配置专业人员：在两个IOS路由器配置示例之间的站点至站点IPSec VPN

Contents

Introduction

本文档为使用 Cisco Configuration Professional (Cisco CP) 配置两台 Cisco IOS® 路由器之间的 LAN 到 LAN（站点到站点）IPsec 隧道提供配置示例。为了简单起见，使用静态路由。

Prerequisites

Requirements

尝试进行此配置前，请确保满足此要求：

- 必须建立端到端 IP 连接才能开始此配置。

Components Used

本文档中的信息基于以下软件和硬件版本：

- 配备 Cisco IOS 软件版本 12.4(15T) 的 Cisco 1841 路由器
- Cisco CP 2.5 版

Note: 请参阅使用 Cisco Configuration Professional 的基本路由器配置，以通过 Cisco CP 配置路由器。

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.

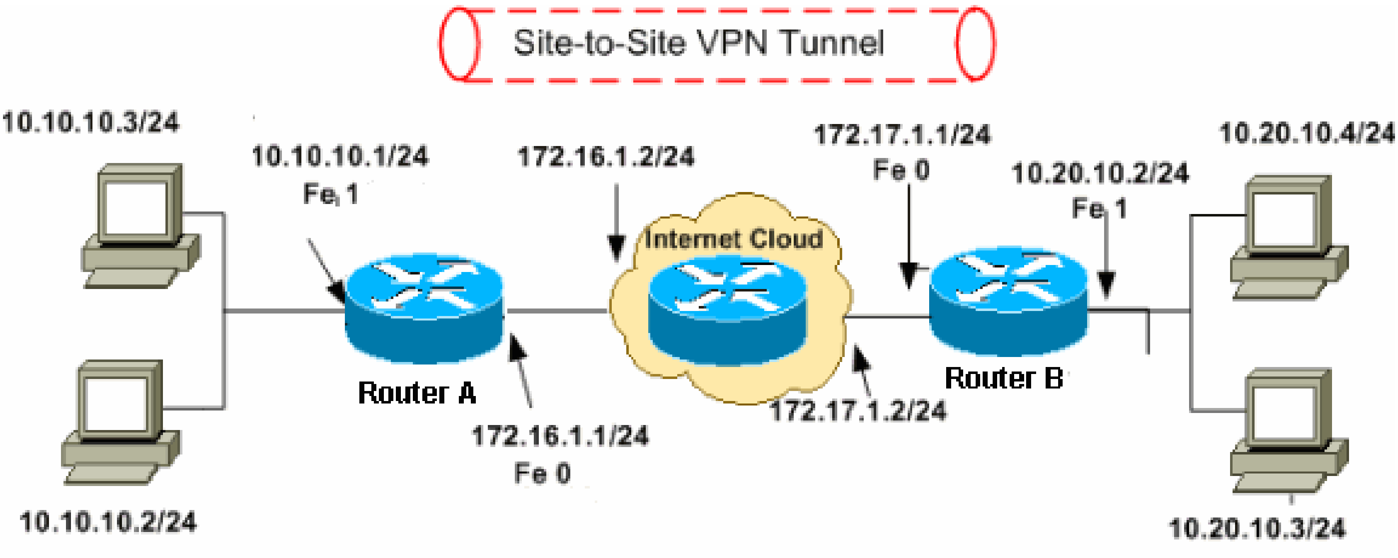
Conventions

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

Network Diagram

本文档使用以下网络设置：



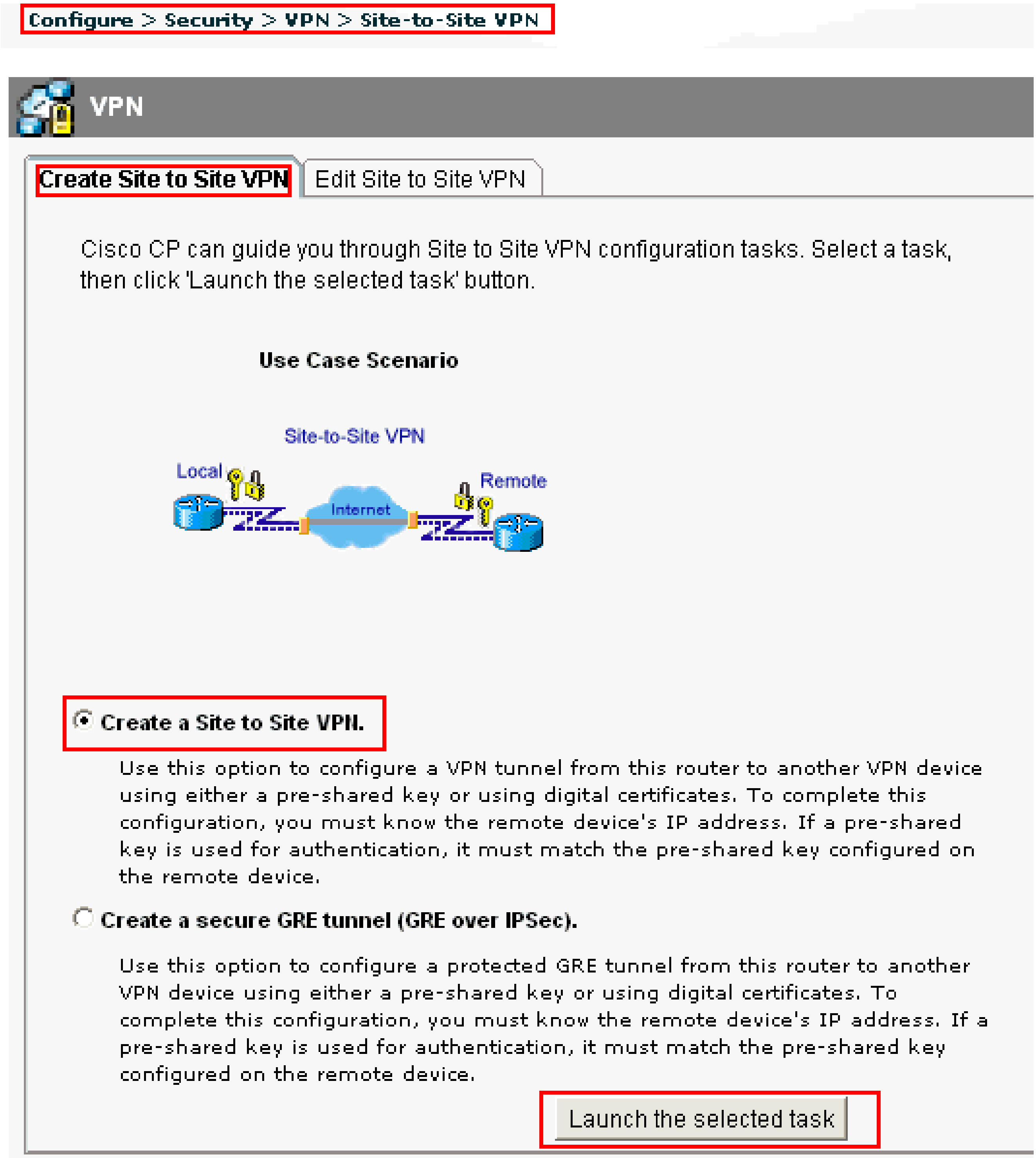
Note: 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

