在 IOS 上使用 SDM 配置 SSL VPN 客户端 (SVC) 的示例

目录

简介

SSL VPN 客户端 (SVC) 提供了与企业内部网络进行安全通信的全隧道。您可以按用户配置用户的访问权限，或者可以创建放置一个或更多用户的不同的 WebVPN 上下文。

以下 IOS 路由器平台支持 SSL VPN 或 WebVPN 技术：

- 870、1811、1841、2801、2811、2821、2851
- 3725、3745、3825、3845、7200 和 7301

您可以在以下模式中配置 SSL VPN 技术：

- **无客户端 SSL VPN (WebVPN) — 提供一个远程客户端，它要求通过启用了 SSL 的 Web 浏览器才能访问公司局域网 (LAN) 上的 HTTP 或 HTTPS Web 服务器。** 此外，利用无客户端 SSL VPN 还可以通过公用 Internet 文件系统 (CIFS) 协议浏览 Windows 文件。Outlook Web Access (OWA) 就是 HTTP 访问的一个示例。要了解有关无客户端 SSL VPN 的详细信息，请参阅在

Cisco IOS 上使用 SDM 配置无客户端 SSL VPN (WebVPN) 的配置示例。

- **瘦客户端 SSL VPN（端口转发）— 提供一个远程客户端，它下载基于 Java 的小程序，并允许以安全方式访问使用静态端口号的传输控制协议 (TCP) 应用程序。**安全访问的示例包括入网点 (POP3)、简单邮件传输协议 (SMTP)、Internet 邮件访问协议 (IMAP)、安全壳 (ssh) 和 Telnet。由于本地计算机上的文件发生更改，因此用户必须有本地管理权限才能使用此方法。这种 SSL VPN 方法不能与使用动态端口分配的应用程序（如某些文件传输协议 (FTP) 应用程序）配合工作。要了解有关瘦客户端 SSL VPN 的详细信息，请参阅使用 SDM 的瘦客户端 SSL VPN (WebVPN) IOS 配置示例。**注意：**不支持用户数据报协议(UDP)。
- **SSL VPN 客户端（SVC 全隧道模式）— 下载一个小型客户端到远程工作站，并允许以完全安全方式访问公司内部网络中的资源。**可以将 SVC 永久下载到远程工作站，也可以在安全会话关闭后删除该客户端。

本文档说明供 SSL VPN 客户端使用的 Cisco IOS 路由器的配置。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- Microsoft Windows 2000 或 XP
- 带 SUN JRE 1.4 或更高版本的 Web 浏览器，或者有 ActiveX 控制的浏览器
- 客户端的本地管理权限
- 在简介中列出的路由器之一带有高级安全映像（12.4(6)T 或更高版本）
- Cisco 安全设备管理器 (SDM) 版本 2.3如果尚未在路由器上加载 Cisco SDM，您可以从软件下载（仅限注册用户）获取该软件的免费副本。 您必须拥有一个已签署服务合同的 CCO 帐户。有关安装和配置 SDM 的详细信息，请参阅 Cisco Router and Security Device Manager。
- 路由器的数字证书您可以使用永久性自签名证书或外部证书颁发机构 (CA) 满足此要求。有关永久自签名证书的详细信息，请参阅永久自签名证书。

使用的组件

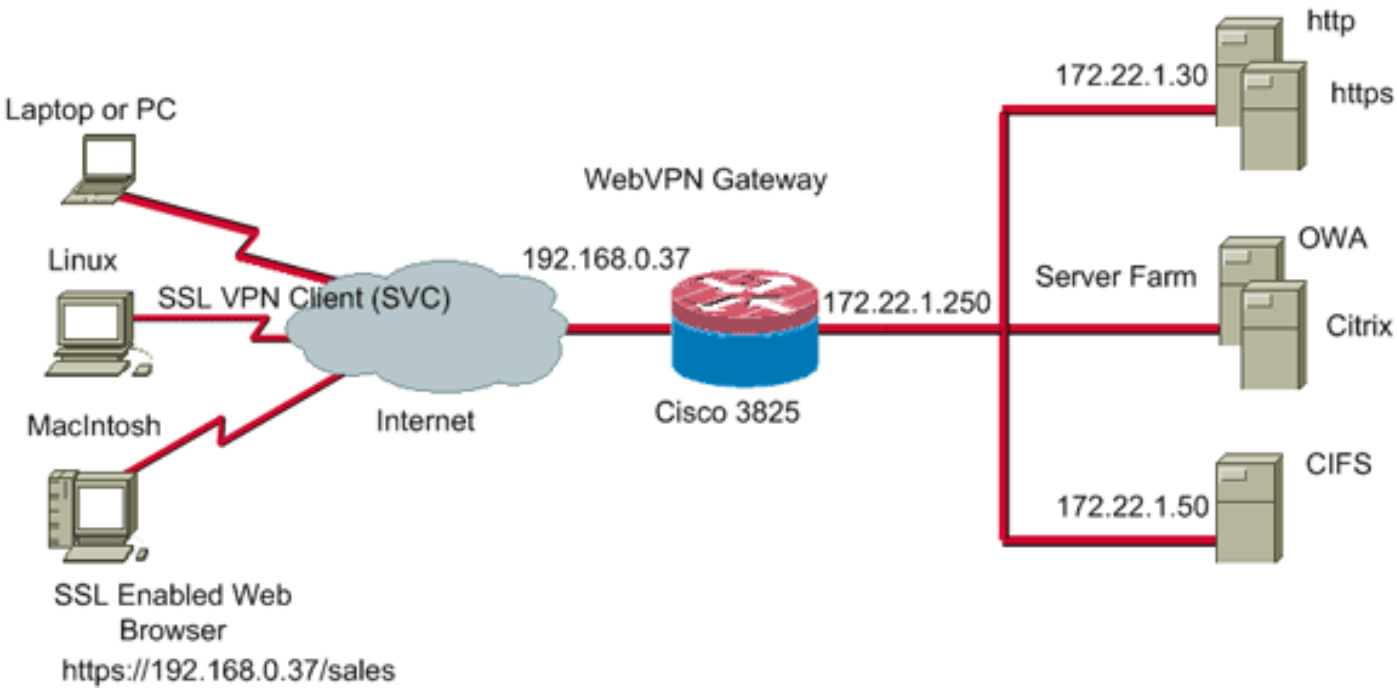
本文档中的信息基于以下软件和硬件版本：

- 带有 12.4(9)T 的 Cisco IOS 路由器 3825 系列
- 安全设备管理器 (SDM) 版本 2.3.1

注意：本文档中的信息是从特定实验环境中的设备创建的。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。

网络图

本文档使用以下网络设置：



配置前的任务

1. 为路由器配置SDM。（可选）具有相应安全链路捆绑许可证的路由器的闪存中已加载了 SDM 应用程序。请参阅下载和安装 Cisco 路由器和安全设备管理器 (SDM)，以获取并配置软件。
2. 将 SVC 副本下载到您的管理 PC。您可以从软件下载获得 SVC 程序包软件副本：Cisco SSL VPN 客户端（仅限注册用户）。 您必须拥有一个已签署服务合同的有效 CCO 帐户。
3. 设置正确日期、时间和时区，然后在路由器上配置数字证书。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

背景信息

SVC 最初加载在 Webvpn 网关路由器上。每当连接客户端时，SVC 副本便动态下载到 PC 上。为了改变此行为，请配置路由器以使软件永久留在客户端计算机上。

在 IOS 上配置 SVC

本部分提供有关配置本文档中所述功能的必要步骤。本配置示例使用 SDM 向导指导在 IOS 路由器上的 SVC 操作。

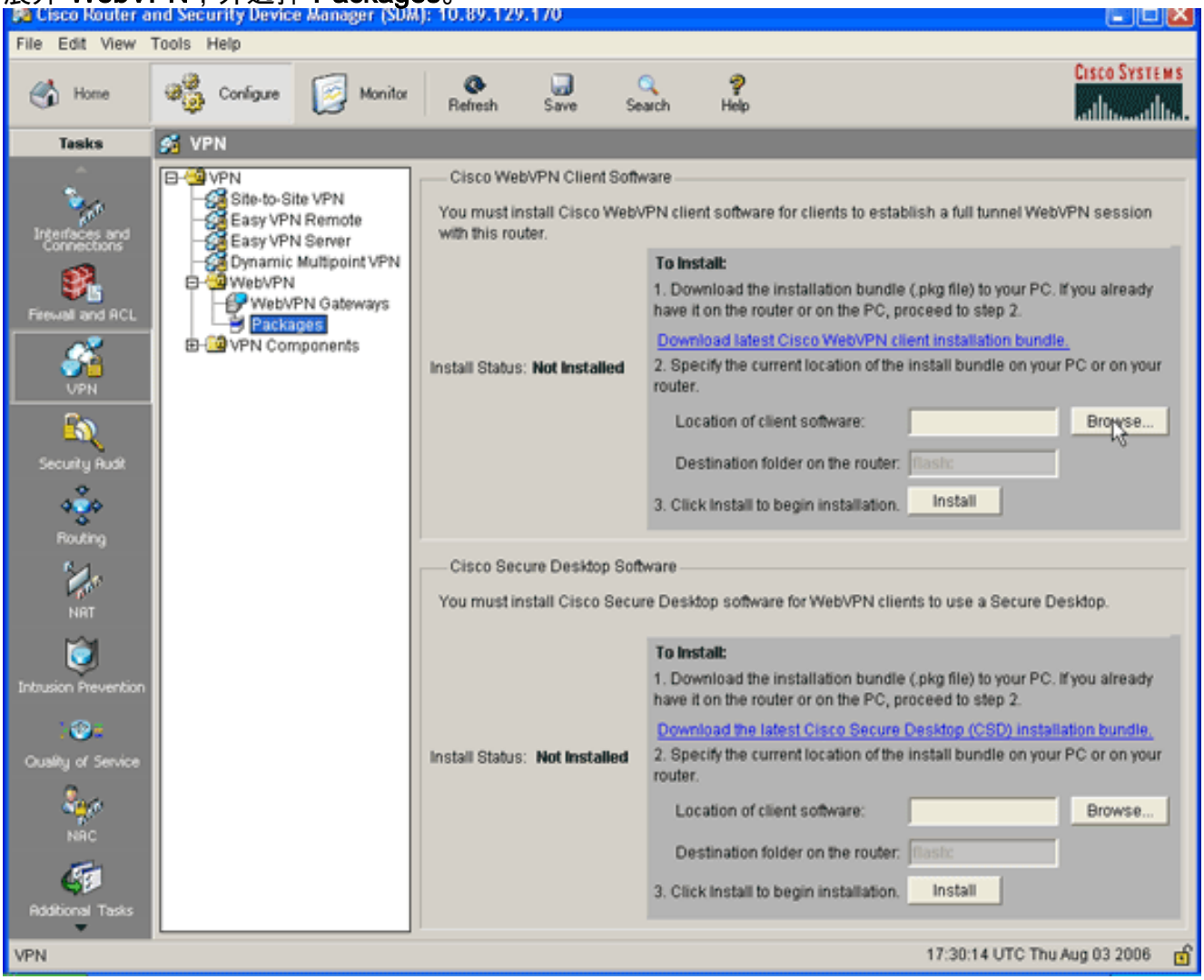
完成这些步骤，以便在 IOS 路由器上配置 SVC：

1. 在 IOS 路由器上安装并启用 SVC 软件
2. 使用 SDM 向导配置 WebVPN 上下文和 WebVPN 网关
3. 配置 SVC 用户的用户数据库
4. 配置面向用户的资源

