

# 帶ASDM的ASA上的瘦客戶端SSL VPN(WebVPN)配置示例

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[網路圖表](#)

[慣例](#)

[背景資訊](#)

[使用ASDM的瘦客戶端SSL VPN配置](#)

[步驟1.在ASA上啟用WebVPN](#)

[步驟2.配置埠轉發特徵](#)

[步驟3.建立組策略並將其連結到埠轉發清單](#)

[步驟4.建立隧道組並將其連結到組策略](#)

[步驟5.建立使用者並將該使用者新增到組策略中](#)

[使用CLI的瘦客戶端SSL VPN配置](#)

[驗證](#)

[程式](#)

[指令](#)

[疑難排解](#)

[SSL握手過程是否完成？](#)

[SSL VPN瘦客戶端是否正常工作？](#)

[指令](#)

[相關資訊](#)

## 簡介

瘦客戶端SSL VPN技術允許具有靜態埠的某些應用程式進行安全訪問，例如Telnet(23)、SSH(22)、POP3(110)、IMAP4(143)和SMTP(25)。您可以將瘦客戶端SSL VPN用作使用者驅動的應用程式、策略驅動的應用程式或同時用作兩者。也就是說，您可以逐個使用者配置訪問許可權，也可以建立新增一個或多個使用者的組策略。

- **無客戶端SSL VPN(WebVPN)** — 提供需要啟用SSL的Web瀏覽器來訪問公司區域網(LAN)上的HTTP或HTTPS Web伺服器的遠端客戶端。此外，無客戶端SSL VPN通過通用網際網路檔案系統(CIFS)協定為Windows檔案瀏覽提供訪問許可權。Outlook Web Access(OWA)是HTTP訪問的一個示例。請參閱[ASA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。
- **瘦客戶端SSL VPN (埠轉發)** — 提供遠端客戶端，可下載基於Java的小程式，並允許使用靜

態埠號的傳輸控制協定(TCP)應用程式的安全訪問。郵局通訊協定(POP3)、簡易郵件傳送通訊協定(SMTP)、網際網路訊息存取通訊協定(IMAP)、安全殼層(ssh)和Telnet都是安全存取的範例。由於本地電腦上的檔案發生更改，因此使用者必須具有本地管理許可權才能使用此方法。SSL VPN的這種方法不適用於使用動態埠分配的應用程式，例如某些檔案傳輸協定(FTP)應用程式。**注意：**不支援使用者資料包協定(UDP)。

- **SSL VPN客戶端 ( 隧道模式 )** — 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訪問。您可以將SSL VPN客戶端(SVC)永久下載到遠端工作站，也可以在安全會話關閉後刪除客戶端。請參閱[ASA上的SSL VPN客戶端\(SVC\)和ASDM配置示例](#)以瞭解有關SSL VPN客戶端的詳細資訊。

本文檔演示了自適應安全裝置(ASA)上瘦客戶端SSL VPN的簡單配置。此配置允許使用者安全telnet至ASA內部的路由器。ASA 7.x及更高版本支援本文檔中的配置。

## [必要條件](#)

### [需求](#)

在嘗試此配置之前，請確保滿足遠端客戶端工作站的以下要求：

- 支援SSL的Web瀏覽器
- SUN Java JRE 1.4或更高版本
- Cookie已啟用
- 已禁用彈出視窗阻止程式
- 本地管理許可權 ( 不需要但強烈建議 )

**註：** Sun Java JRE的最新版本可從Java網站免費下載。

### [採用元件](#)

本文中的資訊係根據以下軟體和硬體版本：

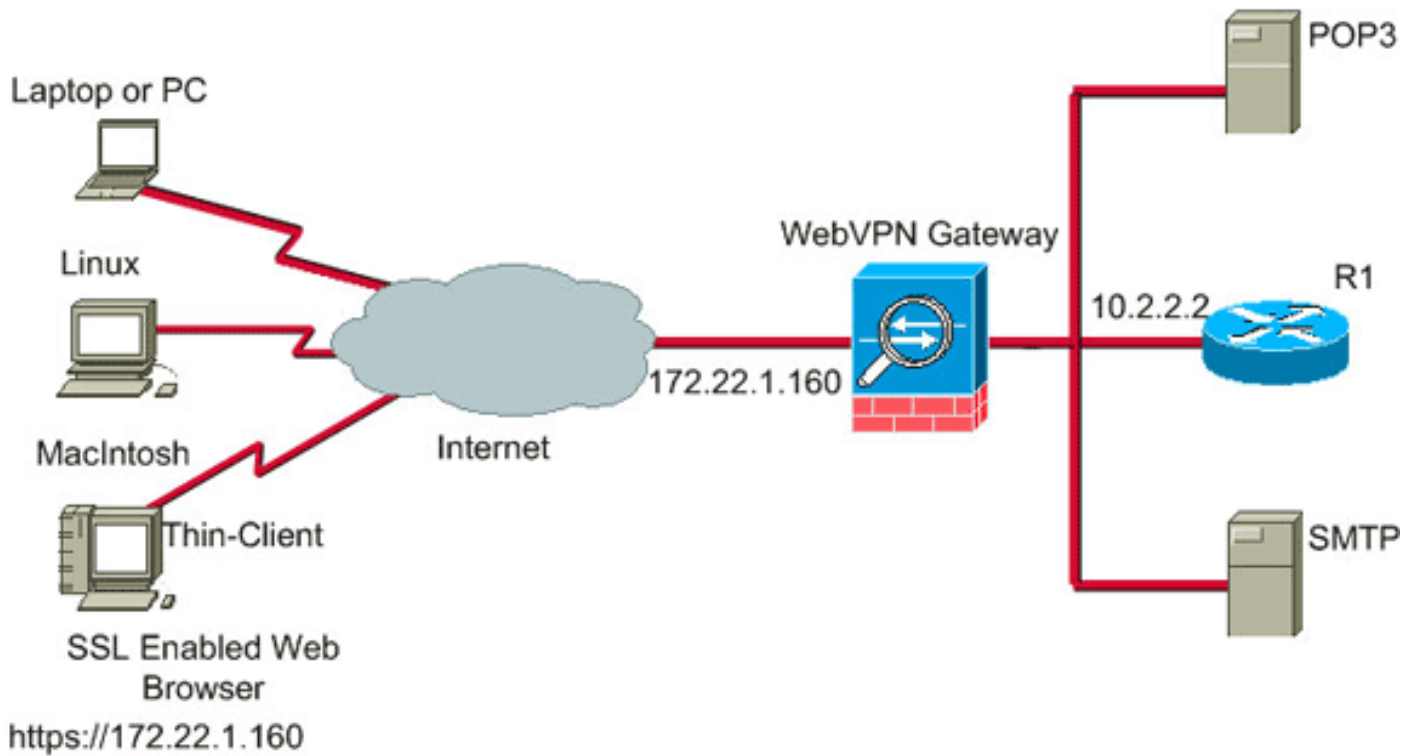
- 思科調適型安全裝置5510系列
- 思科調適型安全裝置管理員(ASDM)5.2(1)**註：**請參閱[允許ASDM進行HTTPS訪問](#)，以便允許ASDM配置ASA。
- 思科調適型安全裝置軟體版本7.2(1)
- Microsoft Windows XP Professional(SP 2)遠端客戶端

本文檔中的資訊是在實驗室環境中開發的。文中使用到的所有裝置已重設為預設組態。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。此配置中使用的所有IP地址都是從實驗室環境中的RFC 1918地址中選擇的；這些IP地址在Internet上不可路由，僅供測試使用。

### [網路圖表](#)

本檔案使用本節所述的網路組態。

當遠端客戶端啟動與ASA的會話時，客戶端將小型Java小程式下載到工作站。系統向客戶端顯示預配置資源的清單。



## 慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例](#)。

## 背景資訊

為了啟動會話，遠端客戶端會開啟一個指向ASA外部介面的SSL瀏覽器。建立會話後，使用者可以使用ASA上配置的引數來呼叫任何Telnet或應用程式訪問。ASA代理安全連線並允許使用者訪問裝置。

