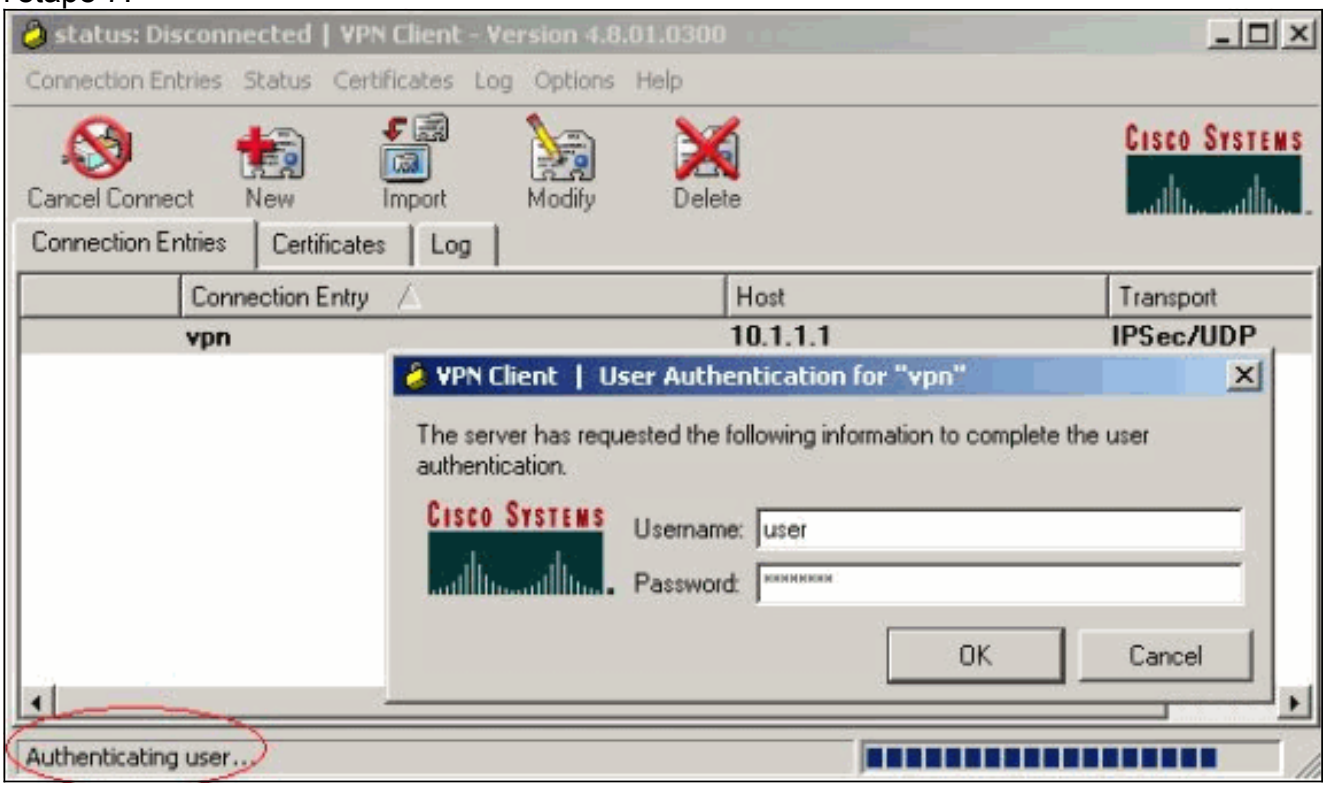


3. Sélectionnez la connexion nouvellement créée et cliquez sur

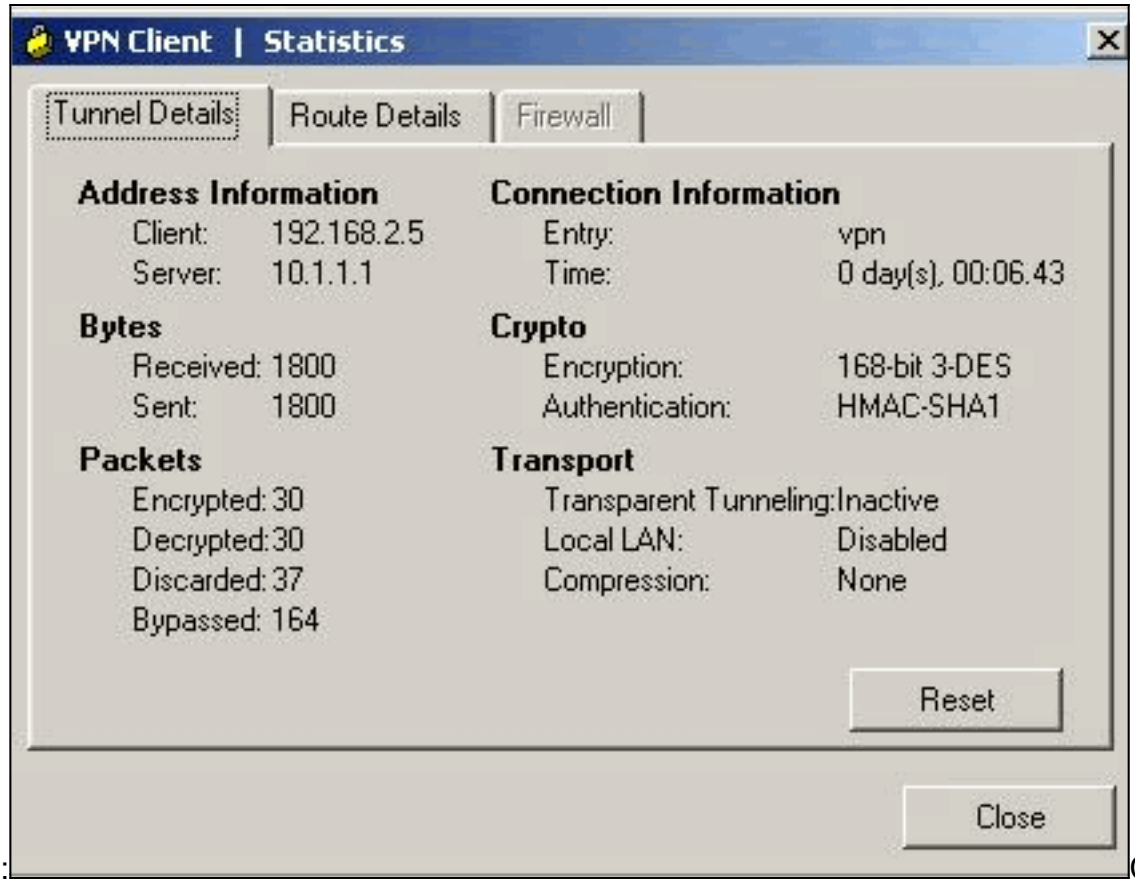
Connect.



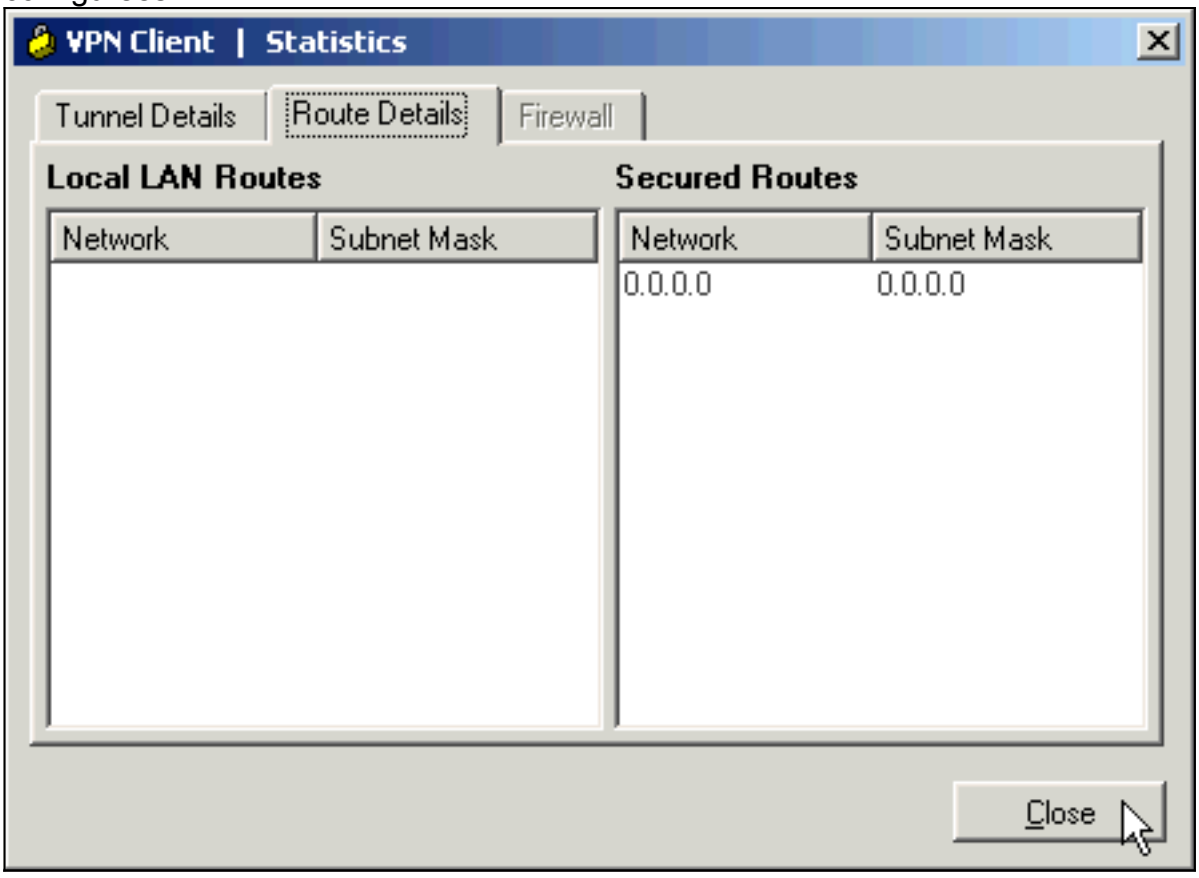
4. Saisissez un nom d'utilisateur et un mot de passe pour une authentification étendue (Xauth). Ces informations sont déterminées par les paramètres Xauth à l'étape 7.



