

SDM : 在ASA/PIX和IOS路由器之间的站点至站点IPSec VPN配置示例

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[相关产品](#)

[规则](#)

[配置](#)

[网络图](#)

[VPN 隧道 ASDM 配置](#)

[路由器 SDM 配置](#)

[ASA CLI 配置](#)

[路由器 CLI 配置](#)

[验证](#)

[ASA/PIX 安全设备 - show 命令](#)

[远程 IOS 路由器 - show 命令](#)

[故障排除](#)

[相关信息](#)

简介

本文档提供 Cisco 安全设备 (ASA/PIX) 和 Cisco IOS 路由器之间的 LAN 到 LAN (站点到站点) IPsec 隧道的示例配置。为了简单起见，使用静态路由。

要了解有关 PIX/ASA 安全设备运行软件版本 7.x 的相同方案的详细信息，请参阅 [PIX/ASA 7.x 安全设备到 IOS 路由器 LAN 到 LAN IPsec 隧道配置示例](#)。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 必须建立端到端 IP 连接才能开始此配置。
- 必须为数据加密标准 (DES) 加密 (在最低加密级别) 启用安全设备许可证。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco 自适应安全设备 (ASA) 版本 8.x 及更高版本
- ASDM 版本 6.x. 及更高版本
- 使用 Cisco IOS® 软件版本 12.3 的 Cisco 1812 路由器
- Cisco 安全设备管理器 (SDM) 版本 2.5

注意：要使 ASDM 可配置 ASA，请参阅[允许 ASDM 进行 HTTPS 访问](#)。

注意：为了允许使用 SDM 配置路由器，请参阅[使用 SDM 执行基本路由器配置](#)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

注意：参考的[配置专业人员：在ASA/PIX和IOS路由器配置示例之间的站点至站点IPSec VPN](#)一相似的配置的使用路由器的Cisco Configuration Professional。

相关产品

此配置也可用于 Cisco PIX 500 系列安全设备，这些设备运行版本 7.x 及更高版本。

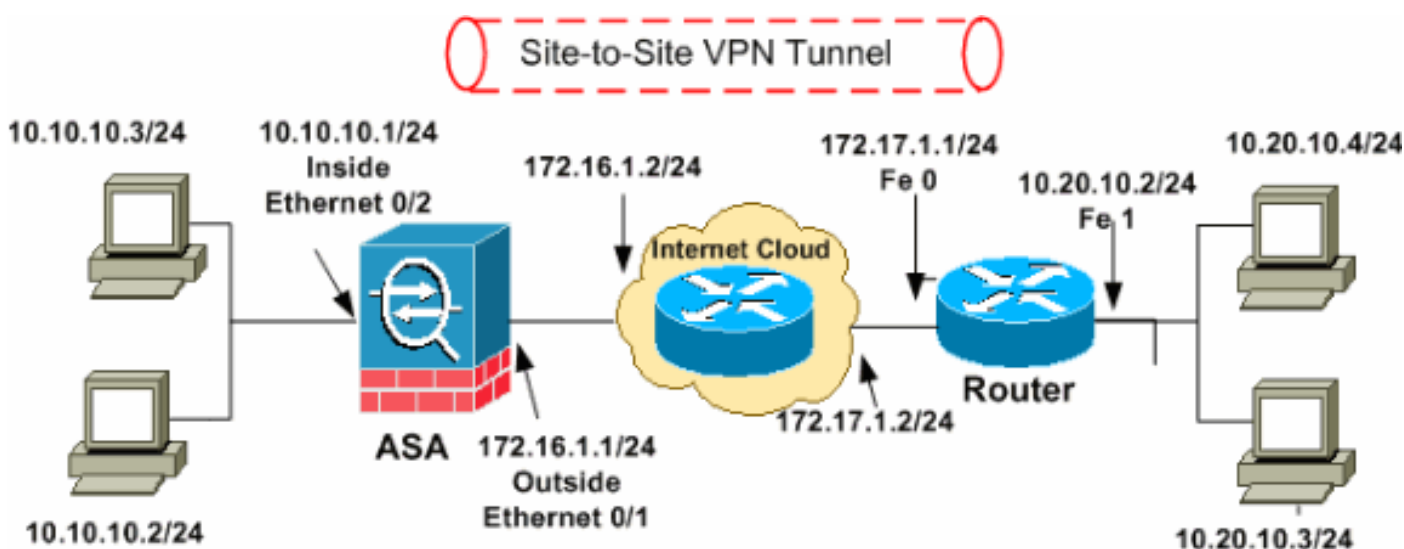
规则

有关文档规则的详细信息，请参阅[Cisco 技术提示规则](#)。

配置

网络图

本文档使用此图所示的网络设置。



注意：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。

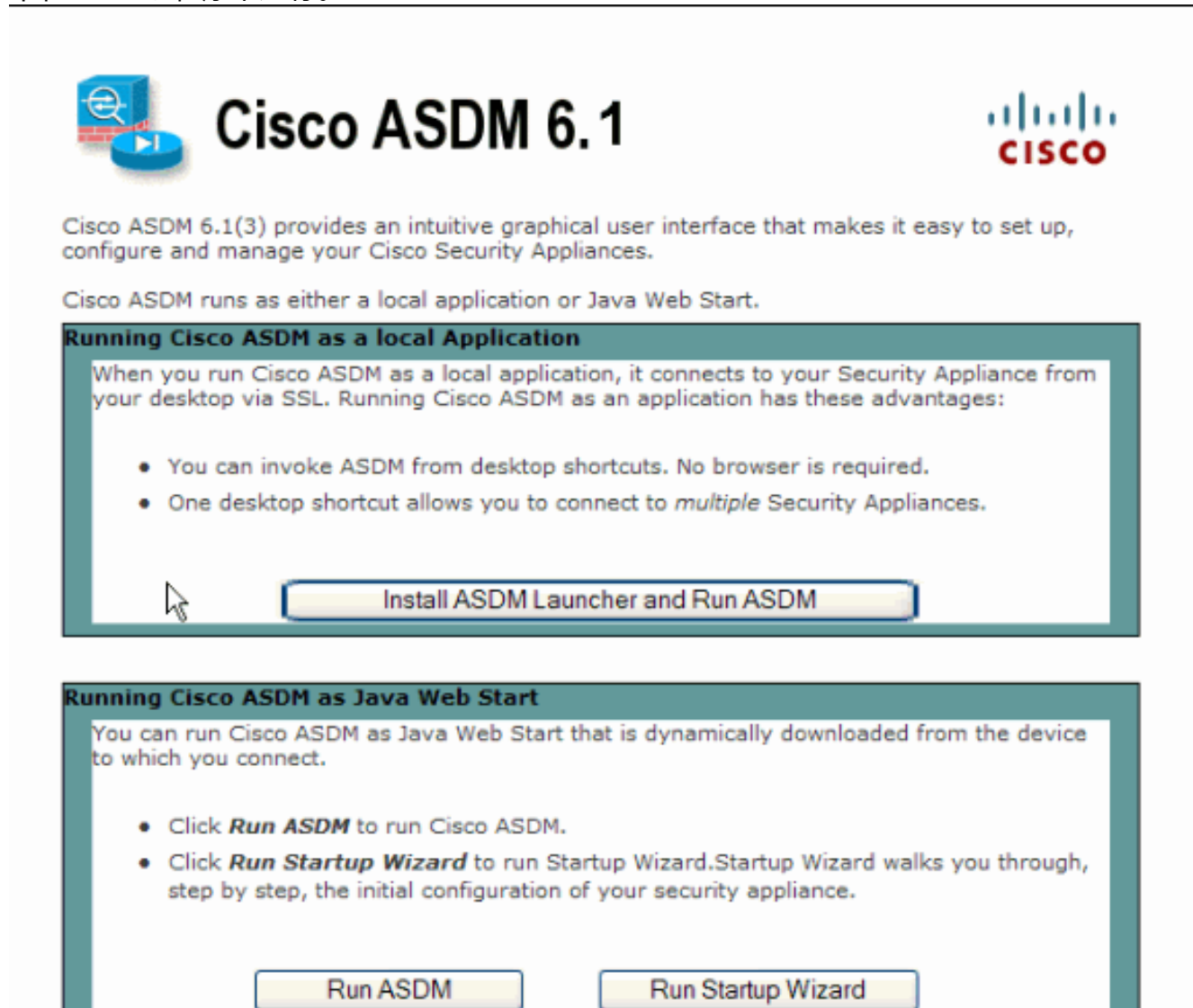
- [VPN 隧道 ASDM 配置](#)
- [路由器 SDM 配置](#)

- [ASA CLI 配置](#)
- [路由器 CLI 配置](#)

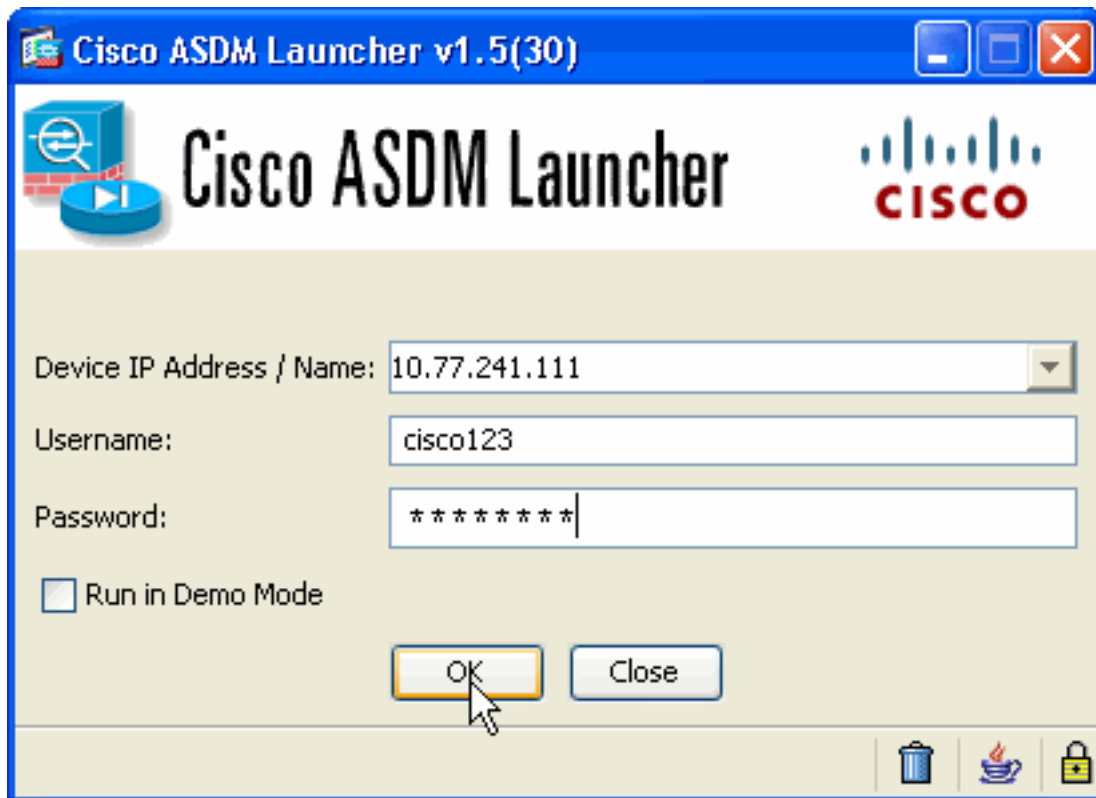
VPN 隧道 ASDM 配置

完成下列步骤以创建 VPN 隧道：

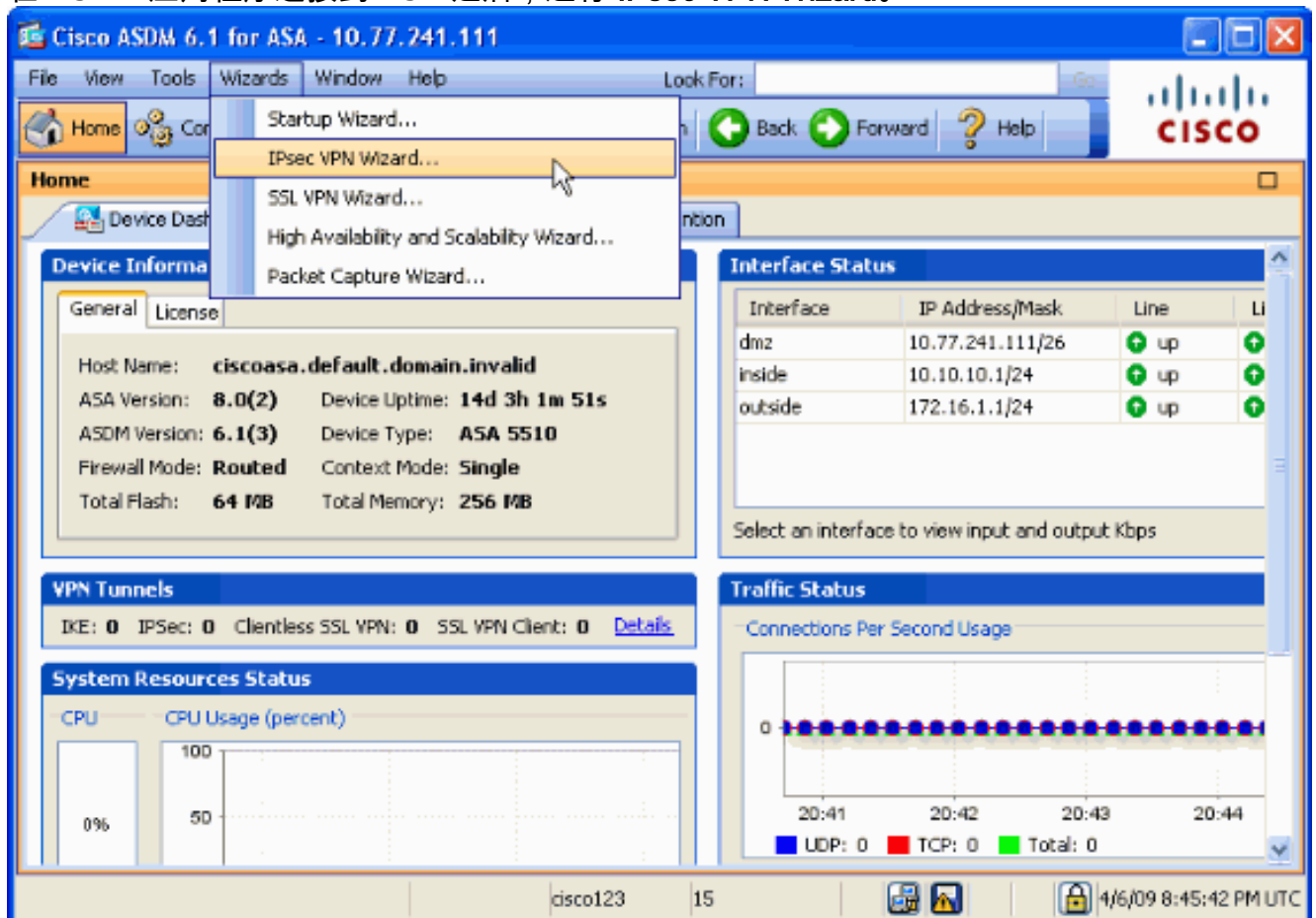
1. 打开浏览器并输入 <https://<为访问 ASDM 而配置的 ASA 接口的 IP 地址>>，以访问 ASA 上的 ASDM。确保核准浏览器提供的有关 SSL 证书真实性的任何警告。默认的用户名和口令均为空。ASA 显示此窗口以允许下载 ASDM 应用程序。此示例将应用程序加载到本地计算机，但不在 Java 小程序中运行。



