在Cisco IOS IPS中配置安全管理器

目录

简介

思科安全管理器是思科安全管理套件的一部分，该套件为思科自防御网络提供全面的策略管理和实施。思科安全管理器是用于管理安全的行业领先的企业级应用。Cisco Security Manager可跨思科路由器、安全设备和安全服务模块处理防火墙、VPN和入侵防御系统(IPS)安全服务的配置管理。

有关思科安全管理器功能和优势以及3.1版中的新功能的摘要，请参阅思科安全管理器3.1产品手册，网址为
http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6498/product_data_sheet0900aecd8062bf6e.html。您可以从Cisco.com下载Cisco Security Manager 3.1，网址为
http://www.cisco.com/cgi-bin/tablebuild.pl/csm-app(仅限注册客户)。

本文档介绍如何使用Cisco Security Manager 3.1来执行IOS IPS的初始配置。对于已配置IOS IPS的路由器，客户可以直接使用Cisco Security Manager 3.1来执行调配任务。

注意：Cisco Security Manager 3.1仅支持IOS 12.4(11)T2及更高版本的IOS映像，以便配置IOS IPS。

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：

- 思科安全管理器3.1
- 思科IOS 12.4(11)T2

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。
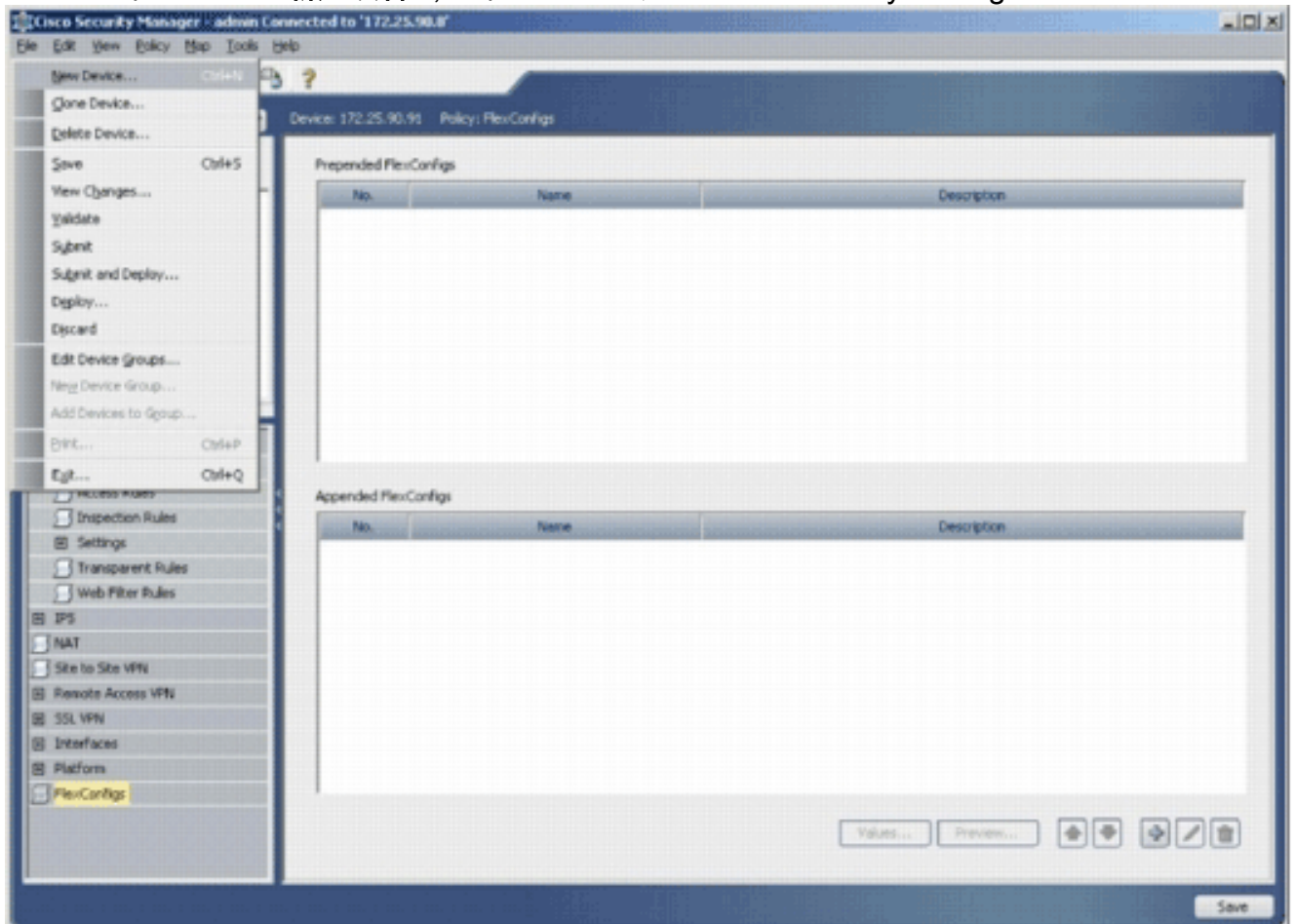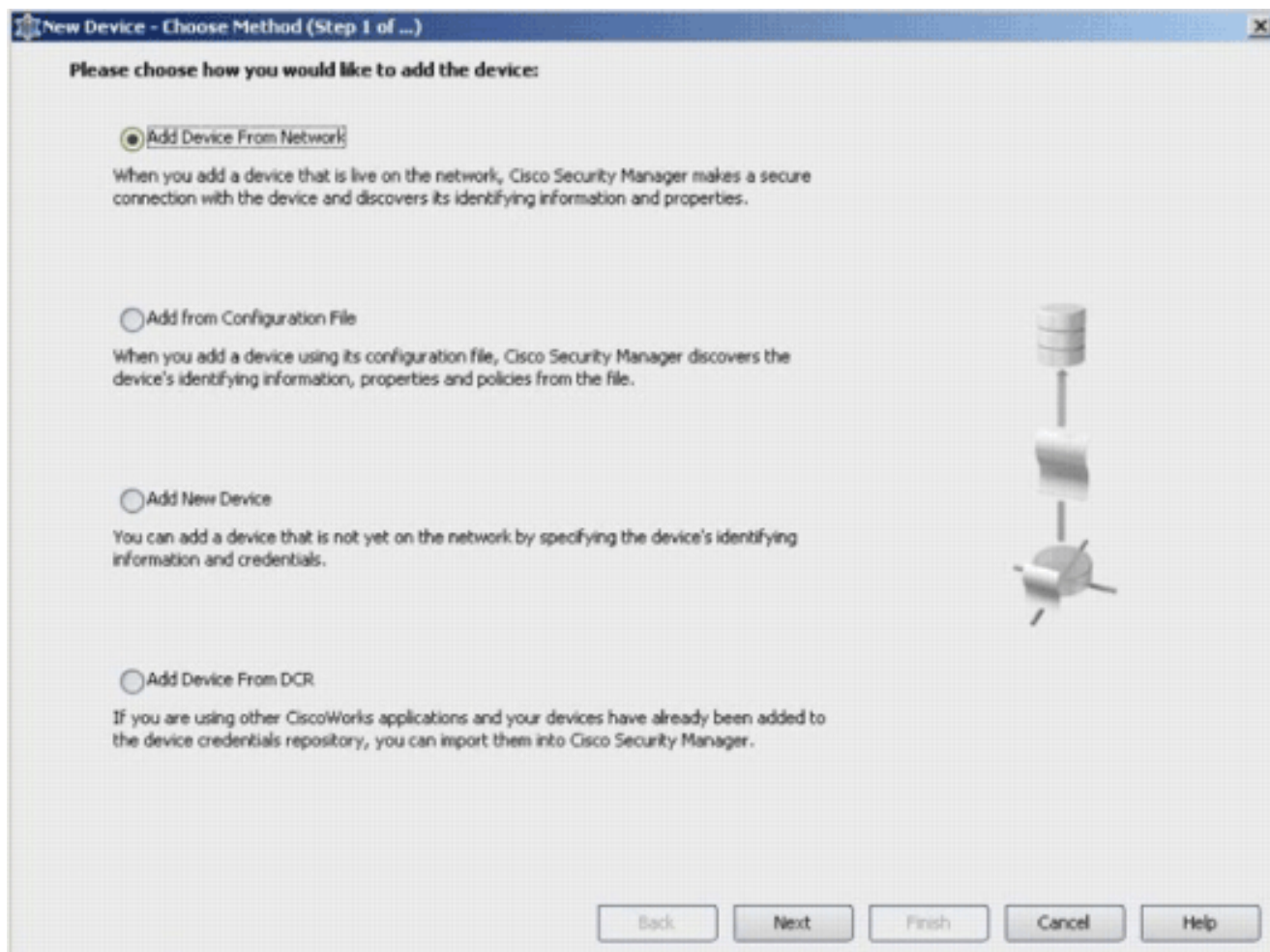
规则

