使用SDM配置瘦客戶端SSL VPN(WebVPN)Cisco IOS

目錄

簡介

瘦客戶端SSL VPN技術可用於允許使用靜態埠的應用程式進行安全訪問。例如Telnet(23)、SSH(22)、POP3(110)、IMAP4(143)和SMTP(25)。 瘦客戶端可以是使用者驅動的、策略驅動的，也可以是兩者兼而有之。可以逐個使用者配置訪問，也可以建立包含一個或多個使用者的組策略。SSL VPN技術可以在三種主要模式下配置：無客戶端SSL VPN(WebVPN)、瘦客戶端SSL VPN（埠轉發）和SSL VPN客戶端（SVC全通道模式）。

1.無客戶端SSL VPN(WebVPN):

遠端客戶端僅需要一個啟用SSL的Web瀏覽器來訪問公司LAN上啟用http或https的Web伺服器。還可以通過通用網際網路檔案系統(CIFS)瀏覽Windows檔案。Outlook Web Access(OWA)客戶端便是http訪問的典型示例。

請參閱使用SDM的Cisco IOS上的無客戶端SSL VPN(WebVPN)配置示例，瞭解有關無客戶端SSL VPN的詳細資訊。

2.瘦客戶端SSL VPN（埠轉發）

遠端客戶端必須下載基於Java的小程式，以便安全訪問使用靜態埠號的TCP應用程式。不支援UDP。示例包括對POP3、SMTP、IMAP、SSH和Telnet的訪問。使用者需要本地管理許可權，因

為會更改本地電腦上的檔案。這種SSL VPN的方法不適用於使用動態埠分配的應用程式，例如多個FTP應用程式。

3. SSL VPN客戶端（SVC — 全通道模式）：

SSL VPN客戶端將小型客戶端下載到遠端工作站，並允許對內部公司網路上的資源進行完全、安全的訪問。SVC可以永久下載到遠端站點，也可以在安全會話結束後刪除。

請參閱使用SDM的IOS上的SSL VPN客戶端(SVC)配置示例，瞭解有關SSL VPN客戶端的詳細資訊。

本檔案將示範精簡使用者端SSL VPN在Cisco IOS® 路由器上的簡單設定。瘦客戶端SSL VPN在這些思科IOS路由器上運行：

- Cisco 870、1811、1841、2801、2811、2821和2851系列路由器
- Cisco 3725、3745、3825、3845、7200和7301系列路由器

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

Cisco IOS路由器的要求

- 列出的所有裝有SDM和IOS版本12.4(6)T或更高版本的高級映像的路由器
- 裝有SDM的管理站Cisco將新路由器附帶預裝的SDM副本。如果路由器未安裝SDM，可從Software Download-Cisco Security Device Manager獲取軟體。您必須擁有具有服務合約的CCO帳戶。有關詳細說明，請參閱使用安全裝置管理器配置路由器。

客戶端電腦的要求

- 遠端客戶端應具有本地管理許可權；這不是必需的，但強烈建議這樣做。
- 遠端客戶端必須具有Java Runtime Environment(JRE)1.4版或更高版本。
- 遠端客戶端瀏覽器：Internet Explorer 6.0、Netscape 7.1、Mozilla 1.7、Safari 1.2.2或Firefox 1.0
- 在遠端客戶端上啟用Cookie和允許彈出視窗

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科進階企業軟體映像12.4(9)T
- 思科3825整合式服務路由器
- Cisco路由器和安全裝置管理員(SDM)版本2.3.1

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態開始。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。用於此配置的IP地址來自RFC 1918地址空間。它們在網際網路上是不合法的。

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

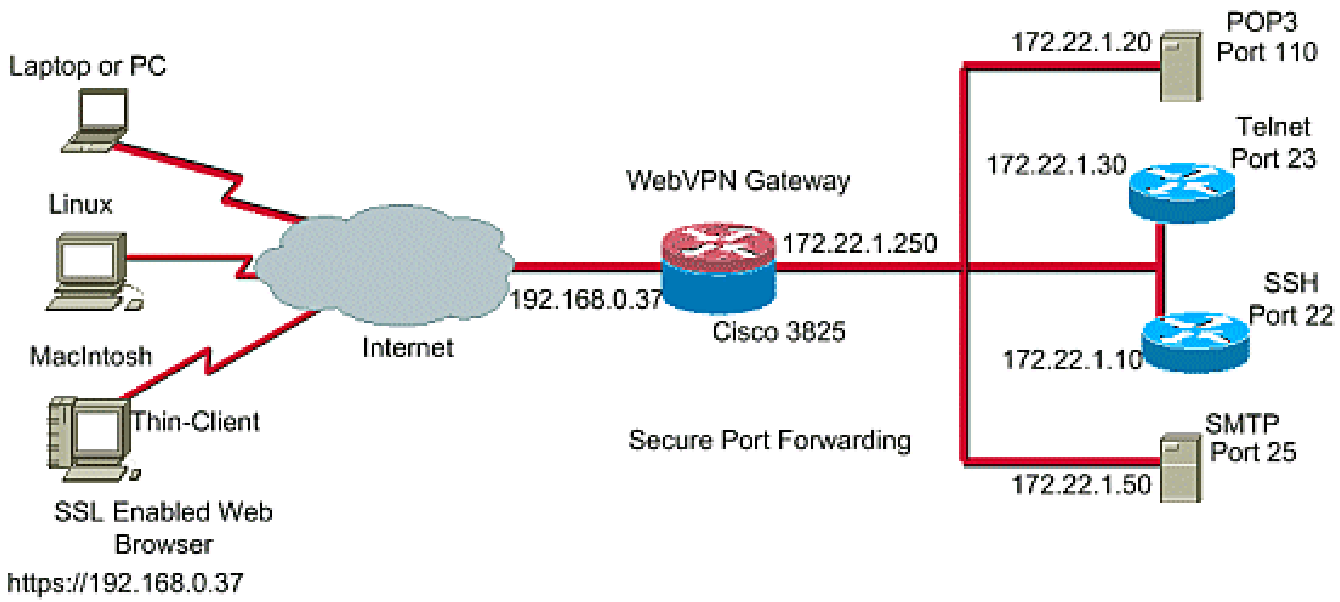
設定

工作

本節包含設定本檔案中所述功能所需的資訊。

網路圖表

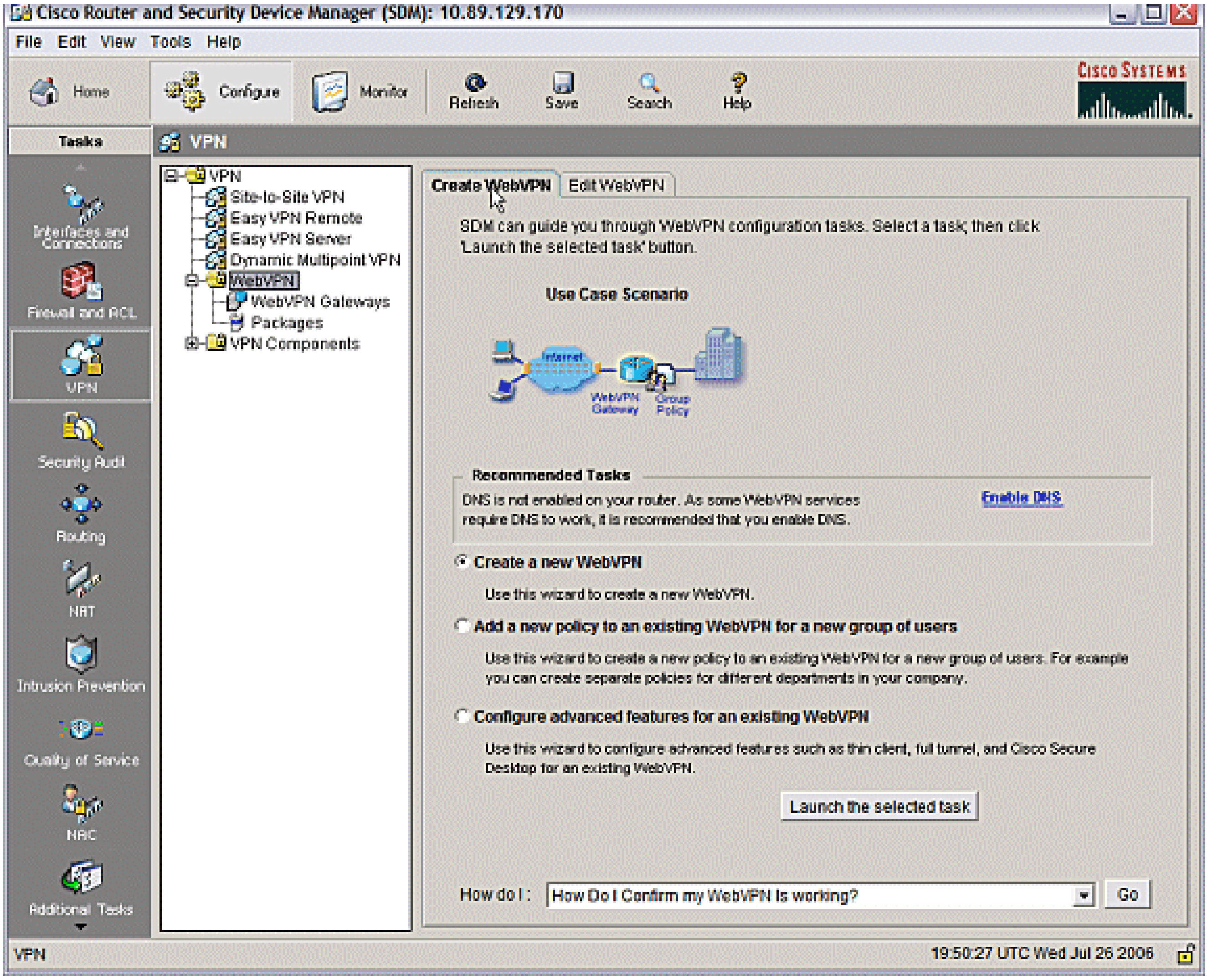
本檔案會使用以下網路設定：



配置瘦客戶端SSL VPN

使用安全裝置管理器(SDM)介面中提供的嚮導在Cisco IOS上配置瘦客戶端SSL VPN，或者在命令列介面(CLI)或在SDM應用程式中手動配置它。此示例使用嚮導。

1. 選擇**Configure**頁籤。在導航窗格中，選擇**VPN > WebVPN**。按一下**Create WebVPN**頁籤。按一下**Create a new WebVPN**旁邊的單選按鈕。按一下**啟動所選任務**按鈕。



SDM can guide you through WebVPN configuration tasks. Select a task; then click 'Launch the selected task' button.

Recommended Tasks

DNS is not enabled on your router. As some WebVPN services require DNS to work, it is recommended that you enable DNS.