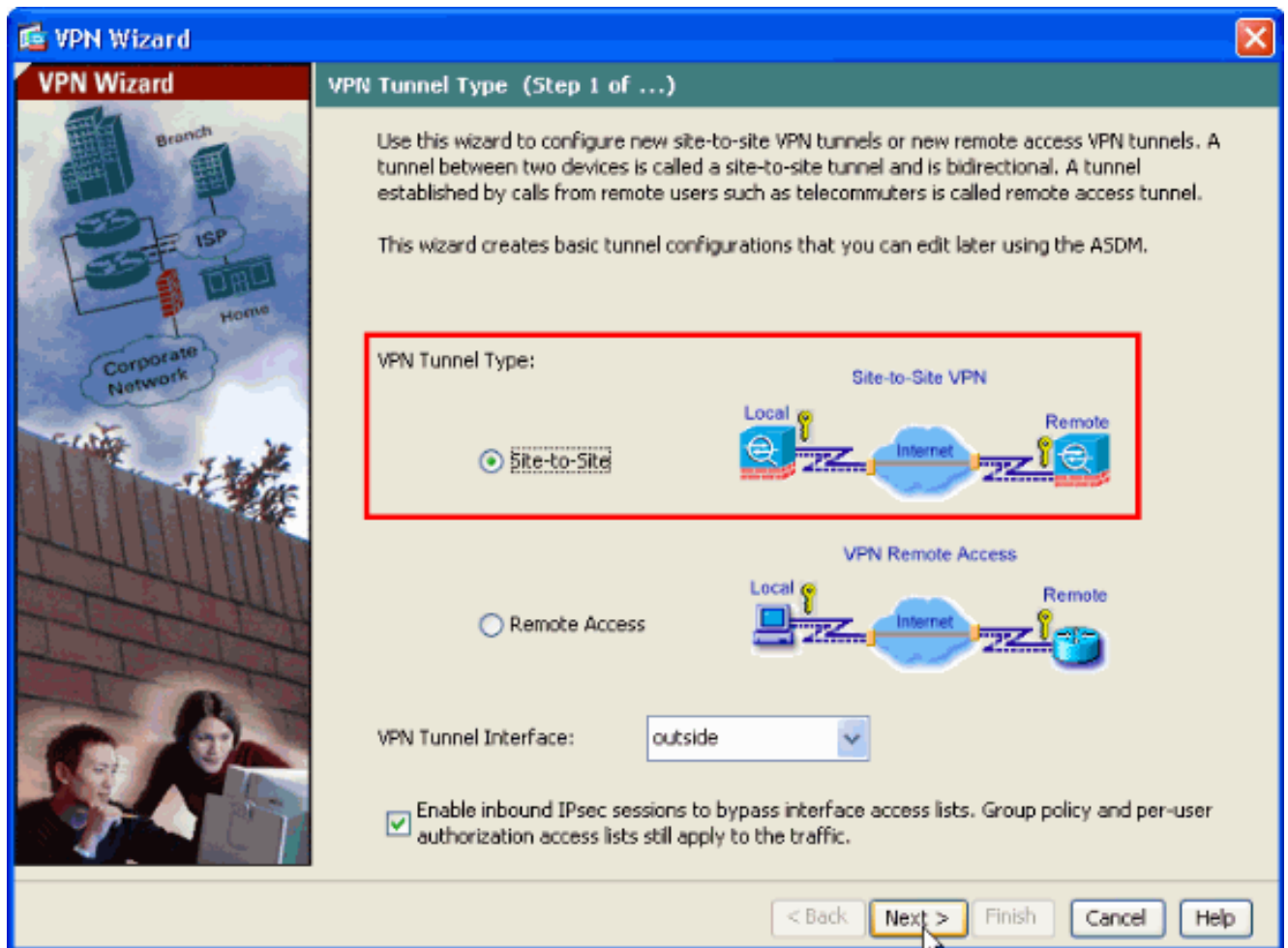
2. 单击 **Download ASDM Launcher and Start ASDM** 以下载 ASDM 应用程序的安装程序。
3. 下载 ASDM 启动程序之后，完成提示所指示的步骤，以便安装该软件并运行 Cisco ASDM 启动程序。
4. 输入使用 **http** - 命令配置的接口的 IP 地址，以及用户名和口令（如果已指定）。此示例使用 **cisco123** 作为用户名并使用 **cisco123** 作为口令。



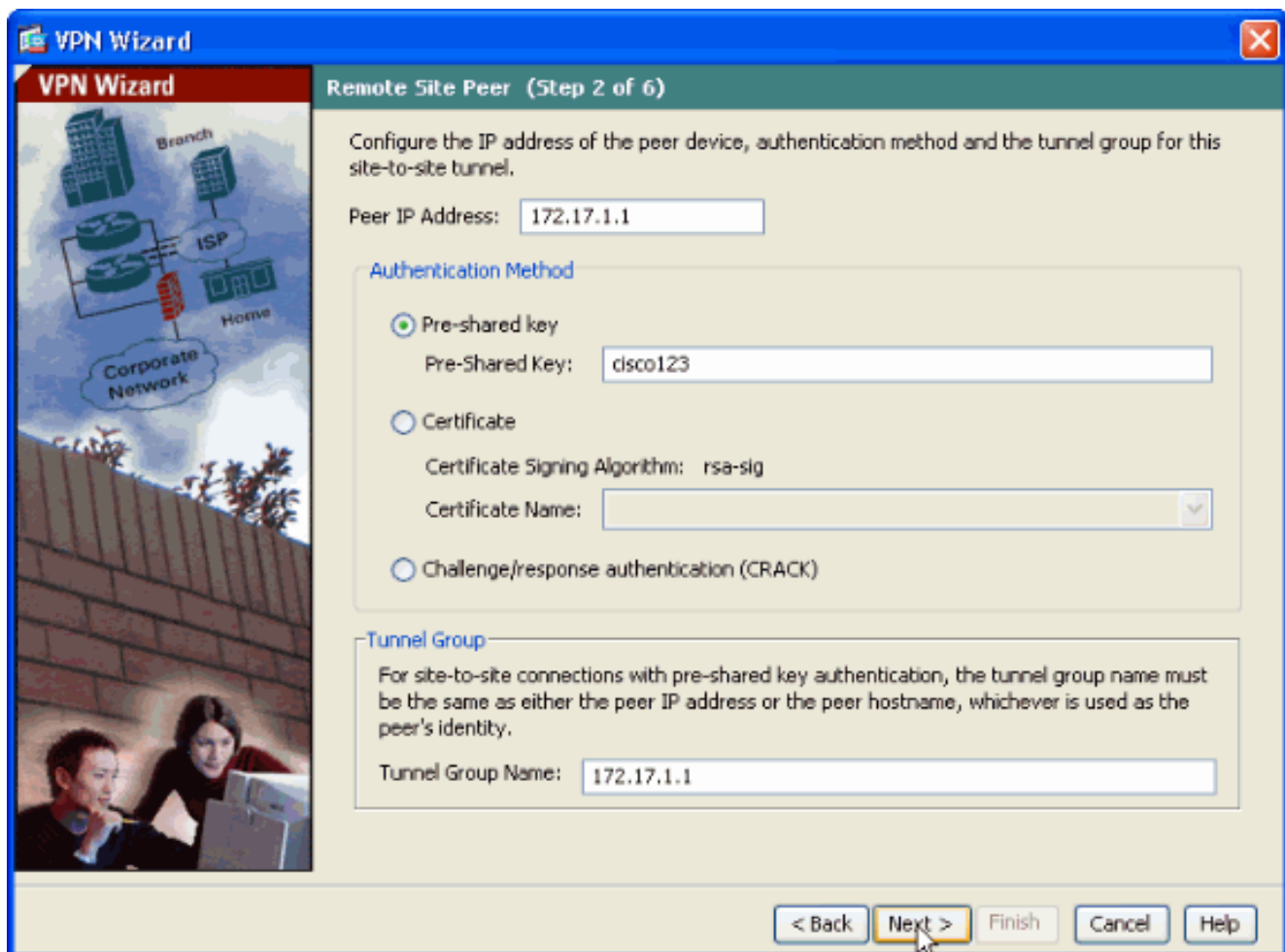
5. 在 ASDM 应用程序连接到 ASA 之后，运行 IPsec VPN Wizard。



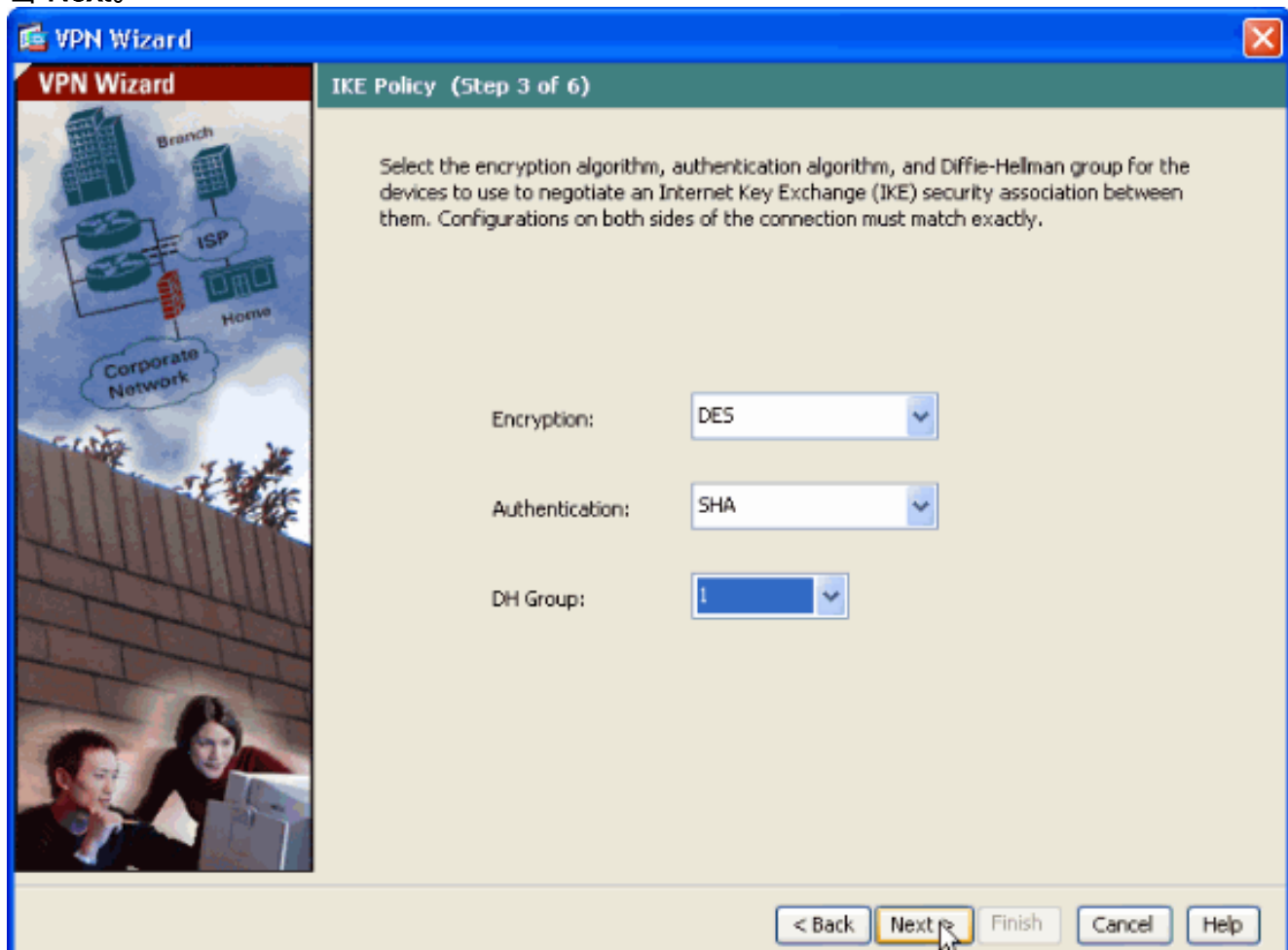
6. 选择 Site-to-Site IPsec VPN 隧道类型，然后单击 Next (如图所示)。



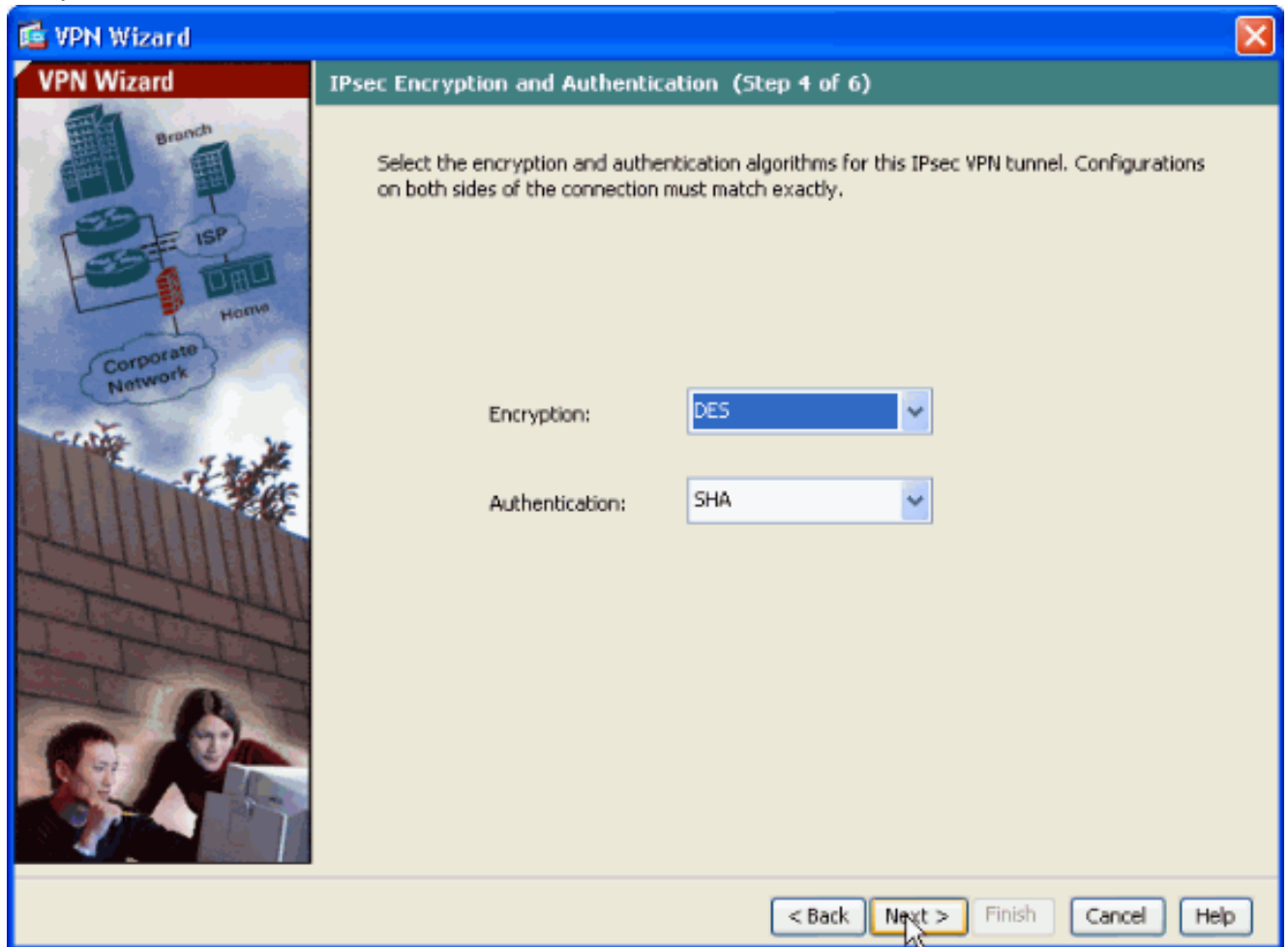
7. 指定远程对等体的外部 IP 地址。输入要使用的身份验证信息，在本示例中是预共享密钥。本示例中使用的预共享密钥是 **cisco123**。如果您配置 L2L VPN，默认情况下 **Tunnel Group Name** 将是外部 IP 地址。单击 **Next**。