**附註：** 這些連線不需要入站訪問清單，因為ASA已經知道什麼是合法會話。

## 使用ASDM的瘦客戶端SSL VPN配置

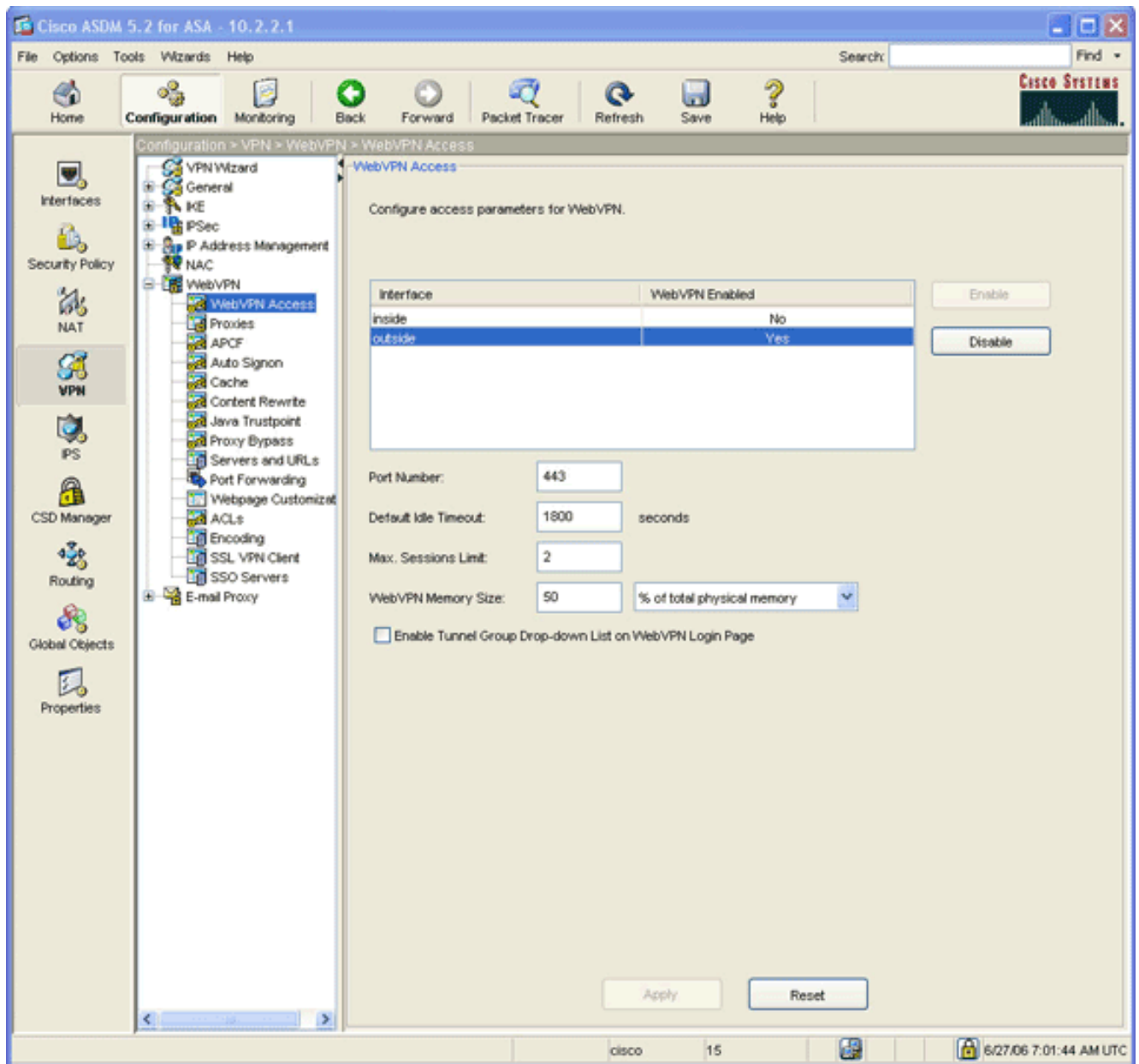
要在ASA上配置瘦客戶端SSL VPN，請完成以下步驟：

1. [在ASA上啟用WebVPN](#)
2. [配置埠轉發特性](#)
3. [建立組策略並將其連結到埠轉發清單](#) (在步驟2中建立)
4. [建立隧道組並將其連結到組策略](#) (在步驟3中建立)
5. [建立使用者並將該使用者新增到組策略](#) (在步驟3中建立)

### 步驟1.在ASA上啟用WebVPN

要在ASA上啟用WebVPN，請完成以下步驟：

1. 在ASDM應用程式中，按一下**Configuration**，然後按一下**VPN**。
2. 展開**WebVPN**，然後選擇**WebVPN Access**。

