使用路由器和SDM配置Cisco IOS IPS

目录

简介

本文档介绍如何使用Cisco路由器和安全设备管理器(SDM)2.5版在12.4(15)T3及更高版本中配置Cisco IOS®入侵防御系统(IPS)。

SDM 2.5 中与 IOS IPS 有关的增强功能如下：

- 签名列表 GUI 中显示已编译签名总数
- SDM 签名文件（zip 文件格式；例如 sigv5-SDM-S307.zip）和 CLI 签名软件包（pkg 文件格式；例如 IOS-S313-CLI.pkg）可以通过一项操作同时下载
- 可以选择将下载的签名软件包自动推送至路由器

初始配置过程中涉及的任务包括：

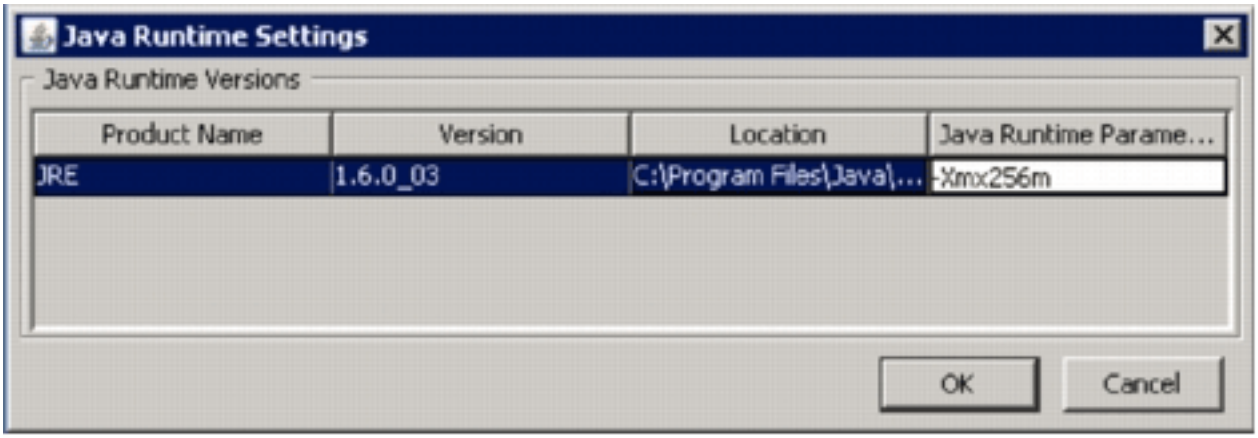
1. 下载并安装 SDM 2.5。
2. 使用 SDM 自动更新将 IOS IPS 签名软件包下载到本地 PC。
3. 启动 IPS 策略向导以配置 IOS IPS。
4. 验证是否已正确加载 IOS IPS 配置和签名

Cisco SDM 是一个基于 Web 的配置工具，它通过智能向导简化了路由器配置和安全配置，这些向导可帮助用户在无需了解命令行界面 (CLI) 的情况下轻松快速地完成 Cisco 路由器的部署、配置和监控。

SDM 2.5版可从Cisco.com下载，网址为http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm(仅限注册客户)。 以下地址提供发行版本注释：http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/software/release/notes/SDMr25.html

注意：Cisco SDM要求屏幕分辨率至少为1024 x 768。

注意：Cisco SDM要求Java内存堆大小不小于256MB才能配置IOS IPS。若要更改 Java 内存堆大小，请打开 Java 控制面板，单击 **Java 选项卡，单击“Java Applet Runtime Settings”下的“View”，然后在“Java Runtime Parameter”列中输入 -Xmx256m。**



先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS IPS 12.4(15)T3 及更高版本
- Cisco Router and Security Device Manager (SDM) 2.5 版

