Exemple de configuration d'un routeur IOS en tant que serveur Easy VPN à l'aide de Configuration Professional

Contenu

Introduction

Ce document décrit comment configurer un routeur Cisco IOS® en tant que serveur Easy VPN (EzVPN) à l'aide de Cisco Configuration Professional (Cisco CP) et de l'interface de ligne de commande. La caractéristique du serveur Easy VPN permet à un utilisateur final distant de communiquer en utilisant la sécurité IP (IPsec) avec n'importe quelle passerelle de réseau privé virtuel (VPN) Cisco IOS. Des stratégies IPsec centralement gérées sont « dirigées » vers le périphérique de client par le serveur, réduisant la configuration par l'utilisateur final.

Pour plus d'informations sur Easy VPN Server, reportez-vous à la section Easy VPN Server de la bibliothèque du Guide de configuration de la connectivité sécurisée, Cisco IOS version 12.4T.

Conditions préalables

Components Used

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

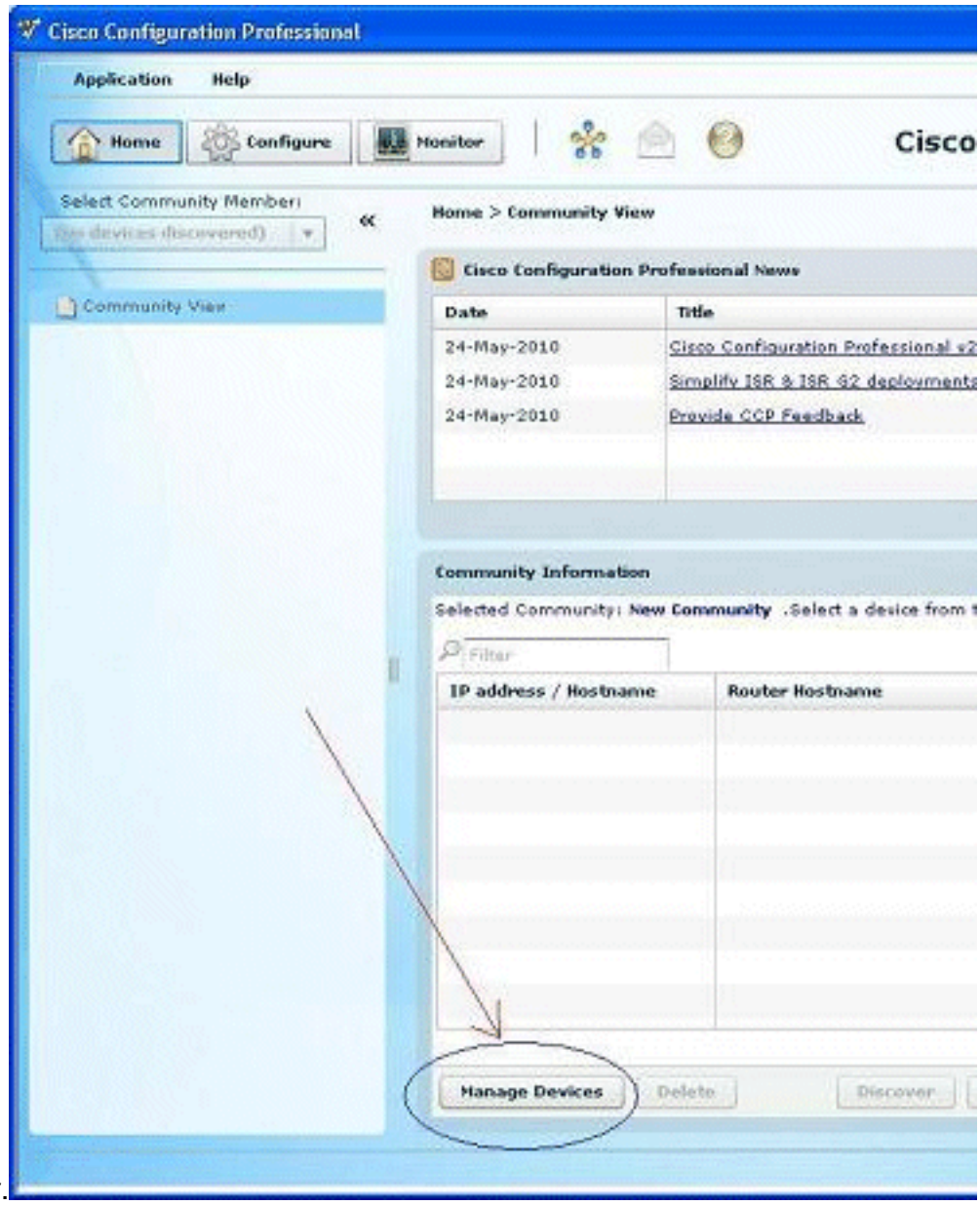
- Routeur Cisco 1841 avec logiciel Cisco IOS Version 12.4(15T)
- Cisco CP, version 2.1

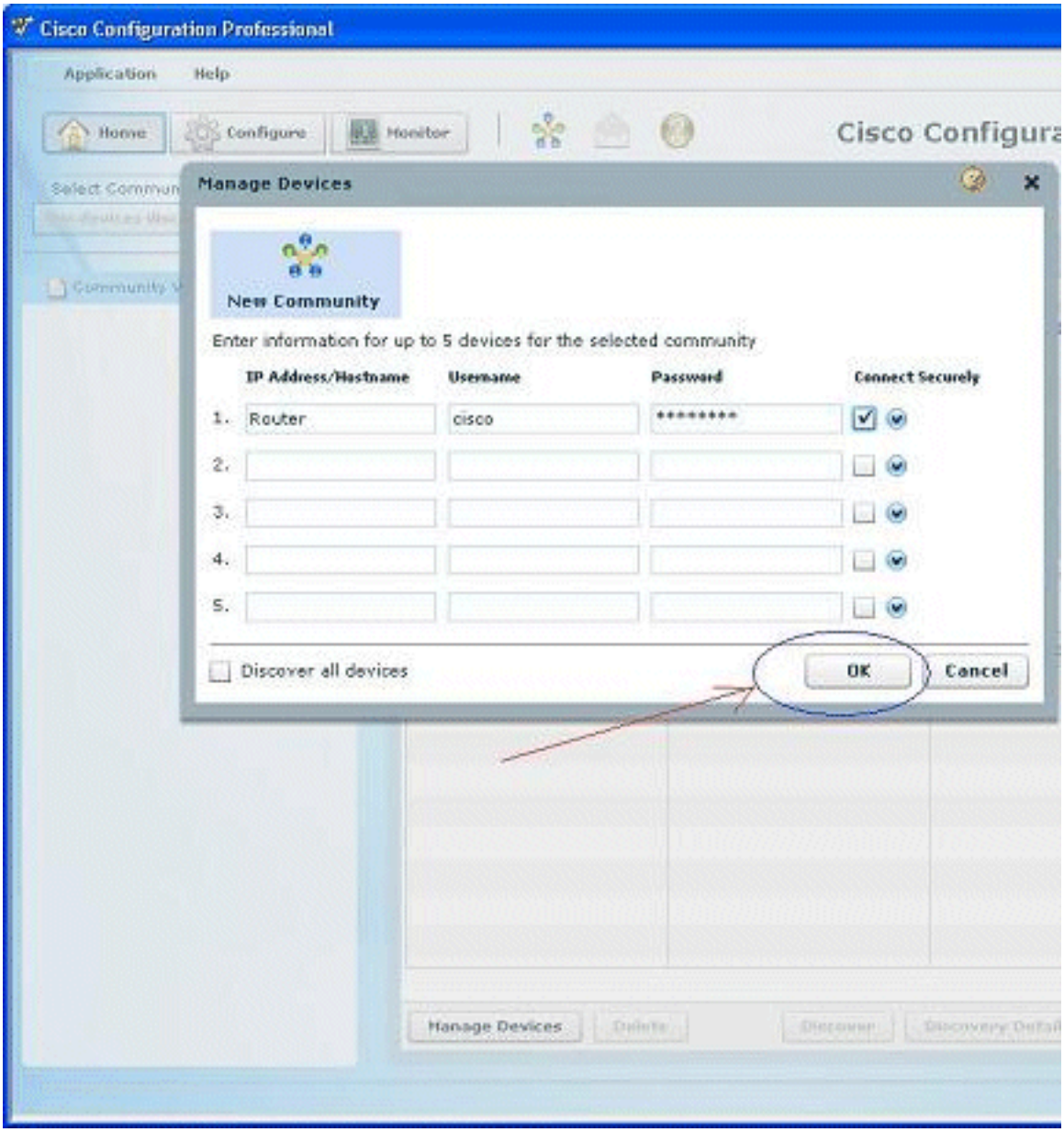
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Installer Cisco CP

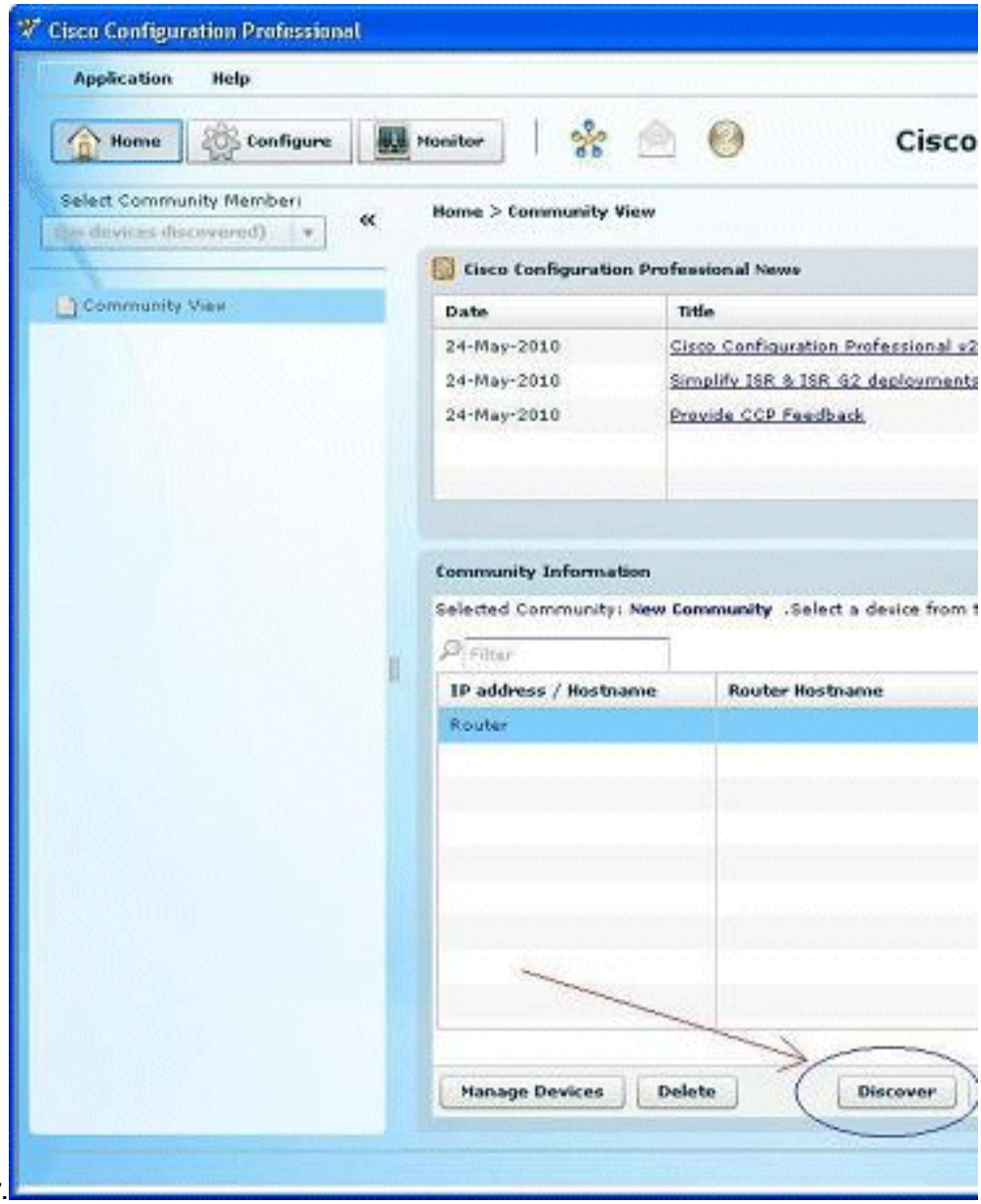
Pour installer Cisco CP, procédez comme suit :

1. Téléchargez Cisco CP V2.1 depuis le Cisco Software Center (clients enregistrés uniquement) et installez-le sur votre ordinateur local.La dernière version de Cisco CP se trouve sur le site Web de Cisco CP.
2. Lancez Cisco CP à partir de votre ordinateur local via **Start > Programs > Cisco Configuration Professional (CCP)** et choisissez la **Communauté** qui a le routeur que vous voulez configurer.