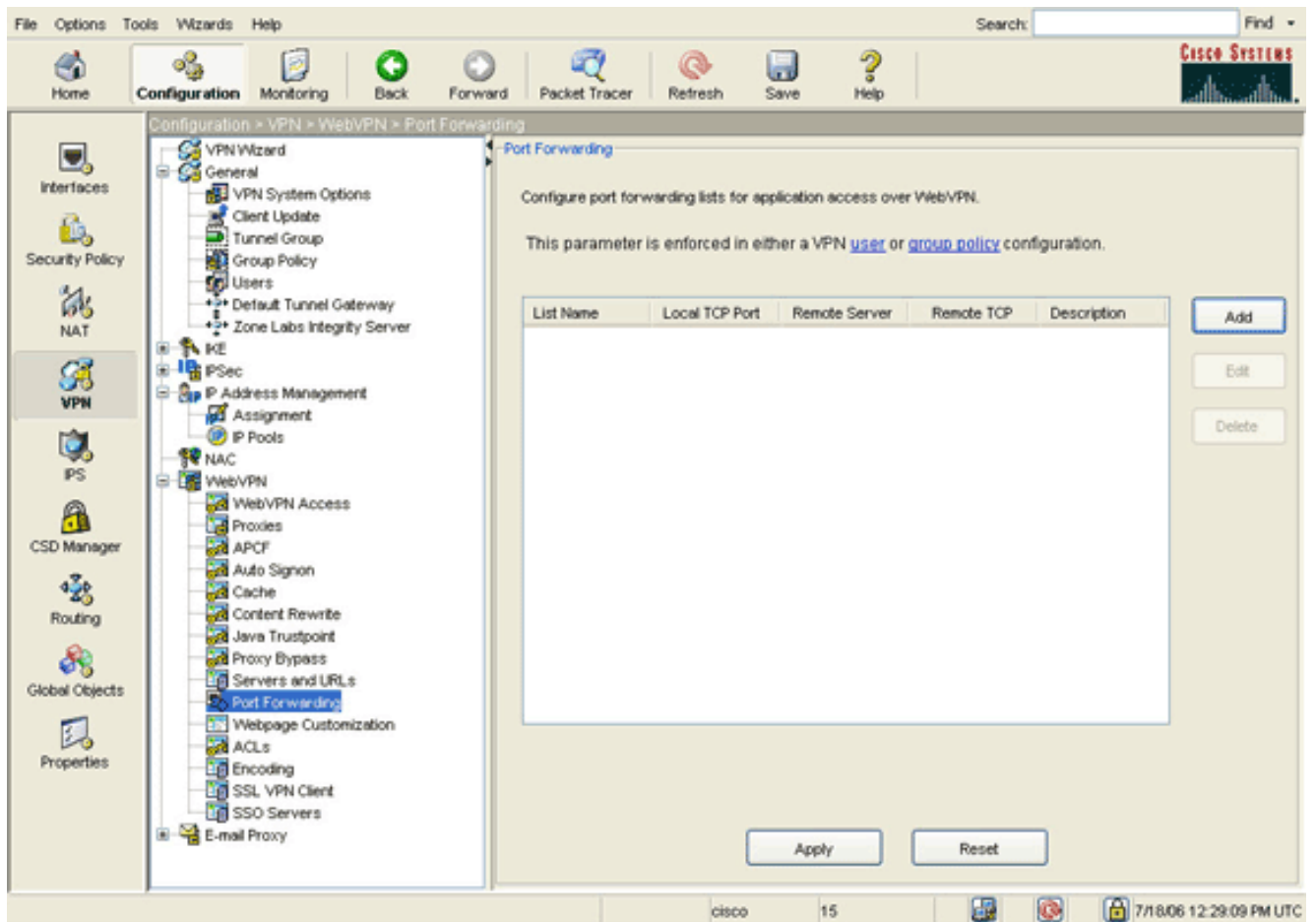


3. 突出顯示介面，然後按一下**Enable**。
4. 按一下**Apply**，按一下**Save**，然後按一下**Yes**接受更改。

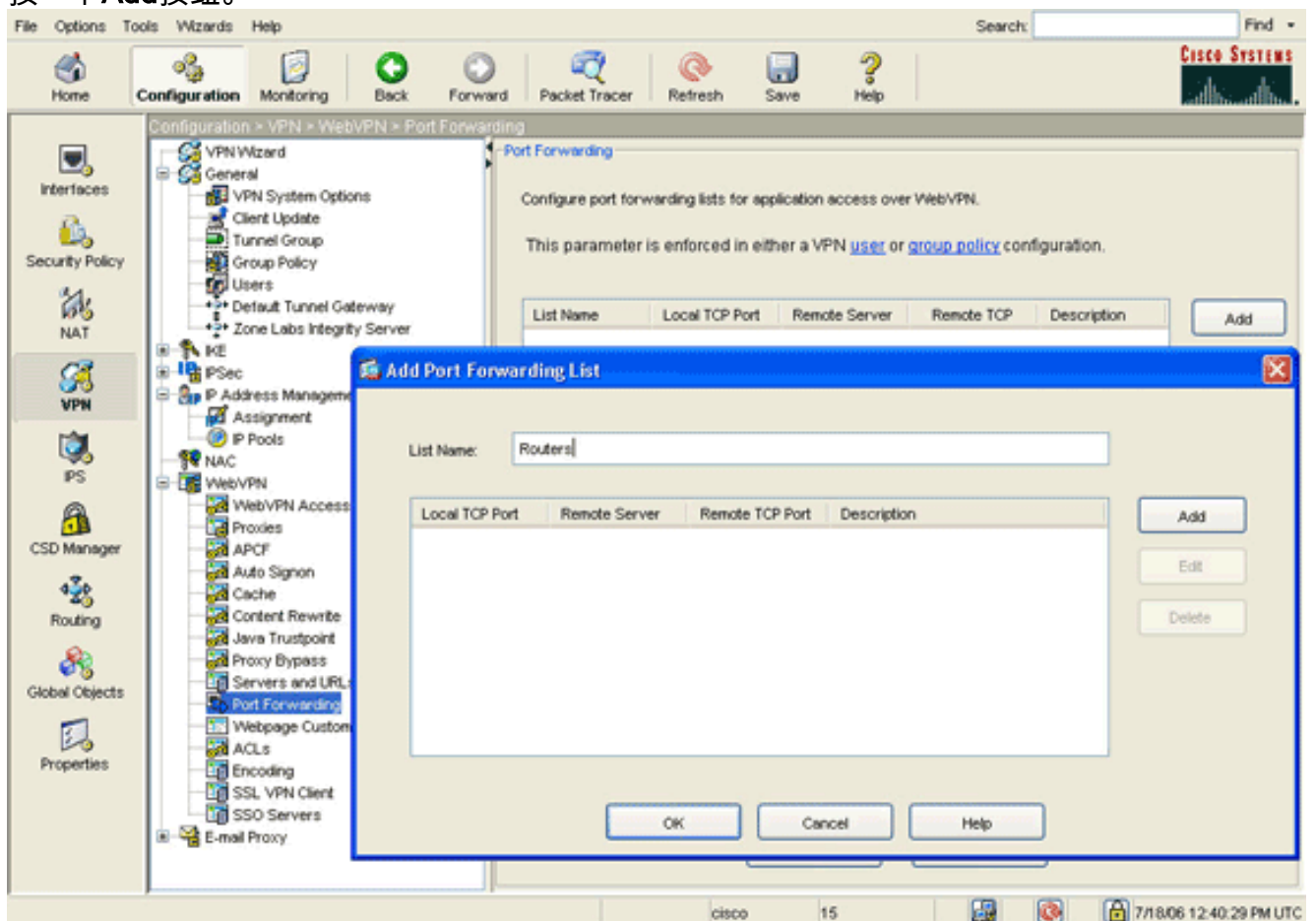
## 步驟2.配置埠轉發特徵

若要設定連線埠轉送特徵，請完成以下步驟：

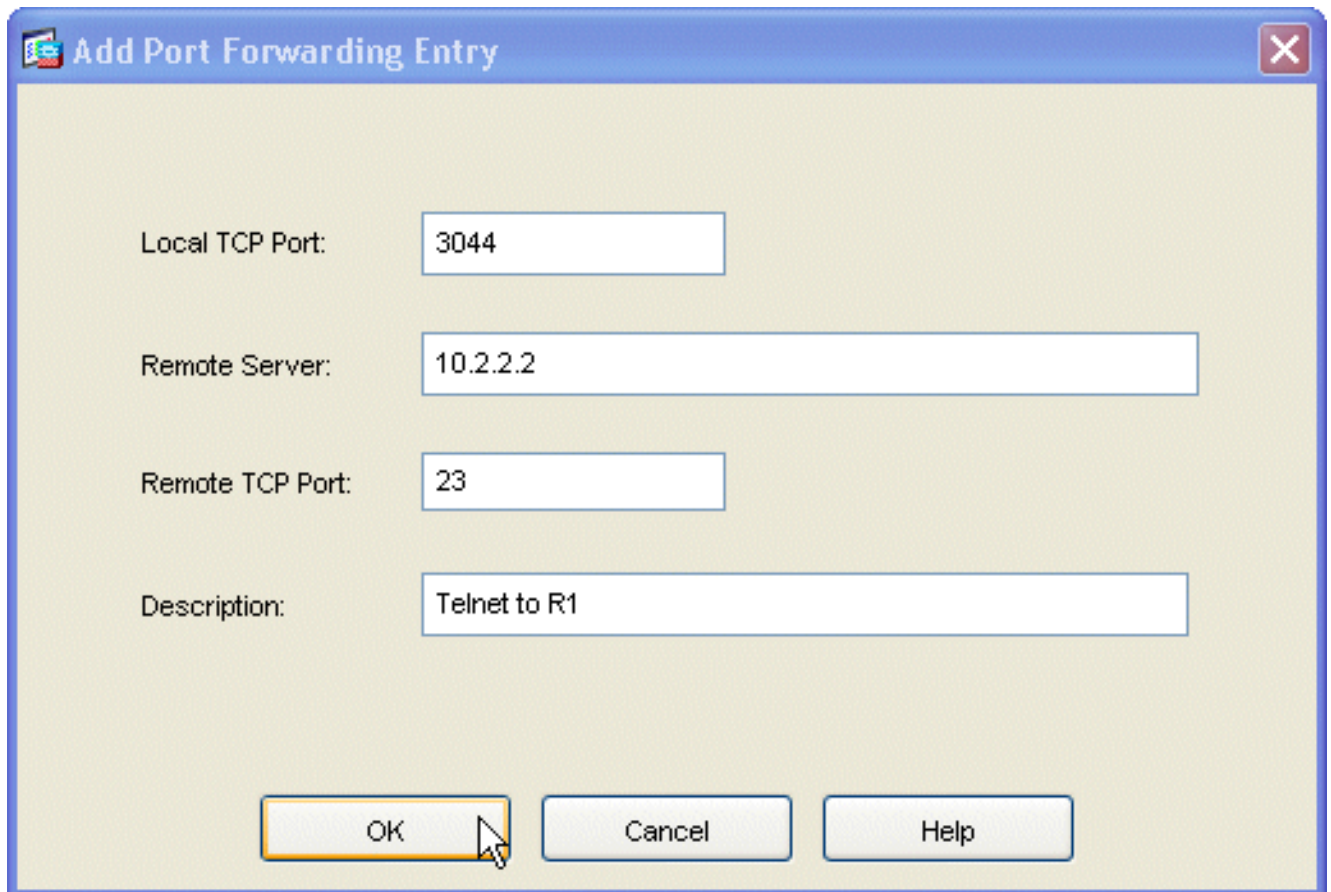
1. 展開**WebVPN**，然後選擇**Port Forwarding**。



2. 按一下Add按鈕。



3. 在Add Port Forwarding List對話方塊中，輸入清單名稱，然後按一下Add。系統將顯示Add Port Forwarding Entry對話方塊。