● Create a new WebVPN

Use this wizard to create a new WebVPN.

○ Add a new policy to an existing WebVPN for a new group of users

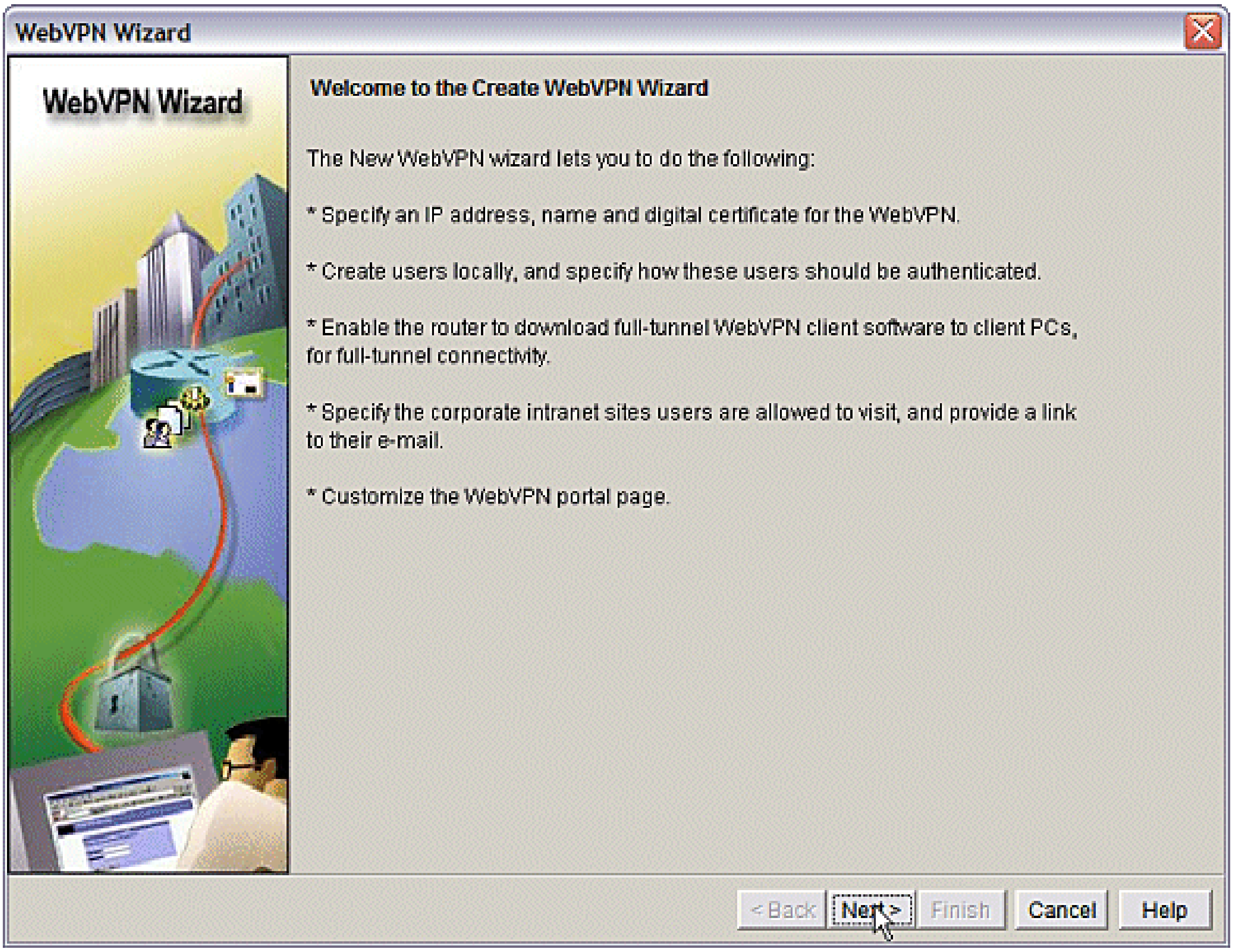
Use this wizard to create a new policy to an existing WebVPN for a new group of users. For example you can create separate policies for different departments in your company.

○ Configure advanced features for an existing WebVPN

Use this wizard to configure advanced features such as thin client, full tunnel, and Cisco Secure Desktop for an existing WebVPN.

How do I: How Do I Confirm my WebVPN is working?

2. WebVPN嚮導啟動。按「**Next**」（下一步）。



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.

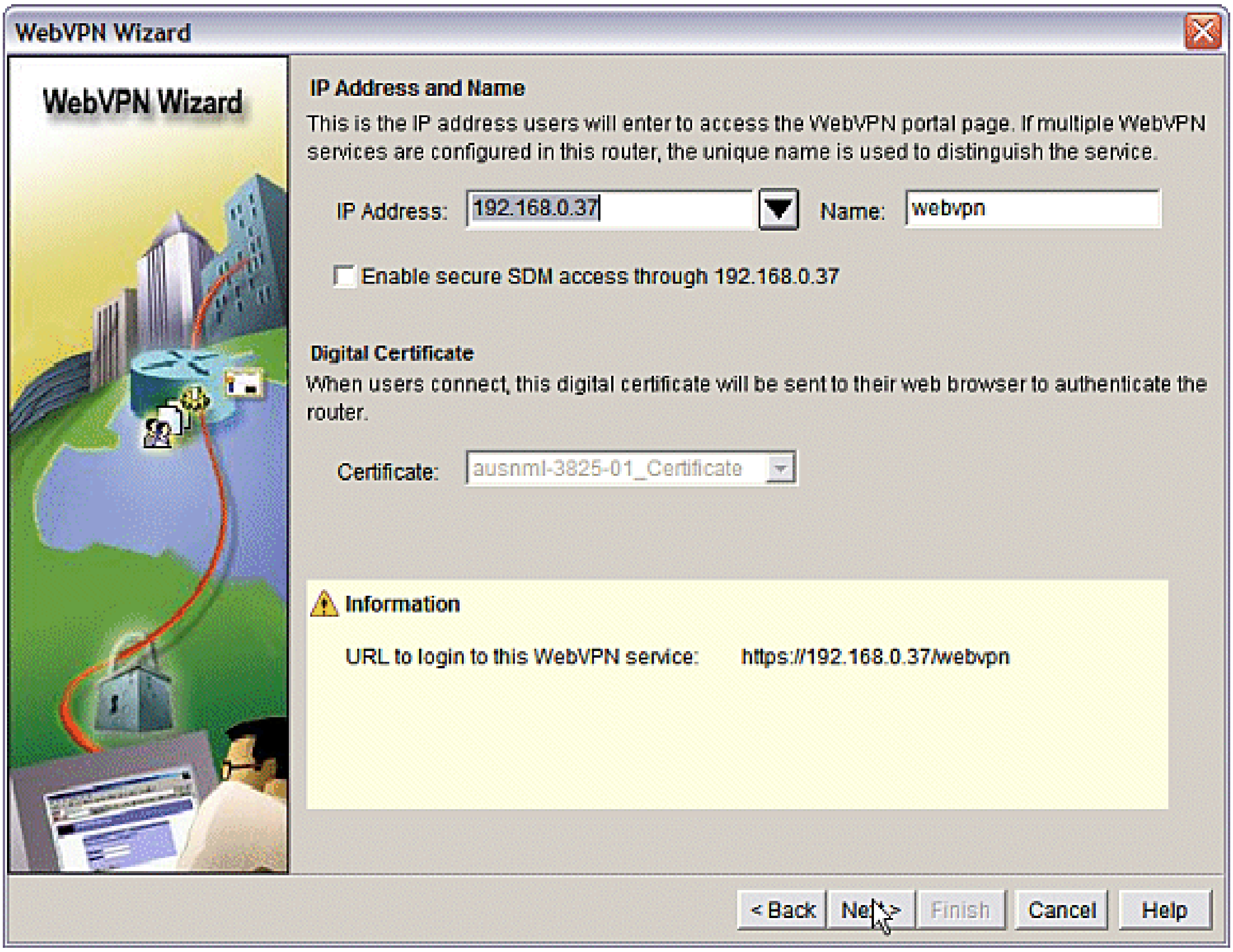
* Create users locally, and specify how these users should be authenticated.

* 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.

輸入此WebVPN網關的IP地址和唯一名稱。按「**Next**」（下一步）。



IP Address and Name

This is the IP address users will enter to access the WebVPN portal page. If multiple WebVPN services are configured in this router, the unique name is used to distinguish the service.

IP Address: 192.168.0.37 Name: webvpn

□ Enable secure SDM access through 192.168.0.37

Digital Certificate

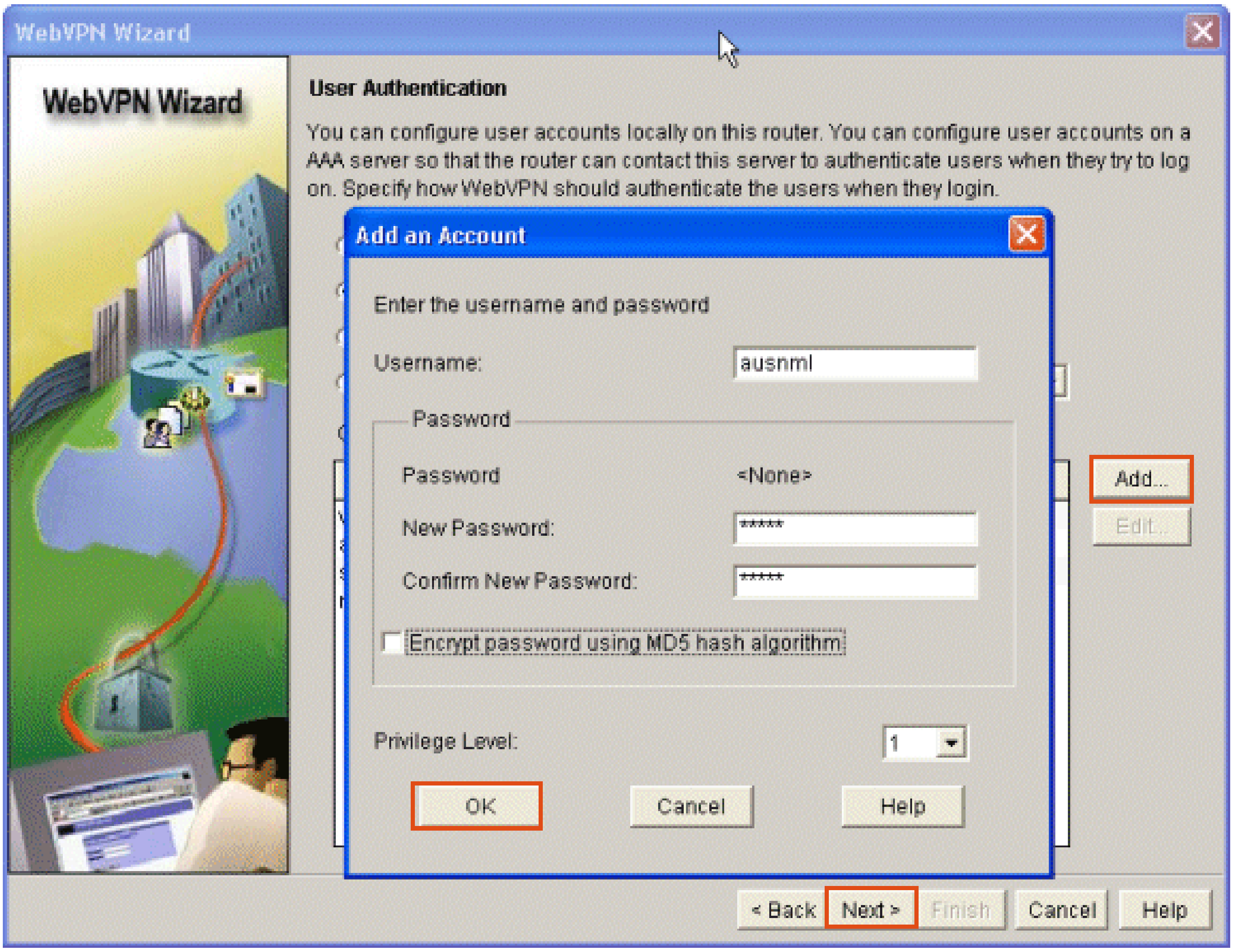
When users connect, this digital certificate will be sent to their web browser to authenticate the router.

