# Exemplo de Configuração do IOS Router as Easy VPN Server Utilizando Configuration Professional

## Contents


[Introduction](#)
[Prerequisites](#)
[Componentes Utilizados](#)
[Instalar o Cisco CP](#)
[Configuração do roteador para executar o Cisco CP](#)
[Requirements](#)
[Conventions](#)
[Configurar](#)
[Diagrama de Rede](#)
[Cisco CP - Configuração fácil do servidor VPN](#)
[Configuração de CLI](#)
[Verificar](#)
[Easy VPN Server - Comandos show](#)
[Troubleshoot](#)
[Informações Relacionadas](#)


## Introduction

Este documento descreve como configurar um Cisco IOS® Router como um Easy VPN (EzVPN) Server usando o Cisco Configuration Professional (Cisco CP) e a CLI. A característica Easy VPN Server permite que um usuário final remoto comunique-se usando a Segurança IP (IPsec) com qualquer gateway da Rede Privada Virtual (VPN) do Cisco IOS. As políticas de IPsec centralmente gerenciadas são "empurradas" ao dispositivo de cliente pelo servidor, minimizando a configuração pelo usuário final.

Para obter mais informações sobre o Easy VPN Server, consulte a seção Easy VPN Server da Secure Connectivity Configuration Guide Library, Cisco IOS versão 12.4T.

## Prerequisites

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Roteador Cisco 1841 com Software Cisco IOS versão 12.4(15T)

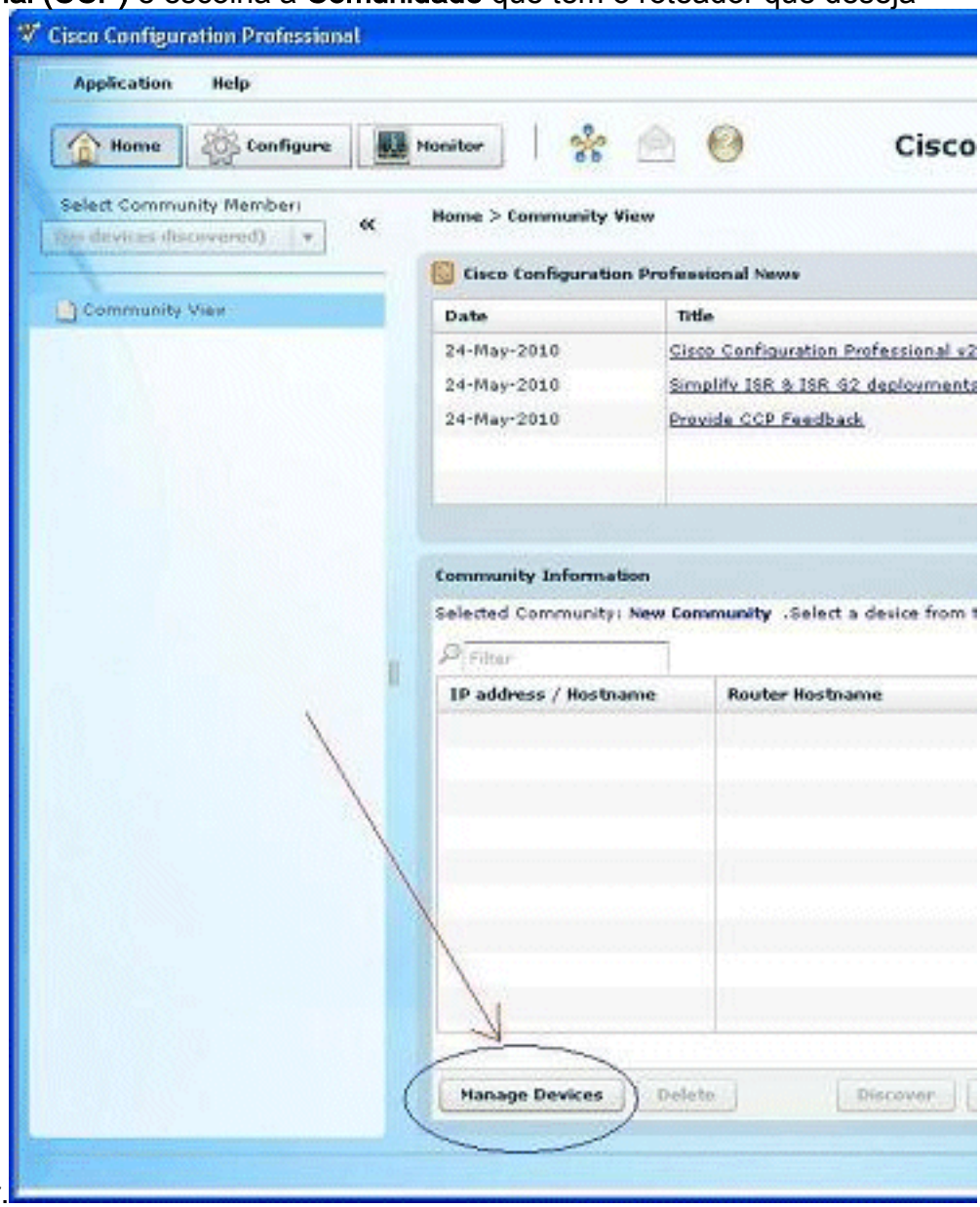
- Cisco CP Versão 2.1

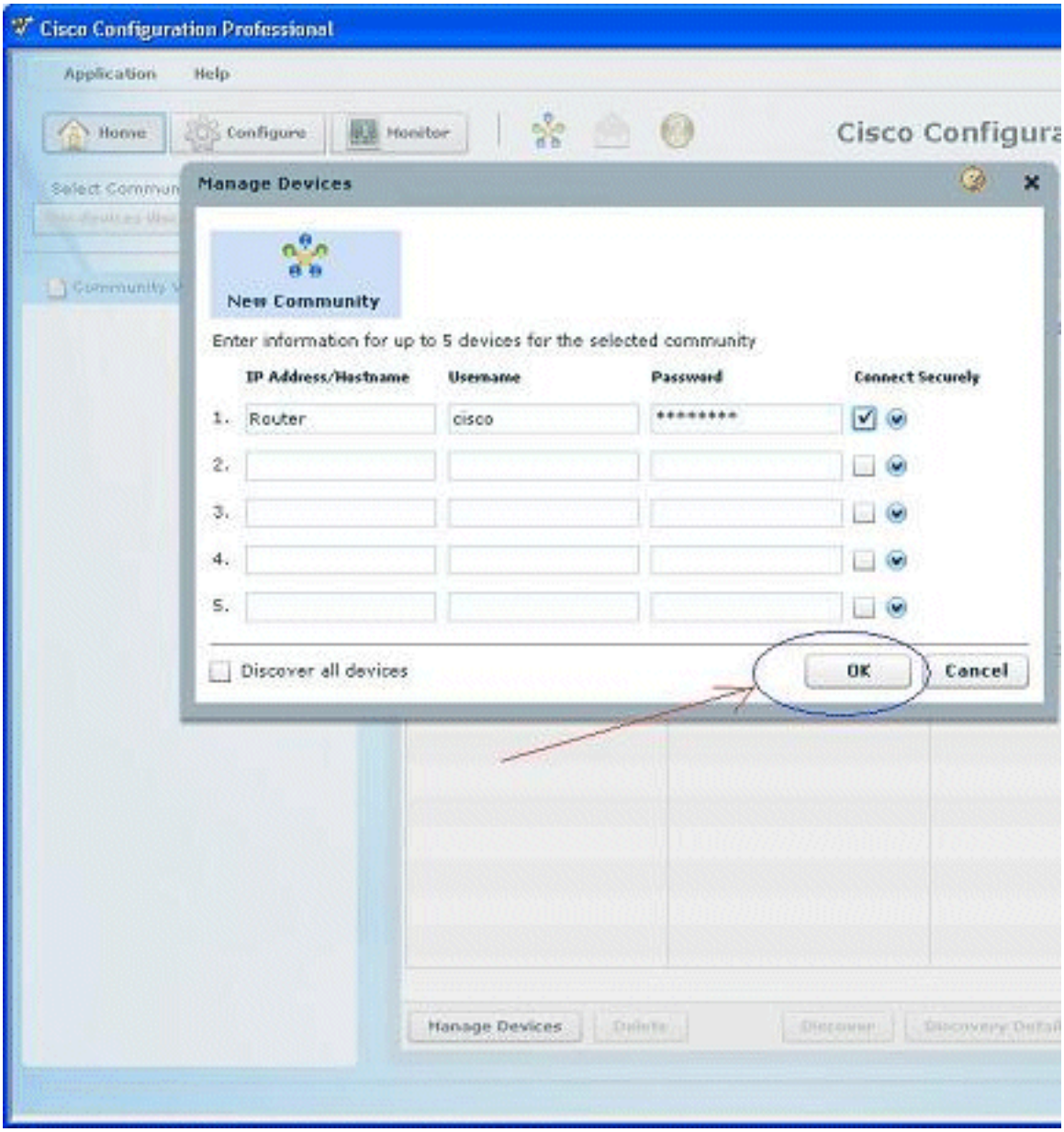
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Instalar o Cisco CP

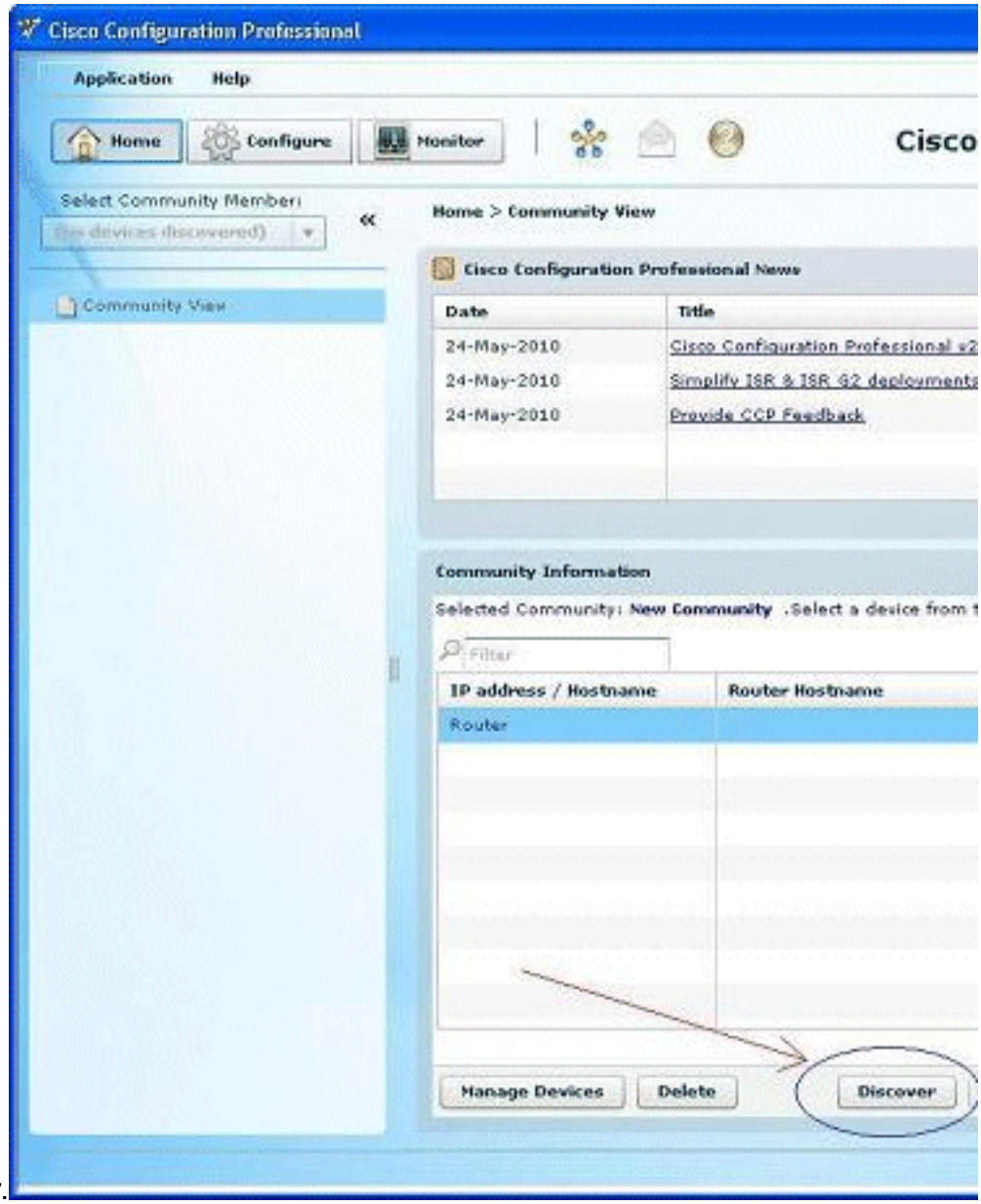
Execute estas etapas para instalar o Cisco CP:

1. Baixe o Cisco CP V2.1 do Cisco Software Center (somente clientes registrados) e instale-o em seu PC local.A versão mais recente do Cisco CP pode ser encontrada no site do Cisco CP.
2. Inicie o Cisco CP no seu PC local através de **Iniciar > Programas > Cisco Configuration Professional (CCP)** e escolha a **Comunidade** que tem o roteador que deseja configurar.






3. Para descobrir o dispositivo que deseja configurar, realce o roteador e clique em




**Descobrir**.

**Observação:** para obter informações sobre os modelos de roteador Cisco e as versões do IOS compatíveis com o Cisco CP v2.1, consulte a seção Compatível com as versões do Cisco IOS.

**Observação:** para obter informações sobre os requisitos do PC que executa o Cisco CP v2.1, consulte a seção Requisitos do sistema.

## Configuração do roteador para executar o Cisco CP

Siga estas etapas de configuração para executar o Cisco CP em um roteador da Cisco:

1. Conecte-se ao roteador usando Telnet, SSH ou por meio do console.Entre no modo de configurações globais usando este comando:
   ```
   Router(config)#enable
   Router(config)#
   ```
2. Se HTTP e HTTPS estiverem habilitados e configurados para usar números de porta fora do padrão, pule essa etapa e use o número da porta já configurado.Habilite o servidor HTTP ou HTTPS do roteador usando estes comandos do Software Cisco IOS:
   ```
   Router(config)# ip http server
   Router(config)# ip http secure-server
   Router(config)# ip http authentication local
   ```

3. Crie um usuário com nível de privilégio 15:
```
Router(config)# username privilege 15 password 0
```

   **Observação:** substitua *<nome de usuário>* e *<senha>* pelo nome de usuário e senha que você deseja configurar.
4. Configure SSH e Telnet para o nível de privilégio e login local 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. (Opcional) Habilite o logon local para oferecer suporte à função de monitoramento de registro:
```
Router(config)# logging buffered 51200 warning
```

## Requirements

Este documento pressupõe que o roteador Cisco está totalmente operacional e configurado para permitir que o Cisco CP faça alterações na configuração.

Para obter informações completas sobre como começar a usar o Cisco CP, consulte Introdução ao Cisco Configuration Professional.

## Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

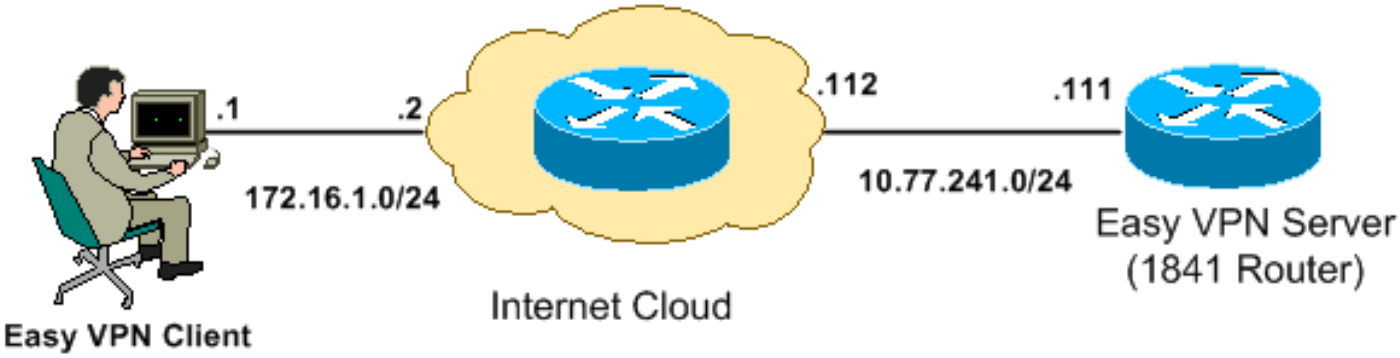
# Configurar

Nesta seção, você recebe informações para definir as configurações básicas de um roteador em uma rede.

**Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.**

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

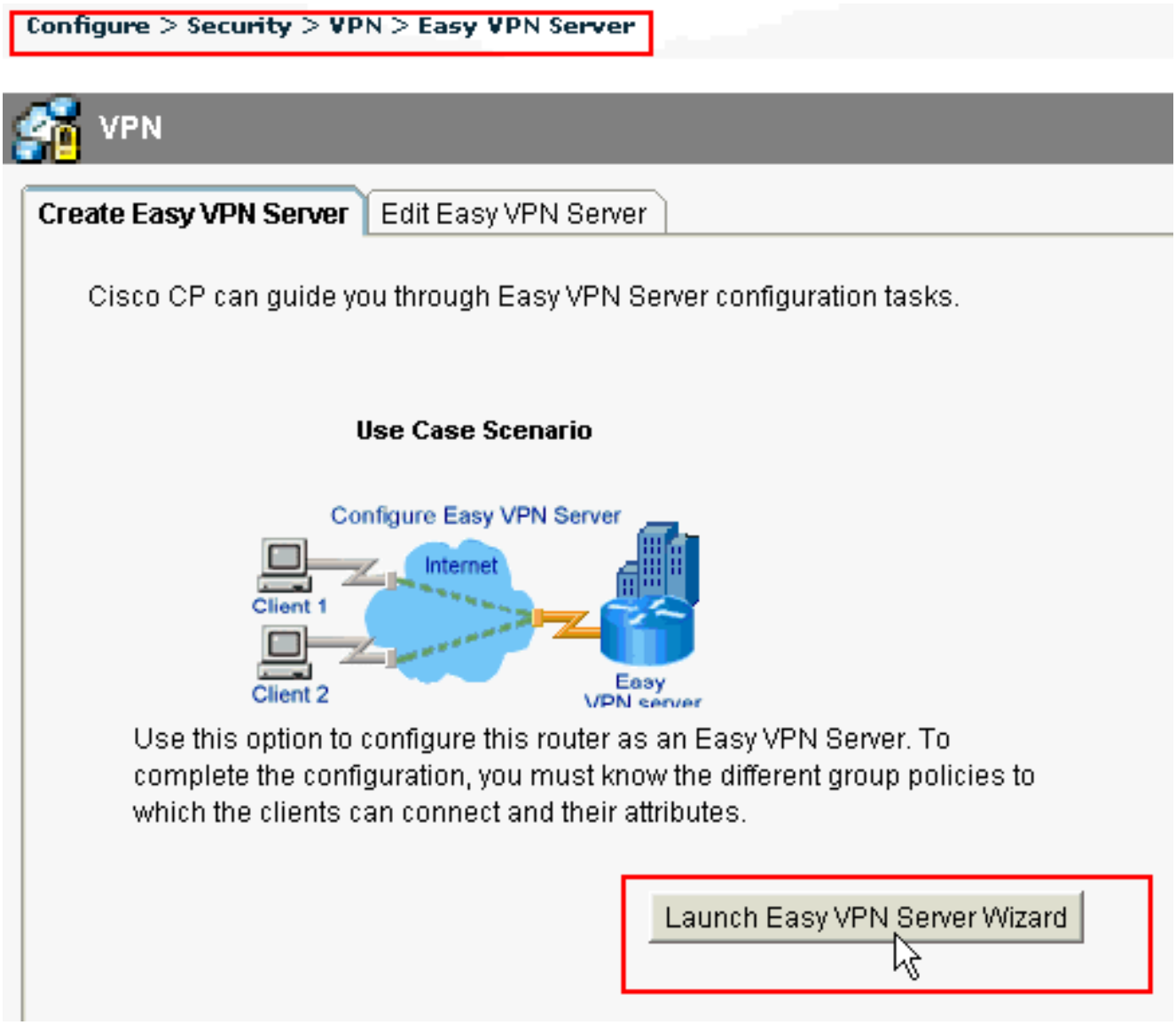



**Observação:** os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São endereços RFC 1918 que foram usados em um ambiente de laboratório.

