使用路由器和SDM配置Cisco IOS IPS

目錄

簡介

本檔案介紹如何使用Cisco Router and Security Device Manager(SDM)版本2.5在12.4(15)T3和更新版本中設定Cisco IOS® Intrusion Prevention System(IPS)。

SDM 2.5中與IOS IPS相關的增強功能如下：

- 在簽名清單GUI中顯示的已編譯簽名總數
- SDM簽名檔案(zip檔案格式；例如，sigv5-SDM-S307.zip)和CLI簽名包(pkg檔案格式；例如，IOS-S313-CLI.pkg)可以在一次操作中一起下載
- 下載的簽名軟體包可以作為一個選項自動推送到路由器

初始調配過程中涉及的任務包括：

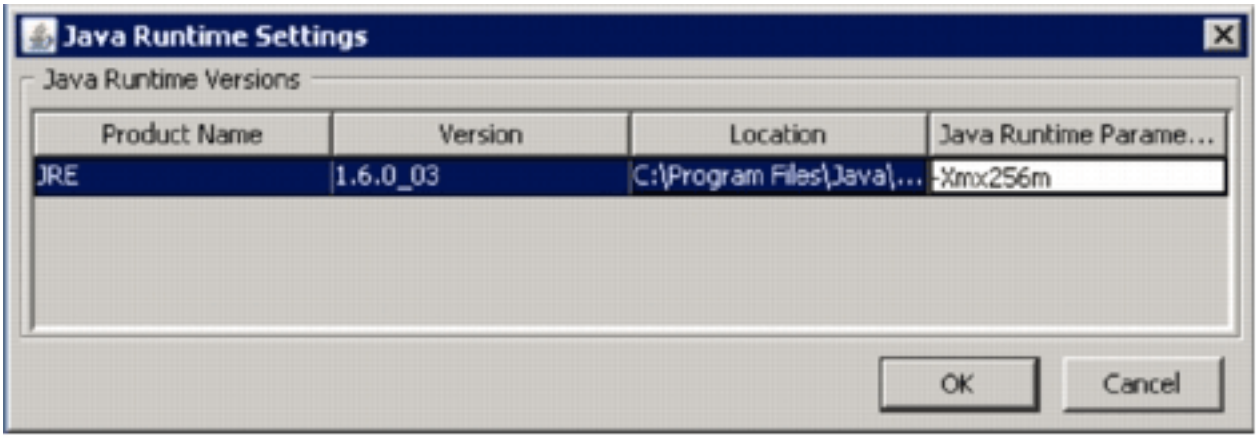
1. 下載並安裝SDM 2.5。
2. 使用SDM自動更新將IOS IPS簽名軟體包下載到本地PC。
3. 啟動IPS策略嚮導以配置IOS IPS。
4. 驗證IOS IPS配置和簽名是否已正確載入

Cisco SDM是一種基於Web的配置工具，它通過智慧嚮導簡化了路由器和安全配置，可幫助客戶快速輕鬆地部署、配置和監控Cisco路由器，而無需瞭解命令列介面(CLI)。

SDM 2.5版可從以下網址下載：Cisco.com http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm(僅限註冊客戶)。 發行說明位於 http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/software/release/notes/SDMr25.html

注意：Cisco SDM要求螢幕解析度至少為1024 x 768。

註：Cisco SDM要求Java記憶體堆大小不小於256MB，以便配置IOS IPS。若要更改Java記憶體堆大小，請開啟Java控制面板，按一下**Java**頁籤，按一下「Java小程式運行時設定」下的**檢視**，然後在「Java運行時引數」列中輸入**-Xmx256m**。



必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 12.4(15)T3及更新版本中的Cisco IOS IPS
- Cisco路由器和安全裝置管理員(SDM)版本2.5

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）的組態來啟動。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。

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。

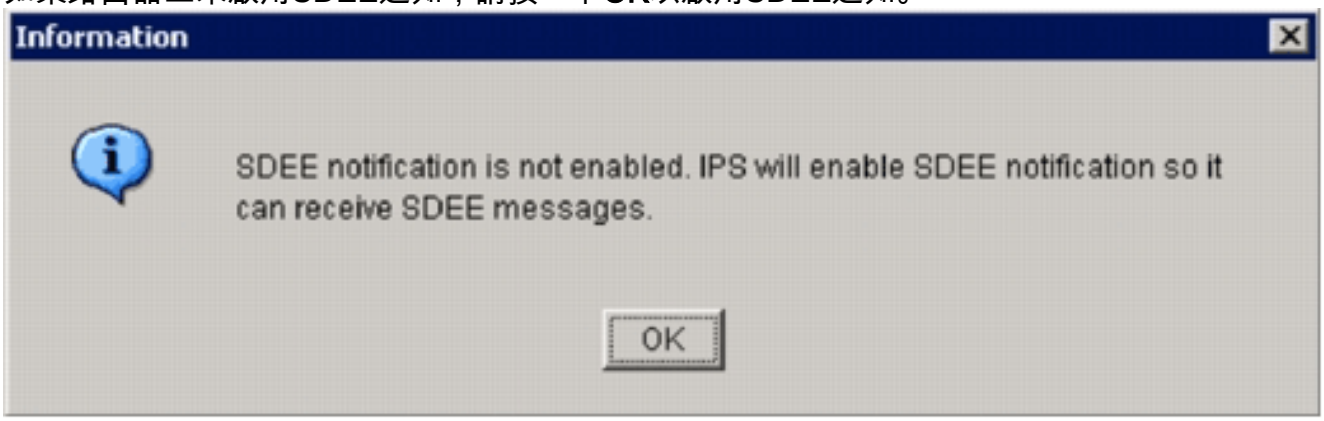
設定

注意：開啟到路由器的控制檯或telnet會話（啟用「term monitor」），以便在使用SDM調配IOS IPS時監控消息。

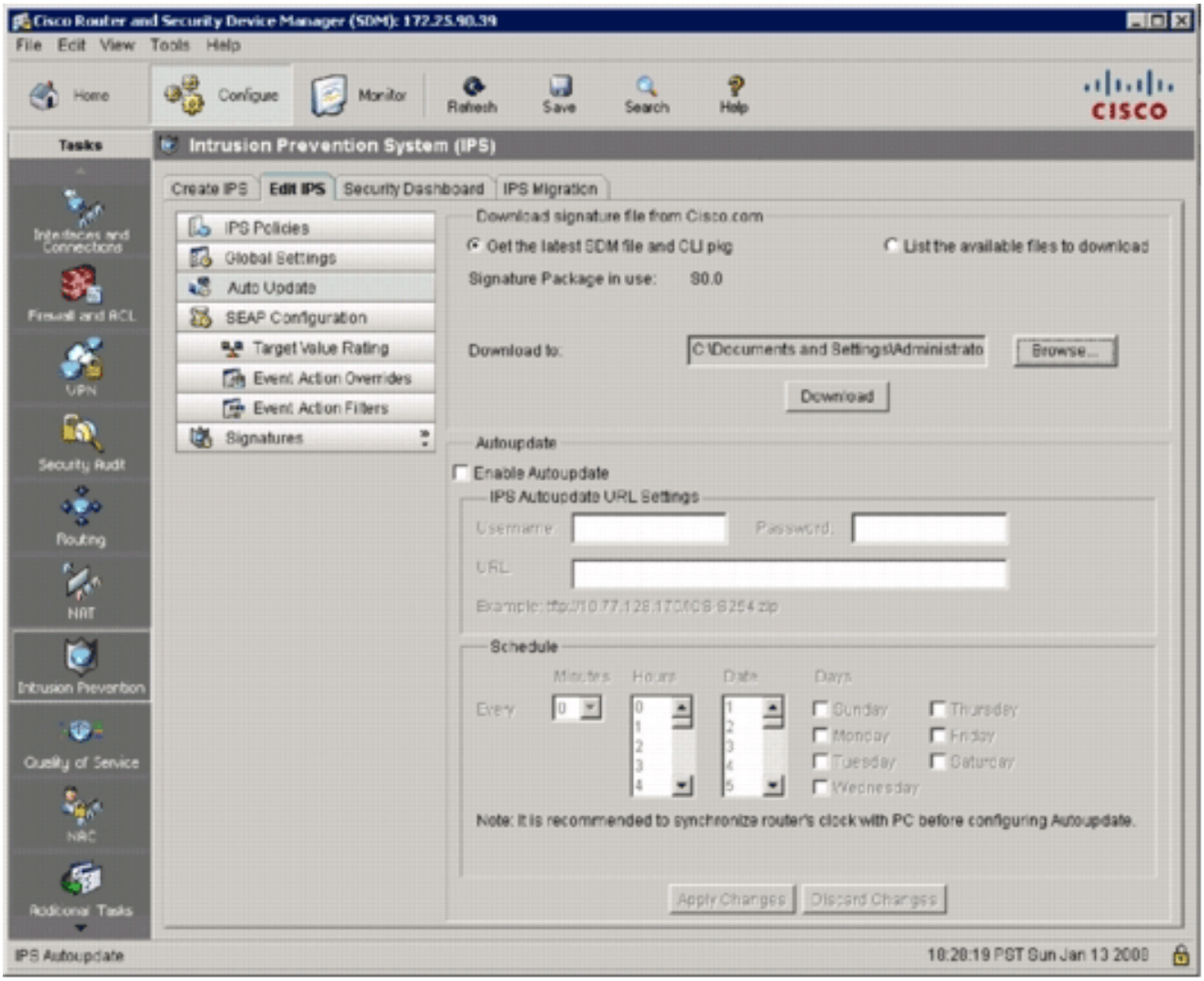
1. 從Cisco.com下載SDM 2.5，網址為http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm(僅供註冊客戶使用)，並將其安裝在本地PC上。
2. 從本地PC運行SDM 2.5。
3. 出現「IOS IPS Login（IOS IPS登入）」對話方塊時，請輸入與路由器的SDM身份驗證相同的