Certificate: ausnml-3825-01_Certificate

Information

URL to login to this WebVPN service: https://192.168.0.37/webvpn

3. User Authentication螢幕允許提供使用者身份驗證的機會。此組態使用路由器上本地建立的帳戶。您也可以使用驗證、授權及記帳(AAA)伺服器。要新增使用者，請按一下**Add**。在Add an Account（新增帳戶）螢幕上輸入使用者資訊，然後按一下**OK**。在User Authentication螢幕上按一下**Next**。



User Authentication

You can configure user accounts locally on this router. You can configure user accounts on a AAA server so that the router can contact this server to authenticate users when they try to log on. Specify how WebVPN should authenticate the users when they login.

Enter the username and password

Username: ausnml

Password

Password <None>

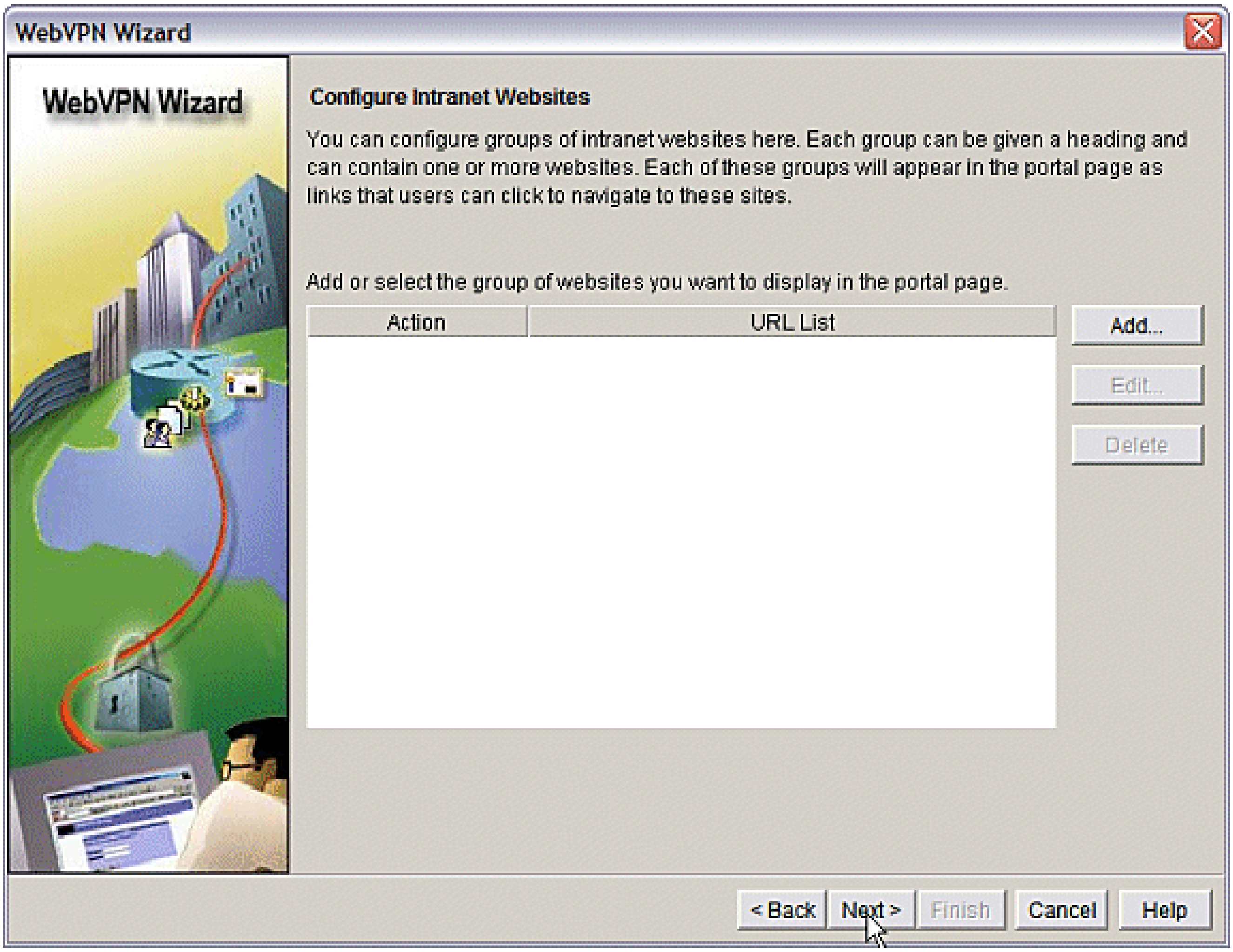
New Password: *****

Confirm New Password: *****

□ Encrypt password using MD5 hash algorithm

Privilege Level: 1

WebVPN Wizard螢幕允許配置Intranet網站，但此步驟被省略，因為此應用程式訪問使用埠轉發。如果要允許訪問網站，請使用無客戶端或完全客戶端SSL VPN配置，這些配置不在本文檔的範圍內。



WebVPN Wizard

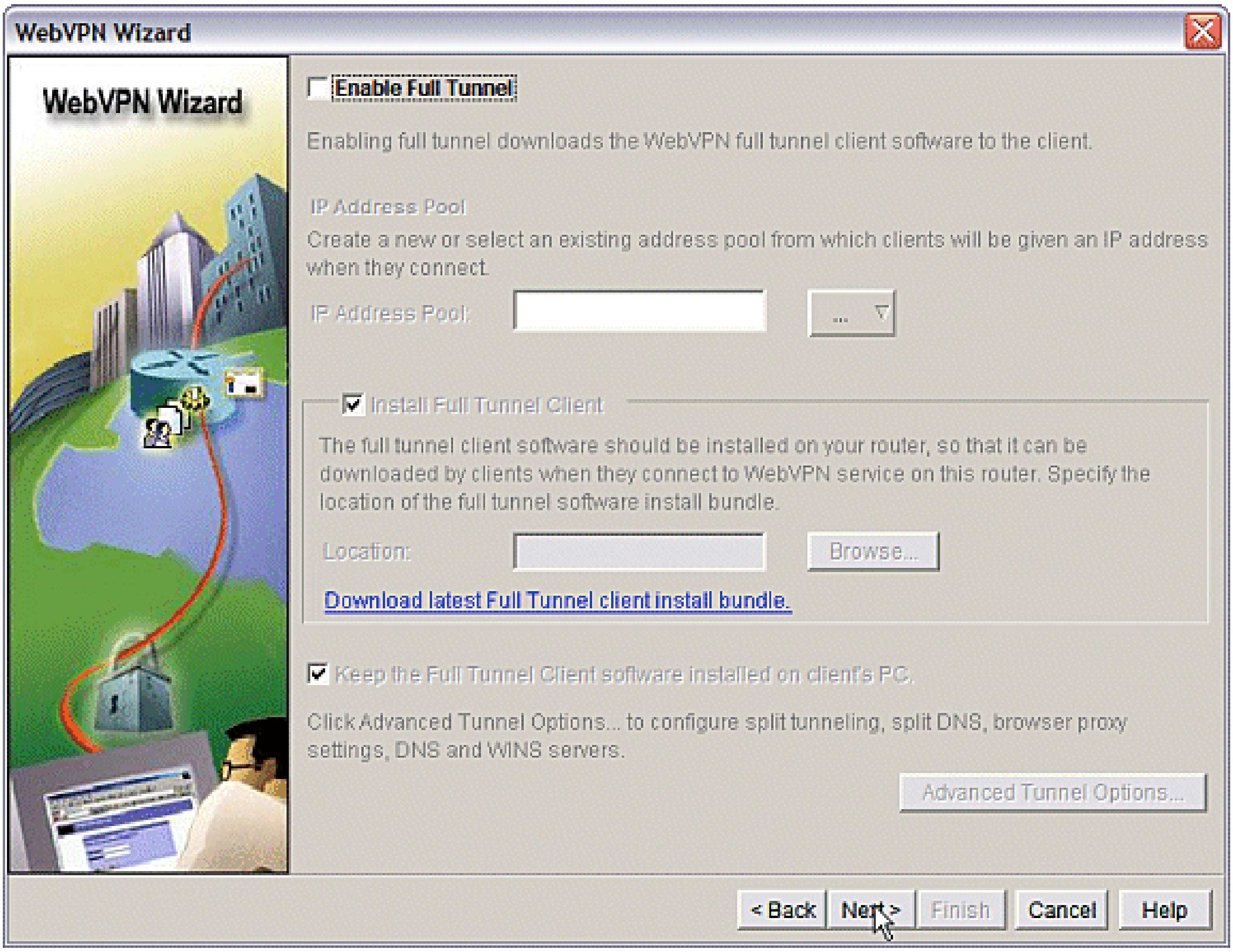
Configure Intranet Websites

You can configure groups of intranet websites here. Each group can be given a heading and can contain one or more websites. Each of these groups will appear in the portal page as links that users can click to navigate to these sites.

Add or select the group of websites you want to display in the portal page.