- 路由器 A Cisco CP 配置
- 路由器 B Cisco CP 配置
- 路由器 B CLI 配置

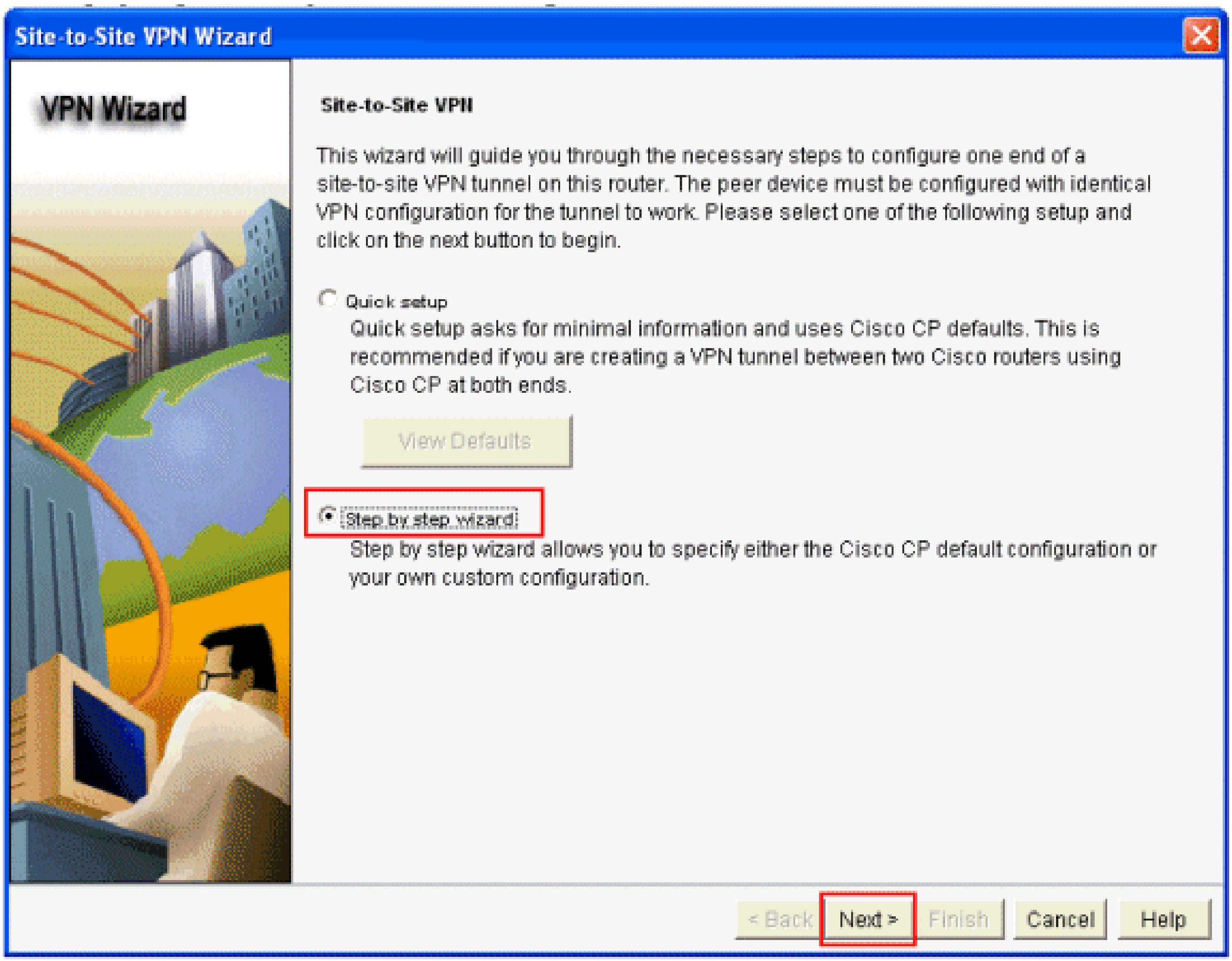
路由器 A Cisco CP 配置

执行以下步骤，以便在 Cisco IOS 路由器上配置站点到站点 VPN 隧道：

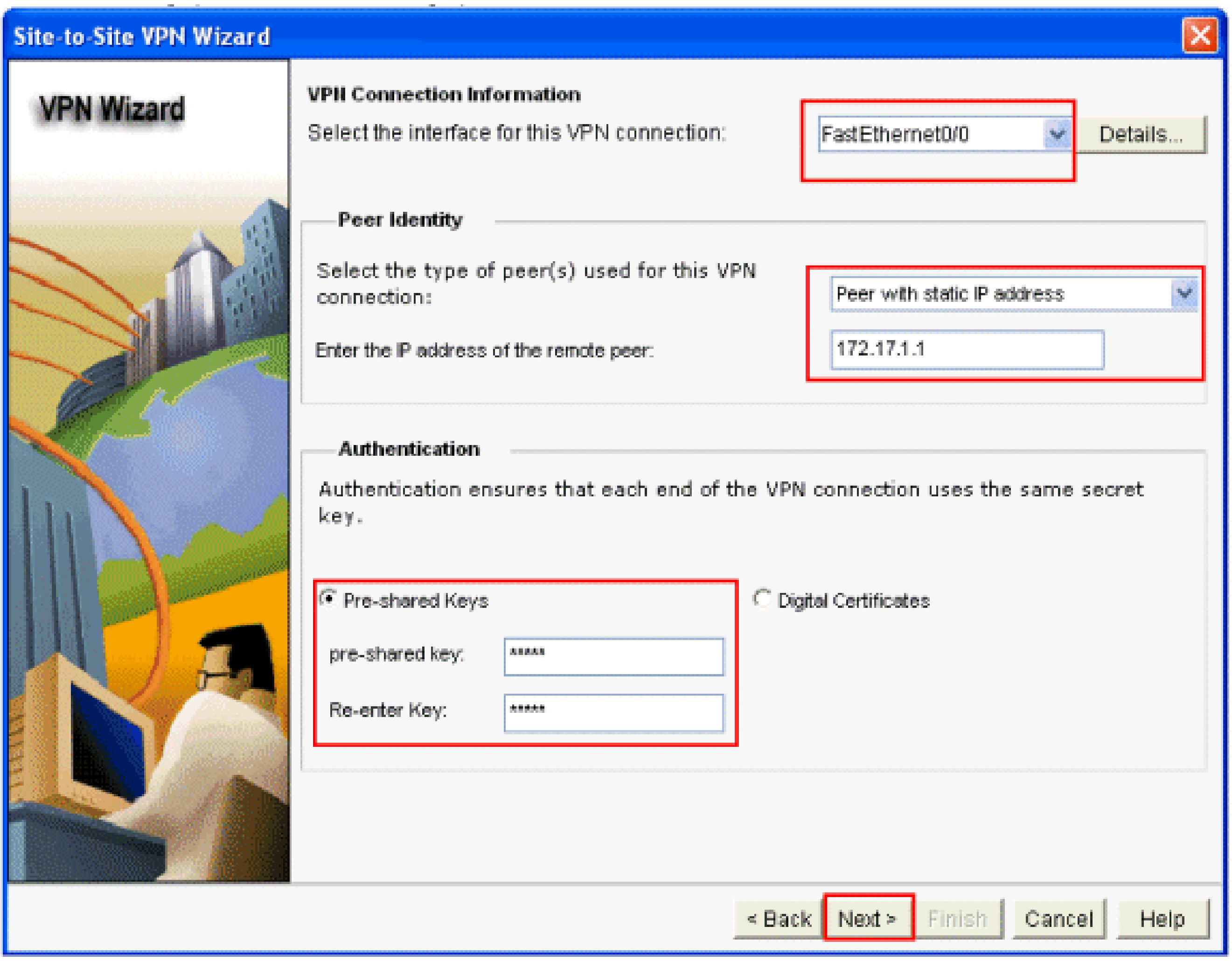
1. 选择 **Configure** > Security > **VPN** > **Site-to-Site VPN**，并单击 **Create a Site-to-Site VPN** 旁边的单选按钮。单击 **Launch the selected task**。



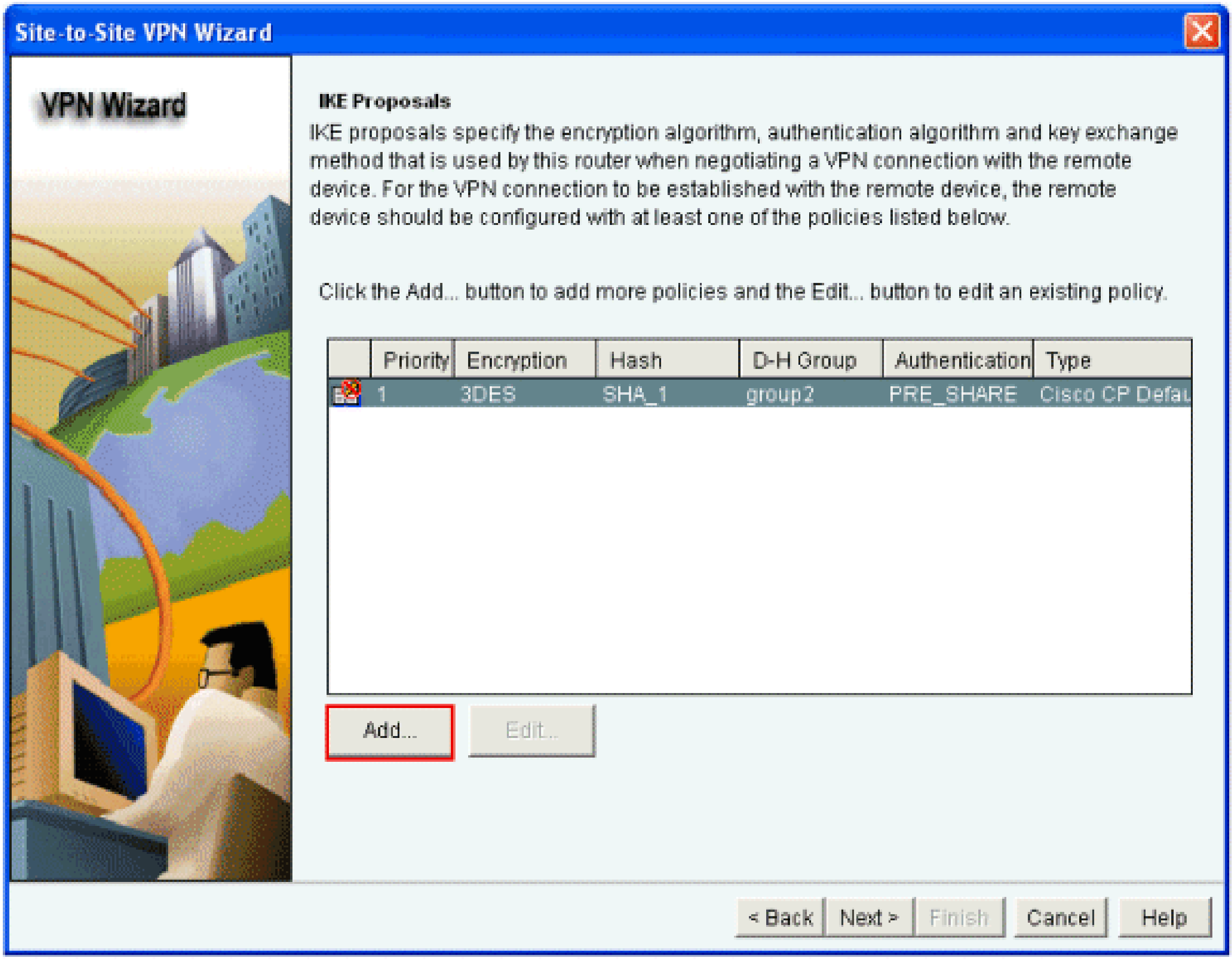
2. 选择 **Step by step wizard** 继续进行配置，然后单击 **Next**。



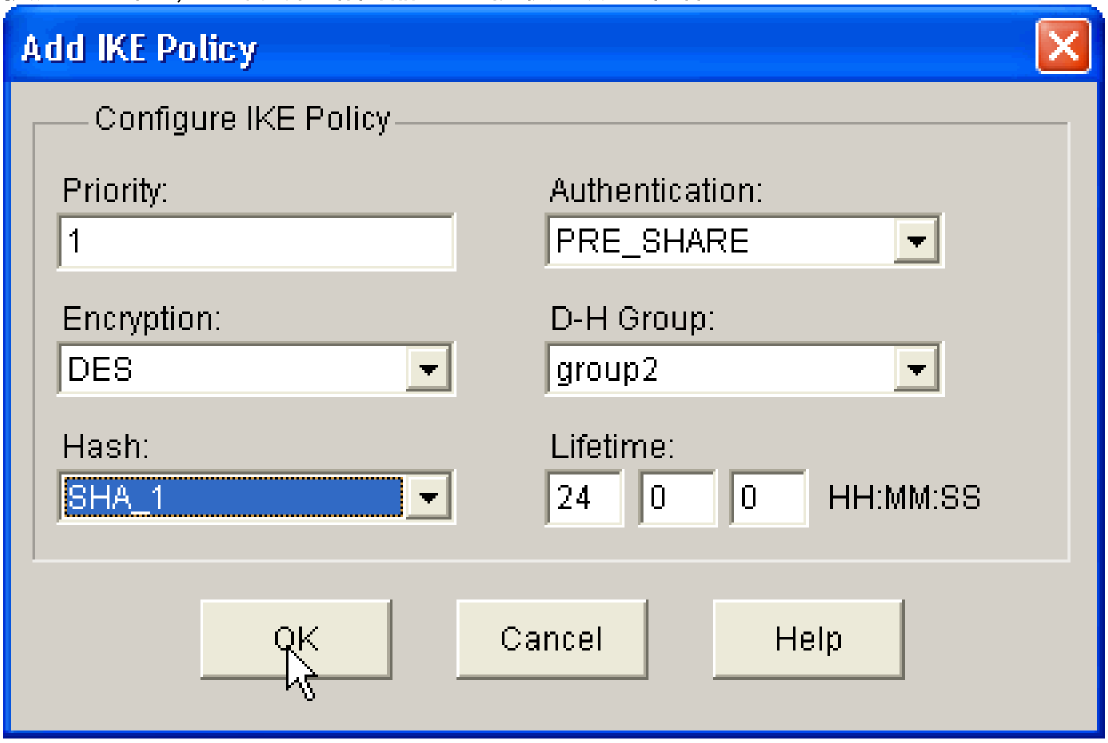
3. 在下一个窗口的相应空白处提供 VPN 连接信息。从下拉菜单中选择 VPN 隧道的接口。此处选择 **FastEthernet0**。在 **Peer Identity** 中，选择具有静态 IP 地址的对等体并提供远程对等体 IP 地址。然后，在 Authentication 部分中提供 Pre-shared Key（在本示例中为 *cisco123*）。最后，单击 **Next**。



