# Ejemplo de Configuración Profesional del Router IOS como Servidor Easy VPN Usando Configuración

## Contenido



# Introducción

Este documento describe cómo configurar un router Cisco IOS® como servidor Easy VPN (EzVPN) usando Cisco Configuration Professional (Cisco CP) y la CLI. La función Easy VPN Server permite a un usuario final remoto comunicarse mediante IP Security (IPsec) con cualquier gateway de Red privada virtual (VPN) de Cisco IOS. Las políticas IPSec administradas de manera centralizada se envían al dispositivo cliente mediante el servidor, lo que minimiza la configuración que debe realizar el usuario final.

Para obtener más información sobre Easy VPN Server, consulte la sección Easy VPN Server de la Biblioteca de la Guía de Configuración de Conectividad Segura, Cisco IOS Release 12.4T.

# Prerequisites

## Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

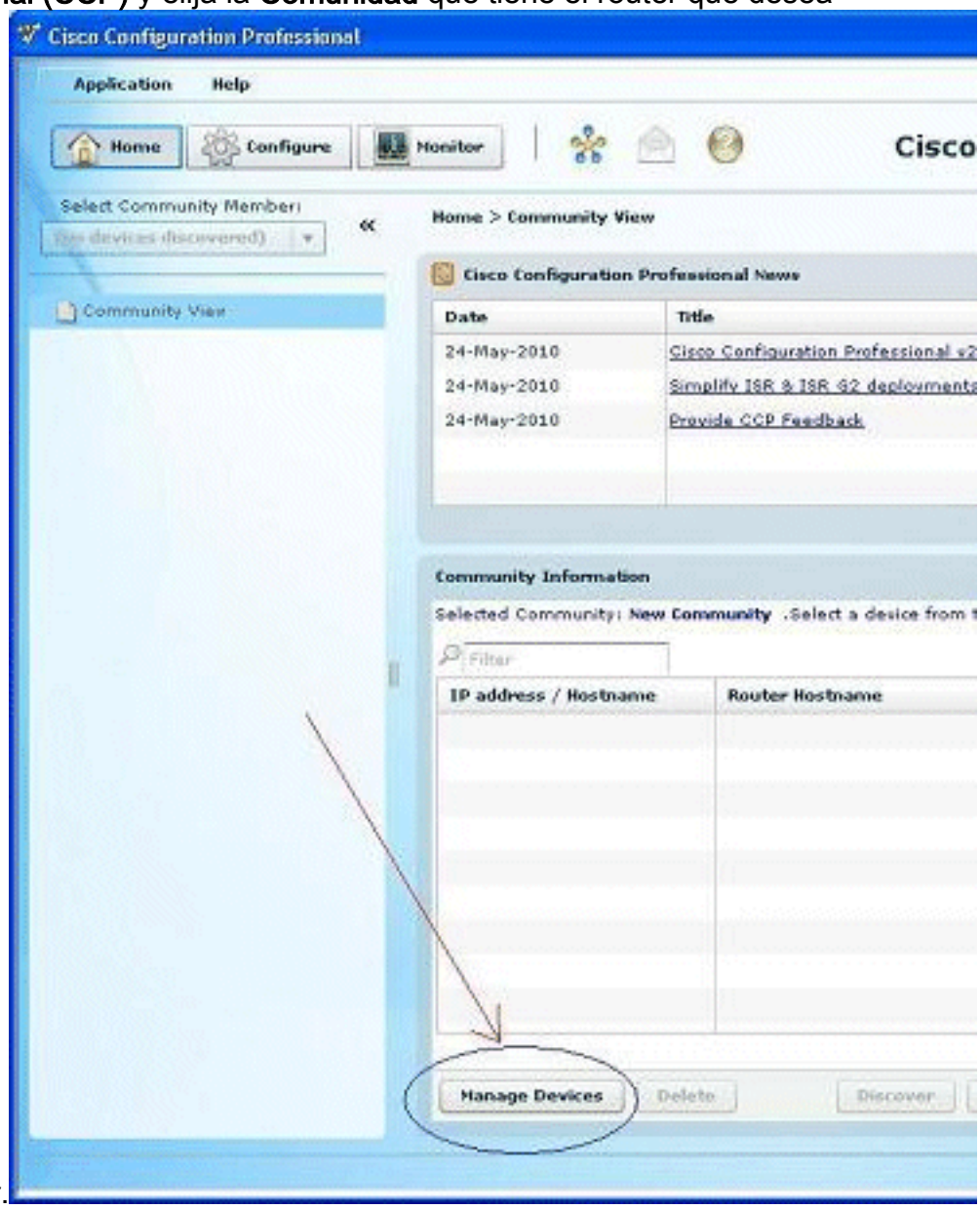
- Router Cisco 1841 con software Cisco IOS versión 12.4(15T)
- Cisco CP versión 2.1

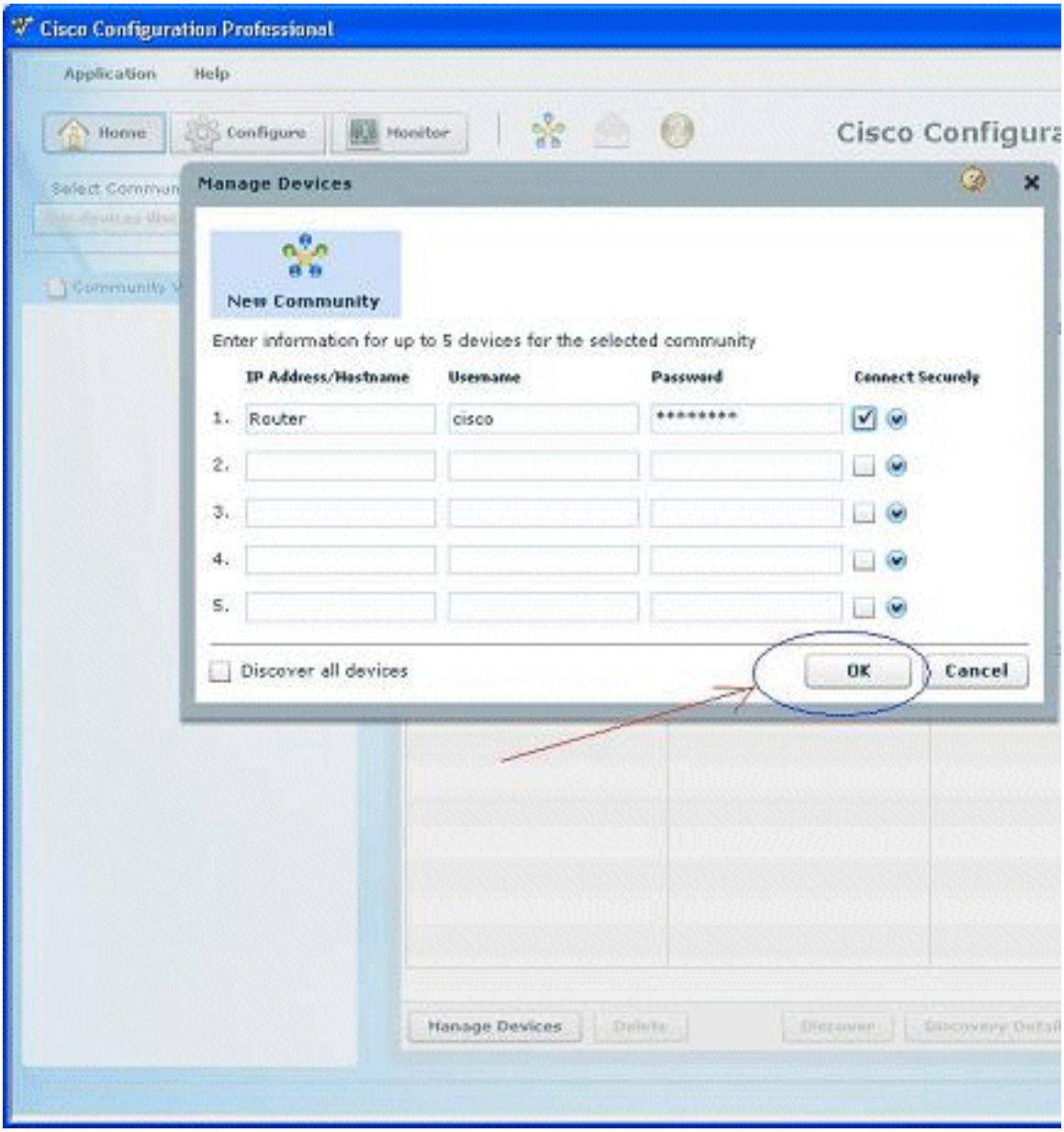
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Instalación de Cisco CP

Realice estos pasos para instalar Cisco CP:

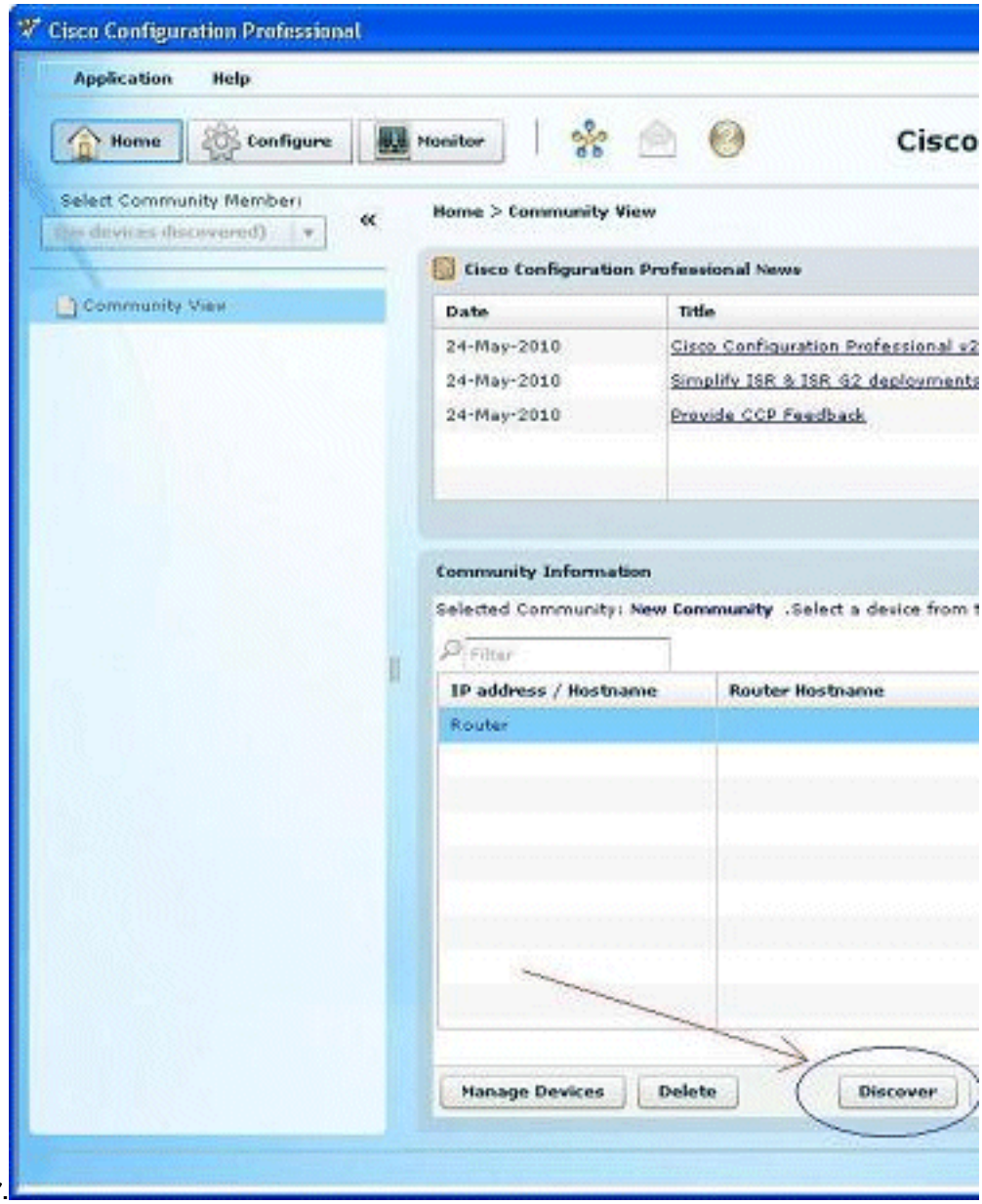
1. Descargue Cisco CP V2.1 desde el Cisco Software Center (sólo clientes registrados) e instálelo en su PC local.La última versión de Cisco CP se puede encontrar en el sitio web de Cisco CP.
2. Inicie Cisco CP desde su PC local a través de **Start > Programs > Cisco Configuration Professional (CCP)** y elija la **Comunidad** que tiene el router que desea configurar.