Action	URL List

按「**Next**」（下一步）。嚮導將顯示一個螢幕，允許配置全通道客戶端。這並不適用於瘦客戶端SSL VPN（埠轉發）。取消選中**Enable Full Tunnel**。按「**Next**」（下一步）。



WebVPN Wizard

☐ Enable Full Tunnel

Enabling full tunnel downloads the WebVPN full tunnel client software to the client.

IP Address Pool

Create a new or select an existing address pool from which clients will be given an IP address when they connect.

IP Address Pool:

☑ Install Full Tunnel Client

The full tunnel client software should be installed on your router, so that it can be downloaded by clients when they connect to WebVPN service on this router. Specify the location of the full tunnel software install bundle.

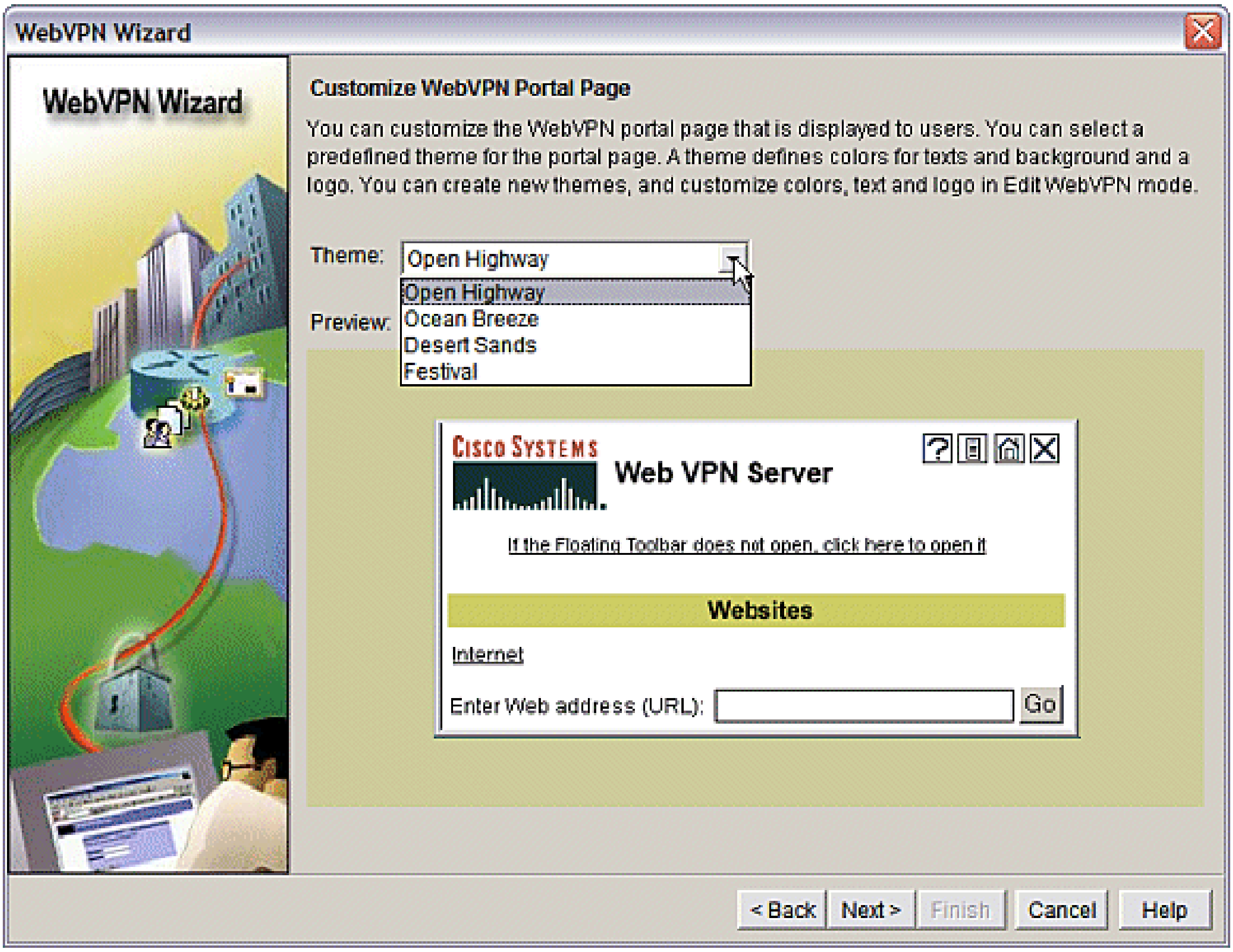
Location:

Download latest Full Tunnel client install bundle.

☑ Keep the Full Tunnel Client software installed on client's PC.

Click Advanced Tunnel Options... to configure split tunneling, split DNS, browser proxy settings, DNS and WINS servers.

4. 自定義WebVPN門戶頁面的外觀或接受預設外觀。按「**Next**」（下一步）。



WebVPN Wizard

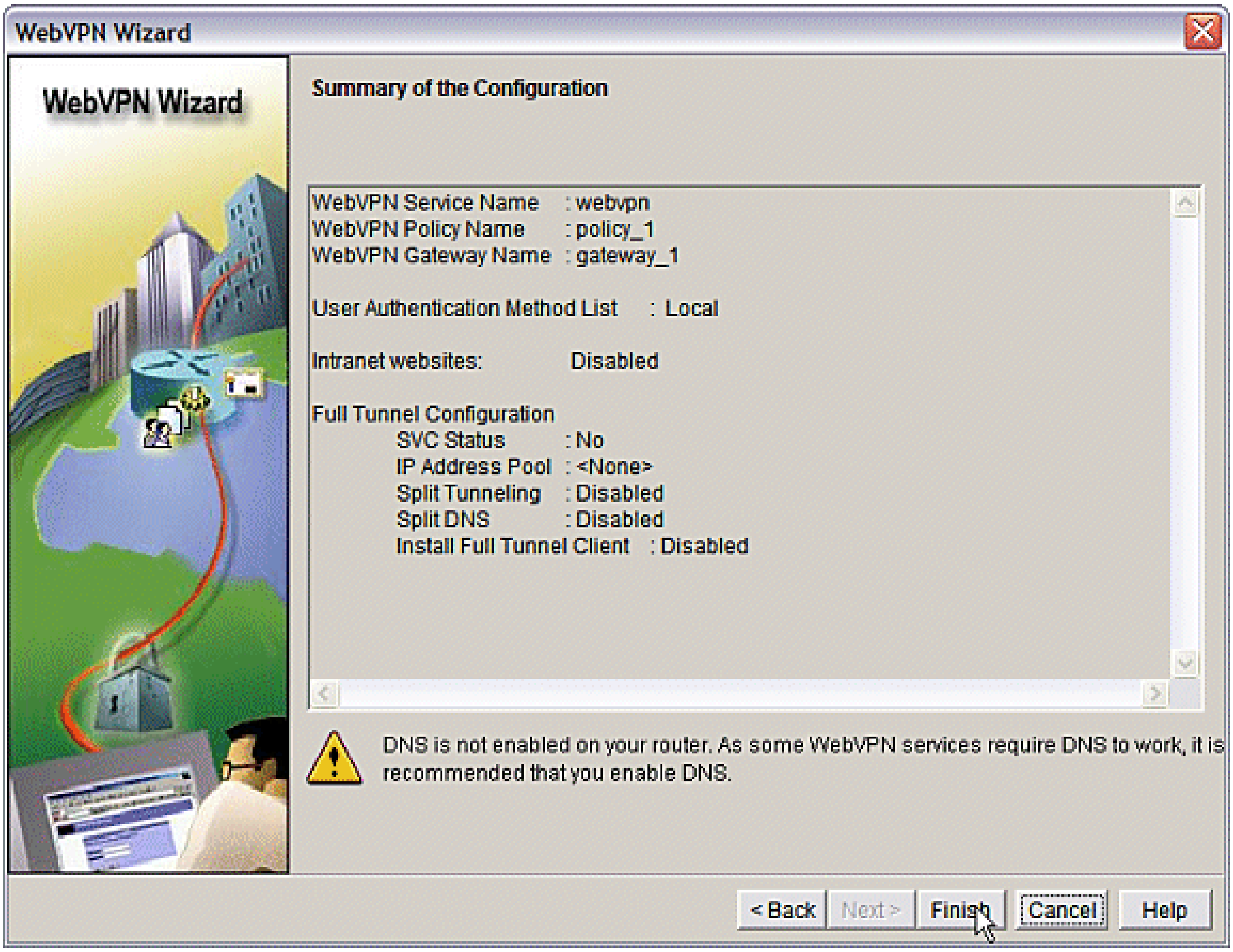
Customize WebVPN Portal Page

You can customize the WebVPN portal page that is displayed to users. You can select a predefined theme for the portal page. A theme defines colors for texts and background and a logo. You can create new themes, and customize colors, text and logo in Edit WebVPN mode.

Theme: Open Highway

Preview:

預覽配置摘要，然後按一下**完成>儲存**。

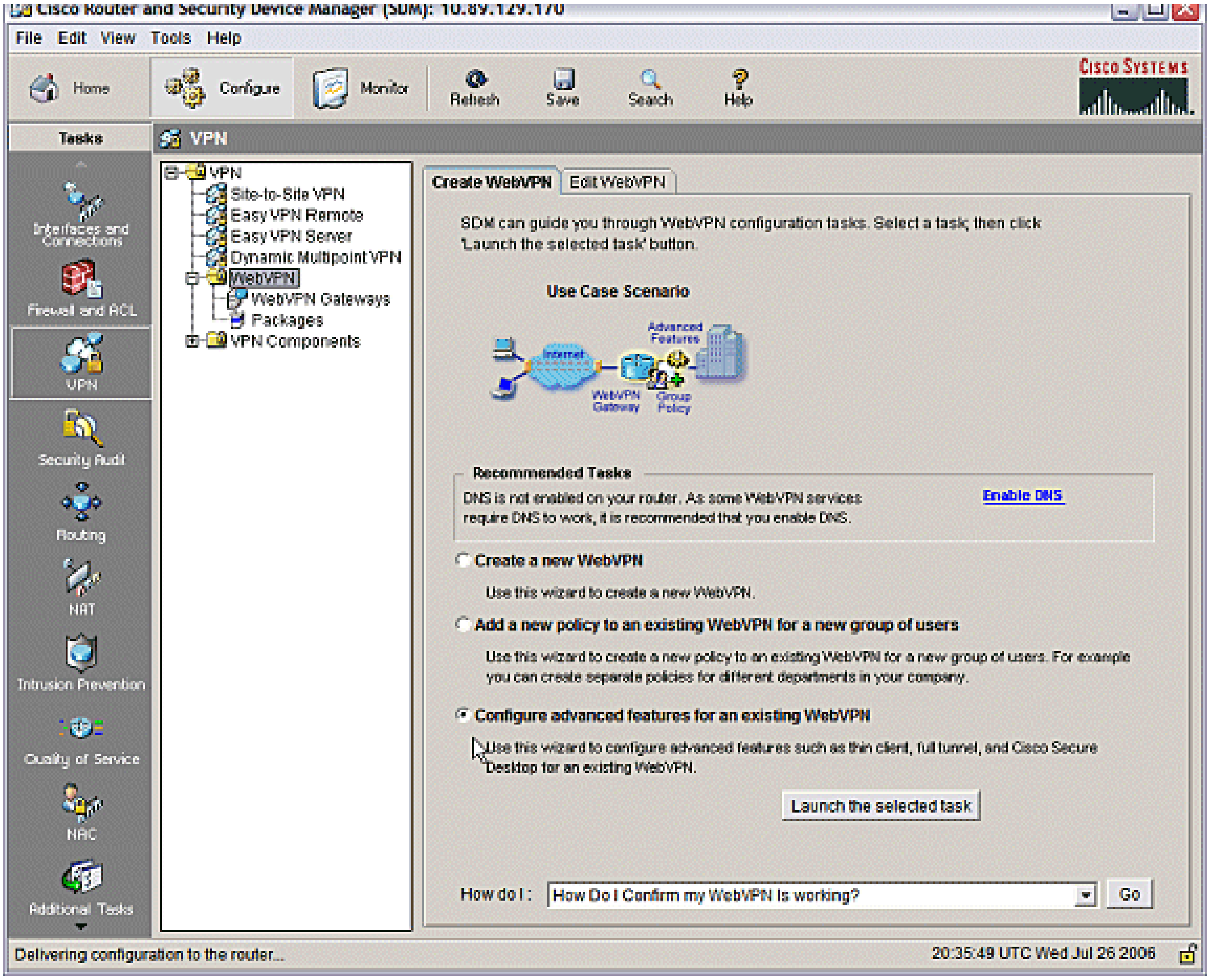


Summary of the Configuration

```
WebVPN Service Name    : webvpn
WebVPN Policy Name     : policy_1
WebVPN Gateway Name    : gateway_1

User Authentication Method List   : Local

Intranet websites:          Disabled

Full Tunnel Configuration
          SVC Status       : No
          IP Address Pool  : <None>
          Split Tunneling  : Disabled
          Split DNS        : Disabled
          Install Full Tunnel Client   : Disabled
```

DNS is not enabled on your router. As some WebVPN services require DNS to work, it is recommended that you enable DNS.

5. 您已建立具有連結組策略的WebVPN網關和WebVPN上下文。配置瘦客戶端埠，這些埠在客戶端連線到WebVPN時可用。選擇**Configure**。選擇**VPN > WebVPN**。選擇**Create WebVPN**。選擇單選按鈕**Configure advanced features for an existing WebVPN**，然後按一下**Launch the selected task**。



SDM can guide you through WebVPN configuration tasks. Select a task, then click 'Launch the selected task' button.

Recommended Tasks

DNS is not enabled on your router. As some WebVPN services require DNS to work, it is recommended that you enable DNS.

○ Create a new WebVPN

Use this wizard to create a new WebVPN.

○ Add a new policy to an existing WebVPN for a new group of users

Use this wizard to create a new policy to an existing WebVPN for a new group of users. For example you can create separate policies for different departments in your company.

● Configure advanced features for an existing WebVPN

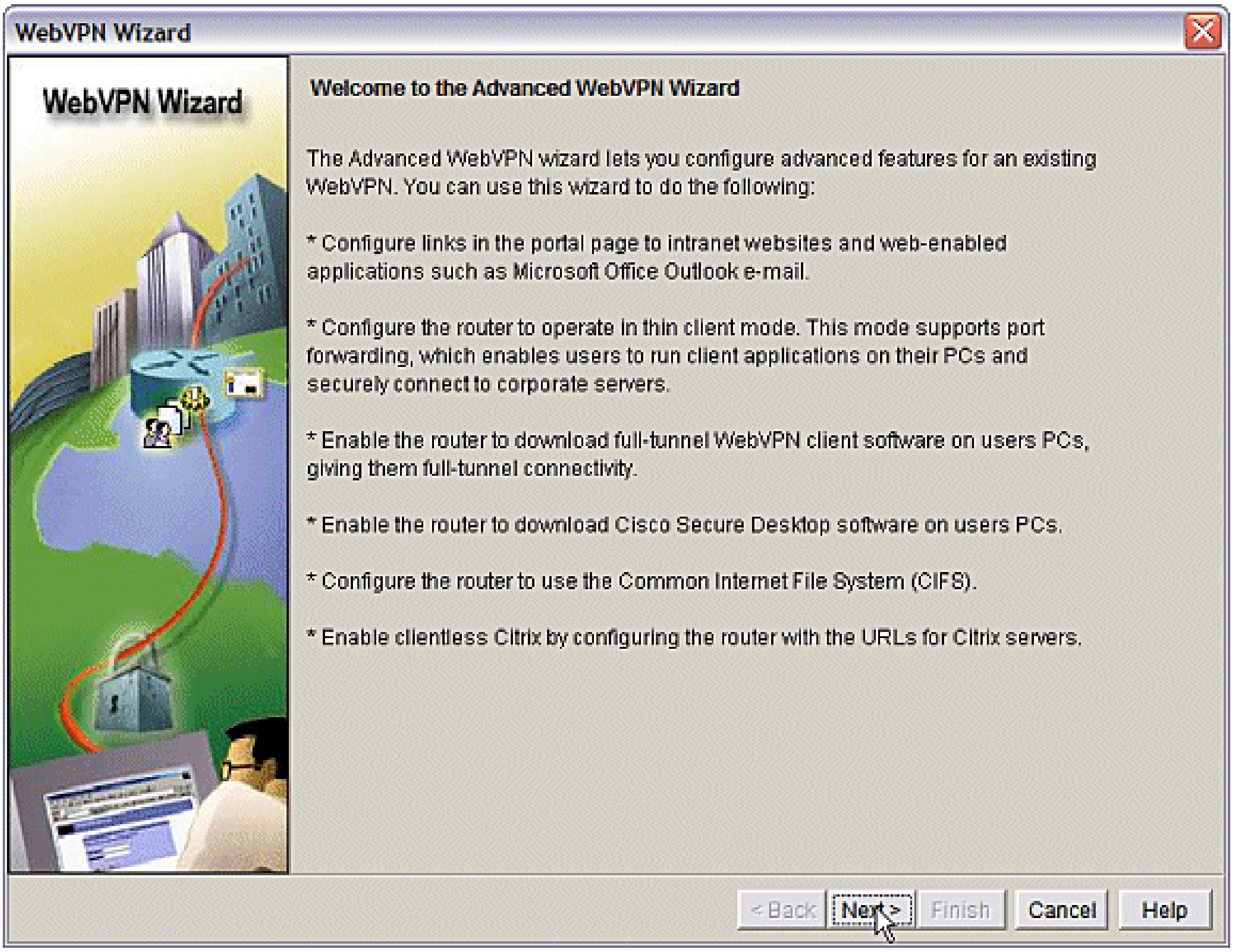
Use this wizard to configure advanced features such as thin client, full tunnel, and Cisco Secure Desktop for an existing WebVPN.

How do I: How Do I Confirm my WebVPN Is working?

Delivering configuration to the router...

20:35:49 UTC Wed Jul 26 2006

歡迎螢幕提供了嚮導功能的亮點。按「Next」（下一步）。



Welcome to the Advanced WebVPN Wizard

The Advanced WebVPN wizard lets you configure advanced features for an existing WebVPN. You can use this wizard to do the following:

* Configure links in the portal page to intranet websites and web-enabled applications such as Microsoft Office Outlook e-mail.

* Configure the router to operate in thin client mode. This mode supports port forwarding, which enables users to run client applications on their PCs and securely connect to corporate servers.

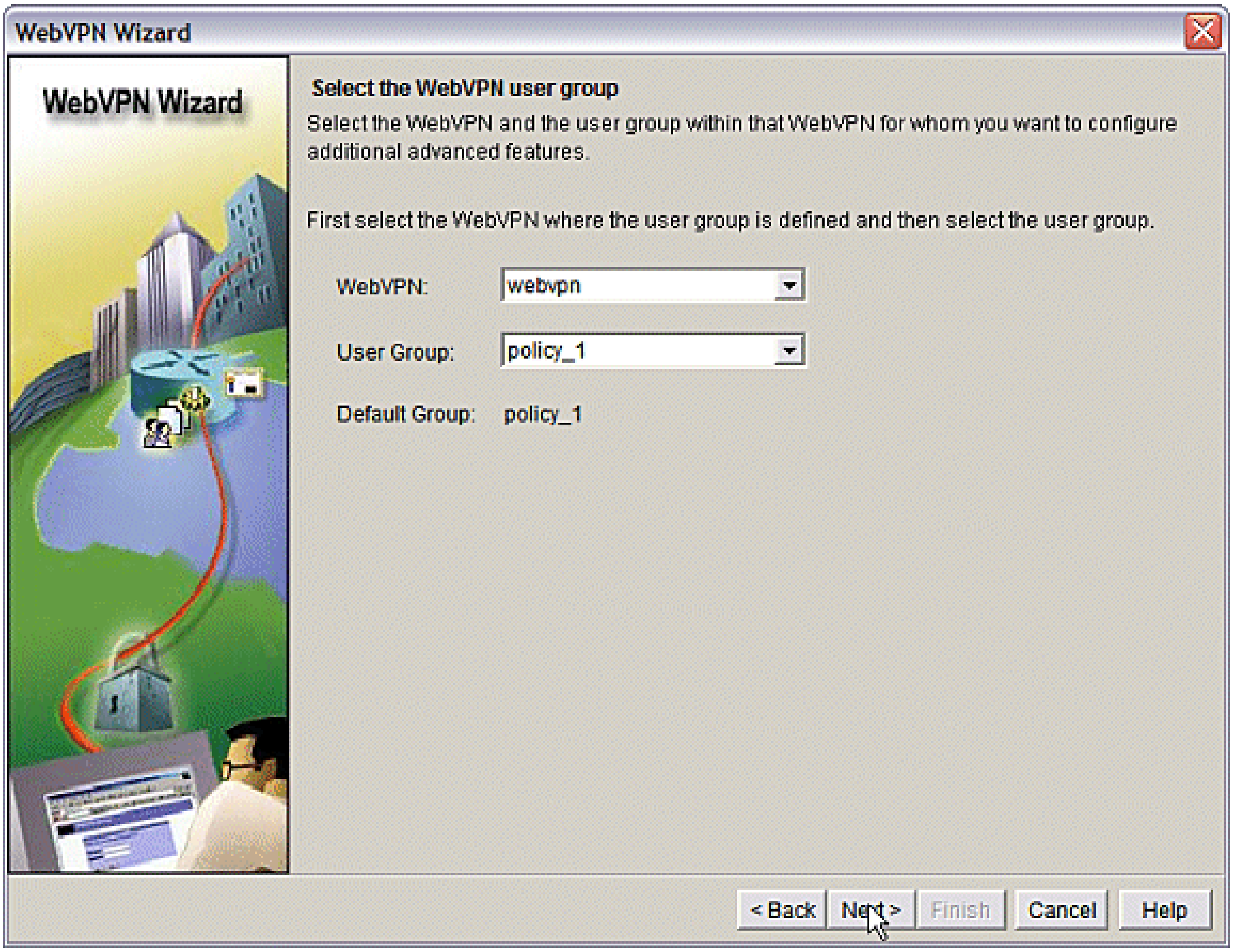
* Enable the router to download full-tunnel WebVPN client software on users PCs, giving them full-tunnel connectivity.