Add Port Forwarding Entry

Local TCP Port: 3044

Remote Server: 10.2.2.2

Remote TCP Port: 23

Description: Telnet to R1

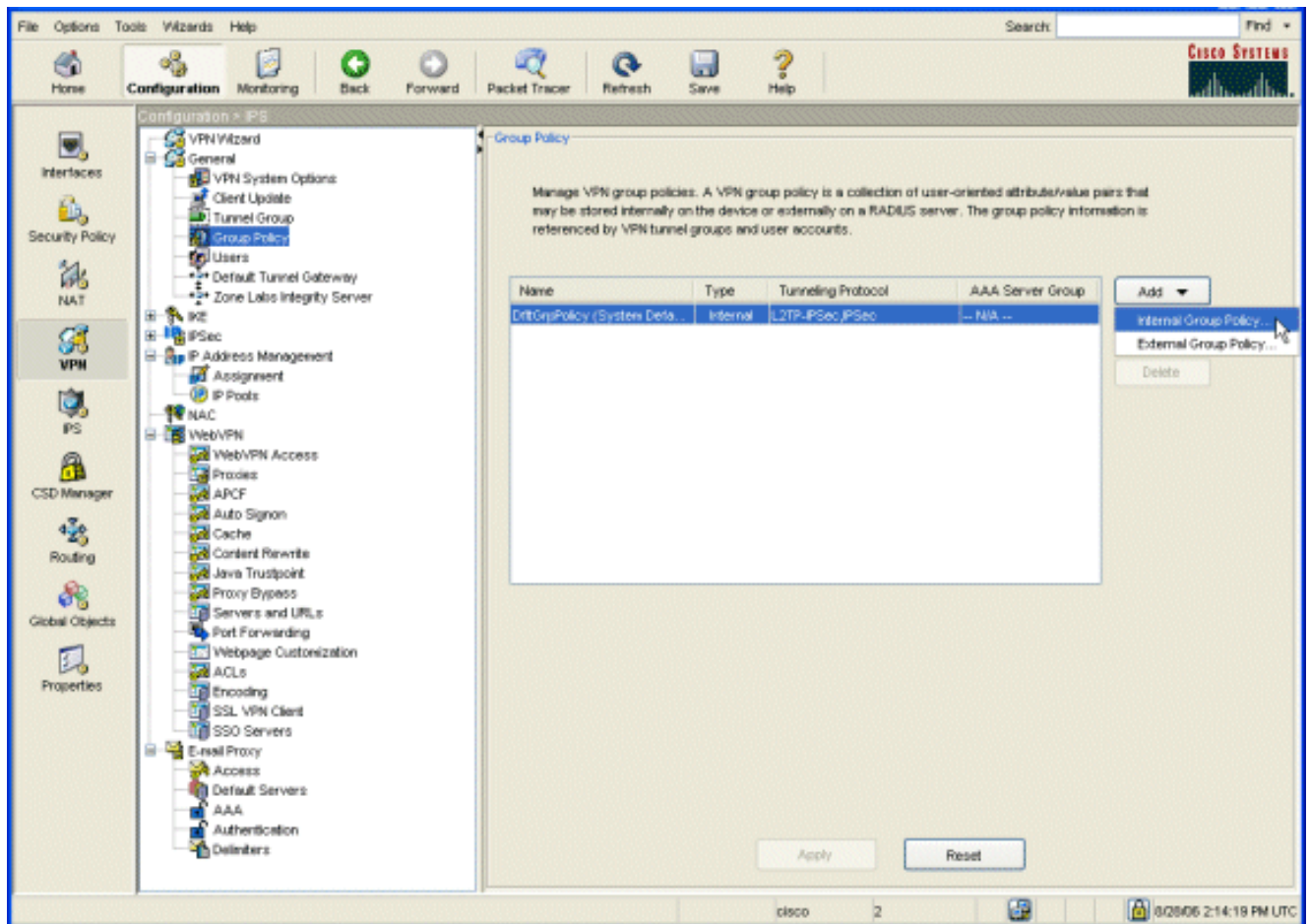
OK Cancel Help

4. 在新增埠轉發條目對話方塊中，輸入以下選項：在Local TCP Port欄位中，輸入埠號或接受預設值。輸入的值可以是從1024到65535之間的任何數字。在Remote Server欄位中，輸入IP地址。本示例使用路由器的地址。在Remote TCP Port欄位中，輸入埠號。此範例使用連線埠23。在「說明」欄位中輸入說明，然後按一下**確定**。
5. 按一下「**OK**」，然後按一下「**Apply**」。
6. 按一下**Save**，然後按一下**Yes**接受更改。