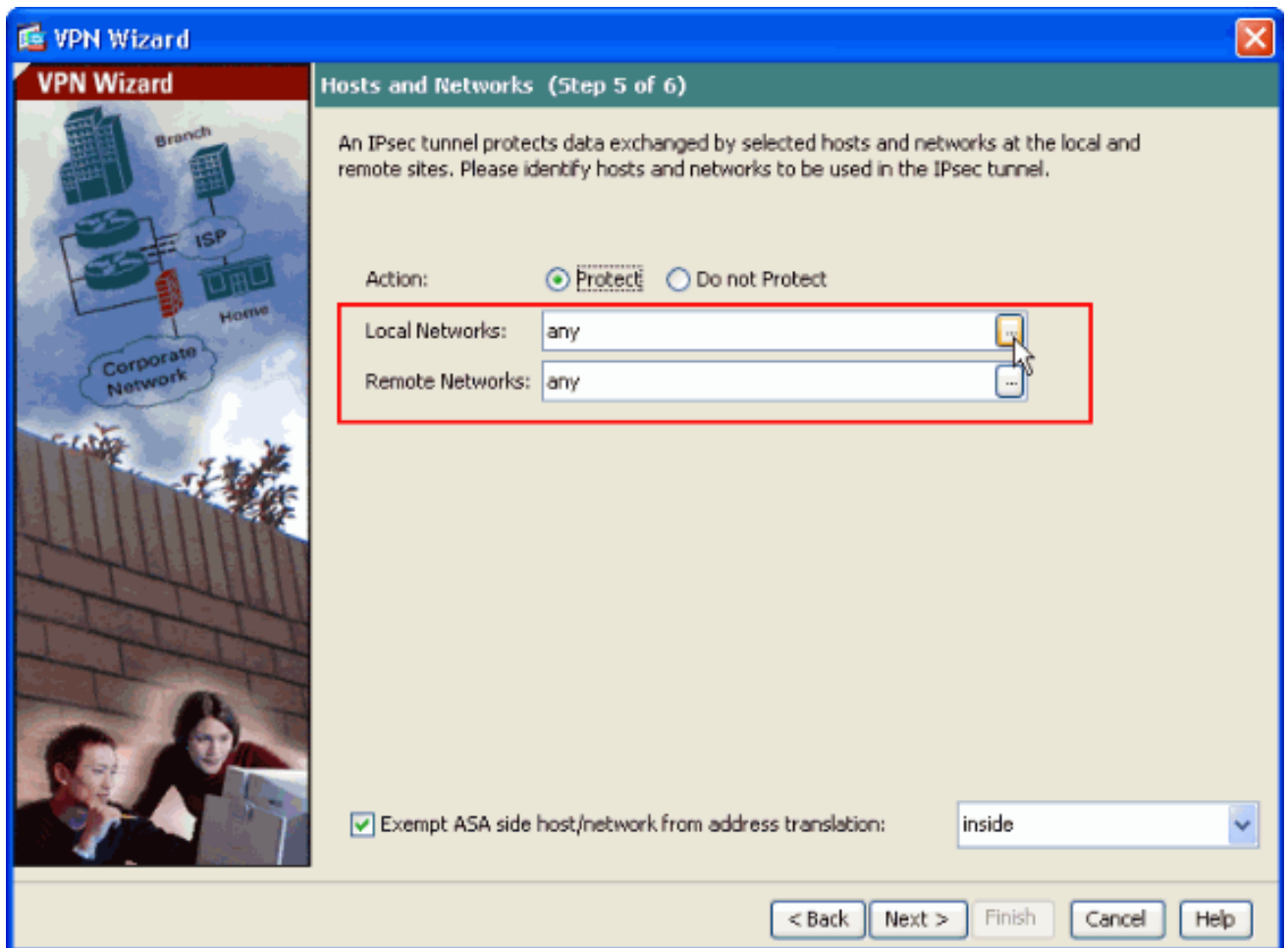
8. 指定要用于 IKE 的属性，也称为“第 1 阶段”。这些属性在 ASA 和 IOS 路由器上必须相同。单击 Next。



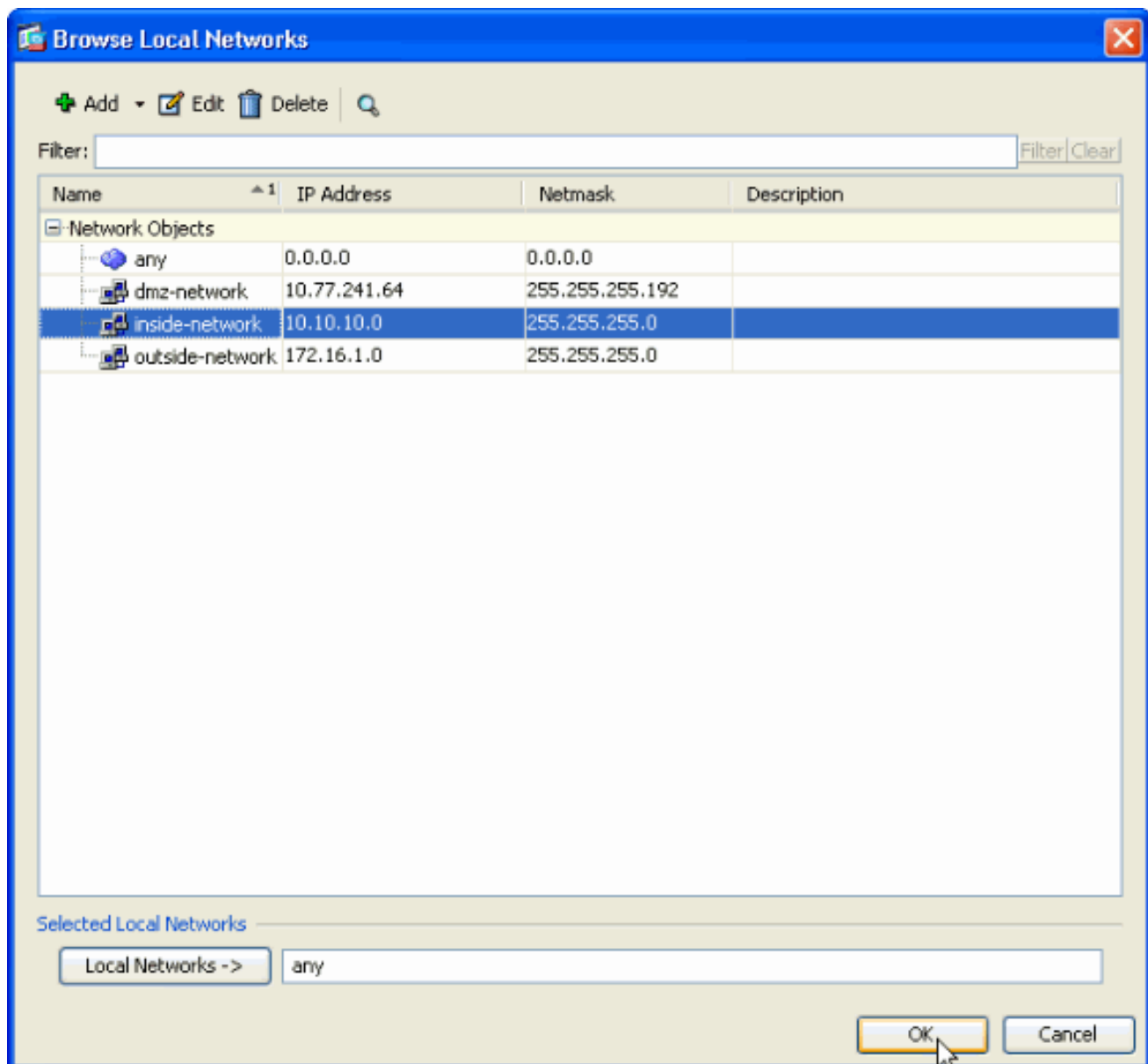
9. 指定要用于 IPsec 的属性，也称为“第 2 阶段”。这些属性在 ASA 和 IOS 路由器上必须匹配。
单击 **Next**。



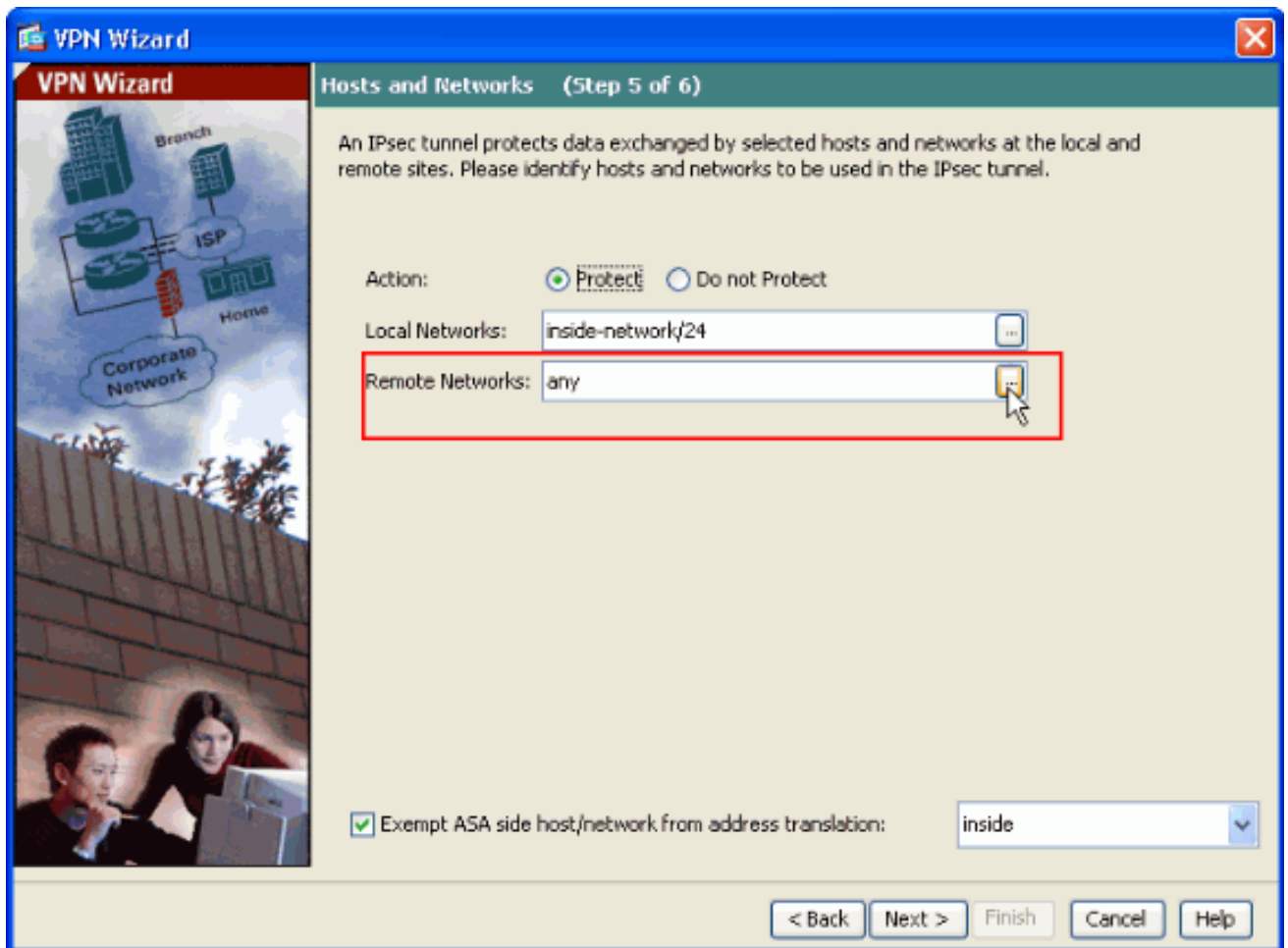
10. 指定应允许其数据流通过 VPN 隧道的主机。在此步骤中，必须提供 VPN 隧道的**本地和远程网络**。单击 **Local Networks** 旁边的按钮（如图所示），从下拉列表中选择本地网络地址。