* Enable the router to download Cisco Secure Desktop software on users PCs.

* Configure the router to use the Common Internet File System (CIFS).

* Enable clientless Citrix by configuring the router with the URLs for Citrix servers.

從下拉選單中選擇WebVPN上下文和使用者組。按「**Next**」（下一步）。



Select the WebVPN user group

Select the WebVPN and the user group within that WebVPN for whom you want to configure additional advanced features.

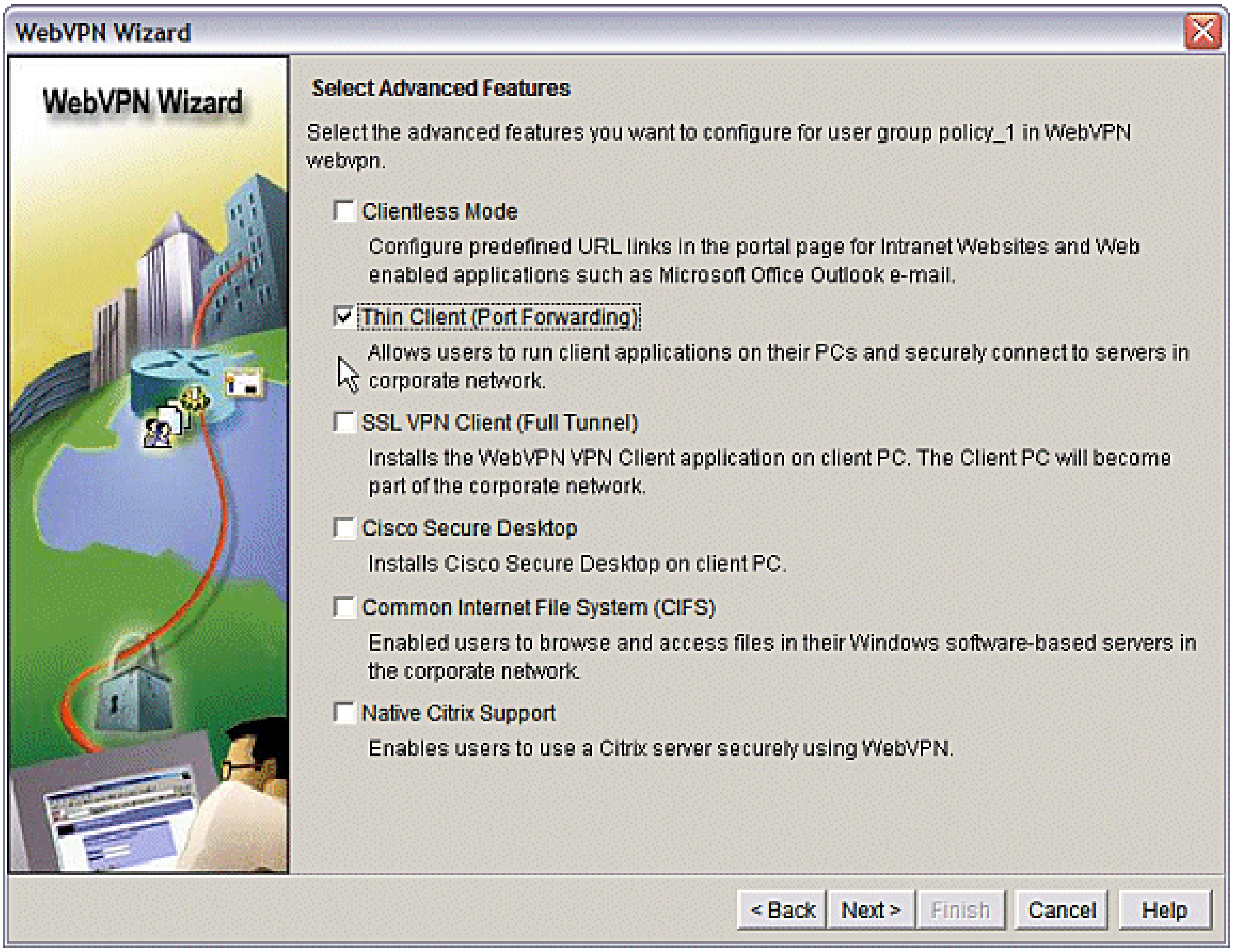
First select the WebVPN where the user group is defined and then select the user group.

WebVPN: webvpn

User Group: policy_1

Default Group: policy_1

選擇Thin Client(Port Forwarding)，然後按一下Next。



Select Advanced Features

Select the advanced features you want to configure for user group policy_1 in WebVPN webvpn.

□ Clientless Mode

Configure predefined URL links in the portal page for Intranet Websites and Web enabled applications such as Microsoft Office Outlook e-mail.

☑ Thin Client (Port Forwarding)

Allows users to run client applications on their PCs and securely connect to servers in corporate network.

□ SSL VPN Client (Full Tunnel)

Installs the WebVPN VPN Client application on client PC. The Client PC will become part of the corporate network.

□ Cisco Secure Desktop

Installs Cisco Secure Desktop on client PC.

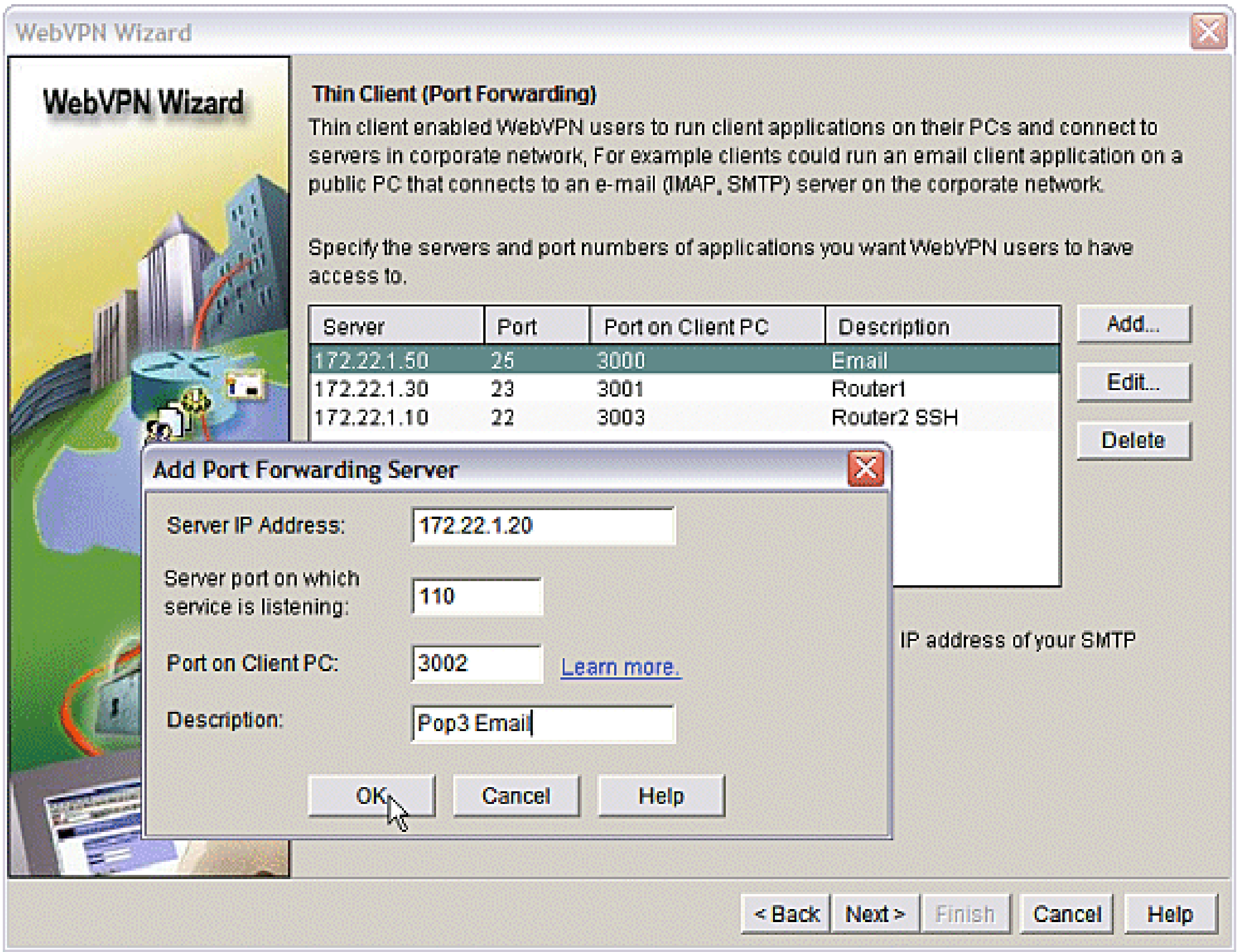
□ Common Internet File System (CIFS)

Enabled users to browse and access files in their Windows software-based servers in the corporate network.

□ Native Citrix Support

Enables users to use a Citrix server securely using WebVPN.

輸入要通過埠轉發提供的資源。服務埠必須是靜態埠，但您可以接受由嚮導分配的客戶端PC上的預設埠。按「**Next**」（下一步）。



Thin Client (Port Forwarding)

Thin client enabled WebVPN users to run client applications on their PCs and connect to servers in corporate network, For example clients could run an email client application on a public PC that connects to an e-mail (IMAP, SMTP) server on the corporate network.

Specify the servers and port numbers of applications you want WebVPN users to have access to.