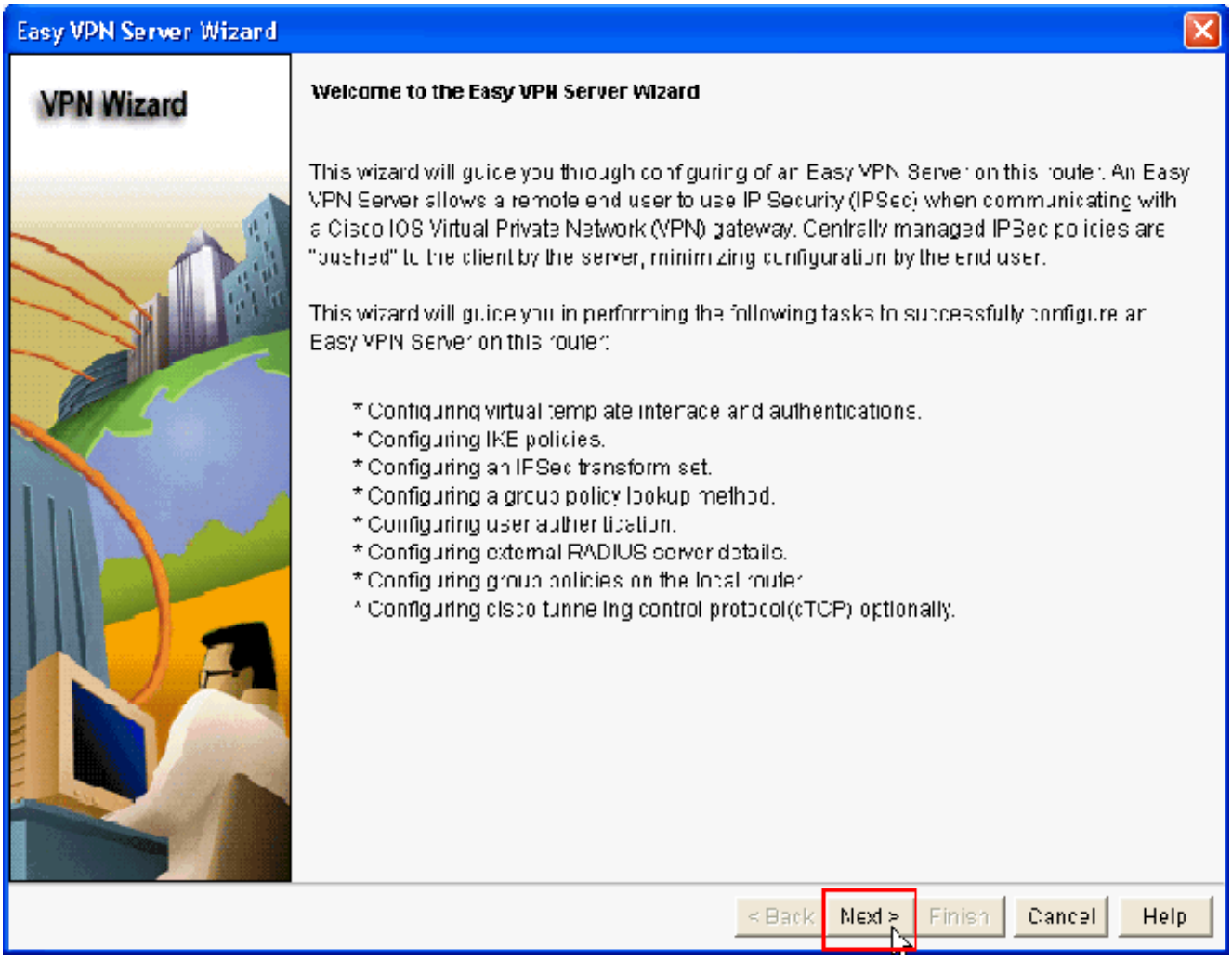
## Cisco CP - Configuração fácil do servidor VPN

Execute estas etapas para configurar o roteador Cisco IOS como um Easy VPN Server:

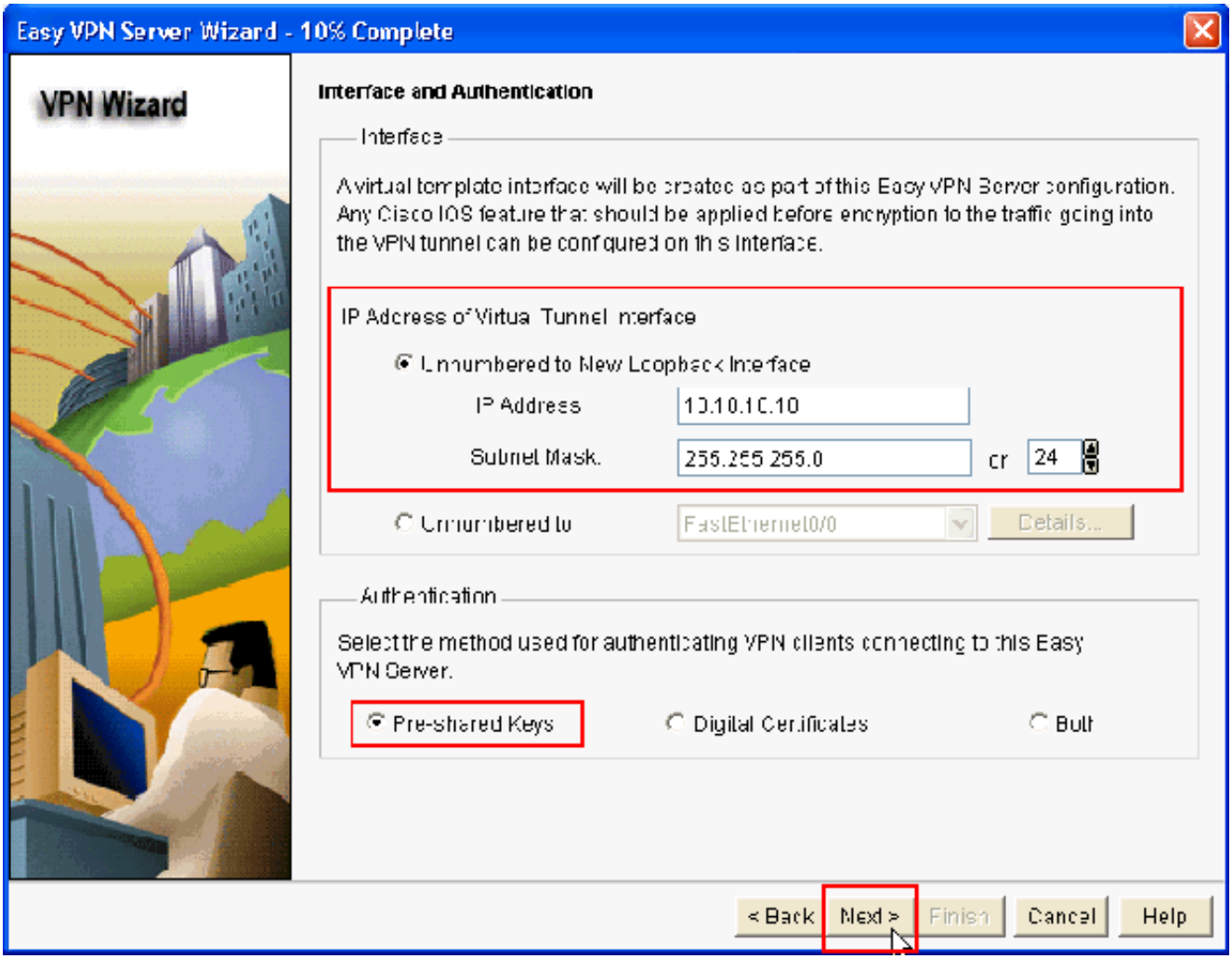
1. Escolha Configure > Security > VPN > **Easy VPN Server** > **Create Easy VPN Server** e clique em **Launch Easy VPN Server Wizard** para configurar o roteador Cisco IOS como um Easy VPN
   Server:



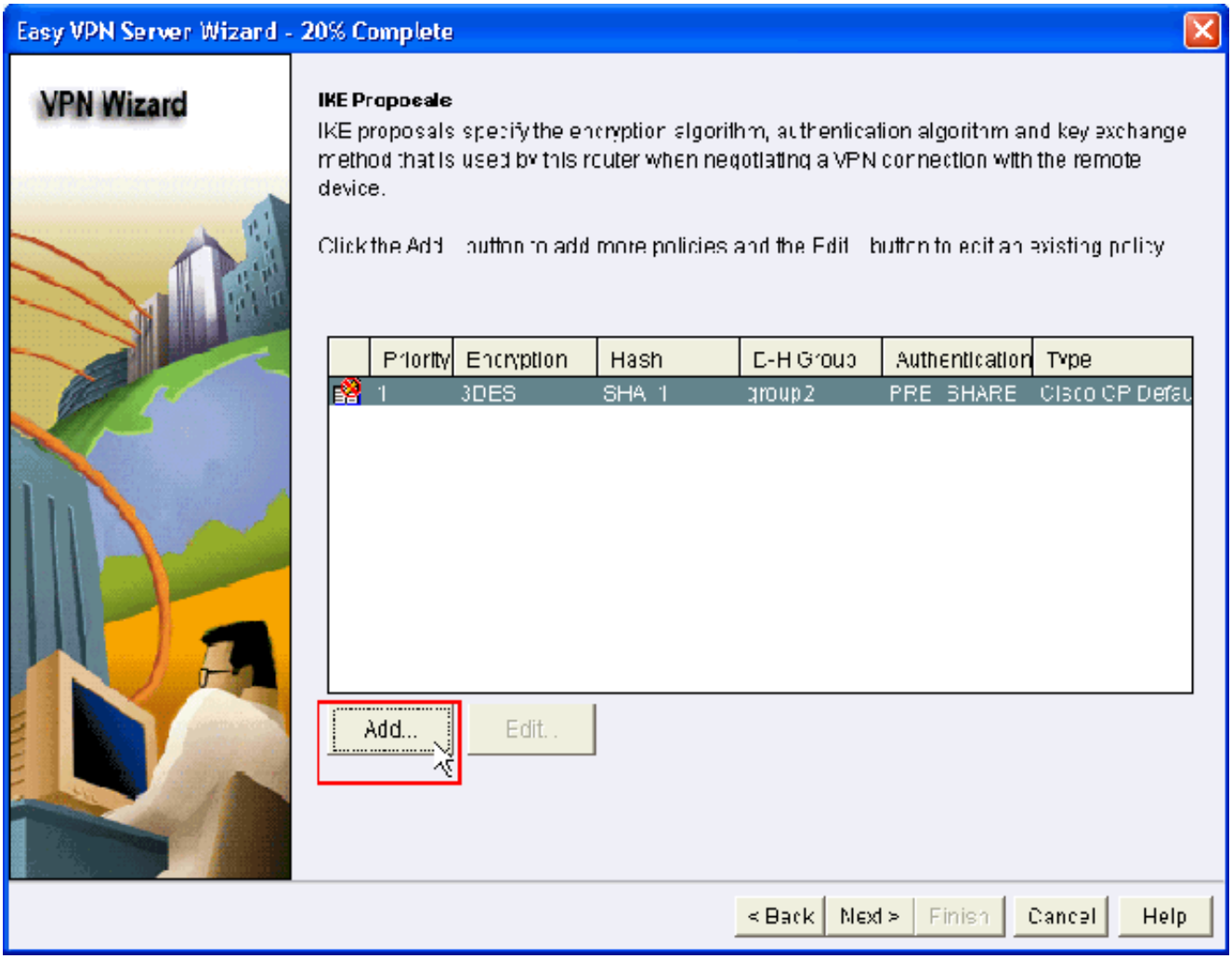
2. Clique em **Next** para continuar com a configuração **Easy VPN Server**.