有关文档约定的更多信息，请参考 Cisco 技术提示约定。

配置

要配置IOS IPS，请完成以下步骤：

1. 从本地PC运行Cisco Security Manager 3.1客户端。
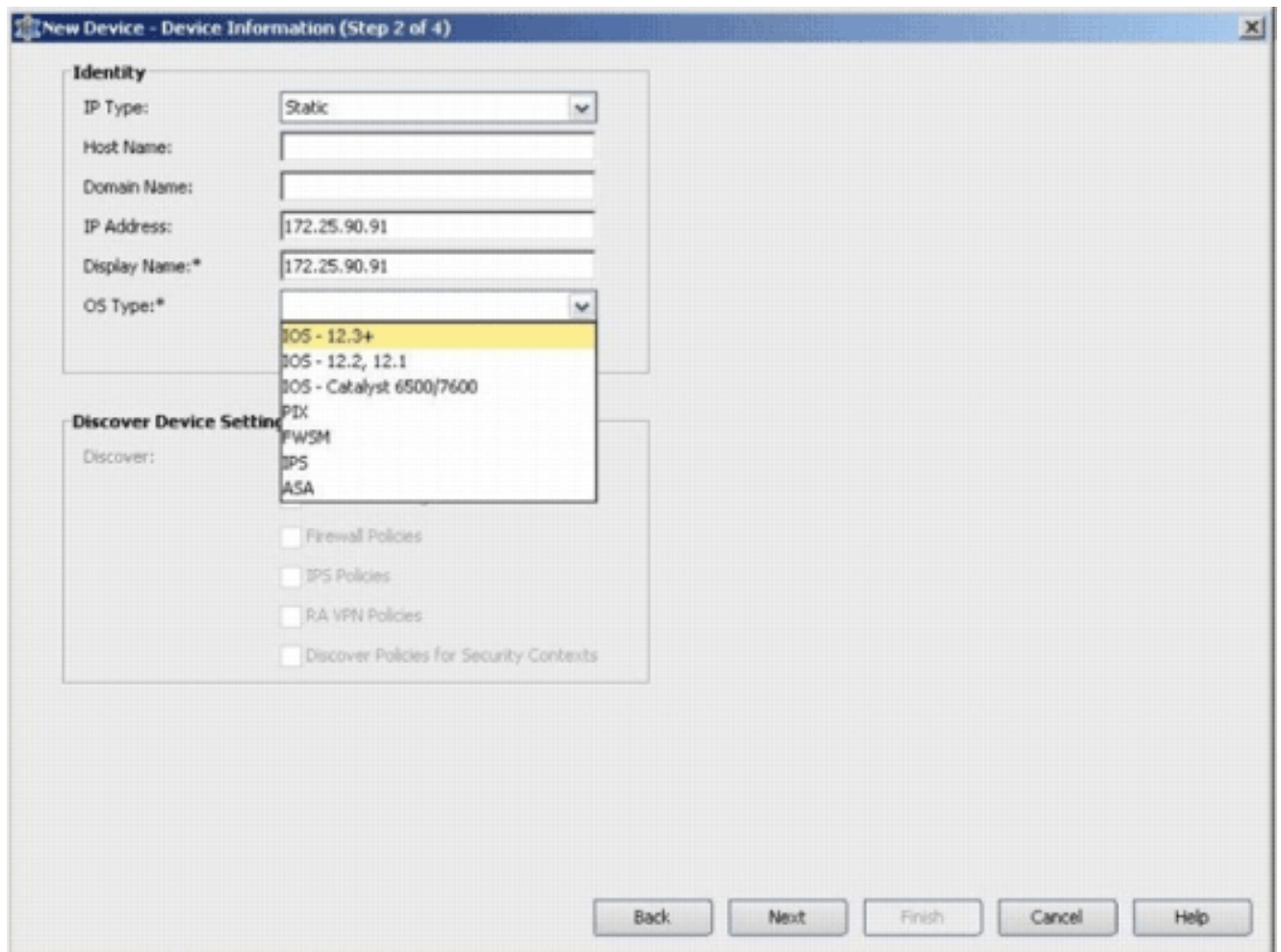2. 从"文件"菜单中选择**"新建设备"**，以便将设备添加到Cisco Security Manager 3.1。

3. 在New Device（新设备）窗口中，选择要添加设备的方式。本示例从网络添加设备。

New Device - Choose Method (Step 1 of ...)

Please choose how you would like to add the device:

○ **Add Device From Network**

When you add a device that is live on the network, Cisco Security Manager makes a secure connection with the device and discovers its identifying information and properties.

○ Add from Configuration File

When you add a device using its configuration file, Cisco Security Manager discovers the device's identifying information, properties and policies from the file.

○ Add New Device

You can add a device that is not yet on the network by specifying the device's identifying information and credentials.

○ Add Device From DCR

If you are using other CiscoWorks applications and your devices have already been added to the device credentials repository, you can import them into Cisco Security Manager.

Back Next Finish Cancel Help

4. 单击 Next。

5. 输入要添加的设备的身份详细信息。例如，主机名和IP地址。

Identity

IP Type:	Static
Host Name:	
Domain Name:	
IP Address:	172.25.90.91
Display Name:*	172.25.90.91
OS Type:*	

IOS - 12.3+
IOS - 12.2, 12.1
IOS - Catalyst 6500/7600
PIX
FWSM
IPS
ASA

Discover Device Setting

Discover:

☐ Firewall Policies

☐ IPS Policies

☐ RA VPN Policies

☐ Discover Policies for Security Contexts

Back   Next   Finish   Cancel   Help

6. 单击 **Next**。

7. 输入要添加的IOS路由器的主要凭证，如用户名、密码、启用密码。

8. 单击**Finish**将设备添加到Cisco Security Manager。**注意：**本示例假设用户已经预配置了路由器，并且可以使用适当的凭证登录路由器。

Primary Credentials

Username: cisco1234

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

Enable Password: ____   Confirm: ____

HTTP Credentials

☑ Use Primary Credentials

Username: ____

Password: ____

Confirm: ____

HTTP Port: 80

HTTPS Port: 443

IPS RDEP Mode: HTTPS ▾

Certificate Common Name: ____   Confirm: ____

[RX-Boot Mode...] [SNMP...]