Server	Port	Port on Client PC	Description
172.22.1.50	25	3000	Email
172.22.1.30	23	3001	Router1
172.22.1.10	22	3003	Router2 SSH

IP address of your SMTP

Add Port Forwarding Server

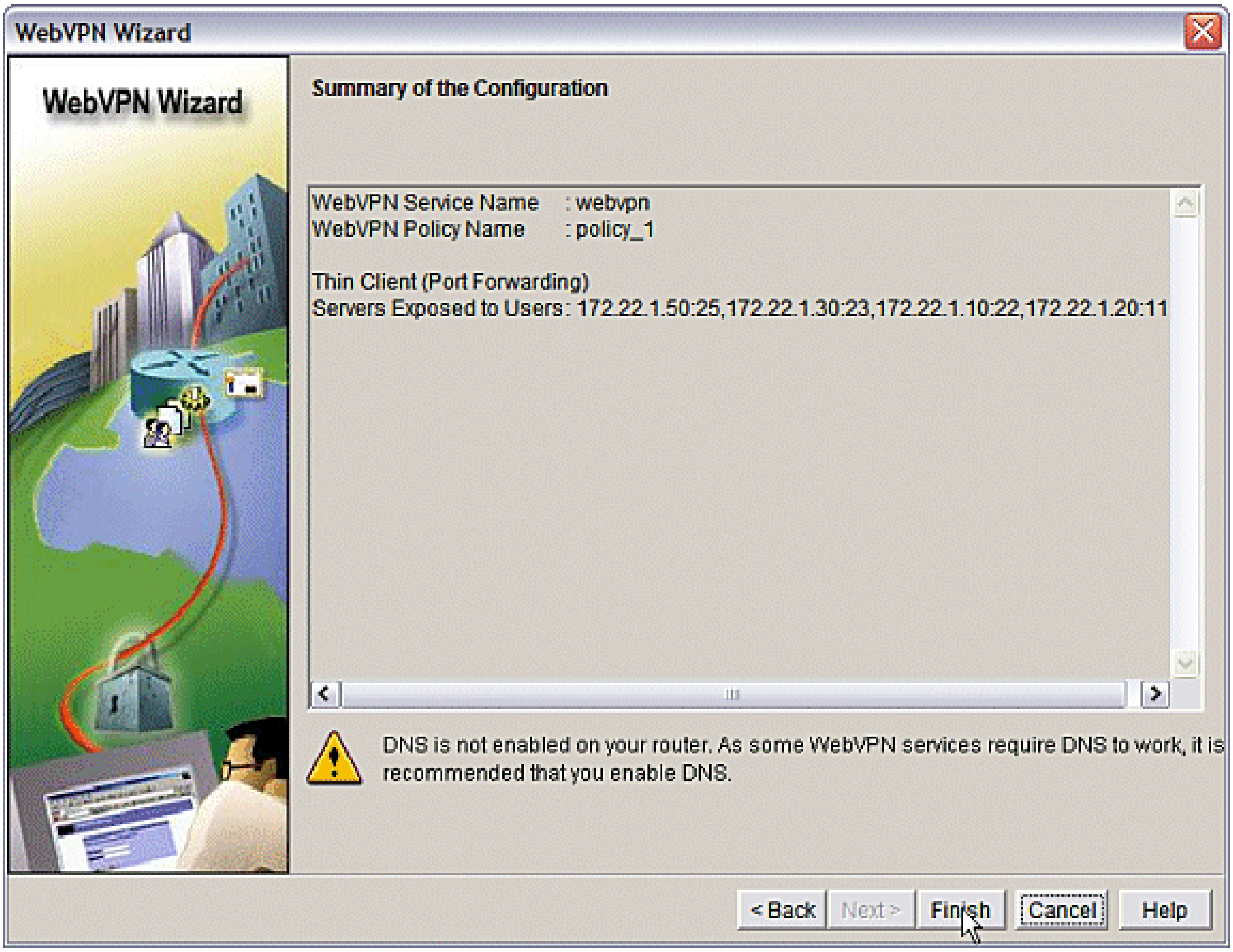
Server IP Address: 172.22.1.20

Server port on which service is listening: 110

Port on Client PC: 3002 Learn more.

Description: Pop3 Email

預覽配置摘要，然後按一下**完成>確定>儲存**。



WebVPN Service Name : webvpn
WebVPN Policy Name : policy_1

Thin Client (Port Forwarding)
Servers Exposed to Users: 172.22.1.50:25,172.22.1.30:23,172.22.1.10:22,172.22.1.20:11

DNS is not enabled on your router. As some WebVPN services require DNS to work, it is recommended that you enable DNS.

組態

SDM配置的結果。

ausnml-3825-01

```
Building configuration...

Current configuration : 4343 bytes
!
! Last configuration change at 15:55:38 UTC Thu Jul 27
2006 by ausnml
! NVRAM config last updated at 21:30:03 UTC Wed Jul 26
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
enable secret 5 $1$KbIu$5o8qKYAVpWvyv9rYbrJLi/
```

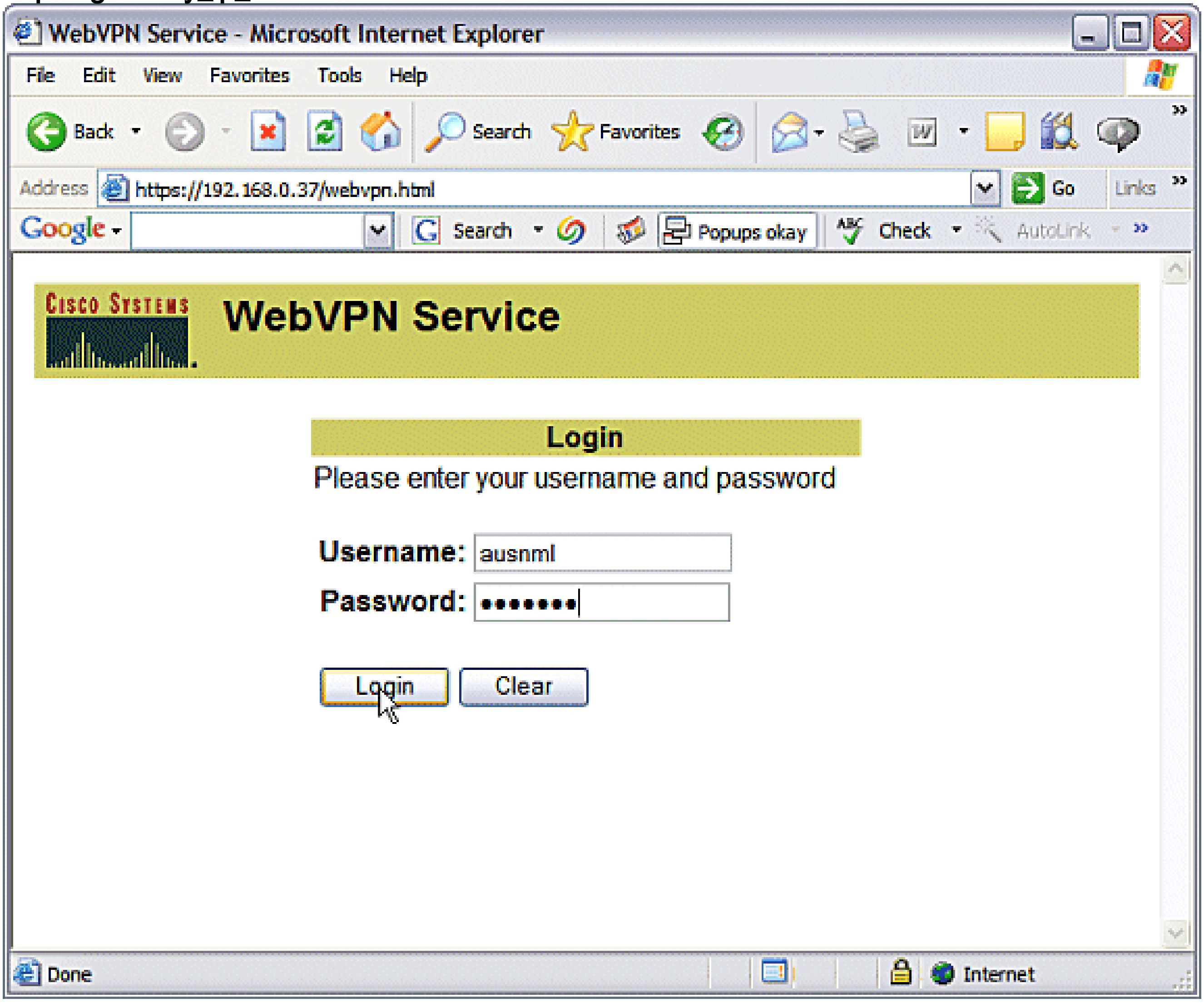
```
!
aaa new-model
!
aaa authentication login default local
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authentication login sdm_vpn_xauth_ml_2 local
aaa authorization exec default local
!
aaa session-id common
!
resource policy
!
ip cef
!
ip domain name cisco.com
!
voice-card 0
 no dspfarm
!--- Self-Signed Certificate Information crypto pki
trustpoint ausnml-3825-01_Certificate enrollment
selfsigned serial-number none ip-address none
revocation-check crl rsakeypair ausnml-3825-
01_Certificate_RSAKey 1024 ! crypto pki certificate
chain ausnml-3825-01_Certificate certificate self-signed
02 30820240 308201A9 A0030201 02020102 300D0609 2A864886
F70D0101 04050030 !--------------------- !--- cut for
brevity quit ! username ausnml privilege 15 password 7
15071F5A5D292421 username fallback privilege 15 password
7 08345818501A0A12 username austin privilege 15 secret 5
$1$3xFv$W0YUsKDx1adDc.cVQF2Ei0 username sales_user1
privilege 5 secret 5 $1$2/SX$ep4fsCpodeyKaRji2mJkX/
username admin0321 privilege 15 secret 5
$1$FxzG$cQUJeUpBWgZ.scSzOt8Ro1 ! interface
GigabitEthernet0/0 ip address 192.168.0.37 255.255.255.0
duplex auto speed auto media-type rj45 ! interface
GigabitEthernet0/1 ip address 172.22.1.151 255.255.255.0
duplex auto speed auto media-type rj45 ! 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 exec-timeout 40 0 privilege
level 15 password 7 071A351A170A1600 transport input
telnet ssh line vty 5 15 exec-timeout 40 0 password 7
001107505D580403 transport input telnet ssh ! scheduler
allocate 20000 1000 !--- the WebVPN Gateway webvpn
gateway gateway_1 ip address 192.168.0.37 port 443 http-
redirect port 80 ssl trustpoint ausnml-3825-
01_Certificate inservice !--- the WebVPN Context webvpn
context webvpn title-color #CCCC66 secondary-color white
text-color black ssl authenticate verify all !---
resources available to the thin-client port-forward
"portforward_list_1" local-port 3002 remote-server
"172.22.1.20" remote-port 110 description "Pop3 Email"
local-port 3001 remote-server "172.22.1.30" remote-port
23 description "Router1" local-port 3000 remote-server
"172.22.1.50" remote-port 25 description "Email" local-
port 3003 remote-server "172.22.1.10" remote-port 22
description "Router2 SSH" !--- the group policy policy
group policy_1 port-forward "portforward_list_1"
default-group-policy policy_1 aaa authentication list
sdm_vpn_xauth_ml_2 gateway gateway_1 domain webvpn max-
users 2 inservice ! end
```