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。

规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

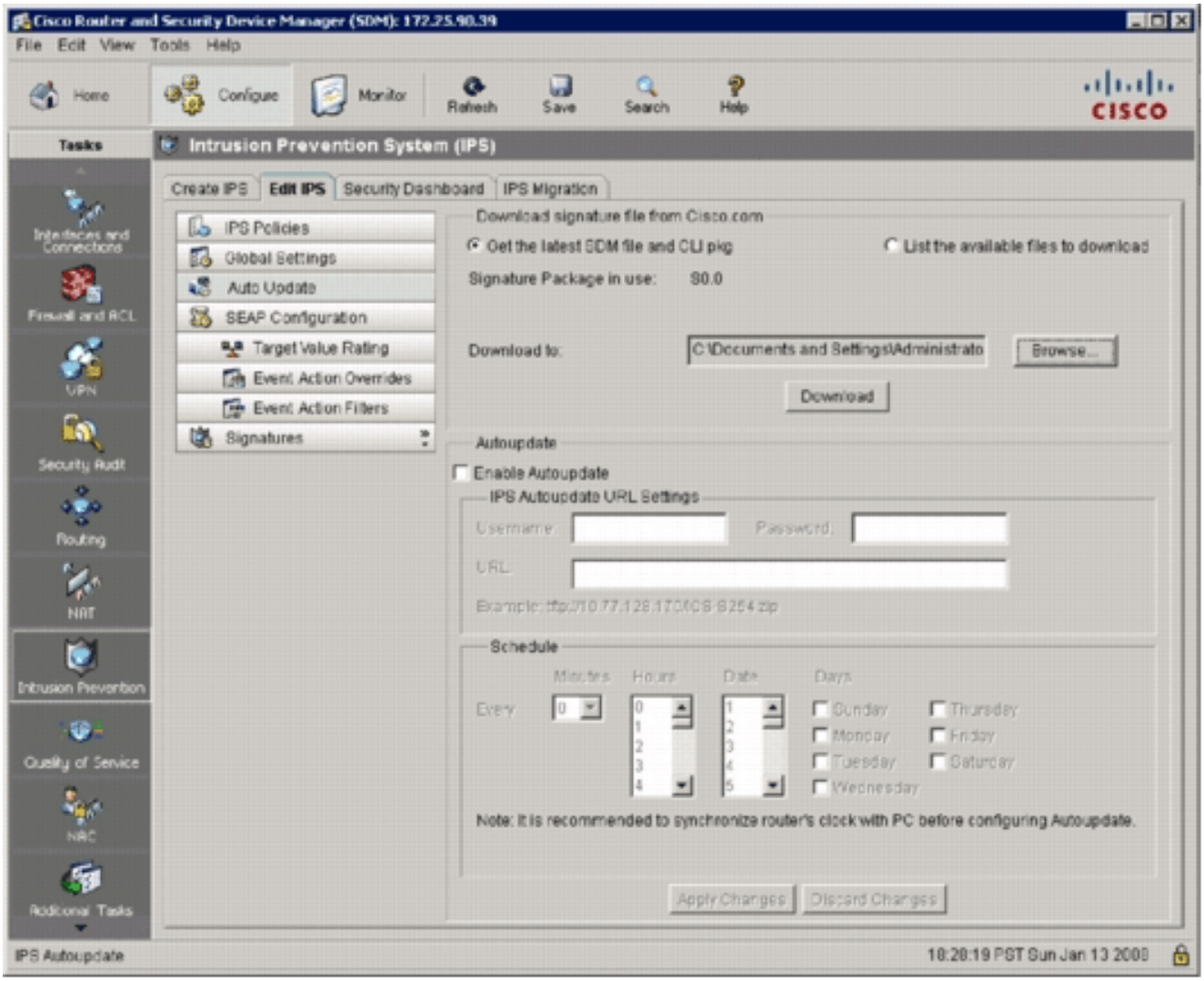
配置

注意：使用SDM调配IOS IPS时，打开控制台或Telnet会话到路由器（启用“term monitor”）以监控消息。

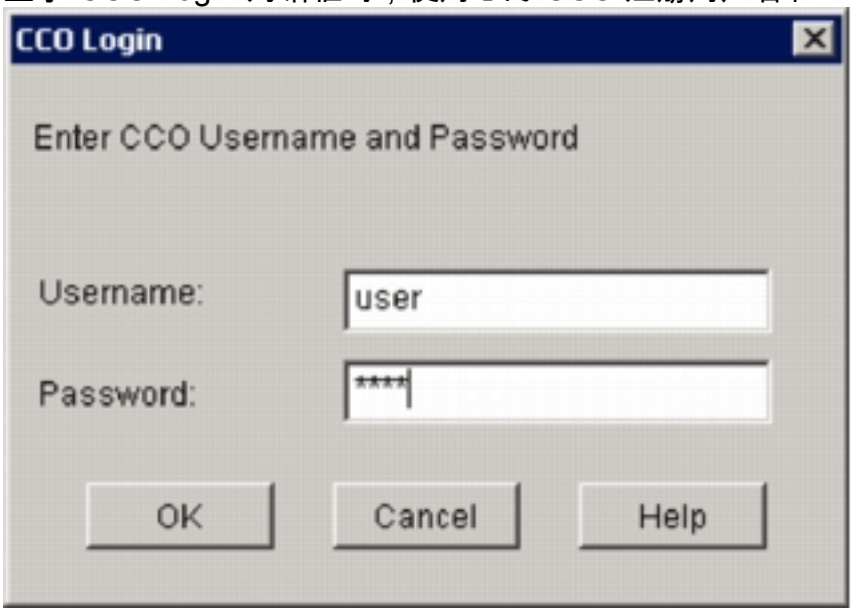
1. 从Cisco.com下载SDM 2.5，网址为http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm(仅限注册客户)，并将其安装在本地PC上。
2. 从本地 PC 运行 SDM 2.5。
3. 显示“IOS IPS Login”对话框时，输入您用于进行 SDM 到路由器的身份验证的用户名和口令。

4. 在 SDM 用户界面中单击 **Configure**，然后单击“Intrusion Prevention”。
5. 单击 **Edit IPS 选项卡。**
6. 如果未启用路由器的 SDEE 通知，请单击 **OK 以启用 SDEE 通知。**

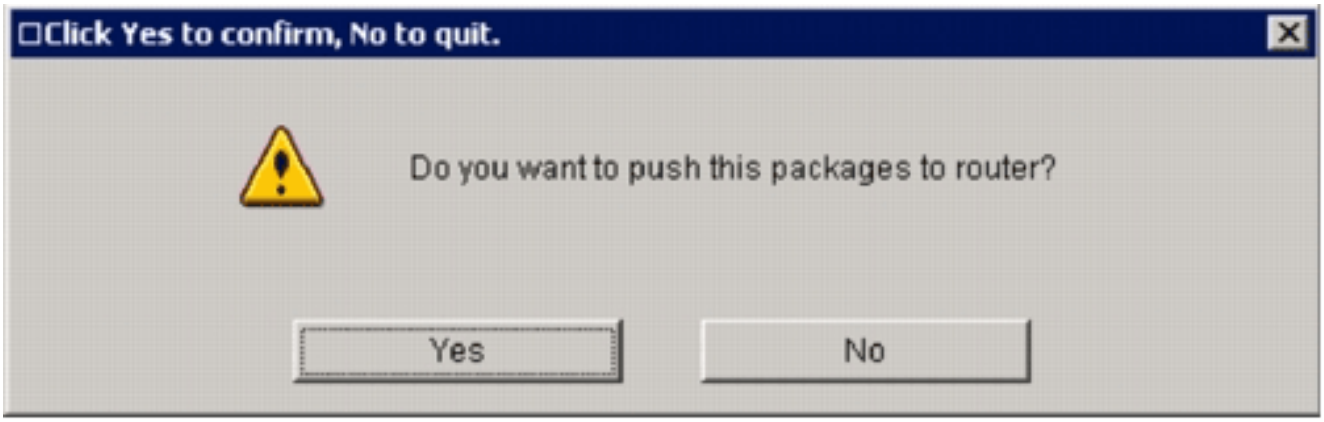
7. 在“Edit IPS”选项卡的“Download signature file from Cisco.com”区域中，单击 **Get the latest SDM file and CLI pkg 单选按钮，然后单击“Browse”以选择本地 PC 上要用于保存下载文件的目录。**可以选择 TFTP 或 FTP 服务器根目录，以后为路由器部署签名软件包时将使用此目录。
8. 单击 **Download。**



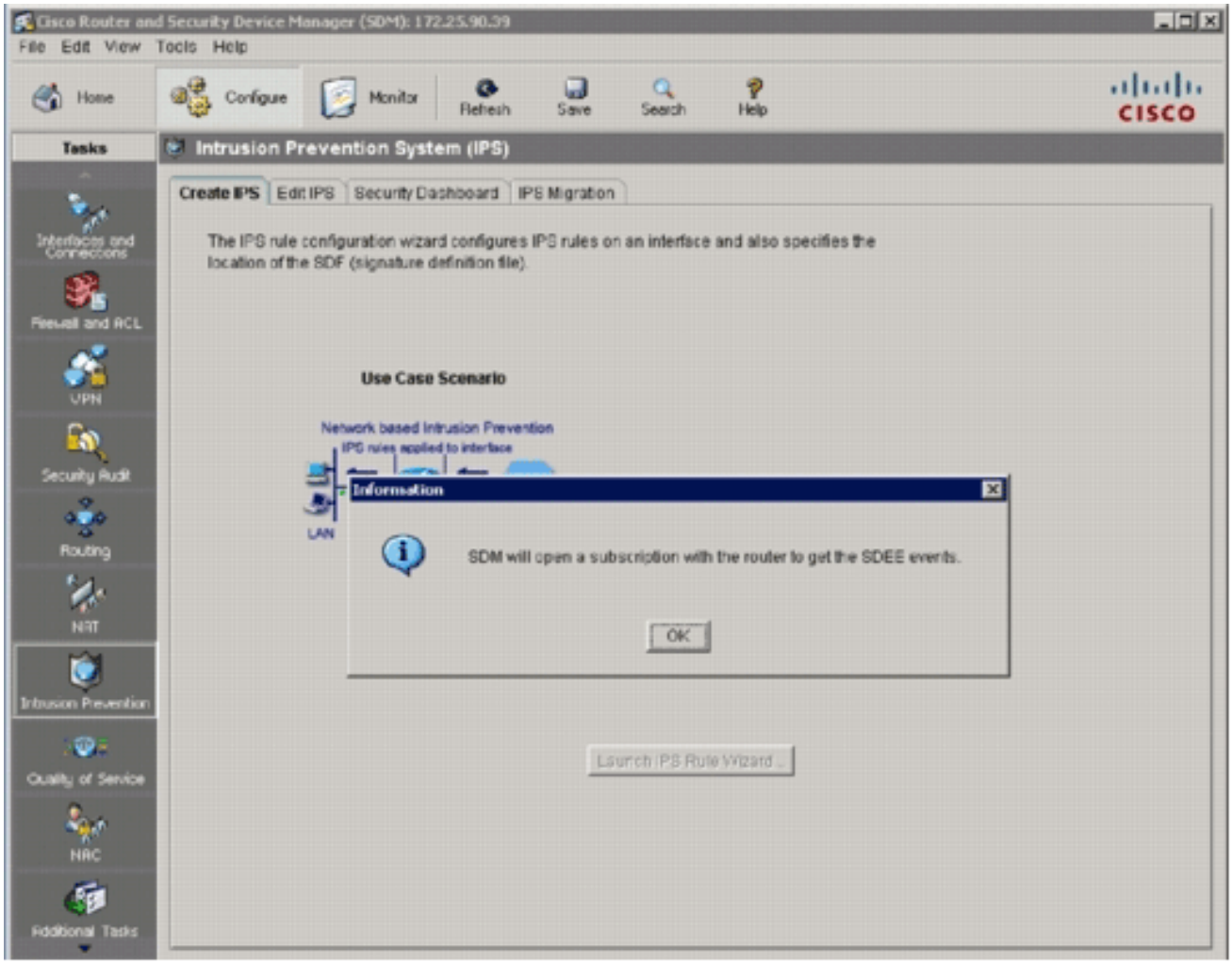
9. 显示“CCO Login”对话框时，使用您的 CCO 注册用户名和口令。



SDM 连接到 Cisco.com 并开始将 SDM 文件（例如 sigv5-SDM-S307.zip）和 CLI pkg 文件（例如 IOS-S313-CLI.pkg）下载到在步骤 7 中选择的目录。两个文件均下载完成后，SDM 会提示您将下载的签名软件包推送至路由器。