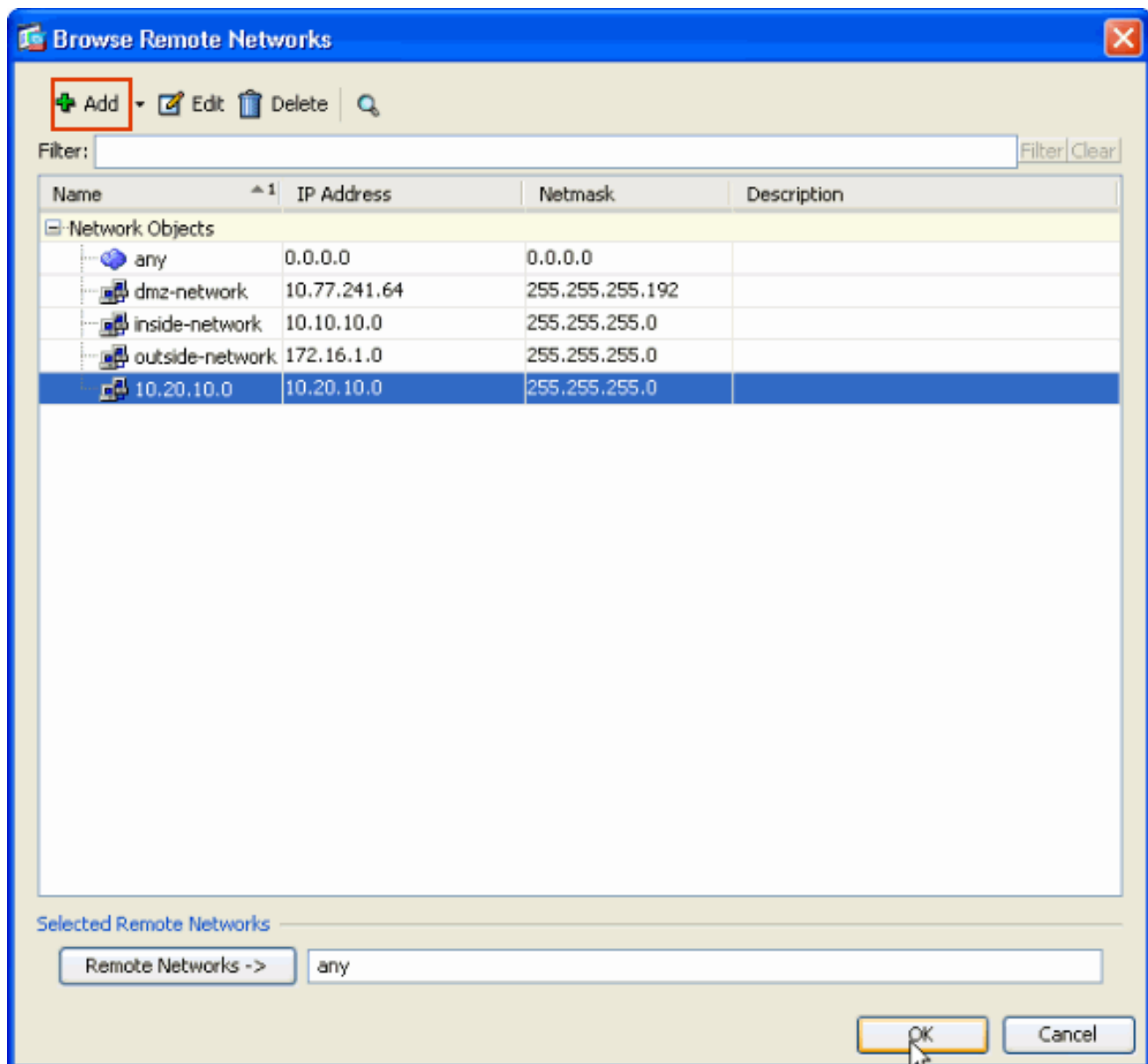
11. 选择 Local Network 地址，然后单击 OK（如图所示）。



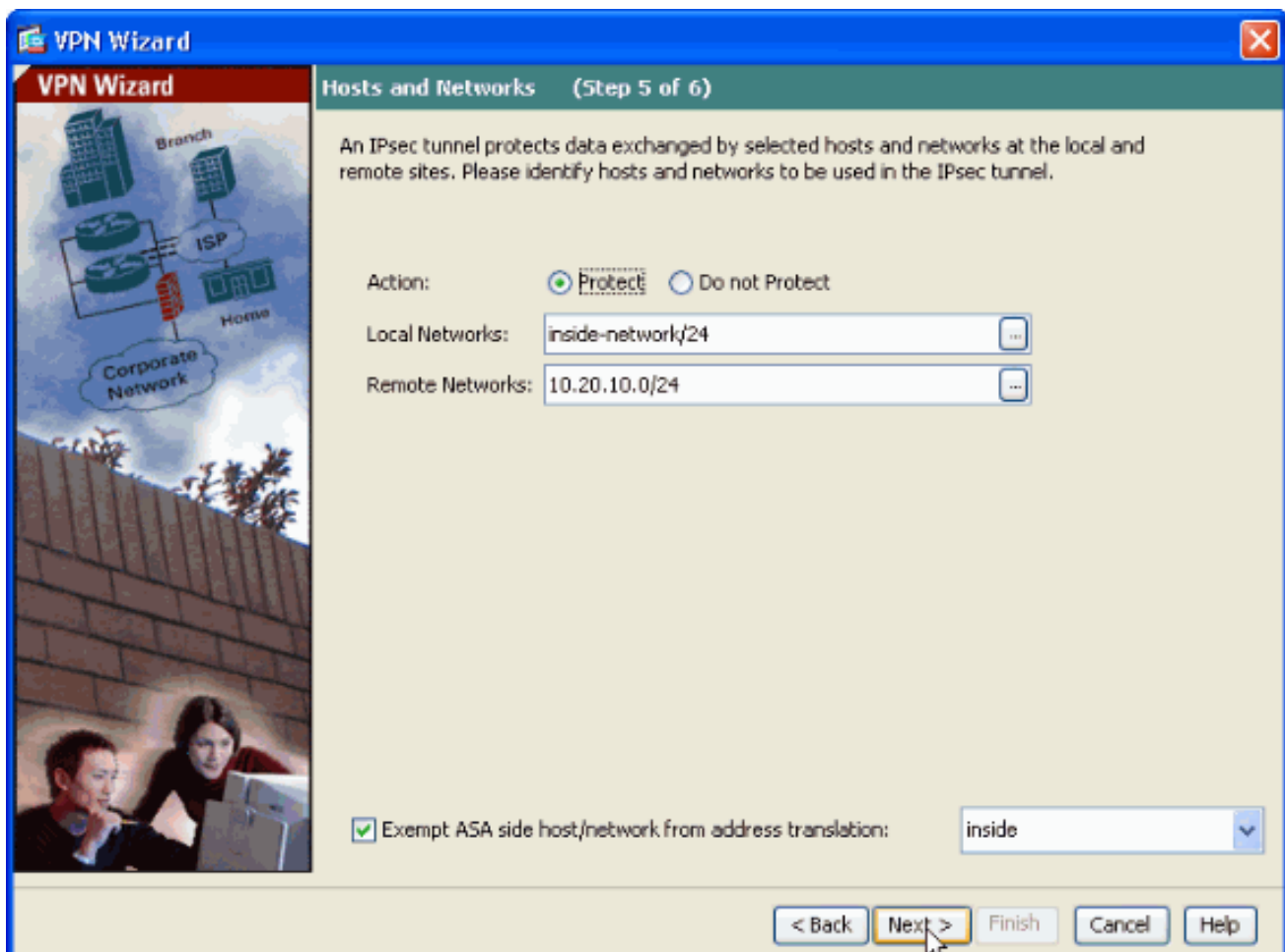
12. 单击 **Remote Networks** 旁边的按钮（如图所示），从下拉列表中选择远程网络地址。



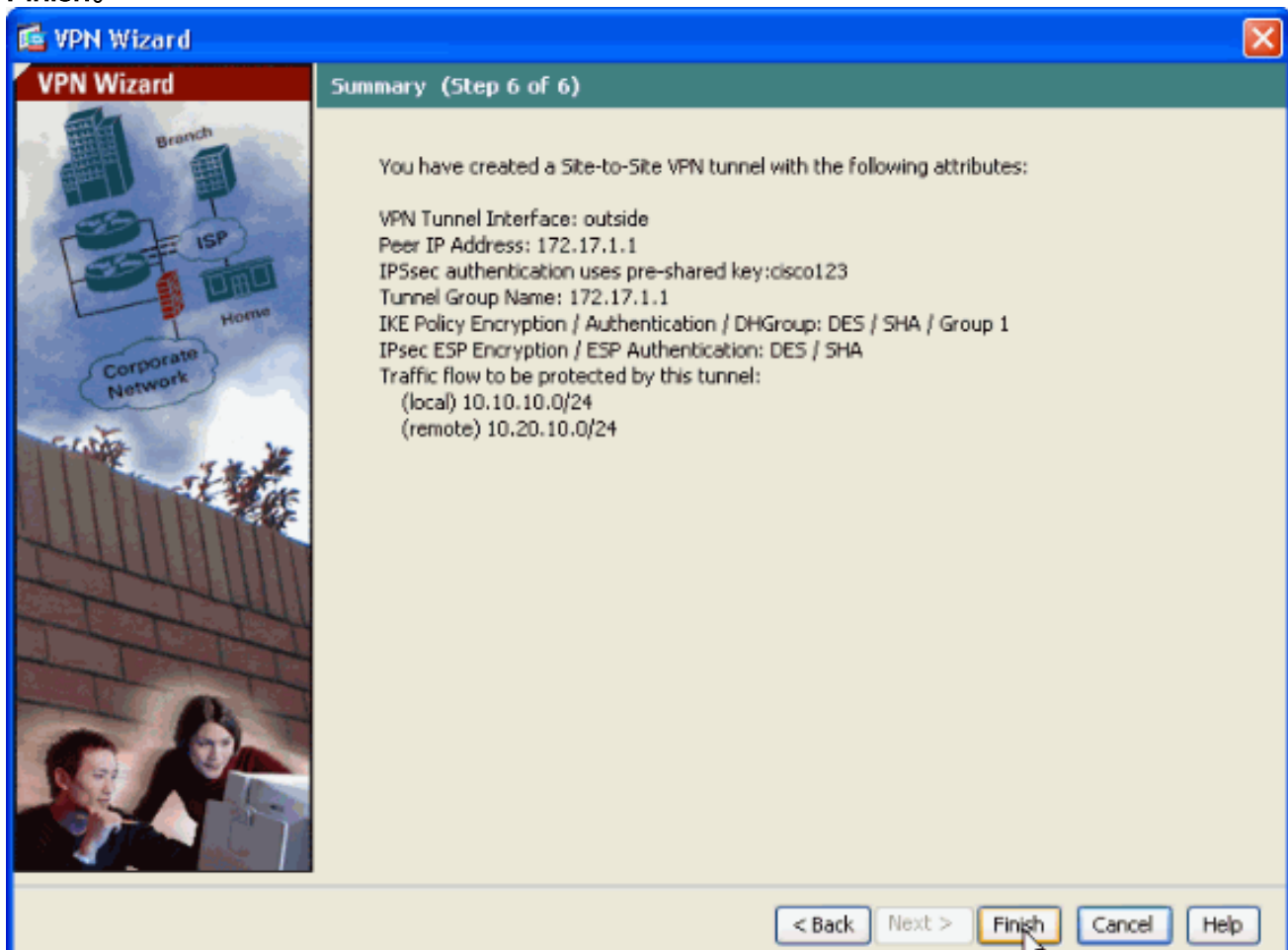
13. 选择 **Remote Network** 地址，然后单击 **OK**（如图所示）。**注意：** 如果列表中没有“远程网络”，则必须通过单击 **Add** 将该网络添加到列表中。



14. 选中 **Exempt ASA side host/network from address translation** 复选框，以防止隧道数据流进行网络地址转换。然后单击 **Next**。



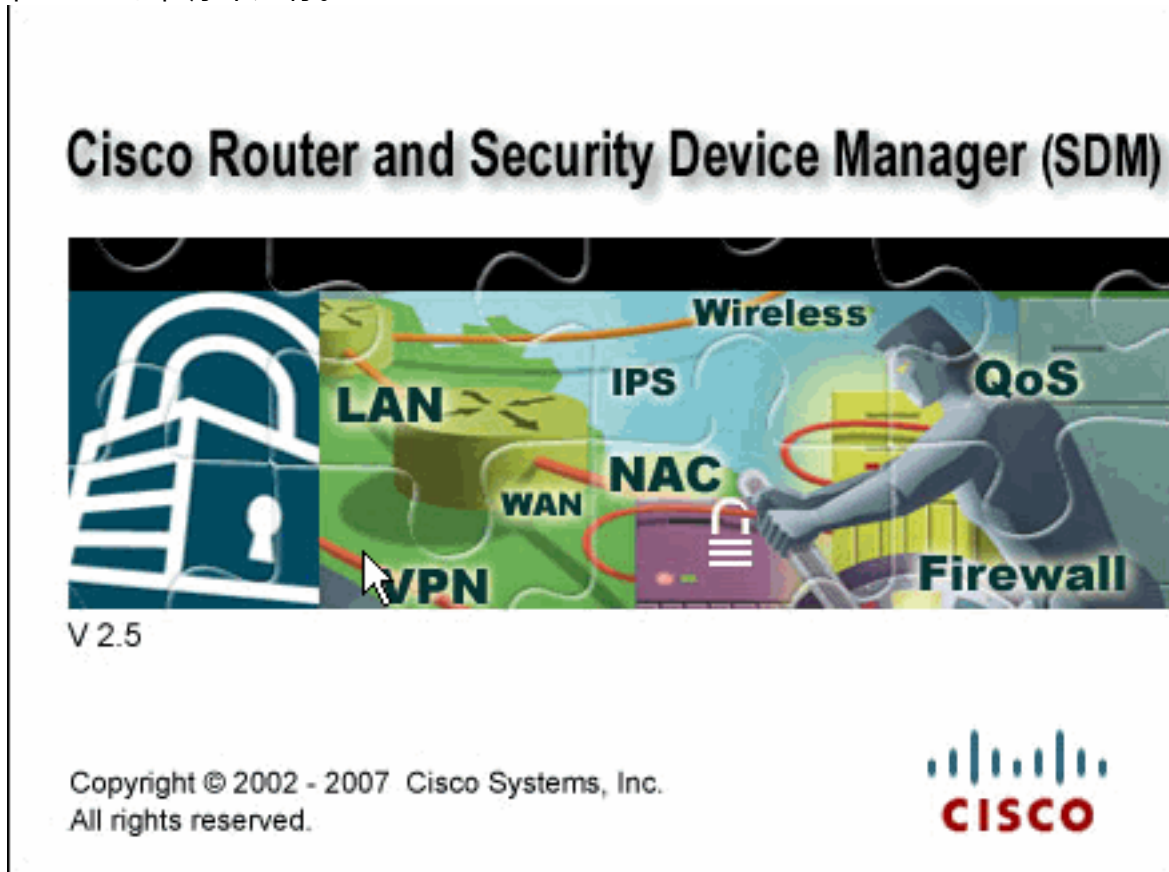
15. 此概要中显示了通过 VPN 向导定义的属性。仔细检查配置，如果您确保设置正确，请单击 Finish。



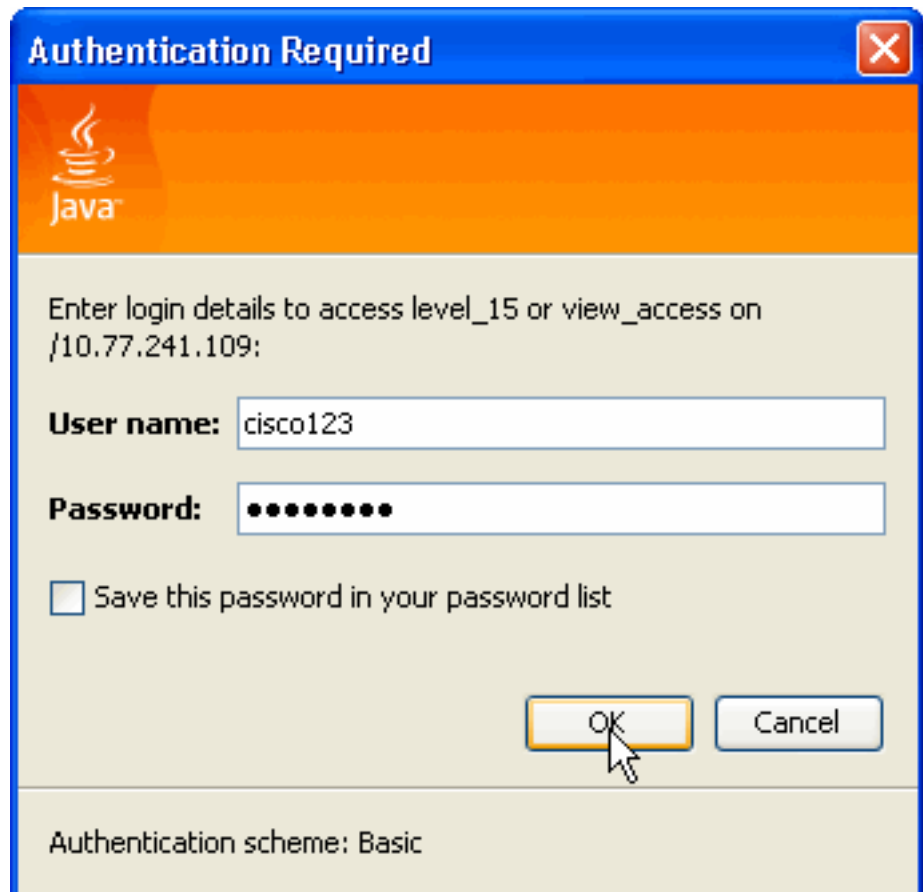
路由器 SDM 配置

完成下列步骤以在 Cisco IOS 路由器上配置站点到站点 VPN 隧道：

1. 打开浏览器并输入 <https://<为访问 SDM 而配置的路由器接口的 IP 地址>>，以访问路由器上的 SDM。确保核准浏览器提供的有关 SSL 证书真实性的任何警告。默认的用户名和口令均为空。路由器显示此窗口以允许下载 SDM 应用程序。此示例将应用程序加载到本地计算机，但不在 Java 小程序中运行。