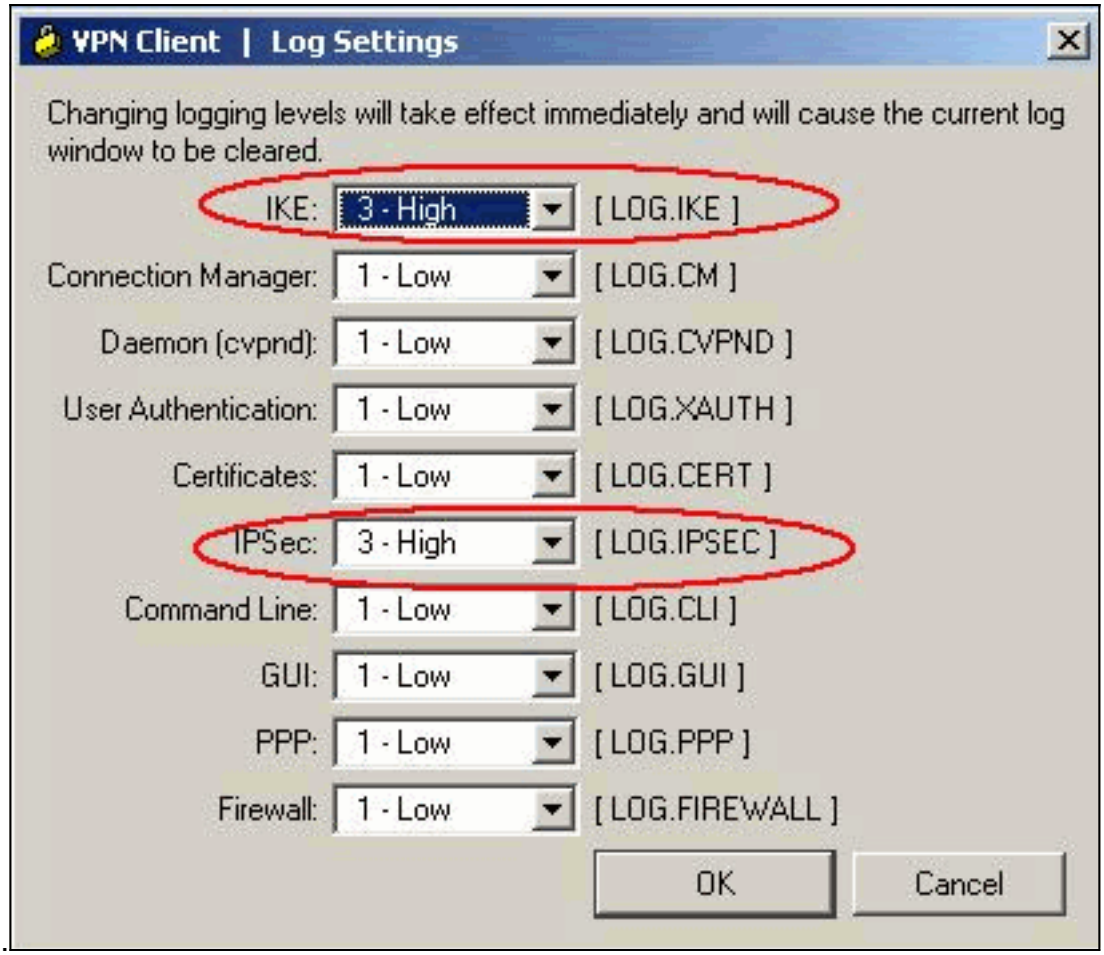
5. Une fois que la connexion est établie avec succès, sélectionnez **Statistics** dans le menu Status pour vérifier les données du tunnel.Cette fenêtre montre les informations de trafic et de cryptage