[Back] [Next] [Finish] [Cancel] [Help]

当"发现状态"窗口中显示"发现已完成"时，您已成功将设备添加到思科安全管理器。成功将设备添加到思科安全管理器后，必须分配公钥才能启用IPS。
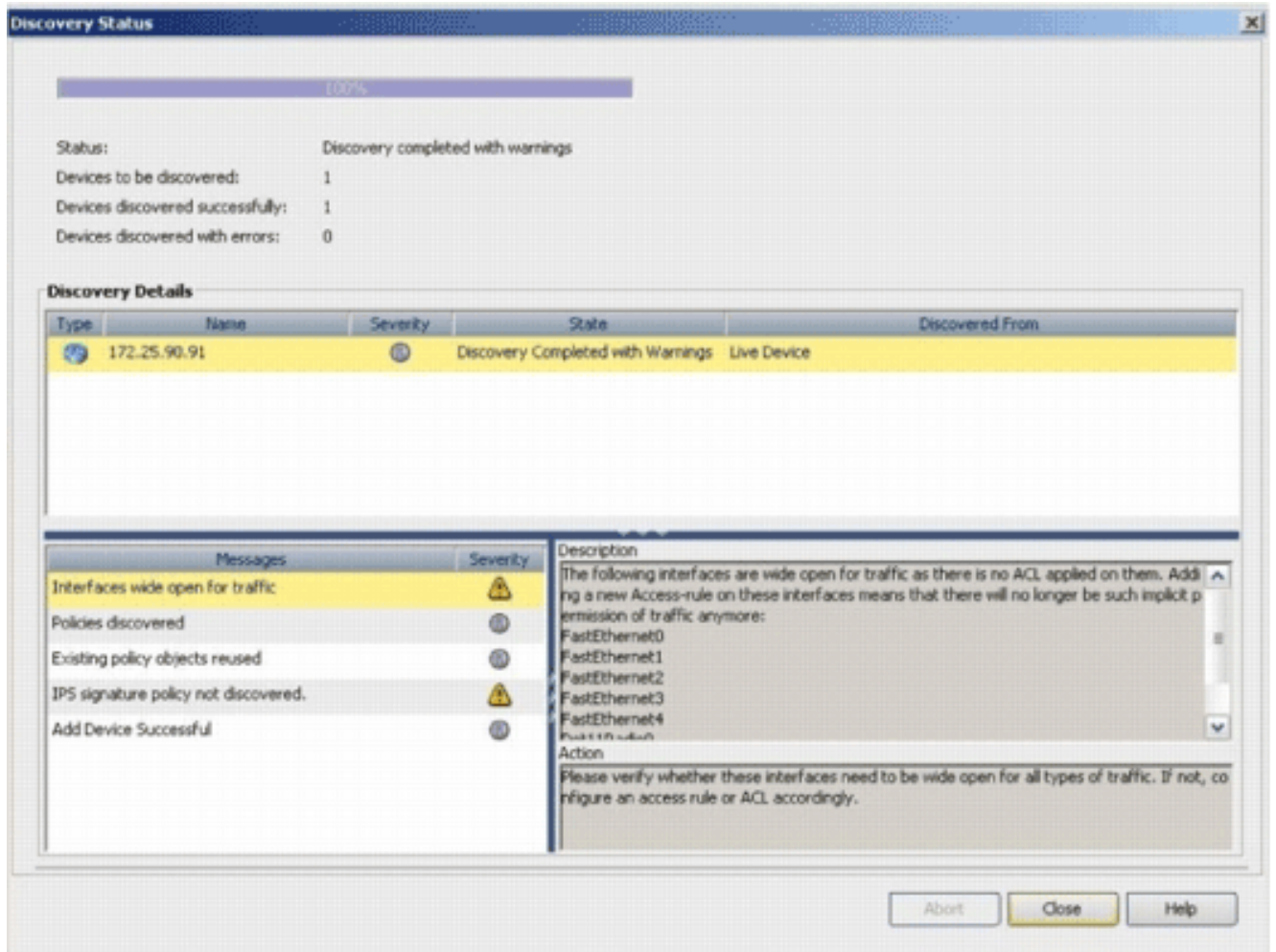
9. 从左侧的菜单中，导航至FlexConfigs配置屏幕。
10. 单击屏幕右侧的FlexConfigs用户界面，然后单击"添加"图标。
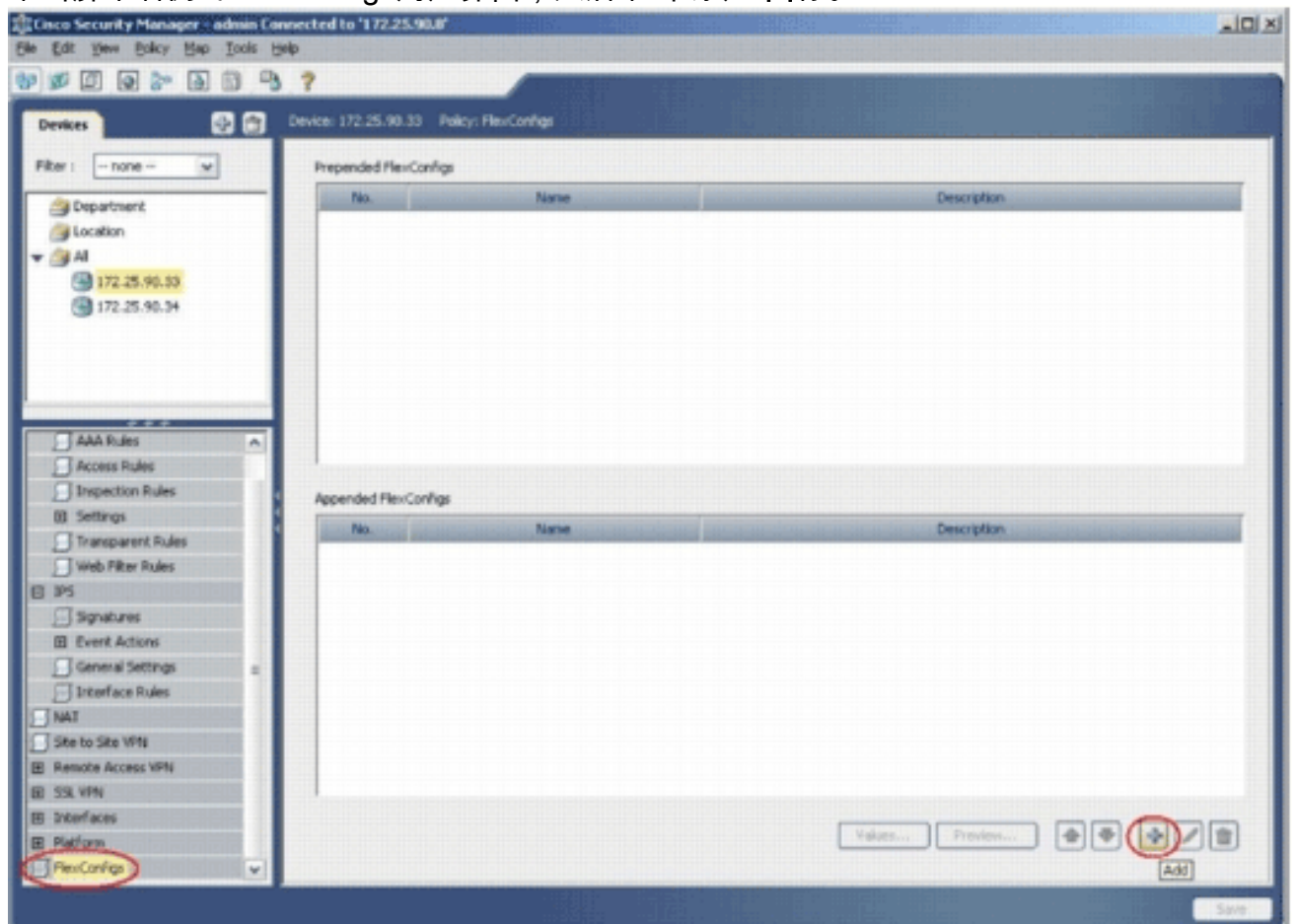
11. 在Selected FlexConfigs列表中，选择**IOS_IPS_PUBLIC_KEY**，然后单击**OK**。