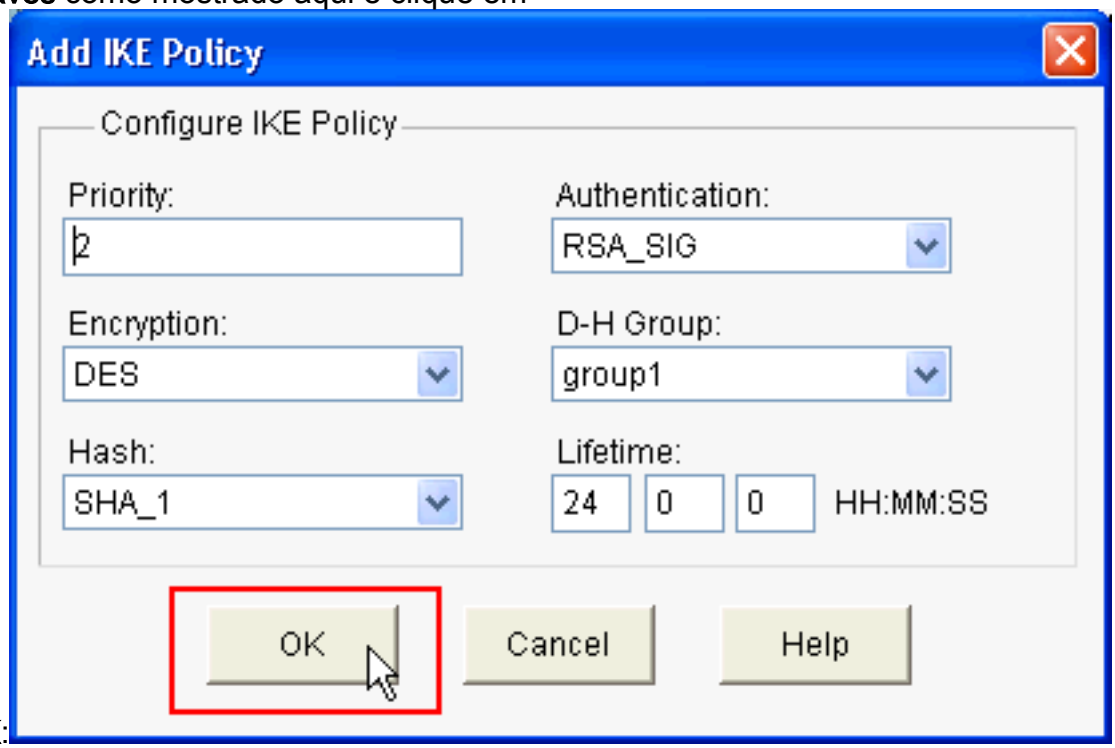

3. Na janela resultante, uma **Interface Virtual** será configurada como parte da configuração do Easy VPN Server. Forneça o **endereço IP da Virtual Tunnel Interface** e também escolha o **método de autenticação** usado para autenticar os clientes VPN. Aqui, **Pre-shared Keys** é o método de autenticação usado. Clique em Next:



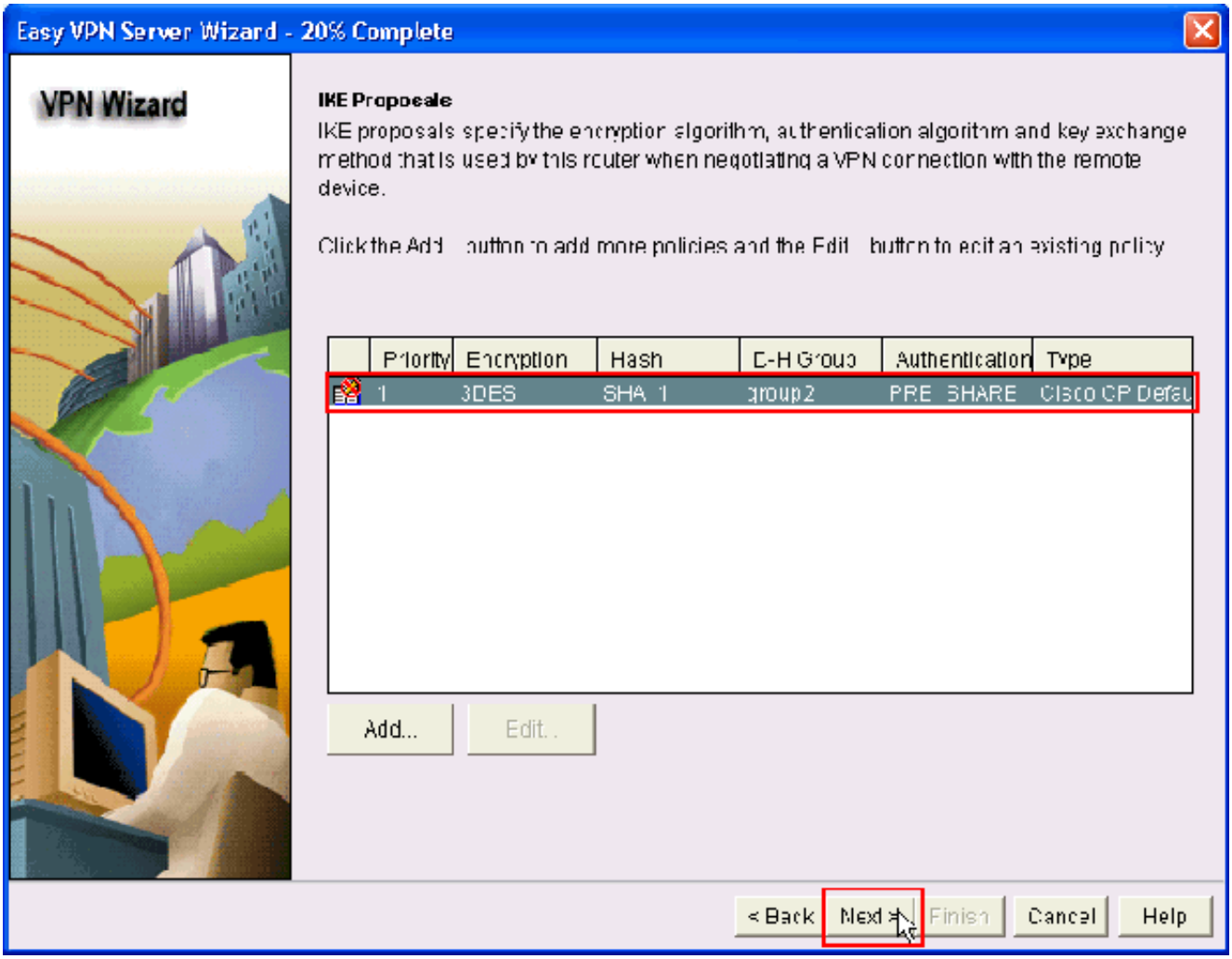

4. Especifique o **algoritmo de criptografia, o algoritmo de autenticação e o método de troca de chaves** a serem usados por este roteador ao negociar com o dispositivo remoto. Uma política IKE padrão está presente no roteador, que pode ser usada se necessário. Para adicionar uma nova política de IKE, clique em
Adicionar.



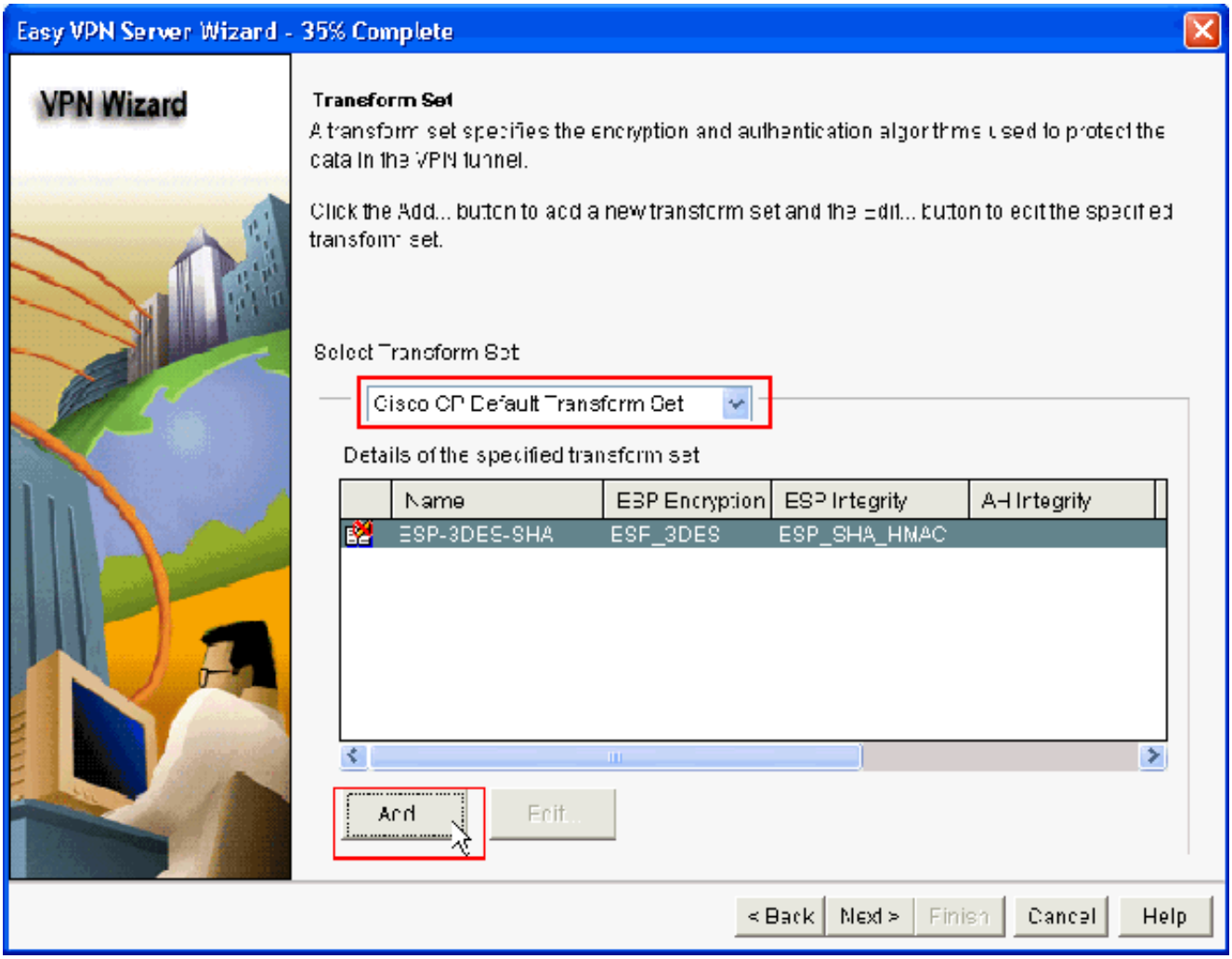

5. Forneça o **algoritmo de criptografia**, o **algoritmo de autenticação** e o **método de troca de chaves** como mostrado aqui e clique em **OK**:



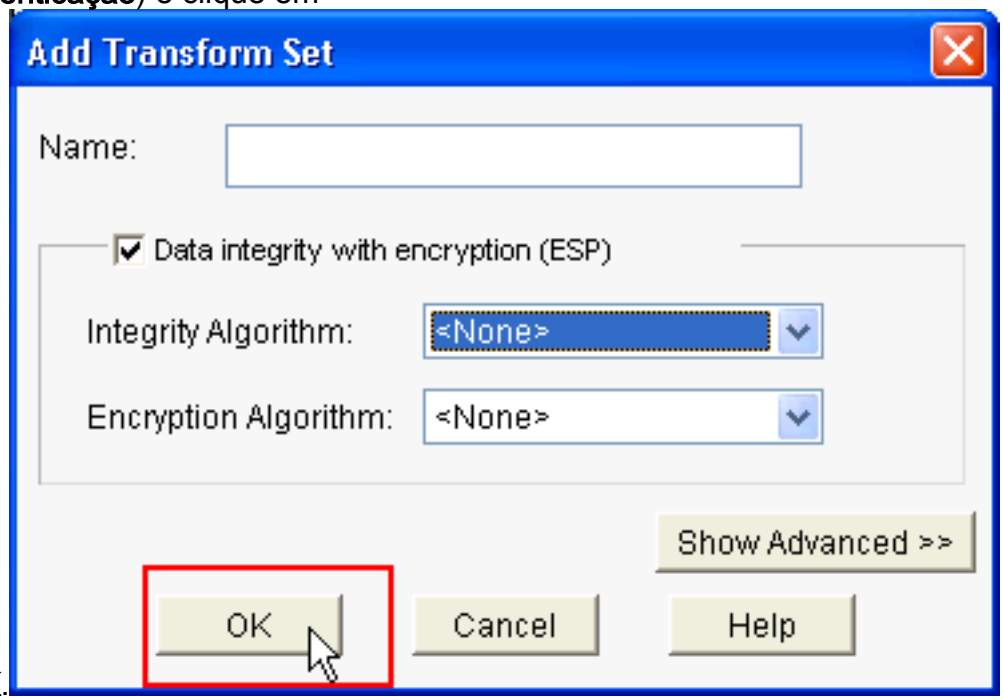

6. A **política IKE padrão** é usada neste exemplo. Como resultado, escolha a política IKE padrão e clique em **Avançar**.