3. Afin de découvrir le périphérique que vous voulez configurer, mettez le routeur en surbrillance et cliquez sur



Découvrir.

Remarque : Pour plus d'informations sur les modèles de routeurs Cisco et les versions IOS compatibles avec Cisco CP v2.1, reportez-vous à la section Versions compatibles de Cisco IOS.

Remarque : Pour plus d'informations sur la configuration requise pour le PC qui exécute Cisco CP v2.1, reportez-vous à la section Configuration système requise.

Configuration du routeur pour exécuter Cisco CP

Suivez les étapes de configuration ci-dessous pour exécuter Cisco CP sur un routeur Cisco :

1. Connectez-vous à votre routeur par l'intermédiaire de Telnet, de SSH ou de la console.Entrez le mode de configuration globale à l'aide de cette commande :
   ```
   Router(config)#enable
   Router(config)#
   ```
2. Si les protocoles HTTP et HTTPS sont activés et configurés pour utiliser des numéros de ports non standards, vous pouvez passer à l'étape suivante et simplement utiliser le numéro de port déjà configuré.Activez le serveur HTTP ou HTTPS du routeur à l'aide de ces commandes de logiciel Cisco IOS :
   ```
   Router(config)# ip http server
   Router(config)# ip http secure-server
   Router(config)# ip http authentication local
   ```

3. Créez un utilisateur en lui attribuant le niveau de privilège 15 :
```
Router(config)# username privilege 15 password 0
```

   Remarque : Remplacez *<nom d'utilisateur>* et *<mot de passe>* par le nom d'utilisateur et le mot de passe que vous souhaitez configurer.
4. Configurez SSH et Telnet pour la connexion locale et le niveau de privilège 15.
```
Router(config)# line vty 0 4
Router(config-line)# privilege level 15
Router(config-line)# login local
Router(config-line)# transport input telnet
Router(config-line)# transport input telnet ssh
Router(config-line)# exit
```

5. (Facultatif) Activez la connexion locale afin de lancer la fonction de surveillance du journal :
```
Router(config)# logging buffered 51200 warning
```

Conditions requises

Ce document suppose que le routeur Cisco est entièrement opérationnel et configuré pour permettre à Cisco CP d'effectuer des modifications de configuration.

Pour plus d'informations sur la façon d'utiliser Cisco CP, reportez-vous à Mise en route de Cisco Configuration Professional.

Conventions

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

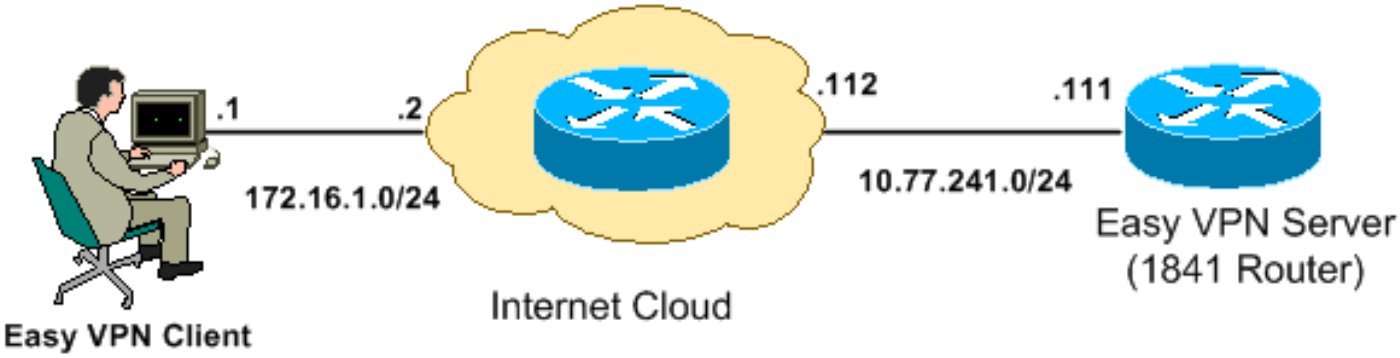
Configuration

Dans la section suivante, vous verrez comment configurer les paramètres de base d'un routeur dans un réseau.

Remarque : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

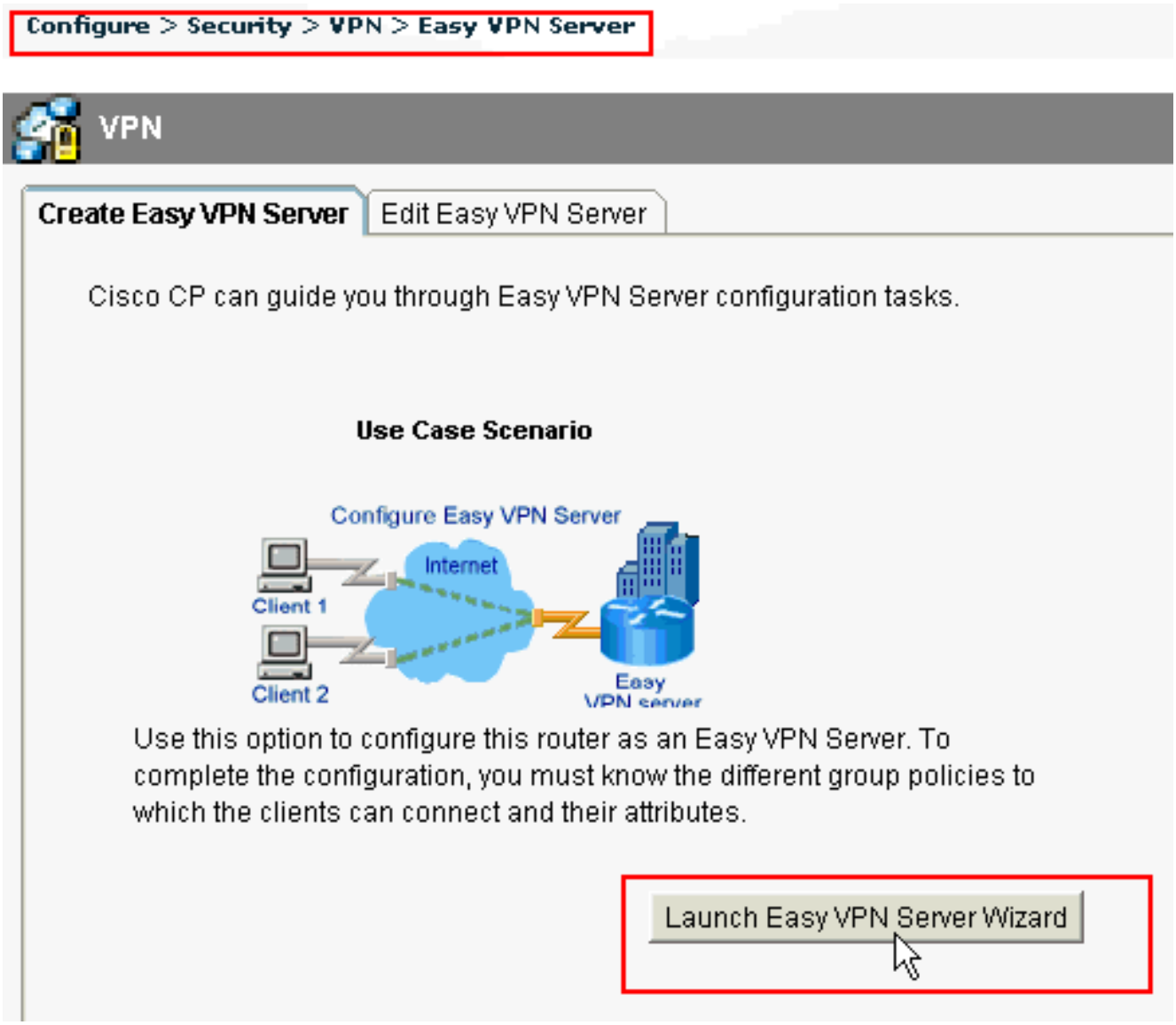


Remarque : les schémas d'adressage IP utilisés dans cette configuration ne sont pas routables légalement sur Internet. Ce sont des adresses RFC 1918 qui ont été utilisés dans un environnement de laboratoire.

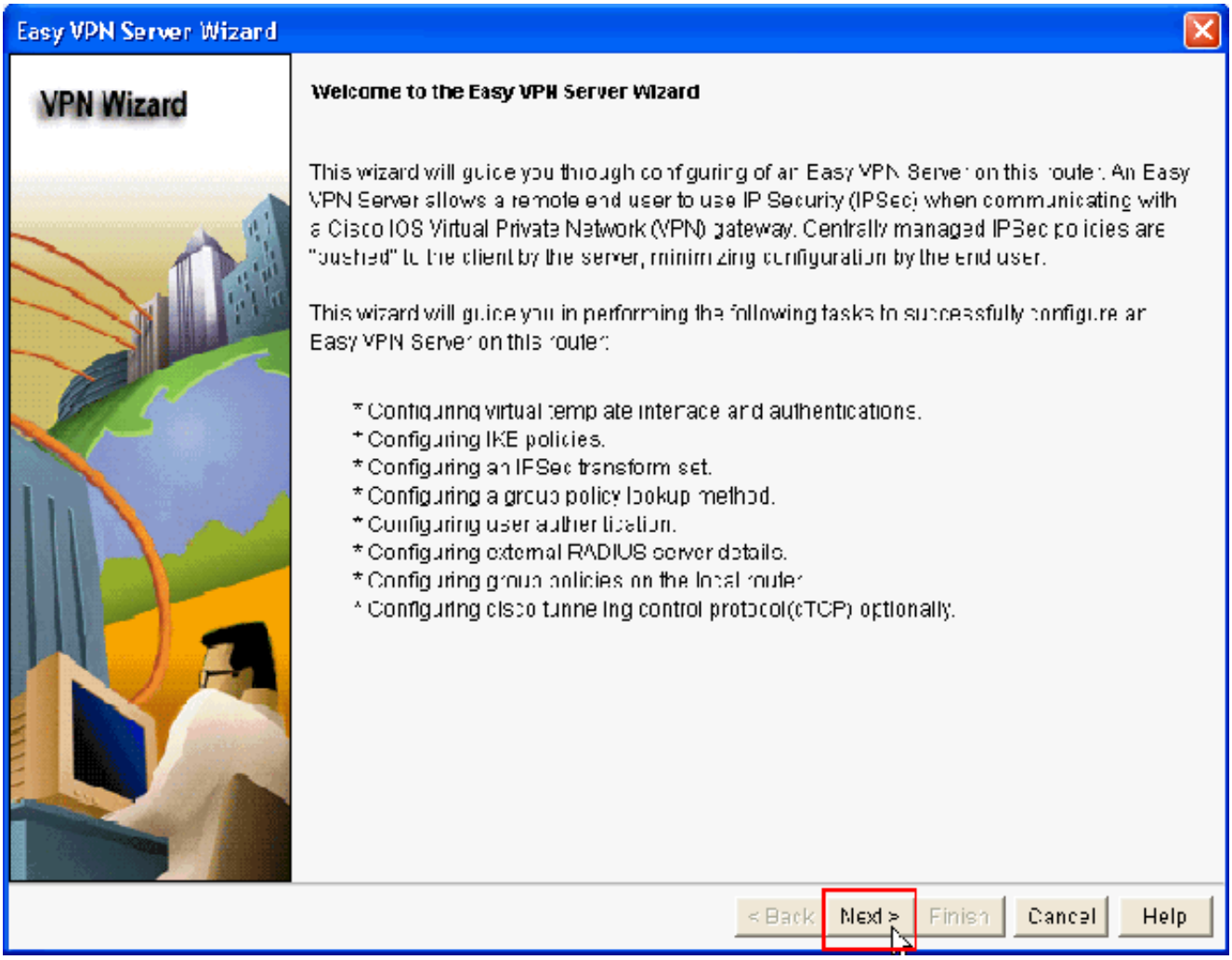
Cisco CP - Configuration Easy VPN Server