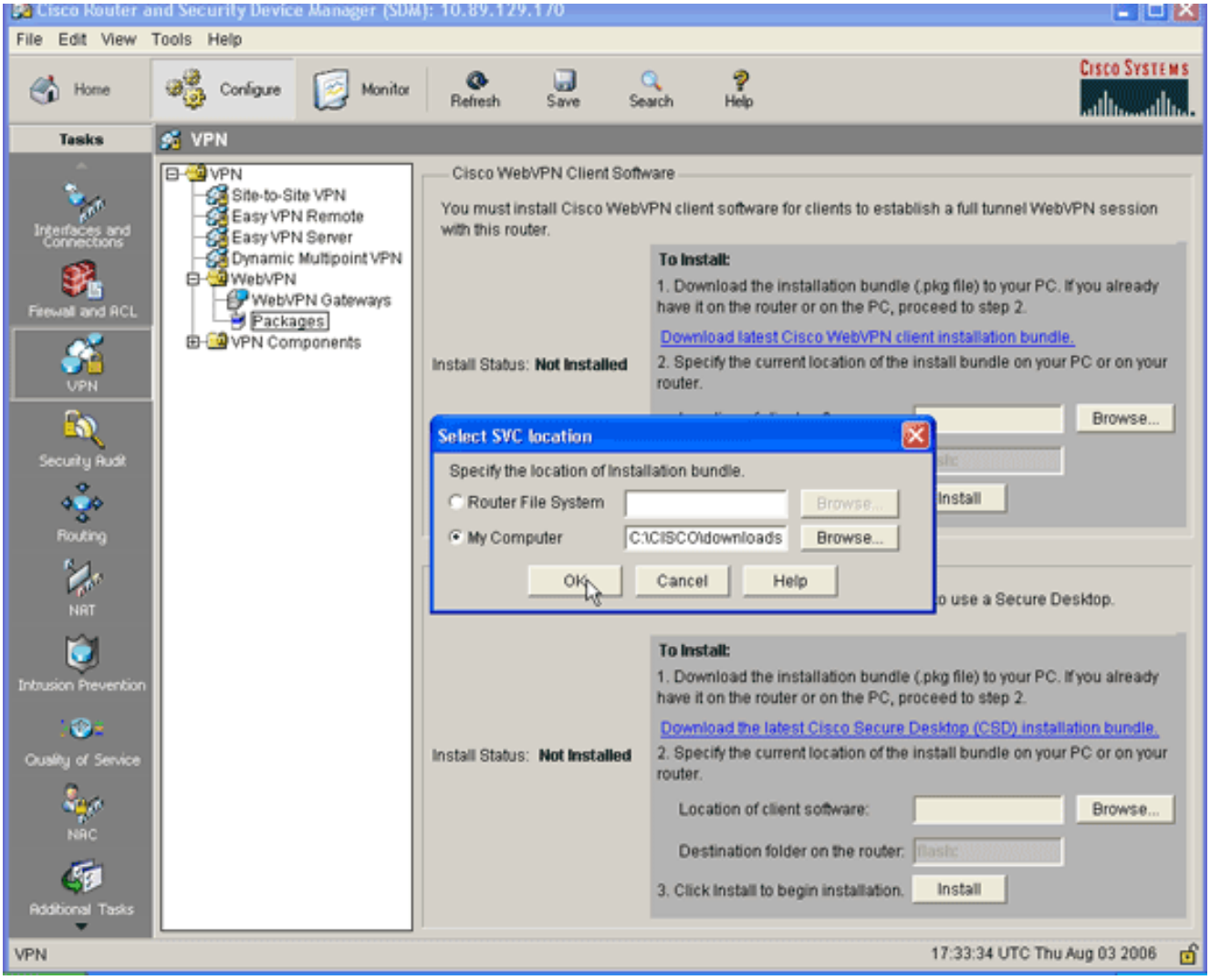
步骤 1. 在 IOS 路由器上安装并启用 SVC 软件

要在 IOS 路由器中安装并启用 SVC 软件，请完成以下步骤：

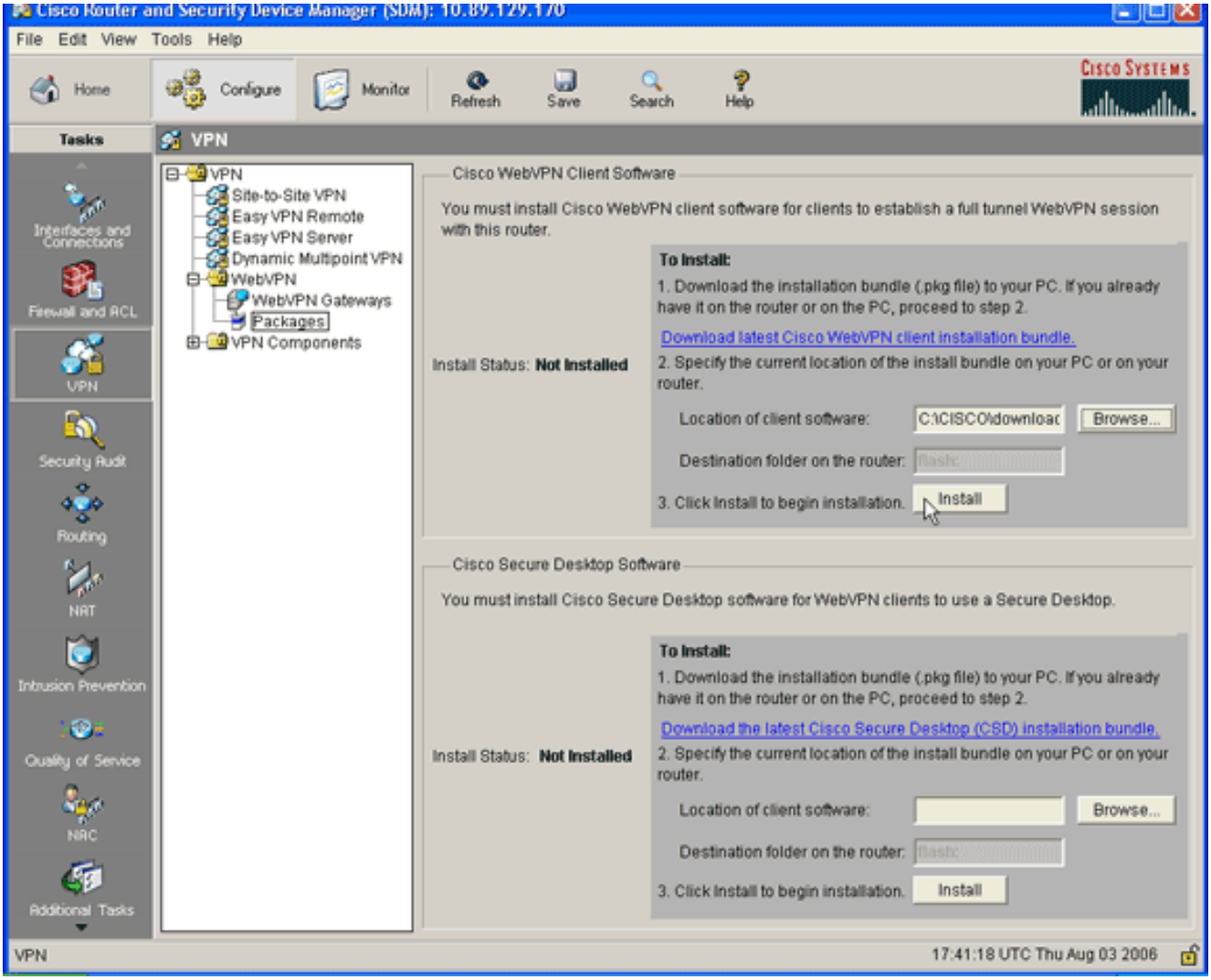
1. 打开 SDM 应用程序，单击 **Configure**，然后单击 **VPN**。
2. 展开 **WebVPN**，并选择 **Packages**。



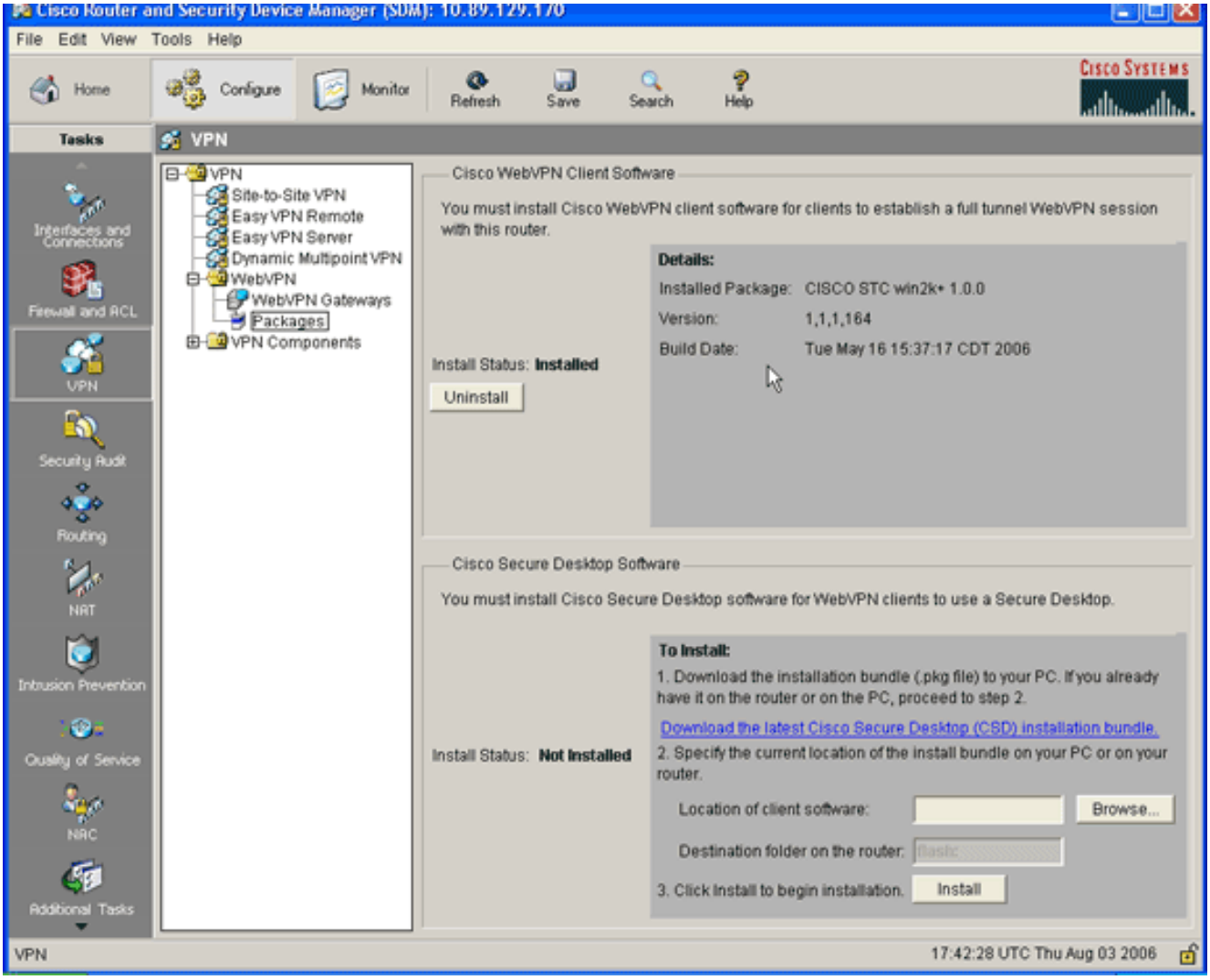
3. 在 Cisco WebVPN 客户端软件区域内，单击 **Browse 按钮。**此时将显示 Select SVC location 对话框。



4. 单击 My Computer 单选按钮，然后单击 Browse，以在您的管理 PC 上找出 SVC 程序包。
5. 单击 OK，然后单击 Install 按钮。



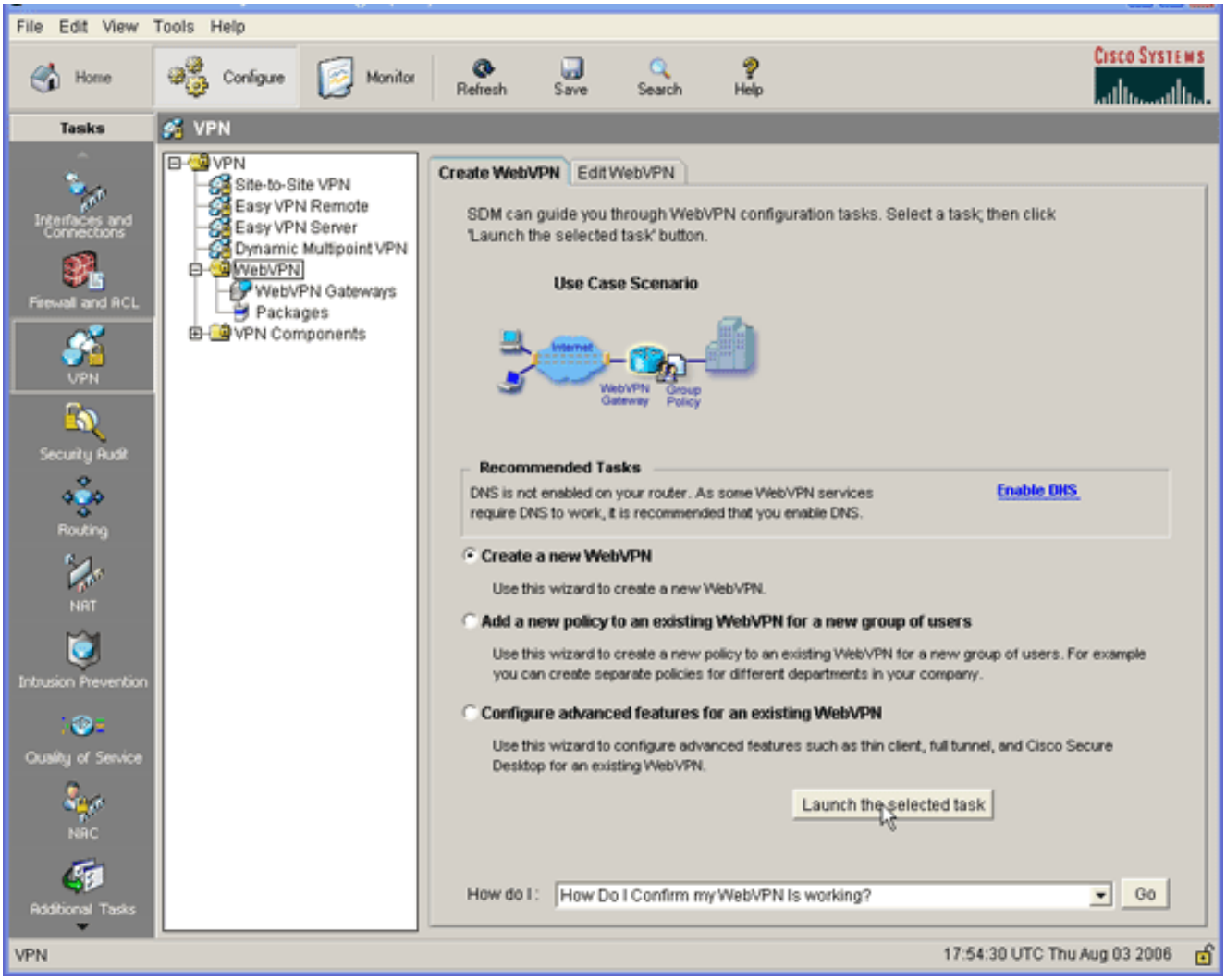
6. 单击 **Yes**，然后单击 **OK**。以下图像显示了 SVC 程序包的成功安装：