3. Para descubrir el dispositivo que desea configurar, resalte el router y haga clic en

Discover.




**Nota:** Para obtener información sobre los modelos de router de Cisco y las versiones de IOS compatibles con Cisco CP v2.1, consulte la sección Versiones compatibles con Cisco IOS.

**Nota:** Para obtener información sobre los requisitos de PC que ejecutan Cisco CP v2.1, consulte la sección Requisitos del sistema.

## Configuración del router para ejecutar Cisco CP

Realice estos pasos de configuración para ejecutar Cisco CP en un router de Cisco:

1. Conecte el router mediante Telnet, SSH o a través de la consola.Ingrese al modo de configuración global usando este comando:
   ```
   Router(config)#enable
   Router(config)#
   ```
2. Si HTTP y HTTPS están habilitados y configurados para utilizar números de puerto no estándar, puede omitir este paso y utilizar simplemente el número de puerto ya configurado.Habilite el router HTTP o el servidor HTTPS con estos comandos de software Cisco IOS:
   ```
   Router(config)# ip http server
   Router(config)# ip http secure-server
   Router(config)# ip http authentication local
   ```

3. Cree un usuario con el nivel de privilegio 15:
```
Router(config)# username privilege 15 password 0
```

   **Nota:** Reemplace *<username>* y *<password>* por el nombre de usuario y la contraseña que desea configurar.
4. Configure SSH y Telnet para el inicio de sesión local y el nivel de privilegio 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 el registro local para admitir la función de monitoreo de registro:
```
Router(config)# logging buffered 51200 warning
```

## Requirements

Este documento asume que el router Cisco está completamente operativo y configurado para permitir que Cisco CP realice cambios en la configuración.

Para obtener información completa sobre cómo empezar a utilizar Cisco CP, refiérase a Introducción a Cisco Configuration Professional.

## Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

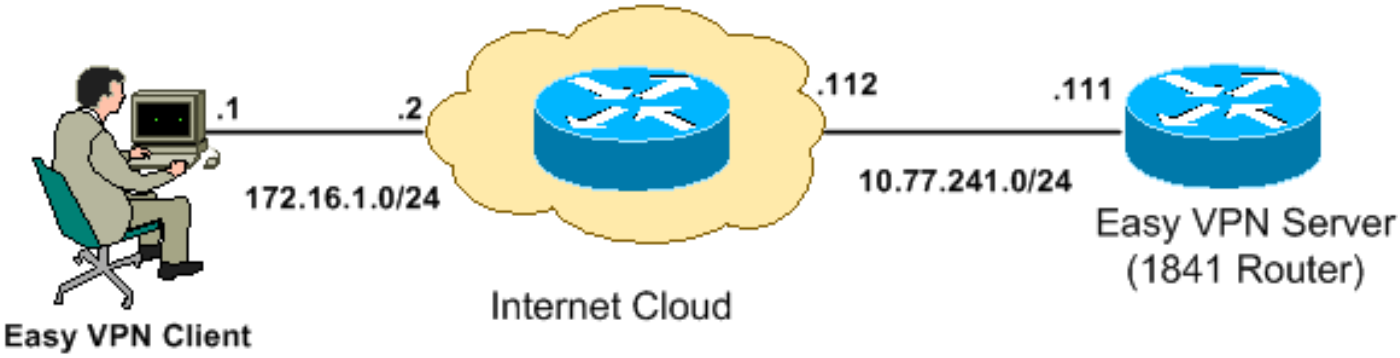
# Configurar

En esta sección se ofrece información para configurar las configuraciones básicas para un router en una red.

**Nota:** Utilice la herramienta Command Lookup (sólo para clientes **registrados) para obtener más información sobre los comandos utilizados en esta sección.**

## Diagrama de la red

En este documento, se utiliza esta configuración de red:

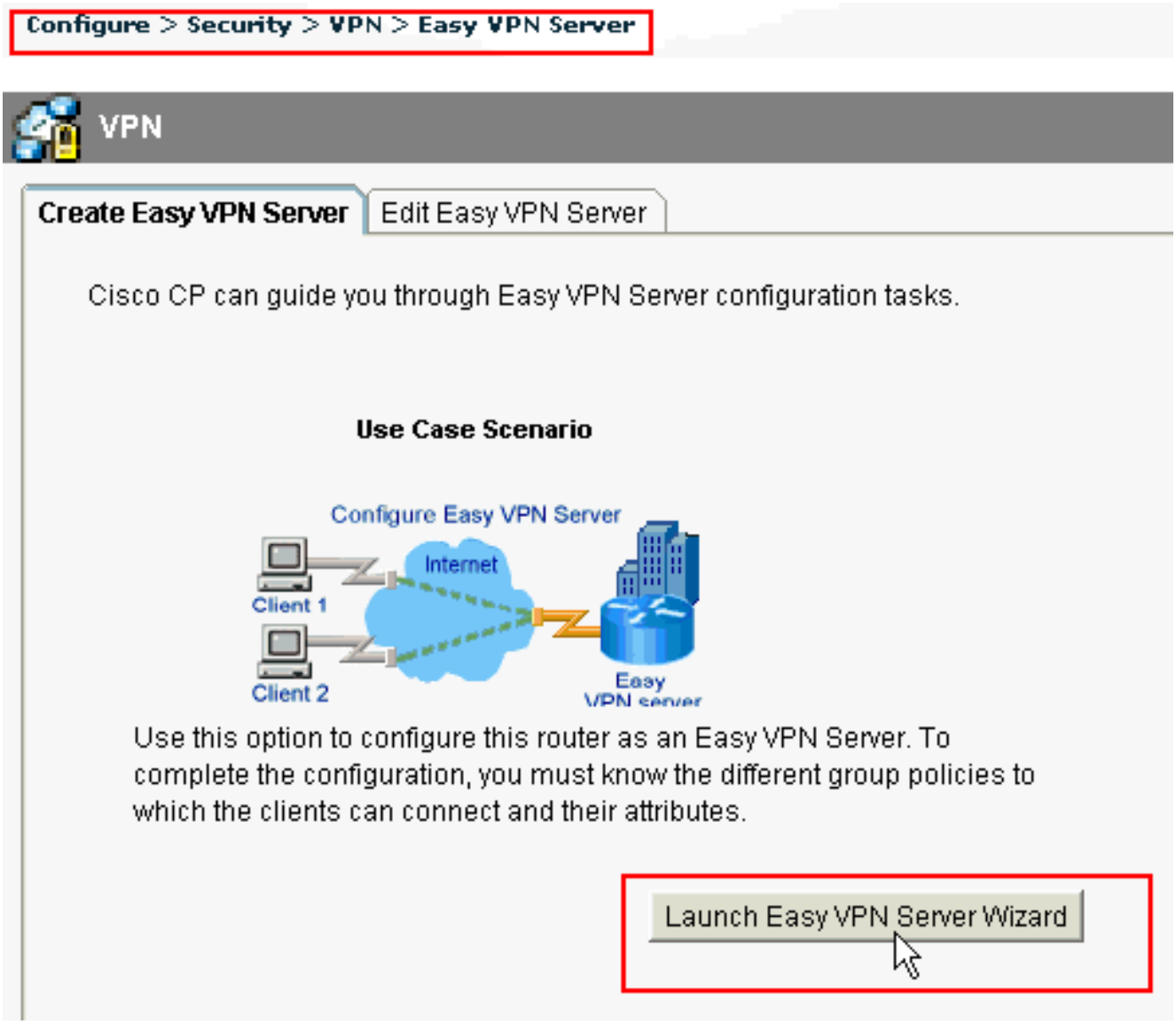



**Nota:** Los esquemas de direccionamiento IP utilizados en esta configuración no son legalmente enrutables en Internet. Son direcciones RFC 1918 que se han utilizado en un entorno de laboratorio.

## Cisco CP - Configuración del servidor Easy VPN

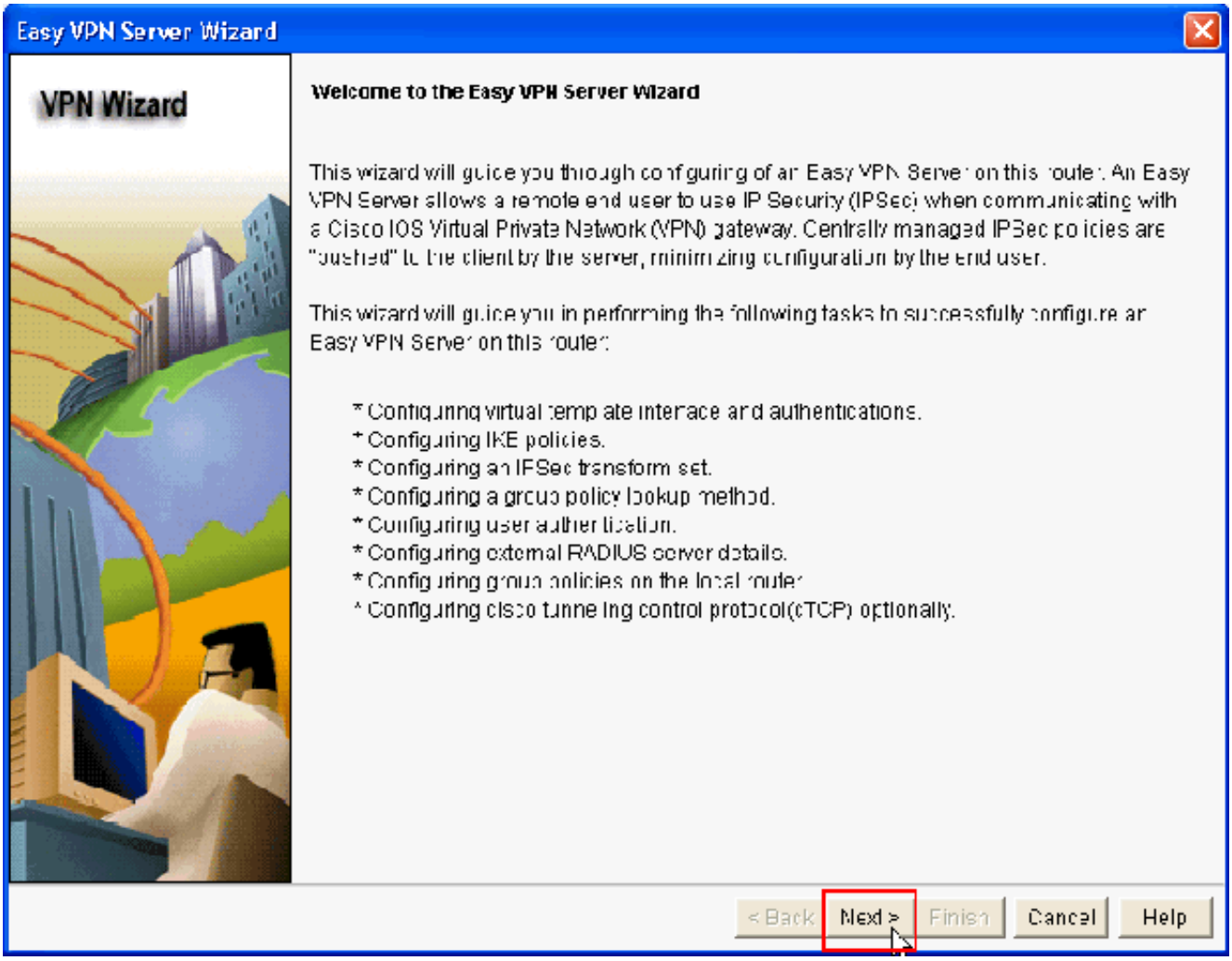
Realice estos pasos para configurar el router Cisco IOS como servidor Easy VPN:

1. Elija Configure > Security > VPN > **Easy VPN Server** > **Create Easy VPN Server** y haga clic en Launch Easy VPN Server Wizard para configurar el router Cisco IOS como un Easy VPN Server:

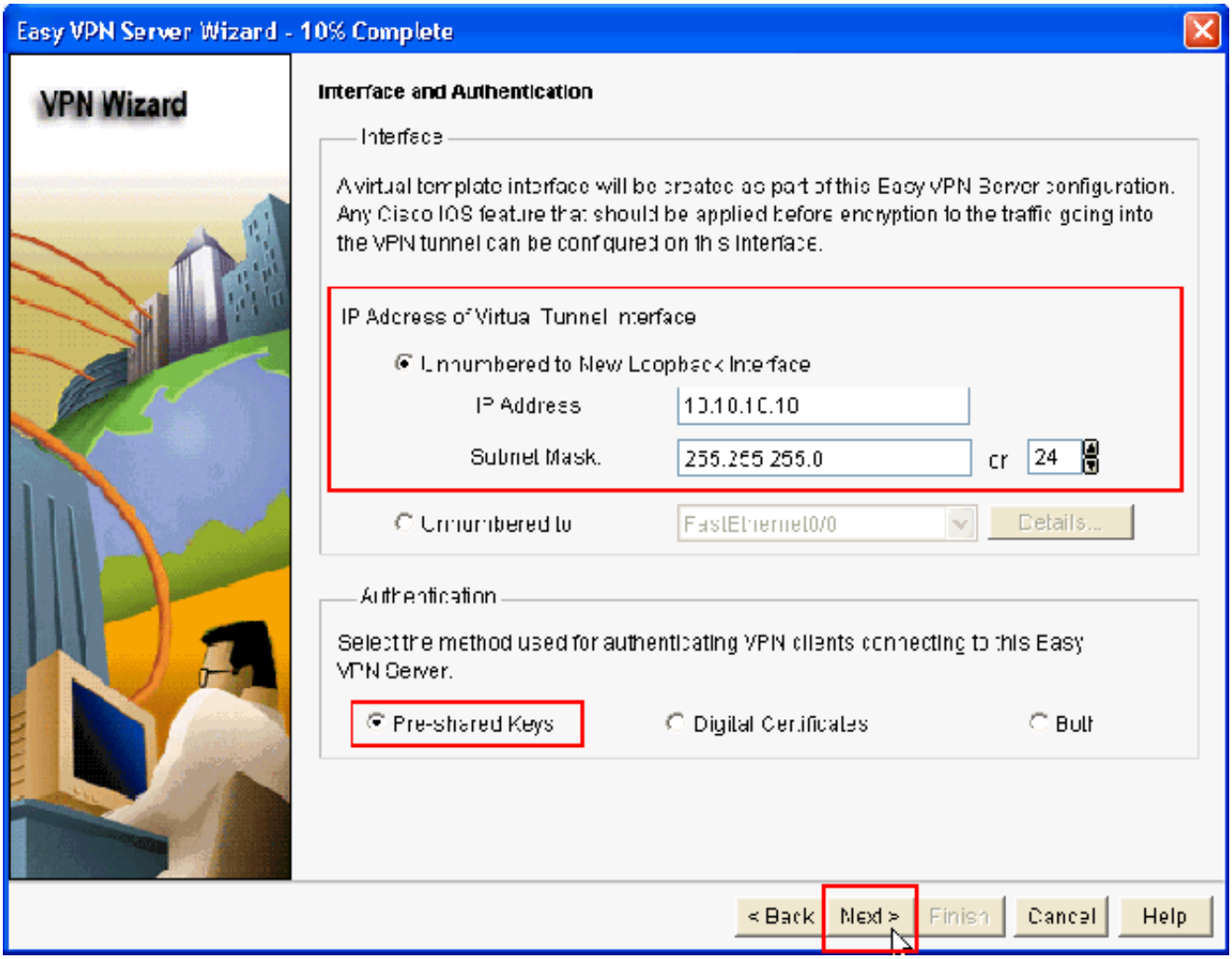



2. Haga clic en **Next** para continuar con la configuración de **Easy VPN**

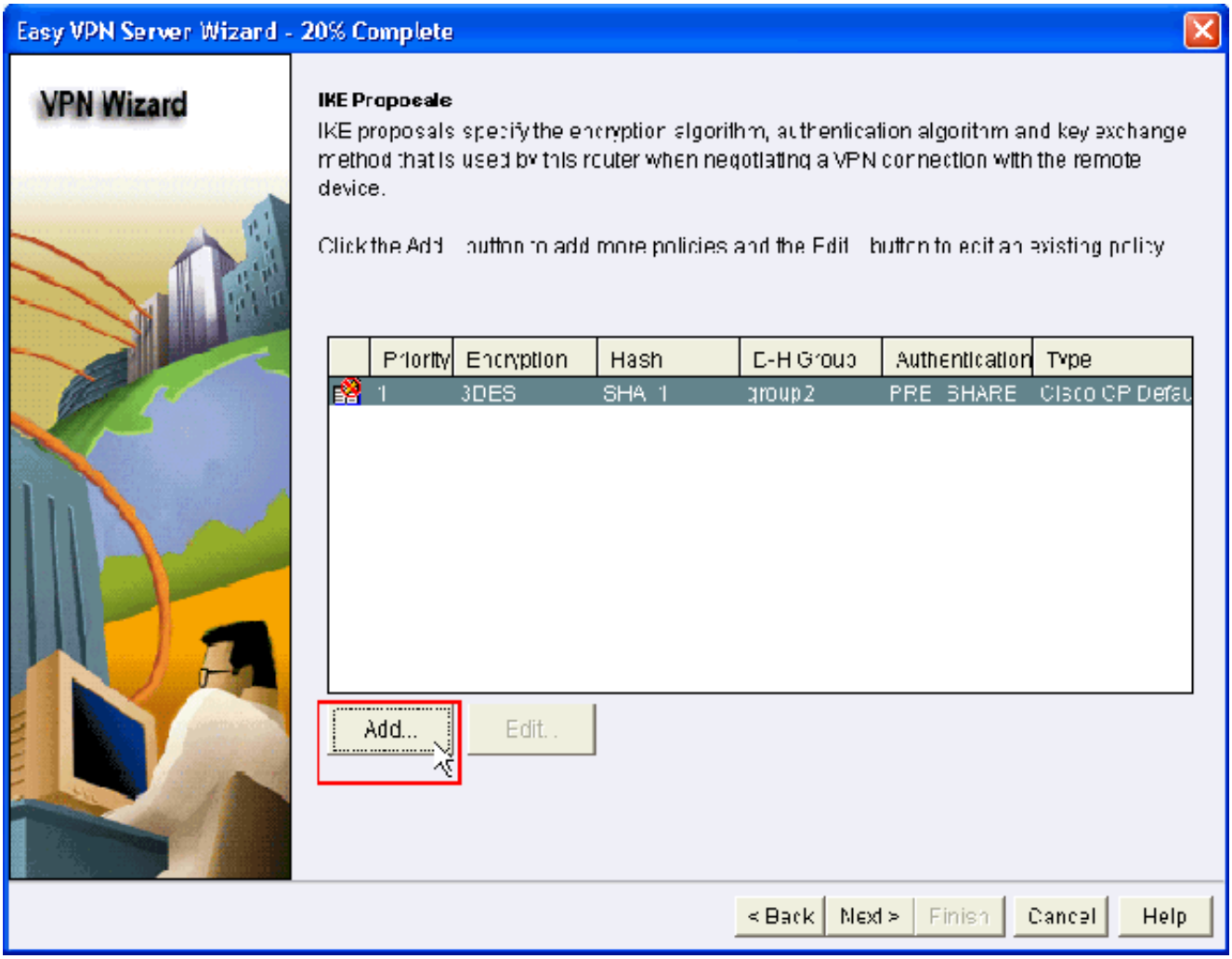
Server.