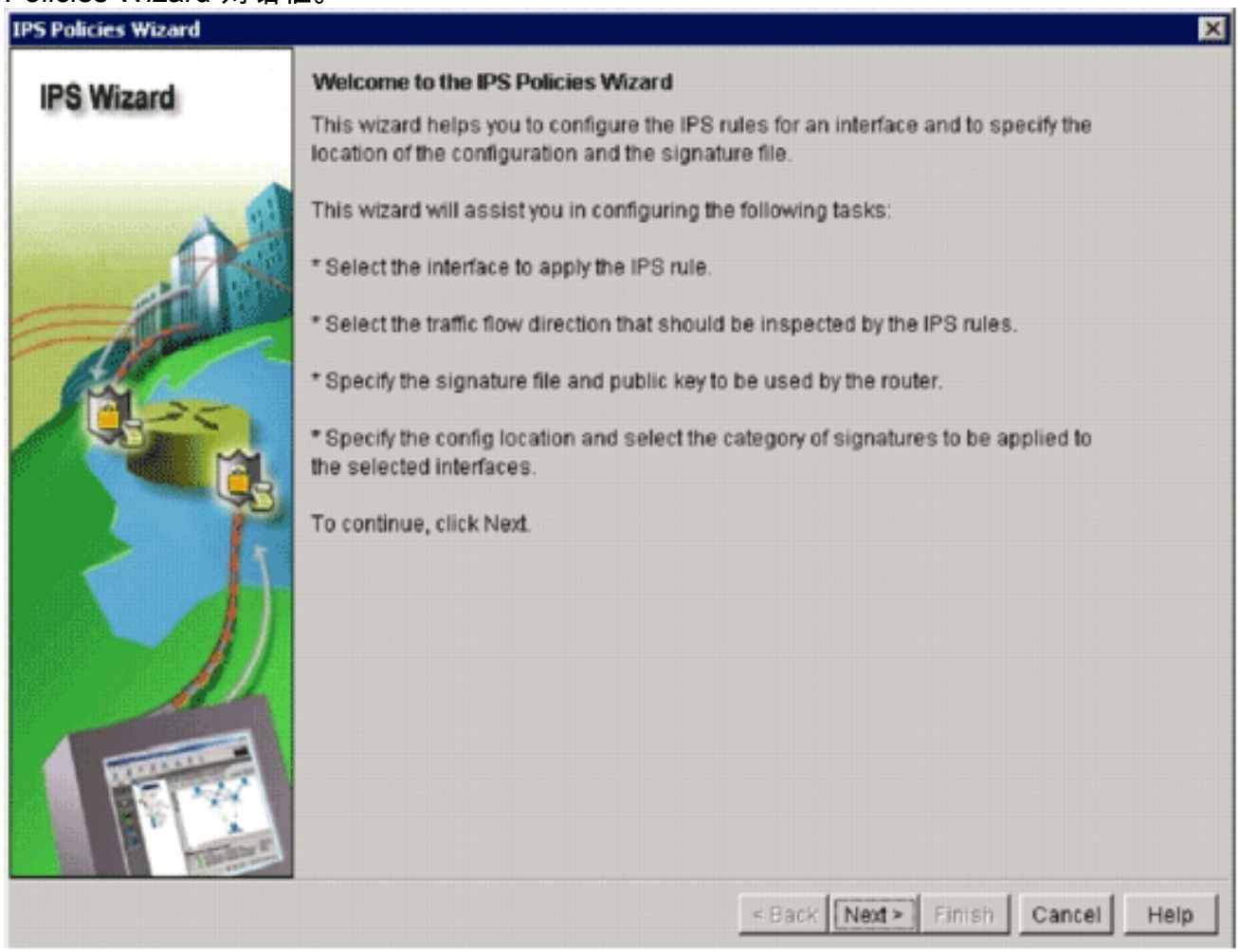


10. 由于尚未配置路由器上的 IOS IPS，因此单击 **No**。
11. 在 SDM 下载最新的 IOS CLI 签名软件包之后，单击 **Create IPS 选项卡以创建初始 IOS IPS 配置。**
12. 如果系统提示您将更改应用于路由器，请单击 **Apply Changes**。
13. 单击 **Launch IPS Rule Wizard**。此时显示一个对话框，提示您 SDM 需要向路由器建立 SDEE 订阅以接收警报。