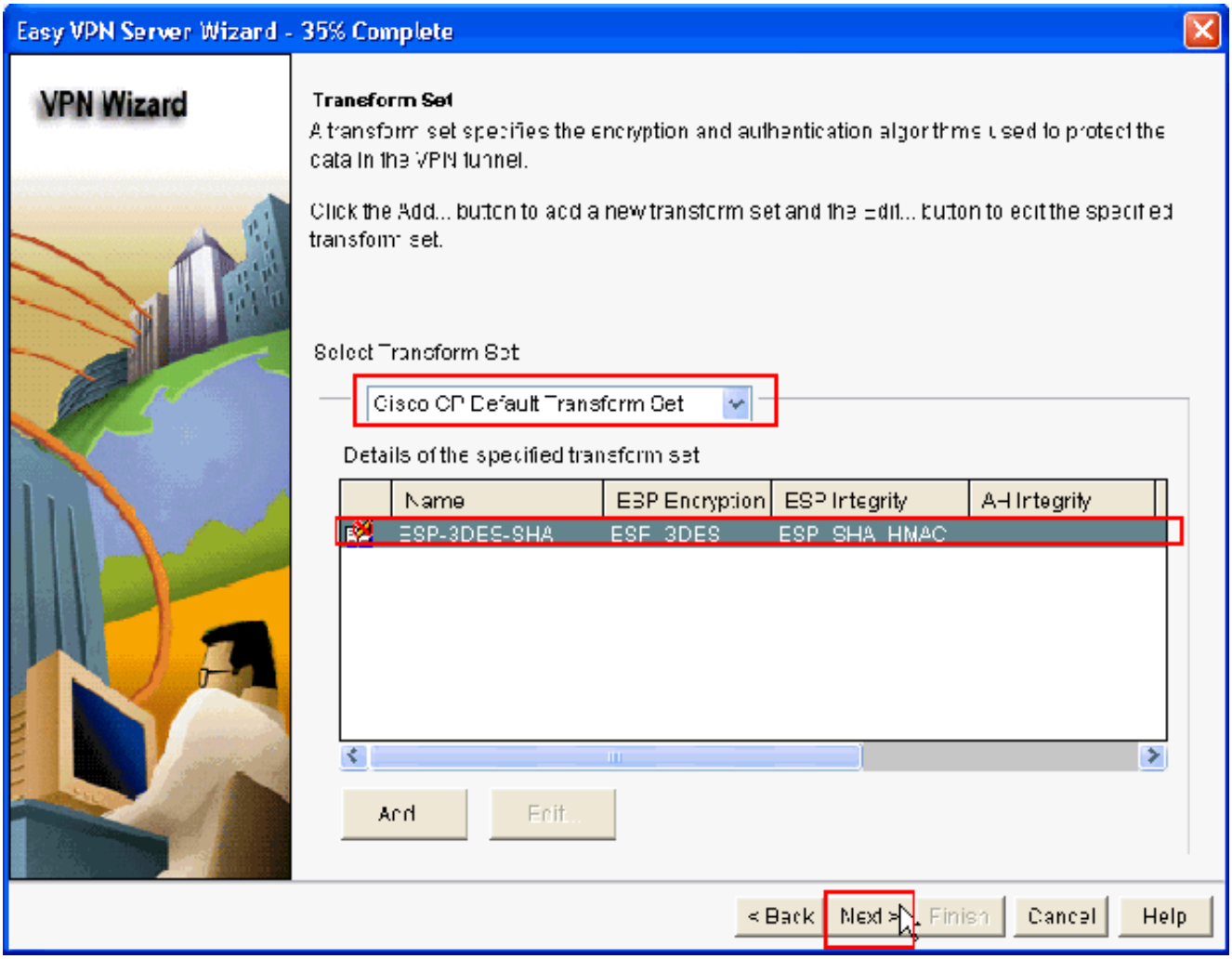

7. Na nova janela, os detalhes do **conjunto de transformações** devem ser fornecidos. O conjunto de transformação especifica os algoritmos **de criptografia** e **autenticação** usados para proteger **dados em túnel VPN**. Clique em **Adicionar** para fornecer estes detalhes. Você pode adicionar qualquer número de Conjuntos de transformação conforme necessário quando clicar em **Adicionar** e fornecer os detalhes.**Observação: CP Default Transform Set** está presente por padrão no roteador quando configurado usando o **Cisco CP**.



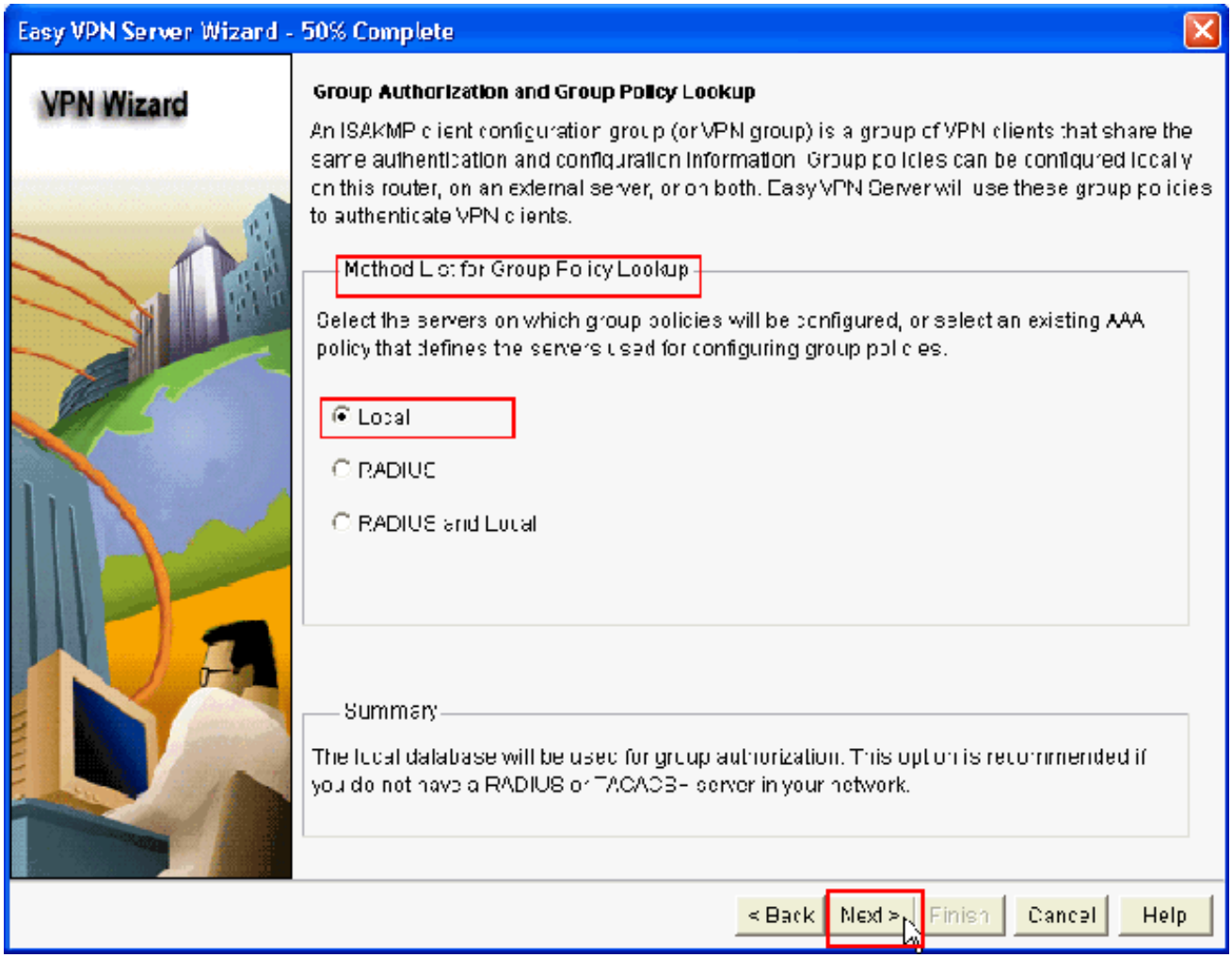

8. Forneça os detalhes **do conjunto de transformações** (**algoritmo de criptografia e autenticação**) e clique em **OK**.



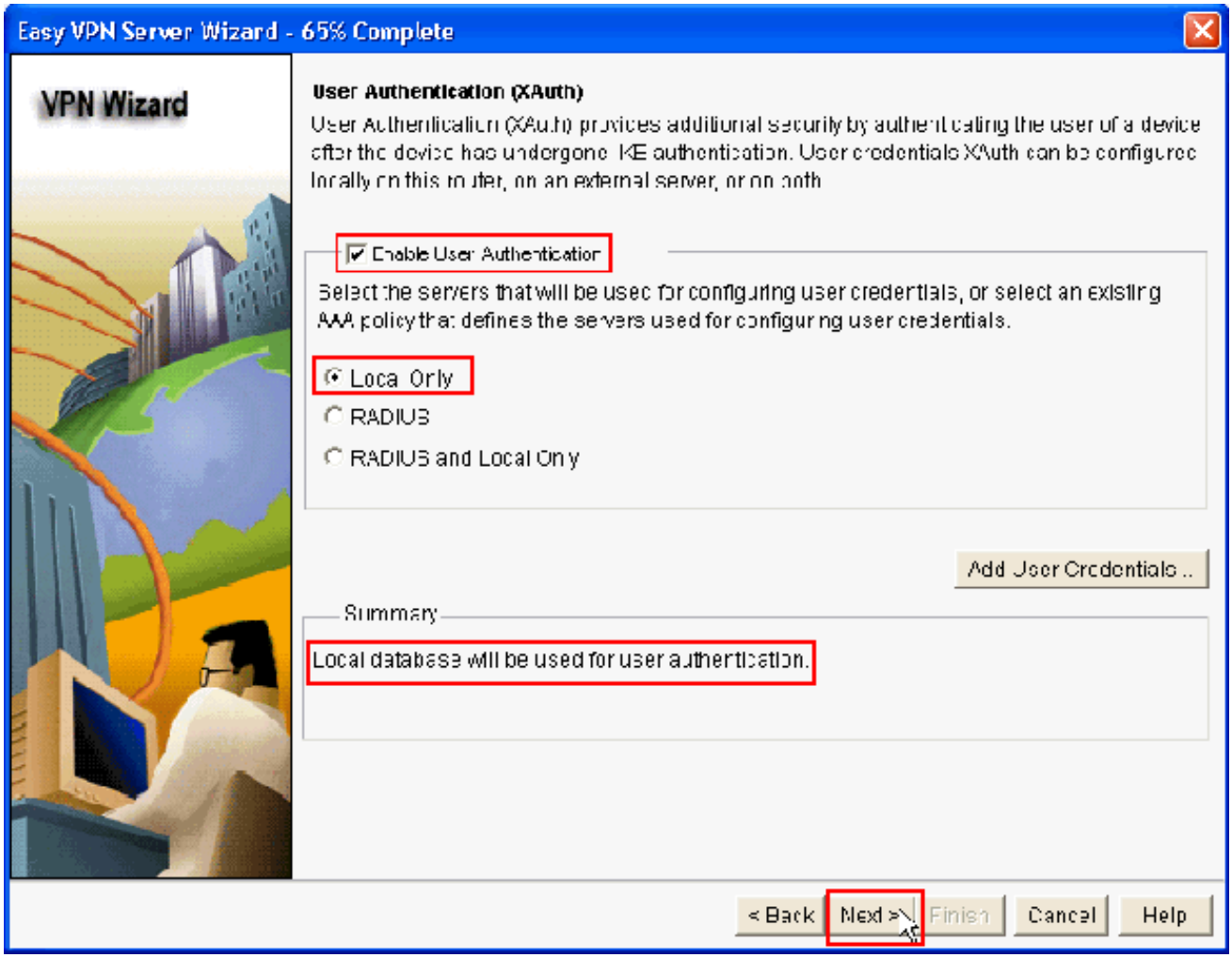

9. O **conjunto de transformações padrão** chamado **CP Default Transform Set** é usado neste exemplo. Como resultado, escolha o conjunto de transformações padrão e clique em **Avançar**.