### **步驟3.建立組策略並將其連結到埠轉發清單**

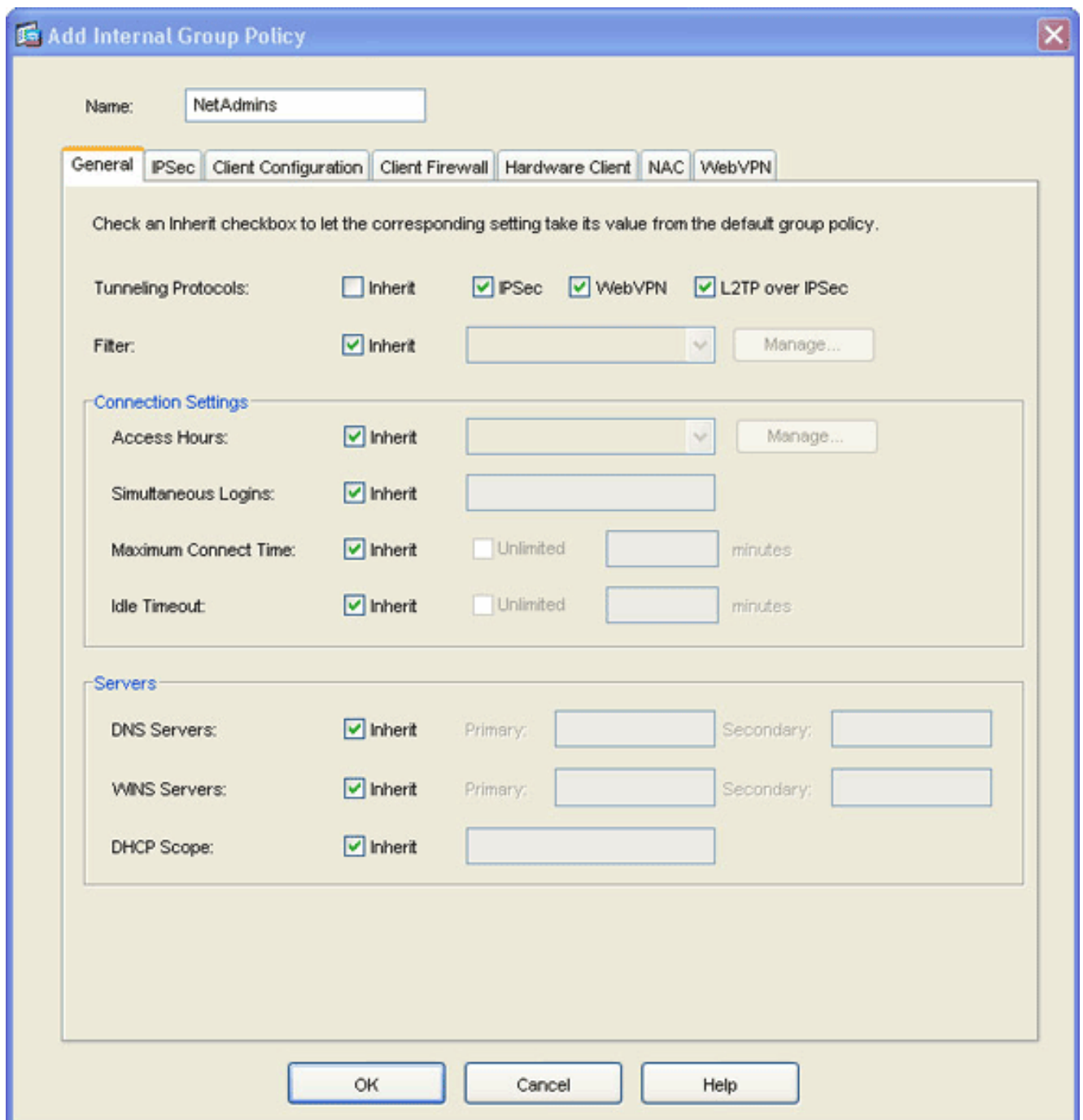
要建立組策略並將其連結到埠轉發清單，請完成以下步驟：

1. 展開**General**，然後選擇**Group Policy**。



2. 按一下Add，然後選擇Internal Group Policy。系統將顯示Add Internal Group Policy對話方塊

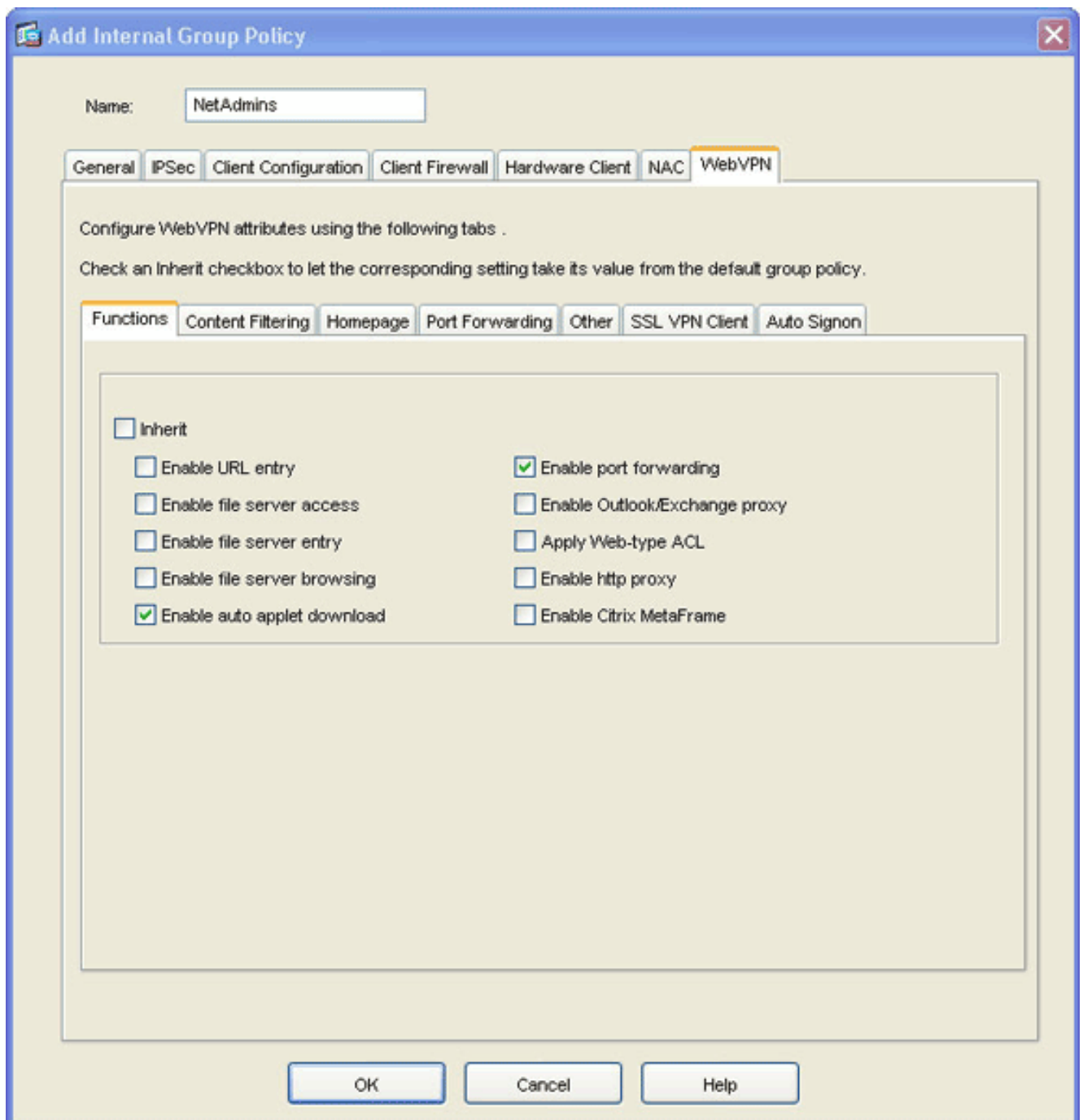
。



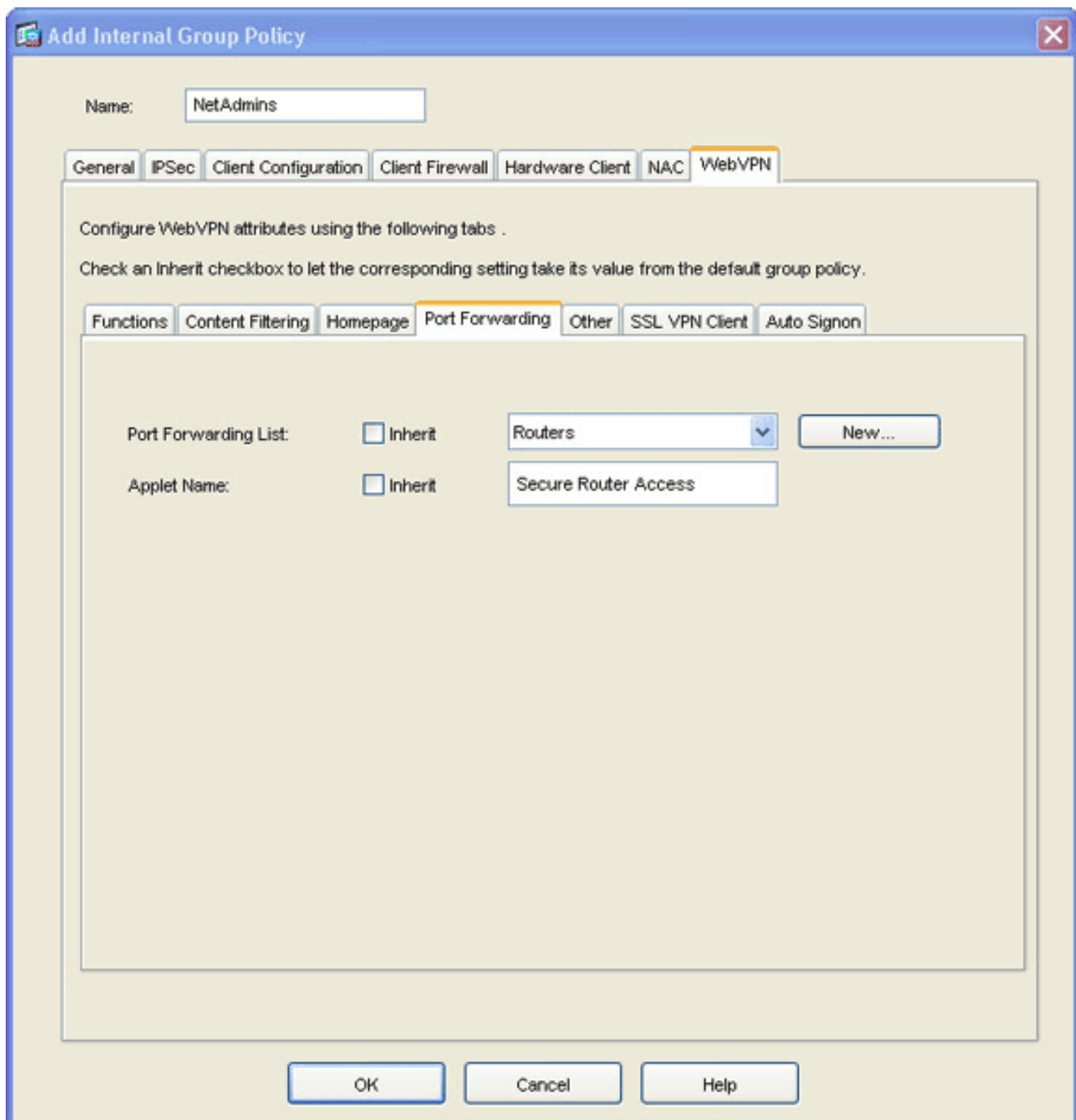
3. 輸入名稱或接受預設組策略名稱。
4. 取消選中Tunneling Protocols **Inherit** 覆取方塊，然後選中**WebVPN** 覆取方塊。
5. 按一下位於對話方塊頂部的**WebVPN** 頁籤，然後按一下**Functions** 頁籤。
6. 取消選中**Inherit** 覆取方塊，然後選中**Enable auto applet download** 和 **Enable port forwarding** 覆取方塊，如下圖所示

:





7. 在WebVPN頁籤中，按一下Port Forwarding頁籤，並取消選中Port Forwarding List Inherit覈取方塊。



8. 按一下**Port Forwarding List**下拉箭頭，然後選擇您在[步驟2中建立的埠轉發清單](#)。
9. 取消選中Applet Name **Inherit**覆取方塊，然後更改文本欄位中的名稱。客戶端在連線時顯示Applet名稱。
10. 按一下「**OK**」，然後按一下「**Apply**」。
11. 按一下**Save**，然後按一下**Yes**接受更改。

#### **步驟4. 建立隧道組並將其連結到組策略**

您可以編輯預設的*DefaultWebVPNGroup*隧道組或建立新的隧道組。

若要建立新的通道組，請完成以下步驟：

1. 展開**General**，然後選擇**Tunnel Group**。

Configuration > VPN > General > Tunnel Group

Manage VPN tunnel groups. A VPN tunnel group represents a connection specific record for a IPsec or WebVPN connection.

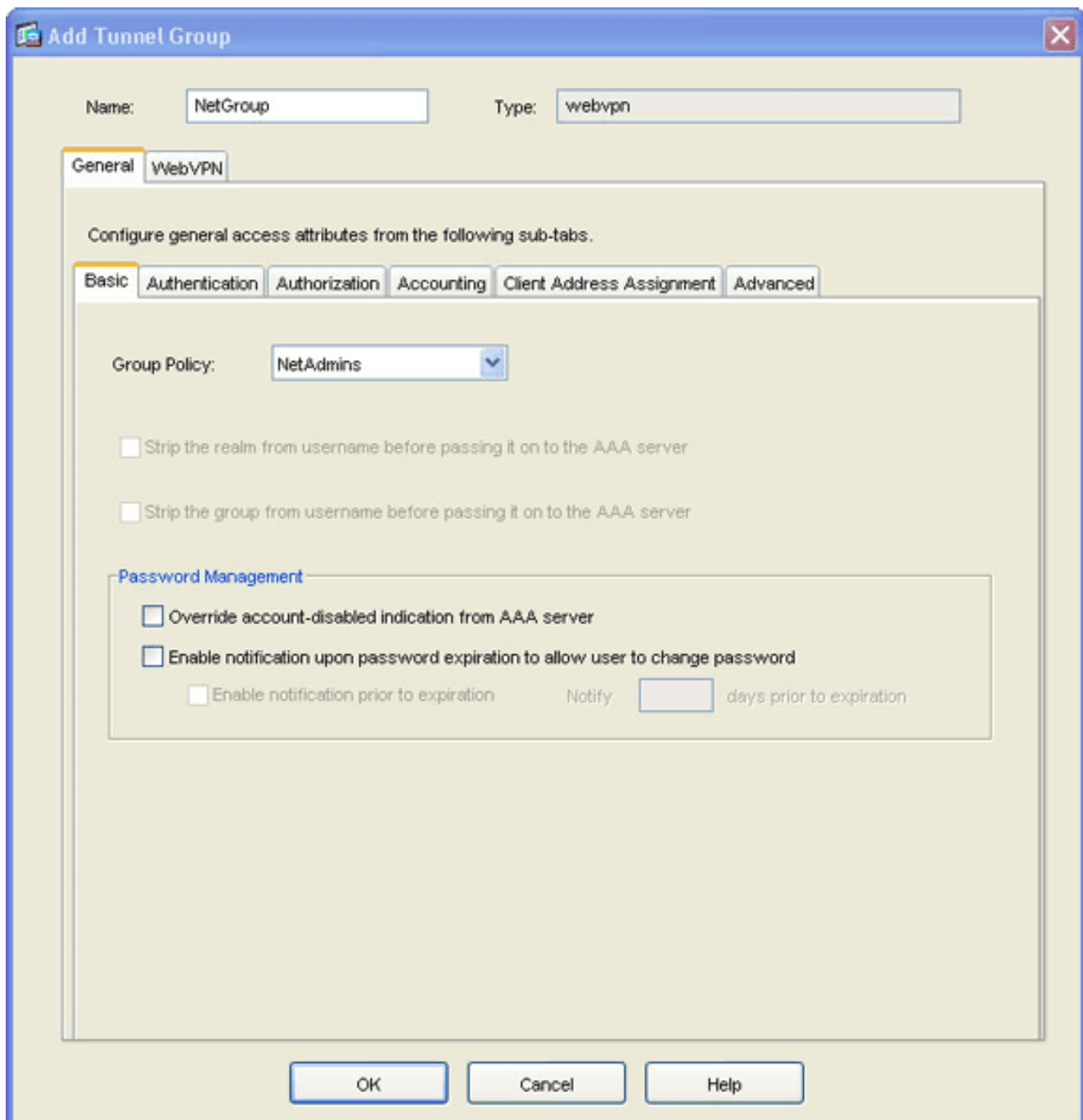
Name	Type	Group Policy
DefaultWEBVPNGroup	webvpn	DfltGrpPolicy
DefaultRAGroup	ipsec-ra	DfltGrpPolicy
DefaultL2LGroup	ipsec-l2l	DfltGrpPolicy

Specify the delimiter to be used when parsing tunnel group names from the user name that are received when tunnels are being negotiated.