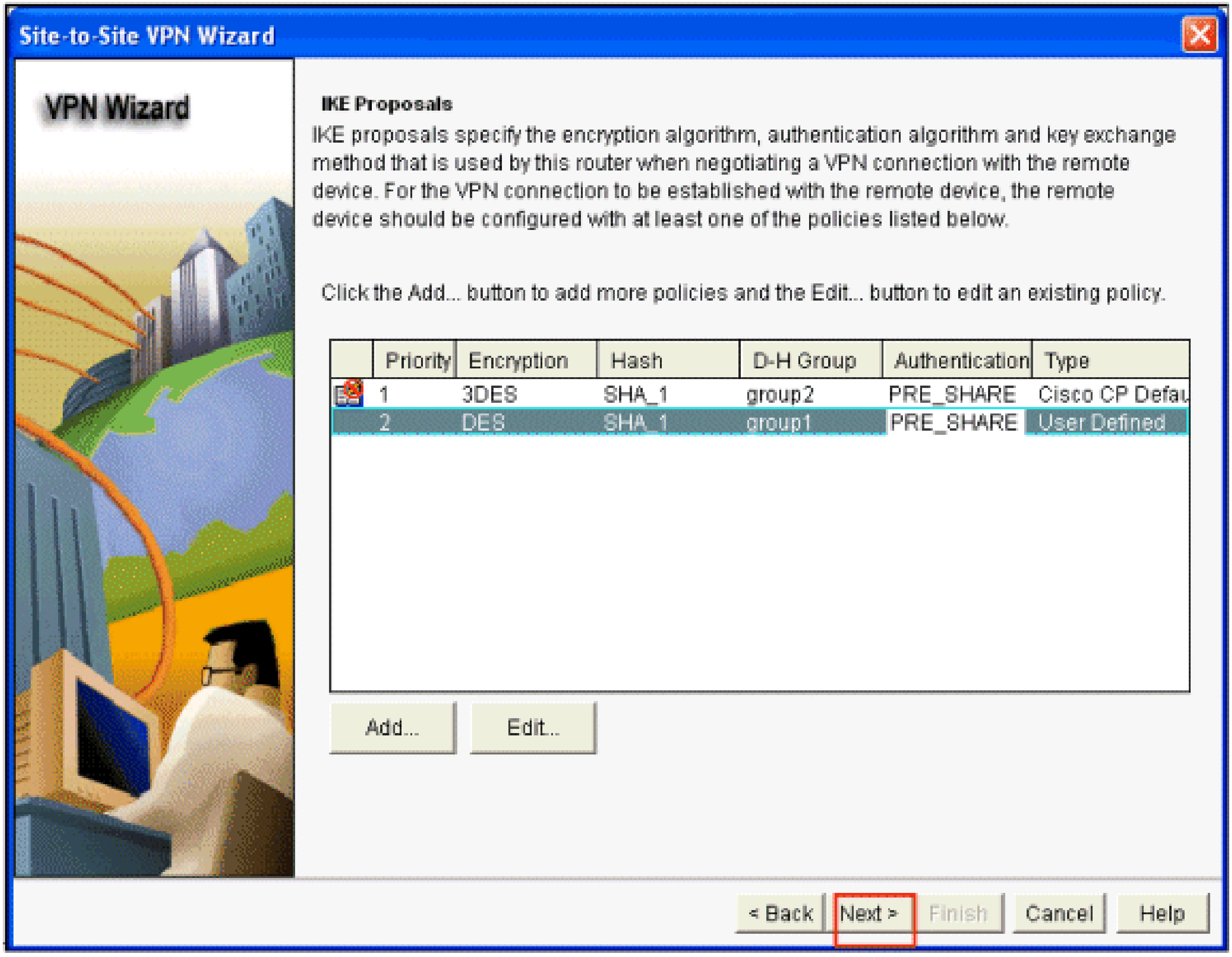
4. 单击 Add 添加指定加密算法、验证算法和密钥交换方法的 IKE 建议。



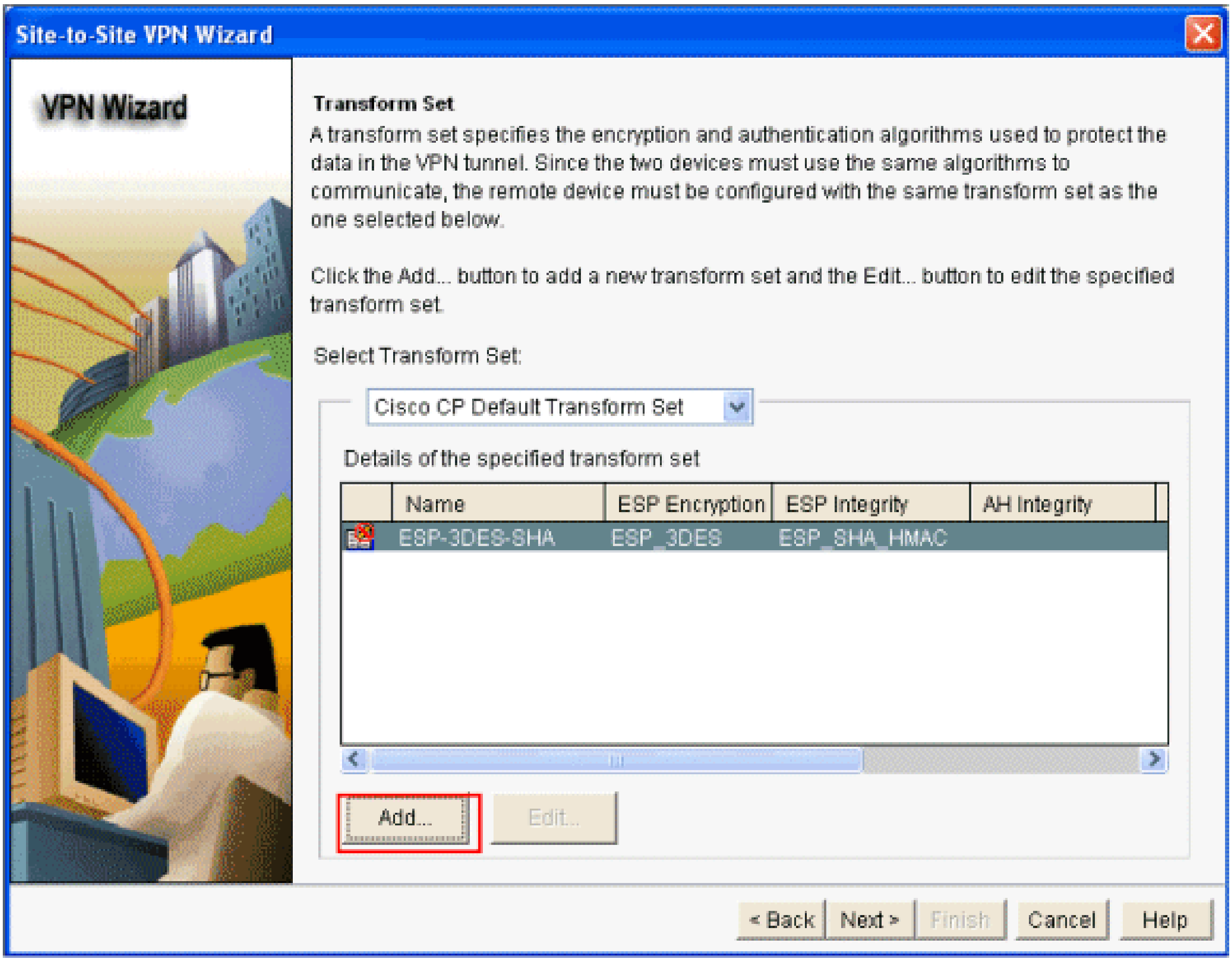
5. 提供加密算法、验证算法和密钥交换方法，然后单击 **OK**。加密算法、身份验证算法和密钥交换方法的值，应与要在路由器 B 上提供的数据匹配。



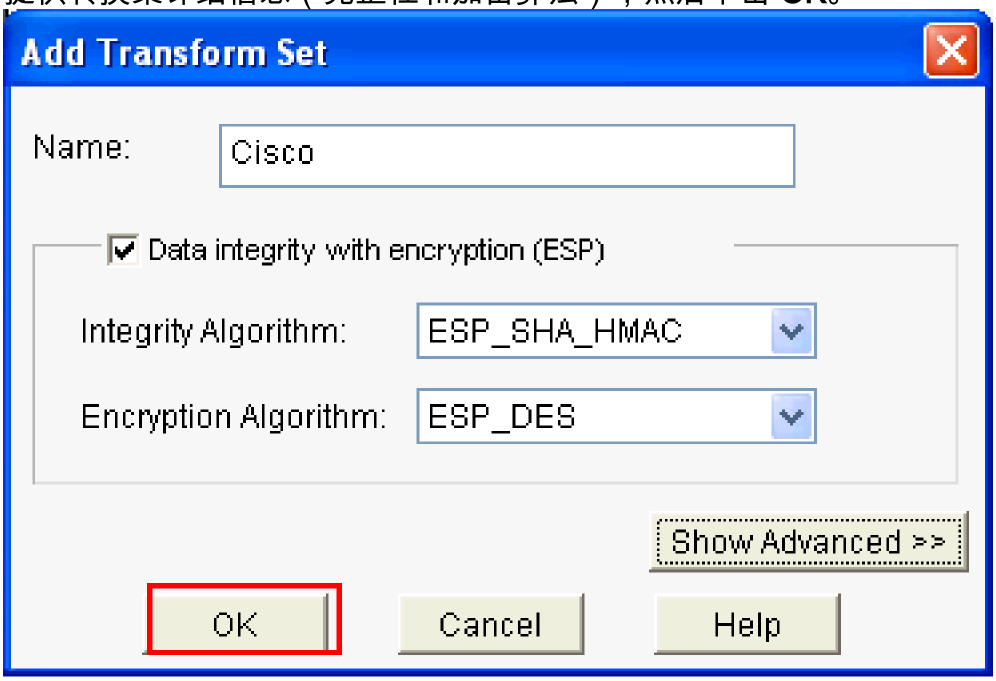
6. 单击 **Next**。



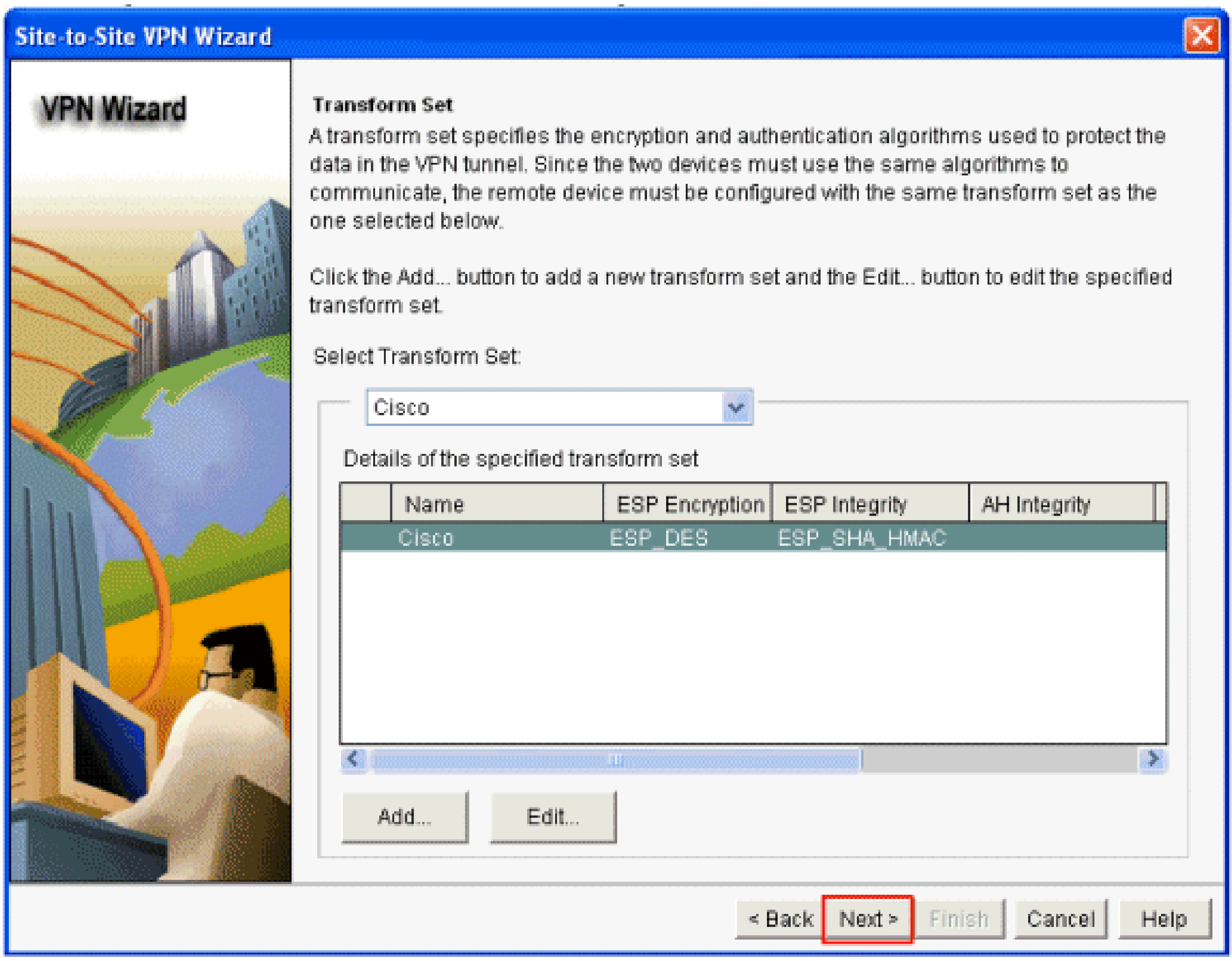
7. 在此新窗口中提供转换集详细信息。“转换集”指定用于保护 VPN 隧道中的数据的**加密**算法和验证算法。单击 **Add** 以提供这些详细信息。使用此方法可根据需要添加任意数量的转换集。