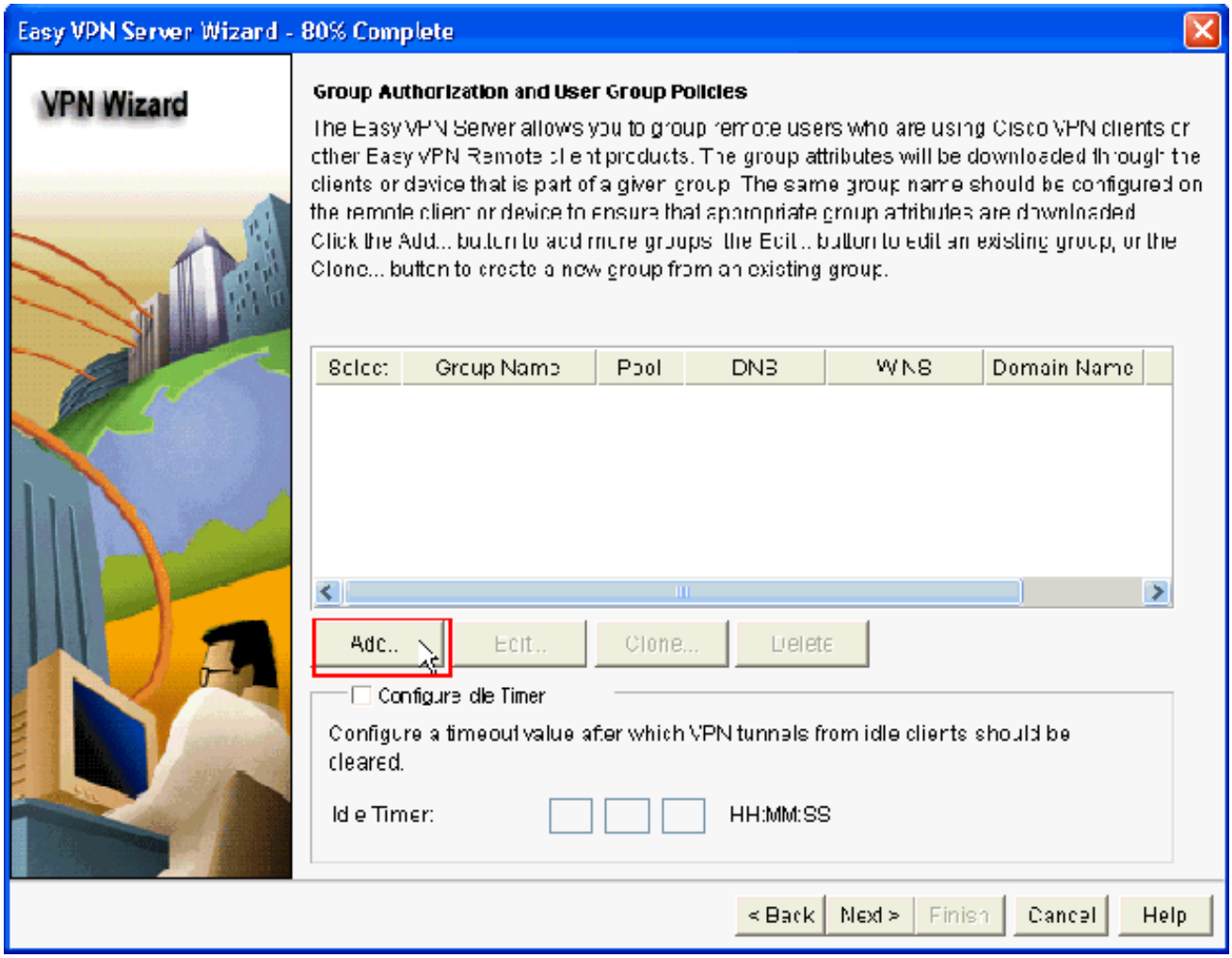

10. Na nova janela, escolha o servidor no qual as políticas de grupo serão configuradas, que pode ser **Local** ou **RADIUS** ou **Local e RADIUS**. Neste exemplo, usamos o **servidor local** para configurar políticas de grupo. Escolha **Local** e clique em **Avançar**.



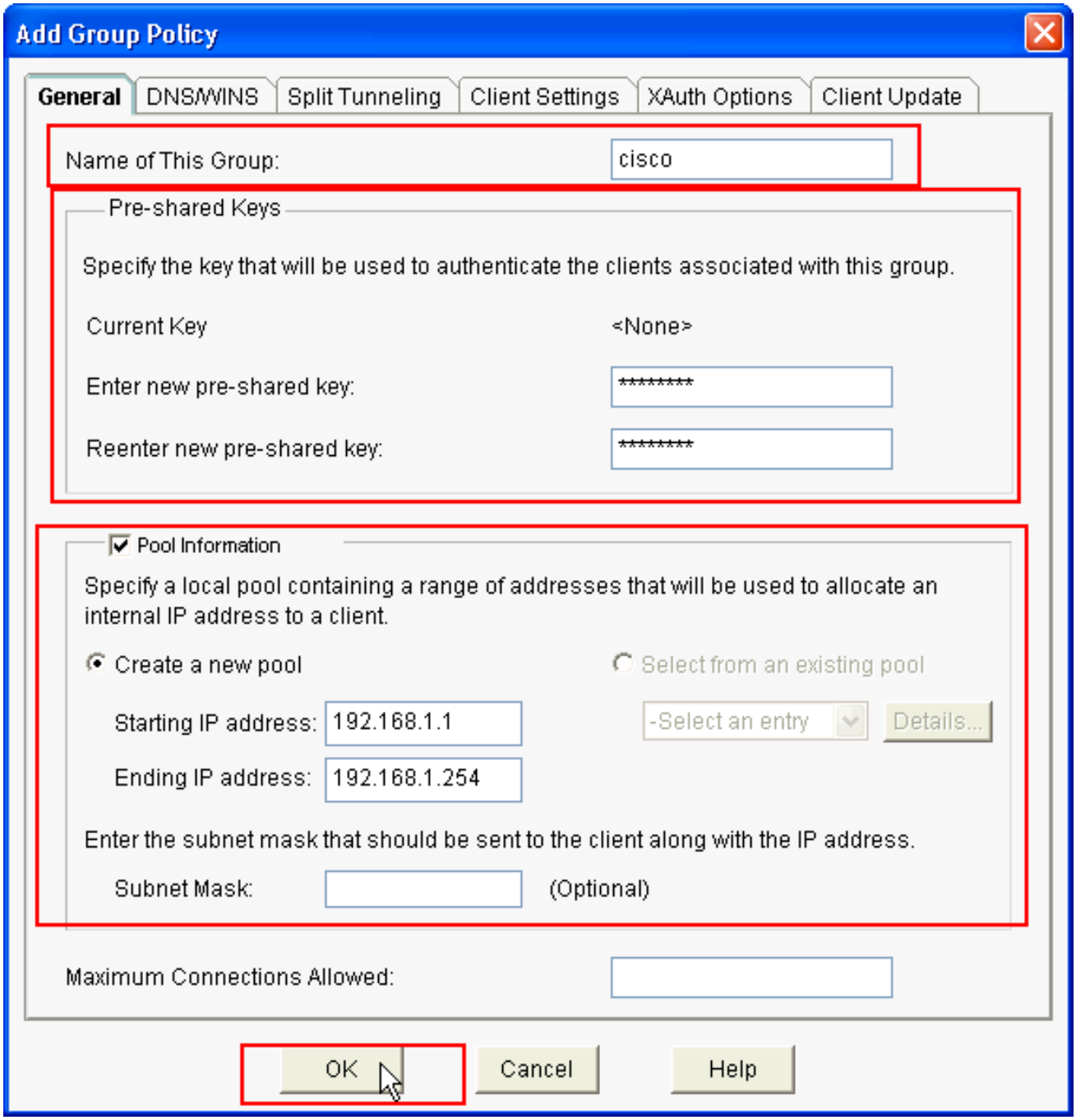

11. Escolha o servidor a ser usado para Autenticação de usuário nesta nova janela que pode ser **Somente local** ou **RADIUS** ou **Somente local e RADIUS**. Neste exemplo, usamos o **servidor local** para configurar as credenciais do usuário para autenticação. Verifique se a caixa de seleção ao lado de **Enable User Authentication** está marcada. Escolha **Somente local** e clique em
**Avançar**.