Group Delimiter:

Configuration changes saved successfully. cisco 15 7/18/06 1:26:59 PM UTC

2. 按一下Add，然後選擇WebVPN Access。系統將顯示Add Tunnel Group對話方塊。

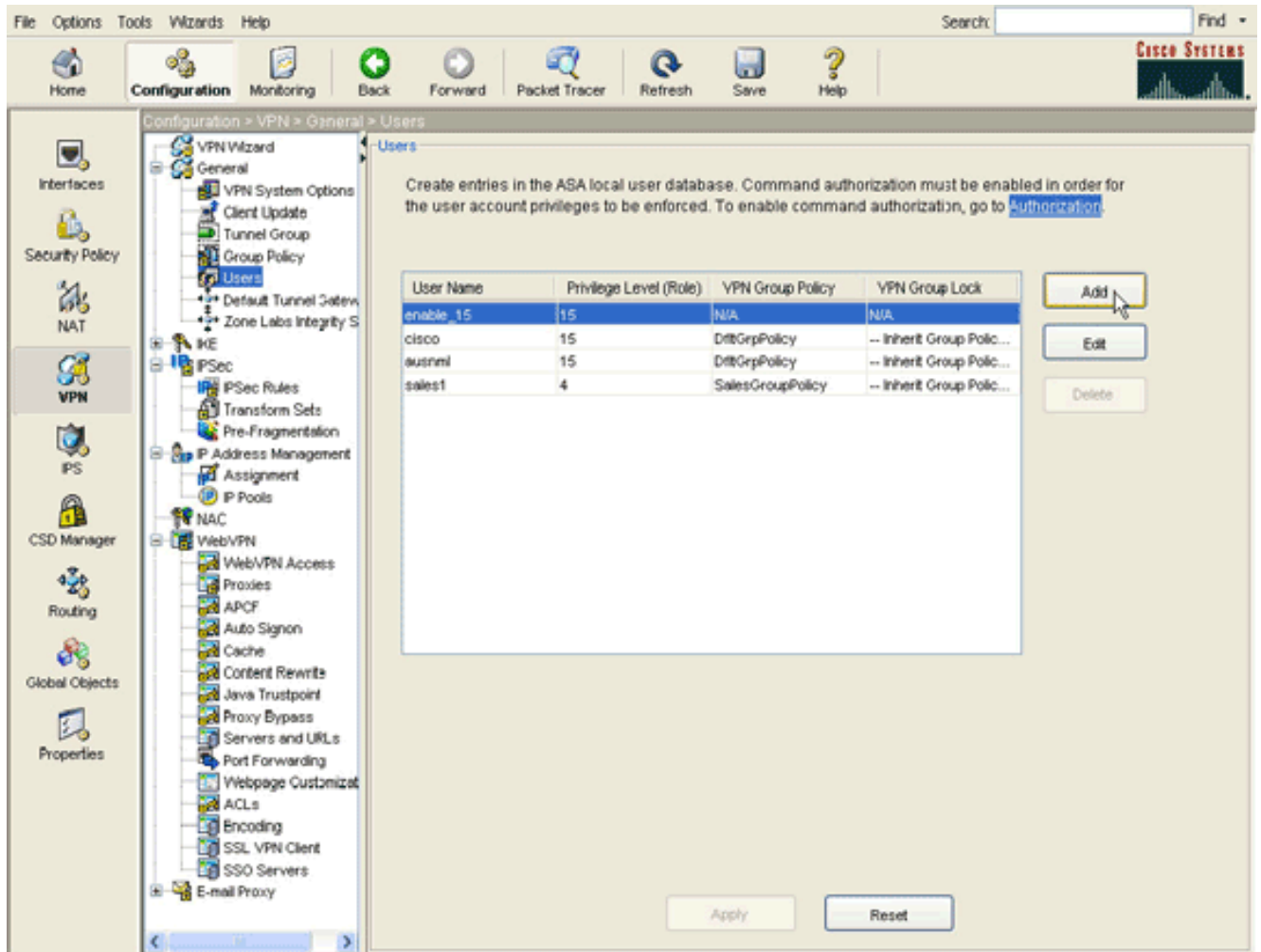


3. 在「名稱」欄位中輸入名稱。
4. 按一下 **Group Policy** 下拉箭頭，然後選擇您在步驟3中建立的組策略。
5. 按一下「OK」，然後按一下「Apply」。
6. 按一下 **Save**，然後按一下 **Yes** 接受更改。隧道組、組策略和埠轉發特性現在已連結。

### 步驟5. 建立使用者並將該使用者新增到組策略中

要建立使用者並將該使用者新增到組策略，請完成以下步驟：

1. 展開 **General**，然後選擇 **Users**。



2. 按一下Add按鈕。系統將顯示Add User Account對話方塊。

**Add User Account**

Identity | VPN Policy | WebVPN

Username: user1

Password: \*\*\*\*\*

Confirm Password: \*\*\*\*\*

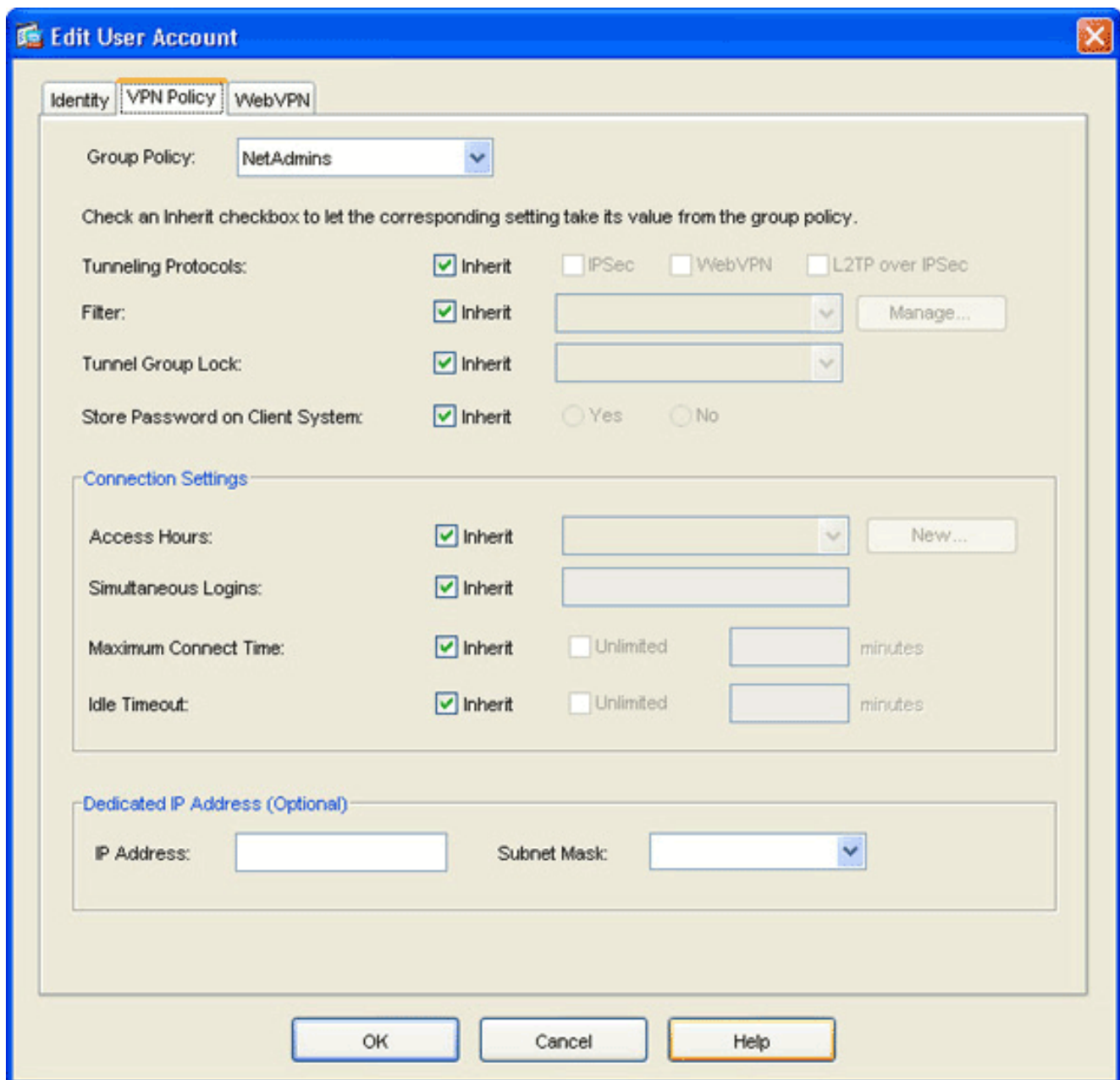
User authenticated using MSCHAP

Privilege level is used with command authorization.