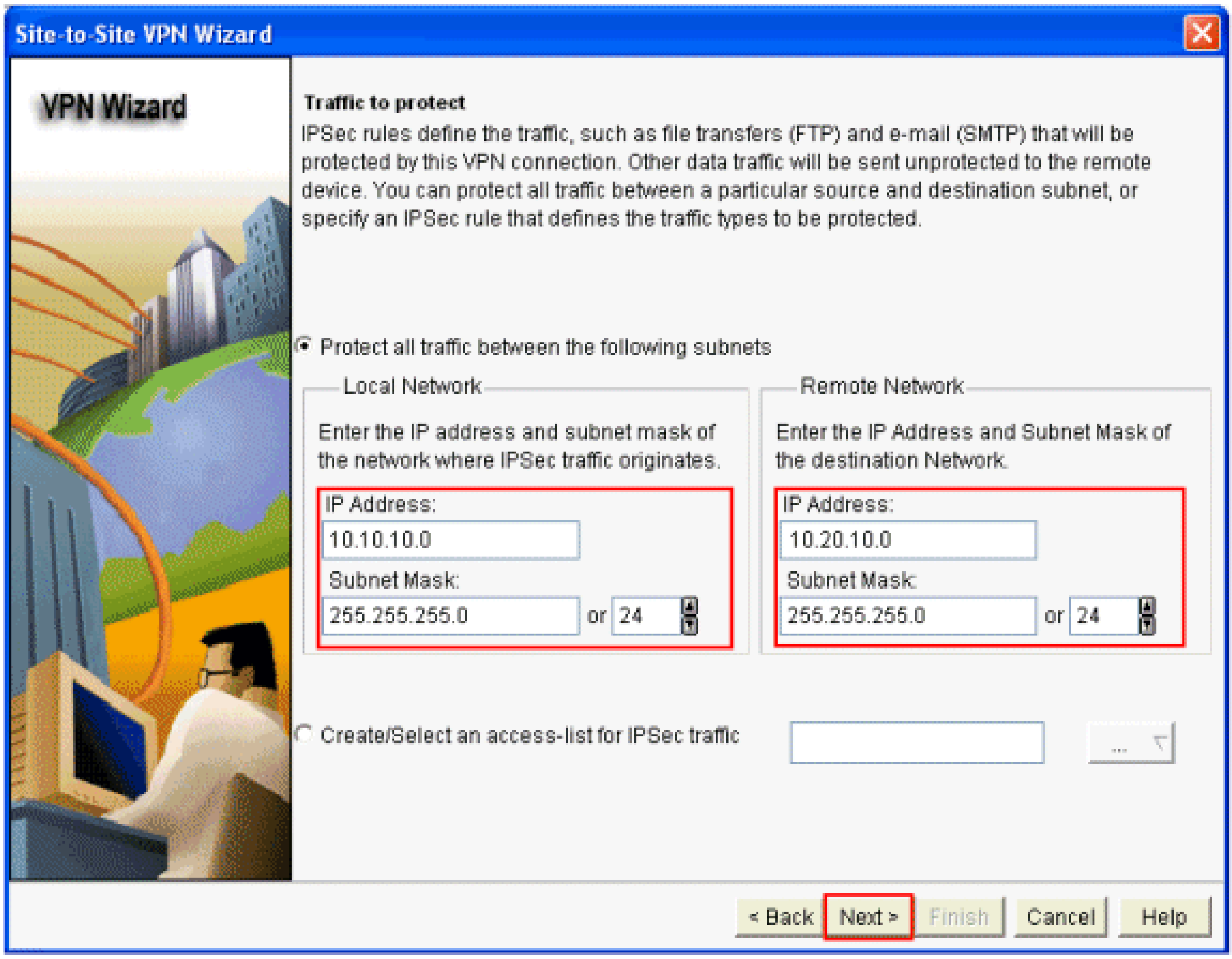
8. 提供转换集详细信息（完整性和加密算法），然后单击 **OK**。



9. 从下拉菜单中选择所需的 **Transform Set**，然后单击 **Next**。



10. 在以下窗口中提供有关要保护的数据流（通过 VPN 隧道）的详细信息。提供要保护的数据流的**源网络和目标网络**，以便保护指定的源网络和目标网络之间的数据流。在本例中，源网络是 *10.10.10.0*，目标网络是 *10.20.10.0*。单击 **Next**。