:Cette fenêtre montre les informations split tunneling si celles-ci sont configurées :



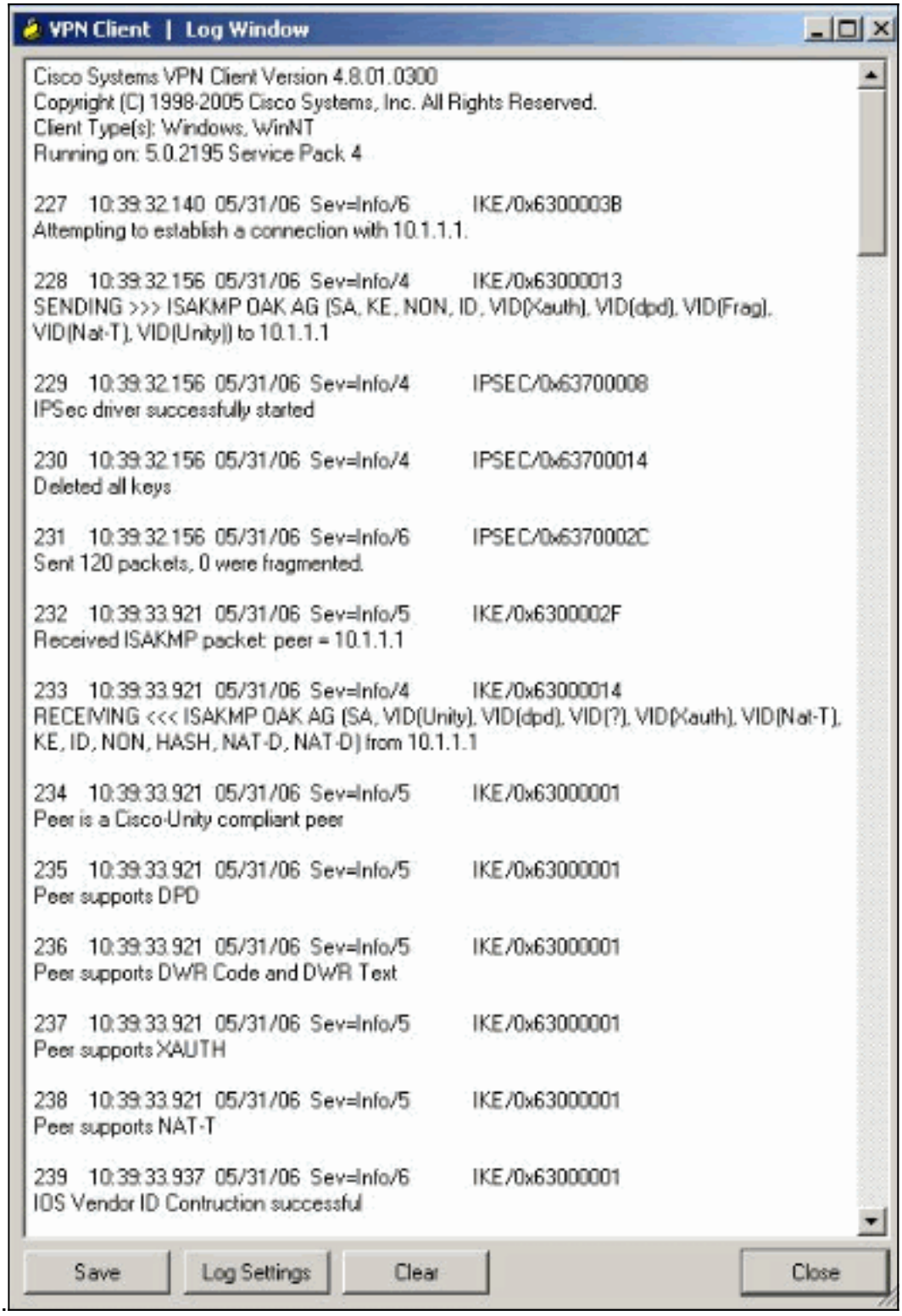
6. Sélectionnez **Log > Log Settings** pour activer les niveaux de log dans le client VPN



Cisco.

7. Sélectionnez **Log > Log Windows** pour afficher les entrées de journal dans le client VPN

Cisco.



Informations connexes

- Téléchargement et installation du routeur Cisco et de Security Device Manager
- Cisco VPN Client Support Page
- Négociation IPSec/Protocoles IKE
- Support et documentation techniques - Cisco Systems