Procédez comme suit afin de configurer le routeur Cisco IOS en tant que serveur Easy VPN :

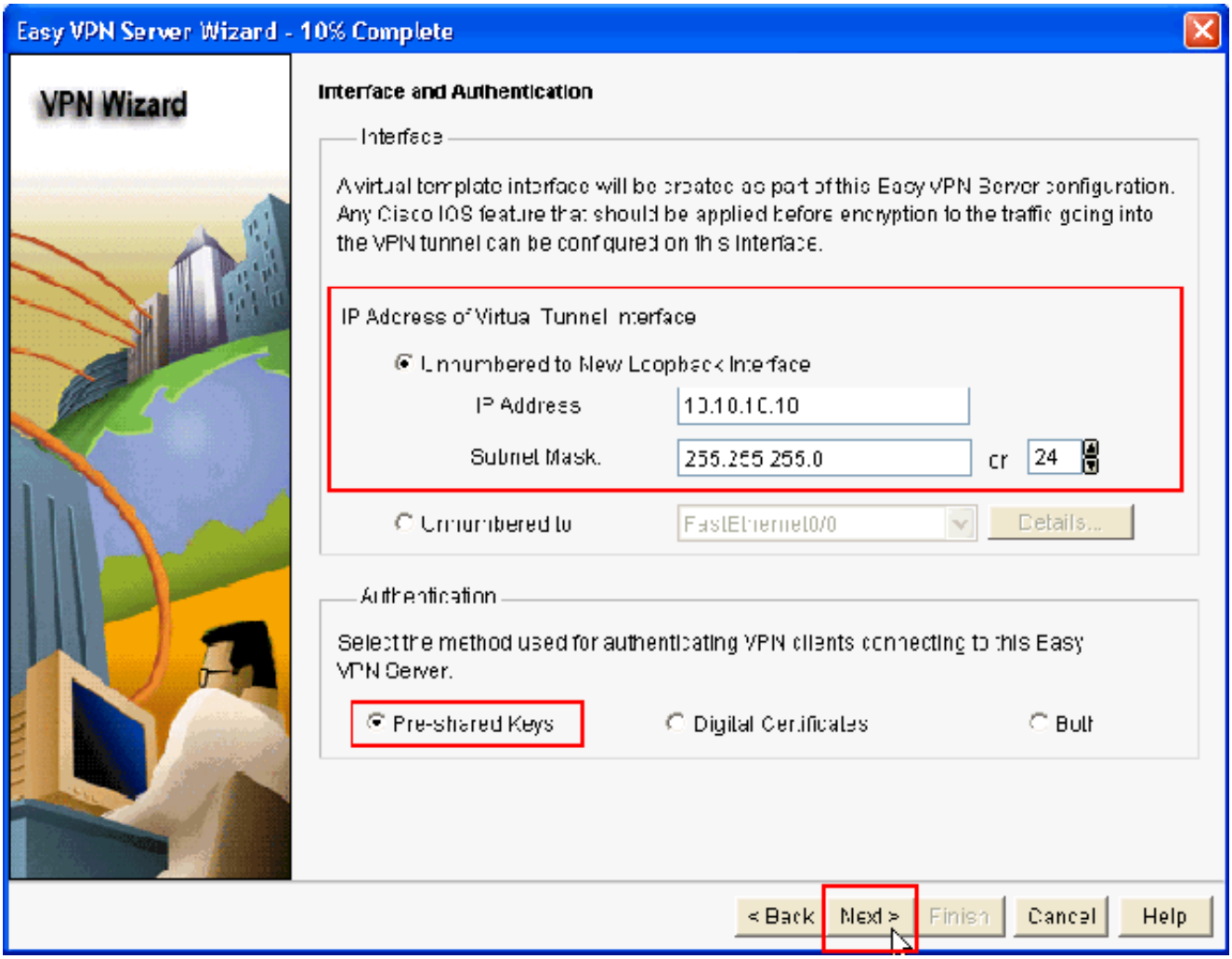
1. Choisissez Configure > Security > VPN > **Easy VPN Server** > **Create Easy VPN Server** et cliquez sur **Launch Easy VPN Server Wizard** afin de configurer le routeur Cisco IOS en tant que serveur Easy VPN Server
:



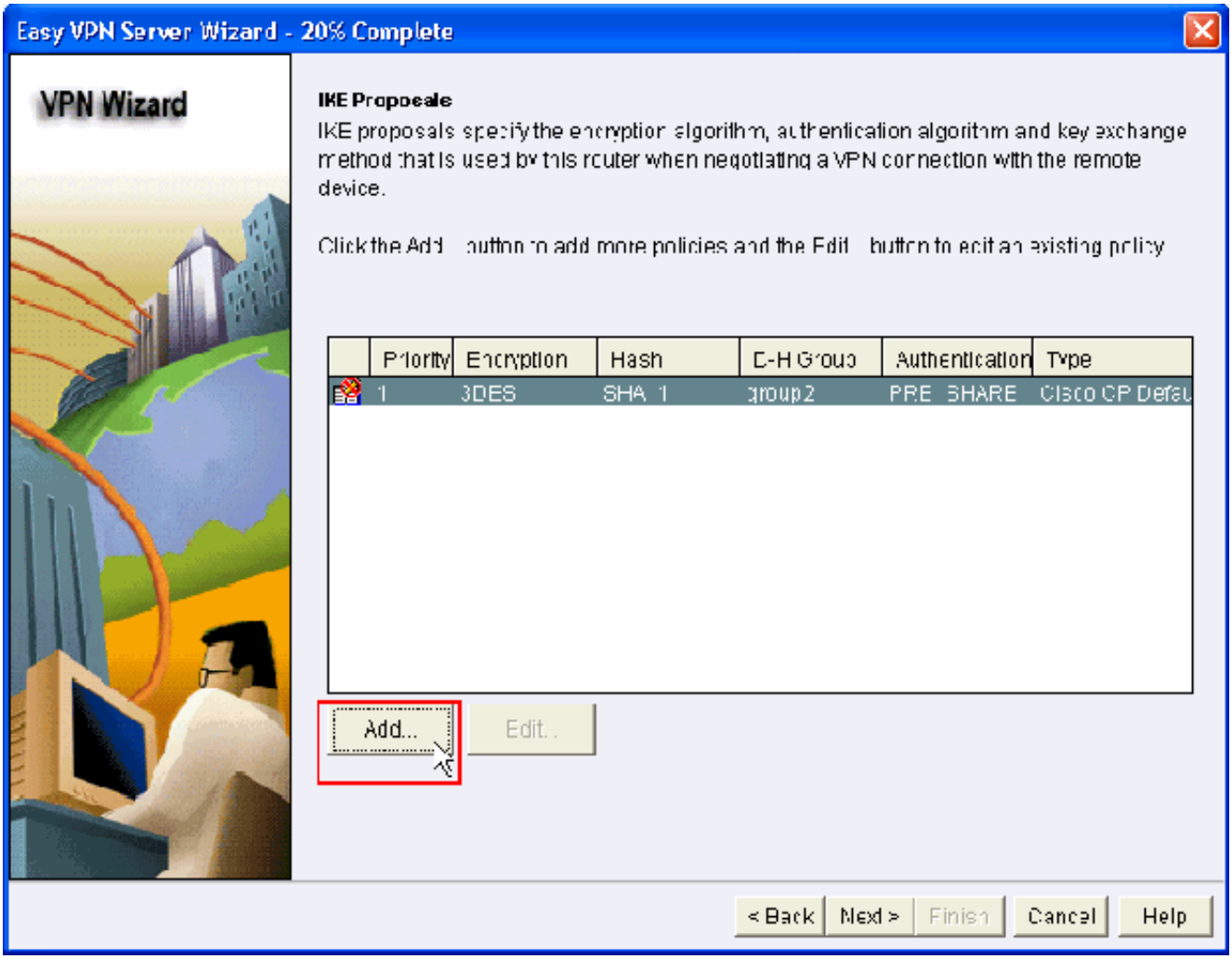
2. Cliquez sur **Next** afin de poursuivre la configuration de **Easy VPN Server**.



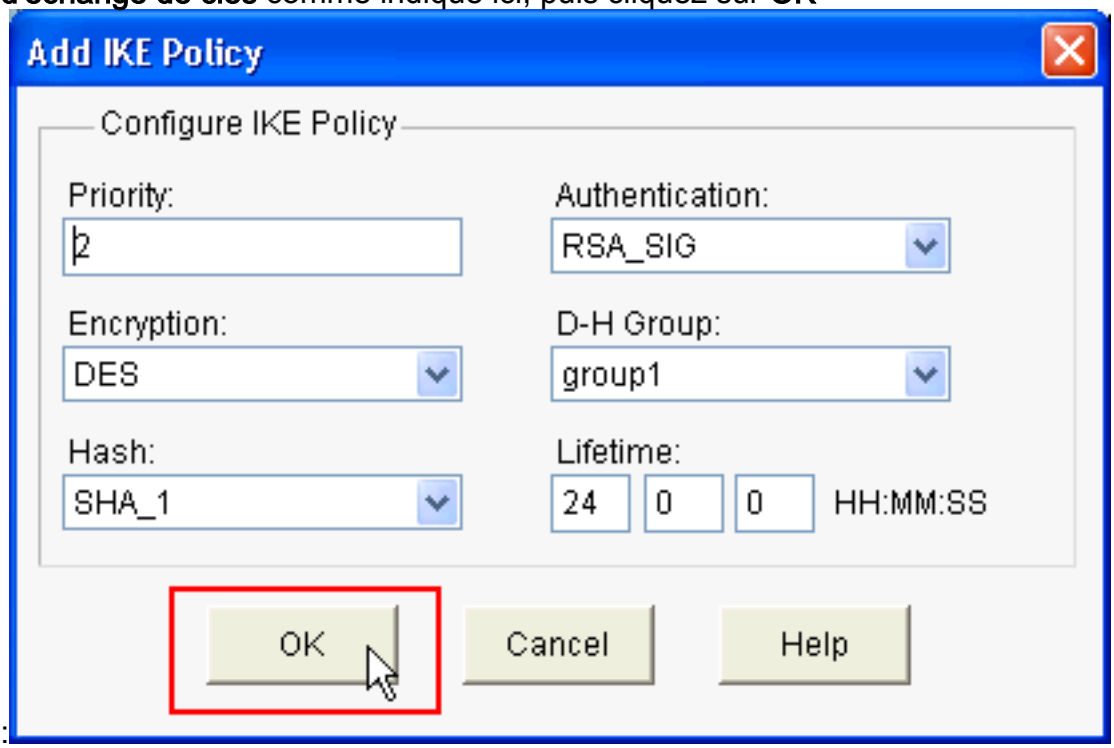
3. Dans la fenêtre qui en résulte, une **interface virtuelle** sera configurée dans le cadre de la configuration du serveur Easy VPN. Fournissez l'**adresse IP de l'interface de tunnel virtuel** et choisissez également la **méthode d'authentification** utilisée pour authentifier les clients VPN. Ici, les **clés prépartagées** sont la méthode d'authentification utilisée. Cliquez sur **Suivant** :



4. Spécifiez l'**algorithme de chiffrement, l'algorithme d'authentification et la méthode d'échange de clés** à utiliser par ce routeur lors de la négociation avec le périphérique distant. Une stratégie IKE par défaut est présente sur le routeur et peut être utilisée si nécessaire. Pour ajouter une nouvelle stratégie IKE, cliquez sur
Ajouter.