Privilege Level: 2

OK Cancel Help

3. 輸入使用者名稱、密碼和許可權資訊的值，然後按一下VPN策略頁籤。



4. 按一下**Group Policy**下拉箭頭，然後選擇您在步驟3中建立的組**策略**。此使用者繼承所選組策略的WebVPN特徵和策略。
5. 按一下「OK」，然後按一下「Apply」。
6. 按一下**Save**，然後按一下**Yes**接受更改。

## 使用CLI的瘦客戶端SSL VPN配置

ASA
<pre> ASA Version 7.2(1) ! hostname ciscoasa domain-name default.domain.invalid enable password 8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0  nameif inside  security-level 100  ip address 10.1.1.1 255.255.255.0 </pre>

```

!--- Output truncated port-forward portforward 3044
10.2.2.2 telnet Telnet to R1
!--- Configure the set of applications that WebVPN
users !--- can access over forwarded TCP ports group-
policy NetAdmins internal
!--- Create a new group policy for enabling WebVPN
access group-policy NetAdmins attributes
  vpn-tunnel-protocol IPSec l2tp-ipsec webvpn
!--- Configure group policy attributes webvpn
  functions port-forward auto-download
!--- Configure group policies for WebVPN port-forward
value portforward
!--- Configure port-forward to enable WebVPN
application access !--- for the new group policy port-
forward-name value Secure Router Access
!--- Configure the display name that identifies TCP
port !--- forwarding to end users username user1
password tJsDL6po9m1UFs.h encrypted
username user1 attributes
  vpn-group-policy NetAdmins
!--- Create and add User(s) to the new group policy
http server enable http 0.0.0.0 0.0.0.0 DMZ no snmp-
server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart tunnel-group NetGroup type webvpn
tunnel-group NetGroup general-attributes
  default-group-policy NetAdmins
!--- Create a new tunnel group and link it to the group
policy telnet timeout 5 ssh timeout 5 console timeout 0
! class-map inspection_default match default-
inspection-traffic !! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323
h225 inspect h323 ras inspect netbios inspect rsh
inspect rtsp inspect skinny inspect esmtp inspect
sqlnet inspect sunrpc inspect tftp inspect sip inspect
xdmcp ! service-policy global_policy global webvpn
enable outside
!--- Enable Web VPN on Outside interface port-forward
portforward 3044 10.2.2.2 telnet Telnet to R1 prompt
hostname context

```

## 驗證

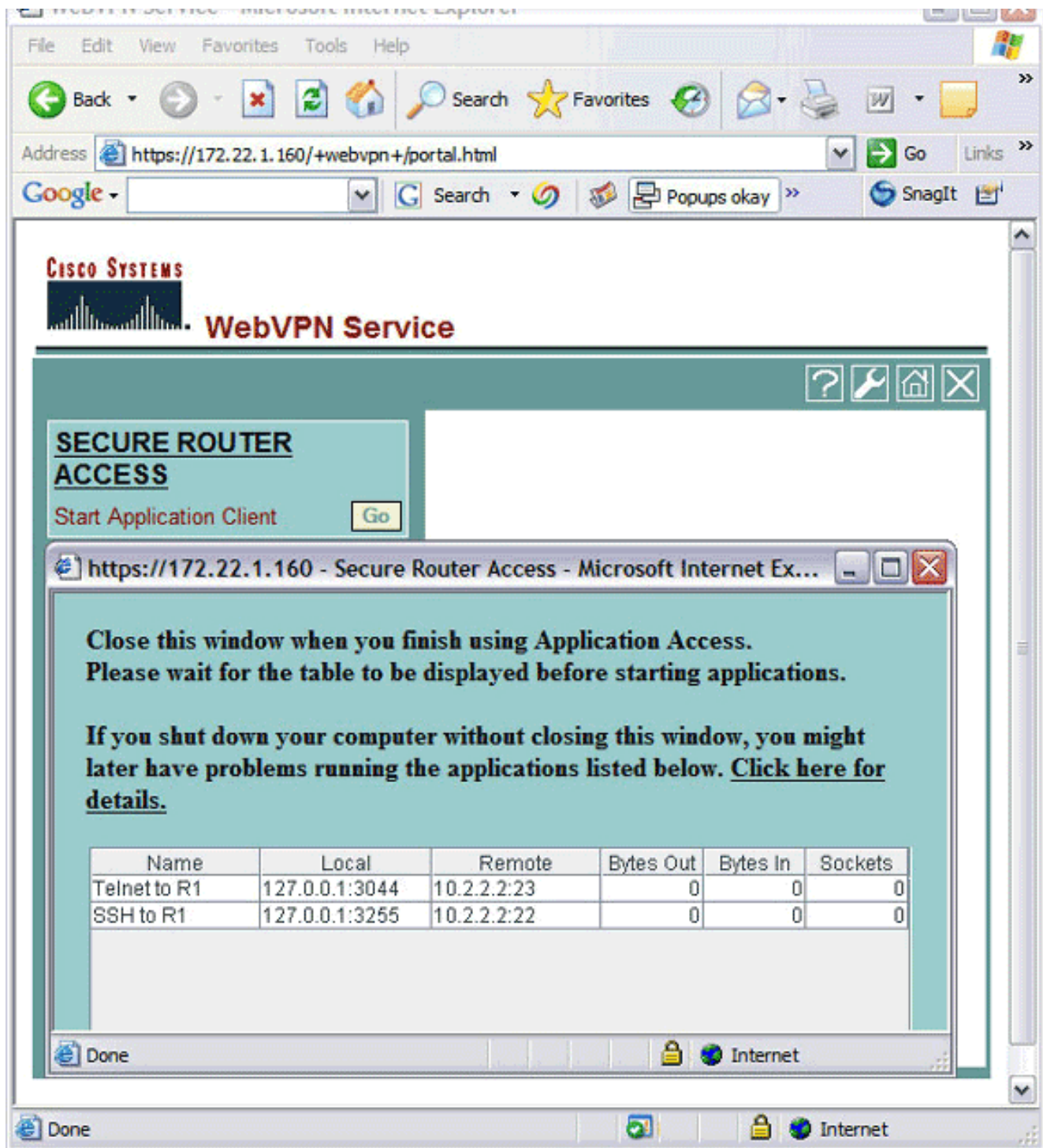
使用本節內容，驗證您的組態是否正常運作。

## 程式

此程式介紹如何確定配置的有效性以及如何測試配置。

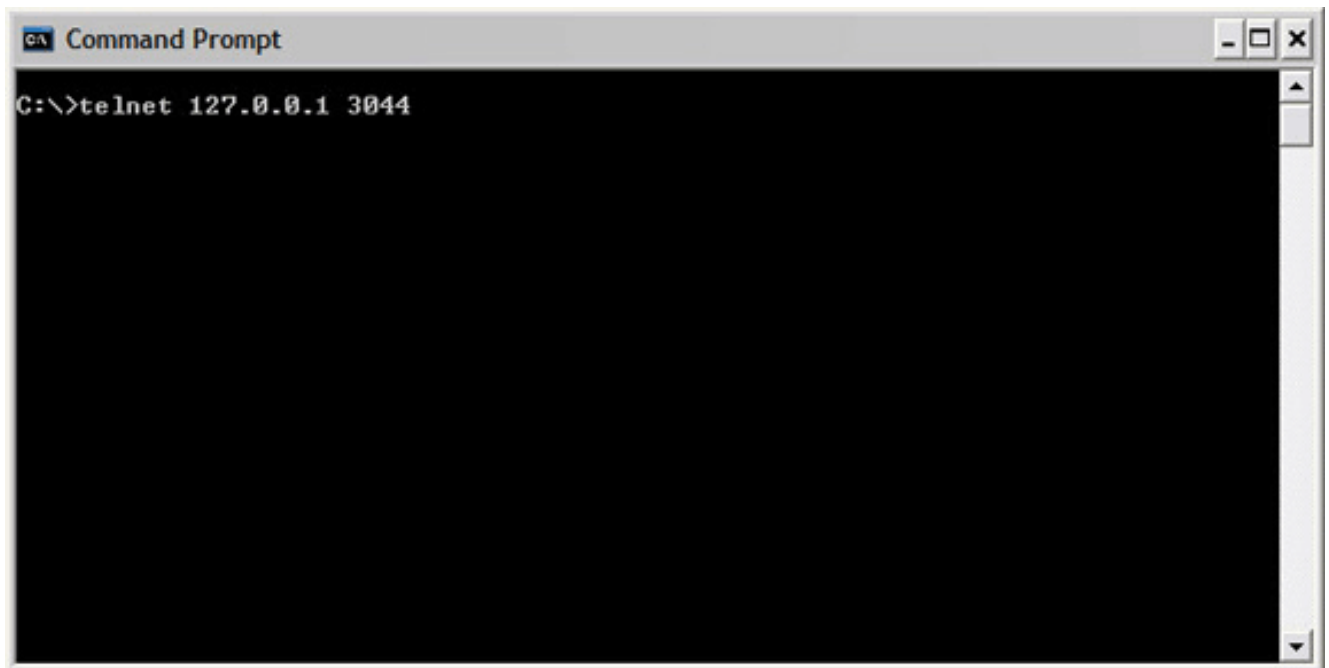
1. 在客戶端工作站上，輸入 **https://outside\_ASA\_IP Address**；其中 *outside\_ASA\_IPAddress* 是 ASA 的 SSL URL。接受數位證書並驗證使用者後，將顯示 WebVPN 服務網頁。