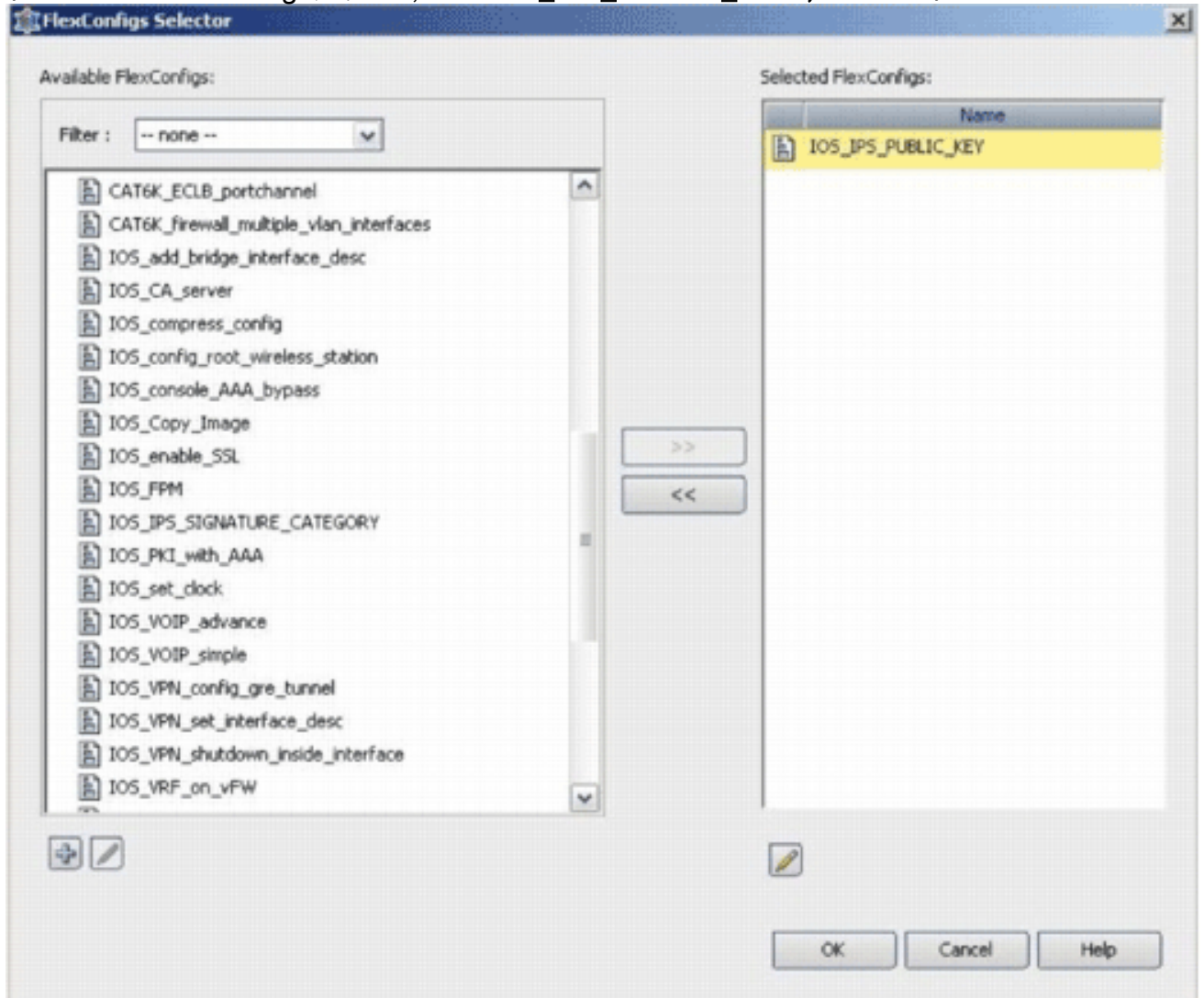
12. 单击**Save**以保存更改。**注意：**IOS_IPS_PUBLIC_KEY FlexConfig保留公钥的配置。
13. 从左侧的菜单中，选择IPS标题下方的General Settings。
14. 在闪存上输入IPS配置位置。这是IPS配置的放置位置。
15. 单击**Save**以保存更改。
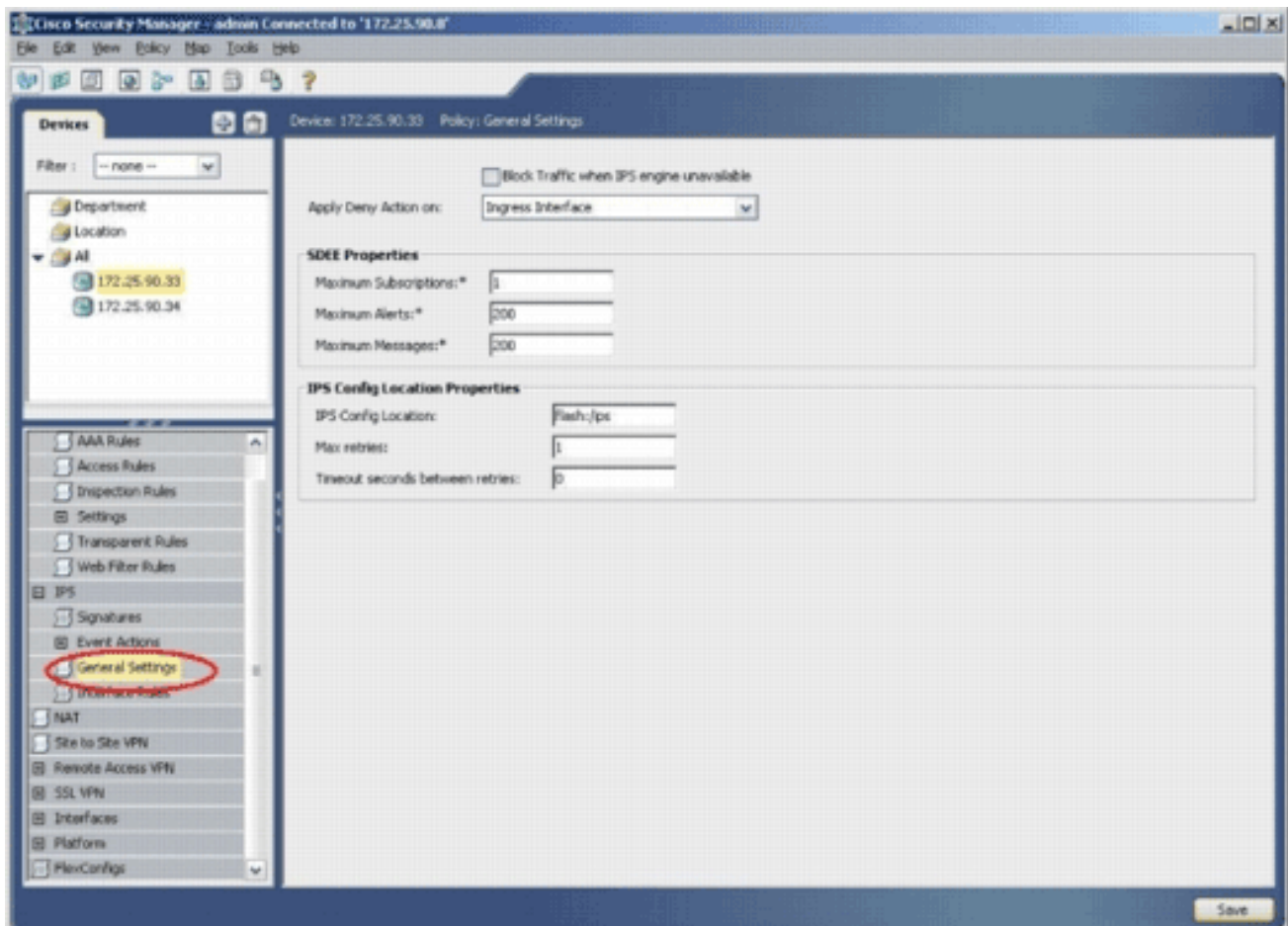
注意：确保已在路由器闪存上创建位置目录。否则，请使用mkdir <directory_name>命令创建位置目录。