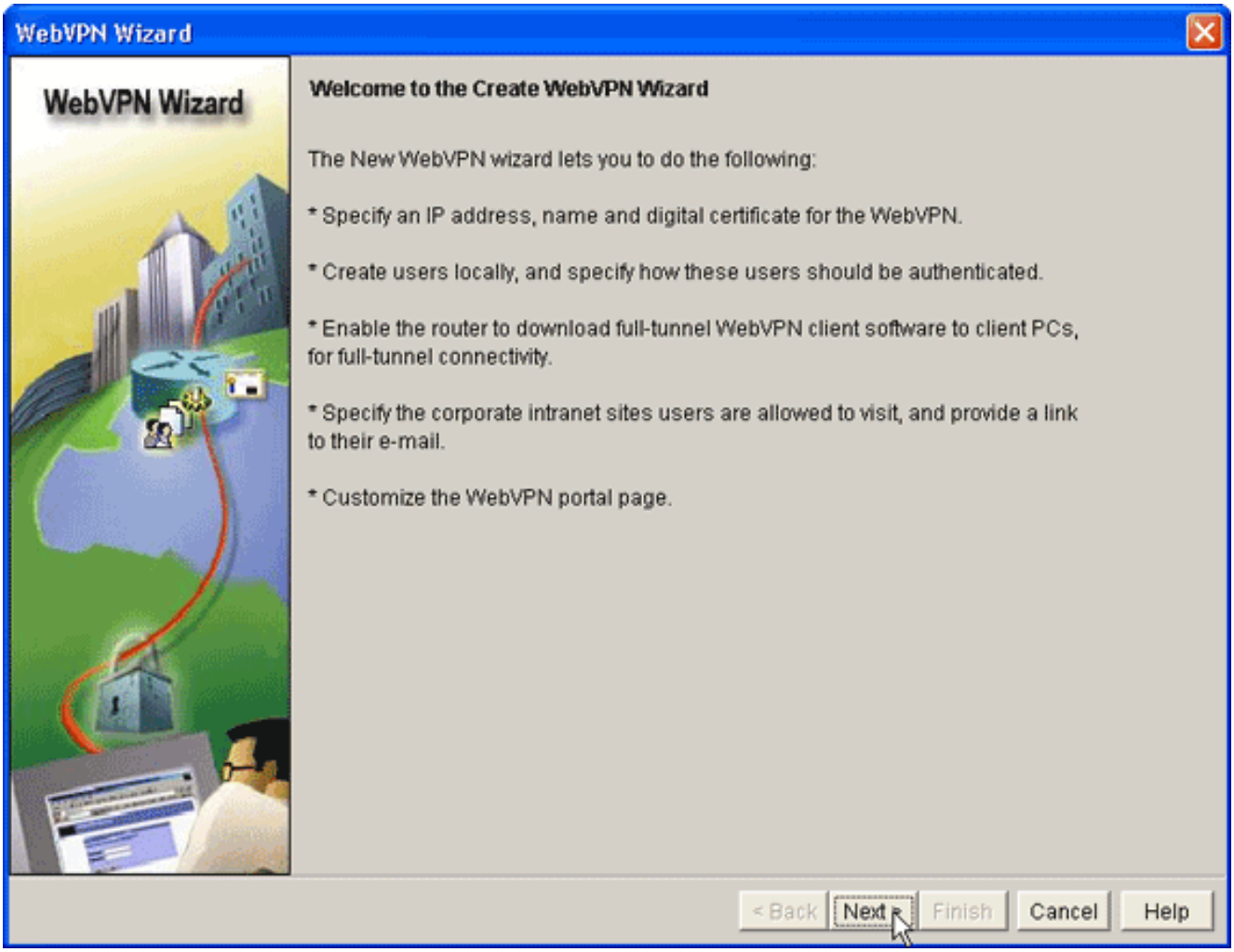
步骤 2. 使用 SDM 向导配置 WebVPN 上下文和 WebVPN 网关

要配置 WebVPN 上下文和 Webvpn 网关，请完成以下步骤：

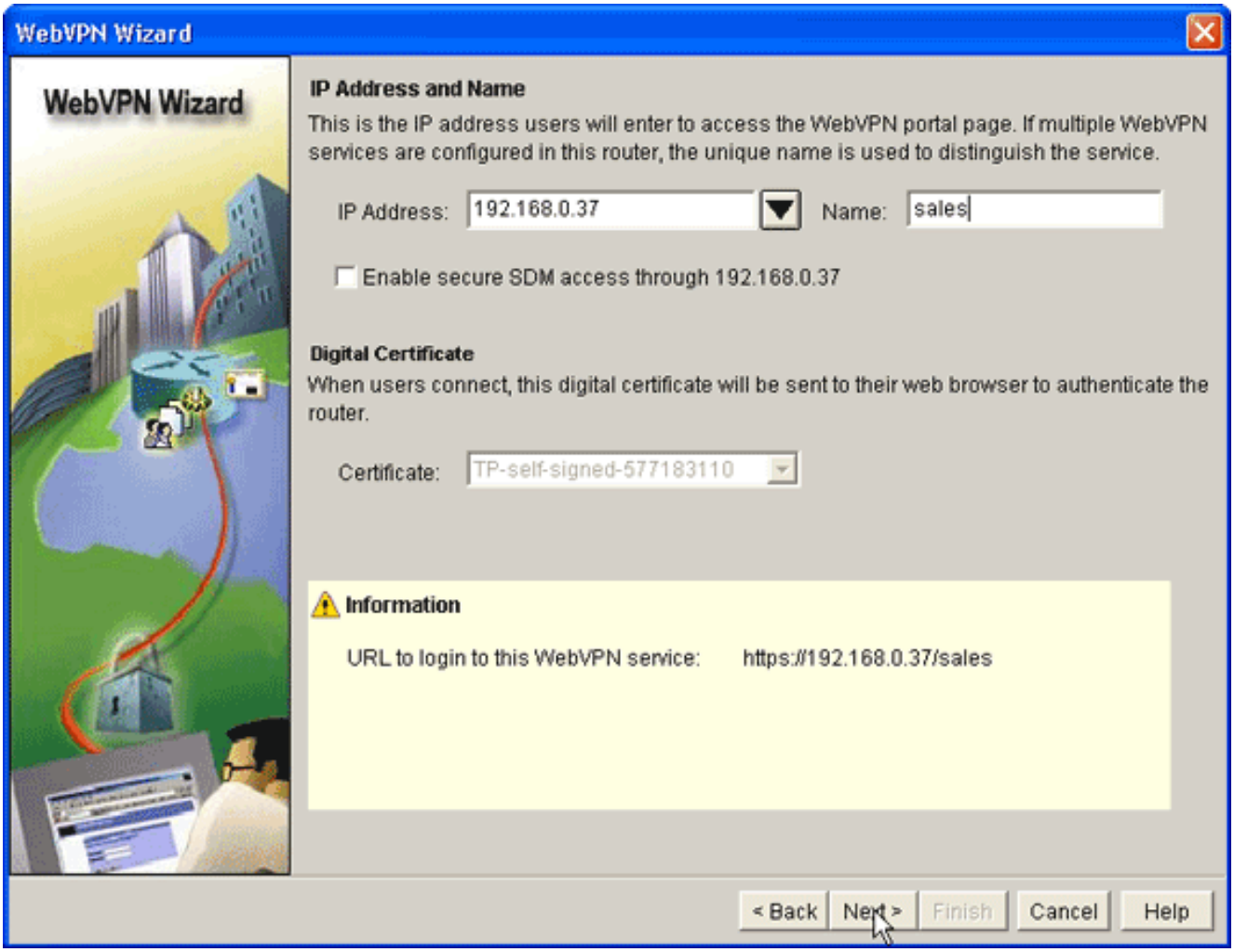
1. 将 SVC 安装在路由器上之后，请单击 **Configure**，然后单击 **VPN**。
2. 单击 **WebVPN**，然后单击 **Create WebVPN 选项卡**。



3. 选中 **Create a New WebVPN 单选按钮，然后单击 Launch the selected task**。此时将出现 WebVPN Wizard 对话框。


WebVPN Wizard
WebVPN Wizard
Welcome to the Create WebVPN Wizard
The New WebVPN wizard lets you to do the following:
* Specify an IP address, name and digital certificate for the WebVPN.
* Create users locally, and specify how these users should be authenticated.
* Enable the router to download full-tunnel WebVPN client software to client PCs, for full-tunnel connectivity.
* Specify the corporate intranet sites users are allowed to visit, and provide a link to their e-mail.
* Customize the WebVPN portal page.
< Back
Next >
Finish
Cancel
Help

4. 单击 **Next**。



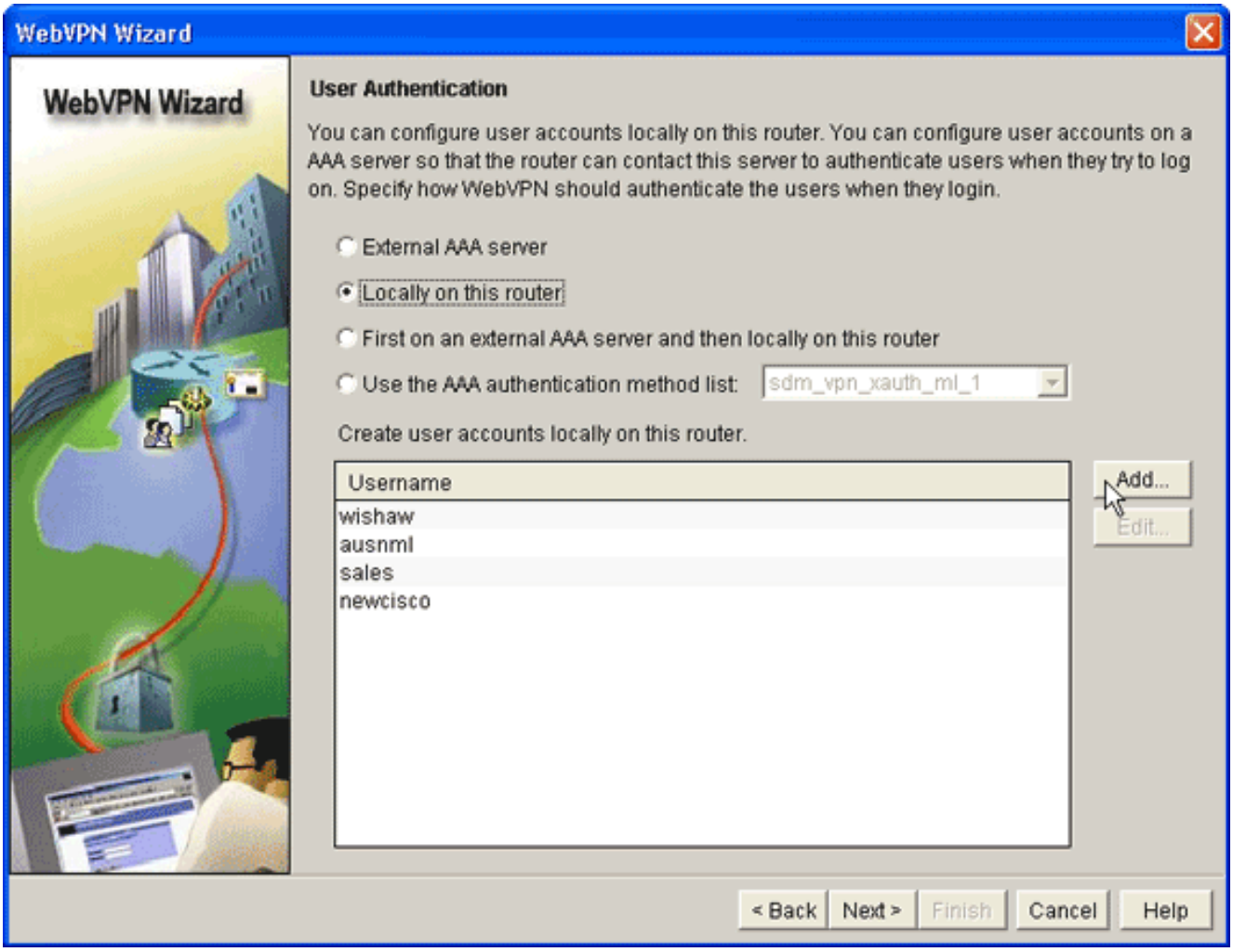
5. 输入新 Webvpn 网关的 IP 地址，并输入此 WebVPN 上下文的唯一名称。您可以为同一个 IP 地址（WebVPN 网关）创建不同的 WebVPN 上下文，但每个名称都必须唯一。本示例使用以下 IP 地址：*https://192.168.0.37/sales*
6. 单击 **Next**，继续进行步骤 3。