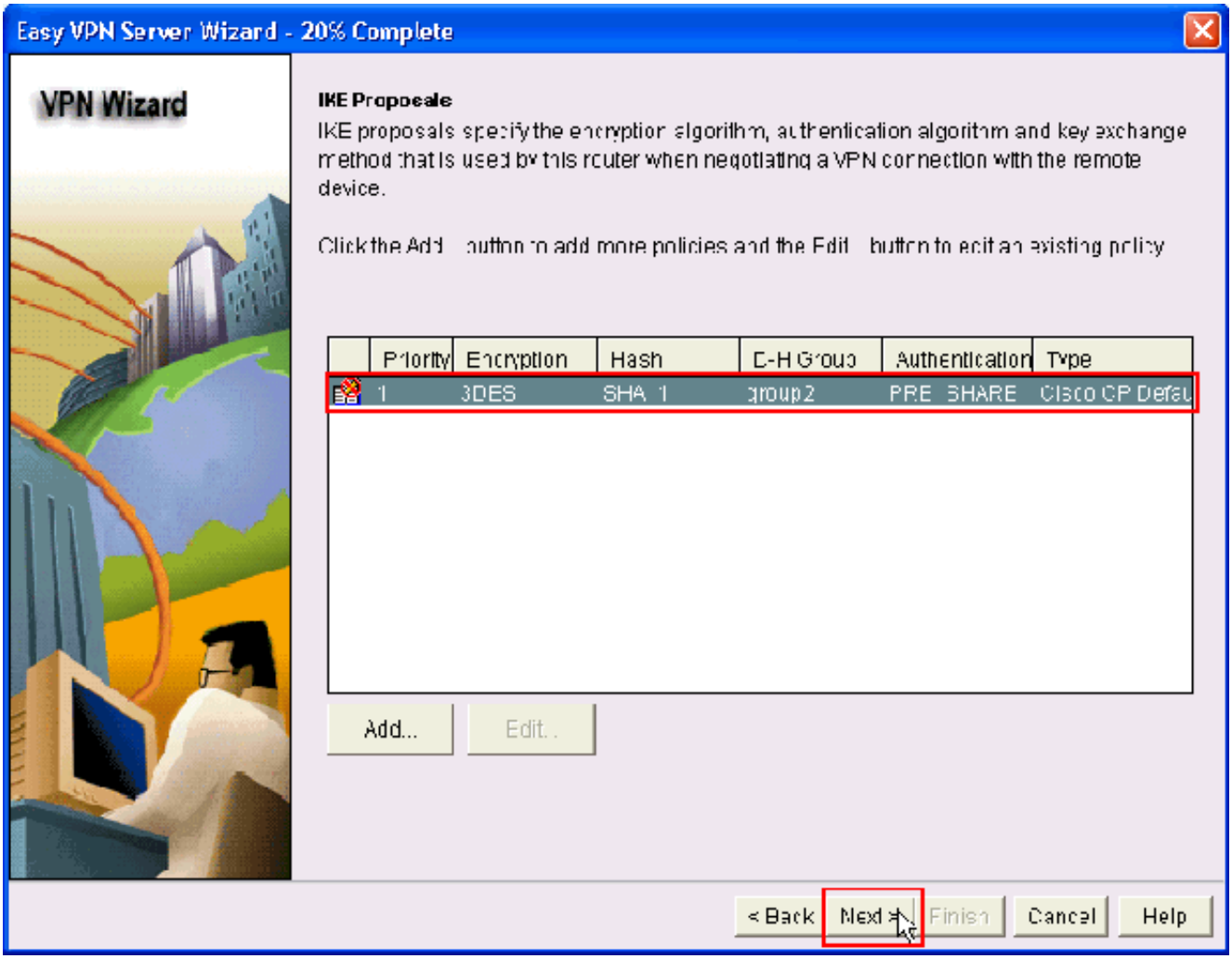


5. Fournissez **l'algorithme de chiffrement**, l'**algorithme d'authentification** et la **méthode d'échange de clés** comme indiqué ici, puis cliquez sur **OK**

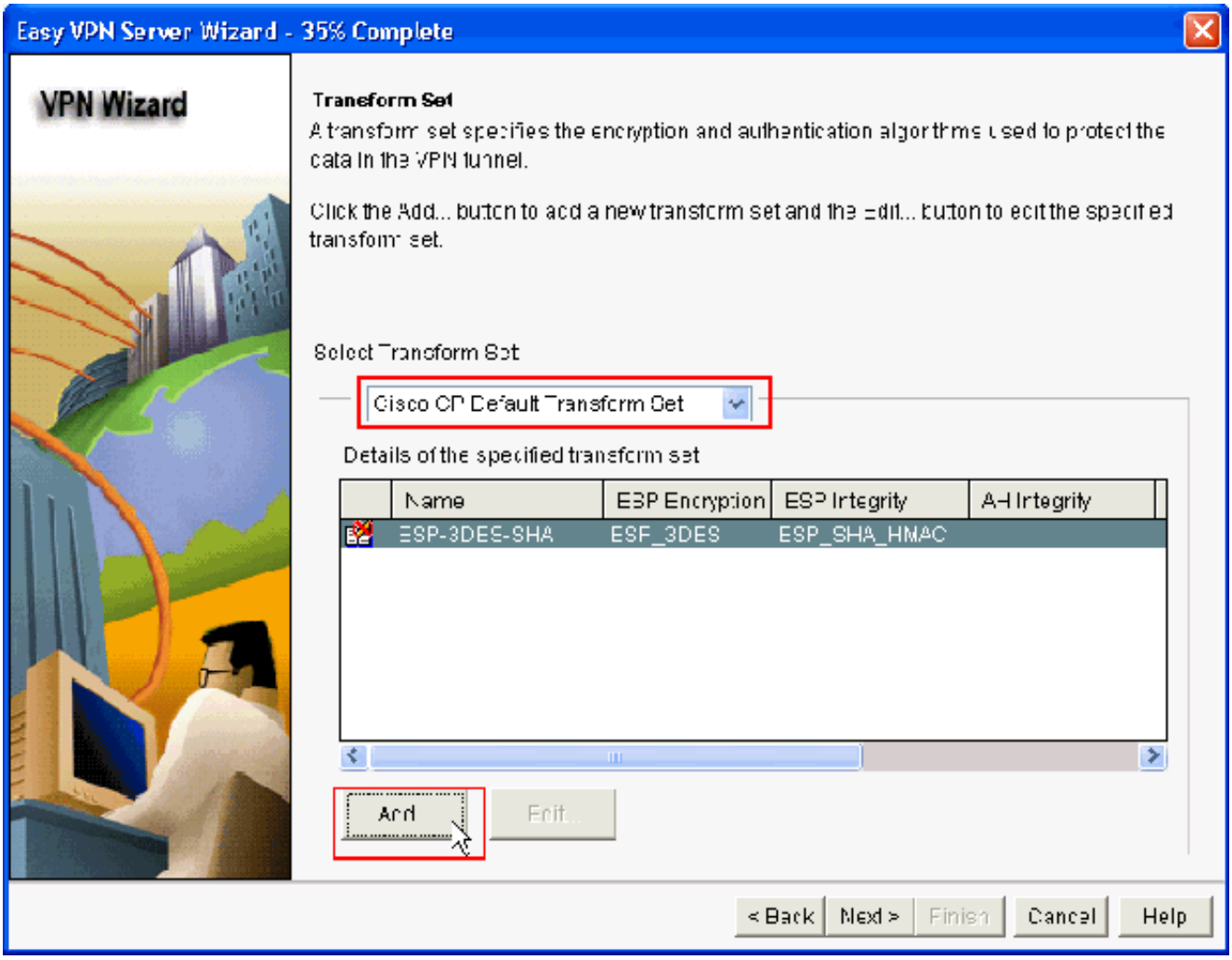


:

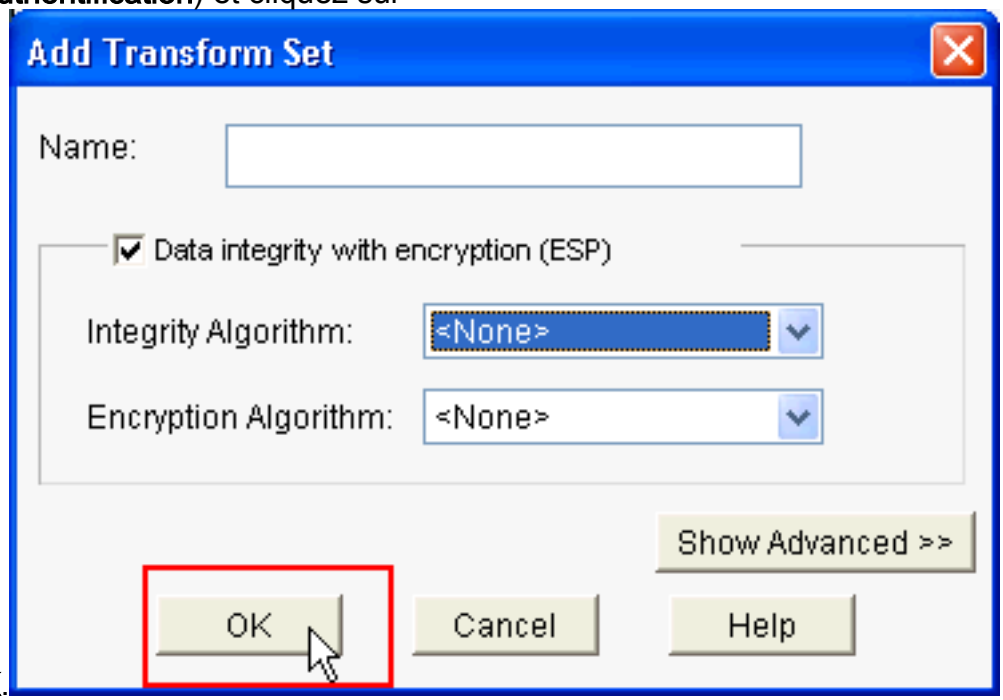
6. La **stratégie IKE par défaut** est utilisée dans cet exemple. Par conséquent, choisissez la stratégie IKE par défaut et cliquez sur **Suivant**.