使用者名稱和密碼。

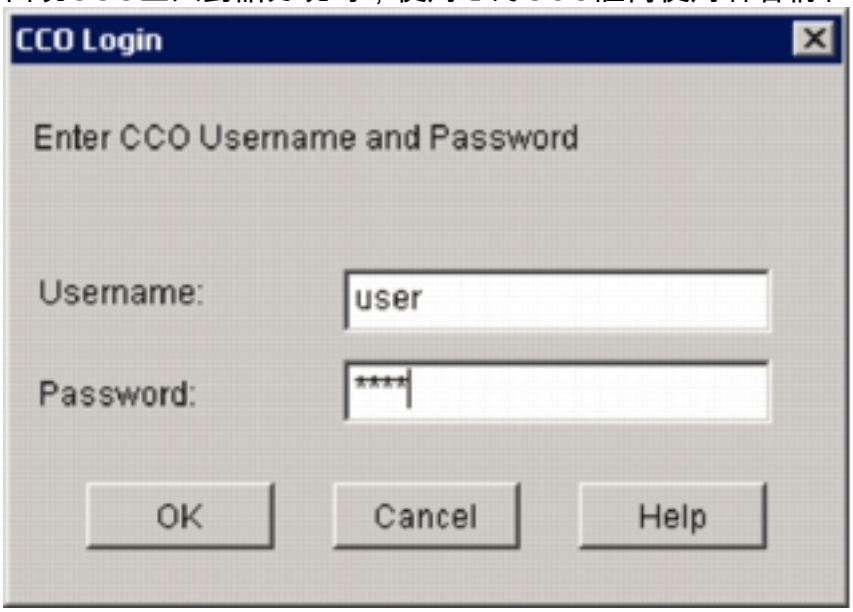
4. 在SDM使用者介面中，按一下**Configure**，然後按一下**Intrusion Prevention**。
5. 按一下**Edit IPS**頁籤。
6. 如果路由器上未啟用SDEE通知，請按一下**OK**以啟用SDEE通知。



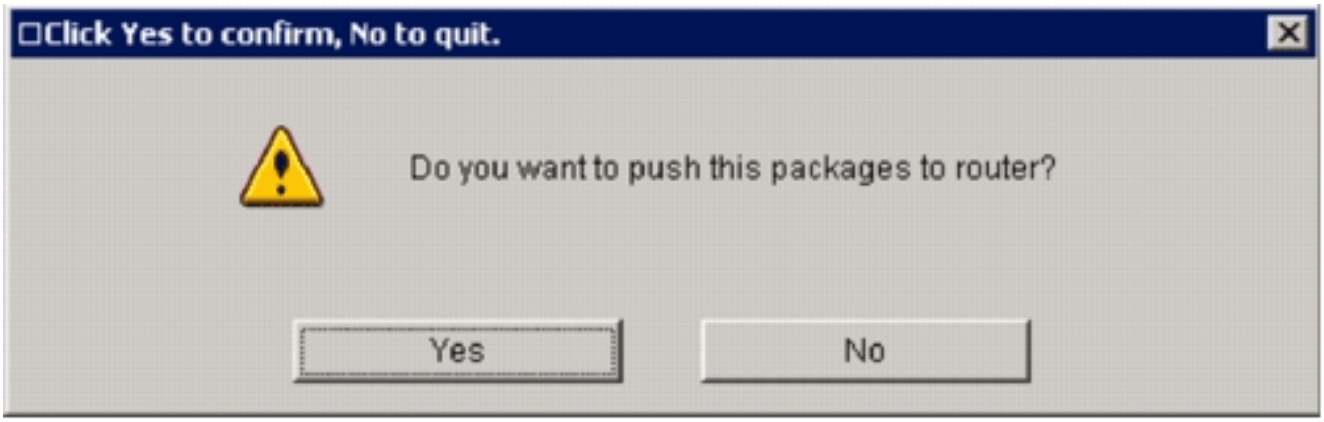
7. 在「編輯IPS」頁籤的「從Cisco.com下載特徵碼檔案」區域中，按一下**Get the latest SDM file and CLI pkg**單選按鈕，然後按一下**Browse**以選擇本地PC上儲存下載檔案的目錄。您可以選擇TFTP或FTP伺服器根目錄，稍後在將簽名軟體包部署到路由器時將使用該目錄。
8. 按一下**「Download」。**