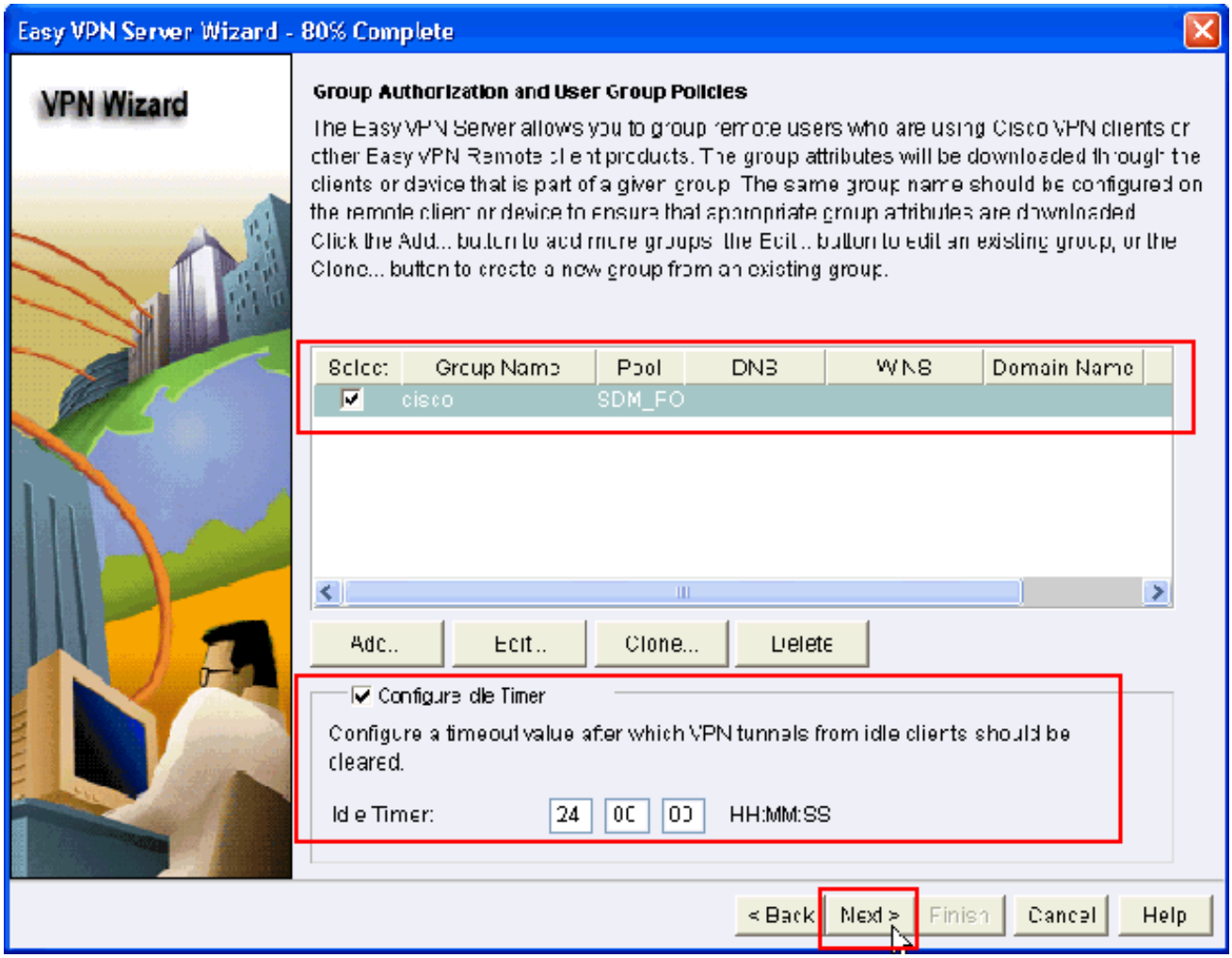

12. Clique em **Adicionar** para criar uma nova política de grupo e adicionar os usuários remotos neste
grupo.



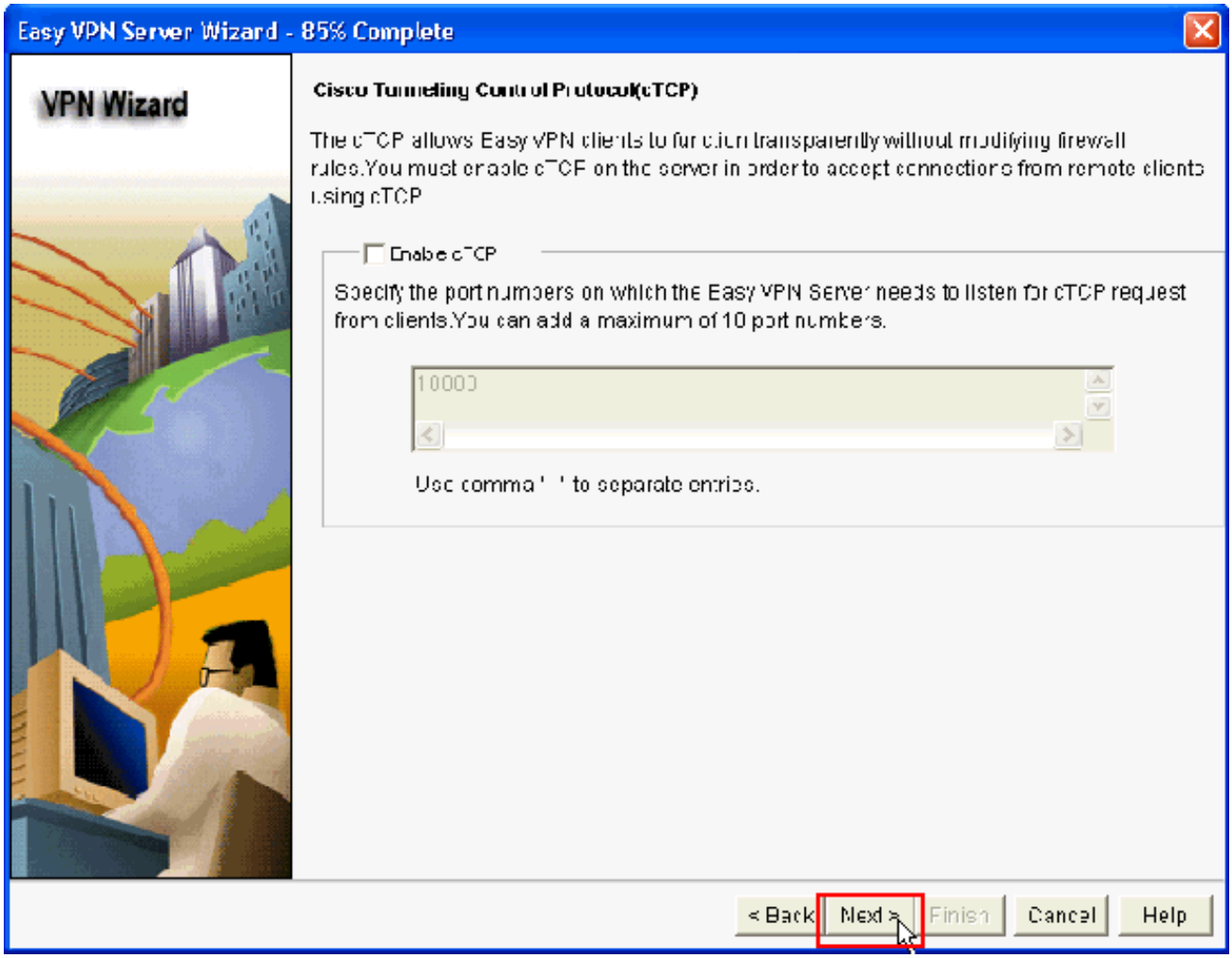

13. Na janela Adicionar política de grupo, forneça o nome do grupo no espaço fornecido para o Nome deste grupo (cisco neste exemplo) junto com a chave pré-compartilhada, e as informações do Pool IP (o endereço IP inicial e o endereço IP final), como mostrado, e clique em **OK**.**Observação:** você pode criar um novo pool de IPs ou usar um pool de IPs existente, se
houver.



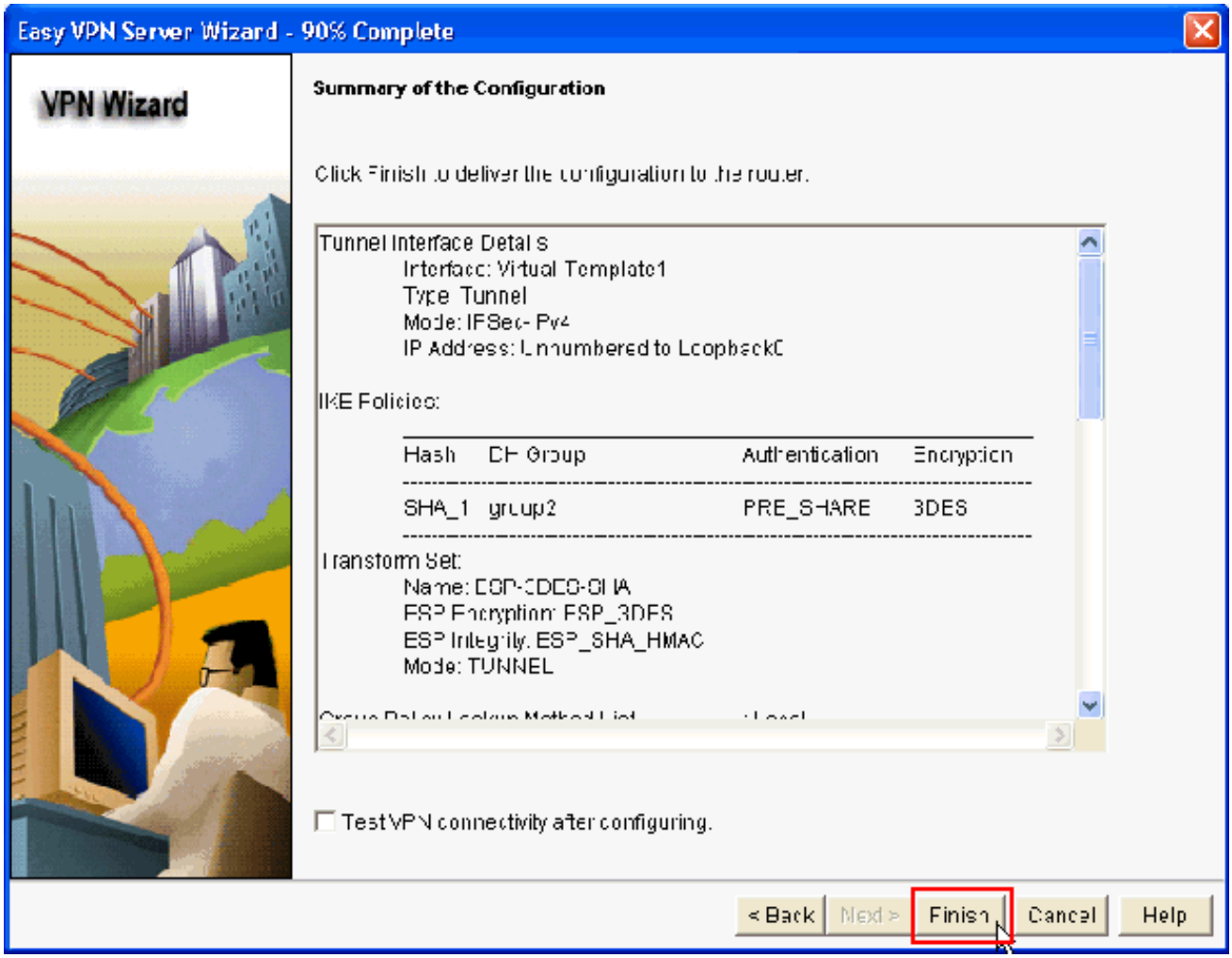

14. Agora escolha a nova **Política de Grupo** criada com o nome **cisco** e clique na caixa de seleção ao lado de **Configurar temporizador de ociosidade** conforme necessário para configurar o **temporizador de ociosidade**. Clique em Next.