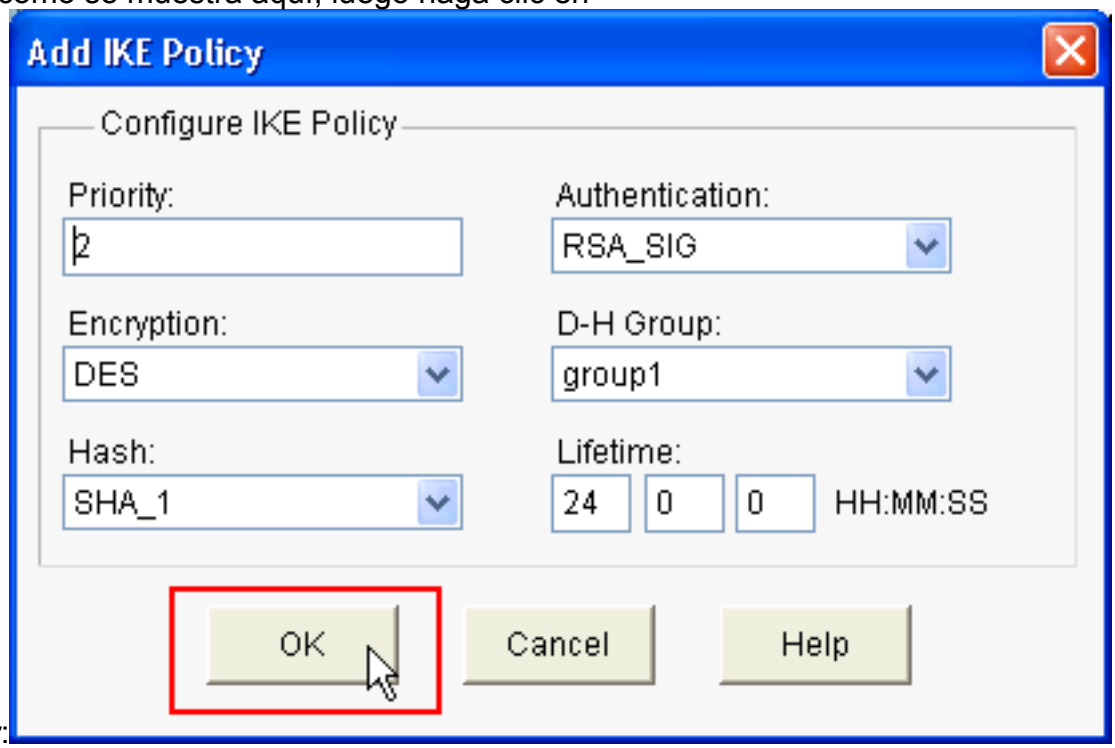

3. En la ventana resultante, una **interfaz virtual** se configurará como parte de la configuración del servidor Easy VPN. Proporcione la **dirección IP de la interfaz de túnel virtual** y también elija el **método de autenticación** utilizado para autenticar los clientes VPN. Aquí, **Pre-shared Keys** es el método de autenticación utilizado. Haga clic en Next (Siguiente):



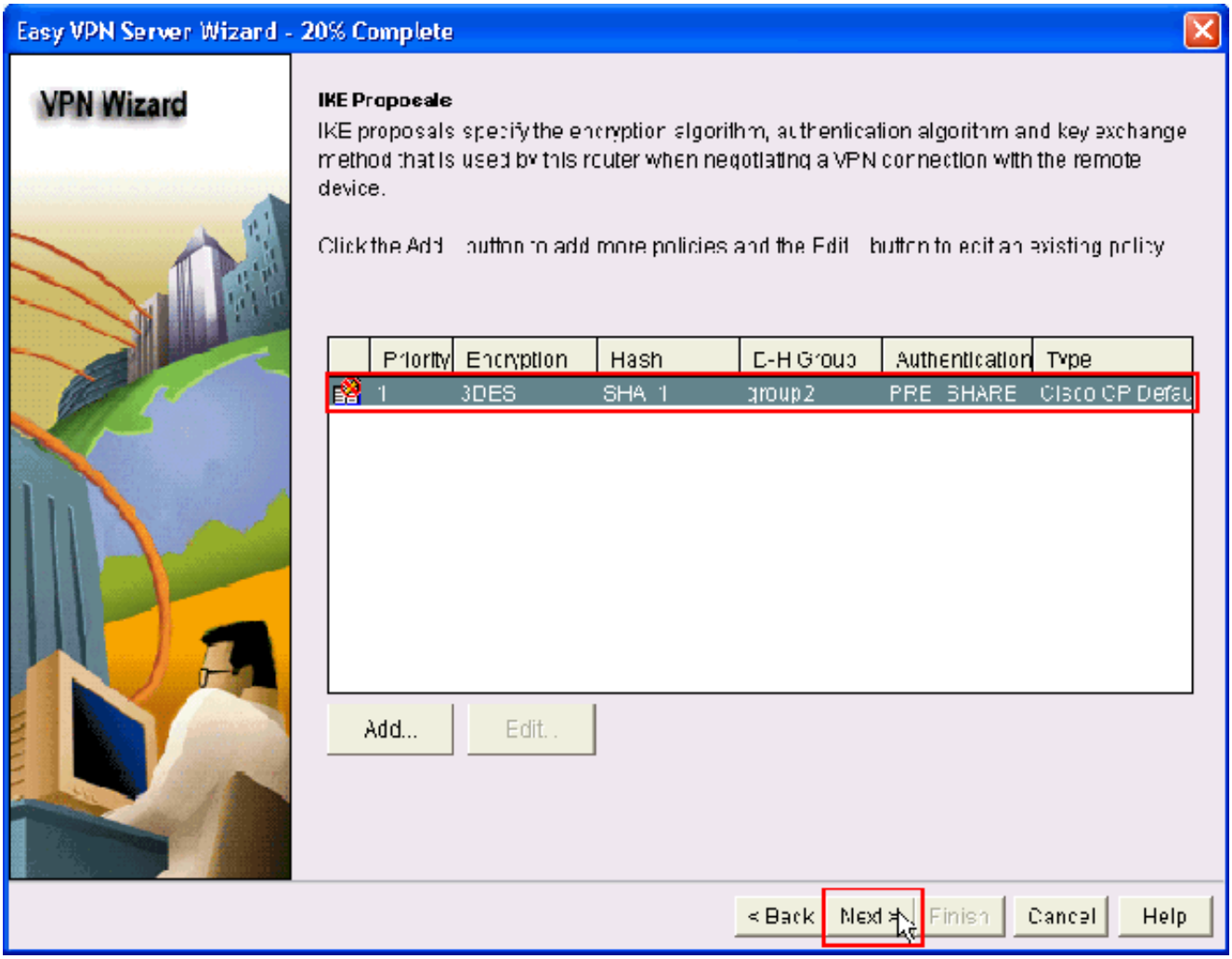

4. Especifique el **algoritmo de cifrado, el algoritmo de autenticación y el método de intercambio de claves** que utilizará este router al negociar con el dispositivo remoto. Hay una política IKE predeterminada en el router que se puede utilizar si es necesario. Si desea agregar una nueva política IKE, haga clic en
Agregar.



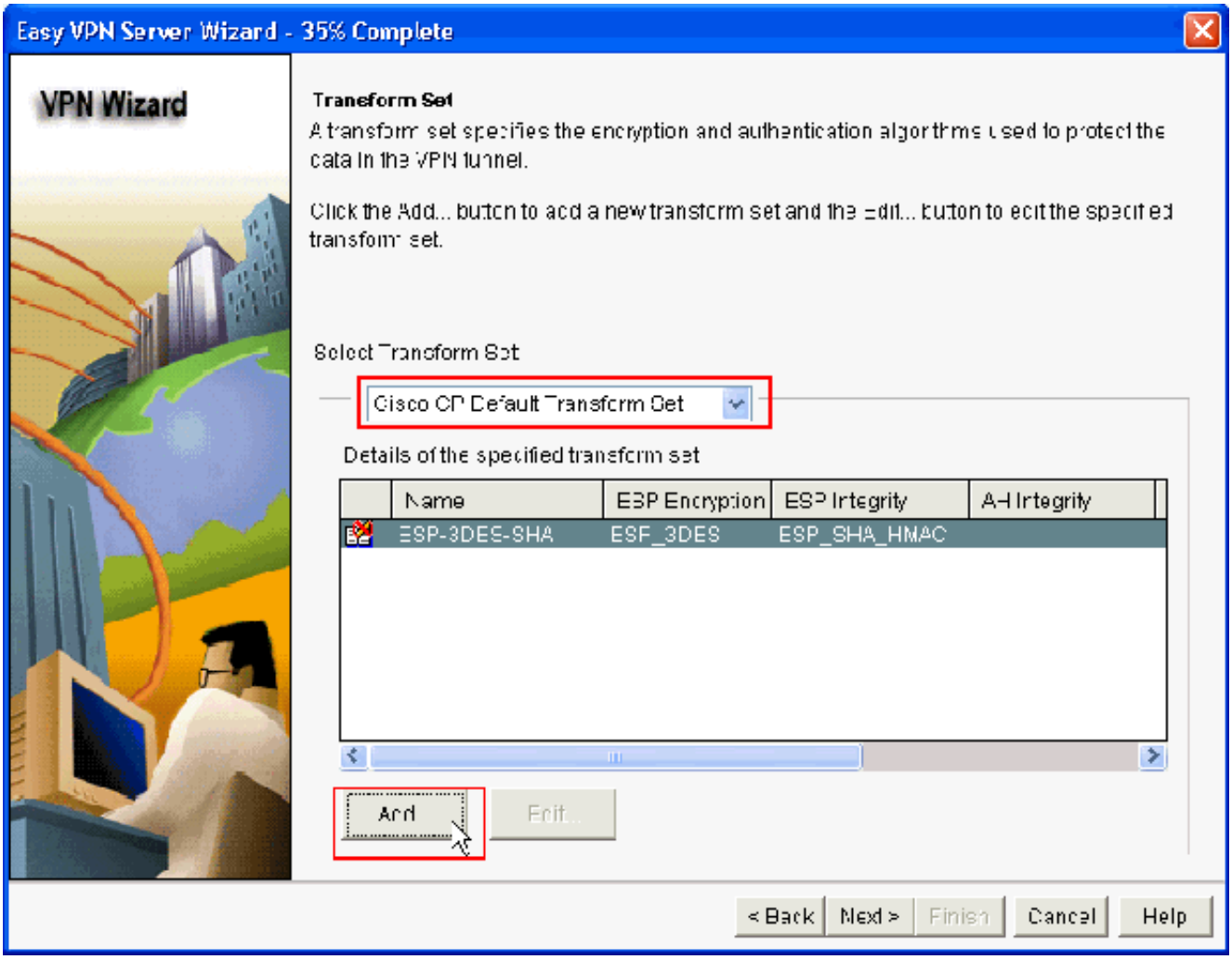

5. Proporcione **Algoritmo de Cifrado**, **Algoritmo de Autenticación** y el **Método de Intercambio de Claves** como se muestra aquí, luego haga clic en **Aceptar**:



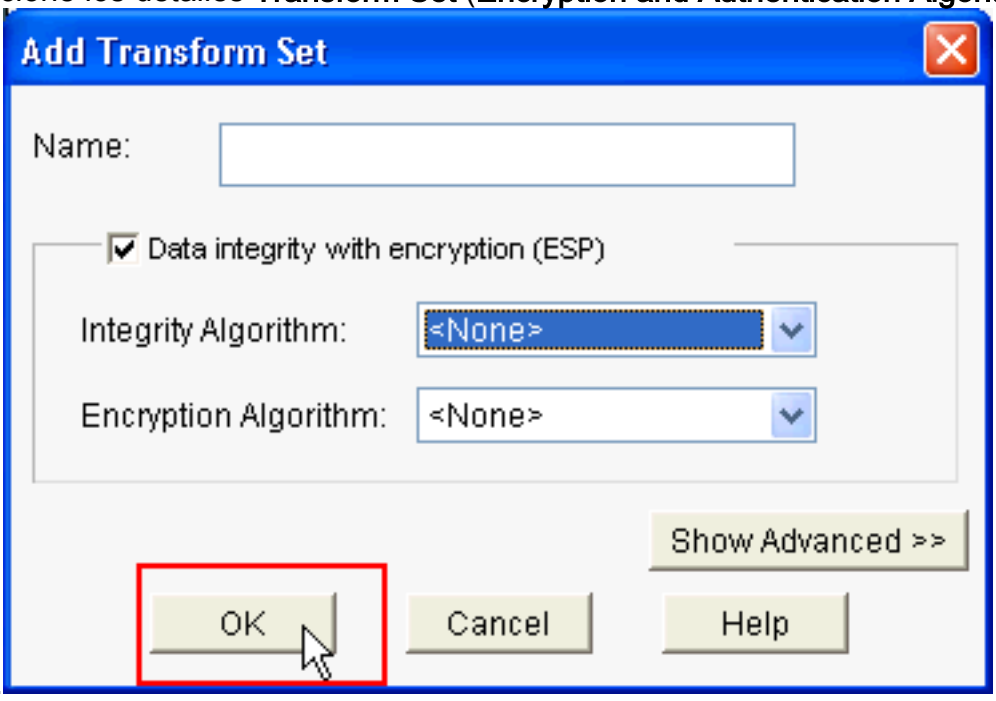

6. En este ejemplo se utiliza la **política IKE predeterminada**. Como resultado, elija la política IKE predeterminada y haga clic en **Next**.