步骤 3. 配置 SVC 用户的用户数据库

您可以使用 AAA 服务器、本地用户或同时使用两者进行身份验证。本配置示例使用本地创建的用户进行身份验证。

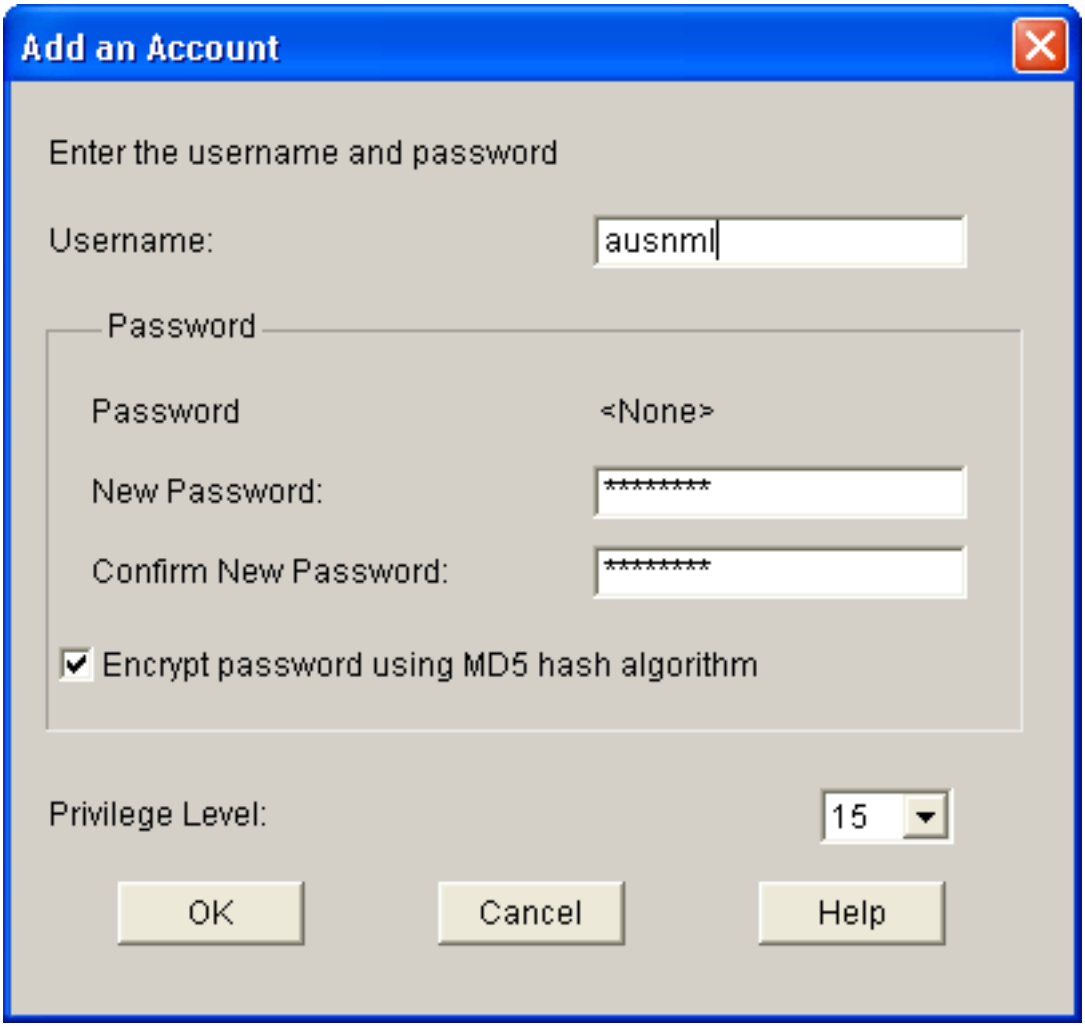
要配置 SVC 用户的用户数据库，请完成以下步骤：

1. 完成步骤 2 后，单击 WebVPN Wizard User Authentication 对话框中的 **Locally on this router 单选按钮。**



可以使用此对话框向本地数据库添加用户。

2. 单击 **Add**，然后输入用户信息。



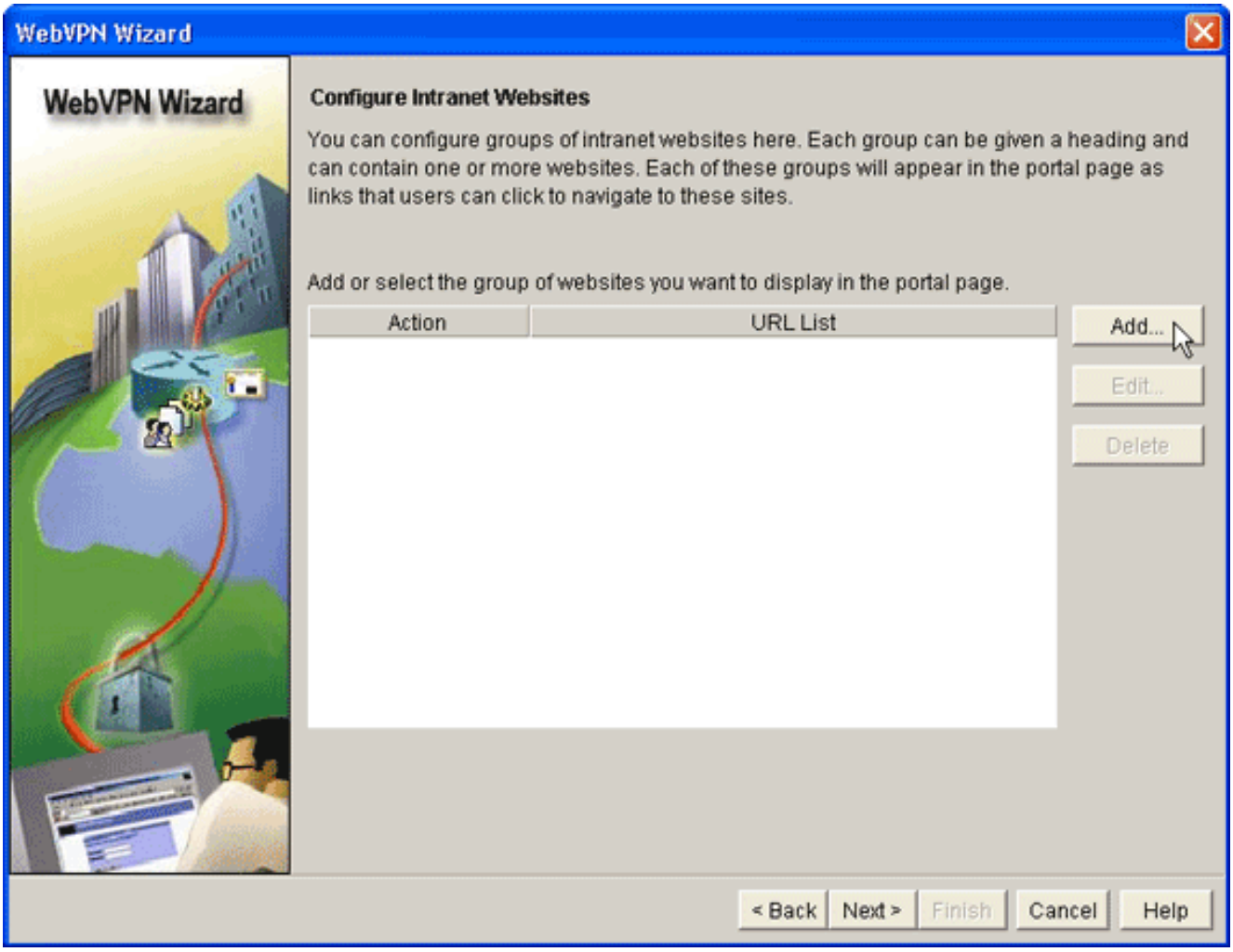
3. 单击 **OK**，并根据需要添加其他用户。
4. 添加所需用户后，单击 **Next**，继续进行步骤 4。

步骤 4. 配置面向用户的资源

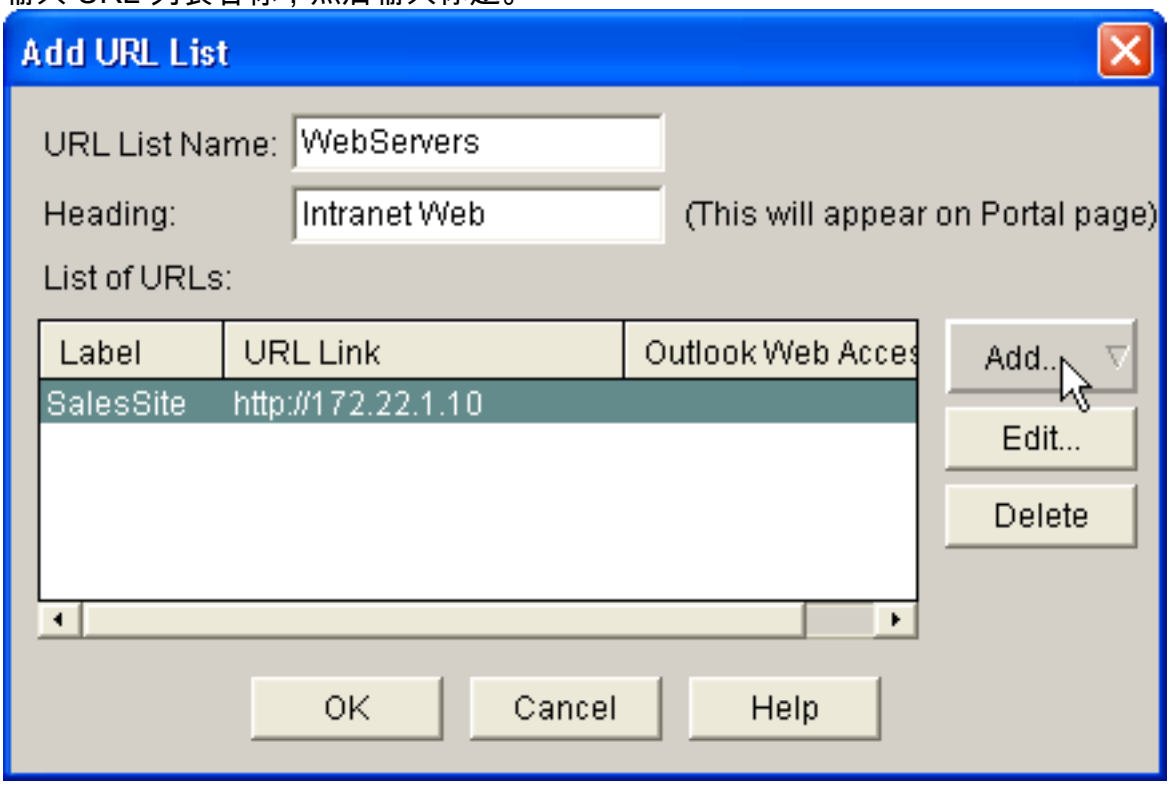
您可以通过 Configure Intranet Websites WebVPN Wizard 对话框，选择您希望向您的 SVC 客户端公开的内联网资源。