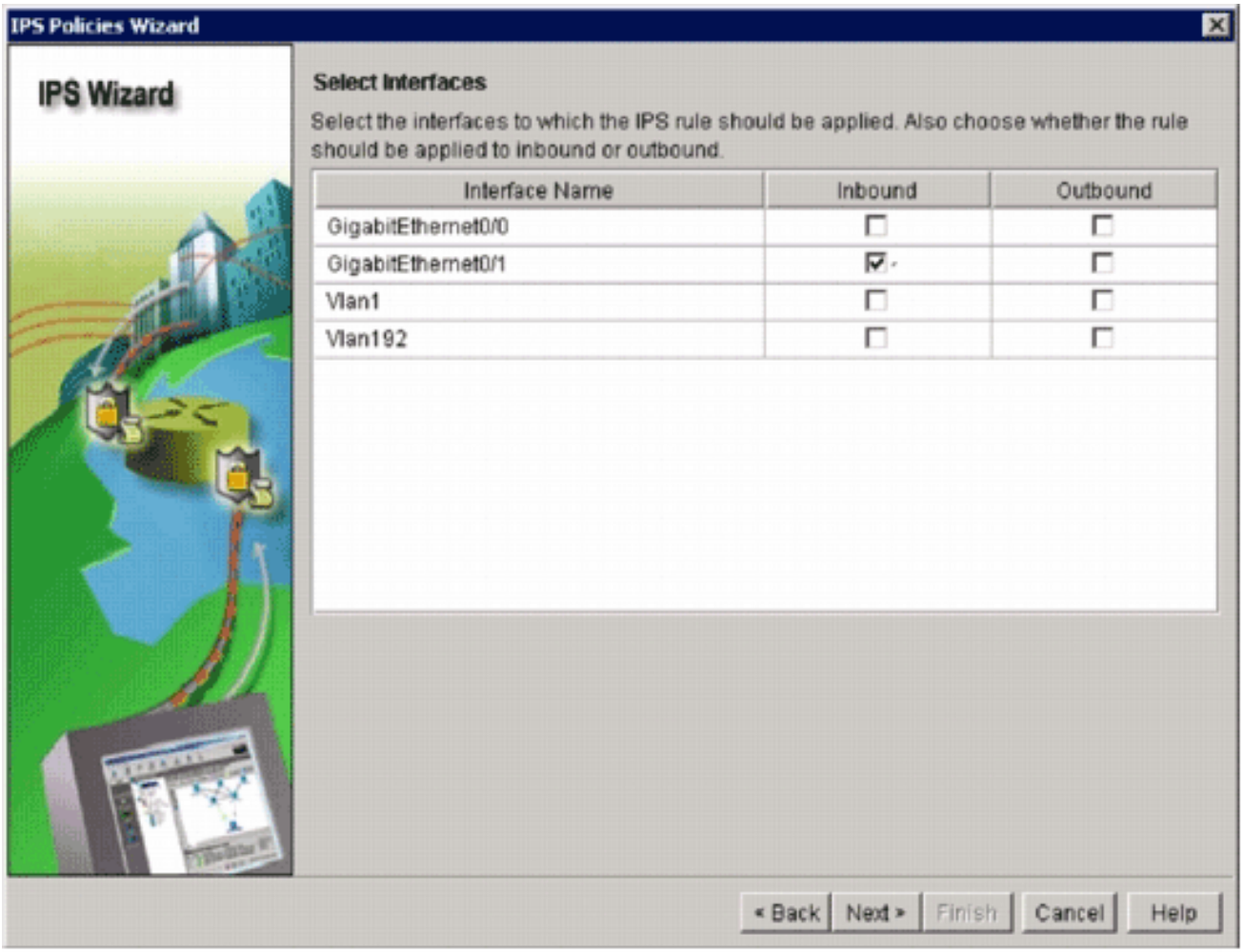


14. Click **OK**.此时显示“Authentication Required”对话框。

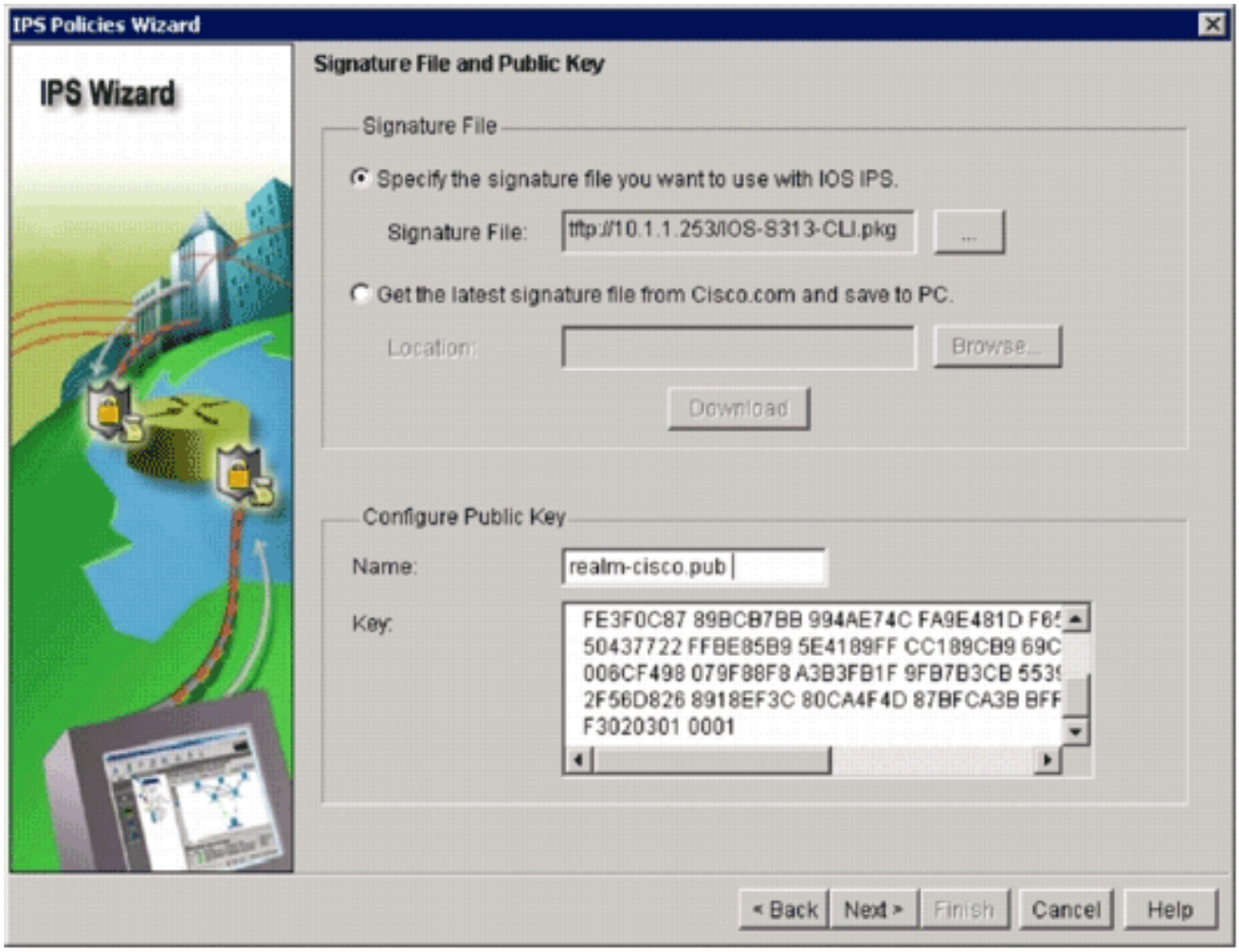
15. 输入您用于进行 SDM 到路由器的身份验证的用户名和口令，然后单击 **OK**。此时显示“IPS Policies Wizard”对话框。



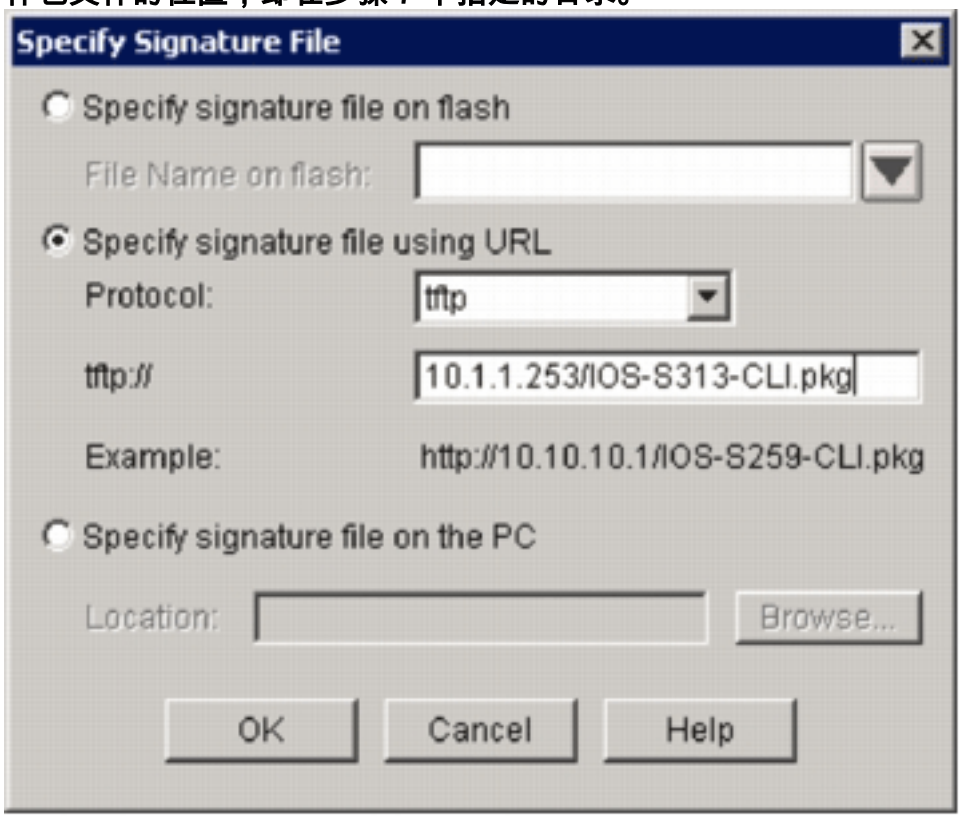
16. 单击 **Next**。



17. 在“Selected Interfaces”窗口中选择将要应用 IOS IPS 的接口和方向，然后单击 **Next to 继续操作。**



18. 在“Signature File and Public Key”窗口的“Signature File”区域中，单击 **Specify the signature file you want to use with IOS IPS** 单选按钮，然后单击**“Signature File”按钮 (...) 以指定签名软件包文件的位置，即在步骤 7 中指定的目录。**