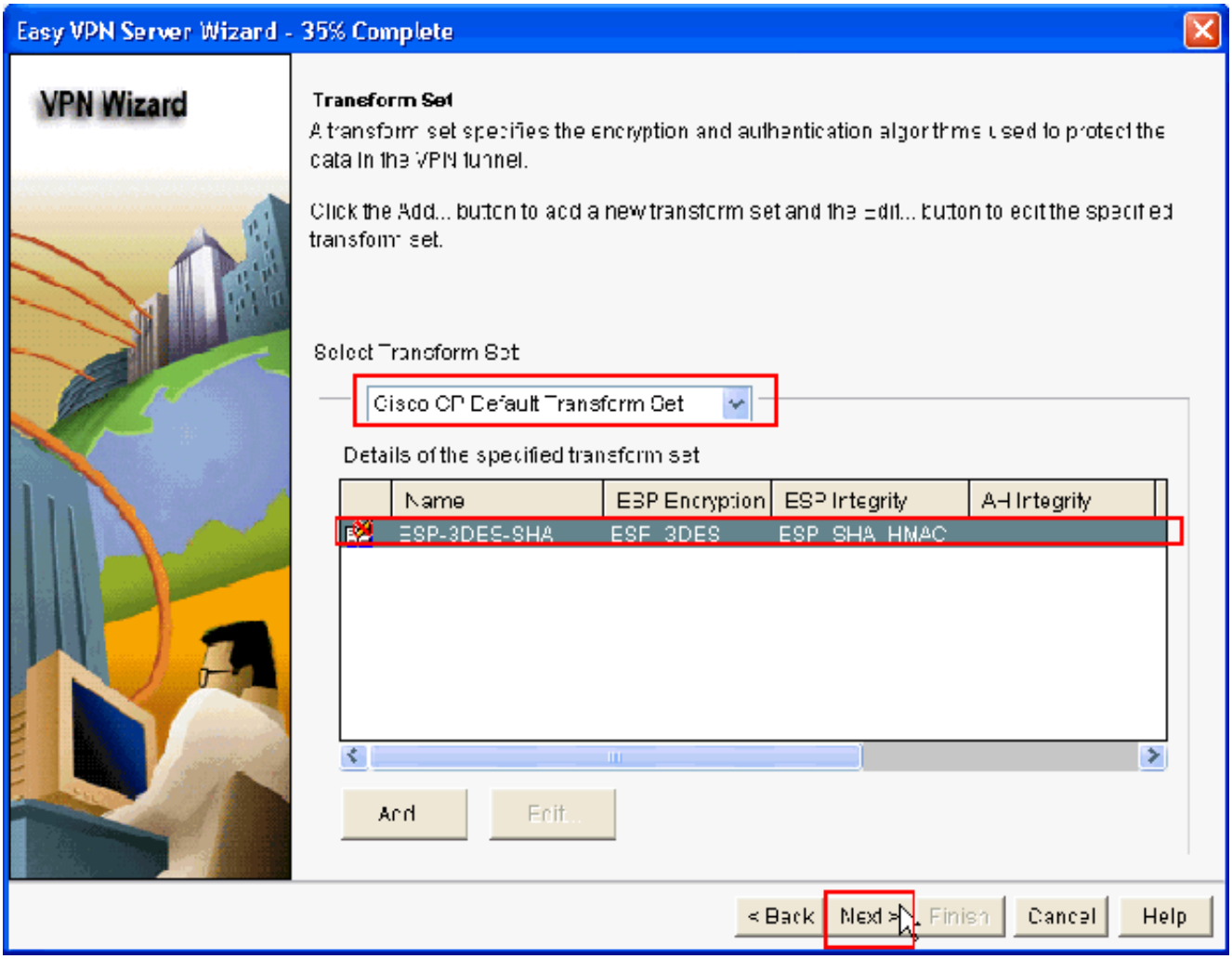

7. En la nueva ventana, se deben proporcionar los detalles del **conjunto de transformación**. El conjunto de transformación especifica los algoritmos **Encryption** y **Authentication** utilizados para proteger los **datos en el túnel VPN**. Haga clic en **Agregar** para proporcionar estos detalles. Puede agregar cualquier número de conjuntos de transformación según sea necesario al hacer clic en **Agregar** y proporcionar los detalles.**Nota: CP Default Transform Set** está presente de forma predeterminada en el router cuando se configura con **Cisco CP.**



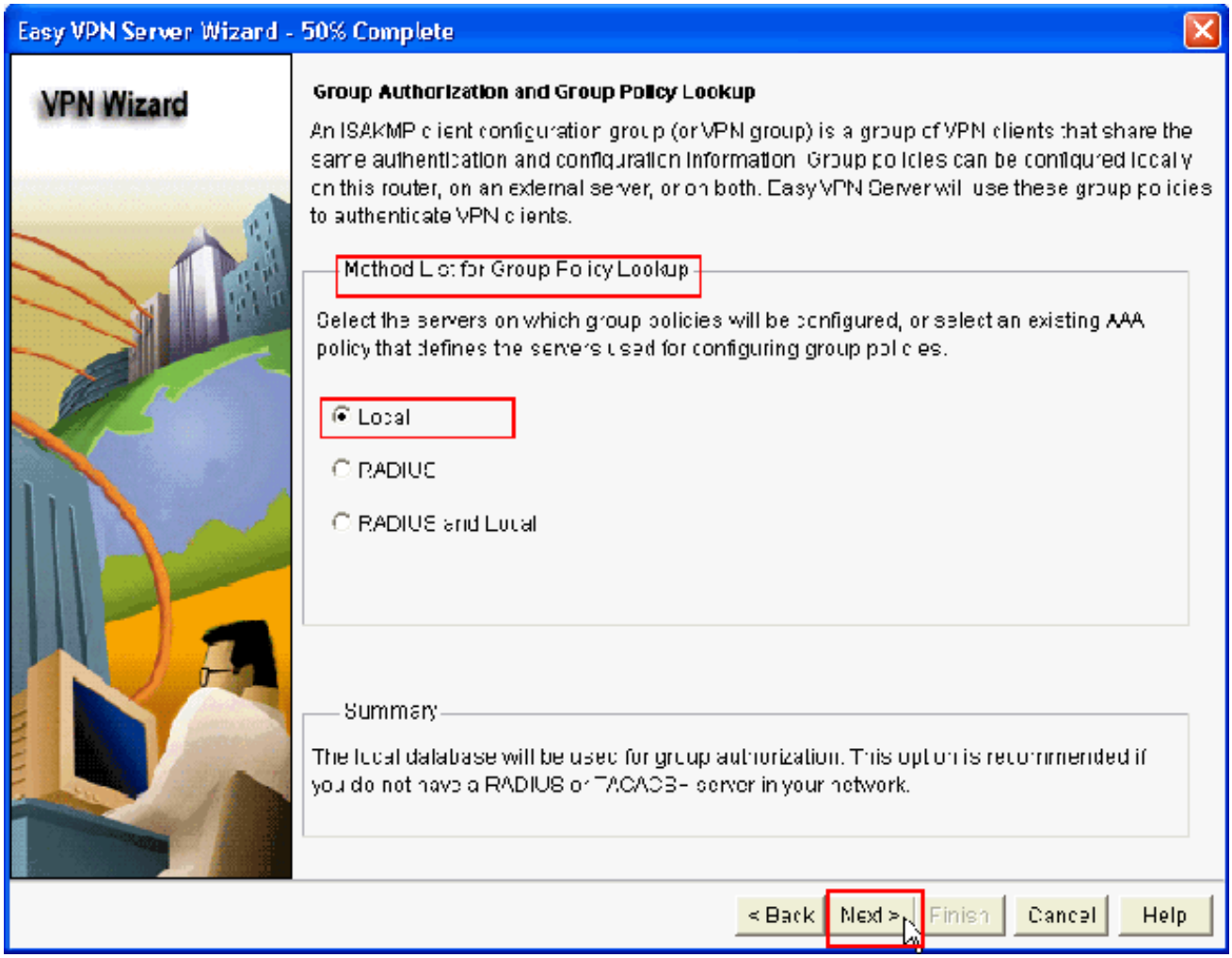

8. Proporcione los detalles **Transform Set** (**Encryption and Authentication Algorithm**) y haga clic en **OK**.



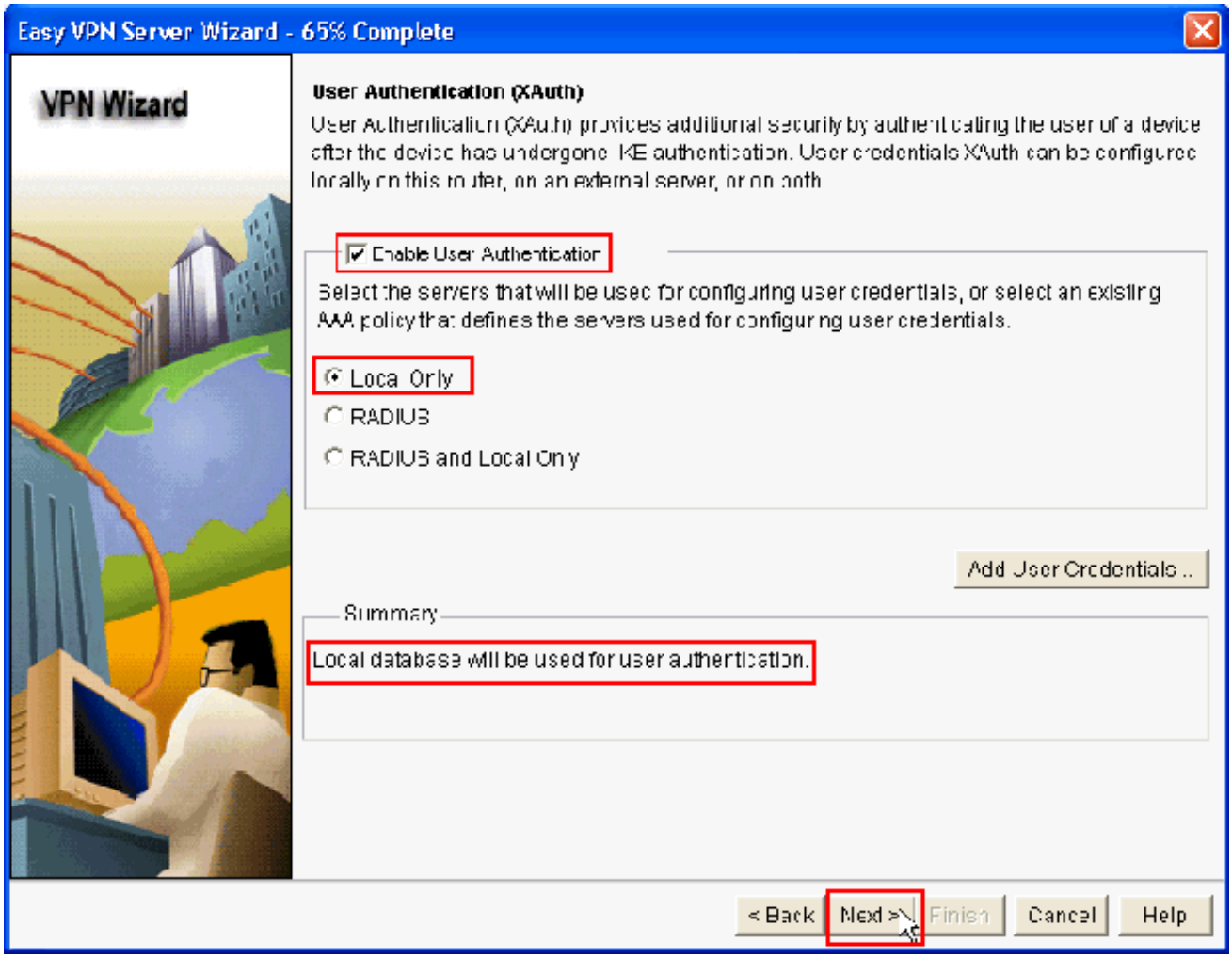

9. En este ejemplo se utiliza el **Conjunto de transformación predeterminado** denominado **Conjunto de transformación predeterminada de CP**. Como resultado, elija el conjunto de transformación predeterminado y haga clic en **Siguiente**.