要配置面向用户的资源，请完成以下步骤：

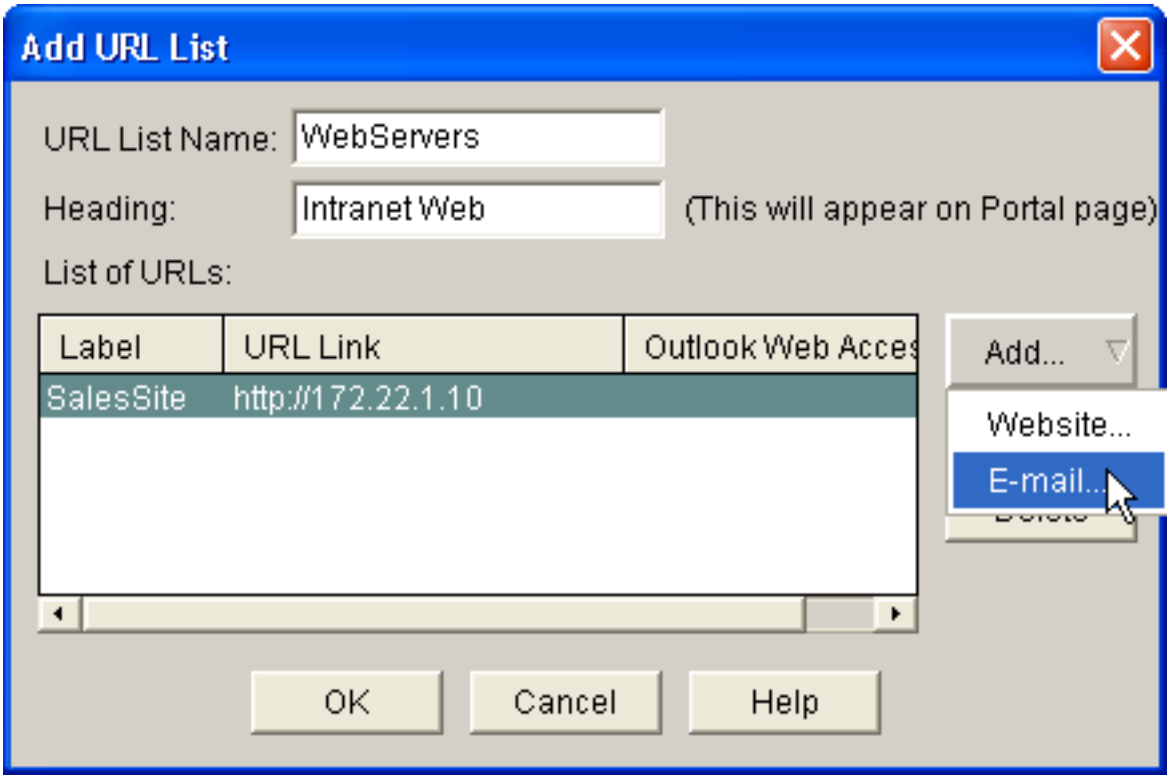
1. 在您完成步骤 3 后，请单击位于 Configure Intranet Websites 对话框内的 **Add 按钮。**



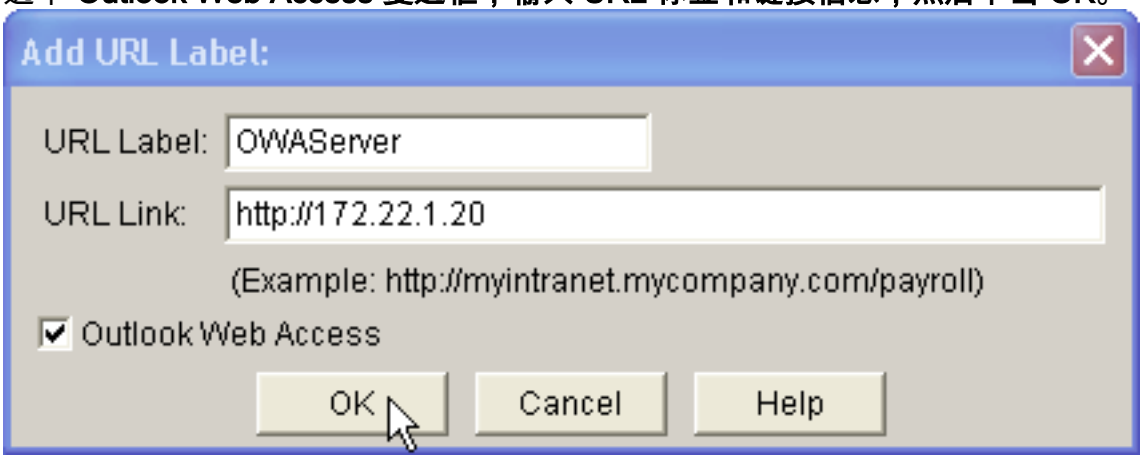
2. 输入 URL 列表名称，然后输入标题。



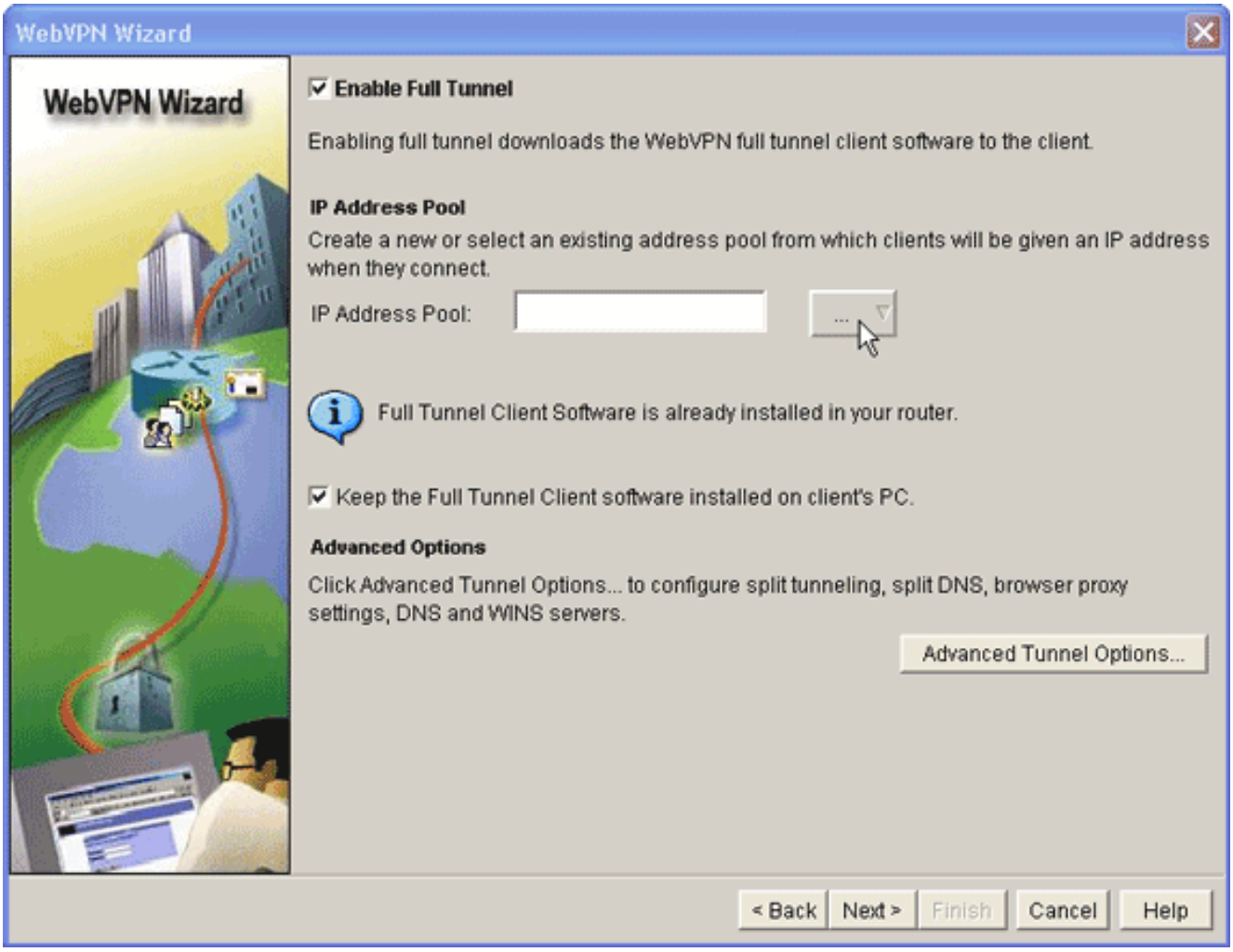
3. 单击 **Add**，并且选择 **Website，以添加您要向此客户端公开的网站。**
4. 输入 URL 和链接信息，然后单击 **OK**。
5. 要向 OWA Exchange 服务器添加访问，请单击 **Add 并选择 E-mail**。



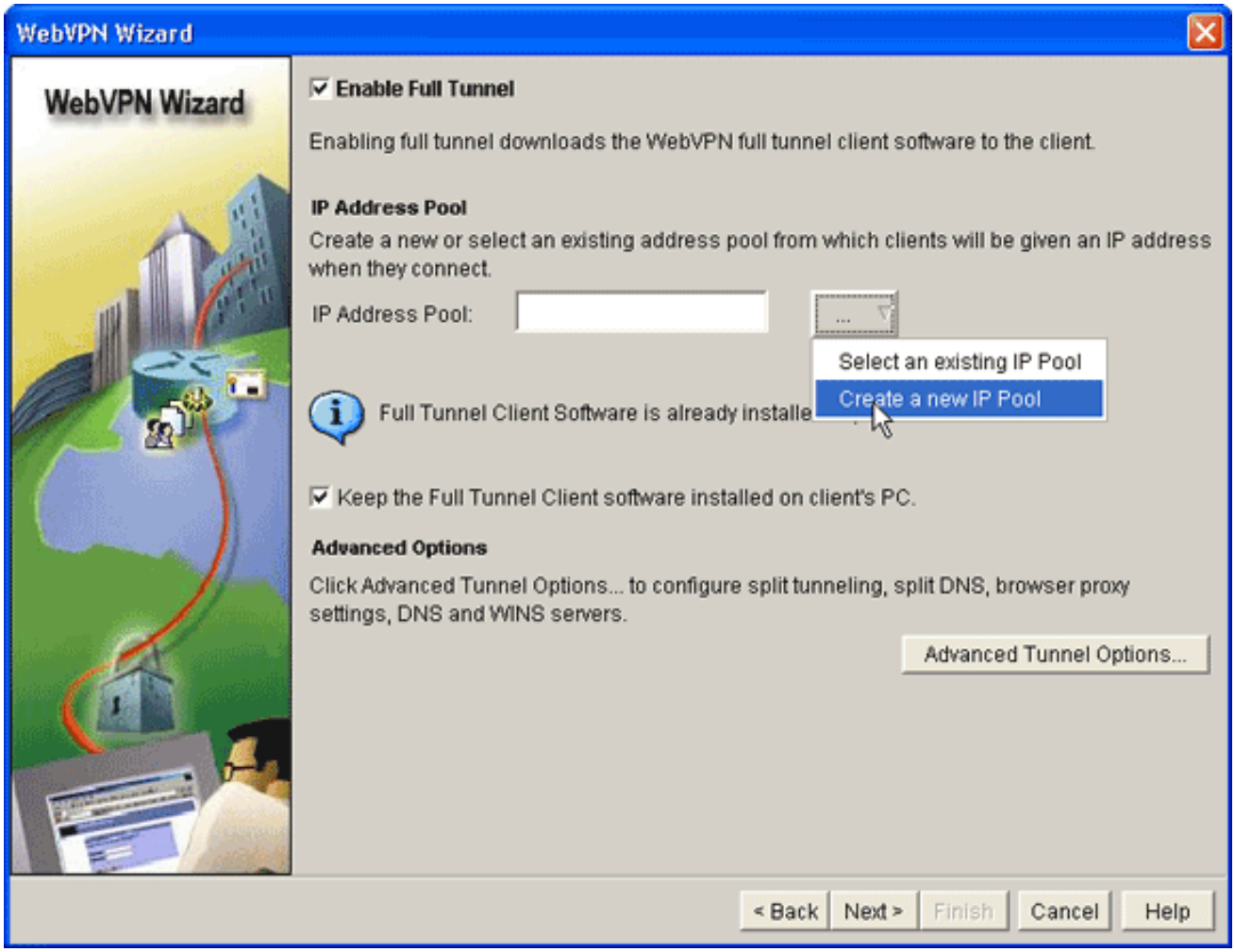
6. 选中 **Outlook Web Access 复选框，输入 URL 标签和链接信息，然后单击 OK。**