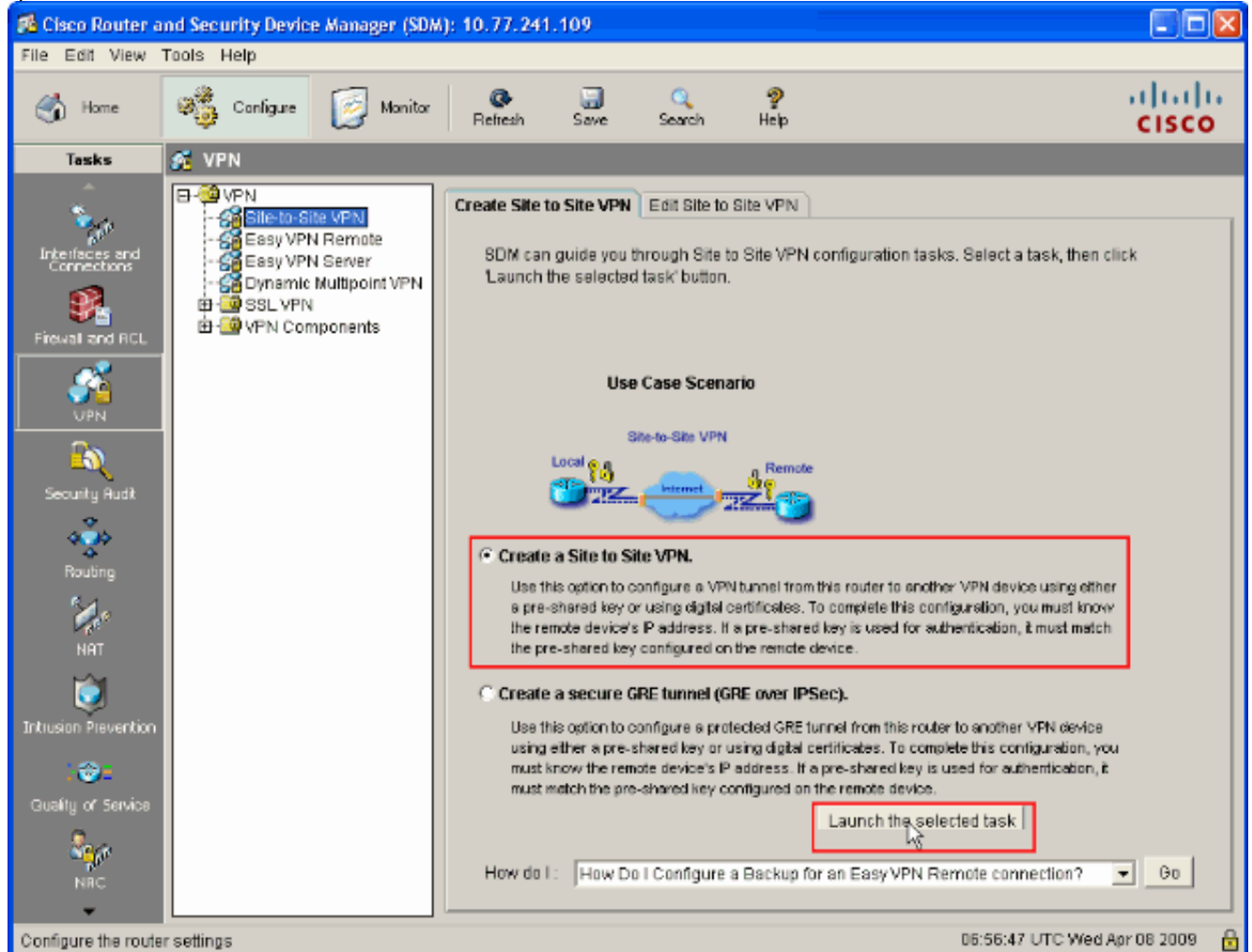


2. SDM 下载现在开始。下载 SDM 启动程序之后，完成提示所指示的步骤，以便安装该软件并运行 Cisco SDM 启动程序。
3. 输入用户名和口令（如果已指定），然后单击 OK。此示例使用 `cisco123` 作为用户名并使用

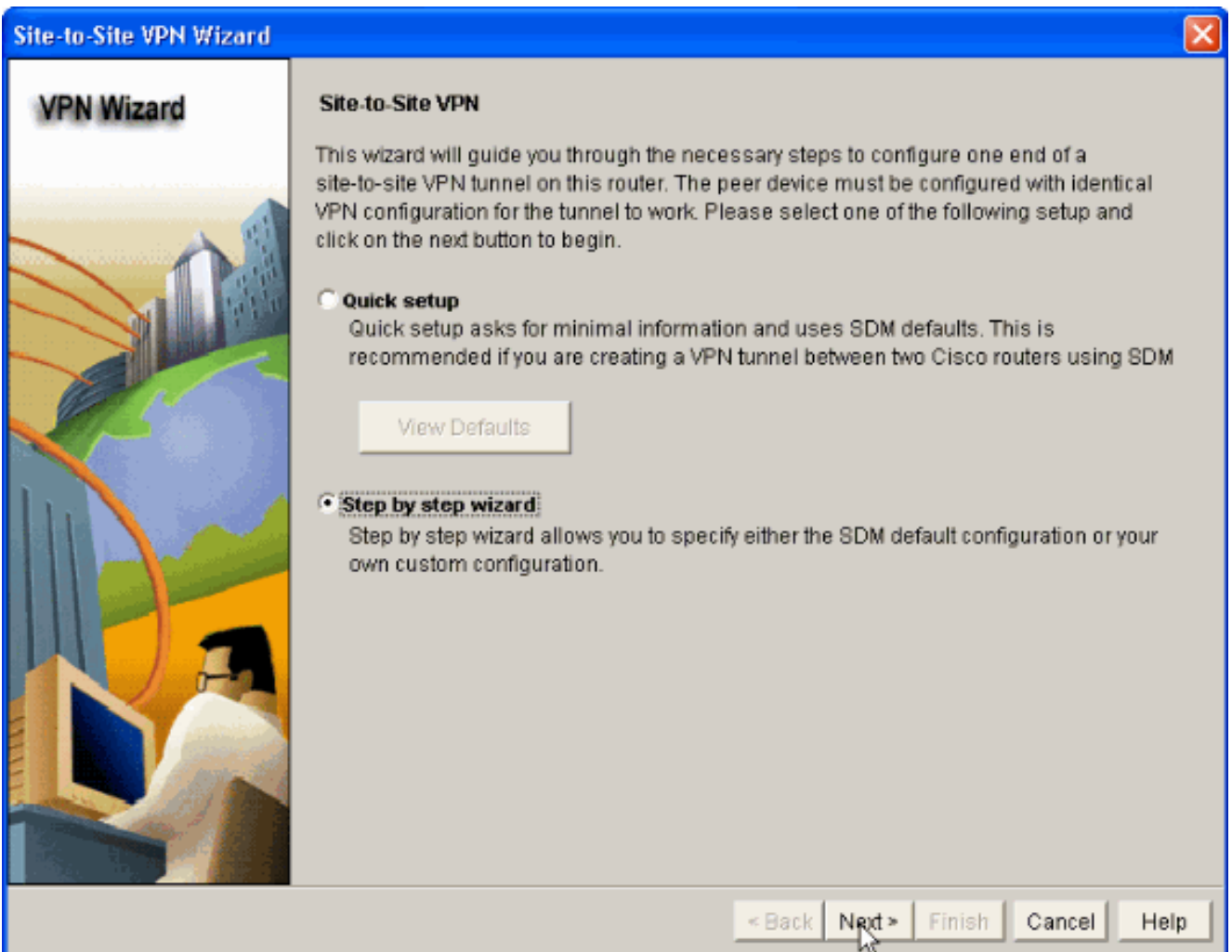


cisco123 作为口令。

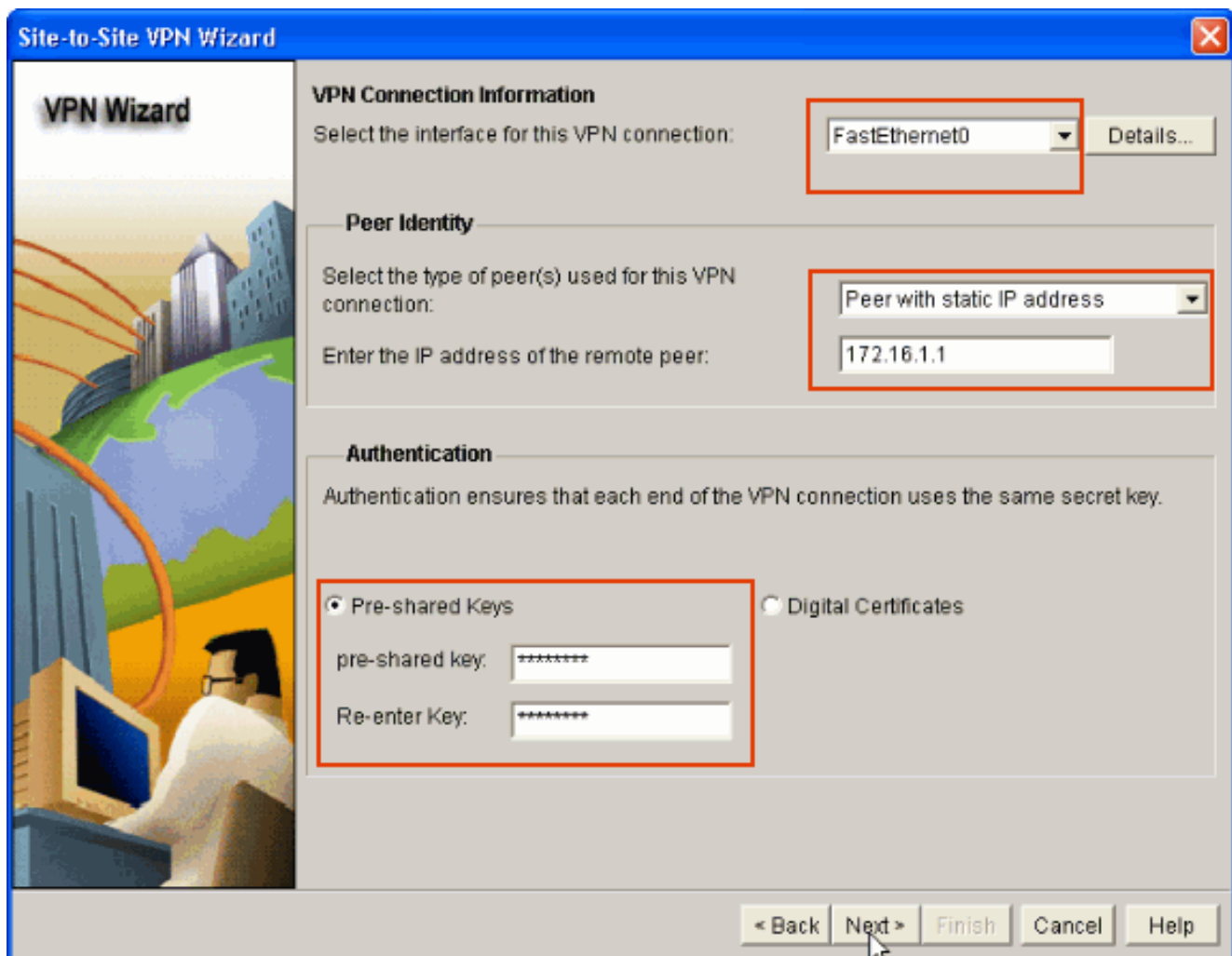
4. 选择 **Configuration -> VPN -> Site-to-Site VPN**，然后在 SDM 主页上单击 **Create a Site-to-Site VPN** 旁边的单选按钮。然后，单击 **Launch The selected Task** (如图所示) :