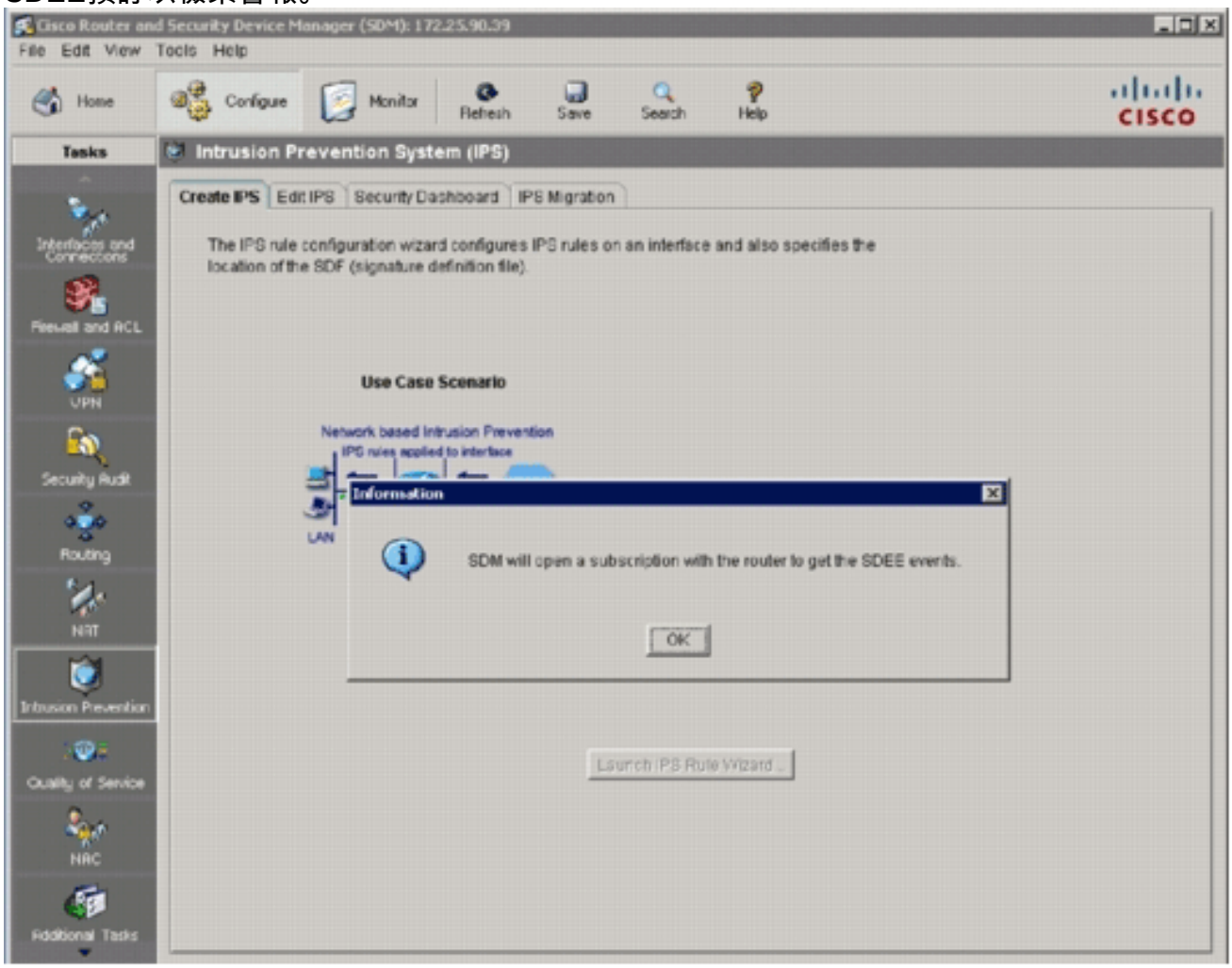
9. 出現CCO登入對話方塊時，使用您的CCO註冊使用者名稱和密碼。



SDM連線到Cisco.com，並開始將SDM檔案（例如sigv5-SDM-S307.zip）和CLI包檔案（例如IOS-S313-CLI.pkg）下載到步驟7中選定的目錄。下載兩個檔案後，SDM會提示您將下載的簽名軟體包推送到路由器。

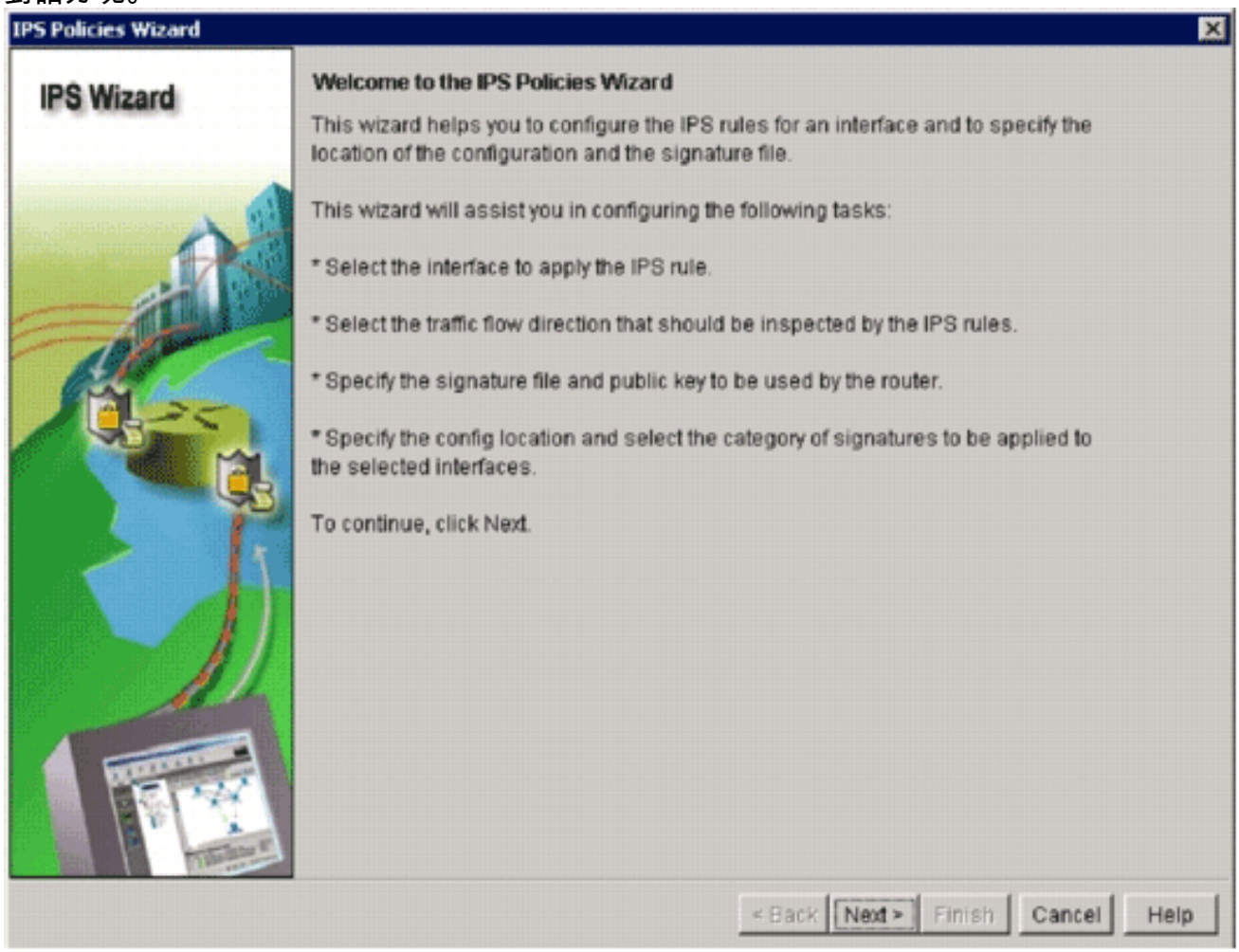


10. 由於路由器上尚未配置IOS IPS，請按一下**No**。
11. SDM下載最新的IOS CLI簽名軟體包後，按一下**Create IPS**頁籤以建立初始IOS IPS配置。
12. 如果系統提示您將變更套用到路由器，請按一下「**Apply Changes**」。
13. 按一下**Launch IPS Rule Wizard**。將出現一個對話方塊，通知您SDM需要建立對路由器的SDEE預訂以檢索警報。