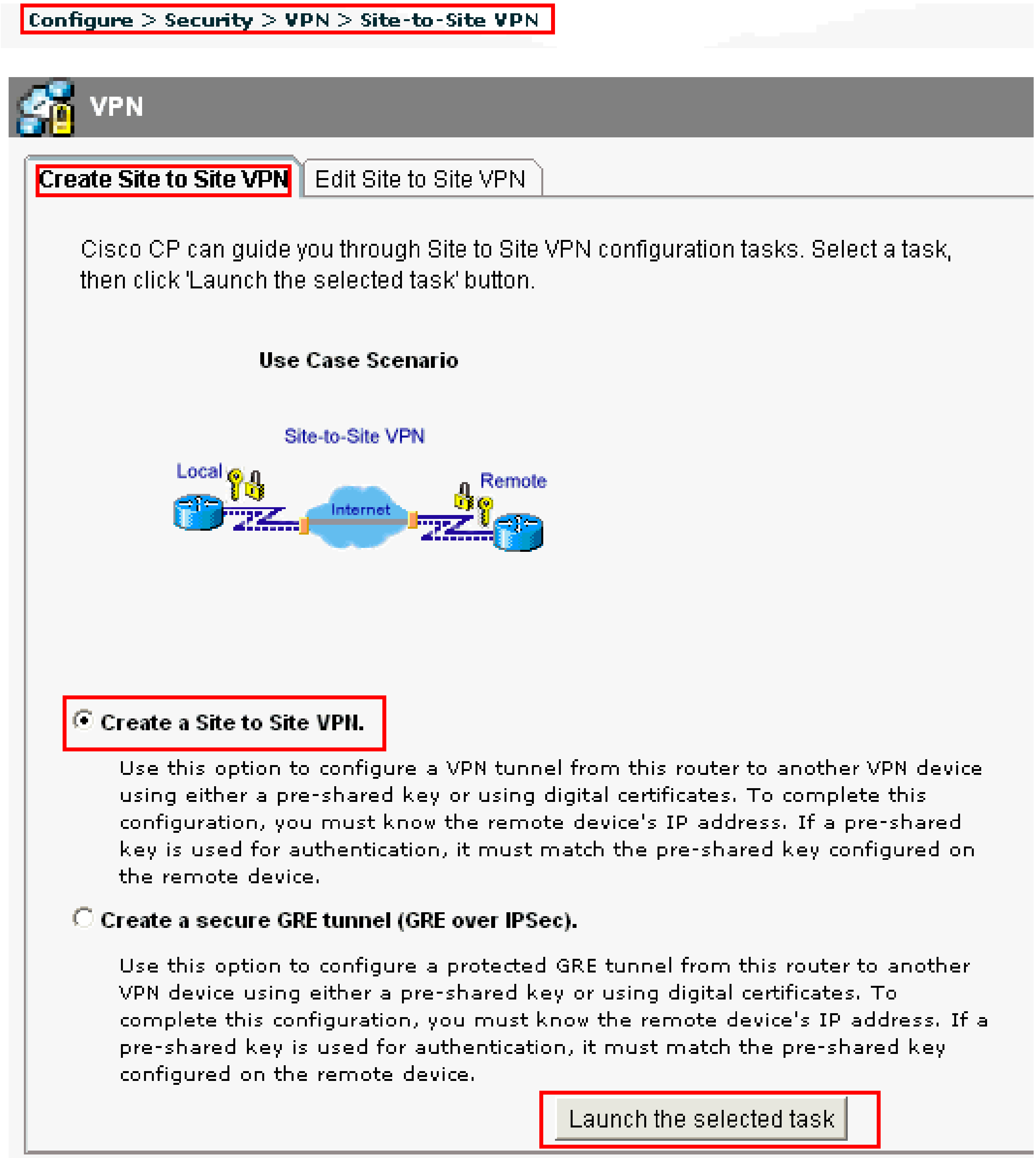


11. 在下一个窗口中点击 **Finish**，完成对路由器 A 的配置。

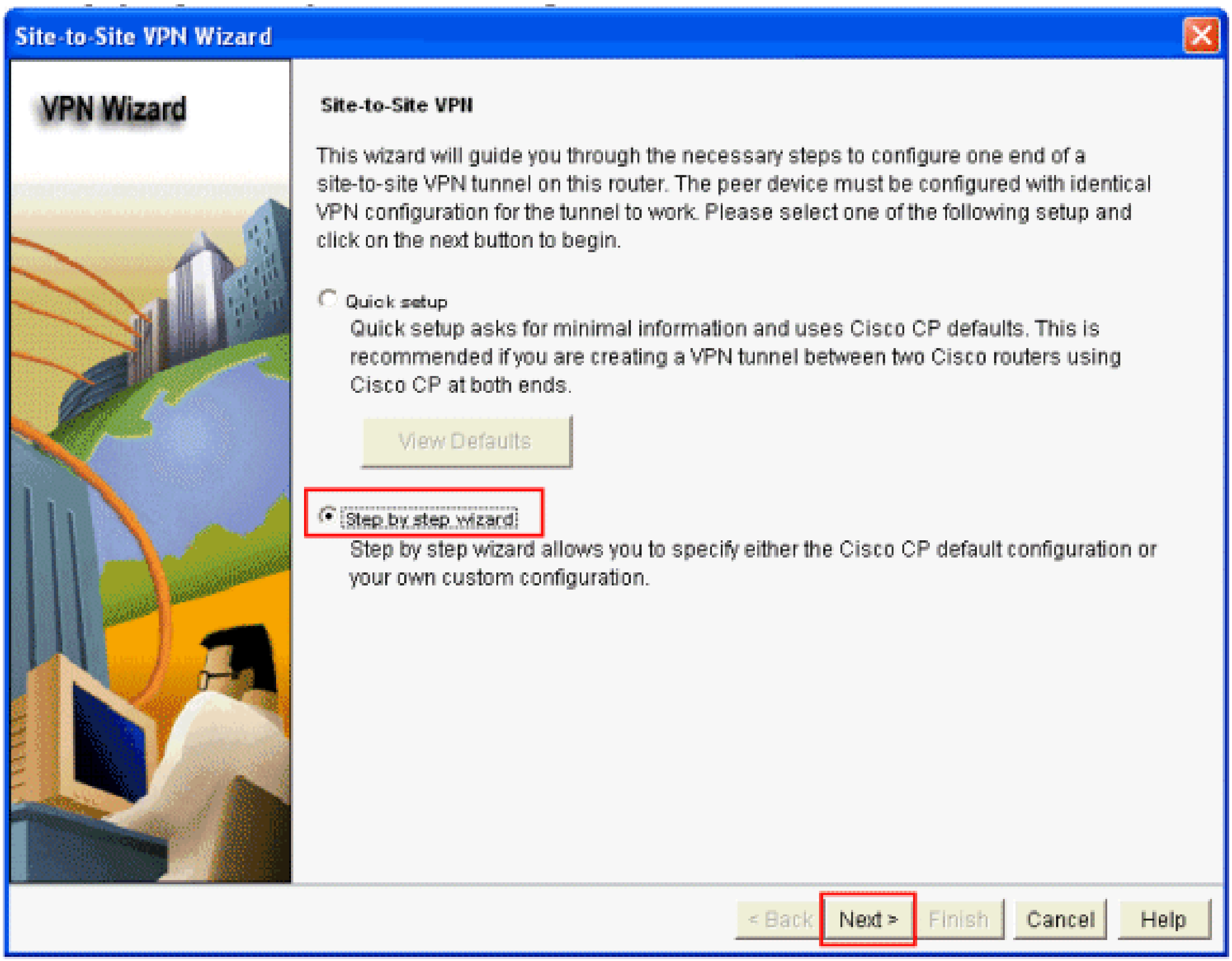
路由器 B Cisco CP 配置

要在 Cisco IOS 路由器（路由器 B）上配置站点到站点 VPN 隧道，请执行以下步骤：

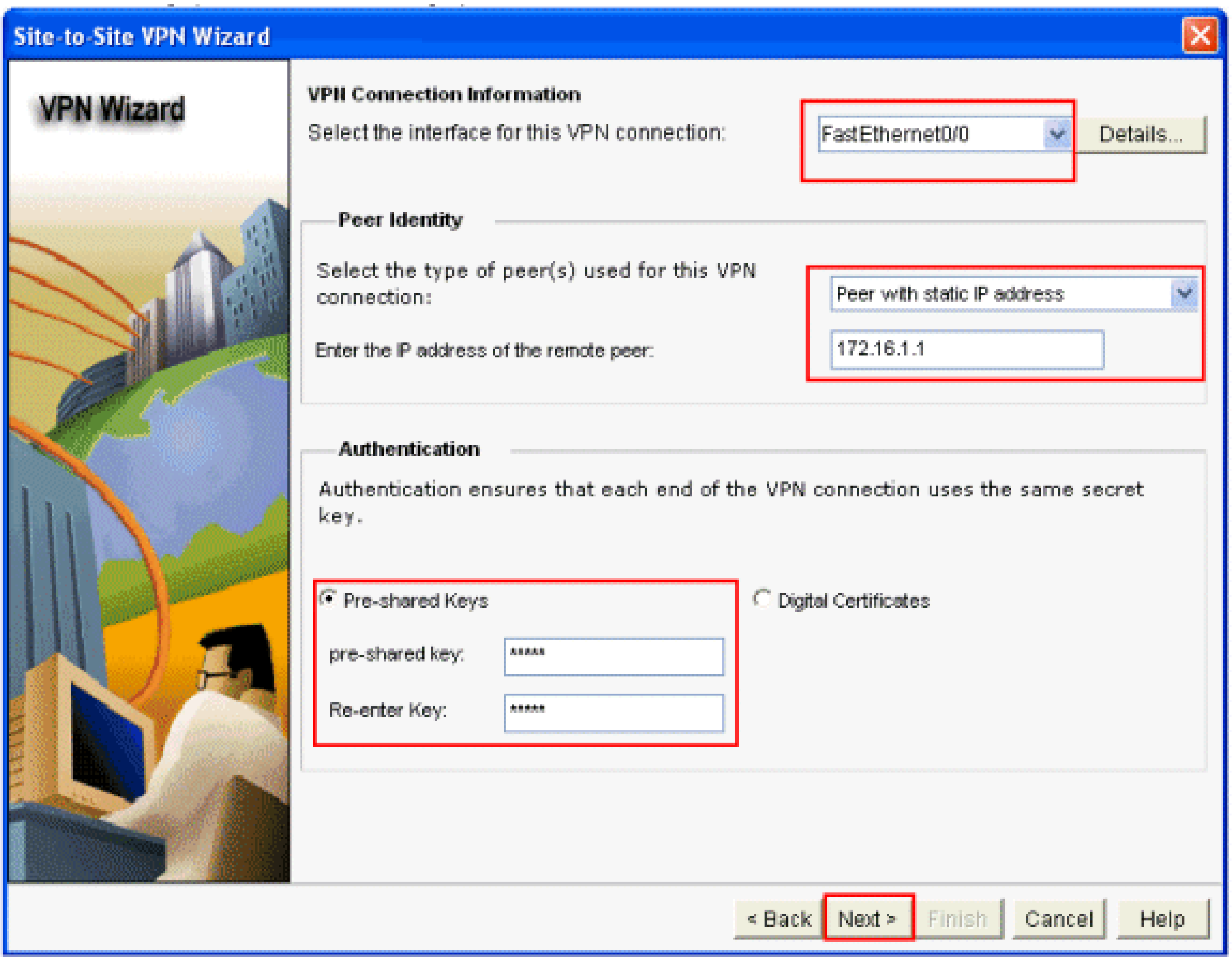
1. 选择 **Configure** > Security > **VPN** > **Site-to-Site VPN**，并单击 **Create a Site-to-Site VPN** 旁边的单选按钮。单击 **Launch the selected task**。



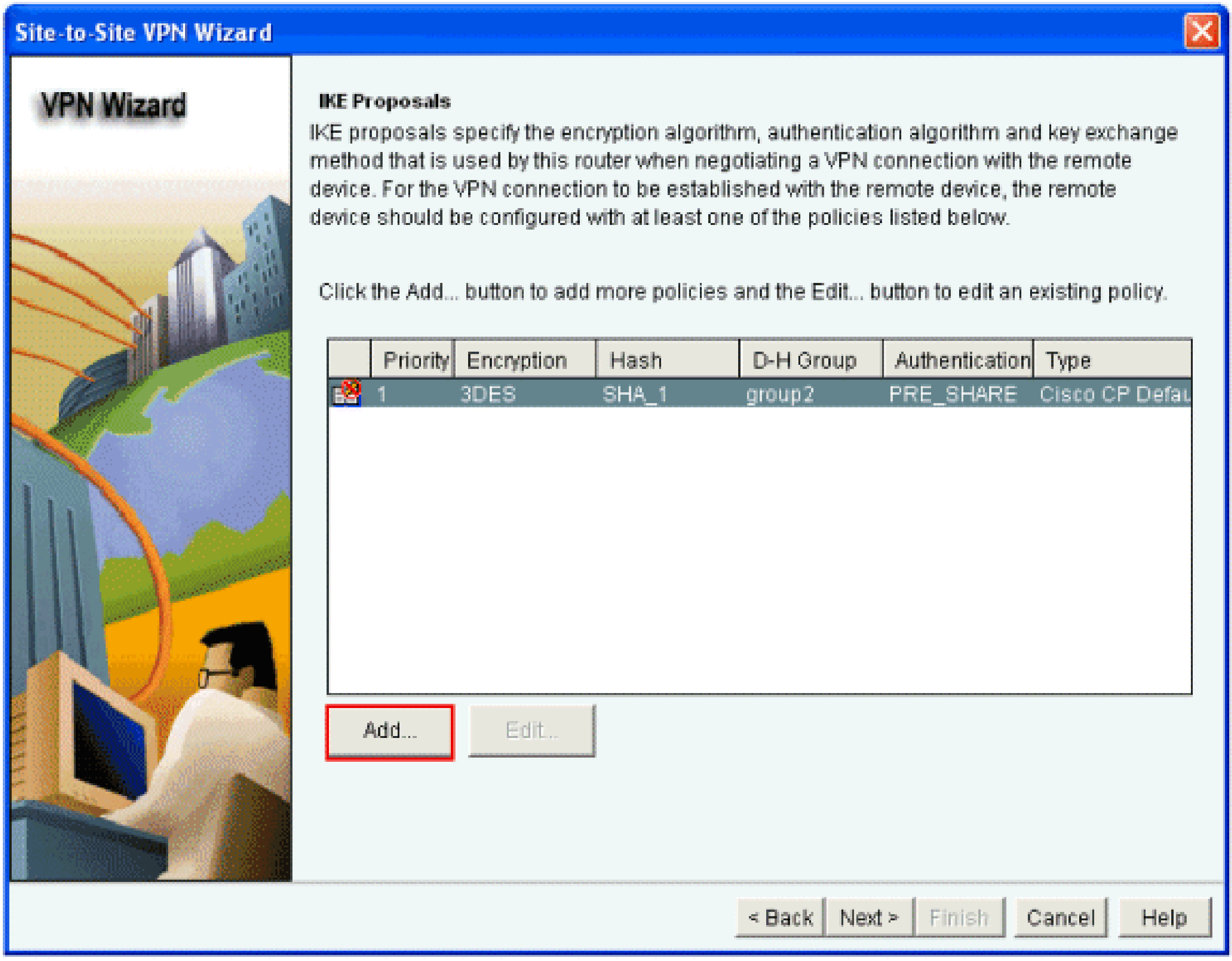
2. 选择 **Step by step wizard** 继续进行配置，然后单击 **Next**。



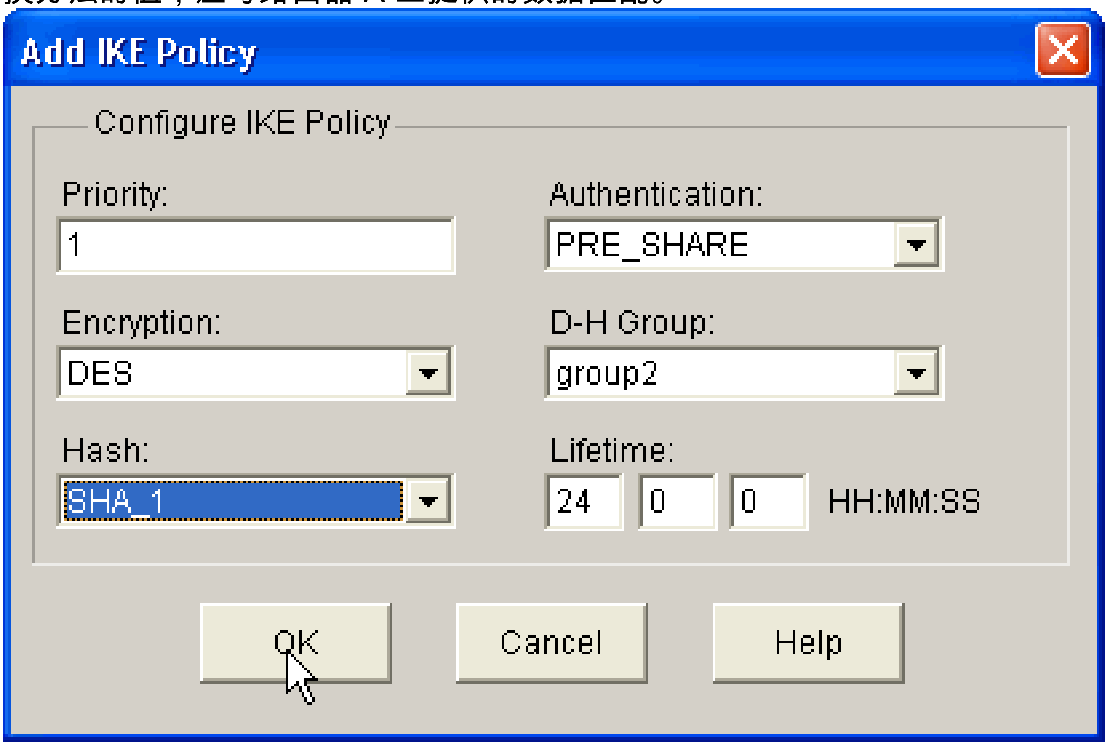
3. 在下一个窗口的相应空白处提供 VPN 连接信息。从下拉菜单中选择 VPN 隧道的接口。此处选择 **FastEthernet0**。在 **Peer Identity** 中，选择具有静态 IP 地址的对等体并提供远程对等体 IP 地址。然后，在 Authentication 部分中提供 Pre-shared Key（在本示例中为 *cisco123*）。最后，单击 **Next**。