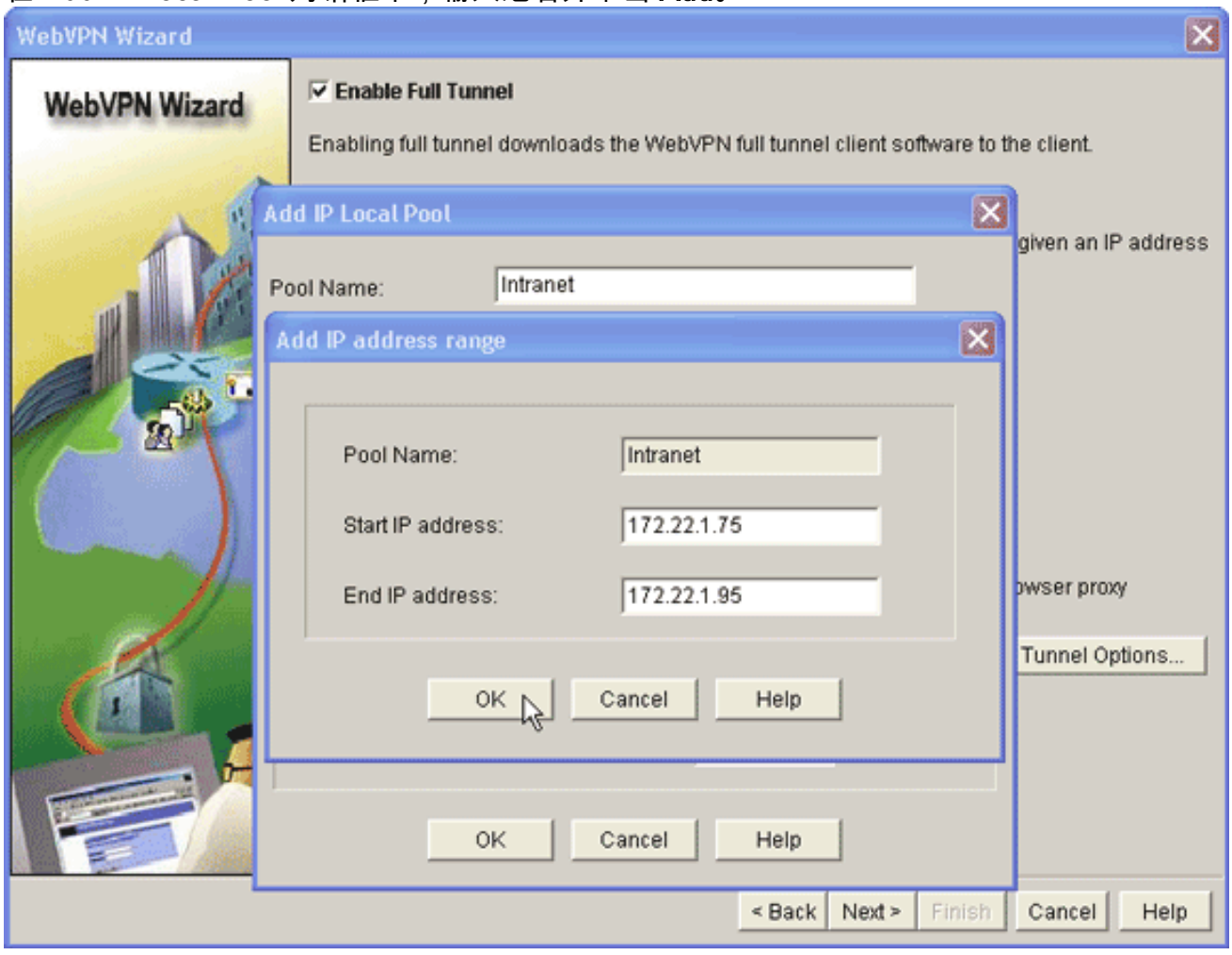
7. 在您添加所需资源后，单击 **OK**，然后单击 **Next**。此时将出现 WebVPN Wizard 全隧道对话框。



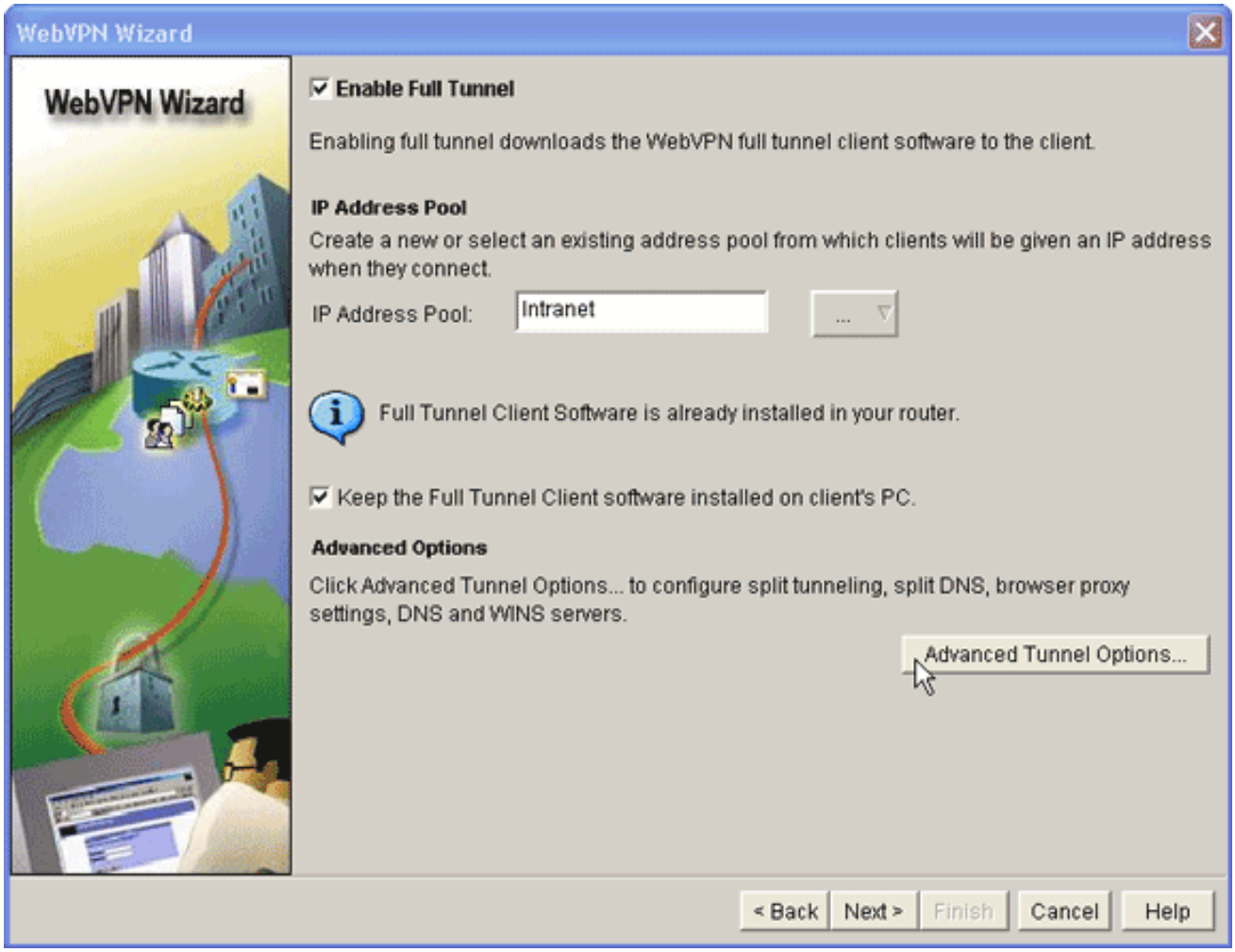
8. 确认 **Enable Full Tunnel 复选框已勾选。**
9. 创建此 WebVPN 上下文客户端可使用的 IP 地址池。地址池必须与 Intranet 上可用且可路由的地址相对应。
10. 单击 IP Address Pool 字段旁的省略号 (...)，选择 **Create a new IP Pool**。



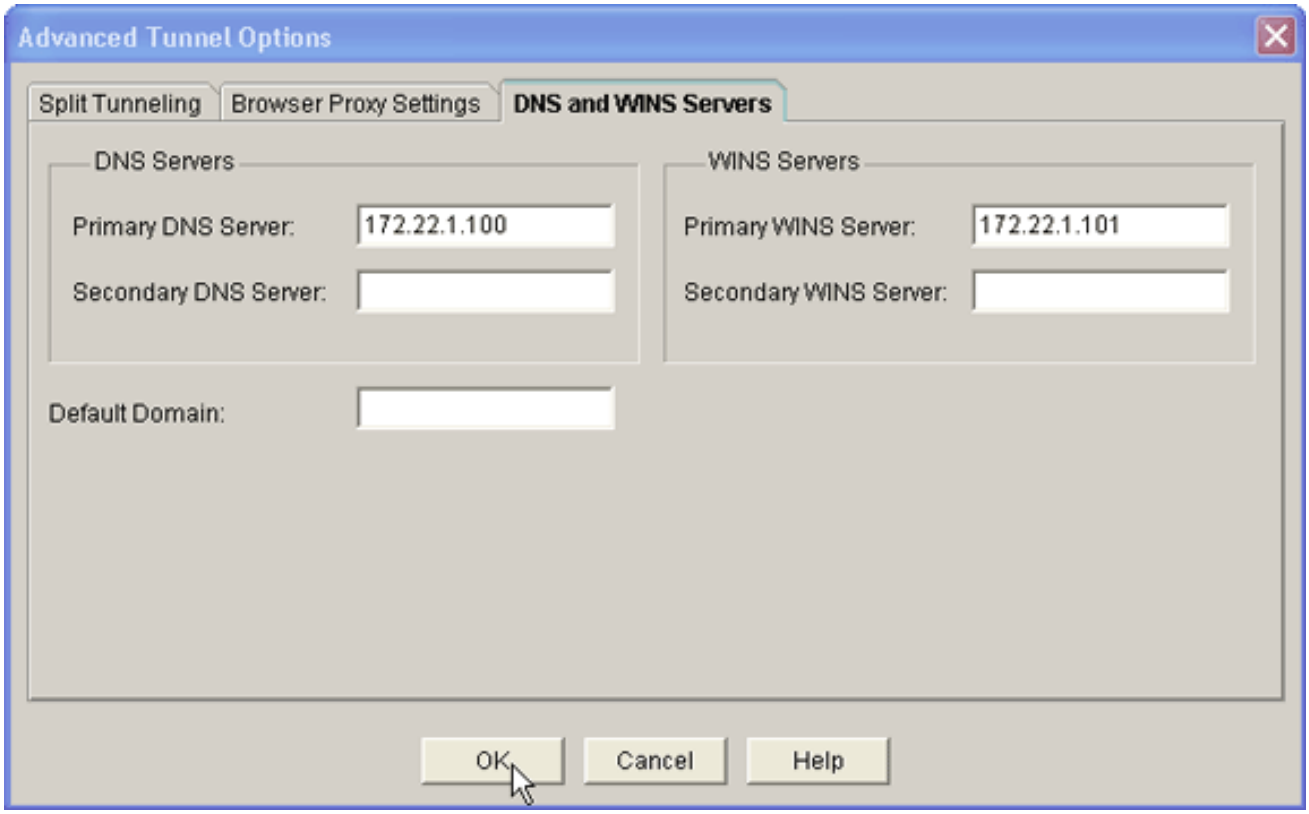
11. 在 Add IP Local Pool 对话框中，输入池名并单击 **Add**。