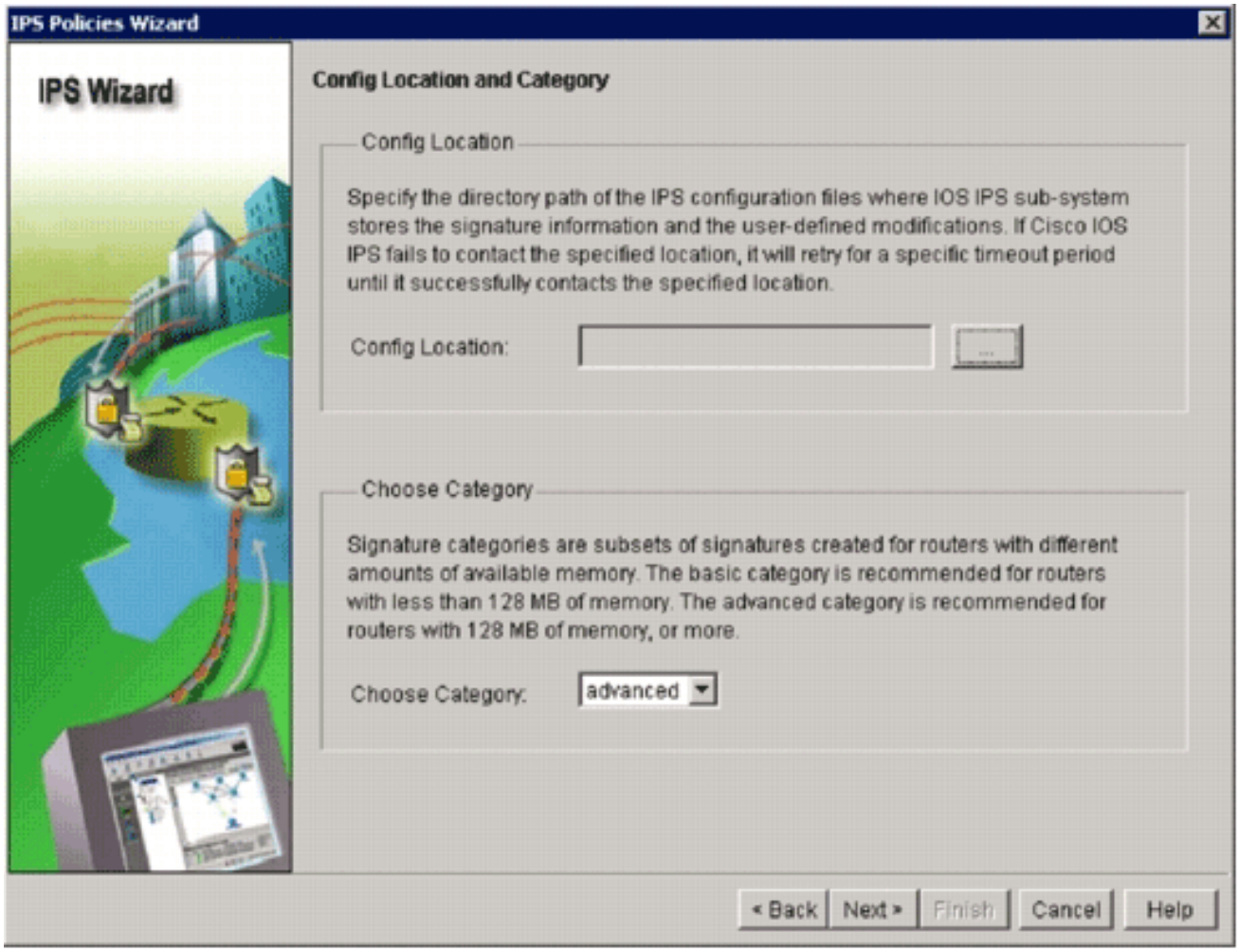


19. 单击 **Specify signature file using URL 单选按钮，然后从“Protocol”下拉列表中选择一个协议。注意：**本示例使用TFTP将签名包下载到路由器。

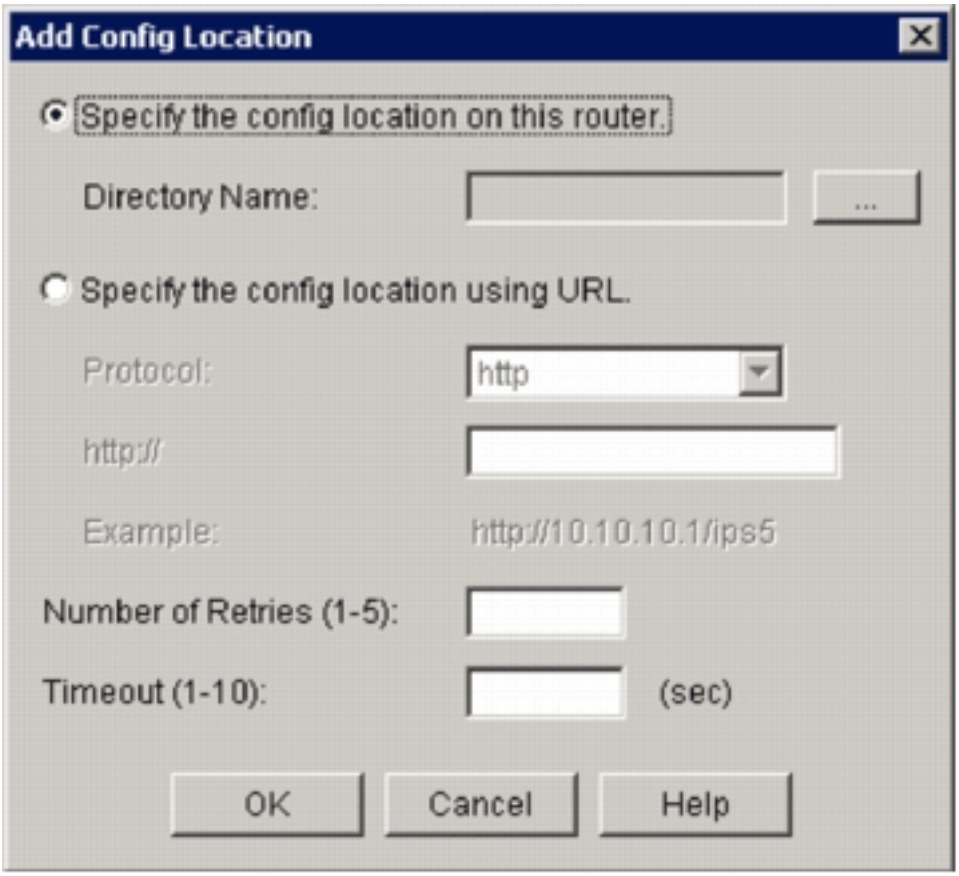
20. 输入签名文件的 URL，然后单击 **OK**。
21. 在“Signature File and Public Key”窗口的“Configure Public Key”区域中，在“Name”字段中输入 **realm-cisco.pub，然后复制此公钥并将其粘贴到“Key”字段中。**

```
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
```

注意： 可以从 Cisco.com 下载此公钥，网址为：http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup（仅限注册用户）。
22. 单击“下一步”继续。



23. 在“Config Location and Category”窗口中，单击 **Config Location 按钮 (...) 以指定将用于存储签名定义和配置文件的位置。**此时显示 **Add Config Location 对话框。**