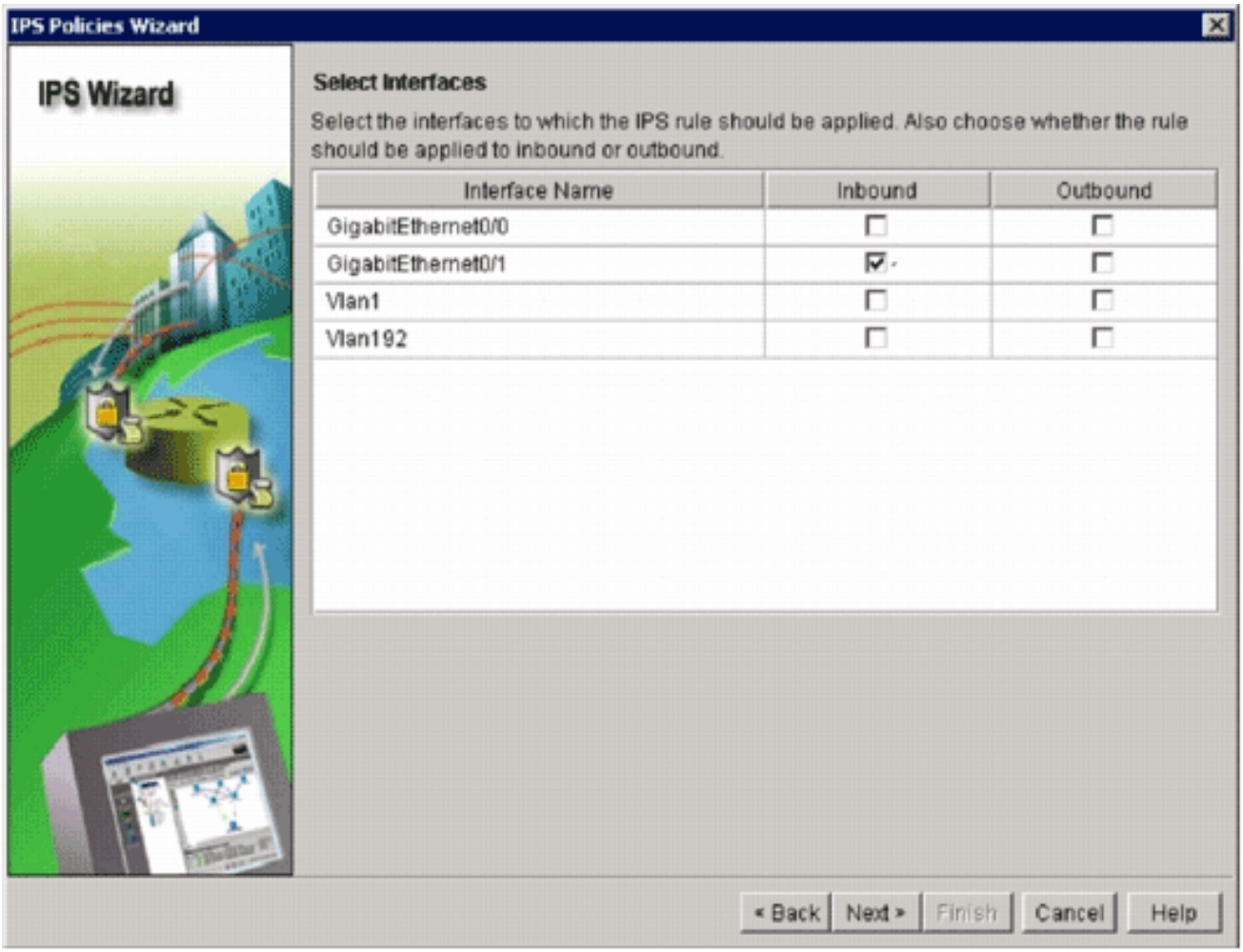


14. 按一下「**OK**」（確定）。出現Authentication Required對話方塊。

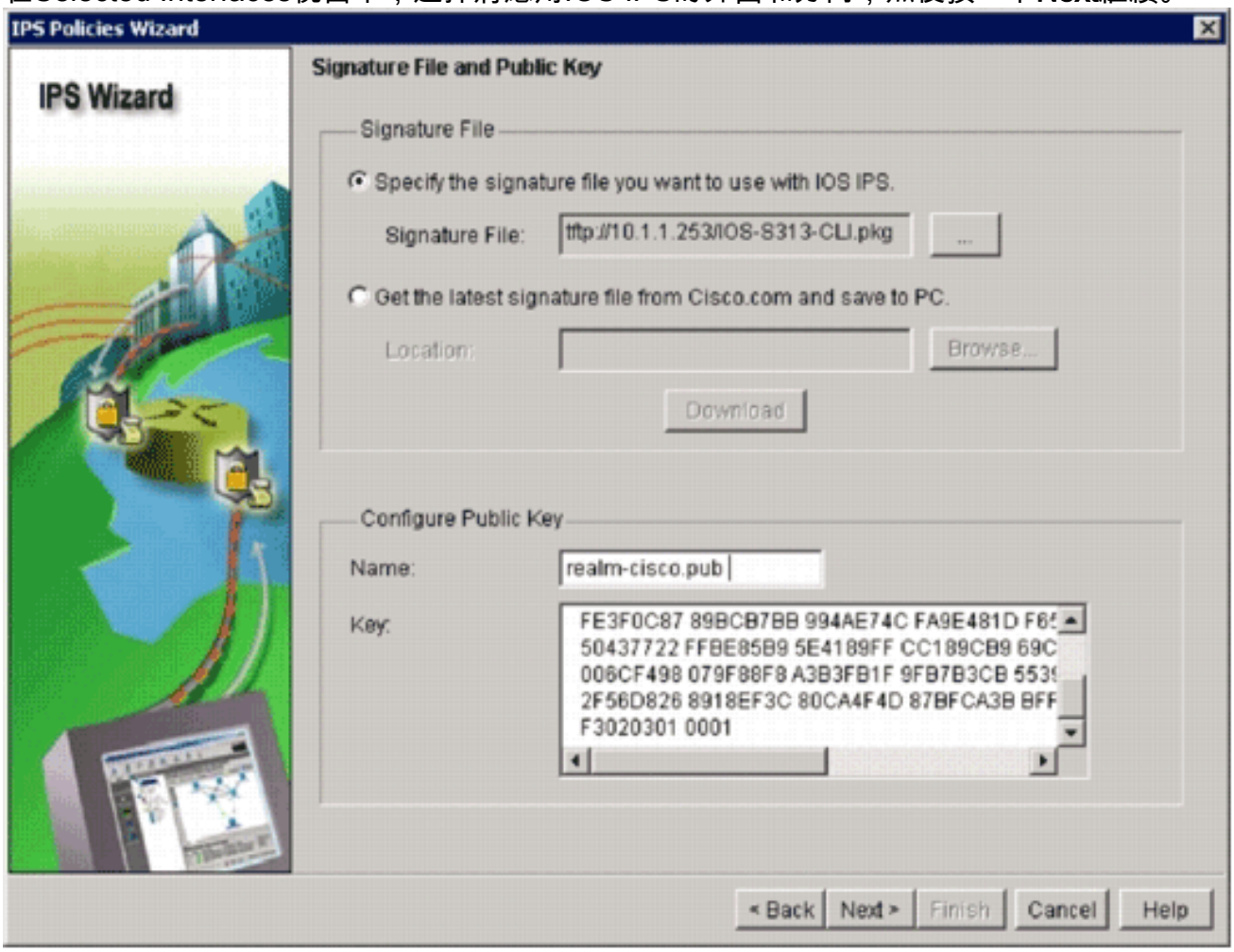
15. 輸入用於SDM驗證到路由器的使用者名稱和密碼，然後按一下**OK**。系統將顯示IPS策略嚮導對話方塊。



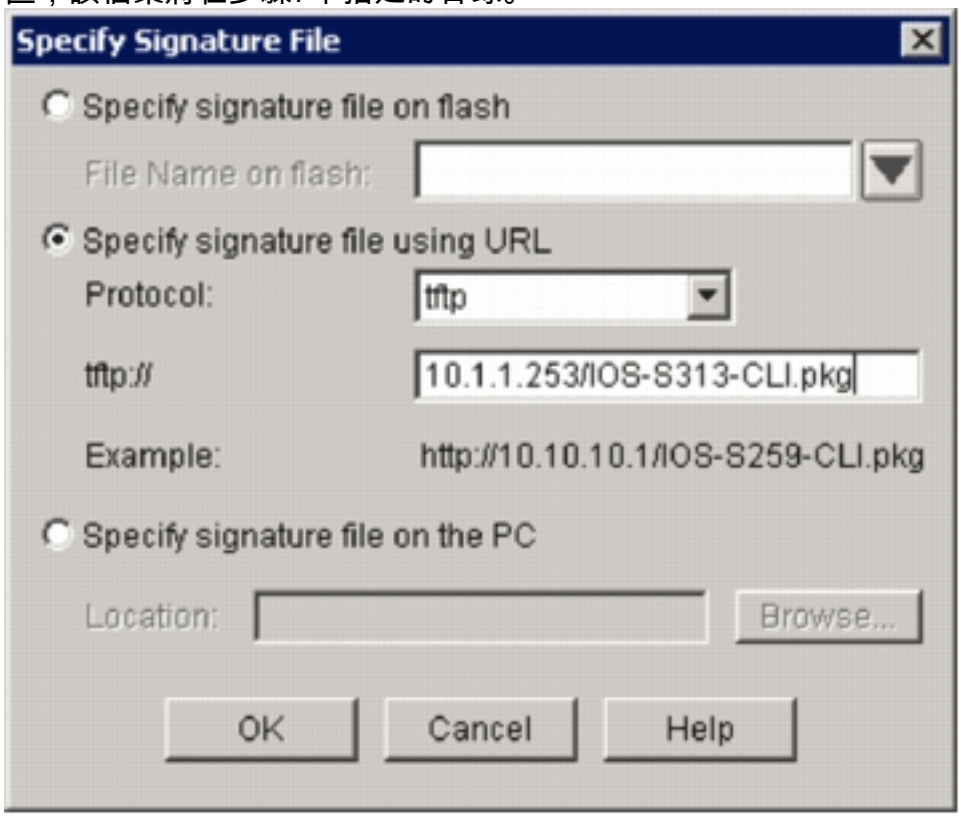
16. 按「**Next**」（下一步）。



17. 在Selected Interfaces視窗中，選擇將應用IOS IPS的介面和方向，然後按一下**Next**繼續。



18. 在「簽名檔案和公鑰」視窗的「簽名檔案」區域中，按一下**Specify the signature file you want to use with IOS IPS**單選按鈕，然後按一下**Signature File**按鈕(..)以指定簽名包檔案的位置，該檔案將在步驟7中指定的目錄。