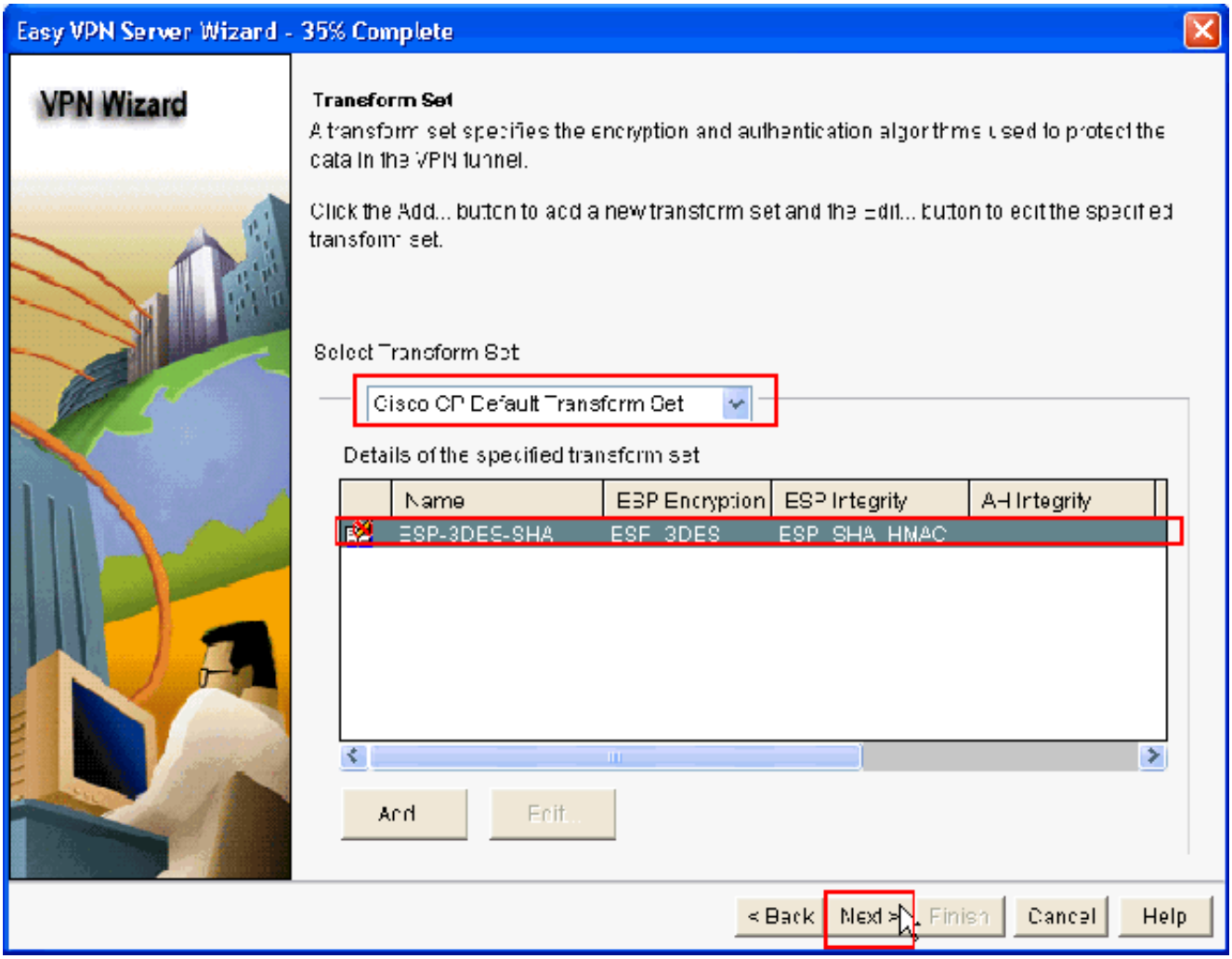
7. Dans la nouvelle fenêtre, les détails **Transform Set** doivent être fournis. Le jeu de transformations (Transform Set) spécifie les algorithmes de **chiffrement et d'intégrité utilisés pour protéger les données dans le tunnel VPN**. Cliquez sur **Ajouter** pour fournir ces détails. Vous pouvez ajouter n'importe quel nombre de jeux de transformation si nécessaire lorsque vous cliquez sur **Ajouter** et fournissez les détails.**Remarque : CP Default Transform Set** est présent par défaut sur le routeur lorsqu'il est configuré à l'aide de **Cisco CP**.



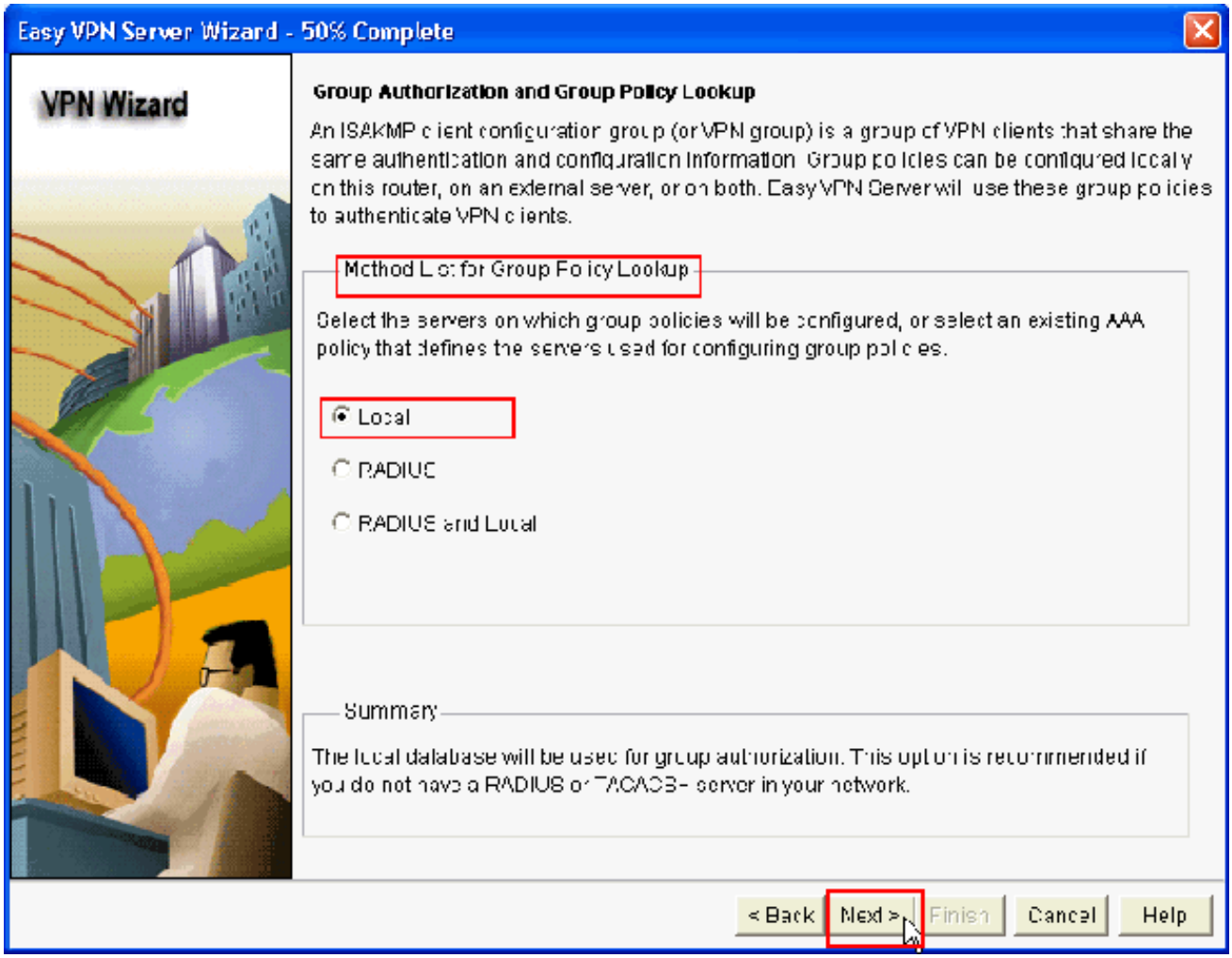
8. Fournissez les détails **du jeu de transformation** (**Algorithme de chiffrement et d'authentification**) et cliquez sur **OK**.



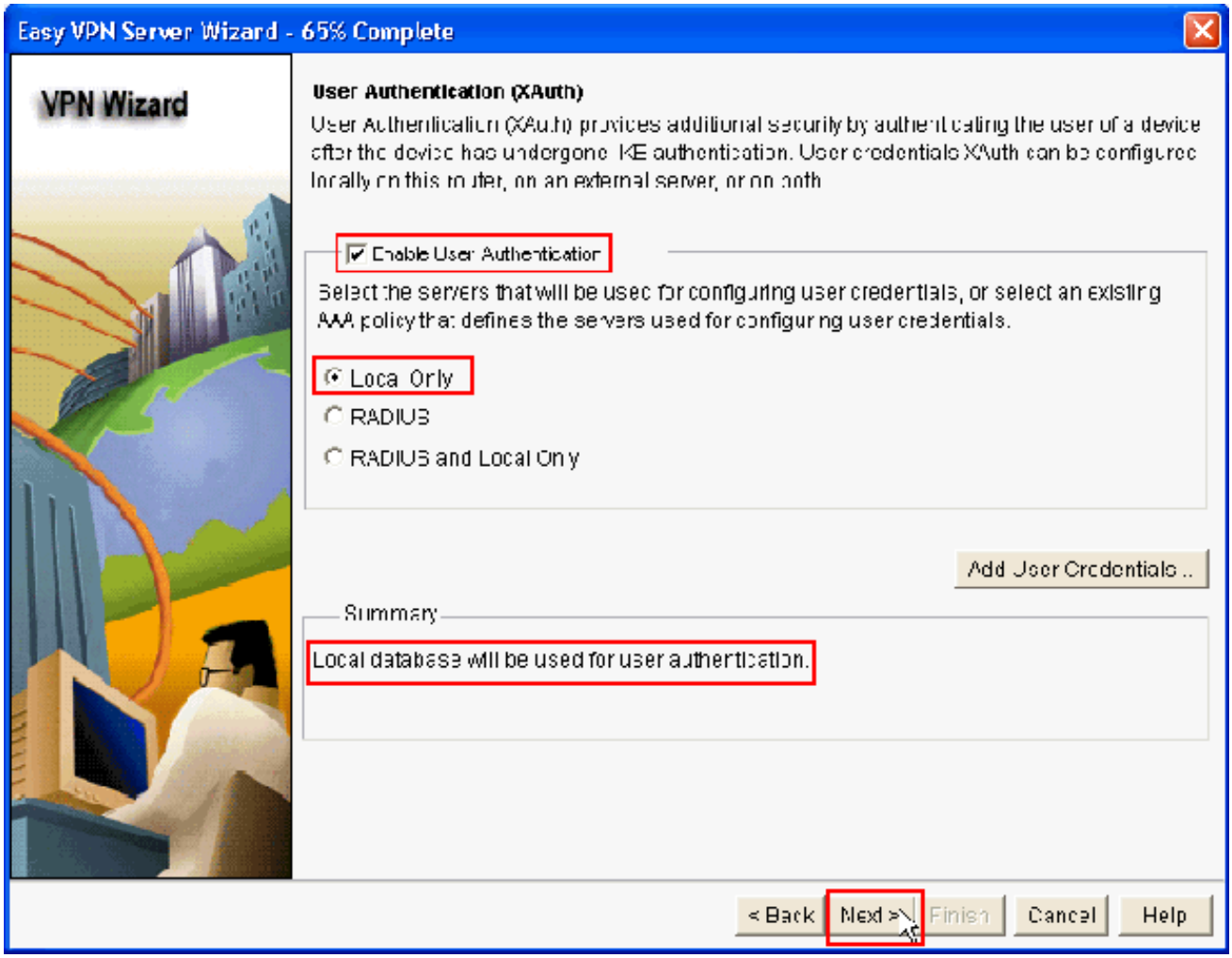
9. Le **jeu de transformation par défaut** nommé **jeu de transformation par défaut CP** est utilisé dans cet exemple. Par conséquent, choisissez le jeu de transformation par défaut et cliquez sur **Suivant**.