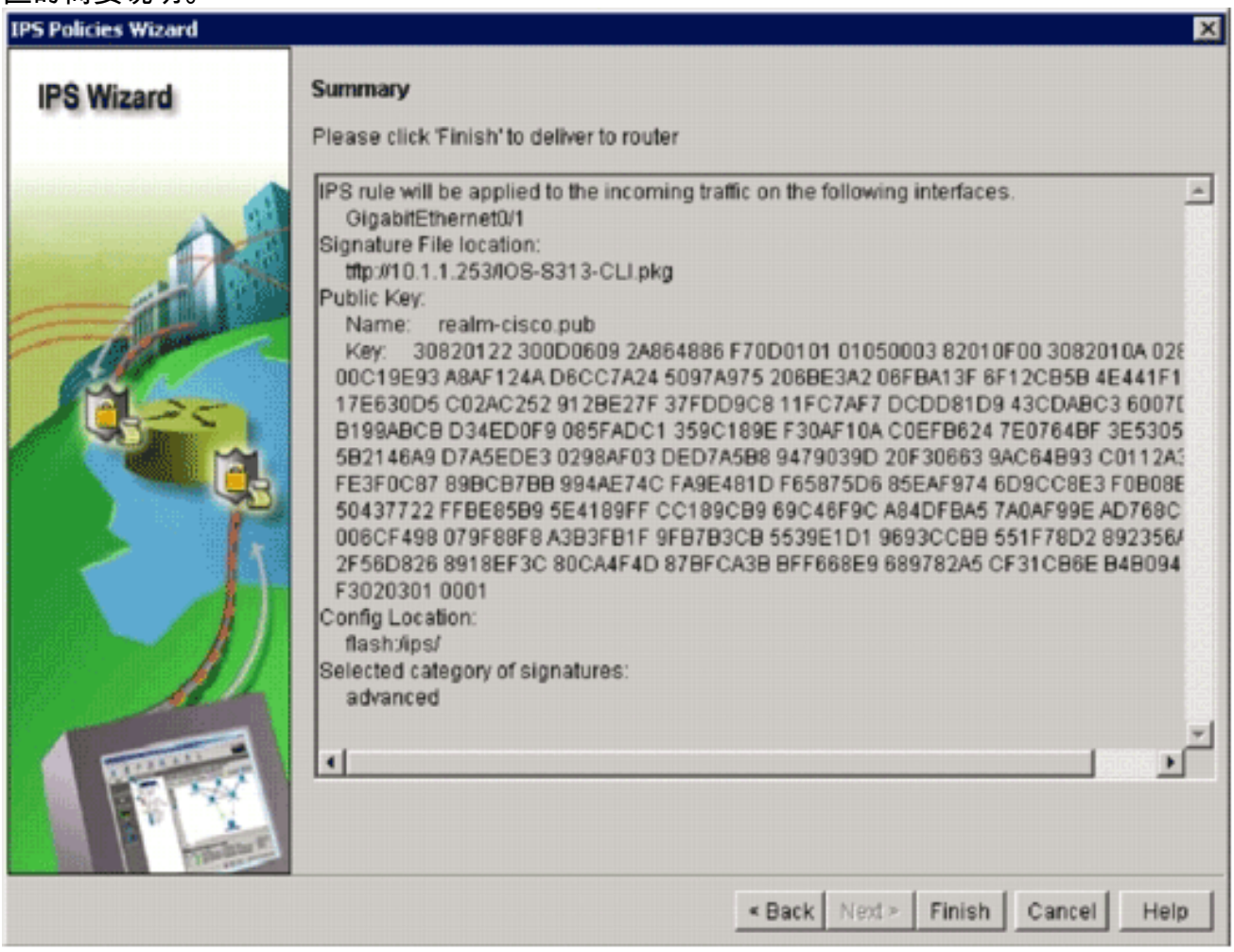


24. 在“Add Config Location”对话框中单击 **Specify the config location on this router 单选按钮，然后单击“Directory Name”按钮 (...) 以查找配置文件。**此时显示“Choose Folder”对话框，允许您在路由器闪存中选择一个现有目录或创建一个新目录，用于存储签名定义和配置文件。

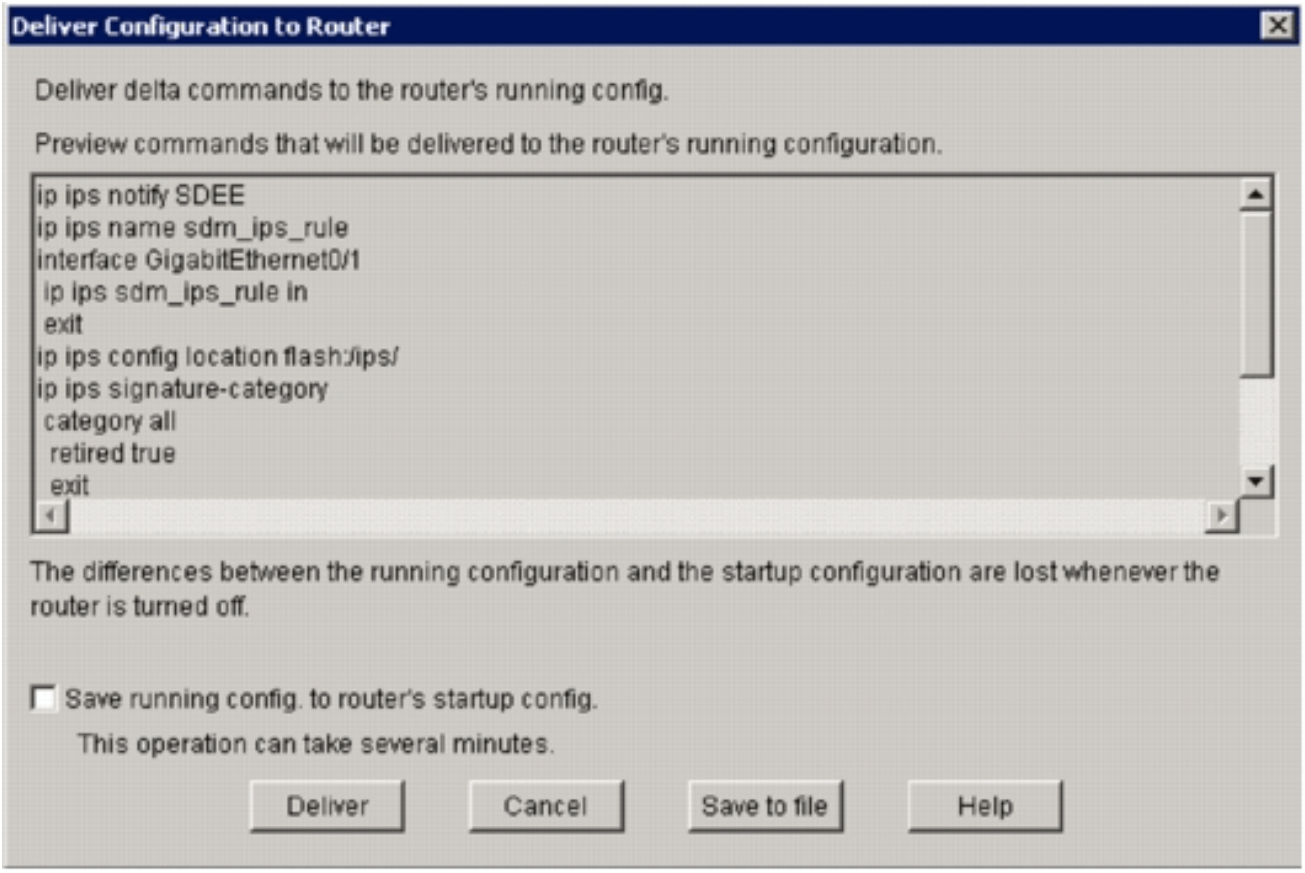
25. 若要创建新目录，请单击位于对话框顶部的 **New Folder。**
26. 选择目录后，单击 **OK 以应用更改，然后单击“OK”关闭“Add Config Location”对话框。**
27. 在“IPS Policies Wizard”对话框中，根据路由器中安装的内存量选择签名类别。在 SDM 中，有以下两种签名类别可供选择：“Basic”和“Advanced”。如果路由器安装的是 128MB DRAM，Cisco 建议您选择“Basic”类别以避免发生内存分配故障。如果路由器安装了 256MB