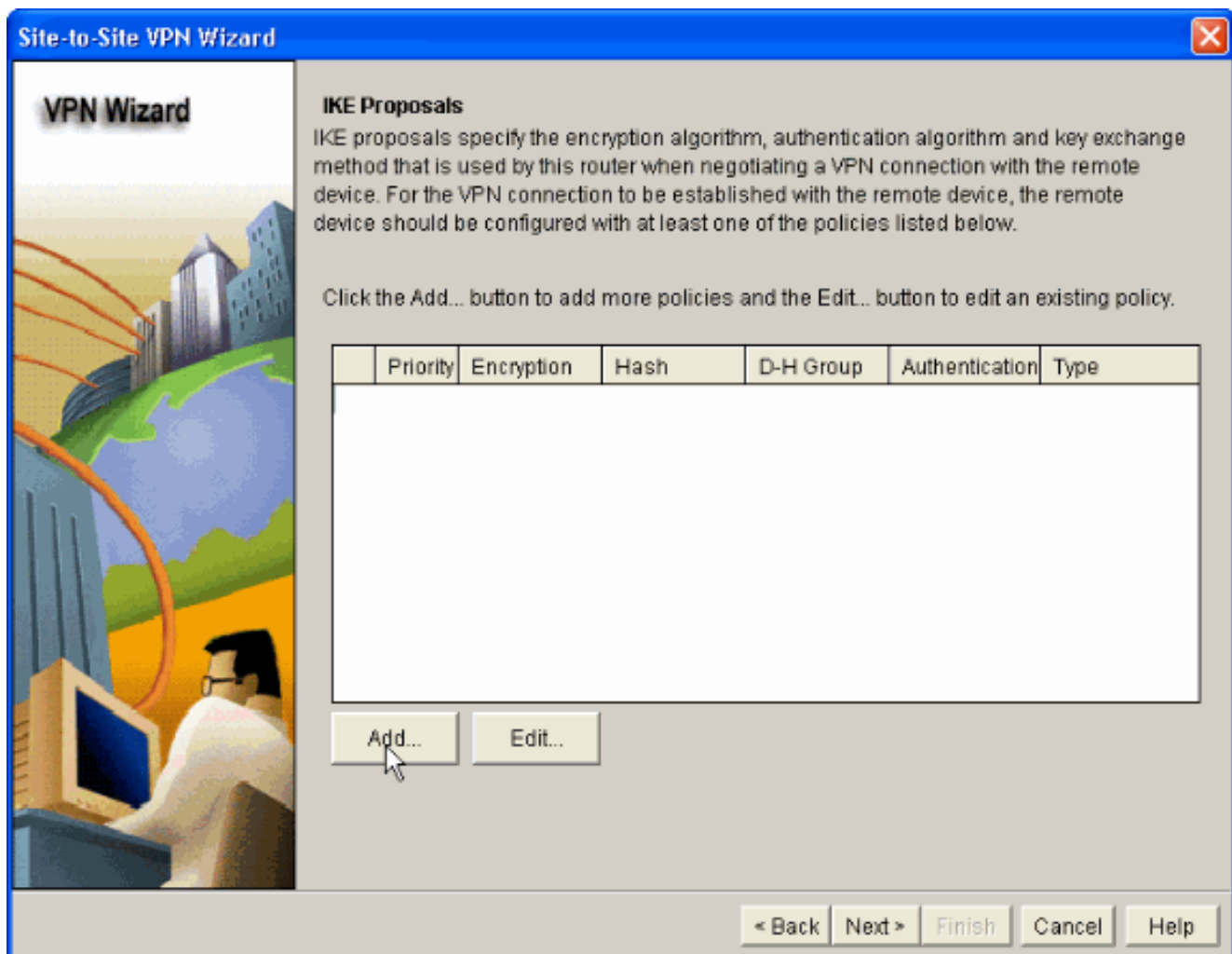
5. 选择 **Step by step wizard** 继续进行配置



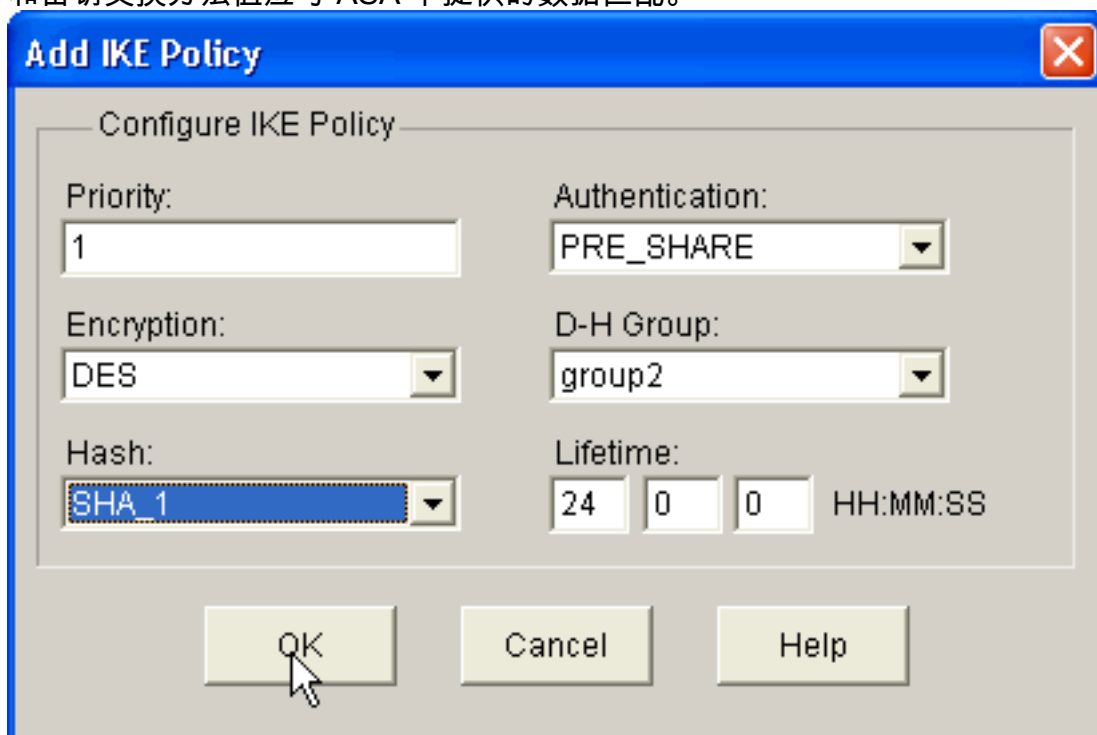
6. 在下一个窗口中，在各自空间中提供 **VPN 连接信息**。从下拉列表中选择 VPN 隧道的接口。此处选择 **FastEthernet0**。在 **Peer Identity** 中，选择具有静态 IP 地址的对等体并提供远程对等体 IP 地址。然后，在 **Authentication** 部分中提供 **Pre-shared key**（在本示例中为 **cisco123**），如图所示。然后单击 **Next**。



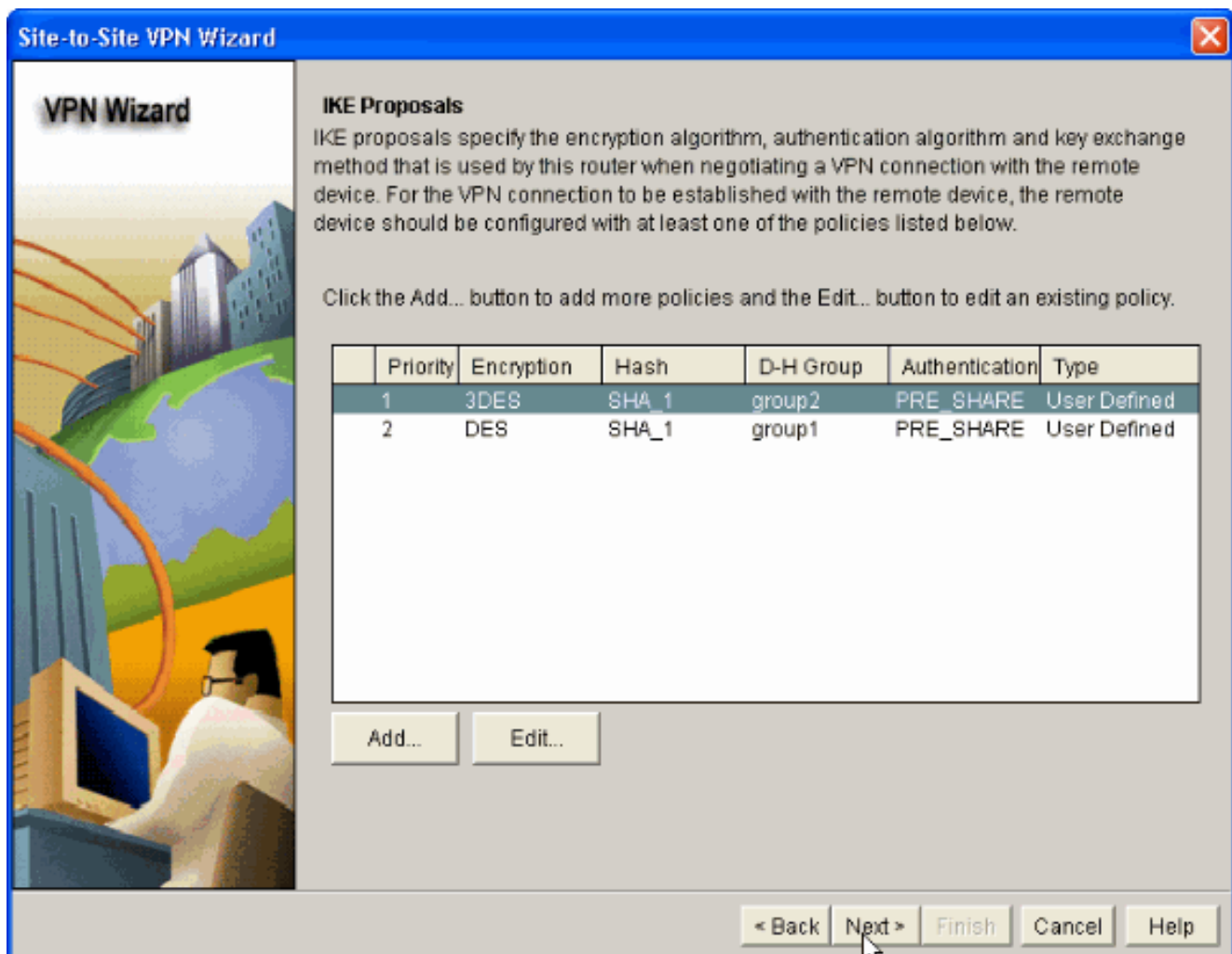
7. 单击 **Add** 添加指定加密算法、验证算法和密钥交换方法的 IKE 建议。



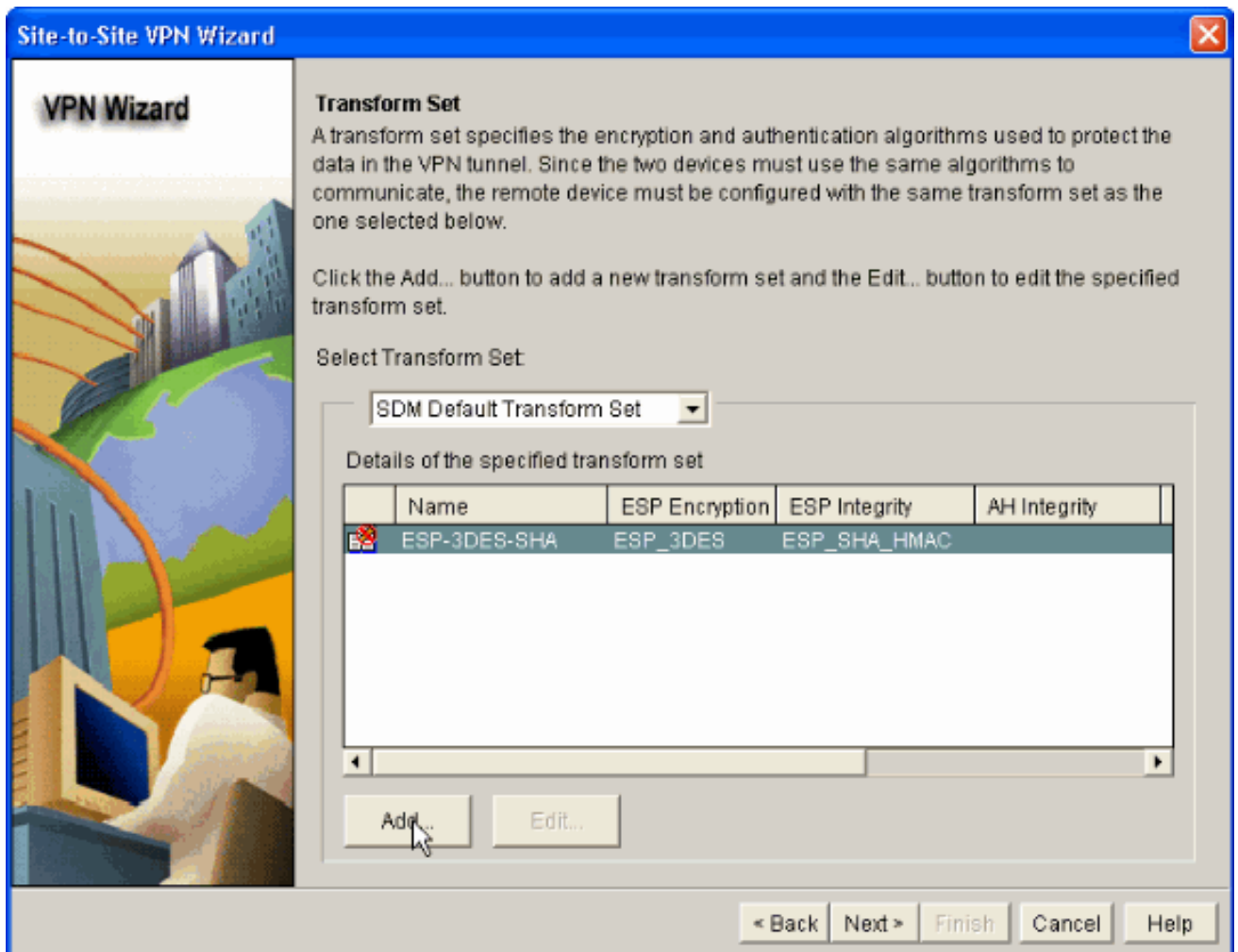
8. 提供**加密算法**、验证算法和密钥交换方法（如图所示），然后单击 OK。**加密算法**、验证算法和密钥交换方法值应与 ASA 中提供的数据匹配。