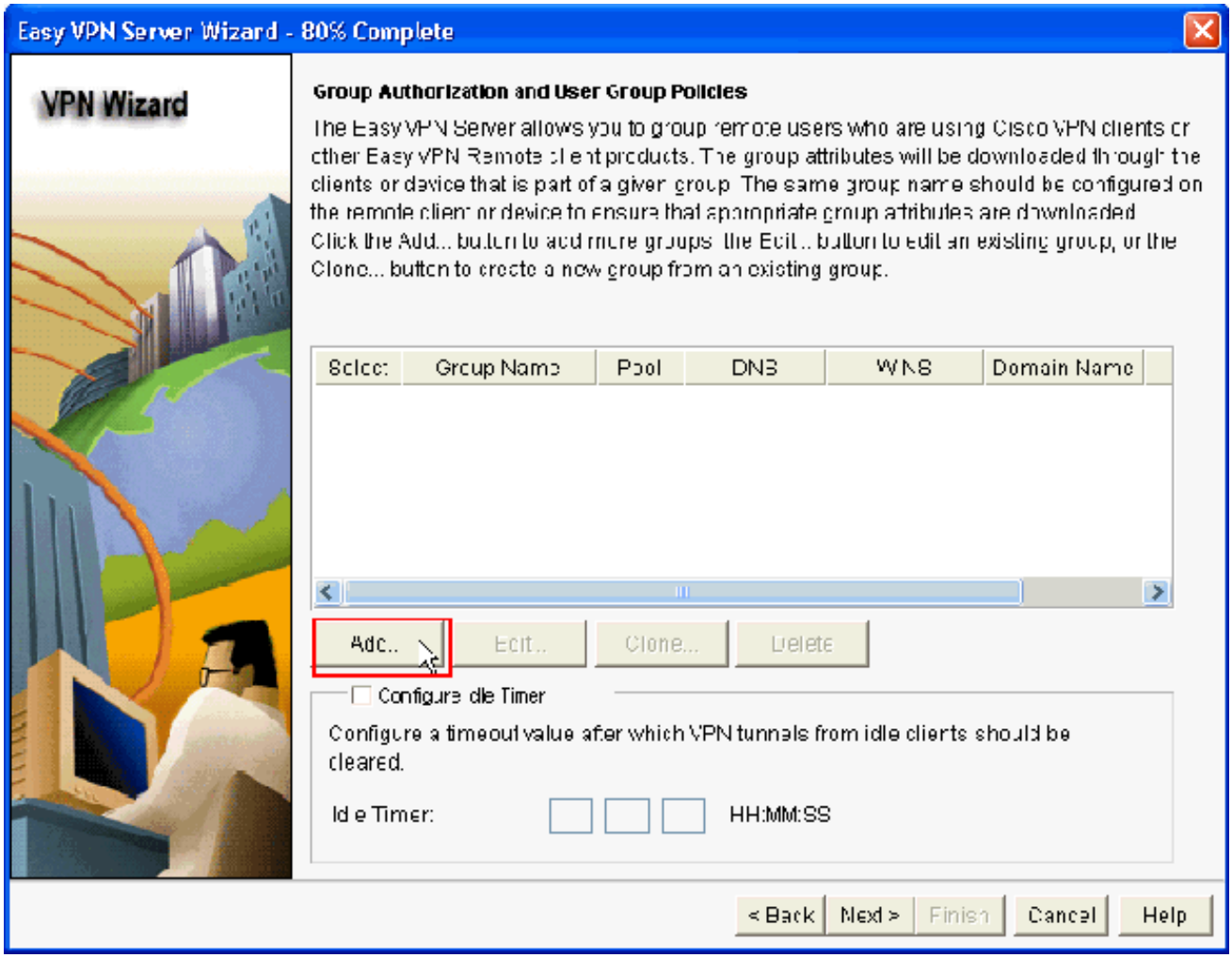
10. Dans la nouvelle fenêtre, sélectionnez le serveur sur lequel les stratégies de groupe seront configurées, qui peut être **Local** ou **RADIUS** ou **Local et RADIUS**. Dans cet exemple, nous utilisons **le serveur local** pour configurer les stratégies de groupe. Choisissez **Local** et cliquez sur
Next.



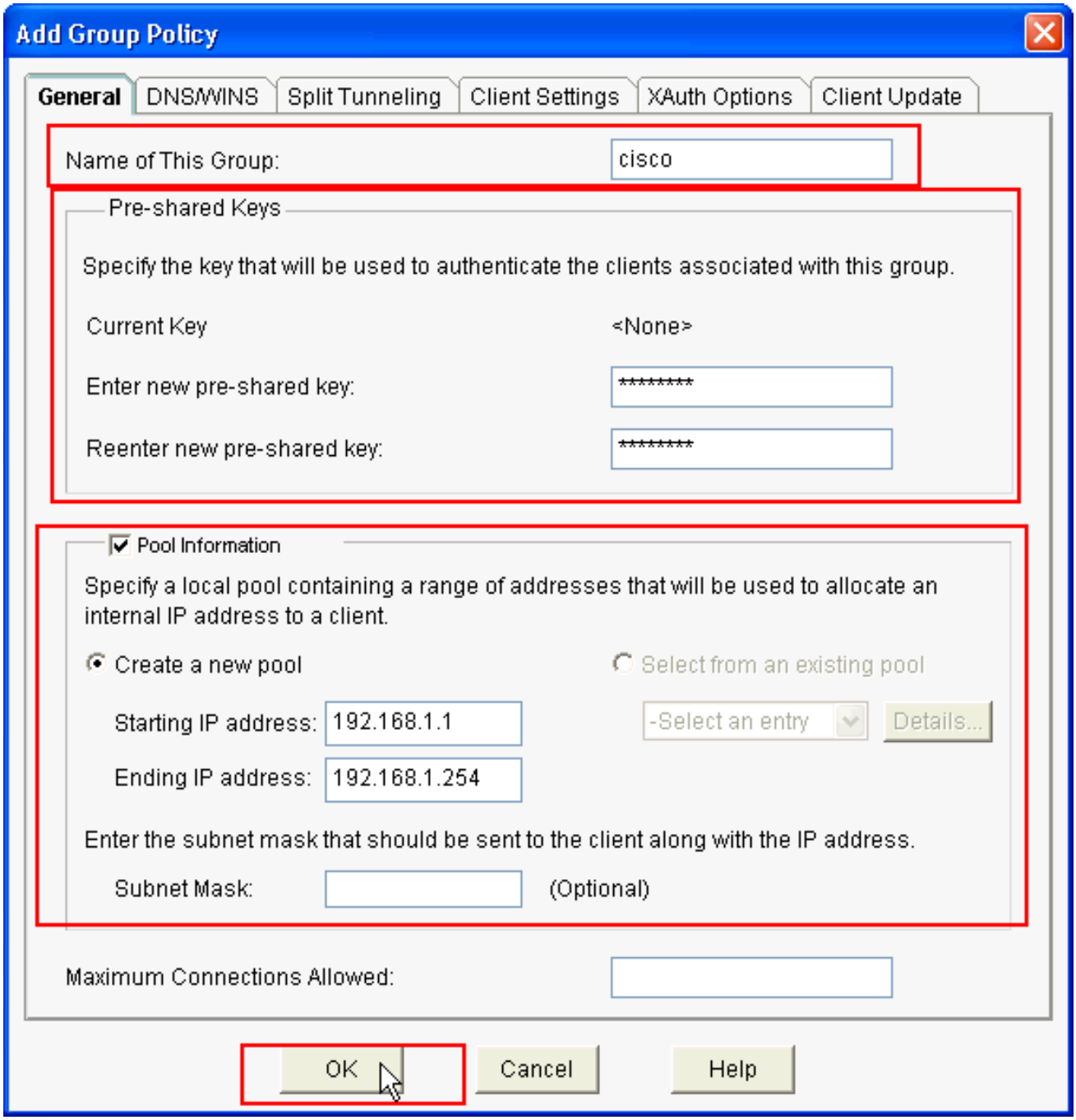
11. Choisissez le serveur à utiliser pour l'authentification utilisateur dans cette nouvelle fenêtre qui peut être **Local Only** ou **RADIUS** ou **Local Only et RADIUS**. Dans cet exemple, nous utilisons **le serveur local** pour configurer les informations d'identification de l'utilisateur pour l'authentification. Assurez-vous que la case à cocher en regard de **Enable User Authentication** est cochée. Choisissez **Local Only** et cliquez sur **Next**.



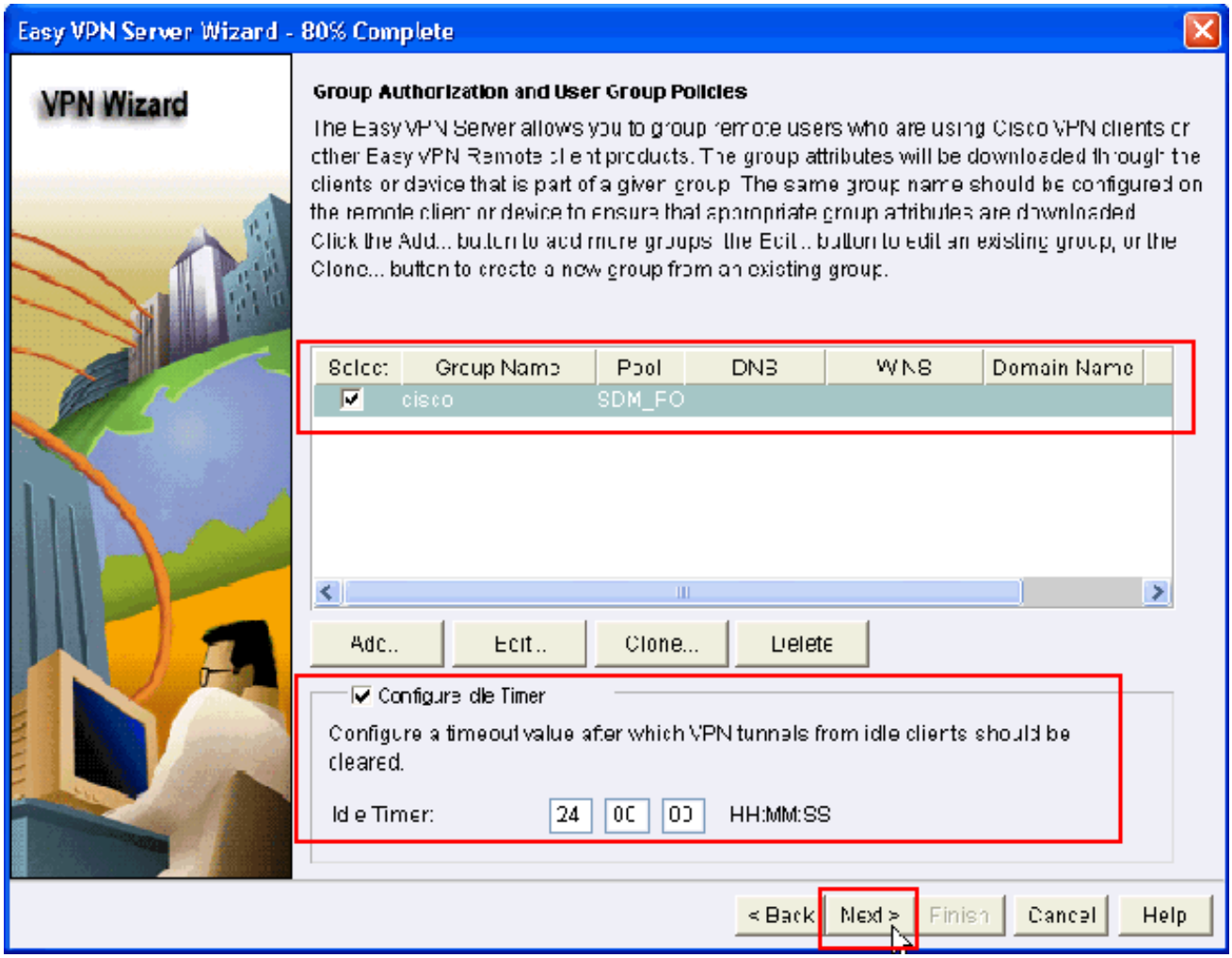
12. Cliquez sur **Ajouter** pour créer une nouvelle stratégie de groupe et ajouter les utilisateurs distants dans ce
groupe.