16. 要启用IPS，请导航至Interface Rules，选中**Enable IPS**复选框，然后单击**Add Row**。

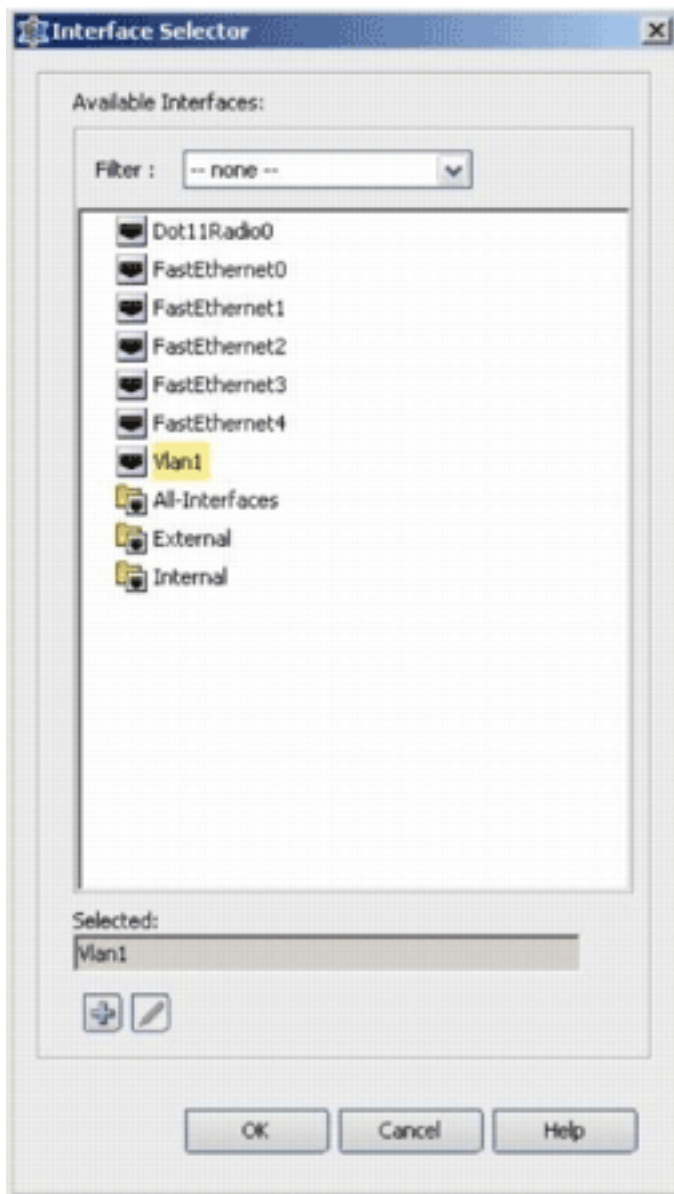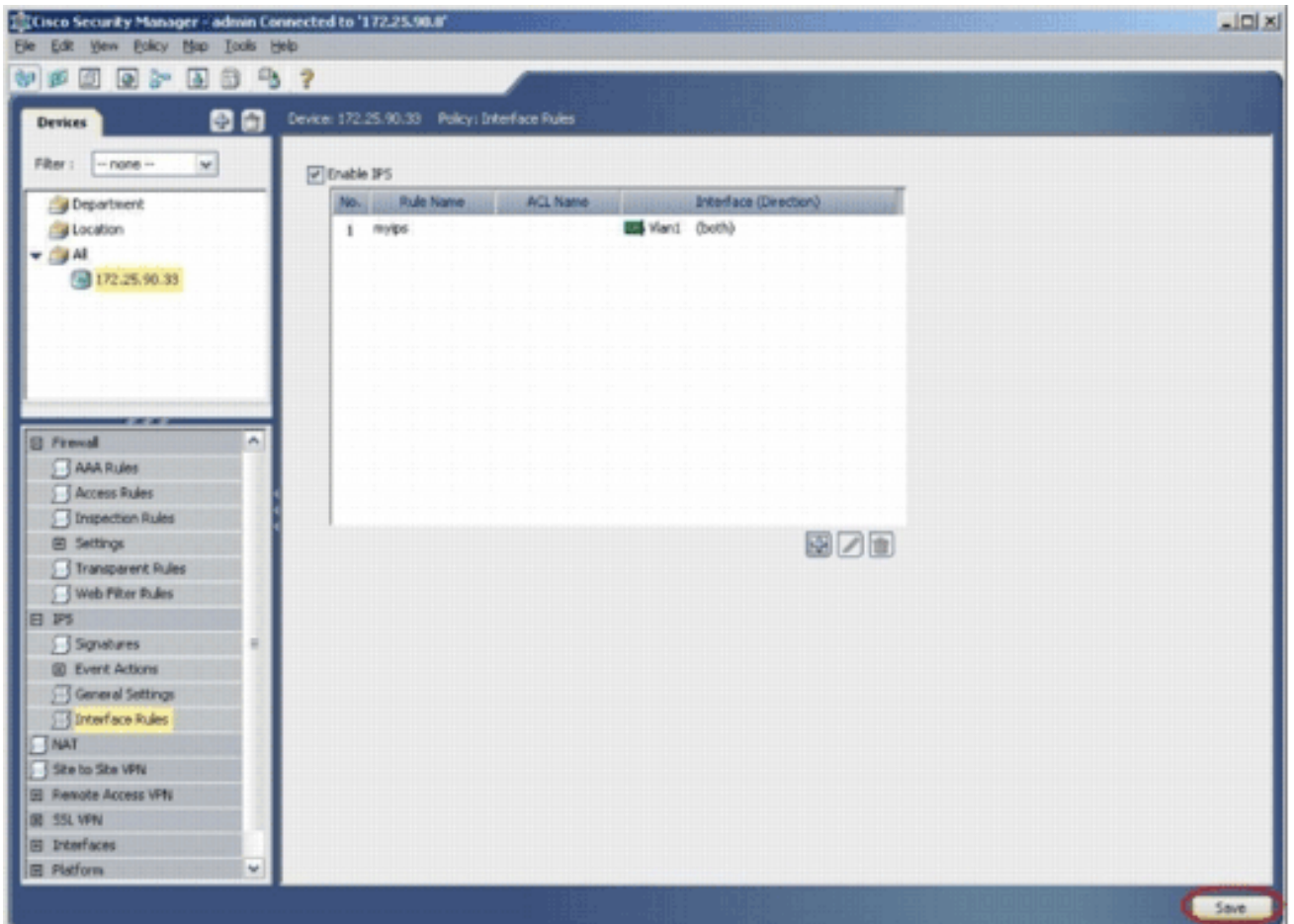17. 在Add IPS Rule对话框的Rule Name字段中，输入IPS规则的名称，然后单击**Add Row**以包括必须应用IPS的接口。
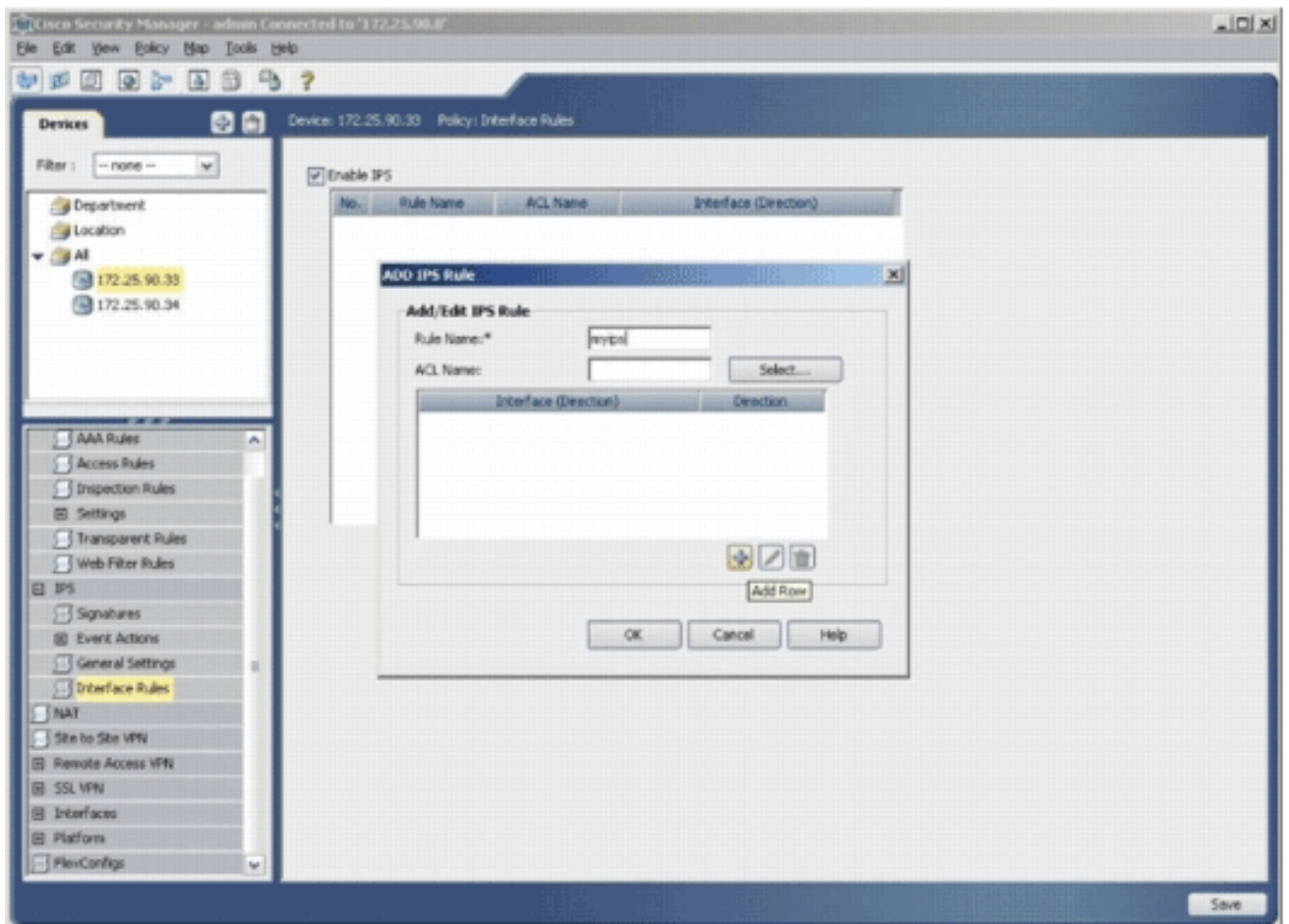
18. 单击指示IPS规则必须应用到哪个方向的单选按钮，然后单击**选择**以选择适当的接口。
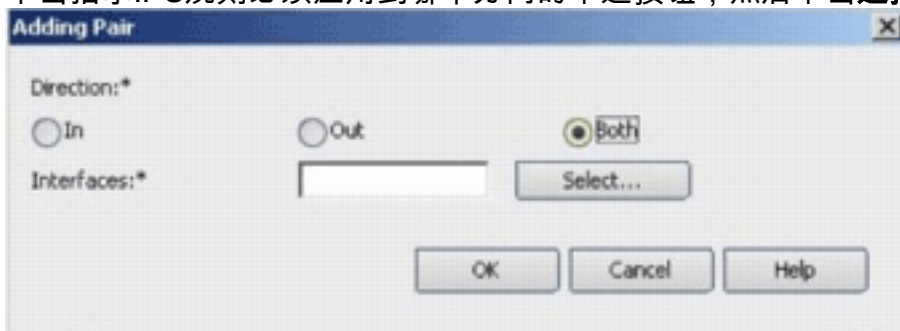
19. 从接口选择器列表中选择接口，然后单击**确定**。