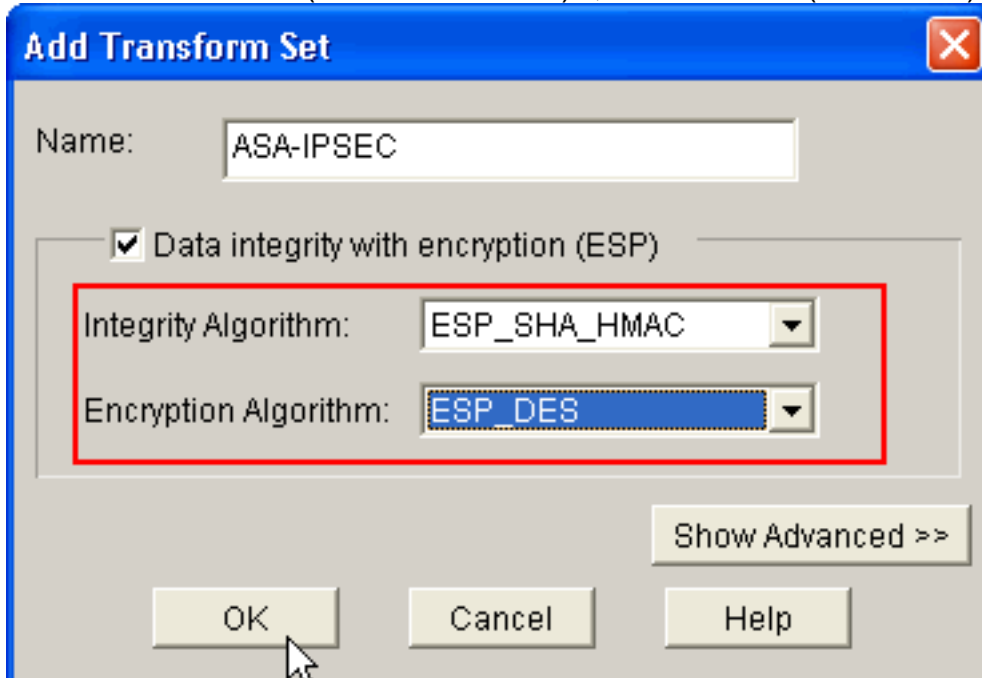
9. 单击 **Next**（如图所示）。



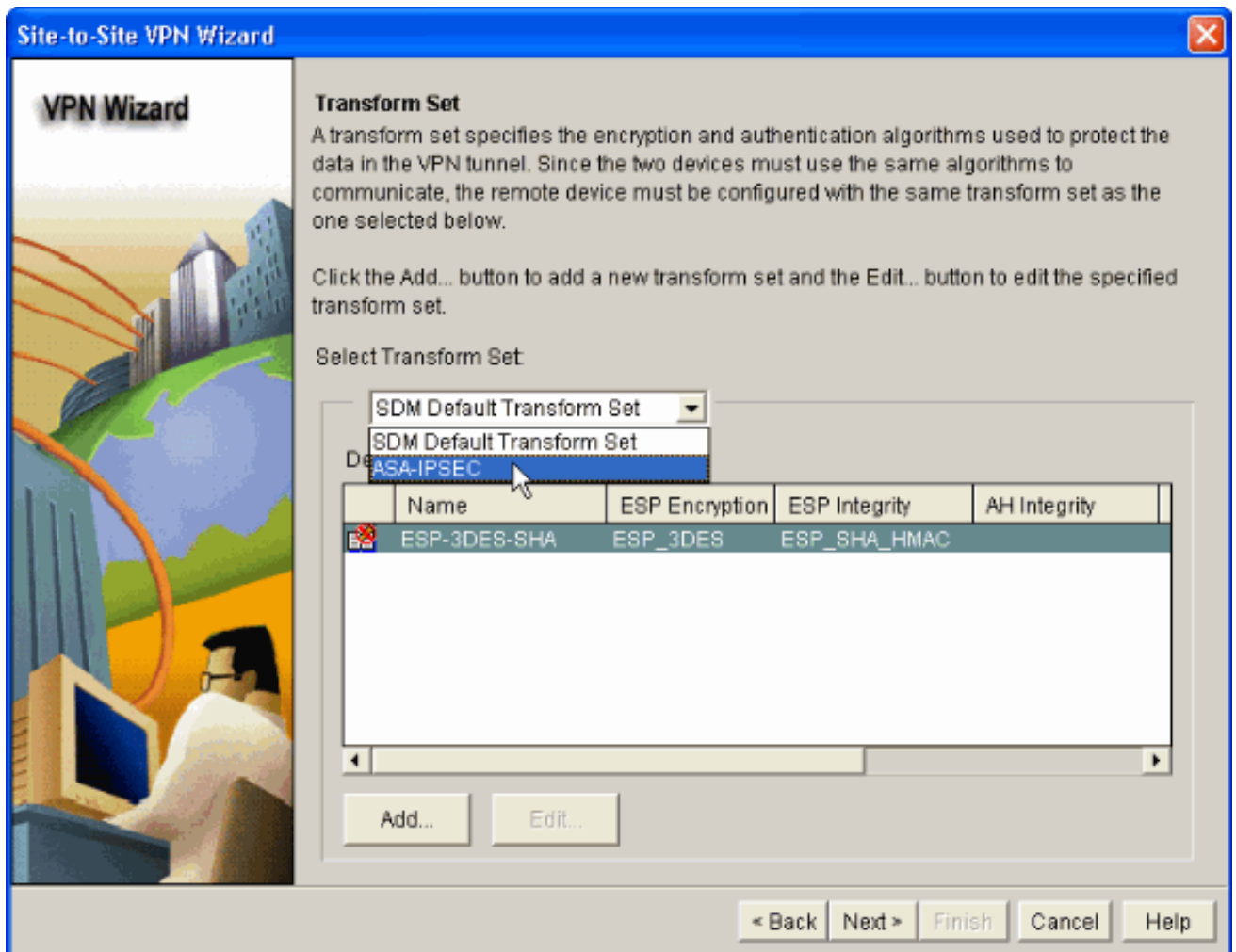
10. 应在此新窗口中提供**转换集**详细信息。“转换集”指定用于保护 VPN 隧道中的数据**的加密算法和验证算法**。然后，单击 **Add** 提供这些详细信息。通过单击 **Add** 并提供详细信息，您可以根据需要添加任何数量的转换集。



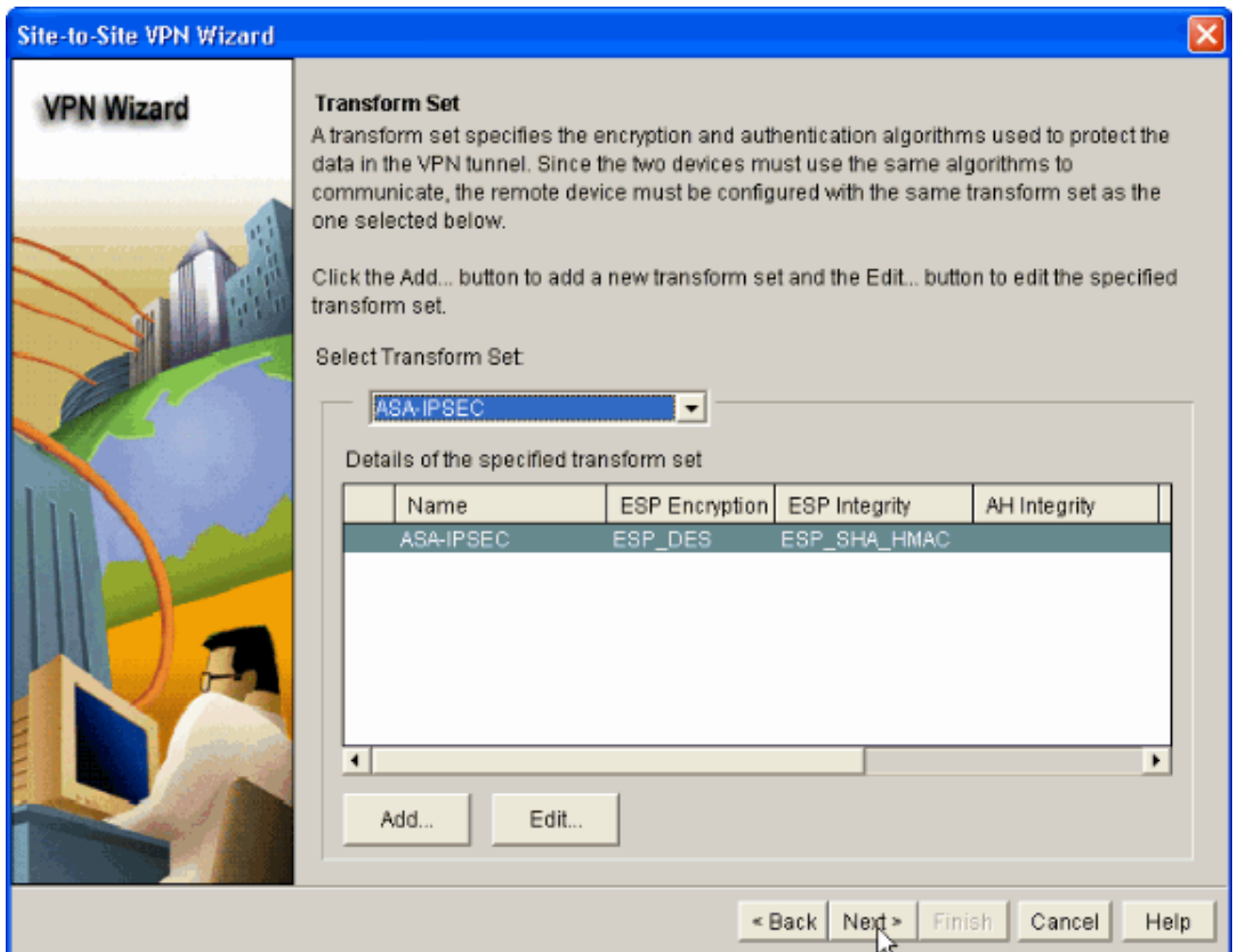
11. 提供**转换集**详细信息（加密和验证算法），并单击“确定”（如图所示）。