驗證

驗證您的設定

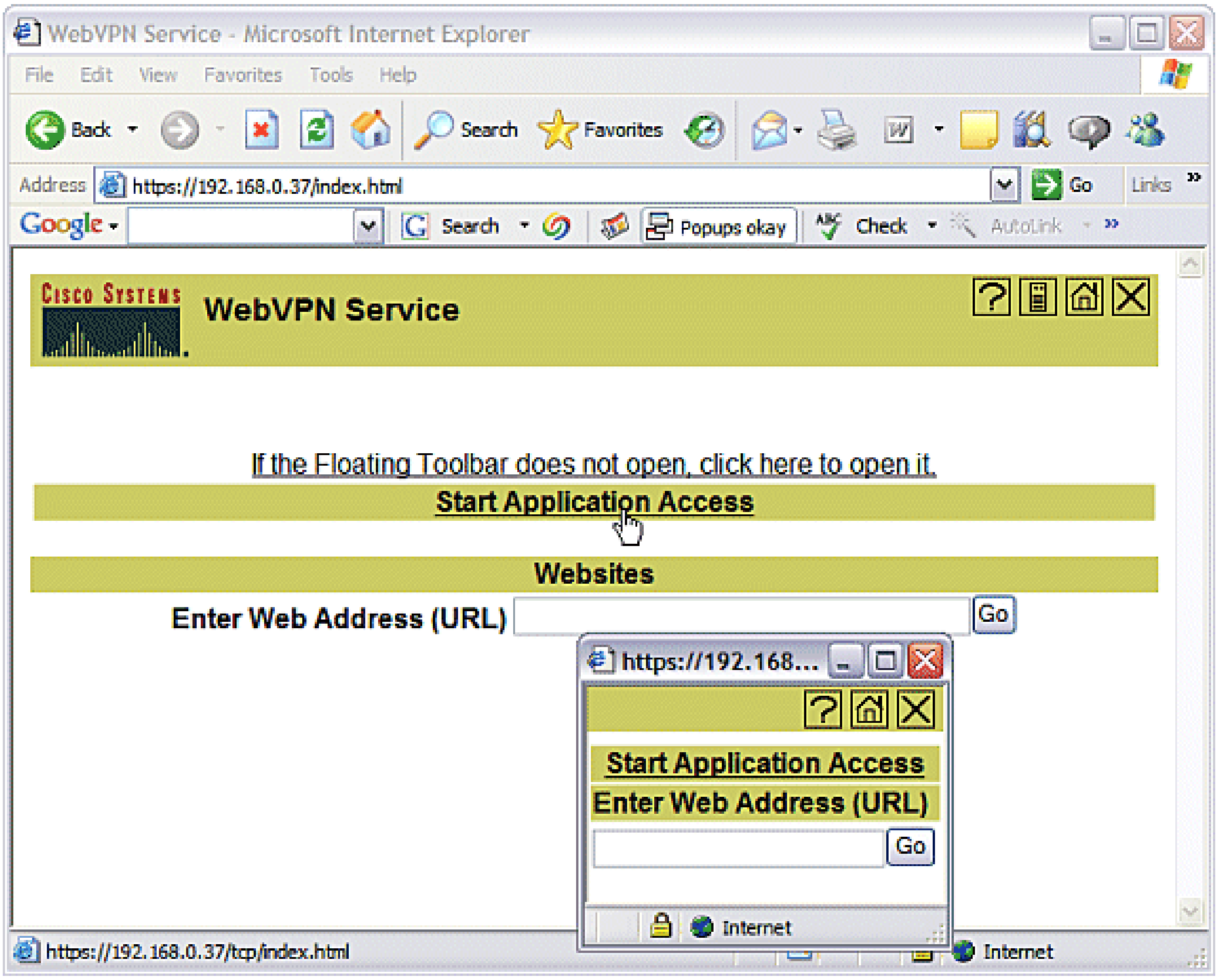
使用本節內容，確認您的組態是否正常運作。

1. 使用客戶端電腦訪問WebVPN網關，網址為**https://gateway_ip_address。**如果建立唯一的WebVPN情景，請記住包含WebVPN域名。例如，如果已建立名為sales的域，請輸入**https://gateway_ip_address/sales**。

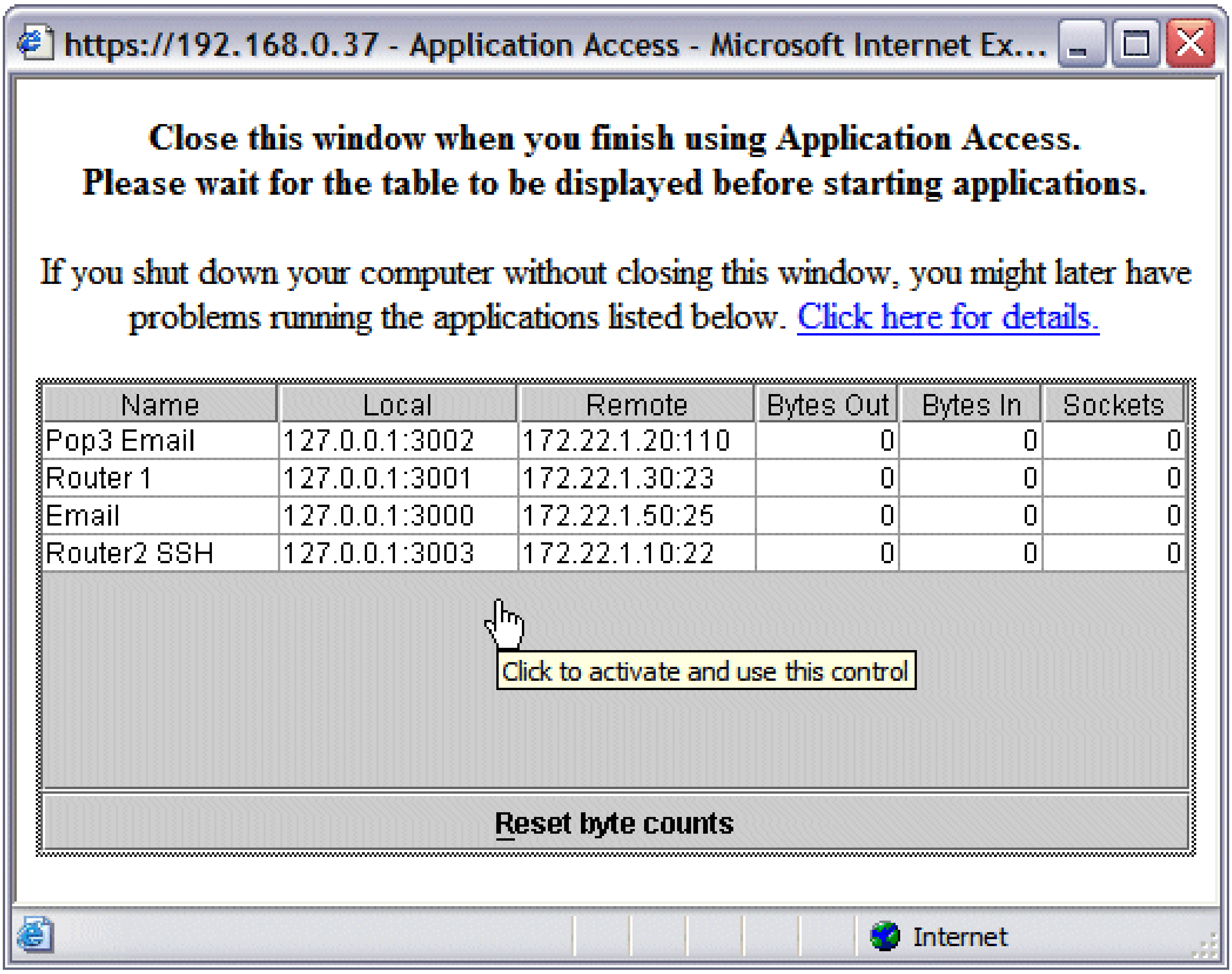

WebVPN Service - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://192.168.0.37/webvpn.html Go Links
Google Search Popups okay Check AutoLink
Cisco Systems
WebVPN Service
Login
Please enter your username and password
Login Clear
Done Internet

Username: ausnml
Password: •••••••

2. 登入並接受WebVPN網關提供的證書。按一下**Start Application Access**。



3. 系統隨即會顯示「應用程式訪問」螢幕。您可以使用本地埠號和本地環回IP地址訪問應用程式。例如，要通過Telnet連線到Router 1，請輸入**telnet 127.0.0.1 3001**。小型Java小程式將此資訊傳送到WebVPN網關，然後WebVPN網關以安全的方式將會話兩端連線在一起。成功的連線會導致**Bytes Out**和**Bytes In**列增加。



https://192.168.0.37 - Application Access - Microsoft Internet Ex...

Close this window when you finish using Application Access.
Please wait for the table to be displayed before starting applications.

If you shut down your computer without closing this window, you might later have problems running the applications listed below. Click here for details.

Name	Local	Remote	Bytes Out	Bytes In	Sockets
Pop3 Email	127.0.0.1:3002	172.22.1.20:110	0	0	0
Router 1	127.0.0.1:3001	172.22.1.30:23	0	0	0
Email	127.0.0.1:3000	172.22.1.50:25	0	0	0
Router2 SSH	127.0.0.1:3003	172.22.1.10:22	0	0	0

指令

有幾個**show**命令與WebVPN關聯。您可以在命令列介面(CLI)上執行這些命令，以顯示統計資訊和其他資訊。要詳細瞭解**show**命令的用法，請參閱驗證WebVPN配置。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

疑難排解

使用本節內容，對組態進行疑難排解。

客戶端電腦必須裝載SUN Java 1.4或更高版本。從Java軟體下載獲取此軟體的副本

用於排除故障的命令

註：使用debug命令前，請先參閱有關Debug命令的重要信息資訊。

- **show webvpn —** — 有許多與**WebVPN**關聯的show命令。可以在CLI中執行這些操作以顯示統計資訊和其他資訊。要詳細瞭解**show**命令的用法，請參閱驗證WebVPN配置。
- **debug webvpn —** — 使用**debug**指令可能對路由器造成負面影響。要詳細瞭解**debug**命令的用法，請參閱使用WebVPN Debug命令。

相關資訊

- Cisco IOS SSLVPN
- SSL VPN - WebVPN
- Cisco IOS WebVPN問答
- 技術支援與文件 - Cisco Systems