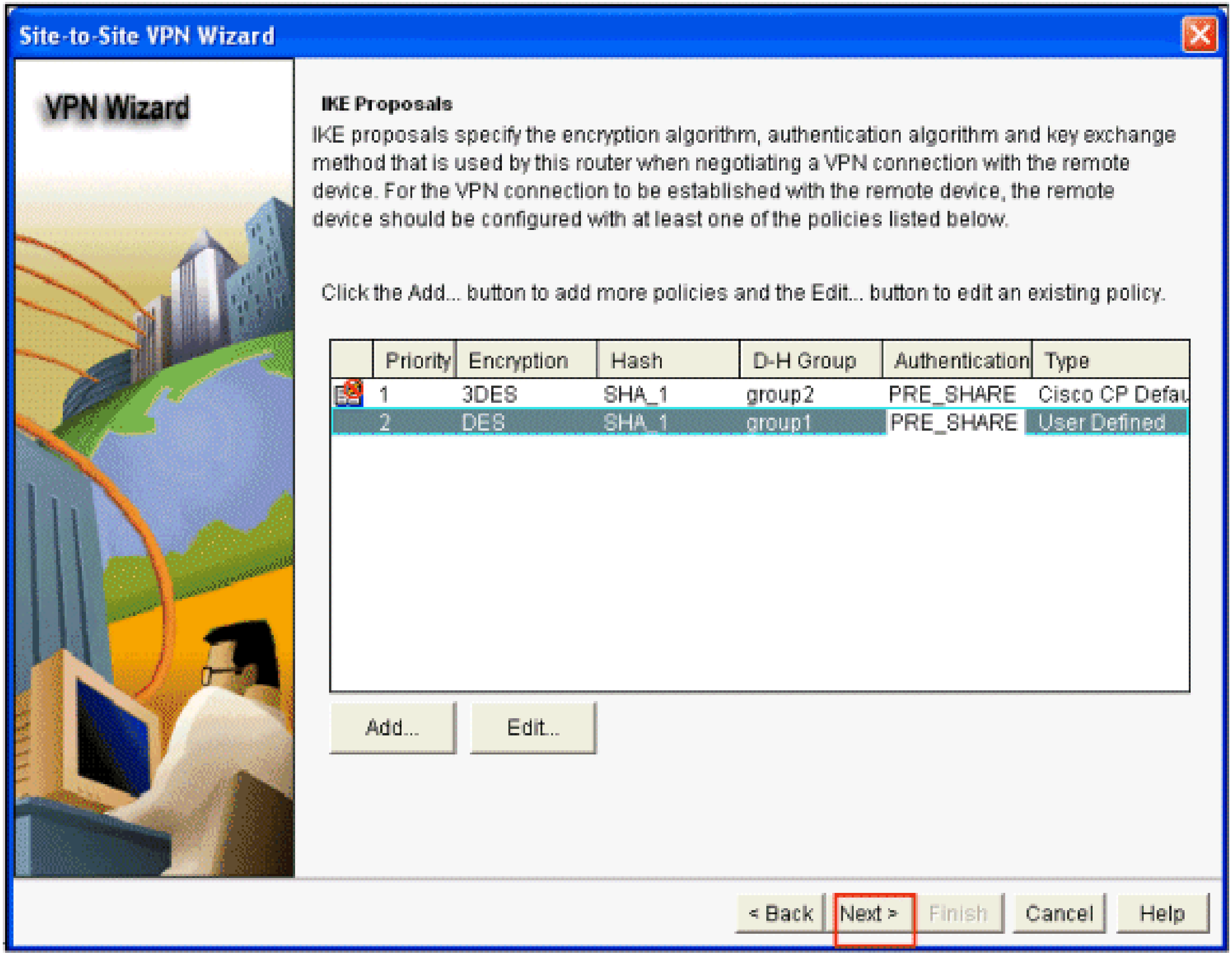
4. 单击 Add 添加指定加密算法、验证算法和密钥交换方法的 IKE 建议。



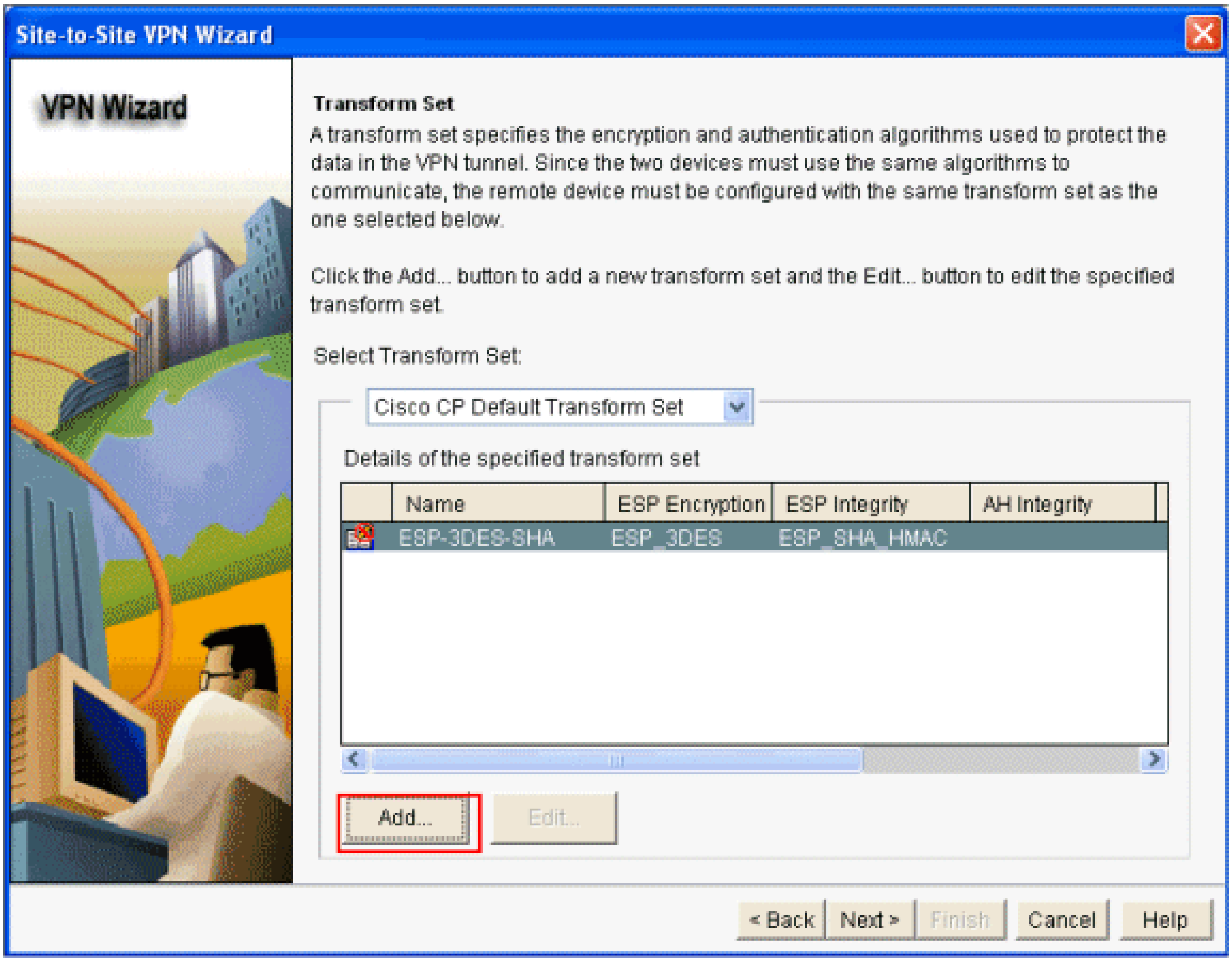
5. 提供加密算法、验证算法和密钥交换方法，然后单击 **OK**。加密算法、身份验证算法和密钥交换方法的值，应与路由器 A 上提供的数据匹配。