或更大的 DRAM，则可以选择任何一种类别。

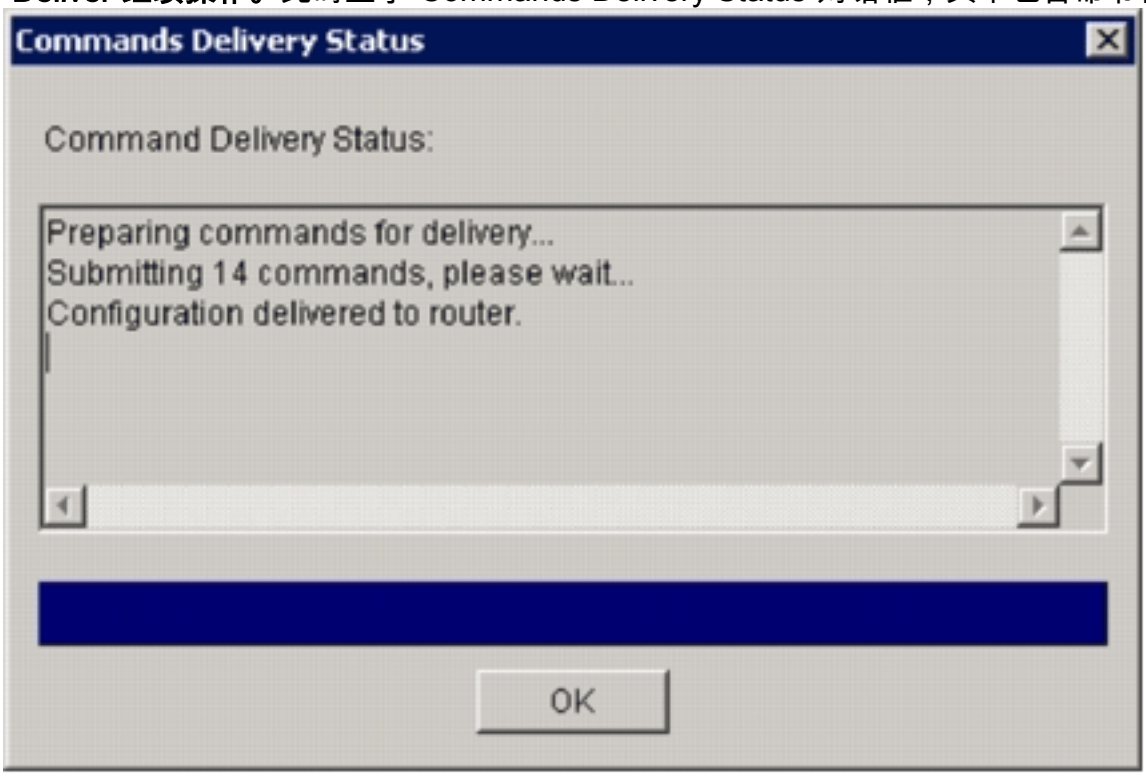
28. 选择要使用的类别后，单击 **Next 继续进入摘要页。**摘要页提供了有关任务 IOS IPS 初始配置的简要说明。



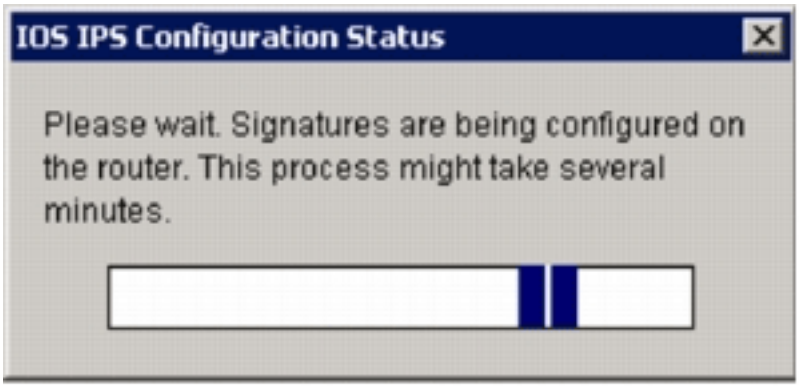
29. 单击摘要页上的 **Finish 将配置和签名软件包传送到路由器。**如果 SDM 中“Preferences”设置的预览命令选项已启用，SDM 将显示“Deliver Configuration to Router”对话框，其中包含 SDM 传送到路由器的 CLI 命令的摘要。