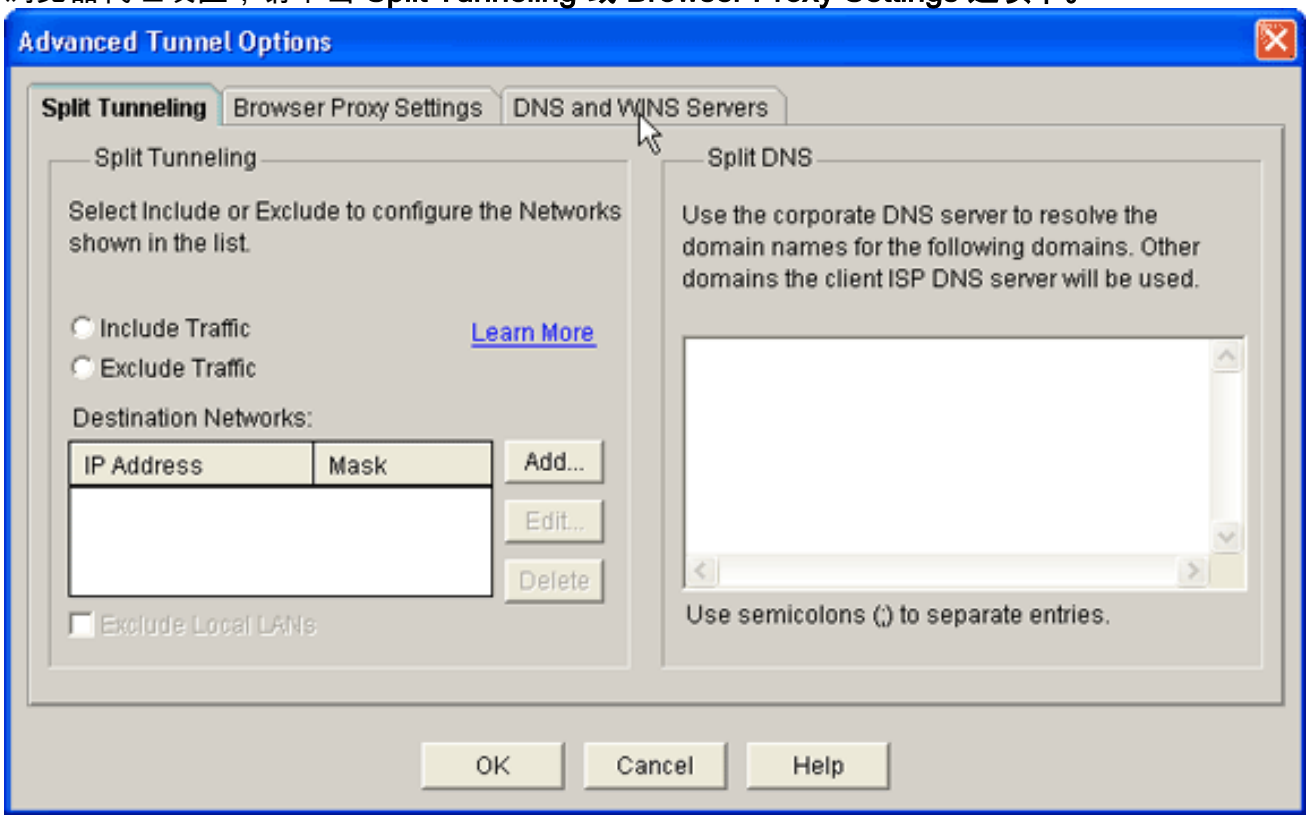
12. 在 Add IP address range 对话框中，输入 SVC 客户端的地址池范围，然后单击 **OK**。**注意**：IP地址池应位于直接连接到路由器的接口的范围内。如果要使用不同的池范围，可以创建与新池关联的环回地址，以满足该要求。
13. Click **OK**.



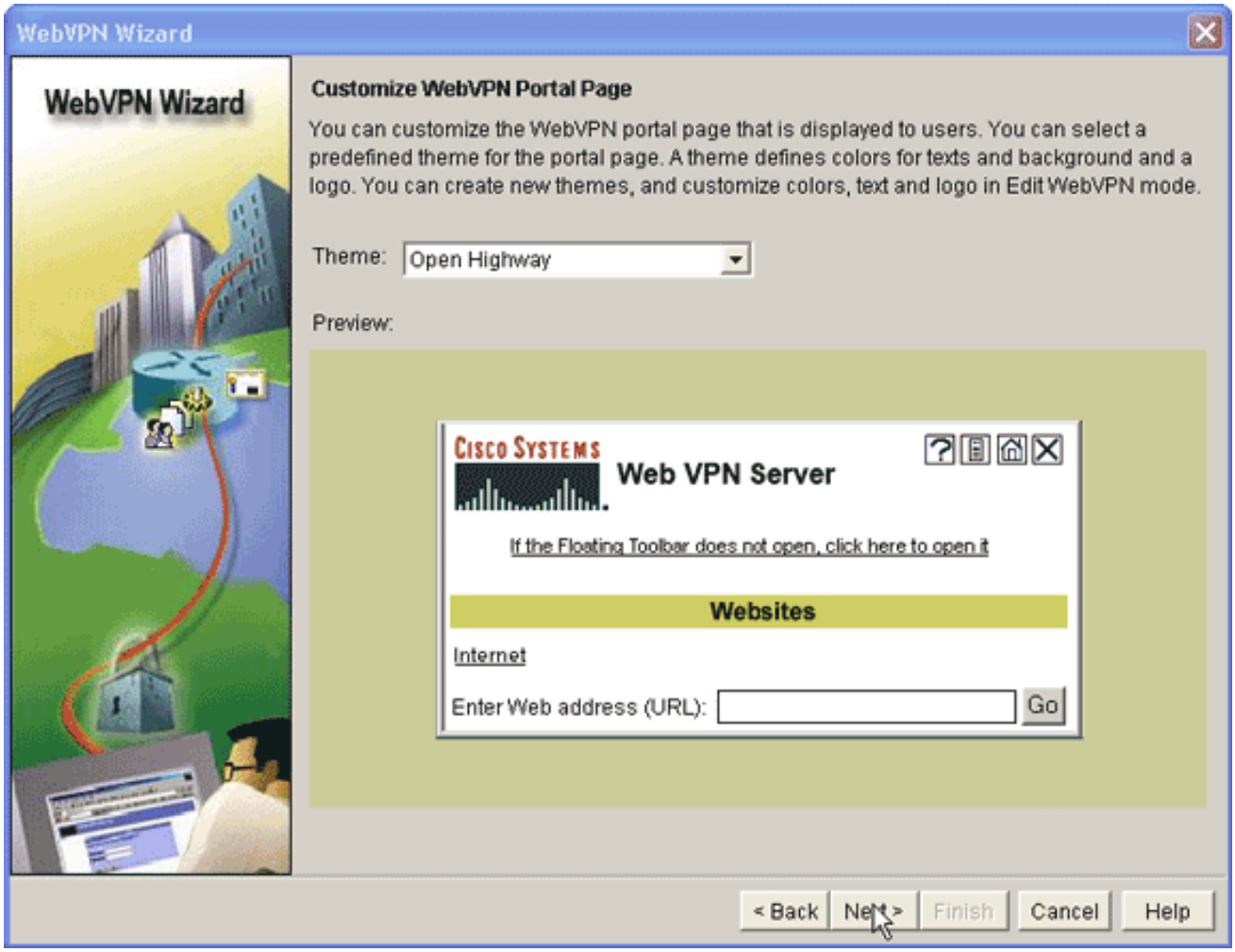
14. 如果您希望您的远程客户端永久存储 SVC 副本，请单击 **Keep the Full Tunnel Client Software installed on client's PC 复选框。**清除此选项，以要求客户端在每次客户端连接时下载SVC软件。
15. 配置高级隧道选项，如分割隧道、分割 DNS、浏览器代理设置以及 DNS 和 WNS 服务器等。Cisco 建议至少配置 DNS 和 WINS 服务器。要配置高级隧道选项，完成以下步骤：单击 **Advanced Tunnel Options 按钮。**



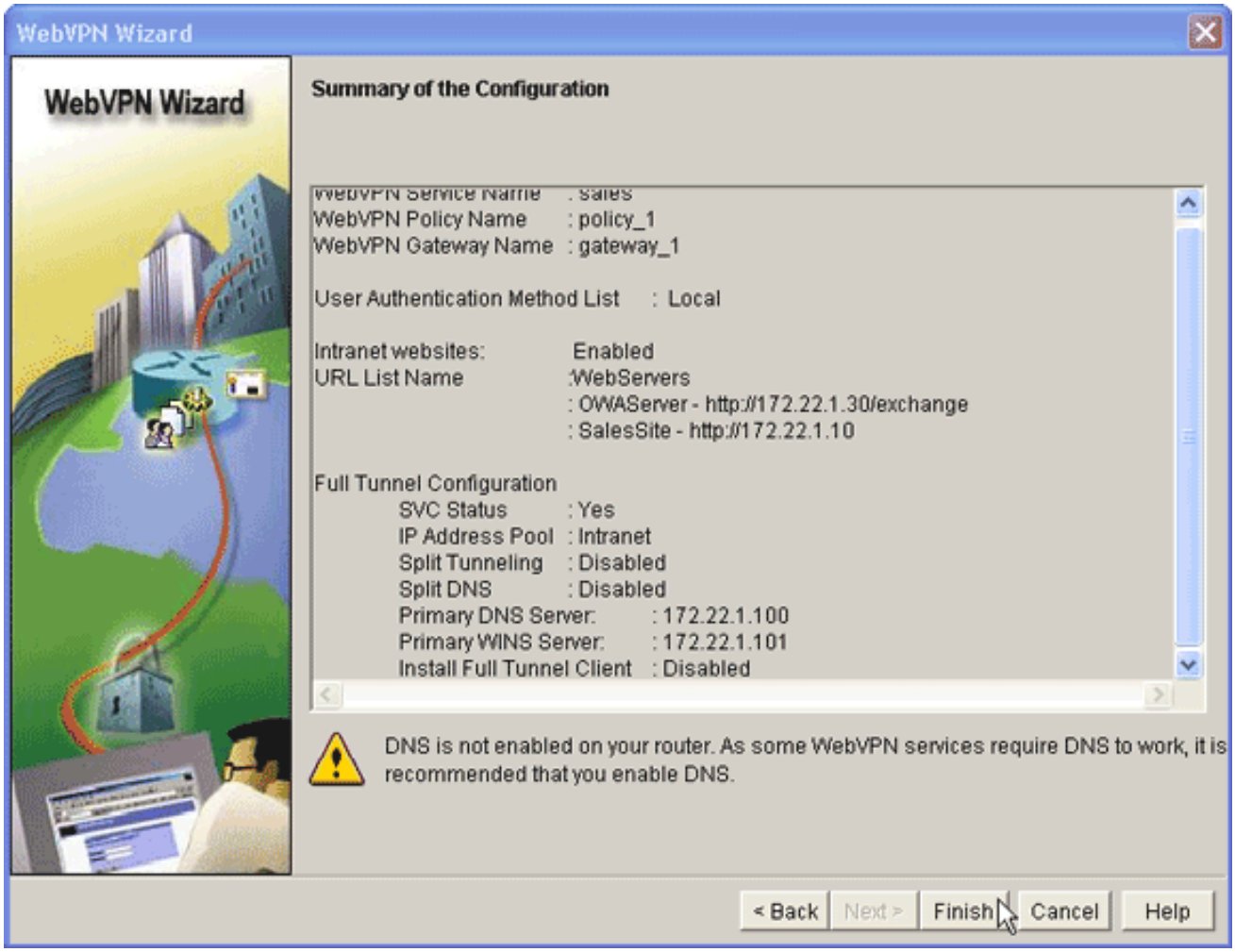
单击 **DNS and WINS Servers 选项卡，输入 DNS 和 WINS 的主 IP 地址。**要配置分割隧道和浏览器代理设置，请单击 **Split Tunneling 或 Browser Proxy Settings 选项卡。**