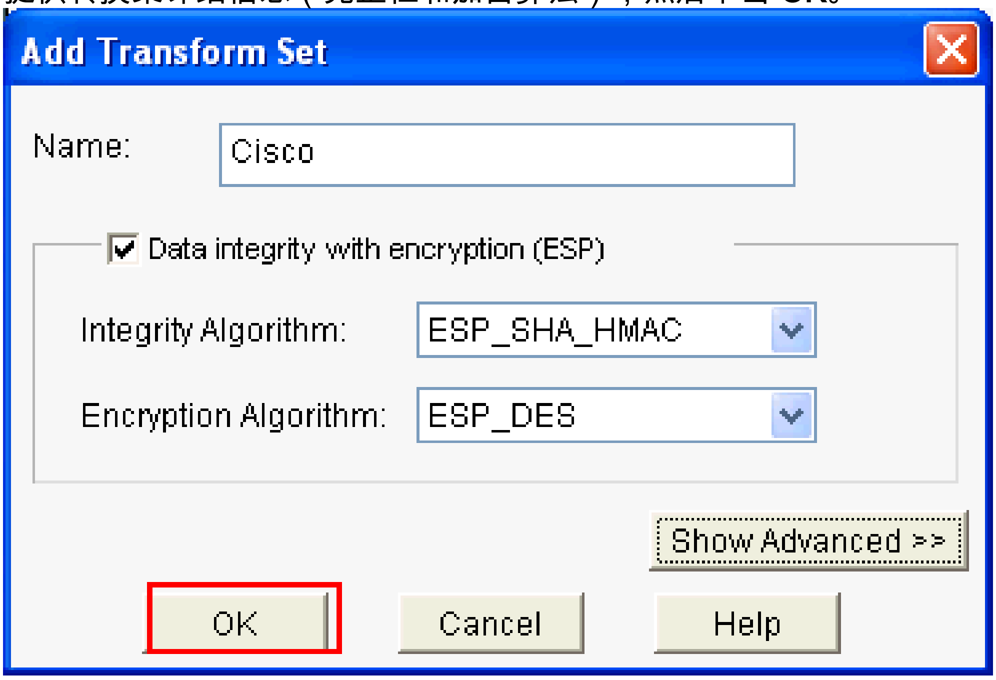
6. 单击 **Next**。



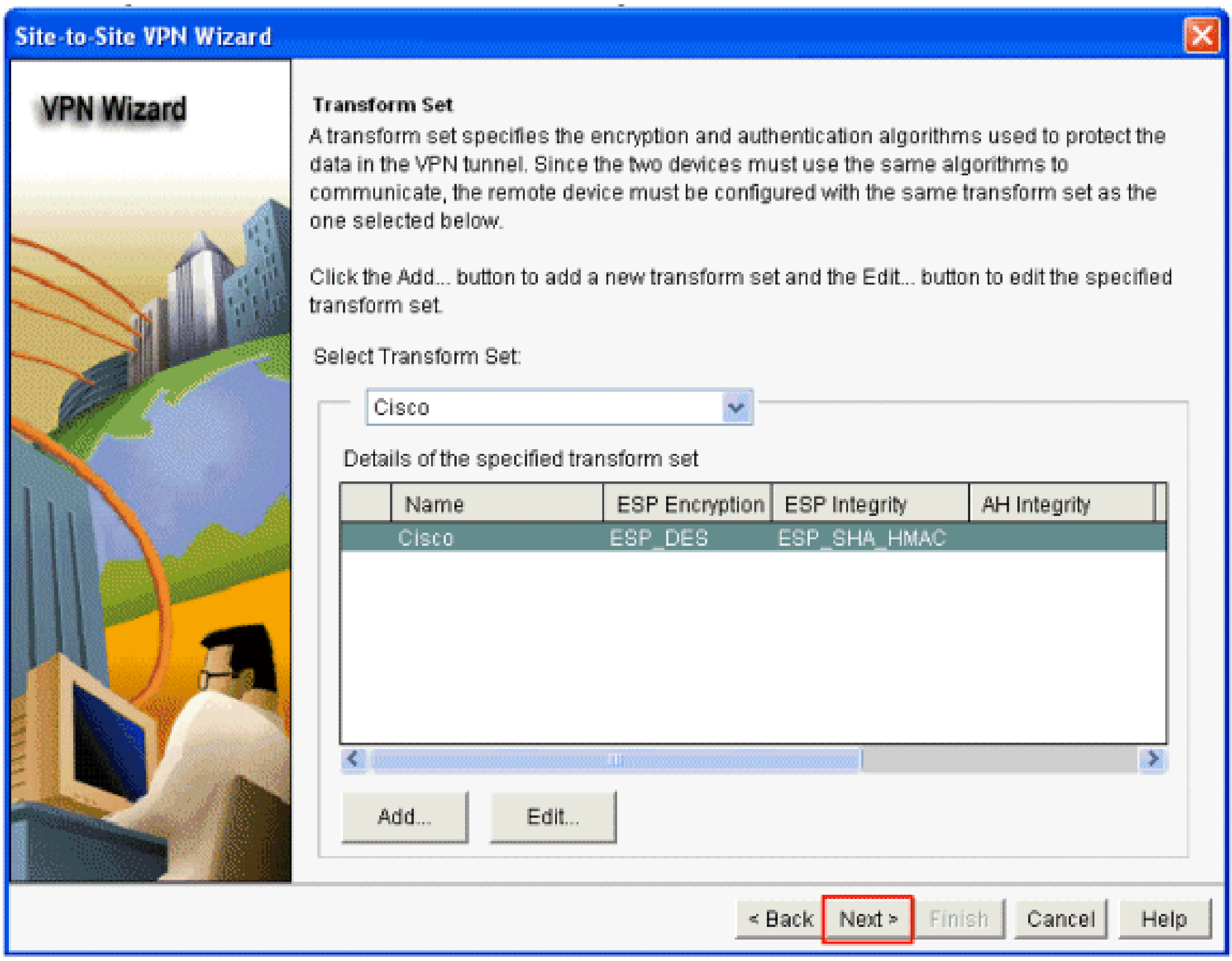
7. 在此新窗口中提供转换集详细信息。“转换集”指定用于保护 VPN 隧道中的数据的**加密**算法和验证算法。单击 **Add** 以提供这些详细信息。使用此方法可根据需要添加任意数量的转换集。



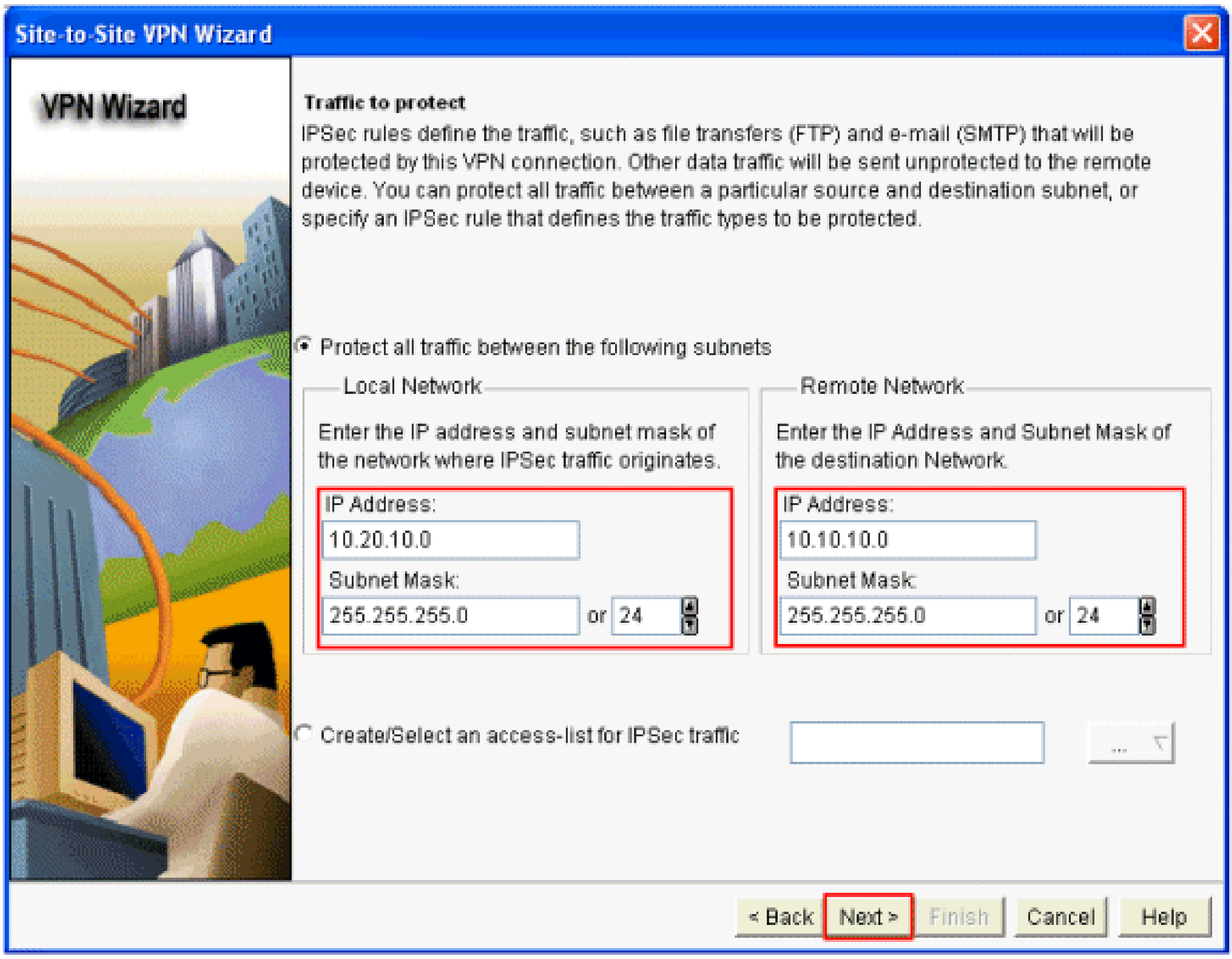
8. 提供转换集详细信息（完整性和加密算法），然后单击 **OK**。



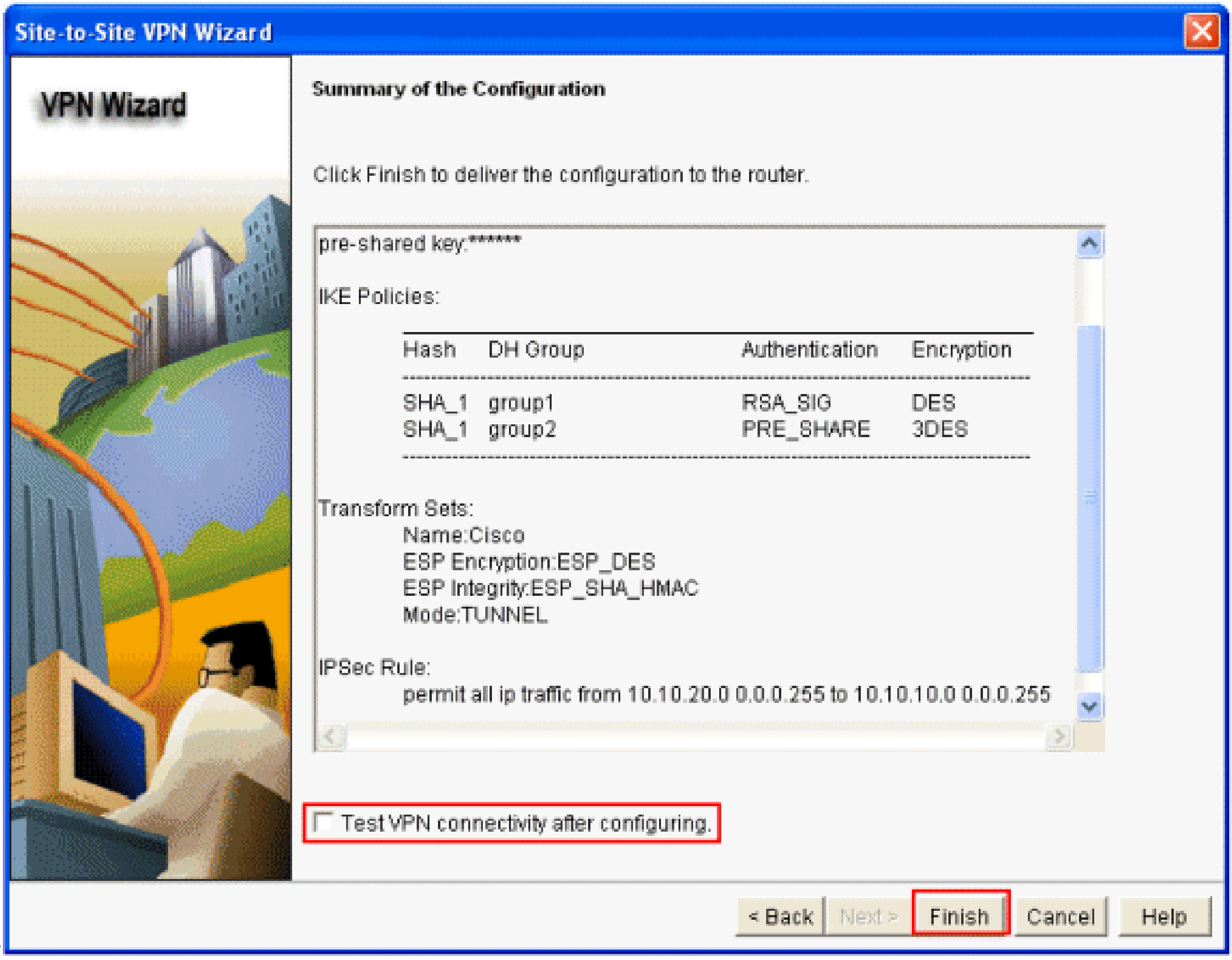
9. 从下拉菜单中选择所需的 **Transform Set**，然后单击 **Next**。