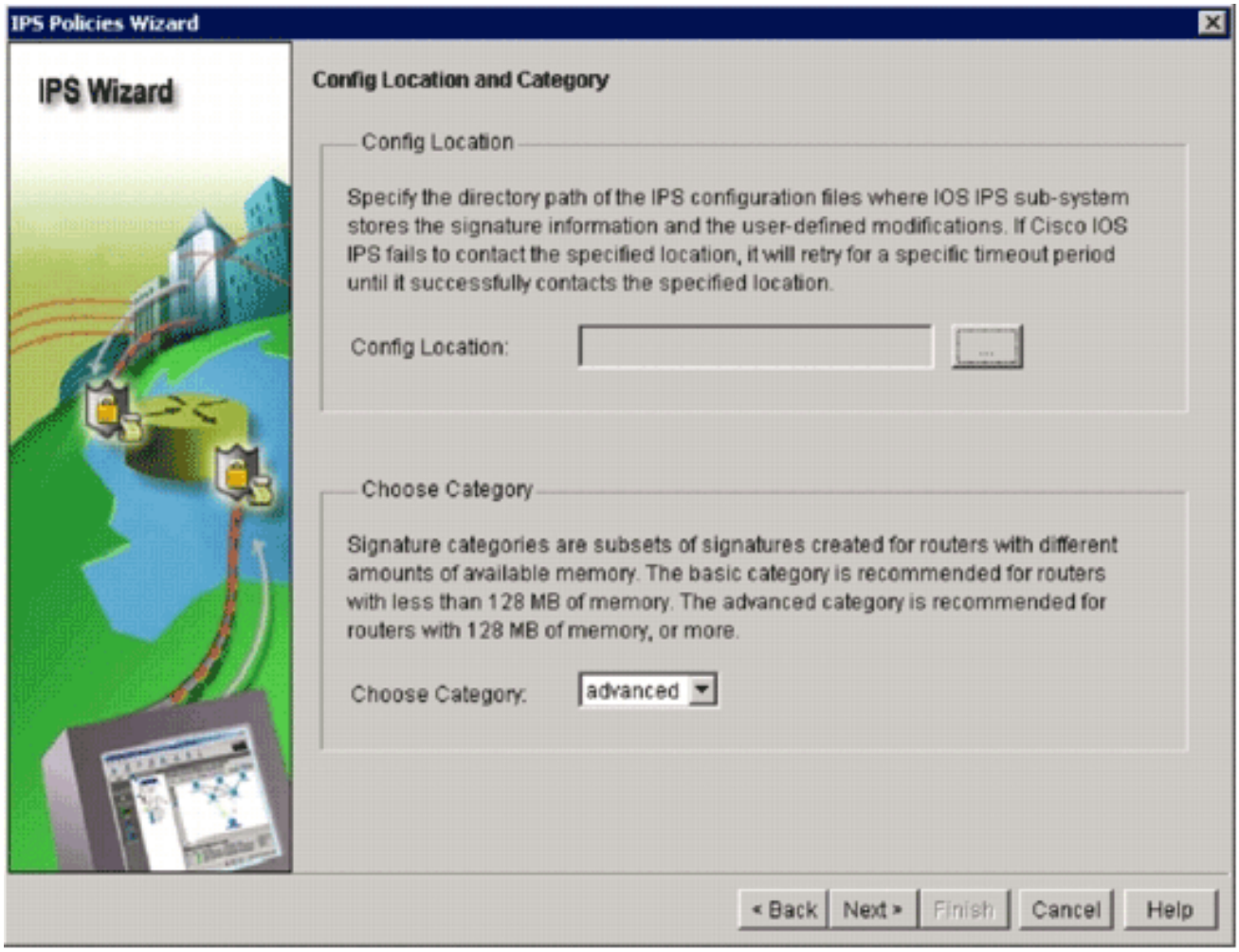


19. 按一下**Specify signature file using URL**單選按鈕，然後從Protocol下拉選單中選擇協定。**注意：**此示例使用TFTP將簽名軟體包下載到路由器。
20. 輸入簽名檔案的URL，然後按一下**OK**。
21. 在「簽名檔案和公鑰」視窗的「配置公鑰」區域中，在「名稱」欄位中輸入**realm-cisco.pub**，然後複製此公鑰並將其貼上到「金鑰」欄位中。

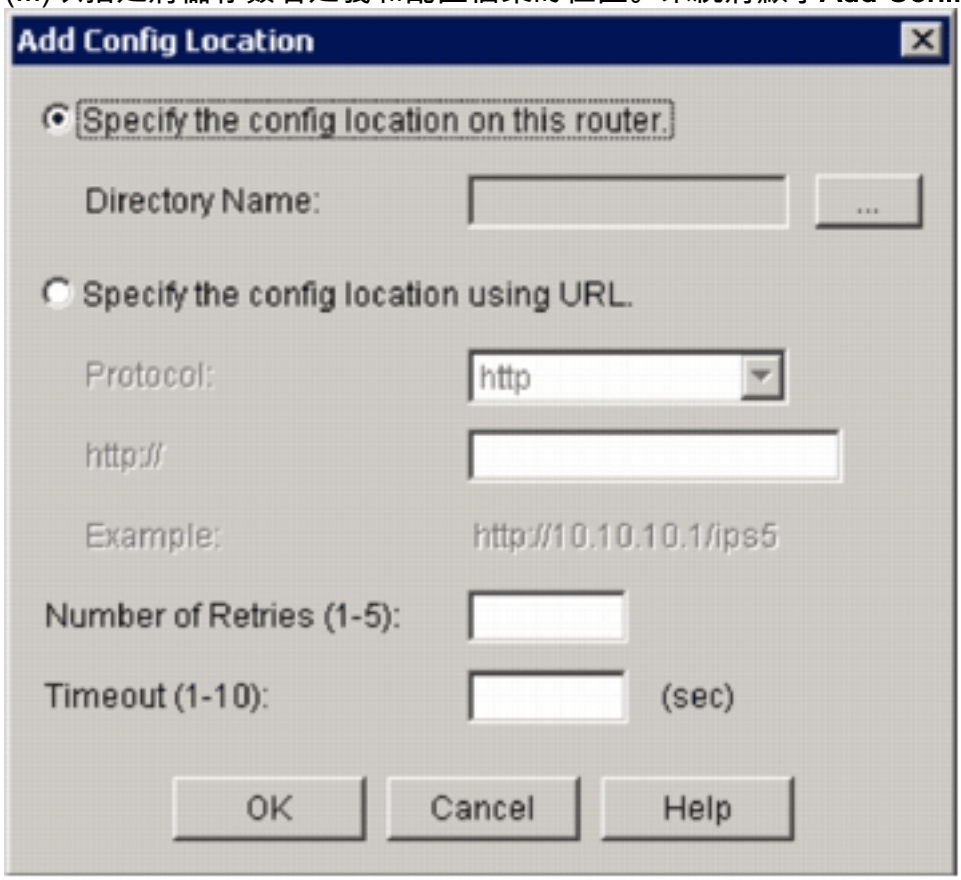
```
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101

00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16

17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128

B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E

5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35

FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85

50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36

006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE

2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3

F3020301 0001
```

附註： 此公鑰可從以下網址下載：Cisco.com:http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup(僅供註冊客戶)。