20. 单击Save以保存更改。

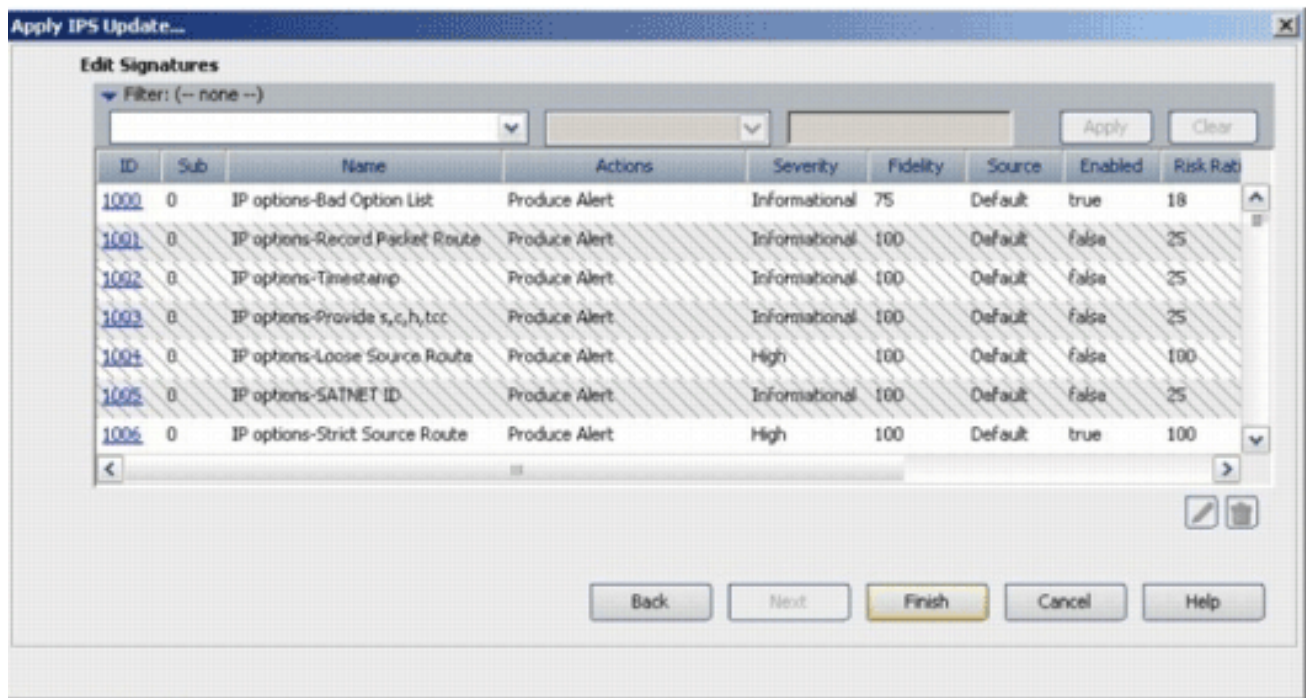21. 选择Tools > Apply IPS Update以安装最新的IPS签名。
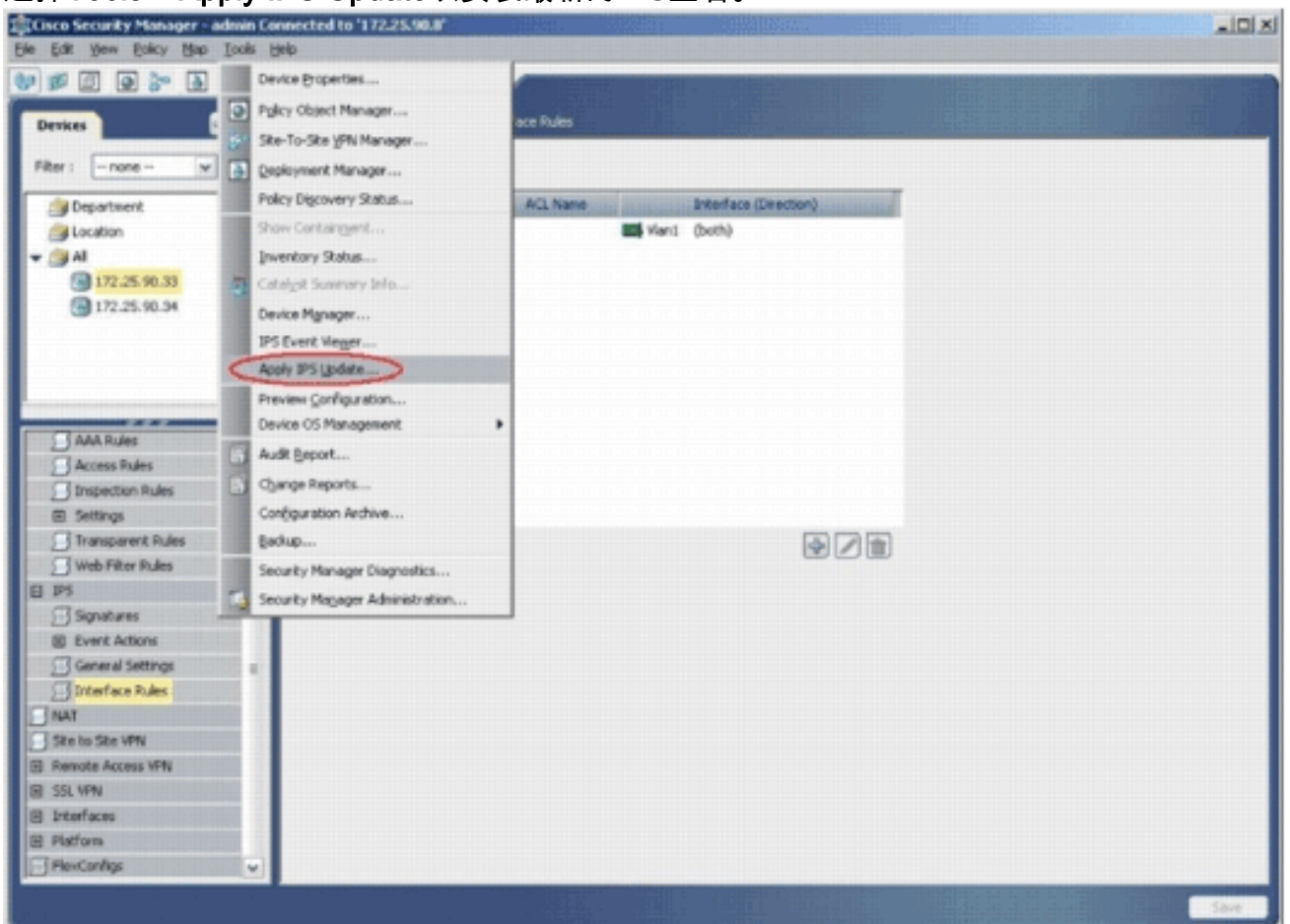