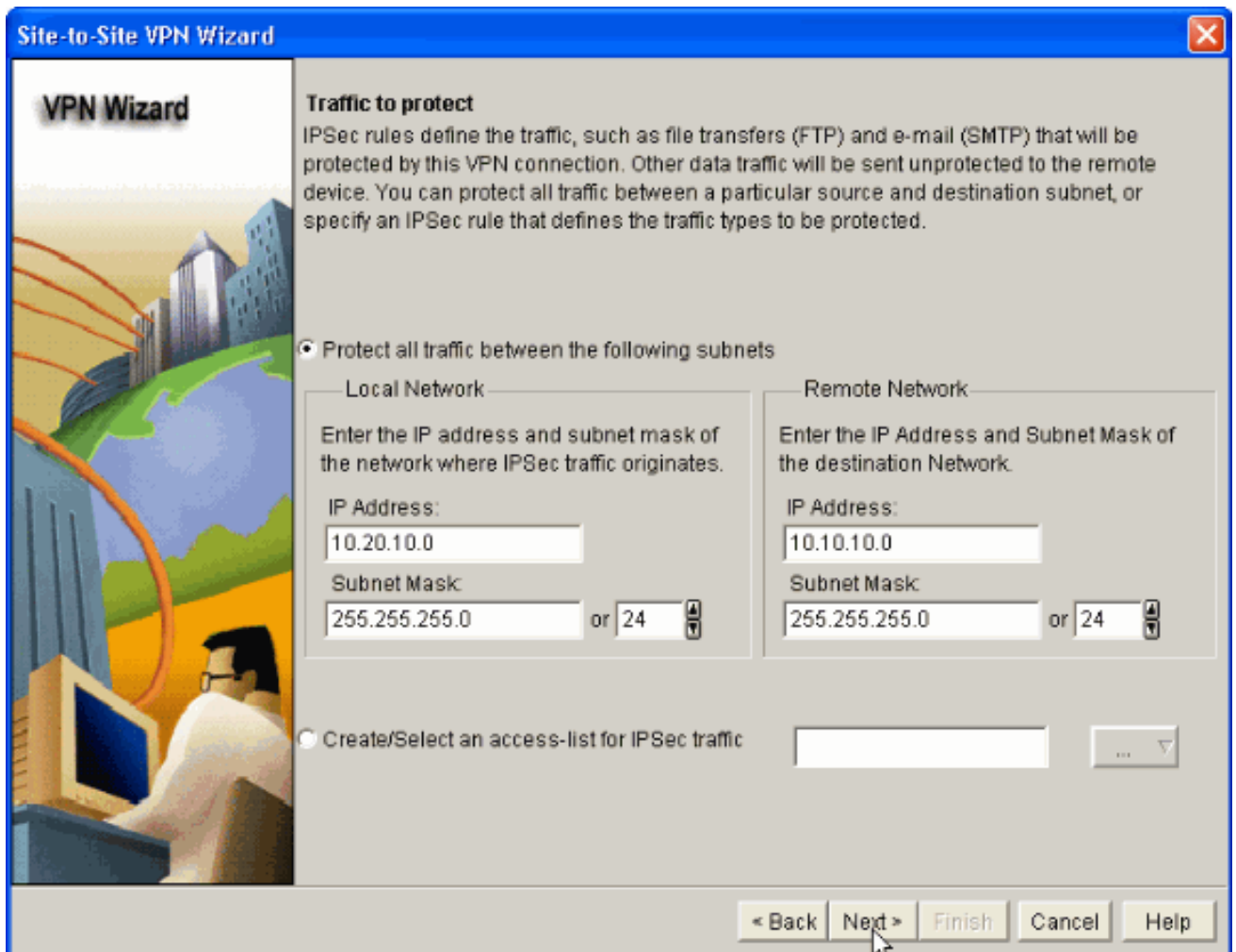
12. 从下拉列表中选择要使用的所需**转换集**（如图所示）。



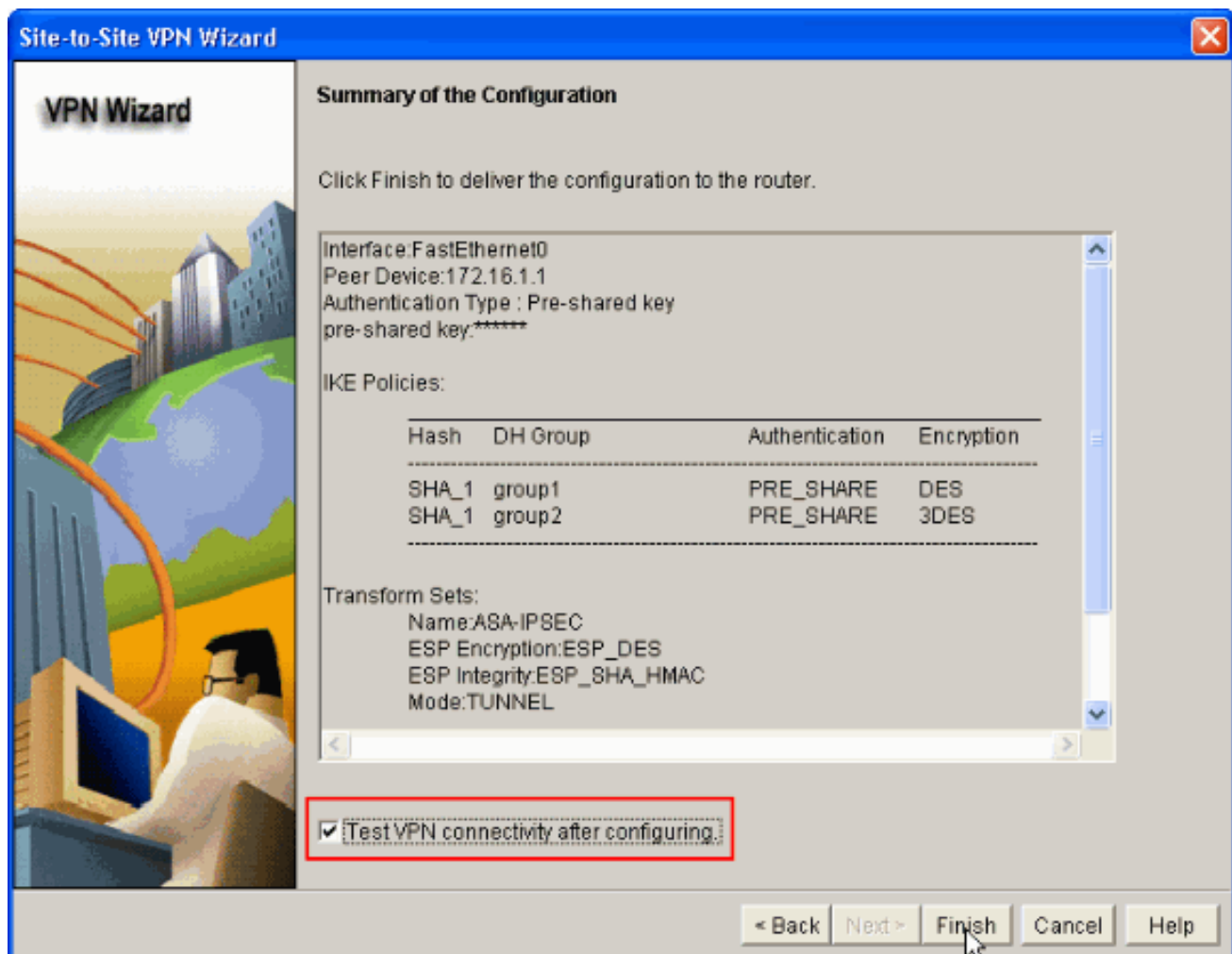
13. 单击 **Next**。



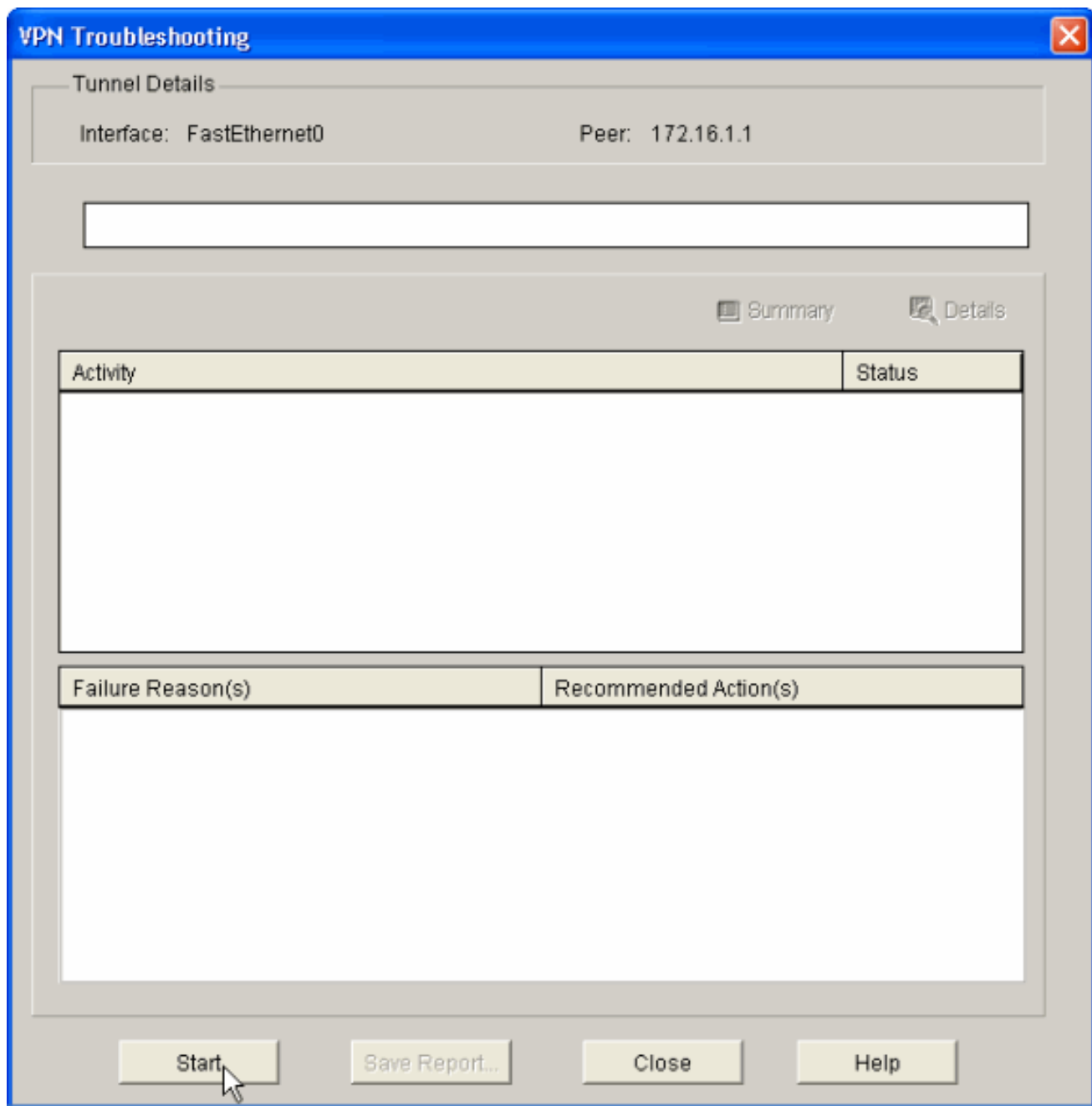
14. 在以下窗口中提供有关**要保护的数据流**（通过 VPN 隧道）的详细信息。提供要保护的数据流的**源网络和目标网络**，以便保护指定的源网络和目标网络之间的数据流。在本示例中，源网络是 10.20.10.0，目标网络是 10.10.10.0。然后单击 **Next**。



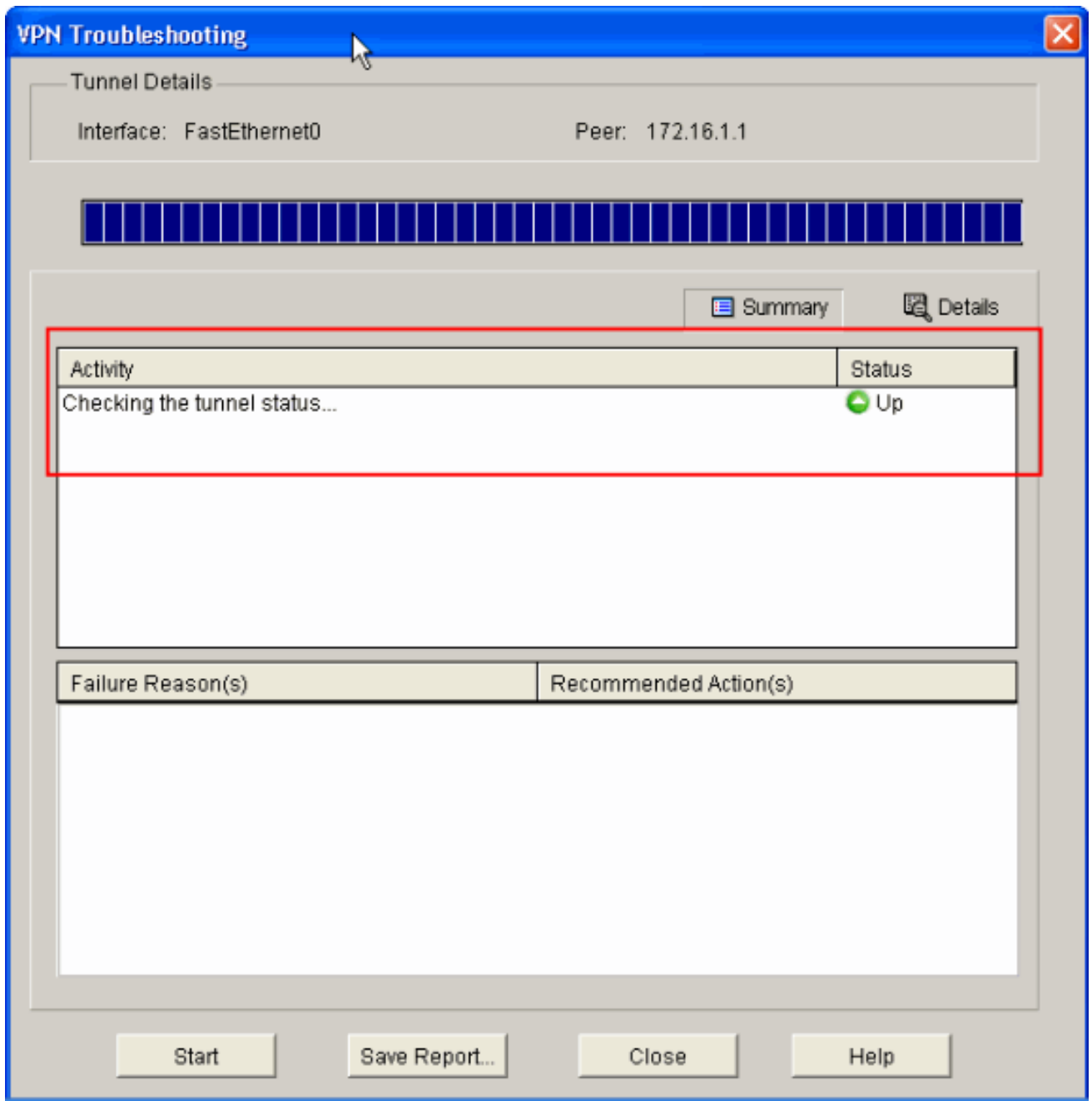
15. 此窗口显示已实现的站点到站点 VPN 配置的汇总。如果您要测试 VPN 连接性，请选中 **Test VPN Connectivity after configuring** 复选框。此处选中此框是因为需要检查连接性。然后单击 **Finish**。



16. 单击 **Start** (如图所示) 以检查 VPN 连接性。



17. 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。



至此已完成对 Cisco IOS 路由器的配置。

ASA CLI 配置

ASA

```
ASA#show run : Saved ASA Version 8.0(2) ! hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted names ! !---
Configure the outside interface. ! interface Ethernet0/1
nameif outside security-level 0 ip address 172.16.1.1
255.255.255.0 !--- Configure the inside interface. !
interface Ethernet0/2 nameif inside security-level 100
ip address 10.10.10.1 255.255.255.0 !-- Output
suppressed ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive dns server-group DefaultDNS domain-name
default.domain.invalid access-list 100 extended permit
ip any any access-list inside_nat0_outbound extended
permit ip 10.10.10.0 255.255.255.0 10.20.10.0
255.255.255.0 !--- This access list
(inside_nat0_outbound) is used !--- with the nat zero
command. This prevents traffic which !--- matches the
```

```
access list from undergoing network address translation
(NAT). !--- The traffic specified by this ACL is traffic
that is to be encrypted and !--- sent across the VPN
tunnel. This ACL is intentionally !--- the same as
(outside_1_cryptomap). !--- Two separate access lists
should always be used in this configuration. access-list
outside_1_cryptomap extended permit ip 10.10.10.0
255.255.255.0 10.20.10.0 255.255.255.0 !--- This access
list (outside_cryptomap) is used !--- with the crypto
map outside_map !--- to determine which traffic should
be encrypted and sent !--- across the tunnel. !--- This
ACL is intentionally the same as (inside_nat0_outbound).
!--- Two separate access lists should always be used in
this configuration. pager lines 24 mtu inside 1500 mtu
outside 1500 no failover asdm image disk0:/asdm-613.bin
asdm history enable arp timeout 14400 global (outside) 1
interface nat (inside) 1 10.10.10.0 255.255.255.0 nat
(inside) 0 access-list inside_nat0_outbound !--- NAT 0
prevents NAT for networks specified in !--- the ACL
inside_nat0_outbound. access-group 100 in interface
outside route outside 0.0.0.0 0.0.0.0 172.16.1.2 1
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout mgcp-pat
0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth
0:05:00 absolute http server enable http 0.0.0.0 0.0.0.0
dmz no snmp-server location no snmp-server contact !---
PHASE 2 CONFIGURATION ---! !--- The encryption types for
Phase 2 are defined here. crypto ipsec transform-set
ESP-DES-SHA esp-des esp-sha-hmac !--- Define the
transform set for Phase 2. crypto map outside_map 1
match address outside_1_cryptomap !--- Define which
traffic should be sent to the IPsec peer. crypto map
outside_map 1 set peer 172.17.1.1 !--- Sets the IPsec
peer crypto map outside_map 1 set transform-set ESP-DES-
SHA !--- Sets the IPsec transform set "ESP-AES-256-SHA"
!--- to be used with the crypto map entry "outside_map".
crypto map outside_map interface outside !--- Specifies
the interface to be used with !--- the settings defined
in this configuration. !--- PHASE 1 CONFIGURATION ---!
!--- This configuration uses isakmp policy 10. !--- The
configuration commands here define the Phase !--- 1
policy parameters that are used. crypto isakmp enable
outside crypto isakmp policy 10 authentication pre-share
encryption des hash sha group 1 lifetime 86400 telnet
timeout 5 ssh timeout 5 console timeout 0 threat-
detection basic-threat threat-detection statistics
access-list ! tunnel-group 172.17.1.1 type ipsec-l2l !--
- In order to create and manage the database of
connection-specific !--- records for ipsec-l2l-IPsec
(LAN-to-LAN) tunnels, use the command !--- tunnel-group
in global configuration mode. !--- For L2L connections
the name of the tunnel group MUST be the IP !--- address
of the IPsec peer. tunnel-group 172.17.1.1 ipsec-
attributes pre-shared-key * !--- Enter the pre-shared-
key in order to configure the !--- authentication
method. telnet timeout 5 ssh timeout 5 console timeout 0
threat-detection basic-threat threat-detection
statistics access-list ! class-map inspection_default
match default-inspection-traffic ! !!-- Output
suppressed! username cisco123 password ffIRGPdSOJh9YLq
encrypted privilege 15
Cryptochecksum:be38dfaef777a339b9e1c89202572a7d : end
```

路由器 CLI 配置

路由器

Building configuration...

Current configuration : 2403 bytes

```
!  
version 12.3  
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 ASA-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 !--- "ASA-IPSEC" defined  
earlier in this configuration. set transform-set ASA-  
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


```

验证

使用本部分可确认配置能否正常运行。

[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。

- [PIX 安全设备 - show 命令](#)
- [远程 IOS 路由器 - show 命令](#)

ASA/PIX 安全设备 - show 命令

- **show crypto isakmp sa** - 显示对等体上的所有当前 IKE SA。ASA#show crypto isakmp sa Active SA: 1 Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey) Total IKE SA: 1 1 IKE Peer: 172.17.1.1 Type : L2L Role : initiator Rekey : no State : MM_ACTIVE
- **show crypto ipsec sa** — 显示对等体上的所有当前 IPsec SA。ASA#show crypto ipsec sa interface: outside Crypto map tag: outside_map, seq num: 1, local addr: 172.16.1.1 local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0) current_peer: 172.17.1.1 #pkts encaps: 9, #pkts encrypt: 9, #pkts digest: 9 #pkts decaps: 9, #pkts decrypt: 9, #pkts verify: 9 #pkts compressed: 0, #pkts decompressed: 0 #pkts not compressed: 9, #pkts comp failed: 0, #pkts decomp failed: 0 #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0 #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0 #send errors: 0, #rcv errors: 0 local crypto endpt.: 172.16.1.1, remote crypto endpt.: 172.17.1.1 path mtu 1500, ipsec overhead 58, media mtu 1500 current outbound spi: 434C4A7F inbound esp sas: spi: 0xB7C1948E (3082917006) transform: esp-des esp-sha-hmac none in use settings ={L2L, Tunnel, PFS Group 2, } slot: 0, conn_id: 12288, crypto-map: outside_map sa timing: remaining key lifetime (kB/sec): (4274999/3588) IV size: 8 bytes replay detection support: Y outbound esp sas: spi: 0x434C4A7F (1129073279) transform: esp-des esp-sha-hmac none in use settings ={L2L, Tunnel, PFS Group 2, } slot: 0, conn_id: 12288, crypto-map: outside_map sa timing: remaining key lifetime (kB/sec): (4274999/3588) IV size: 8 bytes replay detection support: Y

远程 IOS 路由器 - show 命令

- **show crypto isakmp sa** - 显示对等体上的所有当前 IKE SA。Router#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。Router#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** — 显示有关加密和解密数据包 (仅限路由器) 的当前连接和信息。Router#**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

故障排除

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。

注意： 使用 **debug** 命令之前，请参阅[有关 debug 命令的重要信息](#)和 [IP 安全故障排除 - 了解和使用 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。

有关站点到站点 VPN 故障排除的详细信息，请参阅[最常见的 L2L 和远程接入 IPsec VPN 故障排除解决方案](#)。

相关信息

- [Cisco PIX 防火墙软件](#)
- [Cisco 自适应安全设备管理器](#)
- [Cisco ASA 5500 系列自适应安全设备](#)
- [配置专业人员：在ASA/PIX和IOS路由器设置示例之间的站点至站点IPSec VPN](#)
- [Cisco Secure PIX 防火墙命令参考](#)
- [Cisco 路由器和安全设备管理器](#)
- [请求注解 \(RFC\)](#)
- [技术支持和文档 - Cisco Systems](#)