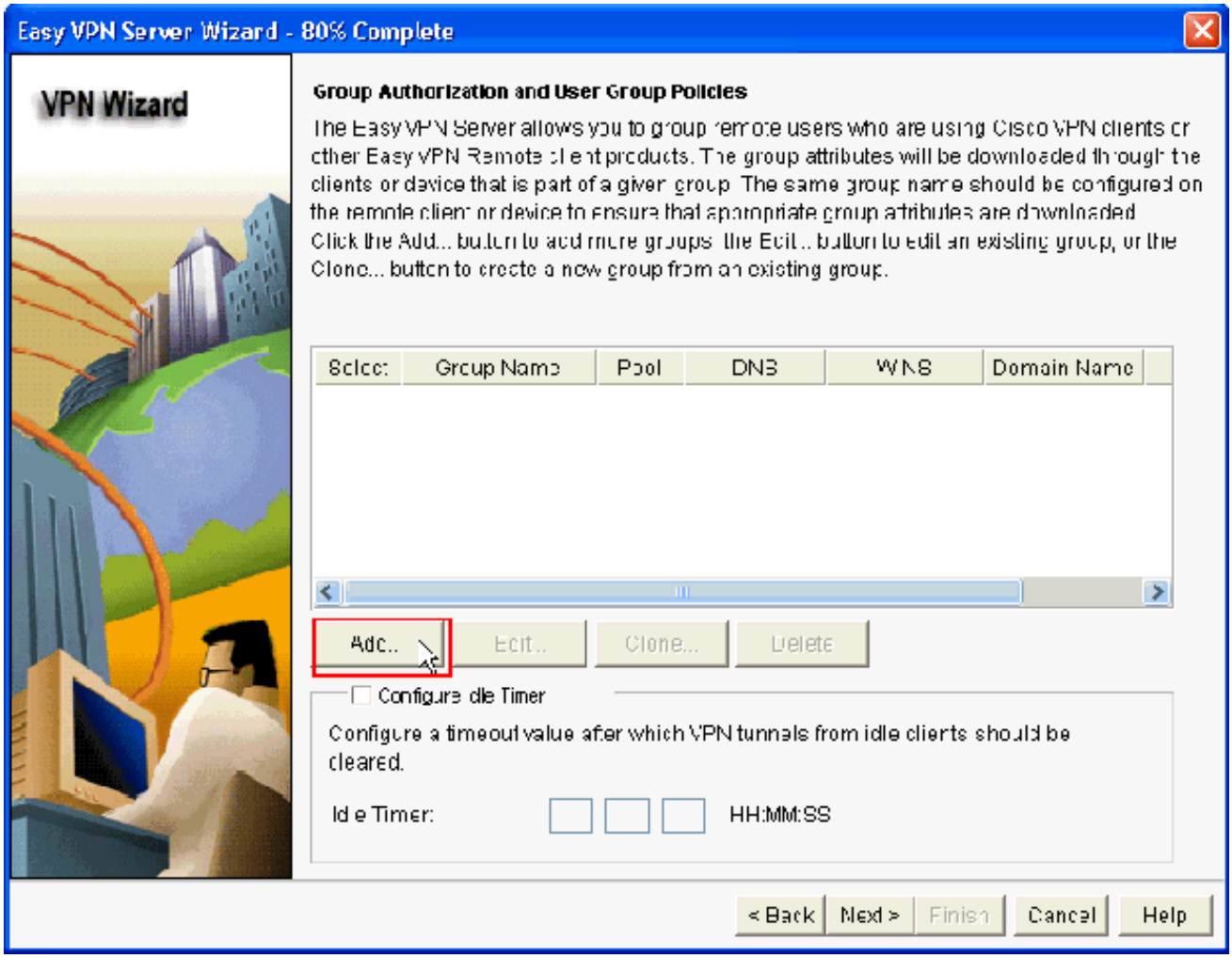

10. En la nueva ventana, elija el servidor en el que se configurarán las políticas de grupo que pueden ser **Local** o **RADIUS** o tanto **Local como RADIUS**. En este ejemplo, utilizamos el **servidor local** para configurar las políticas de grupo. Elija **Local** y haga clic en **Next**.



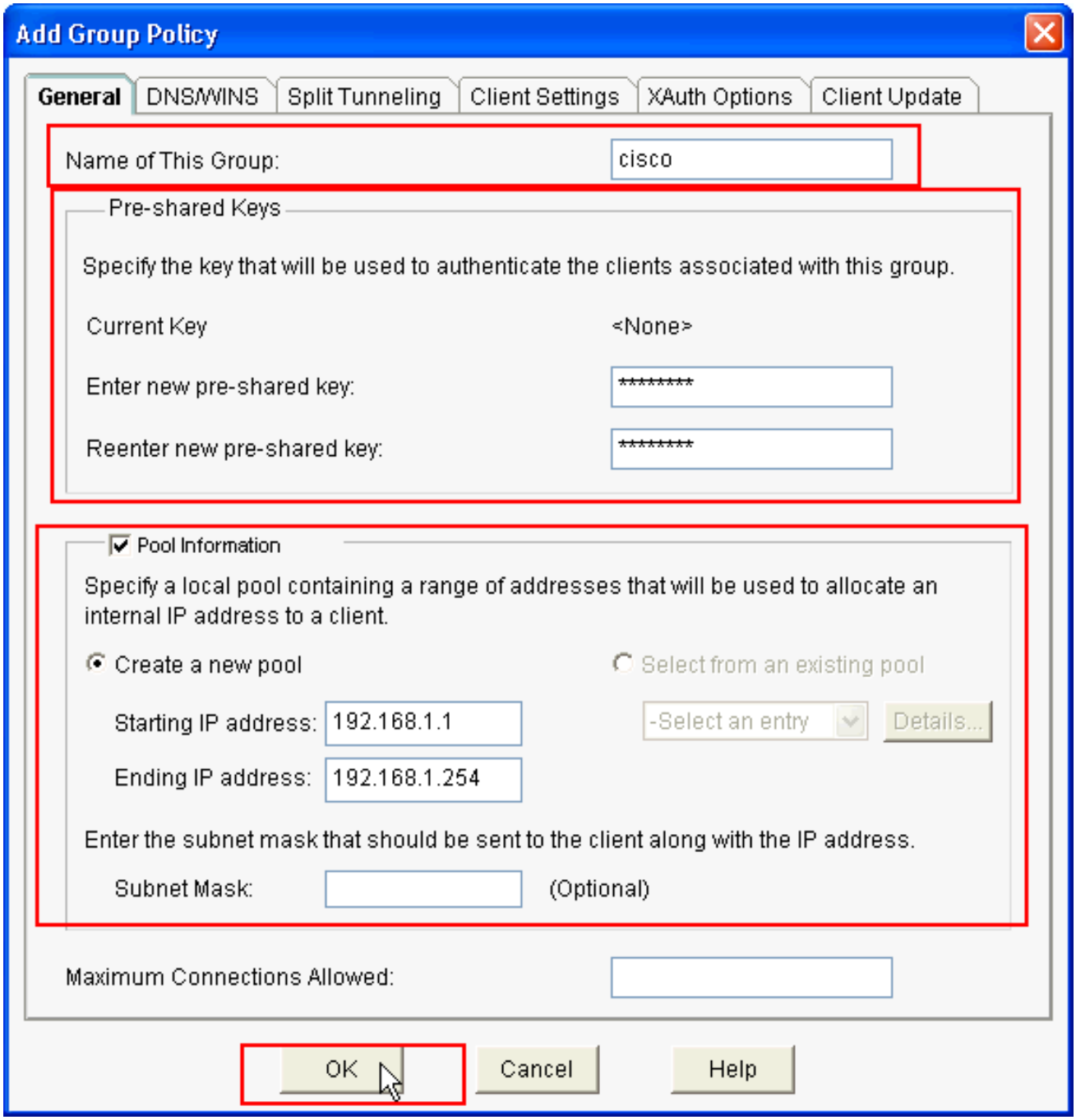

11. Elija el servidor que se utilizará para la autenticación de usuario en esta nueva ventana que puede ser **Local Only** o **RADIUS** o bien **Local Only y RADIUS**. En este ejemplo, utilizamos **servidor local** para configurar las credenciales de usuario para la autenticación. Asegúrese de que la casilla de verificación junto a **Enable User Authentication** esté marcada. Elija **Local Only** y haga clic en
**Next**.