30. 单击 **Deliver 继续操作。**此时显示“Commands Delivery Status”对话框，其中包含命令传送状态。

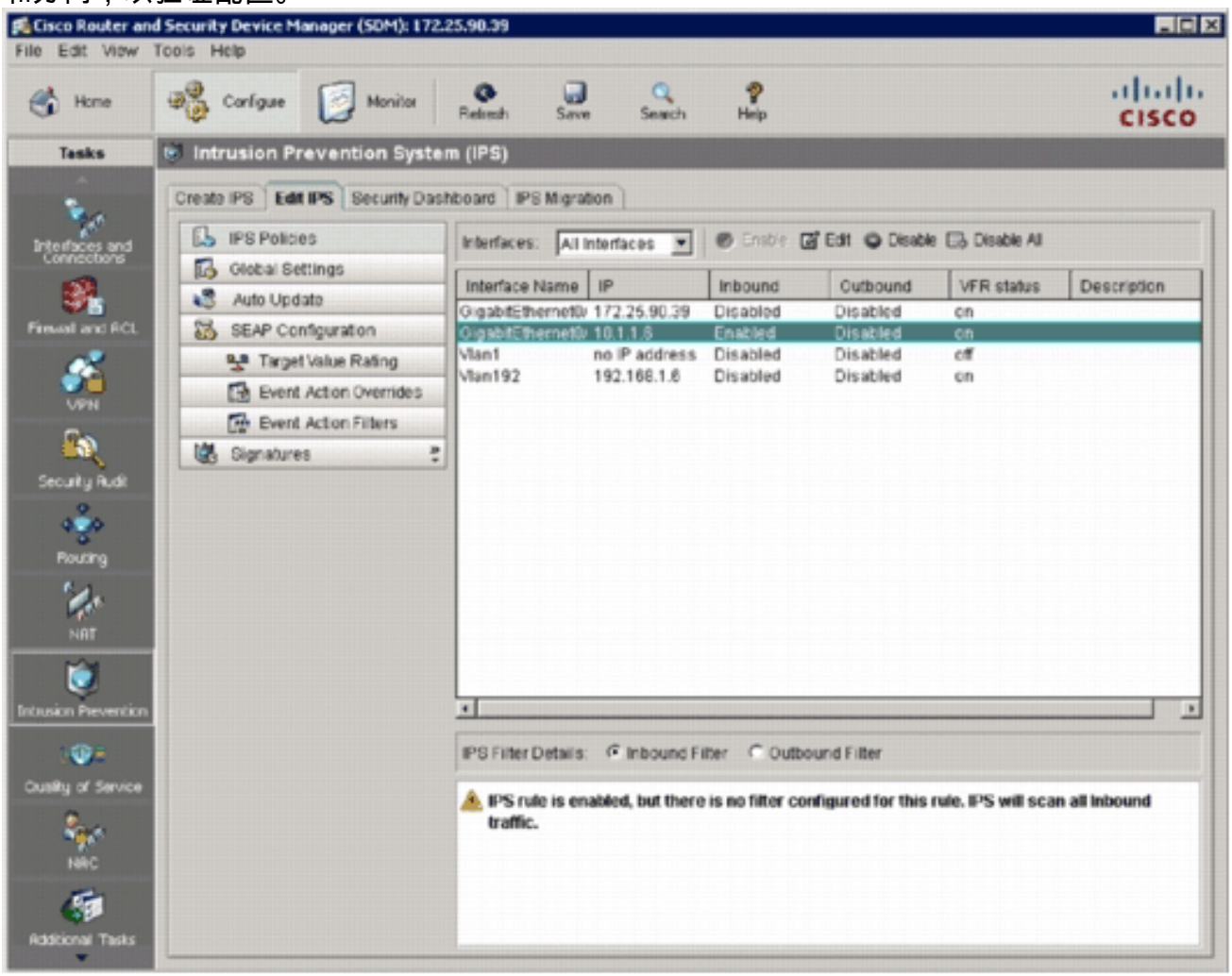


31. 命令传送到路由器后，单击 **OK 继续操作。**此时“IOS IPS Configuration Status”对话框显示正

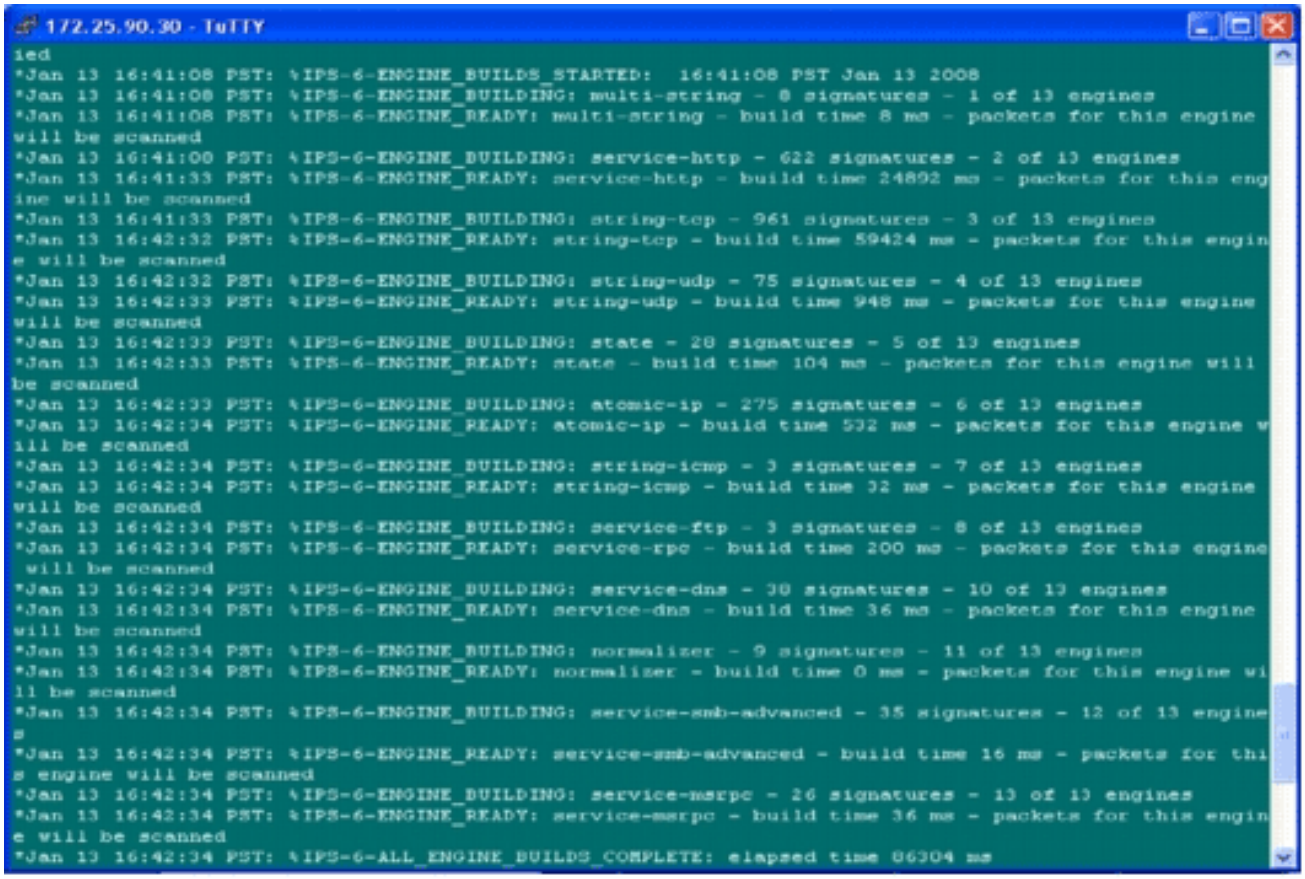


在路由器上加载签名。

32. 签名加载完毕时，SDM 将显示包含当前配置的 **Edit IPS 选项卡。**检查启用 IOS IPS 的接口和方向，以验证配置。



此时路由器控制台显示签名已加载。

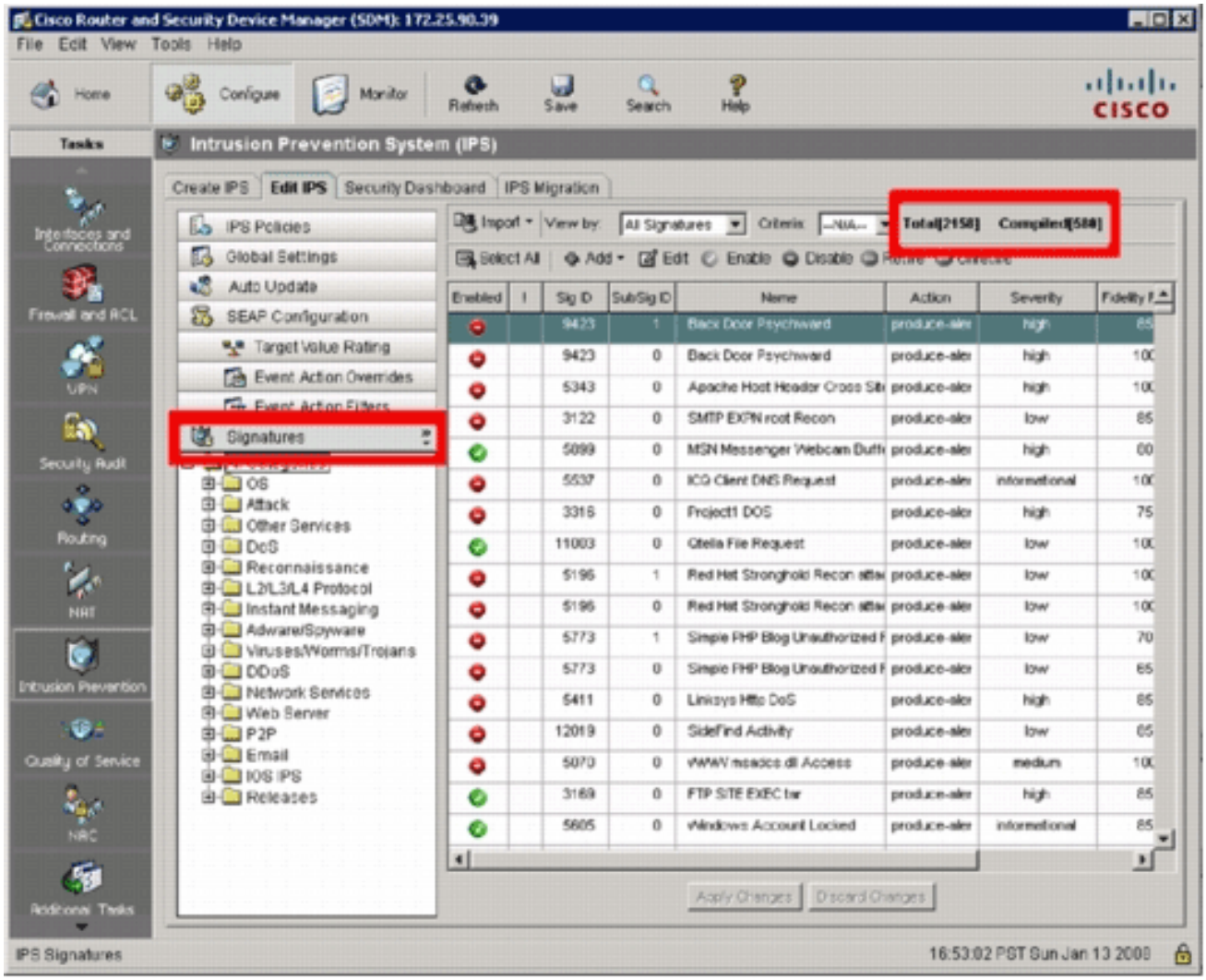


33. 使用 **show ip ips signatures count 命令验证签名是否已正确加载。**

```
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
```

此时使用 SDM 2.5 进行的 IOS IPS 初始配置已完成。

34. 使用 SDM 验证签名数，如下图所示。



相关信息

- Cisco.com 上关于 Cisco IOS IPS 的内容
- Cisco IOS IPS 签名软件包
- 用于 SDM 的 Cisco IOS IPS 签名文件
- 采用 5.x 签名格式的 Cisco IOS IPS 入门
- Cisco IOS IPS 配置指南
- Cisco IDS 事件查看器
- 技术支持和文档 - Cisco Systems