22. 按一下**下一步**繼續。



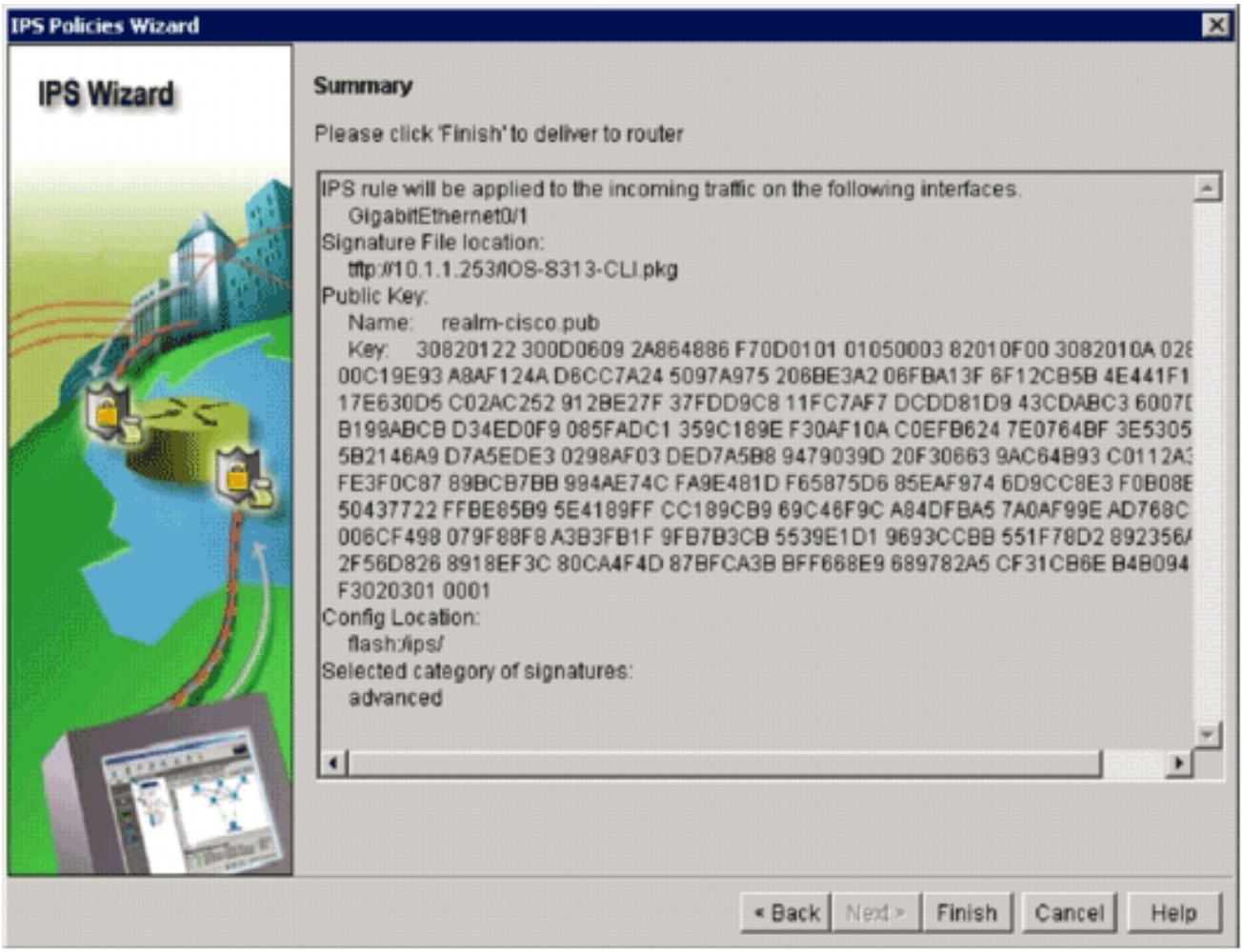
23. 在Config Location and Category（配置位置和類別）視窗中，按一下**Config Location**按鈕(...)以指定將儲存簽名定義和配置檔案的位置。系統將顯示**Add Config Location**對話方塊。



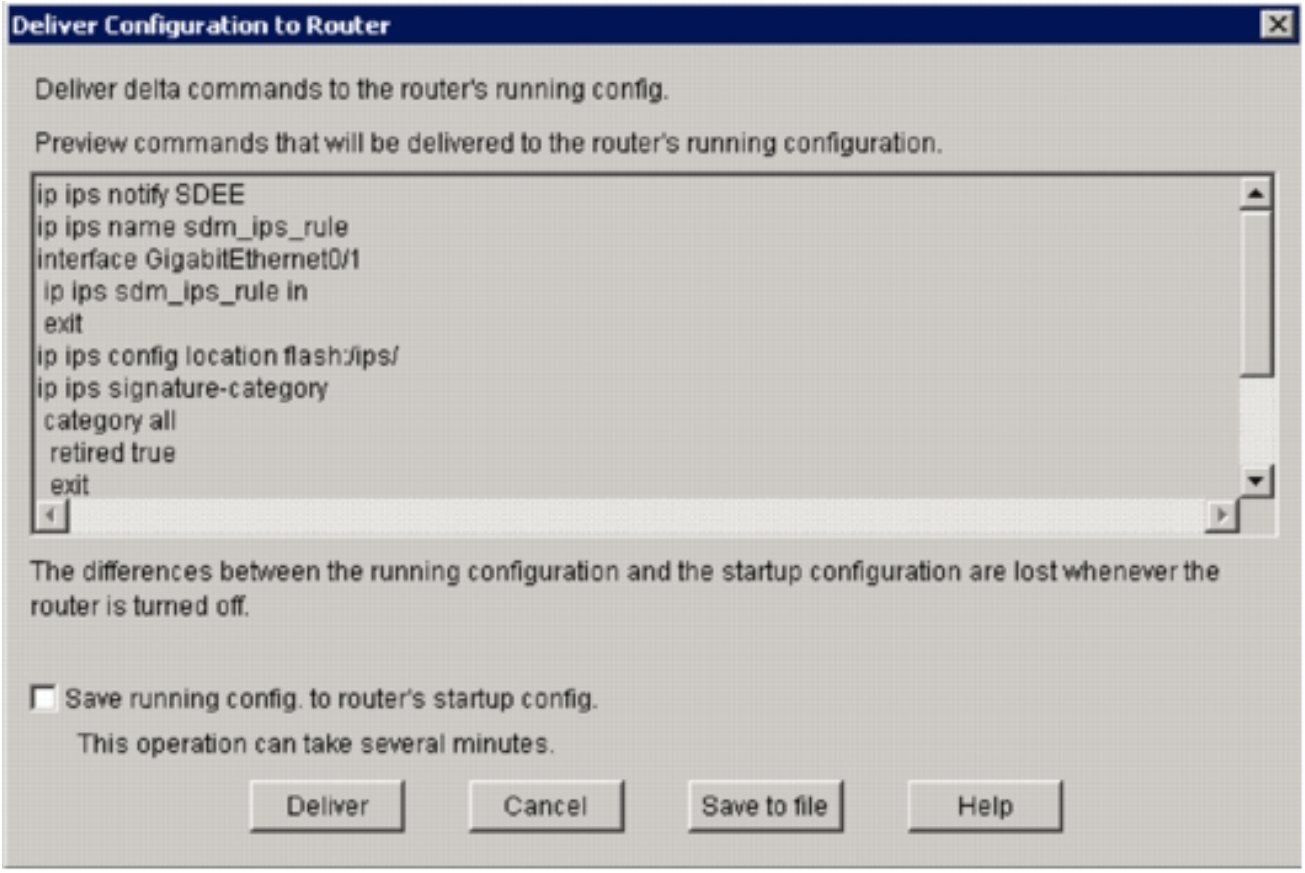
24. 在Add Config Location對話方塊中，按一下**Specify the config location on this router**單選按鈕，然後按一下**Directory Name**按鈕(...)以定位配置檔案。出現「Choose Folder（選擇資料