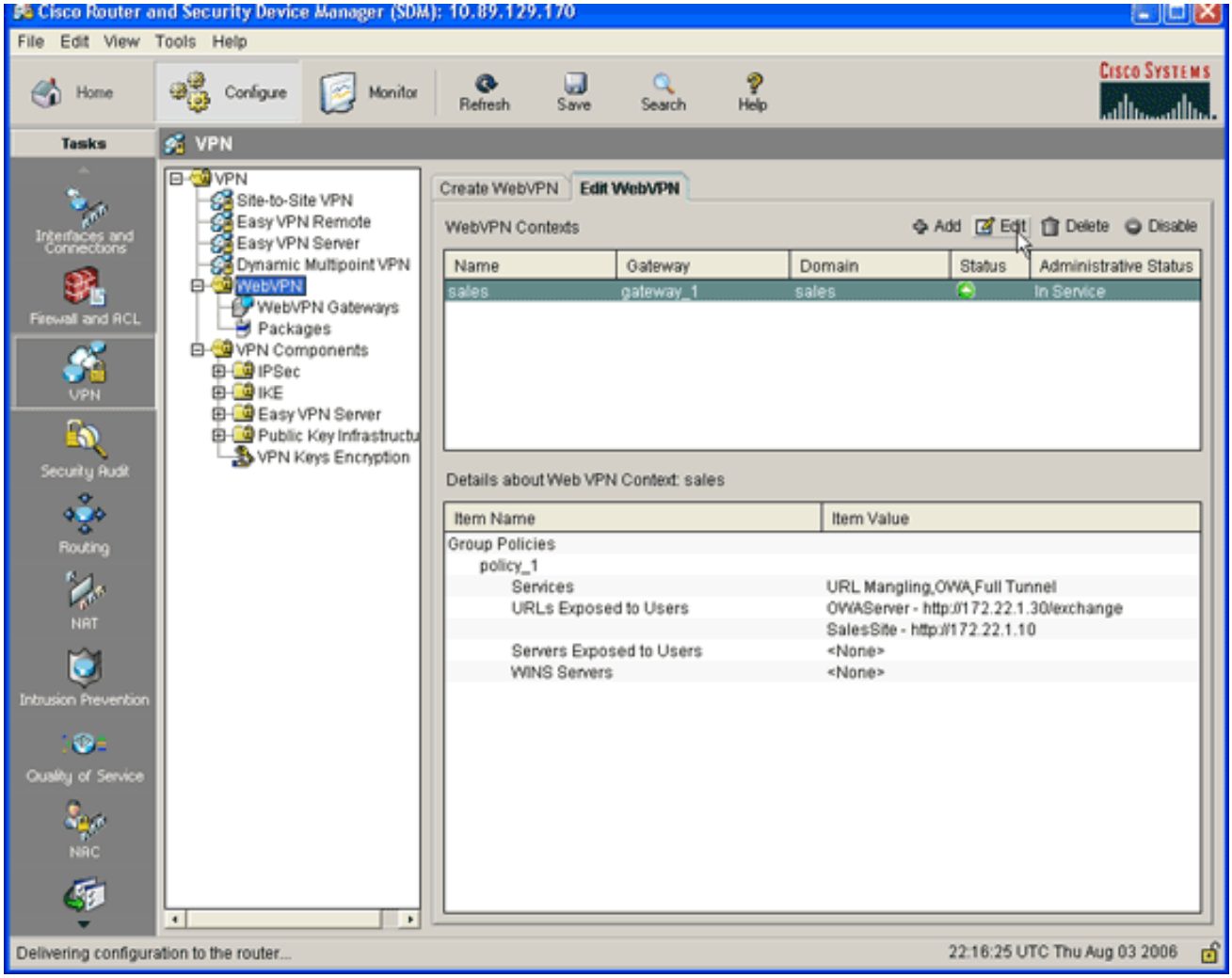
16. 完成必要选项配置后，单击 **Next**。
17. 自定义 WebVPN 门户页或选择默认值。通过 Customize WebVPN Portal Page 可以自定义向客户显示 WebVPN 门户页的方式。



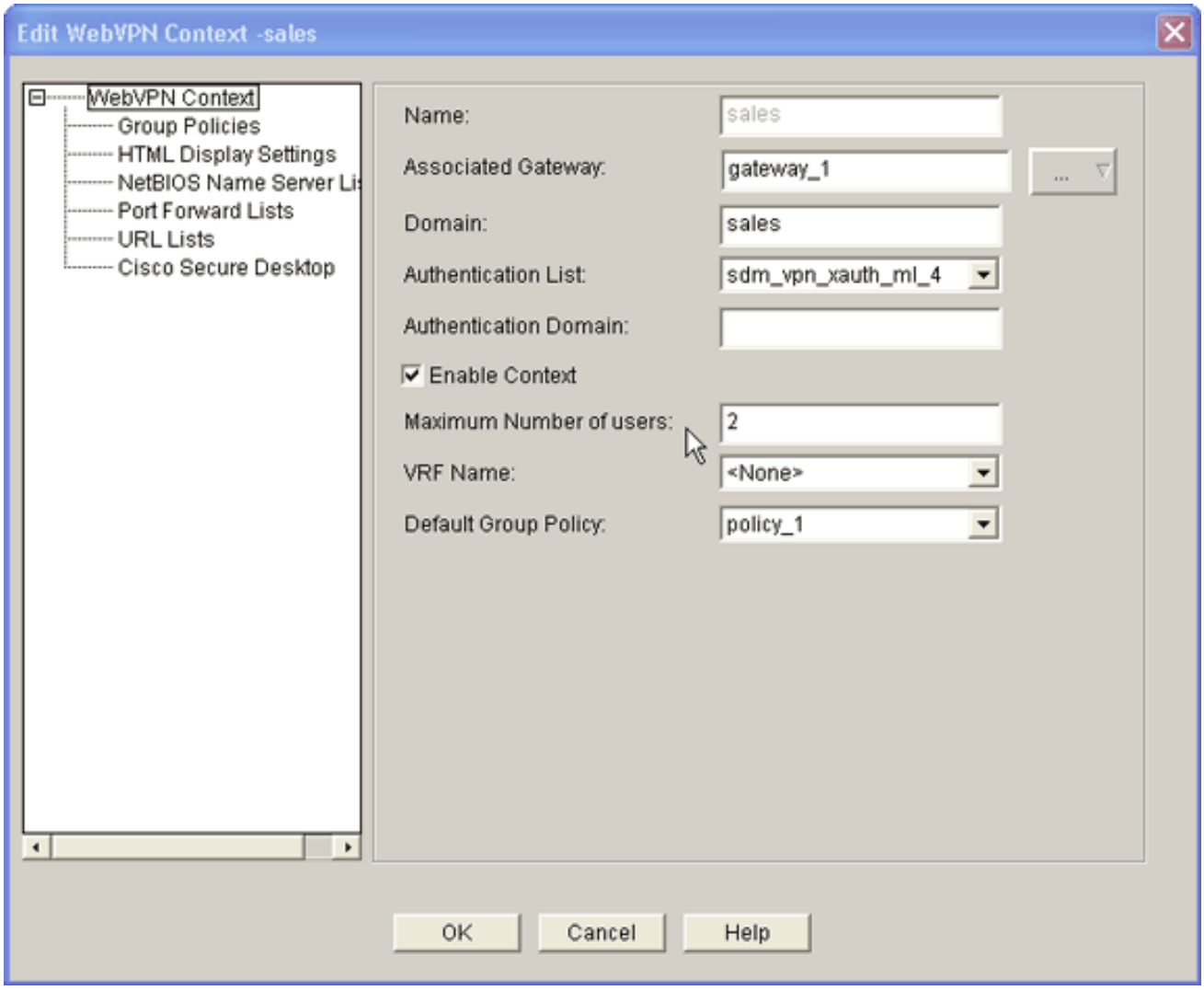
18. 在配置了 WebVPN 门户页之后，请依次单击 **Next**、**Finish** 和 **OK**。WebVPN 向导将浏览命令提交至路由器。
19. 单击“确定”保存所进行的配置。**注意：**如果收到错误消息，则WebVPN许可证可能不正确。以下图像显示了错误消息示例
    ：



要解决许可证问题，完成以下步骤：单击 **Configure**，然后单击 VPN。展开 **WebVPN** 并单击 **Edit WebVPN 选项卡。**



突出显示新建的上下文，并单击 **Edit button。**



在 Maximum Number of users 字段中，输入许可证允许的正确用户数。单击 **OK**，再单击 OK。您的命令已写入配置文件。单击 **Save**，然后单击 Yes 接受更改。

结果

ASDM 创建了以下这些命令行配置：

ausnml-3825-01

```
ausnml-3825-01#show run
Building configuration...

Current configuration : 4393 bytes
!
! Last configuration change at 22:24:06 UTC Thu Aug 3
2006 by ausnml
! NVRAM config last updated at 22:28:54 UTC Thu Aug 3
2006 by ausnml
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname ausnml-3825-01
!
boot-start-marker
```

```
boot system flash c3825-adventerprisek9-mz.124-9.T.bin
boot-end-marker
!
no logging buffered
!
aaa new-model
!
!--- Added by SDM for local aaa authentication. aaa
authentication login sdm_vpn_xauth_ml_1 local aaa
authentication login sdm_vpn_xauth_ml_2 local aaa
authentication login sdm_vpn_xauth_ml_3 local aaa
authentication login sdm_vpn_xauth_ml_4 local ! aaa
session-id common ! resource policy ! ip cef ! ip domain
name cisco.com ! voice-card 0 no dspfarm !--- Digital
certificate information. crypto pki trustpoint TP-self-
signed-577183110 enrollment selfsigned subject-name
cn=IOS-Self-Signed-Certificate-577183110 revocation-
check none rsakeypair TP-self-signed-577183110 ! crypto
pki certificate chain TP-self-signed-577183110
certificate self-signed 01 3082024E 308201B7 A0030201
02020101 300D0609 2A864886 F70D0101 04050030 30312E30
2C060355 04031325 494F532D 53656C66 2D536967 6E65642D
43657274 69666963 6174652D 35373731 38333131 30301E17
0D303630 37323731 37343434 365A170D 32303031 30313030
30303030 5A303031 2E302C06 03550403 1325494F 532D5365
6C662D53 69676E65 642D4365 72746966 69636174 652D3537
37313833 31313030 819F300D 06092A86 4886F70D 01010105
0003818D 00308189 02818100 F43F6DD9 32A264FE 4C5B0829
698265DC 6EC65B17 21661972 D363BC4C 977C3810 !--- Output
suppressed. quit username wishaw privilege 15 secret 5
$1$r4CW$SeP6ZwQEAAU68W9kbR16U. username ausnml privilege
15 password 7 044E1F505622434B username sales privilege
15 secret 5 $1$/Lc1$K.Zt41zF1jSdKZrPgNK1A. username
newcisco privilege 15 secret 5
$1$Axlm$7k5PWspXKxUpoSReHo7IQ1 ! interface
GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0
ip virtual-reassembly duplex auto speed auto media-type
rj45 no keepalive ! interface GigabitEthernet0/1 ip
address 172.22.1.151 255.255.255.0 duplex auto speed
auto media-type rj45 !--- Clients receive an address
from this pool. ip local pool Intranet 172.22.1.75
172.22.1.95 ip route 0.0.0.0 0.0.0.0 172.22.1.1 ! ip
http server ip http authentication local ip http secure-
server ip http timeout-policy idle 600 life 86400
requests 100 ! control-plane ! line con 0 stopbits 1
line aux 0 stopbits 1 line vty 0 4 ! scheduler allocate
20000 1000 !--- Identify the gateway and port. webvpn
gateway gateway_1 ip address 192.168.0.37 port 443 http-
redirect port 80 ssl trustpoint TP-self-signed-577183110
inservice !--- SVC package file. webvpn install svc
flash:/webvpn/svc.pkg ! !--- WebVPN context. webvpn
context sales title-color #CCCC66 secondary-color white
text-color black ssl authenticate verify all ! !---
Resources available to this context. url-list
"WebServers" heading "Intranet Web" url-text "SalesSite"
url-value "http://172.22.1.10" url-text "OWAServer" url-
value "http://172.22.1.20/exchange" ! nbns-list NBNS-
Servers nbns-server 172.22.1.15 master !--- Group policy
for the context. policy group policy_1 url-list
"WebServers" functions svc-enabled svc address-pool
"Intranet" svc default-domain "cisco.com" svc keep-
client-installed svc dns-server primary 172.22.1.100 svc
wins-server primary 172.22.1.101 default-group-policy
policy_1 aaa authentication list sdm_vpn_xauth_ml_4
```

```
gateway gateway_1 domain sales max-users 2 inservice ! !
end
```

验证

使用本部分可确认配置能否正常运行。

步骤

要测试您的配置，请将 *http://192.168.0.37/sales 输入到启用了 SSL 的客户端 Web 浏览器。*

命令

有若干 **show 命令与 WebVPN 关联。**可以在命令行界面 (CLI) 上执行这些命令以显示统计信息和其他信息。有关 **show 命令的详细信息，请参阅**验证 WebVPN 配置。

注意：输出解释器工具(仅注册客户)(OIT)支持某些**show**命令。使用 OIT 可查看对 show 命令输出的分析。

故障排除

使用本部分可排除配置故障。

SSL 连接问题

问题：SSL VPN 客户端无法连接路由器。

解决方案：导致该问题的原因可能是 IP 地址池中的地址不足。可增加路由器 IP 地址池中的地址数，以解决该问题。

故障排除命令

有若干 **clear 命令与 WebVPN 关联。**有关这些命令的详细信息，请参阅"使用 WebVPN Clear 命令"。

有若干 **debug 命令与 WebVPN 关联。**有关这些命令的详细信息，请参阅使用 WebVPN Debug 命令。

注意：使用debug命令可能会对Cisco设备造成负面影响。使用 debug 命令之前，请参阅**有关 Debug 命令的重要信息。**

相关信息

- Cisco IOS SSLVPN
- SSL VPN - WebVPN
- 有 SDM 的 Cisco IOS 的无客户端 SSL VPN (WebVPN) 配置示例
- 使用 SDM 的瘦客户端 SSL VPN (WebVPN) IOS 配置示例
- WebVPN 和 DMVPN 融合部署指南

- 技术支持和文档 - Cisco Systems