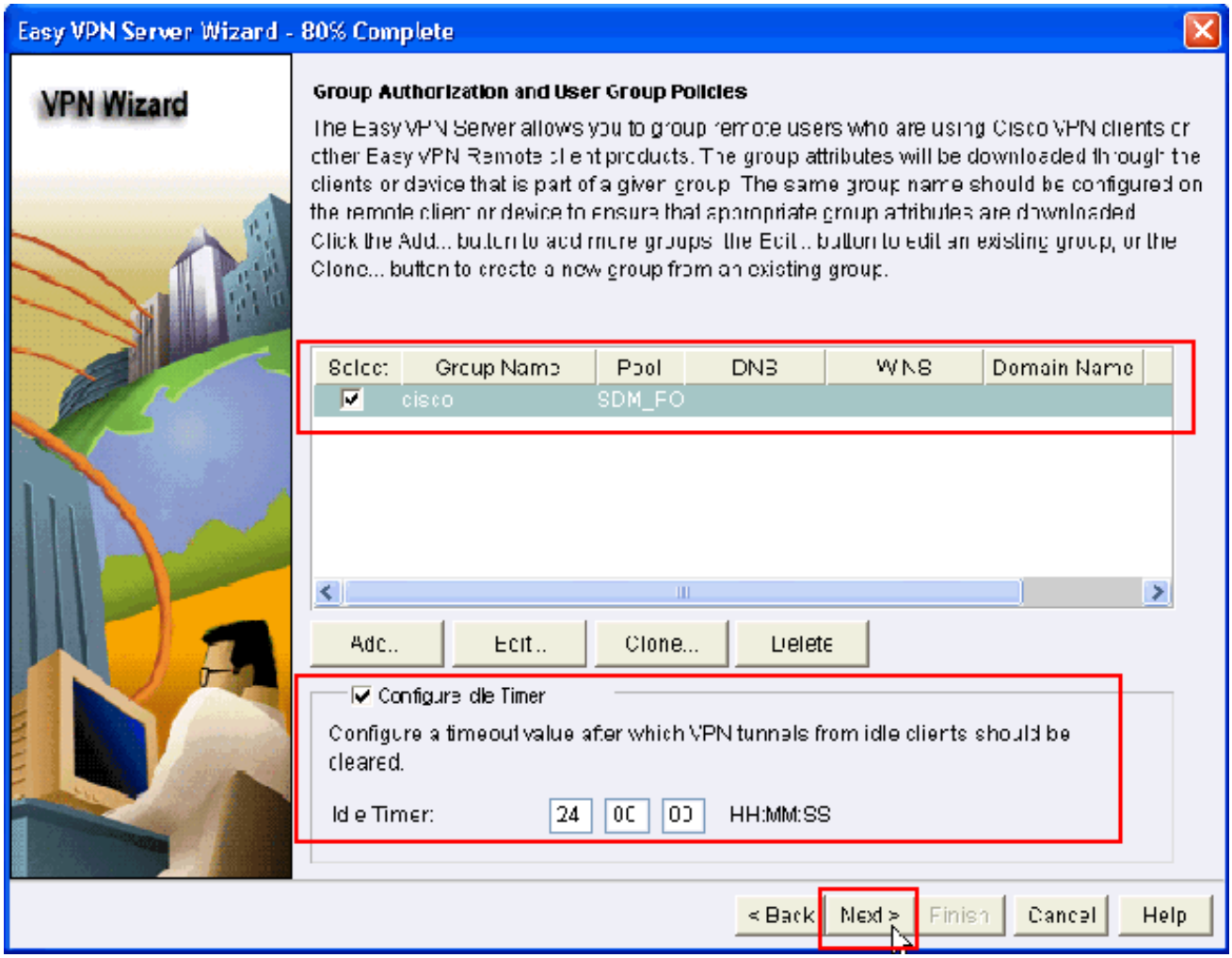

12. Haga clic en **Agregar** para crear una nueva política de grupo y agregar los usuarios remotos en este
grupo.



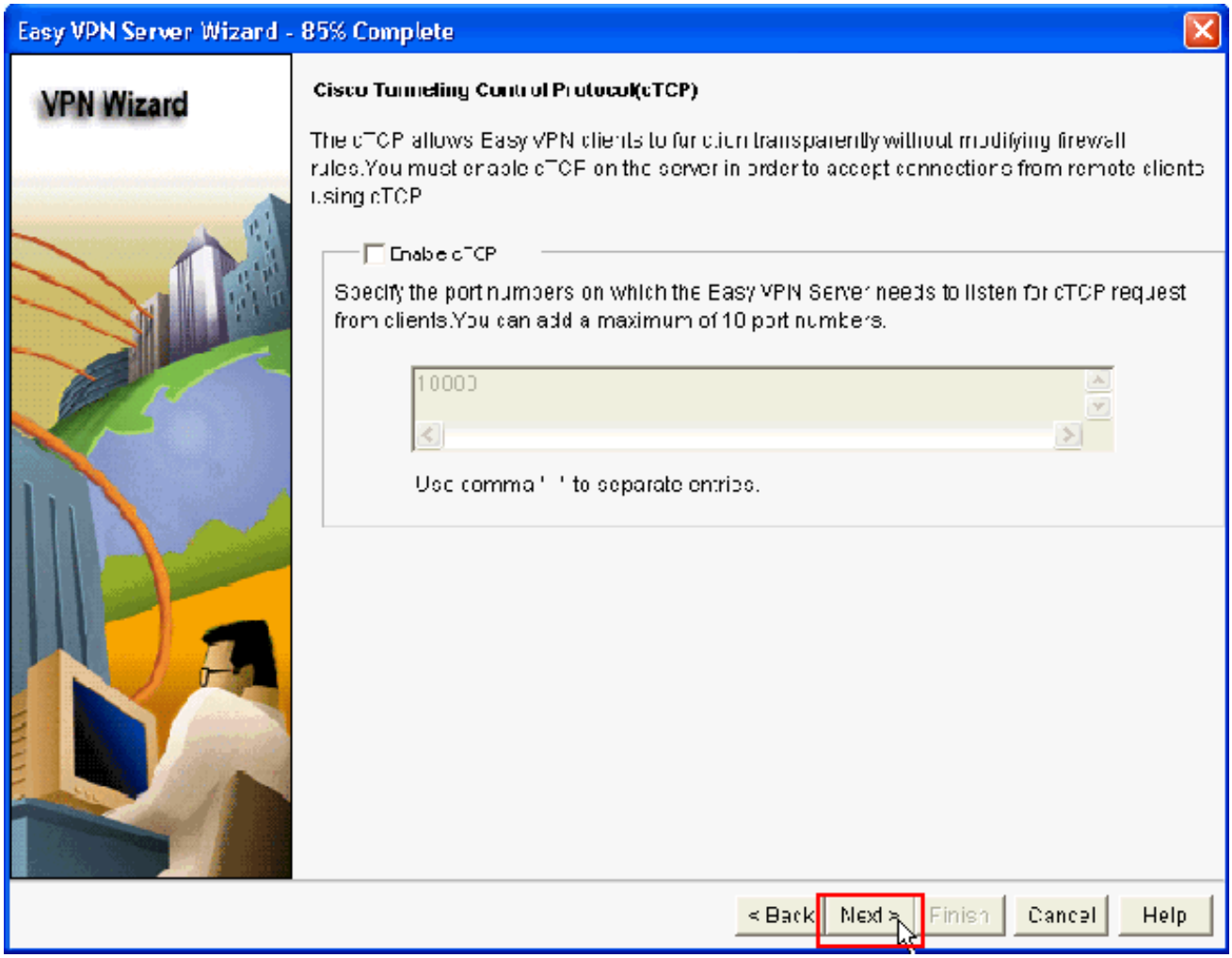

13. En la ventana Agregar política de grupo, proporcione el nombre de grupo en el espacio para proporcionar el nombre de este grupo (cisco en este ejemplo) junto con la clave previamente compartida, y la información sobre el conjunto IP (la dirección IP inicial y la dirección IP final) como se muestra y haga clic en Aceptar.**Nota:** Puede crear un nuevo conjunto IP o utilizar un conjunto IP existente si está presente.



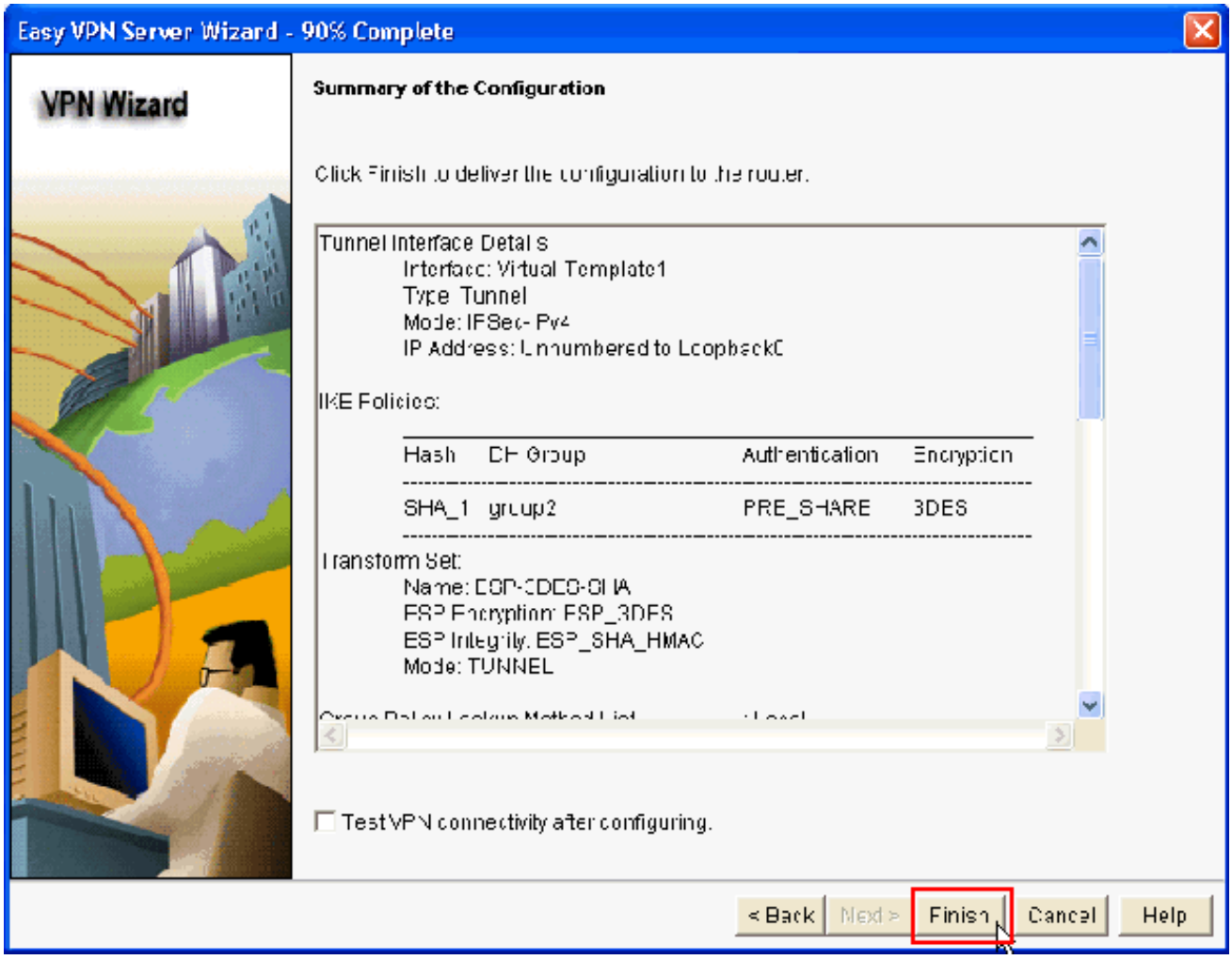

14. Ahora elija la nueva **Política de Grupo** creada con el nombre **cisco** y luego haga clic en la casilla de verificación junto a **Configure Idle Timer** según sea necesario para configurar el **Temporizador de Inactividad**. Haga clic en Next (Siguiente).