夾）」對話方塊，允許您在路由器快閃記憶體上選擇現有目錄或建立新目錄，以儲存簽名定義和配置檔案。

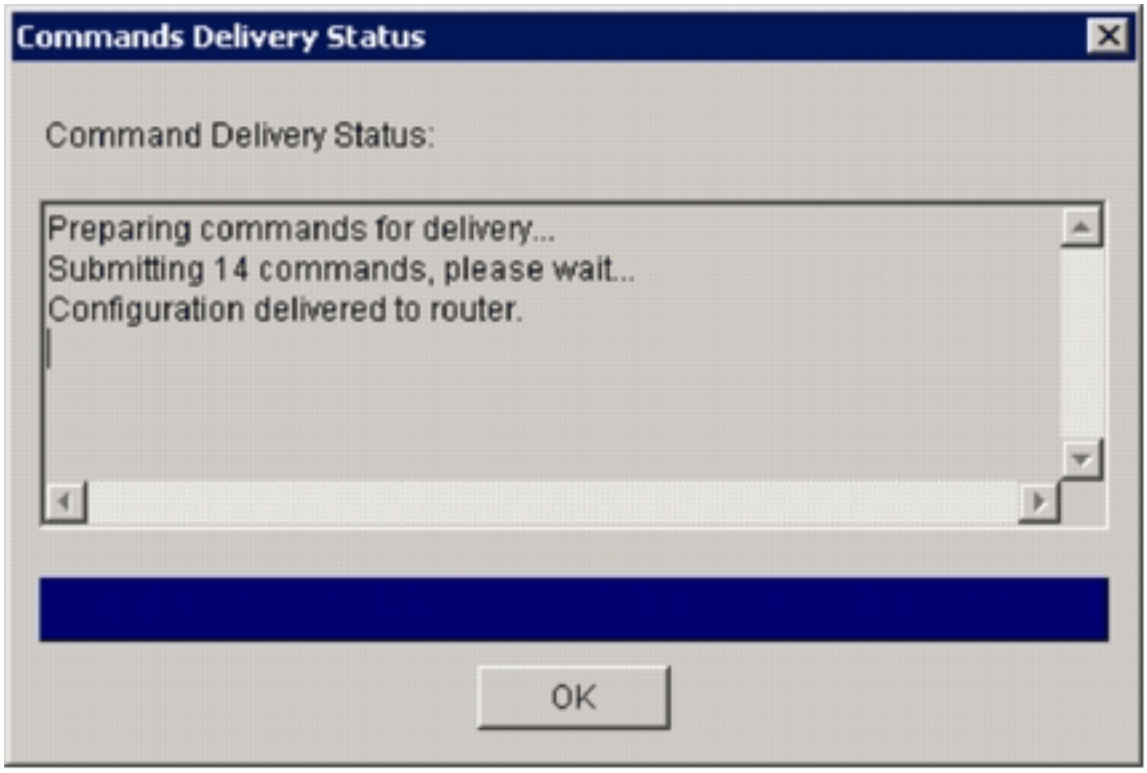
25. 如果要建立新目錄，請按一下對話方塊頂部的**New Folder**。
26. 選擇目錄後，按一下**OK**以應用更改，然後按一下**OK**以關閉Add Config Location對話方塊。
27. 在「IPS策略嚮導」對話方塊中，根據路由器上安裝的記憶體量選擇特徵碼類別。在SDM中可以選擇兩種簽名類別：基本和高級。如果路由器已安裝128MB DRAM，思科建議您選擇「Basic」類別以避免發生記憶體分配故障。如果路由器安裝了256MB或更多DRAM，您可以選擇任一類別。
28. 選擇要使用的類別後，按一下**下一步**以繼續進入摘要頁面。摘要頁面提供有關IOS IPS初始配置任務的簡要說明。



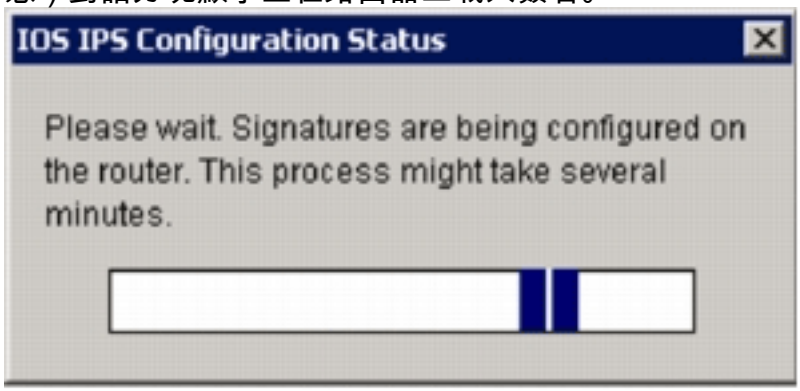
29. 在摘要頁面上按一下**Finish**，將配置和特徵碼包傳送到路由器。如果在SDM的「首選項」設定中啟用了「預覽命令」選項，則SDM會顯示「將配置傳送到路由器」對話方塊，其中顯示了SDM傳送到路由器的CLI命令的摘要。



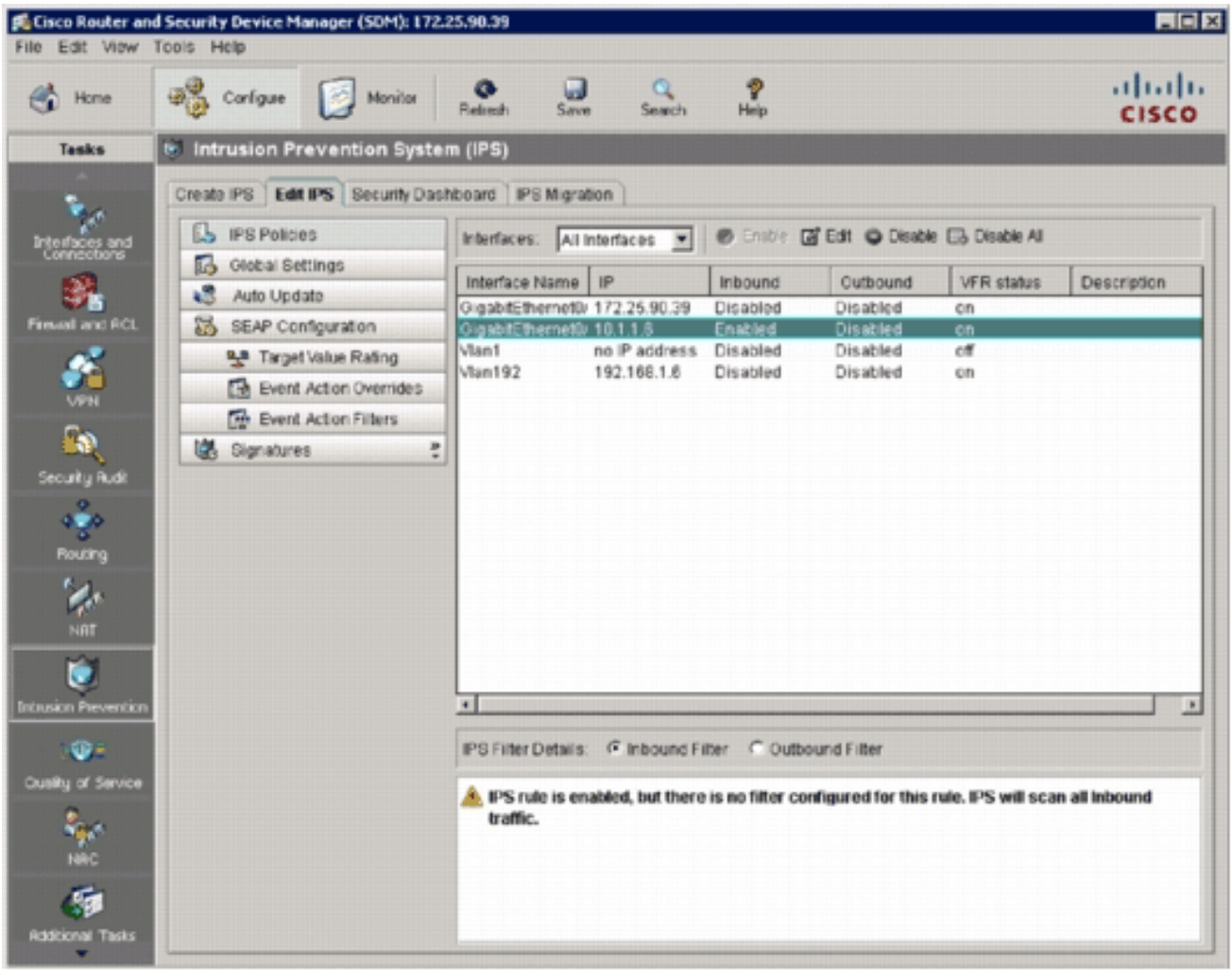
30. 按一下「**Deliver**」以繼續。命令傳送狀態對話方塊顯示命令傳送狀態。