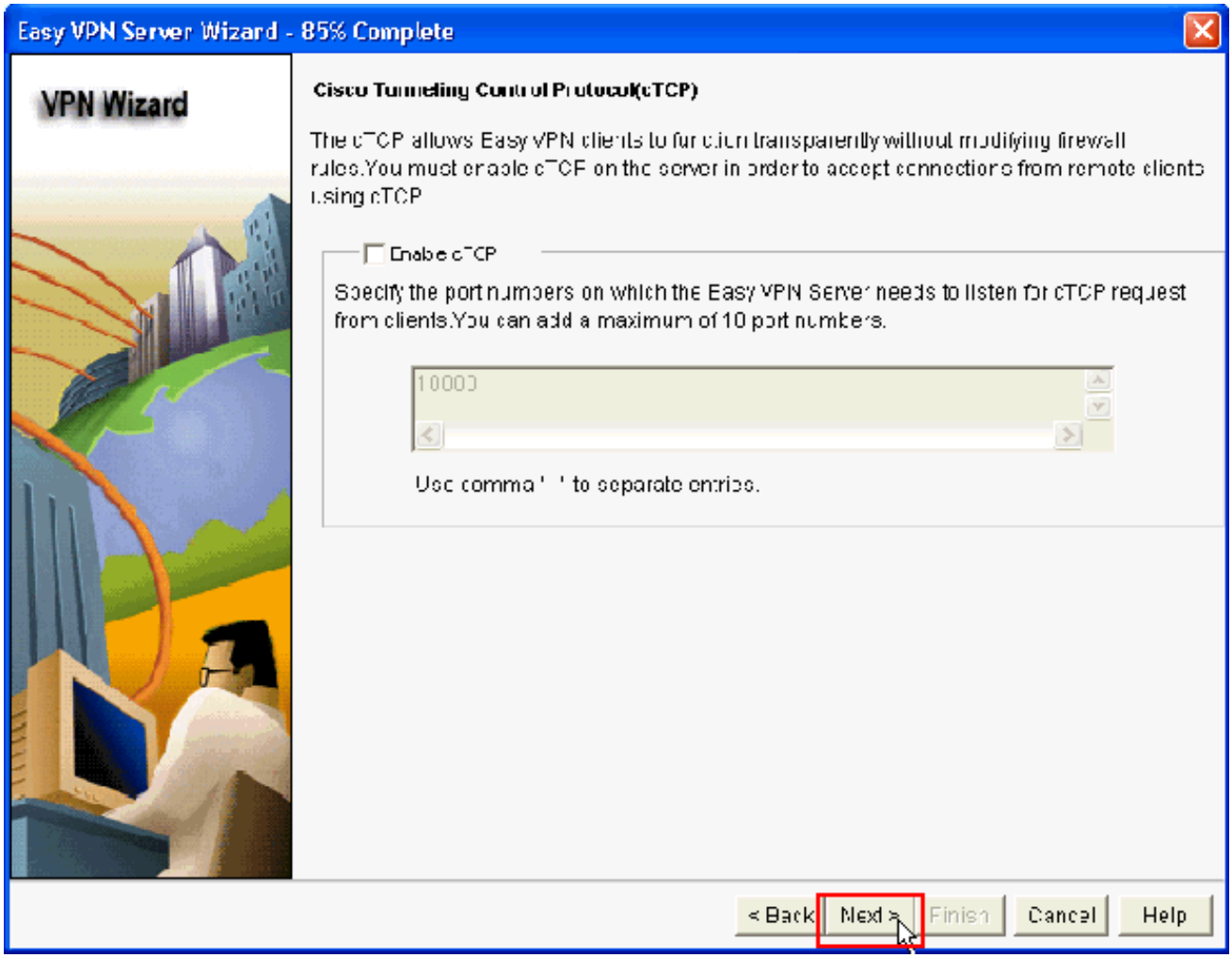
13. Dans la fenêtre Ajouter une stratégie de groupe, indiquez le nom du groupe dans l'espace prévu à cet effet (cisco dans cet exemple) avec la clé prépartagée, et les informations du pool IP (l'adresse IP de début et l'adresse IP de fin) comme indiqué et cliquez sur **OK**.**Remarque :** Vous pouvez créer un nouveau pool d'adresses IP ou utiliser un pool d'adresses IP existant, le cas
échéant.



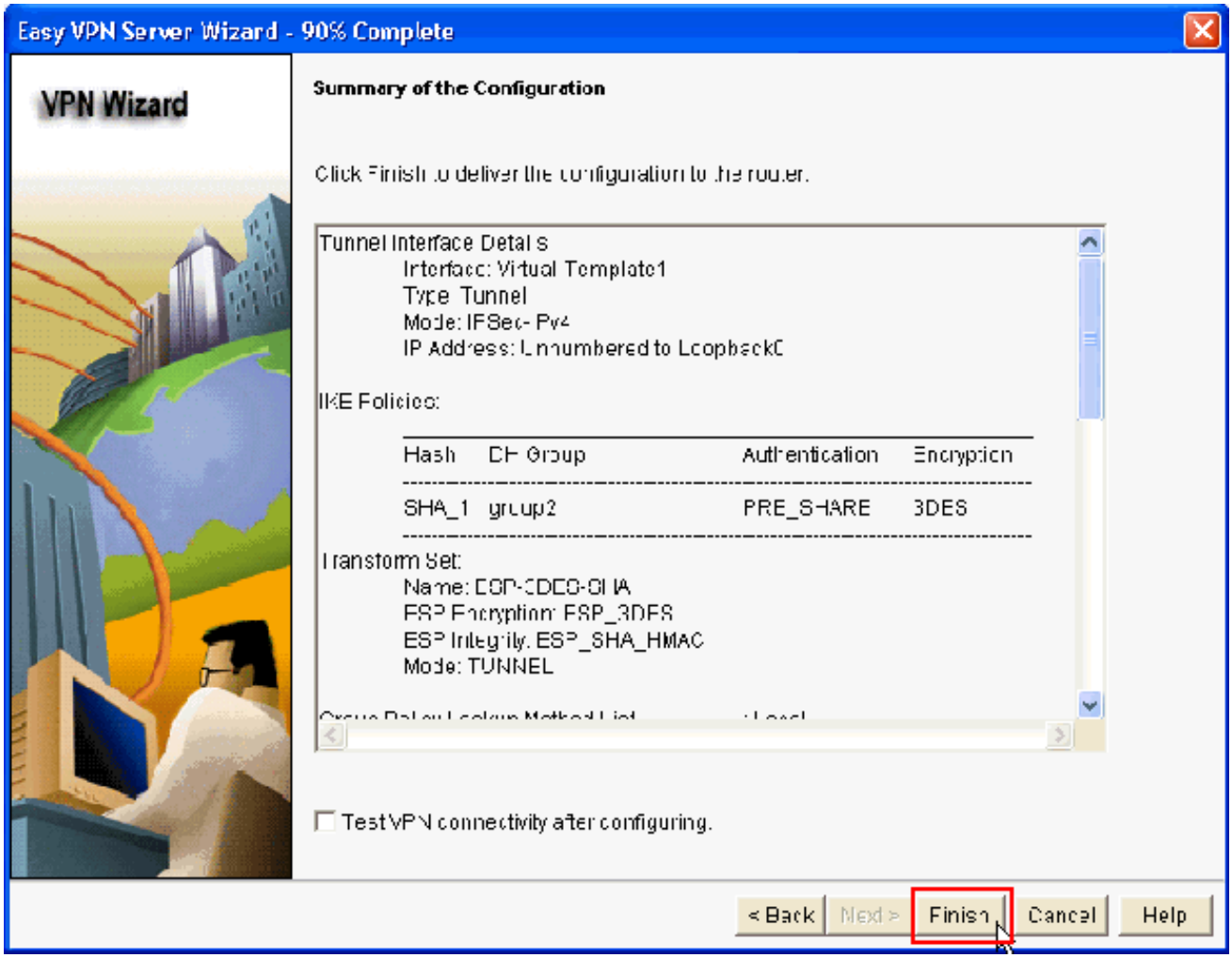
14. Sélectionnez maintenant la nouvelle **stratégie de groupe** créée avec le nom **cisco**, puis cochez la case en regard de **Configurer le minuteur inactif** selon les besoins afin de configurer le **minuteur inactif**. Cliquez sur **Next** (Suivant).



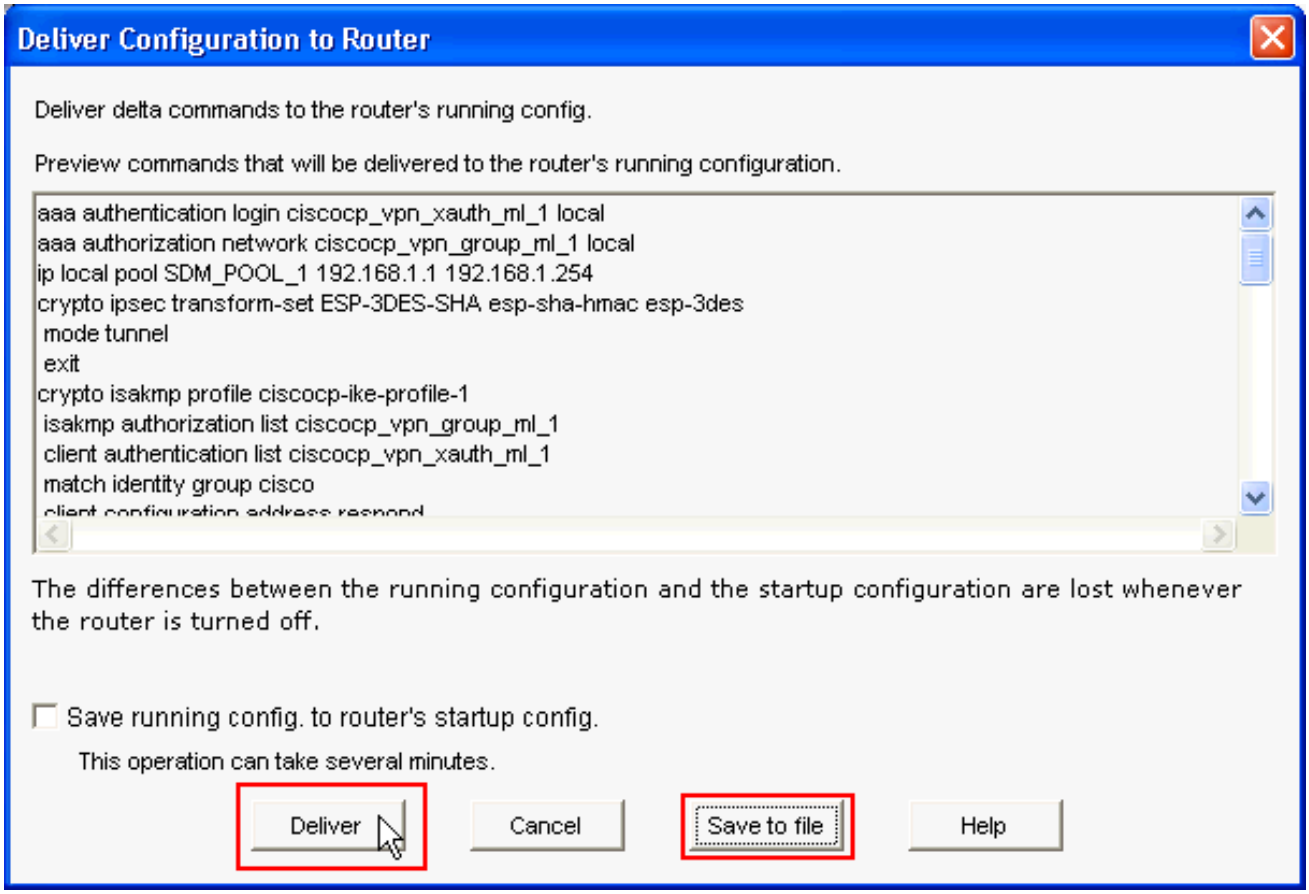
15. Activez **le protocole cTCP (Cisco Tunneling Control Protocol)** si nécessaire. Sinon, cliquez sur
Suivant.