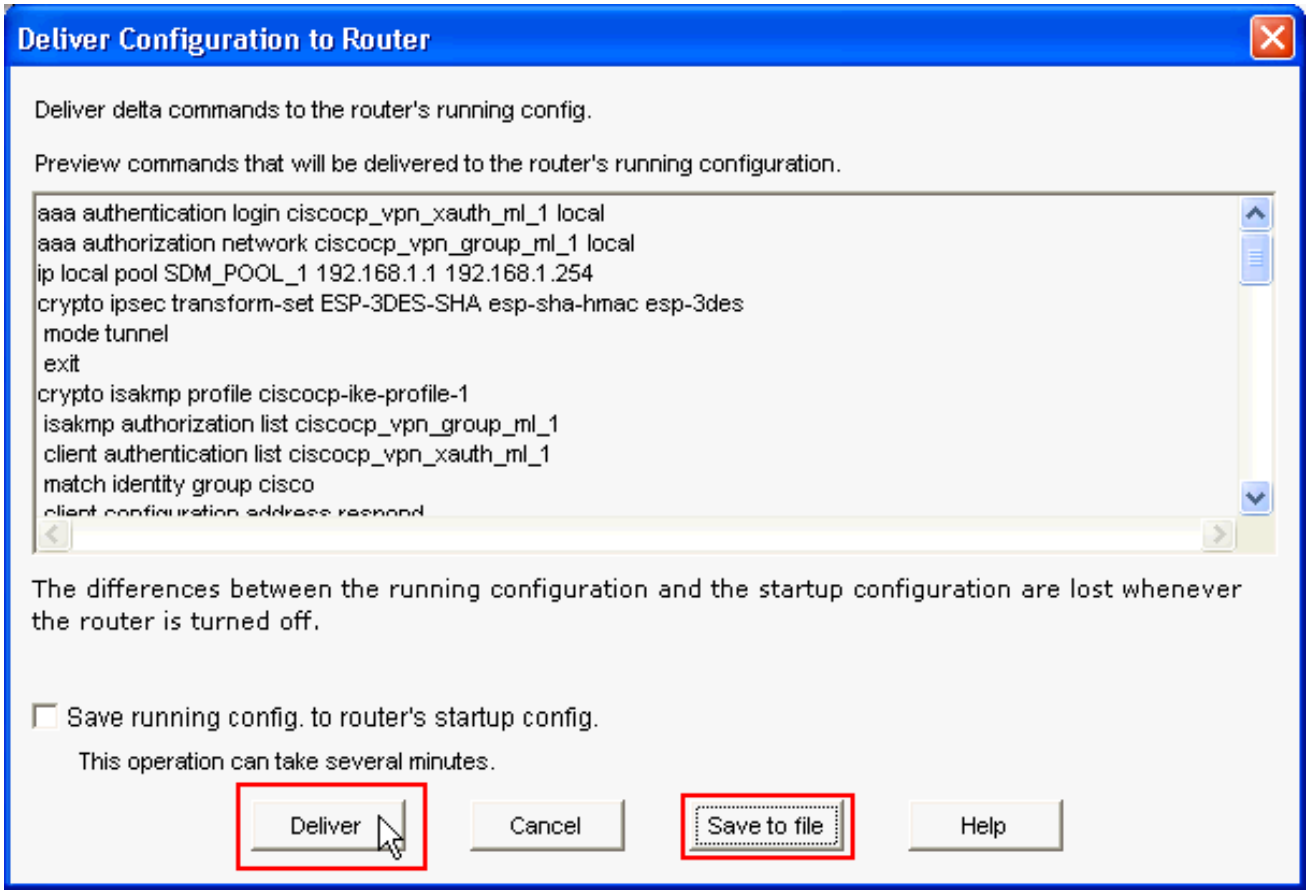

15. Ative o **Cisco Tunneling Control Protocol** (cTCP), se necessário. Caso contrário, clique em **Avançar**.



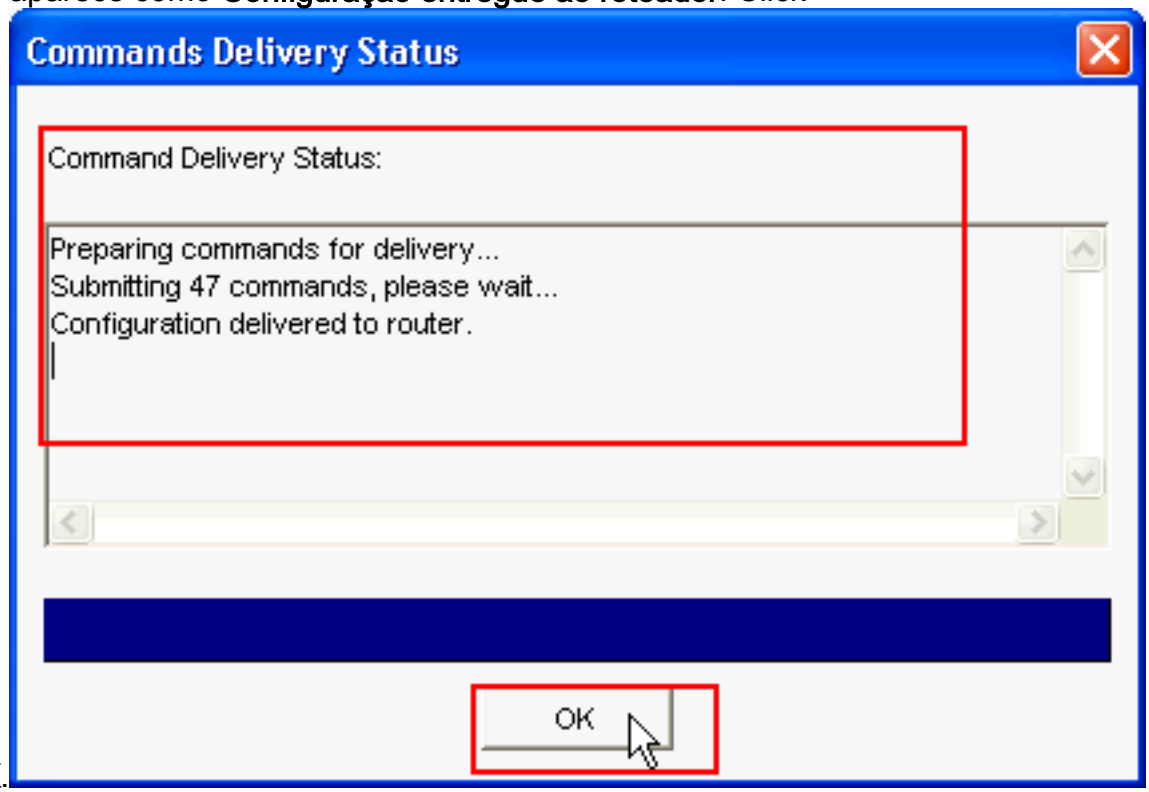

16. Revise o **Resumo da configuração**. Clique em Finish.



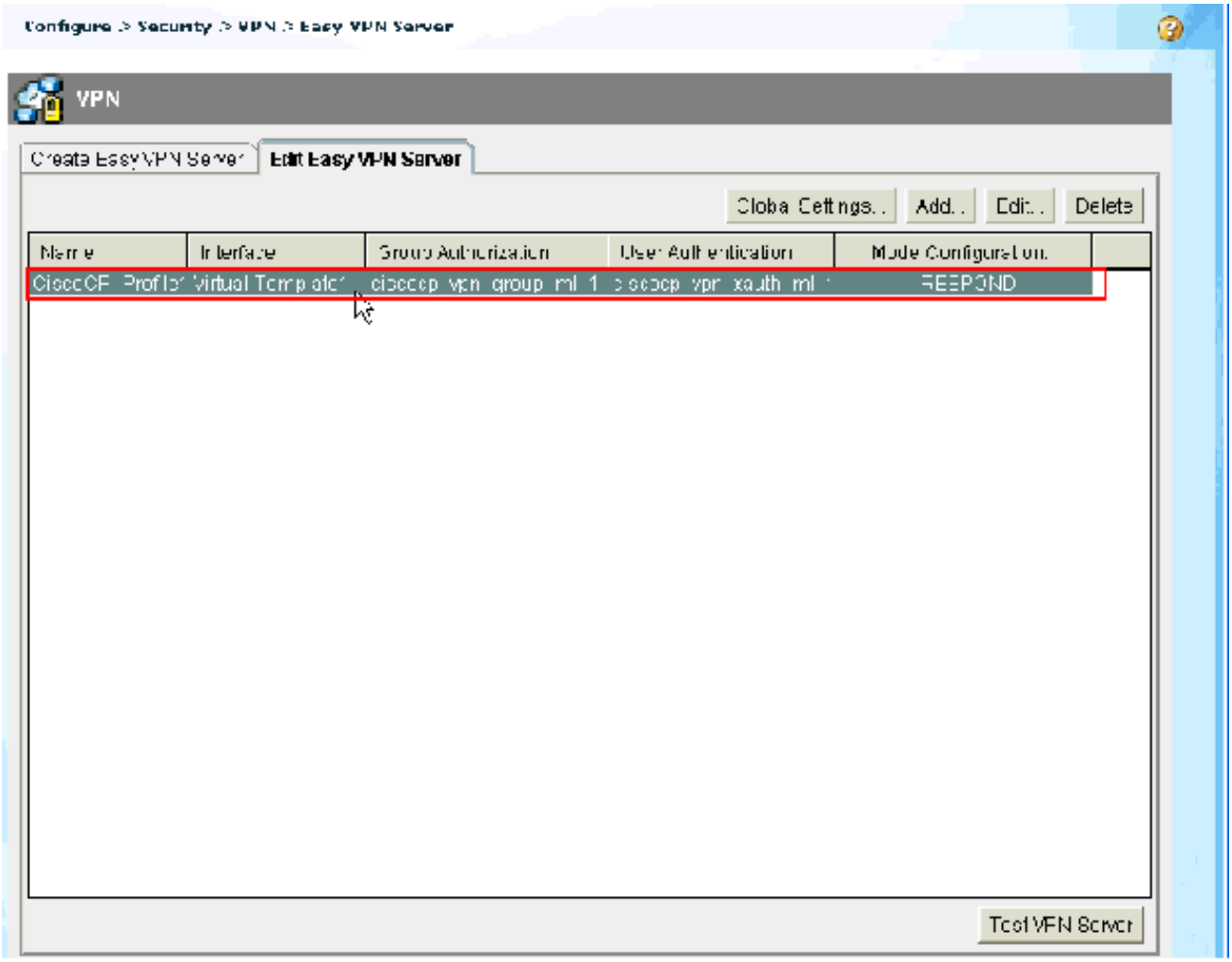

17. Na janela **Deliver Configuration to Router**, clique em **Deliver** para fornecer a configuração ao roteador. Você pode clicar em **Salvar em arquivo** para salvar a configuração como um arquivo no
PC.




18. A janela **Command Delivery Status** mostra o status de entrega dos comandos ao roteador. Ele aparece como **Configuração entregue ao roteador**. Click **OK**.




19. Você pode ver o Easy VPN Server recém-criado. Você pode editar o servidor existente escolhendo **Editar Easy VPN Server**. Isso conclui a configuração do Easy VPN Server no Cisco IOS
Router.




## Configuração de CLI

### Configuração do roteador

```
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
```

# Verificar

## Easy VPN Server - Comandos show

Use esta seção para confirmar se a sua configuração funciona corretamente.

- **show crypto isakmp sa** — Mostra todas as SAs IKE atuais em um peer.

```
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** — Mostra todas as SAs IPsec atuais em um peer.

```
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
```

# Troubleshoot

A Output Interpreter Tool ( somente clientes registrados) (OIT) oferece suporte a determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

**Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar os comandos debug.**

# Informações Relacionadas

- Negociação IPsec/Protocolos IKE
- Guia de início rápido do Cisco Configuration Professional (CCP)
- Página de suporte de produto da Cisco - Roteadores
- Suporte Técnico e Documentação - Cisco Systems