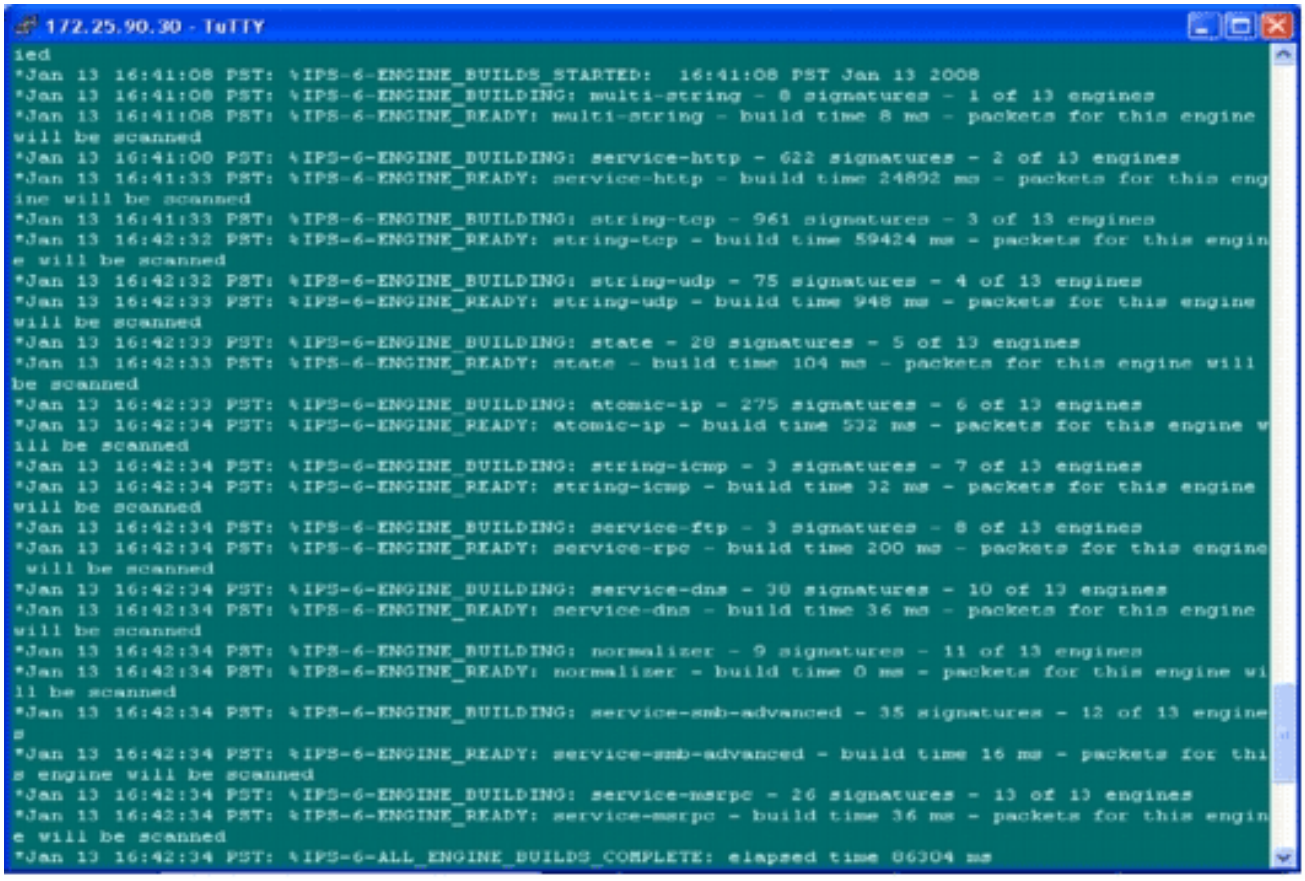
31. 將命令傳送到路由器時，按一下**OK**以繼續。IOS IPS Configuration Status（IOS IPS配置狀態）對話方塊顯示正在路由器上載入簽名。



32. 載入簽名後，SDM會顯示**Edit IPS**頁籤，其中包含當前配置。檢查啟用IOS IPS的介面和方向，以驗證配置。



路由器控制檯顯示已載入簽名。



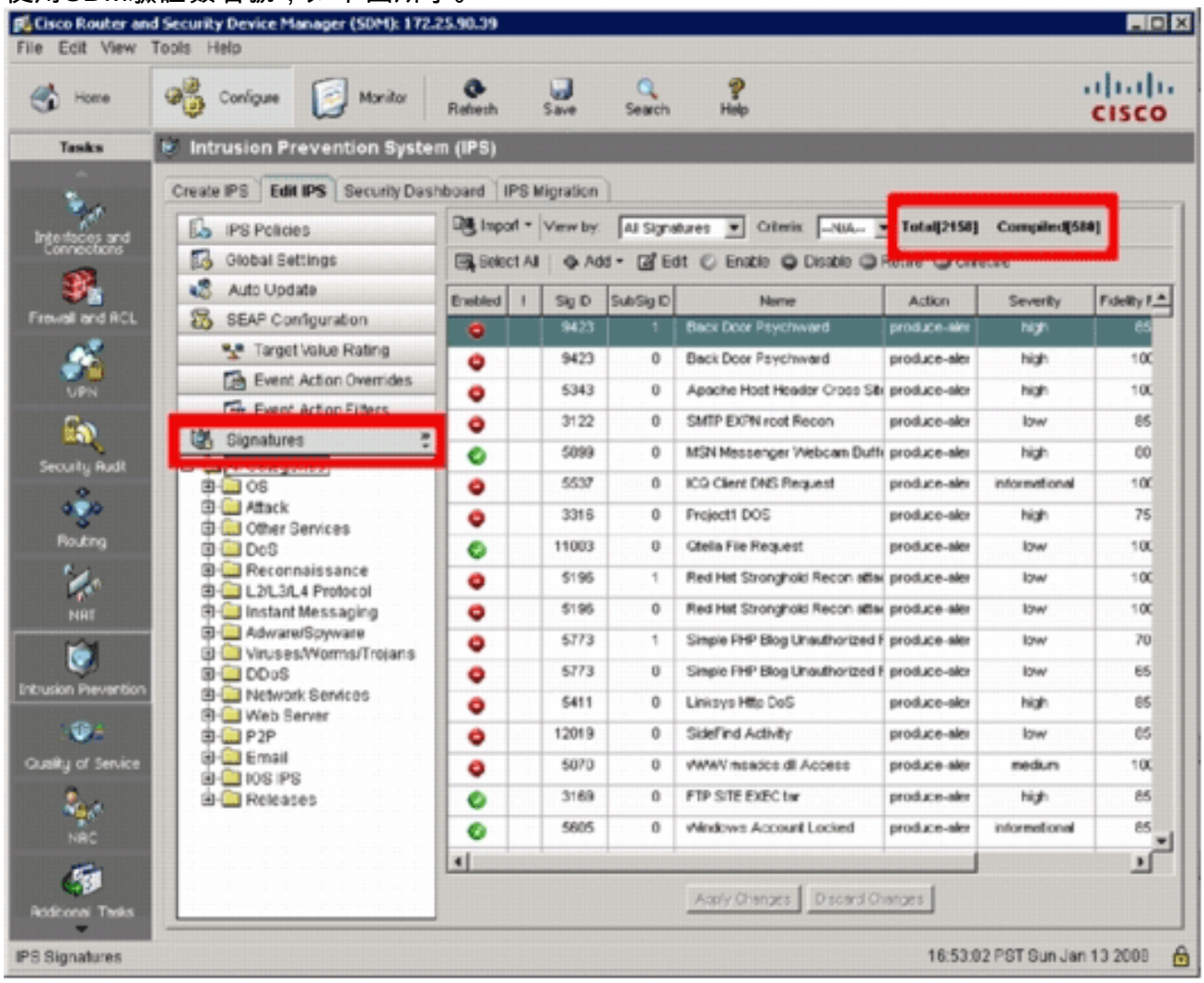
33. 使用**show ip signatures count**命令驗證是否已正確載入簽名。

```
router#show ip ips signatures count
```

```
Cisco SDF release version S313.0
Trend SDF release version V0.0
|
snip
|
Total Signatures: 2158
 Total Enabled Signatures: 829
 Total Retired Signatures: 1572
 Total Compiled Signatures: 580
 Total Signatures with invalid parameters: 6
        Total Obsoleted Signatures: 11
```

使用SDM 2.5完成對IOS IPS的初始調配。

34. 使用SDM驗證簽名號，如下圖所示。



相關資訊

- Cisco.com上的Cisco IOS IPS
- Cisco IOS IPS簽名包
- 用於SDM的Cisco IOS IPS簽名檔案
- 採用5.x簽名格式的Cisco IOS IPS入門
- Cisco IOS IPS配置指南
- Cisco IDS事件檢視器
- 技術支援與文件 - Cisco Systems