22. 选择最新的签名文件，然后单击Next。
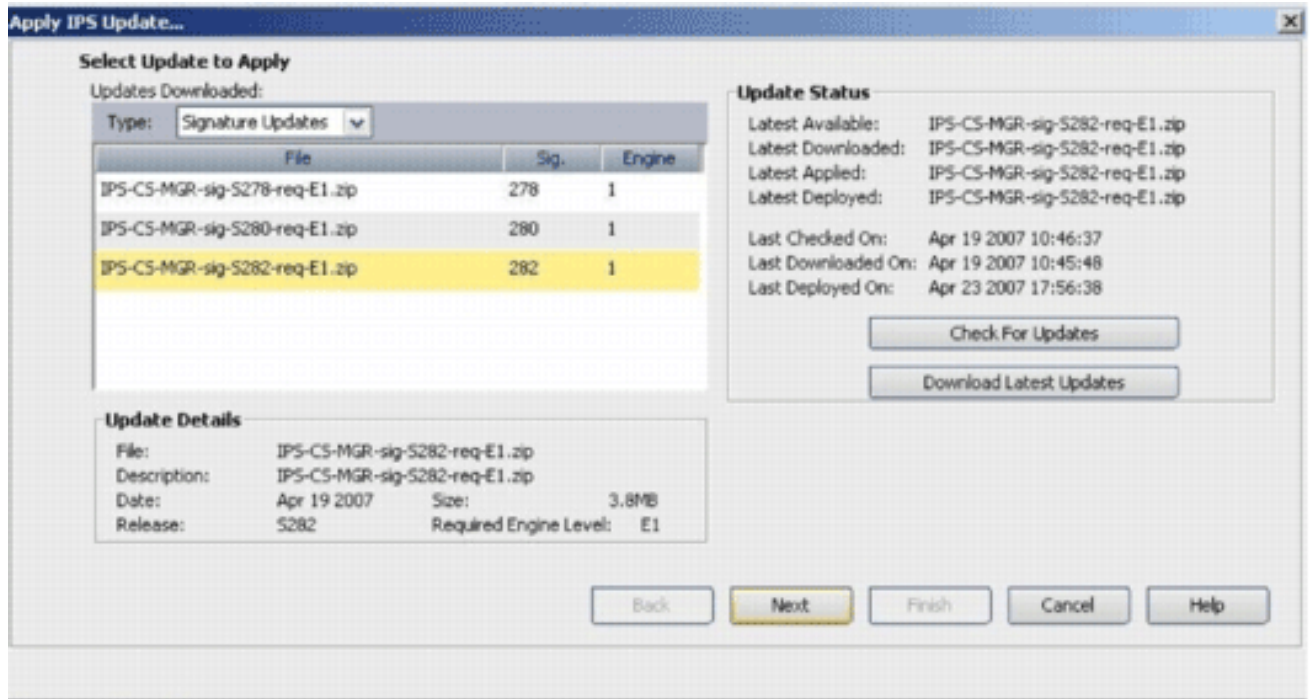
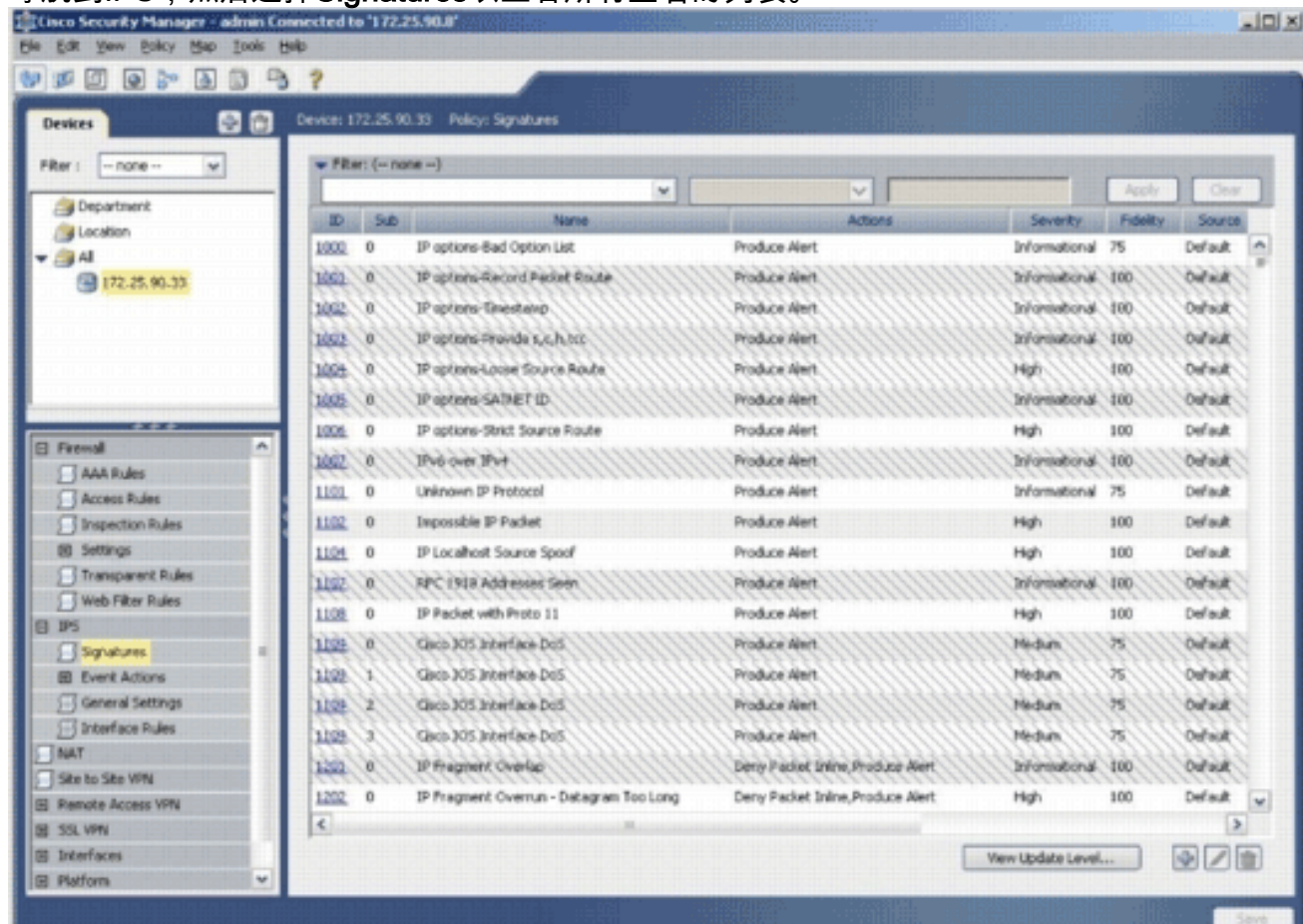23. 选择必须应用IPS更新的设备，然后单击**Next**。