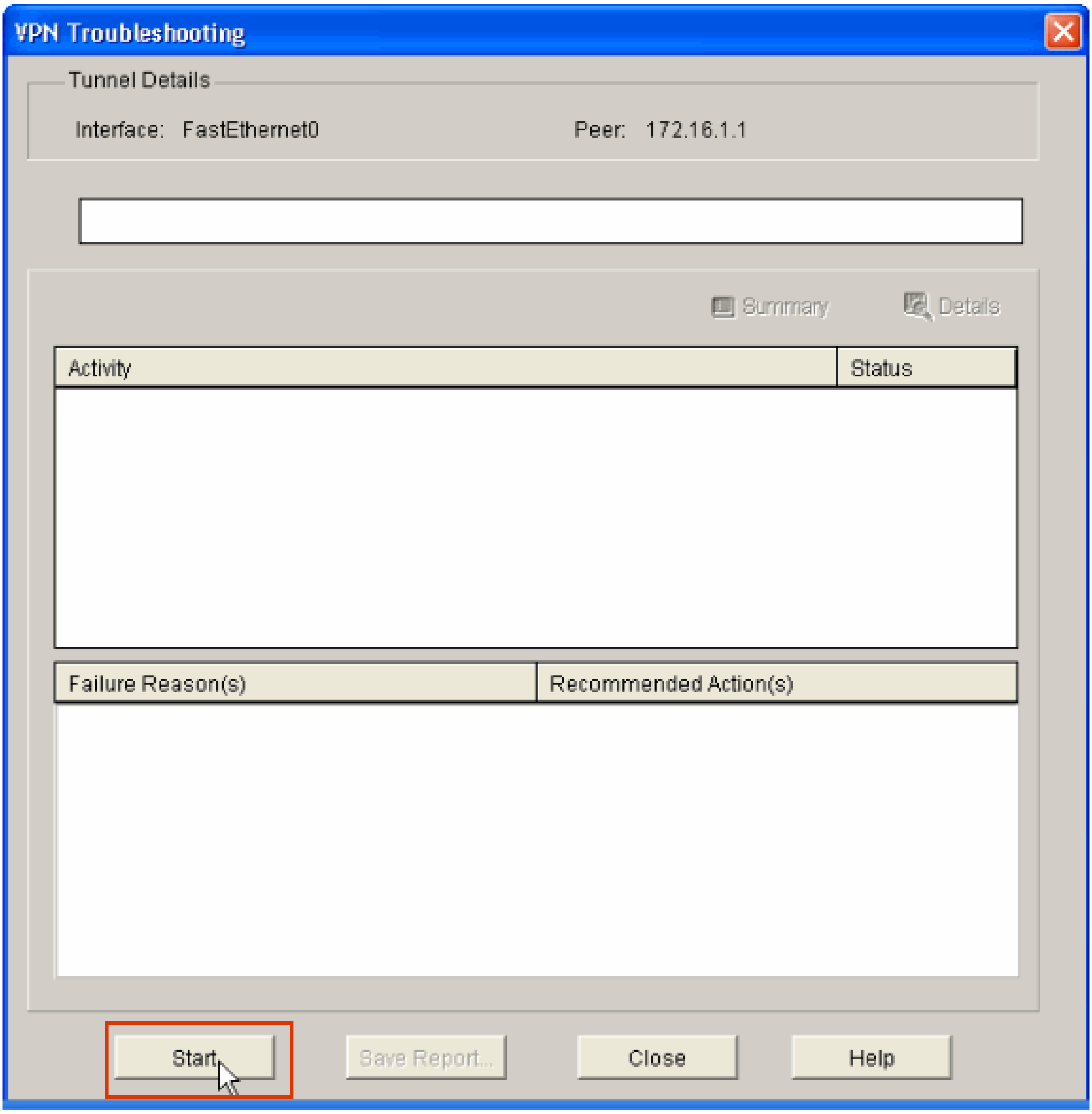
10. 在以下窗口中提供有关要保护的数据流（通过 VPN 隧道）的详细信息。提供要保护的数据流的**源网络和目标网络**，以便保护指定的源网络和目标网络之间的数据流。在本示例中，源网络是 10.20.10.0，目标网络是 10.10.10.0。单击 **Next**。



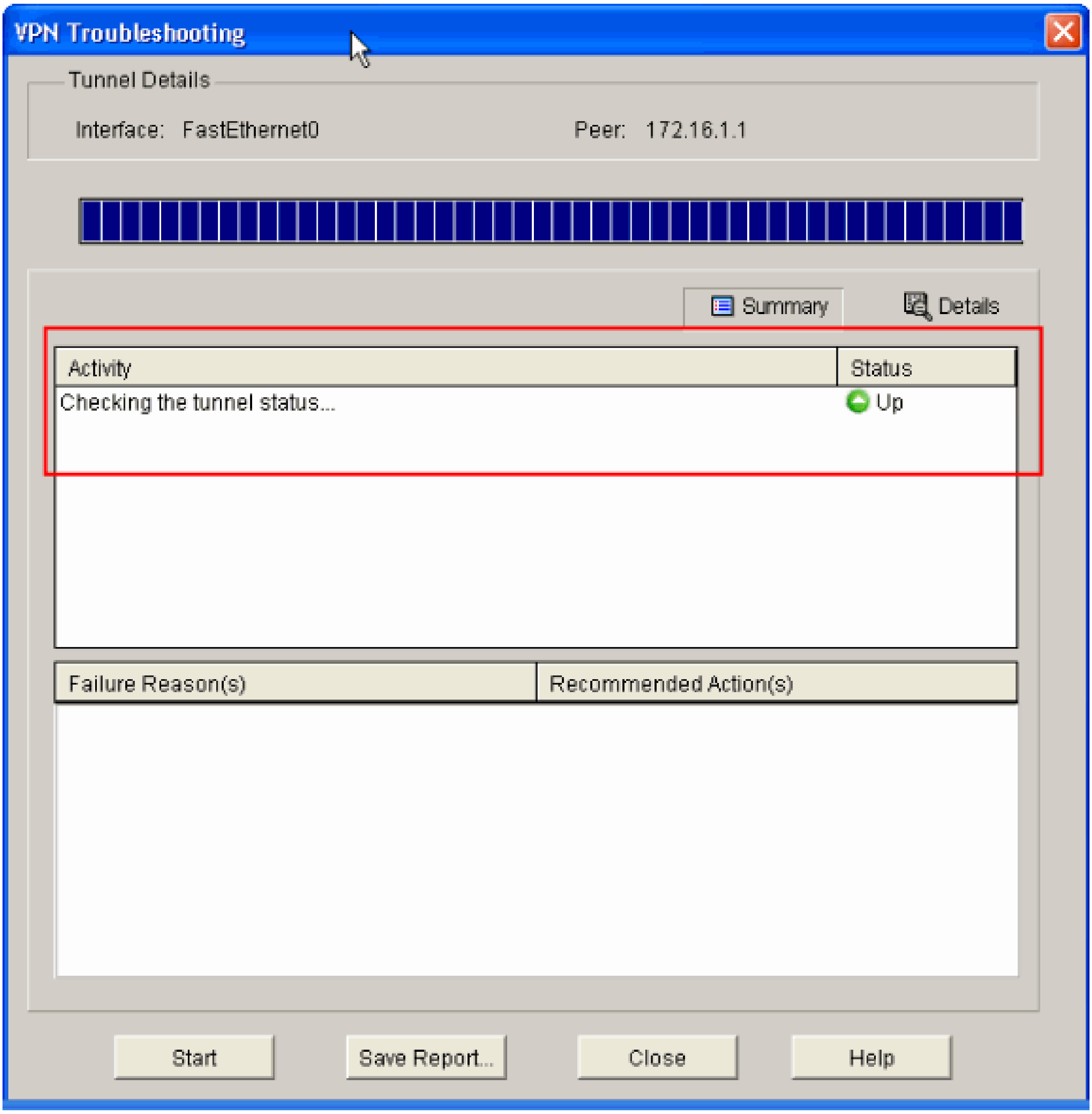
11. 此窗口显示站点到站点 VPN 配置的汇总。如果您要测试 VPN 连接性，请选中 **Test VPN Connectivity after configuring** 复选框。此处选中此框是因为需要检查连接性。单击 **完成**。



12. 单击 **Start** 以检查 VPN 连接性。



13. 下一个窗口中提供了 VPN 连接性测试的结果。您可以在此处看到隧道处于**启用还是禁用**状态。在此示例配置中，隧道处于“启用”状态，显示为绿色。



至此，Cisco IOS 路由器 B 配置完成，并显示隧道已建立。

路由器 B CLI 配置

路由器 B

```
Building configuration...

Current configuration : 2403 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R3
!
boot-start-marker
boot-end-marker
!
```

```
no logging buffered
!
username cisco123 privilege 15 password 7
1511021F07257A767B
no aaa new-model
ip subnet-zero
!
!
ip cef
!
!
ip ips po max-events 100
no ftp-server write-enable
!

!--- 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 2
 authentication pre-share

!--- Specifies the pre-shared key "cisco123" which
should !--- be identical at both peers. This is a global
!--- configuration mode command. crypto isakmp key
cisco123 address 172.16.1.1
!
!
!--- 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 Router-
IPSEC esp-des esp-sha-hmac
!

!--- Indicates that IKE is used to establish !--- the
IPsec Security Association for protecting the !---
traffic specified by this crypto map entry. crypto map
SDM_CMAP_1 1 ipsec-isakmp
 description Tunnel to172.16.1.1

!--- Sets the IP address of the remote end. set peer
172.16.1.1

!--- Configures IPsec to use the transform-set !---
"Router-IPSEC" defined earlier in this configuration.
set transform-set Router-IPSEC

!--- Specifies the interesting traffic to be encrypted.
match address 100
!
!
!
!--- Configures the interface to use the !--- crypto map
"SDM_CMAP_1" for IPsec. interface FastEthernet0 ip
address 172.17.1.1 255.255.255.0 duplex auto speed auto
crypto map SDM_CMAP_1
!
interface FastEthernet1
 ip address 10.20.10.2 255.255.255.0
 duplex auto
 speed auto
!
```

```
interface FastEthernet2
 no ip address
!
interface Vlan1
 ip address 10.77.241.109 255.255.255.192
!
ip classless
ip route 10.10.10.0 255.255.255.0 172.17.1.2
ip route 10.77.233.0 255.255.255.0 10.77.241.65
ip route 172.16.1.0 255.255.255.0 172.17.1.2
!
!
ip nat inside source route-map nonat interface
FastEthernet0 overload
!
ip http server
ip http authentication local
ip http secure-server
!
!--- Configure the access-lists and map them to the
Crypto map configured. access-list 100 remark SDM_ACL
Category=4
access-list 100 remark IPSec Rule
access-list 100 permit ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255
!
!
!
!--- This ACL 110 identifies the traffic flows using
route map access-list 110 deny ip 10.20.10.0 0.0.0.255
10.10.10.0 0.0.0.255
access-list 110 permit ip 10.20.10.0 0.0.0.255 any
route-map nonat permit 10
 match ip address 110
!
control-plane
!
!
line con 0
 login local
line aux 0
line vty 0 4
 privilege level 15
 login local
 transport input telnet ssh
!
end
```

Verify

Use this section to confirm that your configuration works properly.

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- IOS 路由器 - **show** 命令

IOS 路由器 - show 命令

- **show crypto isakmp sa** - 显示对等体上的所有当前 IKE SA。

```
RouterB# show crypto isakmp sa

dst             src             state          conn-id slot status
172.17.1.1      172.16.1.1      QM_IDLE              3    0 ACTIVE
```

- **show crypto ipsec sa** — 显示对等体上的所有当前 IPsec SA。

```
RouterB# show crypto ipsec sa
interface: FastEthernet0
    Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
   current_peer 172.16.1.1 port 500
     PERMIT, flags={origin_is_acl,}
  #pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68
    #pkts decaps: 68, #pkts decrypt: 68, #pkts verify: 68
    #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 0

     local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
     path mtu 1500, ip mtu 1500
     current outbound spi: 0xB7C1948E(3082917006)

     inbound esp sas:
      spi: 0x434C4A7F(1129073279)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2001, flow_id: C18XX_MBRD:1, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4578719/3004)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0xB7C1948E(3082917006)
        transform: esp-des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2002, flow_id: C18XX_MBRD:2, crypto map: SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4578719/3002)
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

     outbound pcp sas:
```

- **show crypto engine connections active** - 显示当前连接及关于加密和解密数据包的信息。

```
RouterB#show crypto engine connections active

  ID Interface        IP-Address      State  Algorithm           Encrypt  Decrypt
   3 FastEthernet0    172.17.1.1      set    HMAC_SHA+DES_56_CB        0        0
2001 FastEthernet0    172.17.1.1      set    DES+SHA                   0       59
2002 FastEthernet0    172.17.1.1      set    DES+SHA                  59        0
```

Troubleshoot

本部分提供的信息可用于对配置进行故障排除。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

Note: 请先阅读关于调试命令的重要信息和IP 安全故障排除：理解和使用调试命令，再使用 **debug** 命令。

- **debug crypto ipsec 7** - 显示第 2 阶段的 IPsec 协商。**debug crypto isakmp 7** - 显示第 1 阶段的 ISAKMP 协商。
- **debug crypto ipsec** - 显示第 2 阶段的 IPsec 协商。**debug crypto isakmp** - 显示第 1 阶段的 ISAKMP 协商。

Related Information

- Cisco Configuration Professional 快速入门指南
- 请求注解 (RFC)
- Technical Support & Documentation - Cisco Systems