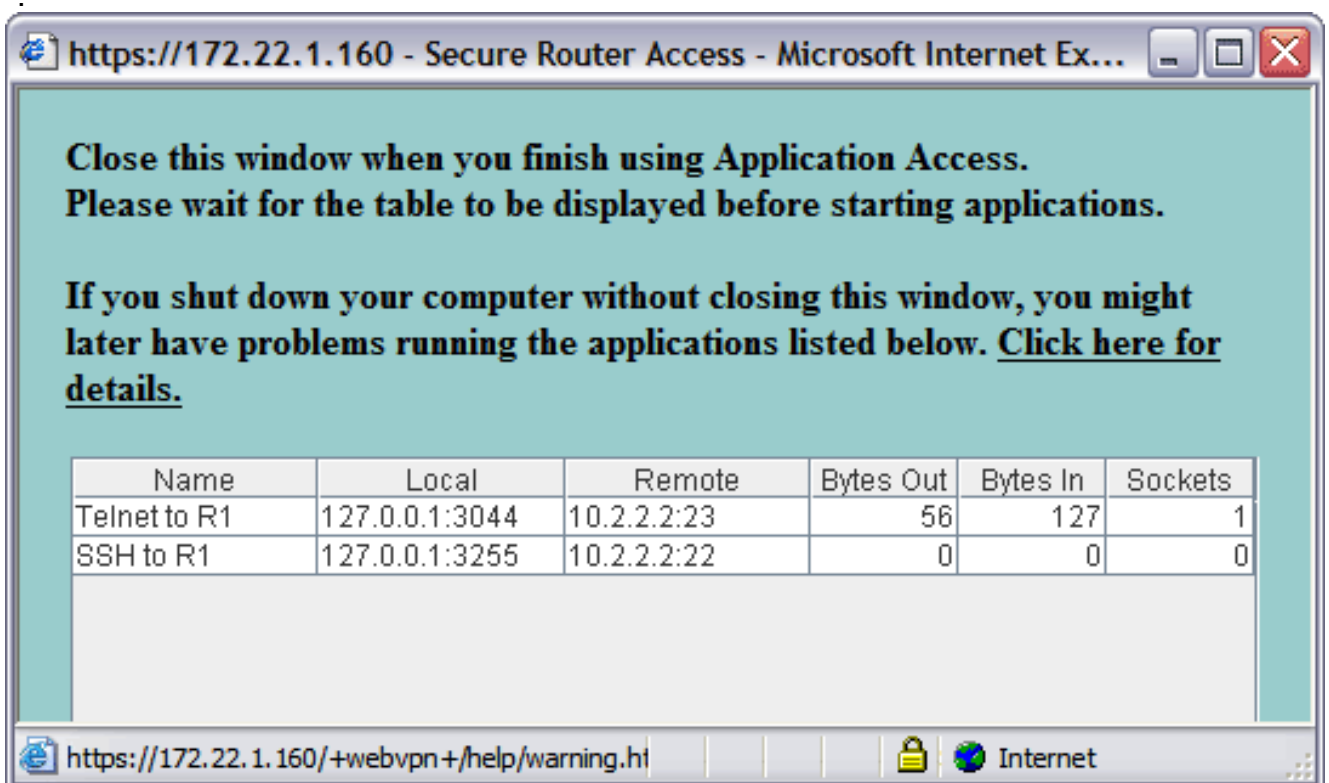
訪問應用程式所需的地址和埠資訊顯示在本地列中。Bytes Out和Bytes In列不顯示任何活動，因為此時尚未呼叫應用程式。

2. 使用DOS提示符或其他Telnet應用程式啟動Telnet會話。
3. 在命令提示符下，輸入`telnet 127.0.0.1 3044`。**注意：**此命令提供如何訪問本文檔中WebVPN服務網頁影象中所顯示的本地埠的示例。命令不包含冒號(:)。按本文所述鍵入命令。ASA通過安全會話接收命令，並且由於它儲存了資訊對映，因此ASA知道立即開啟到對映裝置的安全Telnet會話。



輸入使用者名稱和密碼後，即可完成裝置訪問。

4. 若要驗證對裝置的存取許可權，請檢查Bytes Out和Bytes In列，如下圖所示



## 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。有關show命令的詳細資訊，請參閱[驗證WebVPN配置](#)。

註：[Output Interpreter Tool\(僅限註冊客戶\)](#)(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。

## SSL握手過程是否完成？

連線到ASA後，檢查即時日誌是否顯示SSL握手的完成。

Severity	Date	Time	Syslog	Source IP	Destination IP	Description
2	Jun 27 2006	11:40:42	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3102 to 216.239.53.147
2	Jun 27 2006	11:40:34	106006	172.22.1.203	171.70.157.215	Deny inbound UDP from 172.22.1.203/3101 to 171.70.157.215/1029 on interface
2	Jun 27 2006	11:40:34	106006	172.22.1.203	64.101.176.170	Deny inbound UDP from 172.22.1.203/3101 to 64.101.176.170/1029 on interface
2	Jun 27 2006	11:40:34	106006	172.22.1.203	171.68.222.149	Deny inbound UDP from 172.22.1.203/3101 to 171.68.222.149/1029 on interface
2	Jun 27 2006	11:40:32	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3100 to 216.239.53.147
2	Jun 27 2006	11:40:24	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3098 to 216.239.53.147
2	Jun 27 2006	11:40:22	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3098 to 216.239.53.147
6	Jun 27 2006	11:40:18	725002	172.22.1.203		Device completed SSL handshake with client outside:172.22.1.203/3097
6	Jun 27 2006	11:40:18	725003	172.22.1.203		SSL client outside:172.22.1.203/3097 request to resume previous session
6	Jun 27 2006	11:40:18	725001	172.22.1.203		Starting SSL handshake with client outside:172.22.1.203/3097 for TLSv1
6	Jun 27 2006	11:40:18	302013	172.22.1.203	172.22.1.160	Built inbound TCP connection 3711 for outside:172.22.1.203/3097 (172.22.1.160)
6	Jun 27 2006	11:40:18	725007	172.22.1.203		SSL session with client outside:172.22.1.203/3096 terminated.
6	Jun 27 2006	11:40:17	302014	172.22.1.203	172.22.1.160	Tear down TCP connection 3710 for outside:172.22.1.203/3096 to NP Id
6	Jun 27 2006	11:40:17	725002	172.22.1.203		Device completed SSL handshake with client outside:172.22.1.203/3096
6	Jun 27 2006	11:40:17	725001	172.22.1.203		Starting SSL handshake with client outside:172.22.1.203/3096 for TLSv1
6	Jun 27 2006	11:40:17	302013	172.22.1.203	172.22.1.160	Built inbound TCP connection 3710 for outside:172.22.1.203/3096 (172.22.1.160)
3	Jun 27 2006	11:40:16	305005	64.101.176.170		No translation group found for udp src inside:10.2.2.4/1830 dst outside:64.101.176.170
3	Jun 27 2006	11:40:16	305005	171.70.157.215		No translation group found for udp src inside:10.2.2.4/1830 dst outside:171.70.157.215
3	Jun 27 2006	11:40:16	305005	171.68.222.149		No translation group found for udp src inside:10.2.2.4/1830 dst outside:171.68.222.149
2	Jun 27 2006	11:40:15	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3095 to 216.239.53.147
2	Jun 27 2006	11:40:12	106001	172.22.1.203	216.239.53.147	Inbound TCP connection denied from 172.22.1.203/3095 to 216.239.53.147

## SSL VPN瘦客戶端是否正常工作？

要驗證SSL VPN瘦客戶端是否正常工作，請完成以下步驟：

1. 按一下**Monitoring**，然後按一下**VPN**。
2. 展開**VPN Statistics**，然後按一下**Sessions**。您的SSL VPN瘦客戶端會話應出現在會話清單中。請務必按WebVPN進行過濾，如下圖所示：

The screenshot shows the Cisco ASDM interface for monitoring VPN sessions. The left sidebar contains navigation options like Interfaces, VPN, IPS, Routing, Properties, and Logging. The main content area is titled 'Monitoring > VPN > VPN Statistics > Sessions'. It features a summary table for session types and a detailed table for individual sessions.

Remote Access	LAN-to-LAN	WebVPN	SSL VPN Client	E-mail Proxy	Total	Total Cumulative
0	0	1	0	0	1	22

Username	Group Policy	Protocol	Login Time
P Address	Tunnel Group	Encryption	Duration
user1	NetAdmins	WebVPN	11:41:23 UTC Tue Jun 27 2006
172.22.1.203	DefaultWEBVPNGroup	3DES	0h:01m:06s

## 指令

有幾個debug命令與WebVPN關聯。有關這些命令的詳細資訊，請參閱[使用WebVPN Debug命令](#)。

**注意：**使用debug指令可能會對思科裝置造成負面影響。使用debug指令之前，請先參閱[有關Debug指令的重要資訊](#)。

## 相關資訊

- [ASA上的無客戶端SSL VPN\(WebVPN\)配置示例](#)
- [帶ASDM的ASA上的SSL VPN客戶端\(SVC\)配置示例](#)
- [Cisco ASA 5500系列調適型安全裝置](#)
- [使用ASDM和NTLMv1的WebVPN和單一登入的ASA配置示例](#)
- [技術支援與文件 - Cisco Systems](#)