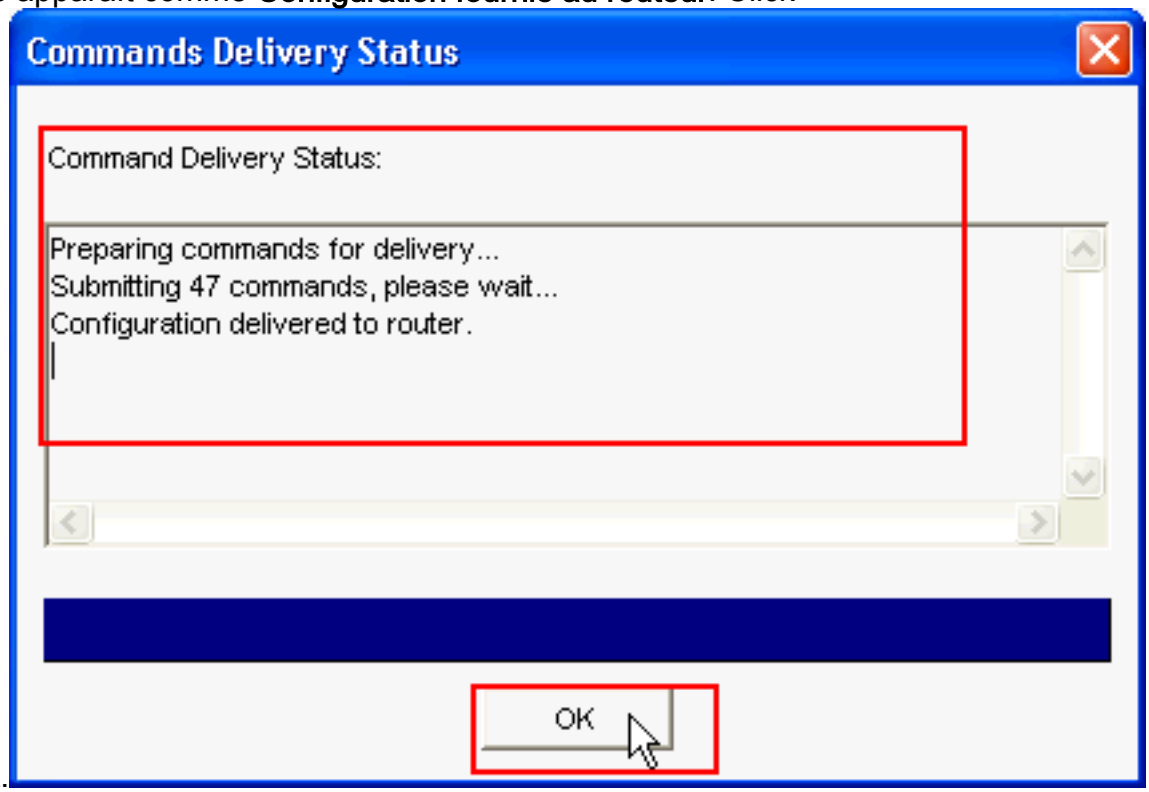
16. Examinez le **récapitulatif de la configuration**. **Cliquez sur Finish.**



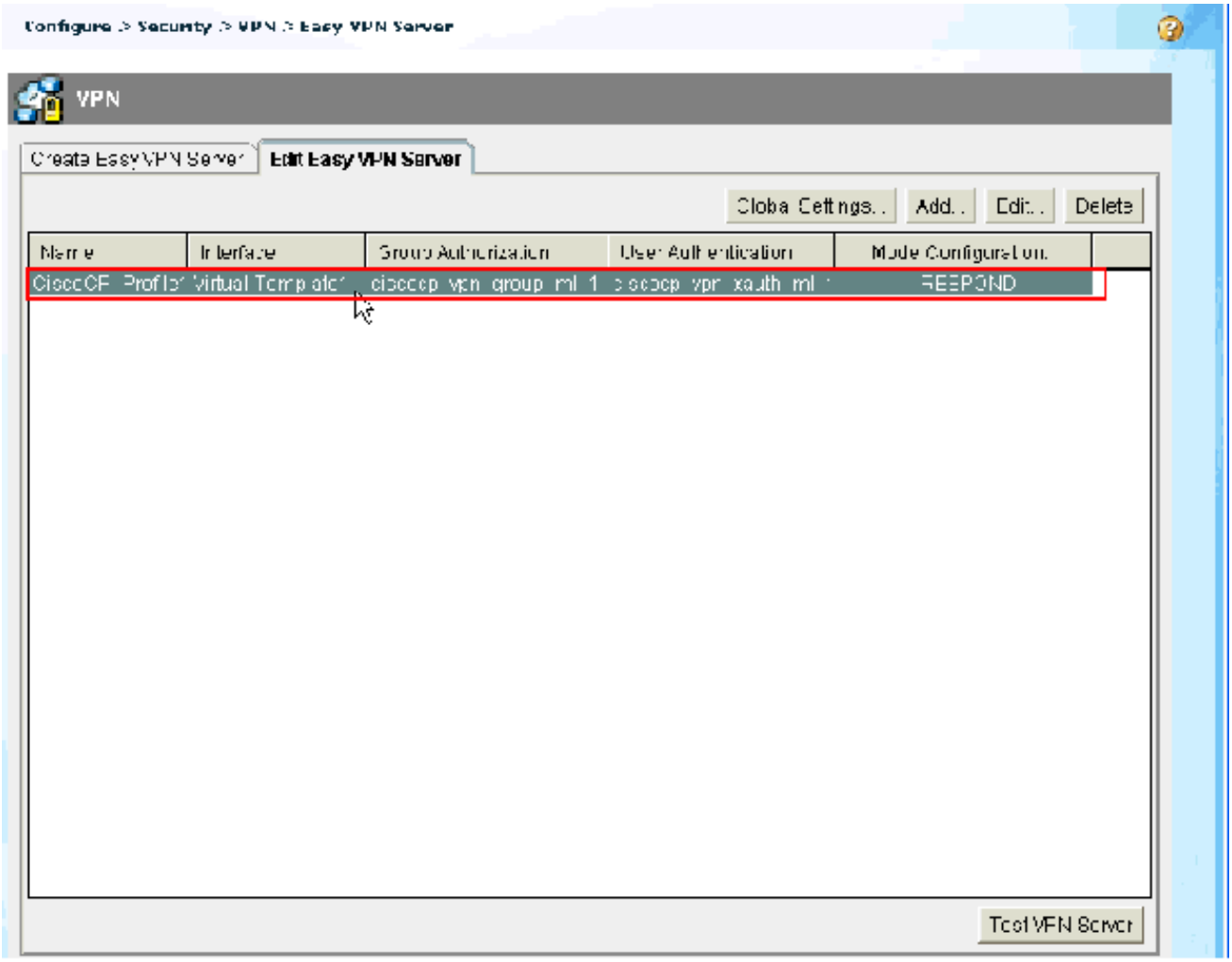
17. Dans la fenêtre **Deliver Configuration to Router**, cliquez sur **Deliver** pour remettre la configuration au routeur. Vous pouvez cliquer sur **Enregistrer dans un fichier** pour enregistrer la configuration sous forme de fichier sur le PC.



18. La fenêtre **Command Delivery Status** affiche l'état de remise des commandes au routeur. Elle apparaît comme **Configuration fournie au routeur**. Click OK.



19. Vous pouvez voir le nouveau serveur Easy VPN. Vous pouvez modifier le serveur existant en sélectionnant **Edit Easy VPN Server**. Ceci termine la configuration du serveur Easy VPN Server sur le routeur Cisco IOS.



Configuration CLI

Configuration du routeur

```
Router#show run
Building configuration...

Current configuration : 2069 bytes
! version 12.4 service timestamps debug datetime msec
service timestamps log datetime msec no service
password-encryption hostname Router boot-start-marker
boot-end-marker no logging buffered enable password
cisco !---AAA enabled using aaa newmodel command. Also
AAA Authentication and Authorization are enabled---! aaa
new-model
!
!
aaa authentication login ciscocp_vpn_xauth_ml_1 local
aaa authorization network ciscocp_vpn_group_ml_1 local
!
!
aaa session-id common
ip cef
!
!
!
!
ip domain name cisco.com
!
```

```
multilink bundle-name authenticated
!
!
!--- Configuration for IKE policies. !--- Enables the
IKE policy configuration (config-isakmp) !--- command
mode, where you can specify the parameters that !--- are
used during an IKE negotiation. Encryption and Policy
details are hidden as the default values are chosen.
crypto isakmp policy 1
 encr 3des
 authentication pre-share
 group 2
crypto isakmp keepalive 10
!
crypto isakmp client configuration group cisco
 key cisco123
 pool SDM_POOL_1
crypto isakmp profile ciscocp-ike-profile-1
   match identity group cisco
   client authentication list ciscocp_vpn_xauth_ml_1
   isakmp authorization list ciscocp_vpn_group_ml_1
   client configuration address respond
   virtual-template 1
!
!
!--- Configuration for IPsec policies. !--- Enables the
crypto transform configuration mode, !--- where you can
specify the transform sets that are used !--- during an
IPsec negotiation. crypto ipsec transform-set ESP-3DES-
SHA esp-3des esp-sha-hmac
!
crypto ipsec profile CiscoCP_Profile1
 set security-association idle-time 86400
 set transform-set ESP-3DES-SHA
 set isakmp-profile ciscocp-ike-profile-1
!
!
!
!--- RSA certificate generated after you enable the !---
ip http secure-server command.

crypto pki trustpoint TP-self-signed-1742995674
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-1742995674
 revocation-check none
 rsakeypair TP-self-signed-1742995674

!--- Create a user account named cisco123 with all
privileges.

username cisco123 privilege 15 password 0 cisco123
archive
 log config
  hidekeys
!
!
!--- Interface configurations are done as shown below---
! interface Loopback0 ip address 10.10.10.10
255.255.255.0 ! interface FastEthernet0/0 ip address
10.77.241.111 255.255.255.192 duplex auto speed auto !
interface Virtual-Template1 type tunnel ip unnumbered
Loopback0 tunnel mode ipsec ipv4 tunnel protection ipsec
profile CiscoCP_Profile1 ! !--- VPN pool named
SDM_POOL_1 has been defined in the below command---! ip
```

```
local pool SDM_POOL_1 192.168.1.1 192.168.1.254

!--- This is where the commands to enable HTTP and HTTPS
are configured. ip http server ip http authentication
local ip http secure-server ! ! ! ! control-plane ! line
con 0 line aux 0 !--- Telnet enabled with password as
cisco. line vty 0 4 password cisco transport input all
scheduler allocate 20000 1000 ! ! ! ! end
```

Vérification

Easy VPN Server - Commandes show

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

- **show crypto isakmp sa — Affiche toutes les SA IKE en cours au niveau d'un homologue.**

```
Router#show crypto isakmp sa

IPv4 Crypto ISAKMP SA
dst             src             state          conn-id slot status
10.77.241.111   172.16.1.1     QM_IDLE           1003    0 ACTIVE
```

- **show crypto ipsec sa — Affiche toutes les SA IPsec en cours au niveau d'un homologue.**

```
Router#show crypto ipsec sa
interface: Virtual-Access2
    Crypto map tag: Virtual-Access2-head-0, local addr 10.77.241.111

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (192.168.1.3/255.255.255.255/0/0)
   current_peer 172.16.1.1 port 1086
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 28, #pkts encrypt: 28, #pkts digest: 28
    #pkts decaps: 36, #pkts decrypt: 36, #pkts verify: 36
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 2

     local crypto endpt.: 10.77.241.111, remote crypto endpt.: 172.16.1.1
     path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
     current outbound spi: 0x186C05EF(409732591)

     inbound esp sas:
      spi: 0x42FC8173(1123844467)
        transform: esp-3des esp-sha-hmac
```

Dépannage

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

Remarque : reportez-vous à Informations importantes sur les commandes de débogage avant d'émettre des commandes de débogage.

Informations connexes

- Négociation IPSec/Protocoles IKE
- Guide de démarrage rapide de Cisco Configuration Professional
- Page d'assistance de produit Cisco - Routeurs
- Support et documentation techniques - Cisco Systems