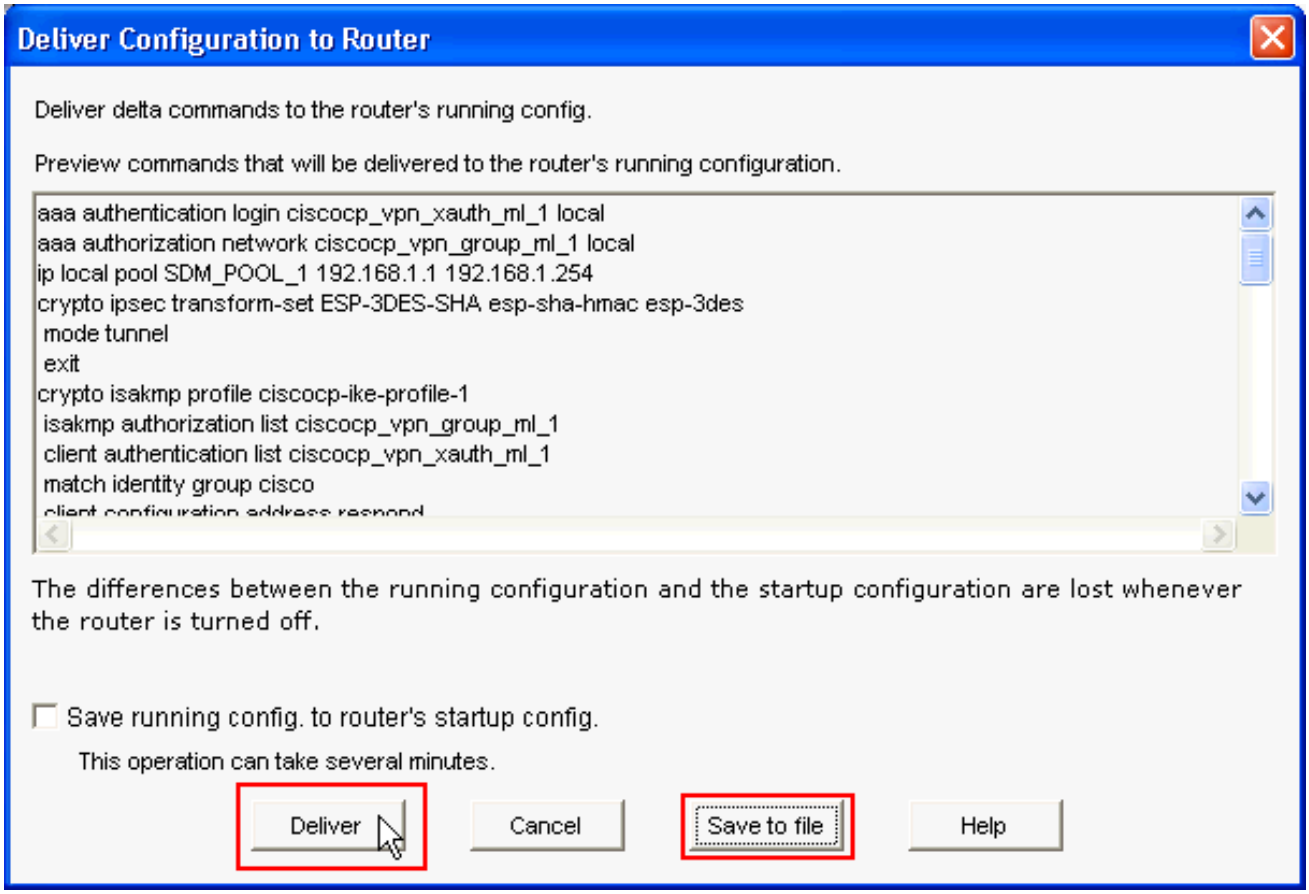

15. Habilite **Cisco Tunneling Control Protocol** (cTCP) si es necesario. De lo contrario, haga clic en
**Siguiente**.



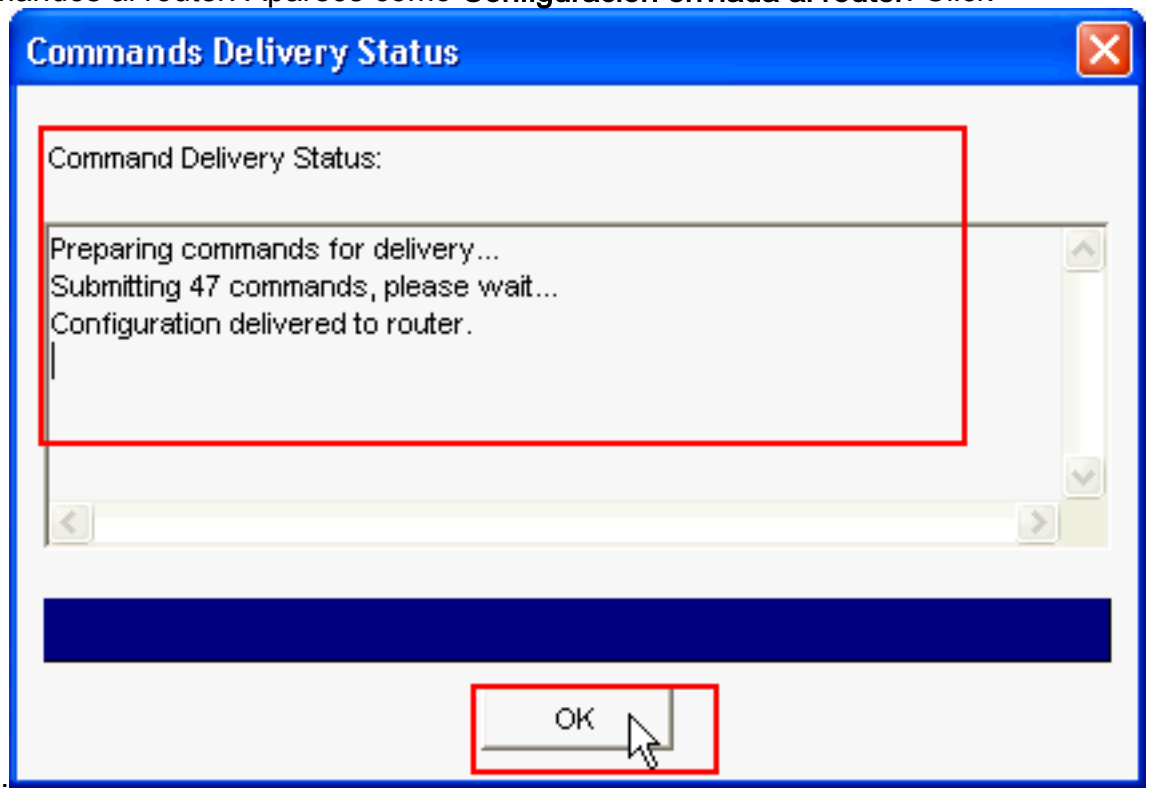

16. Revise el **resumen de la configuración**. Haga clic en Finish (Finalizar).



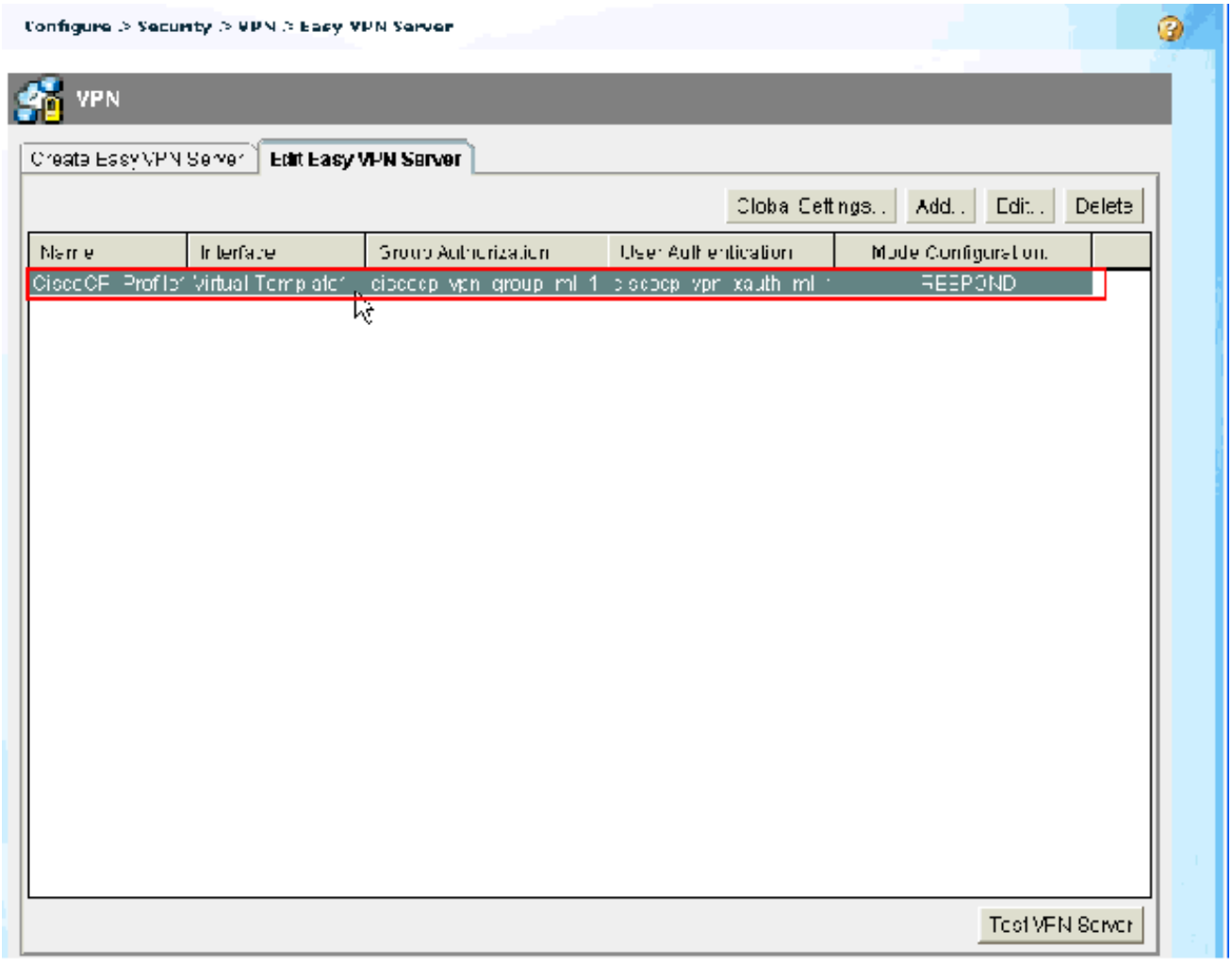

17. En la ventana **Entregar configuración al router**, haga clic en **Entregar** para entregar la configuración al router. Puede hacer clic en **Guardar en archivo** para guardar la configuración como un archivo en el equipo.




18. La ventana **Estado de Entrega de Comandos** muestra el estado de entrega de los comandos al router. Aparece como **Configuración enviada al router**. Click OK.




19. Puede ver el servidor Easy VPN recién creado. Puede editar el servidor existente seleccionando **Editar servidor Easy VPN**. Esto completa la configuración del servidor Easy VPN en el router Cisco IOS.




## Configuración de CLI

### Configuración del router

```
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
```

# Verificación

## Servidor Easy VPN - Comandos show

Use esta sección para confirmar que su configuración funciona correctamente.

- **show crypto isakmp sa — Muestra todas las IKE SAs actuales en un par.**

```
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**: muestra todas las SAs IPsec actuales en un par.

```
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

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

**Nota:** Consulte Información Importante sobre Comandos Debug antes de ejecutar los comandos debug.

# Información Relacionada

- Negociación IPSec/Protocolos IKE
- Guía de inicio rápido de Cisco Configuration Professional
- Páginas de Soporte de Productos de Cisco - Routers
- Soporte Técnico y Documentación - Cisco Systems