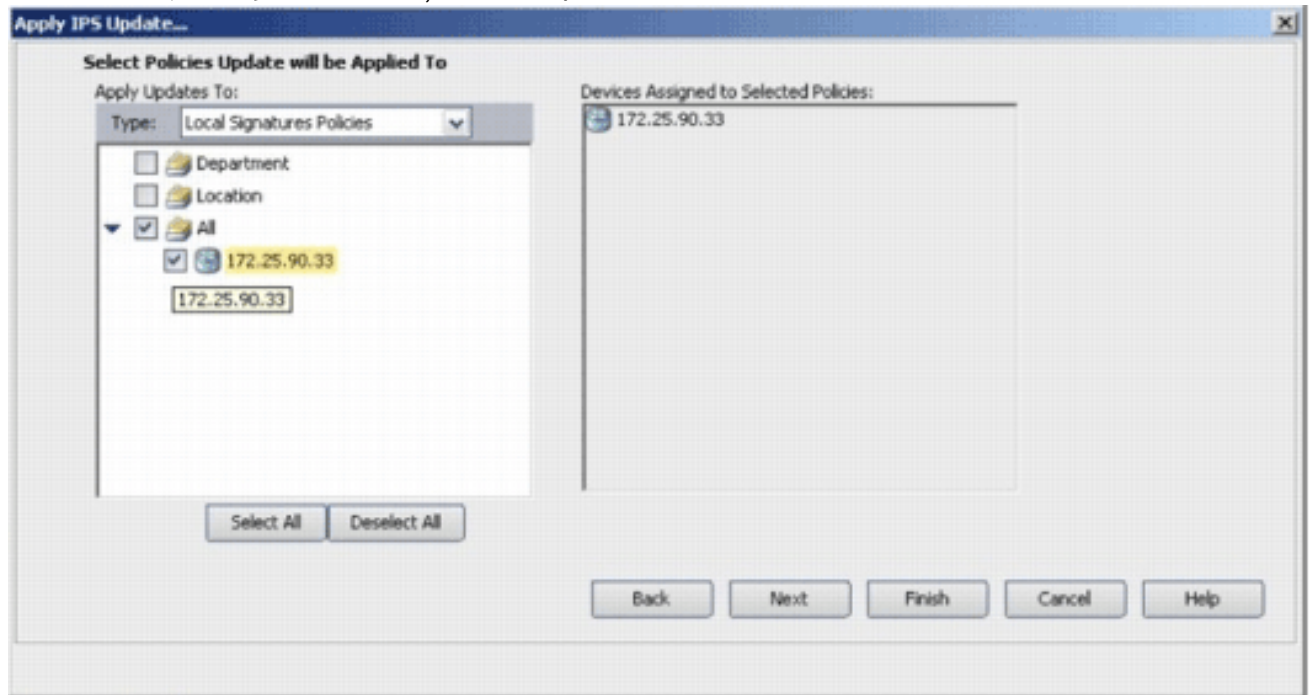
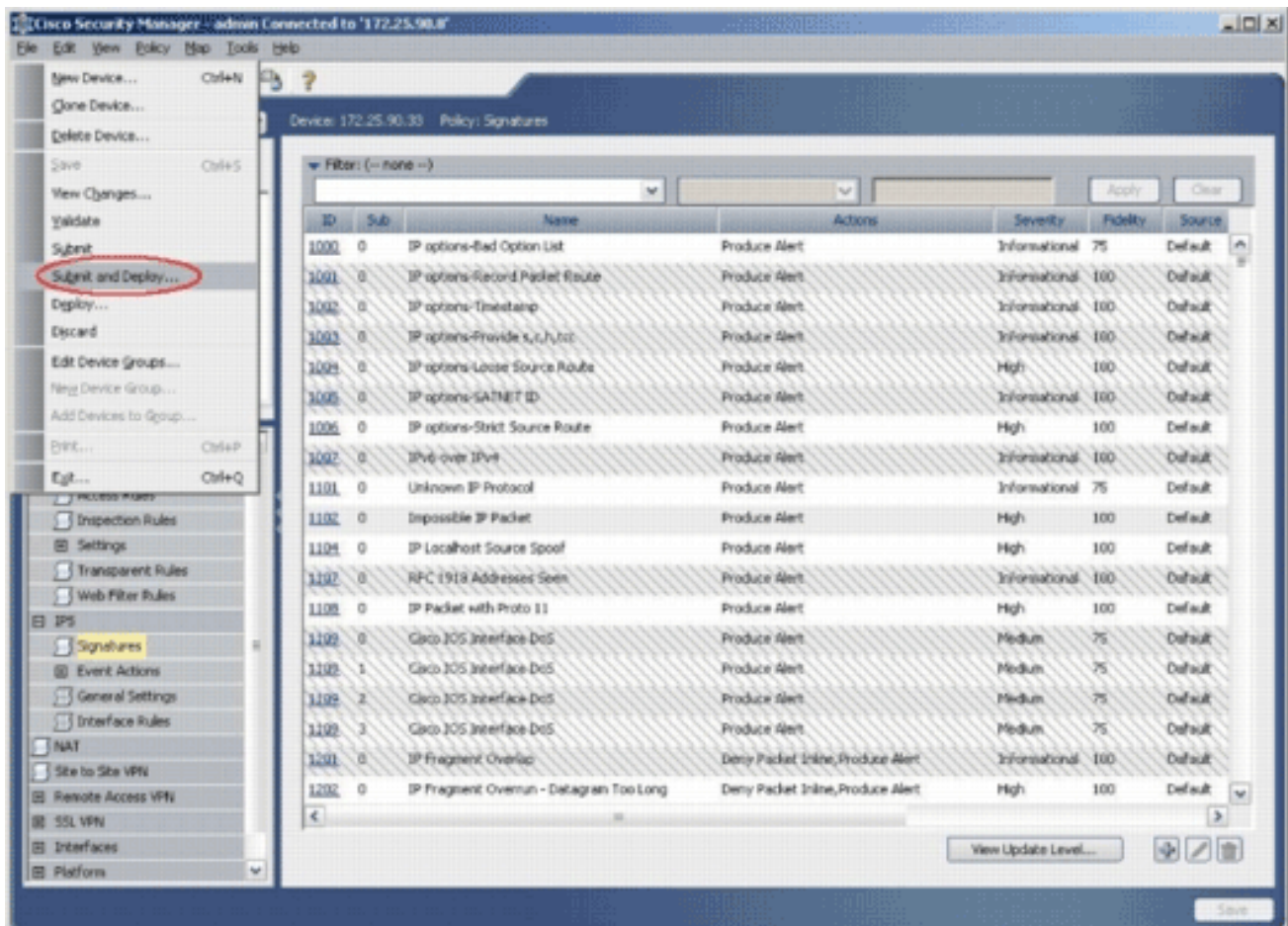24. 单击**Finish**以应用签名。

25. 导航到IPS，然后选择Signatures以查看所有签名的列表。

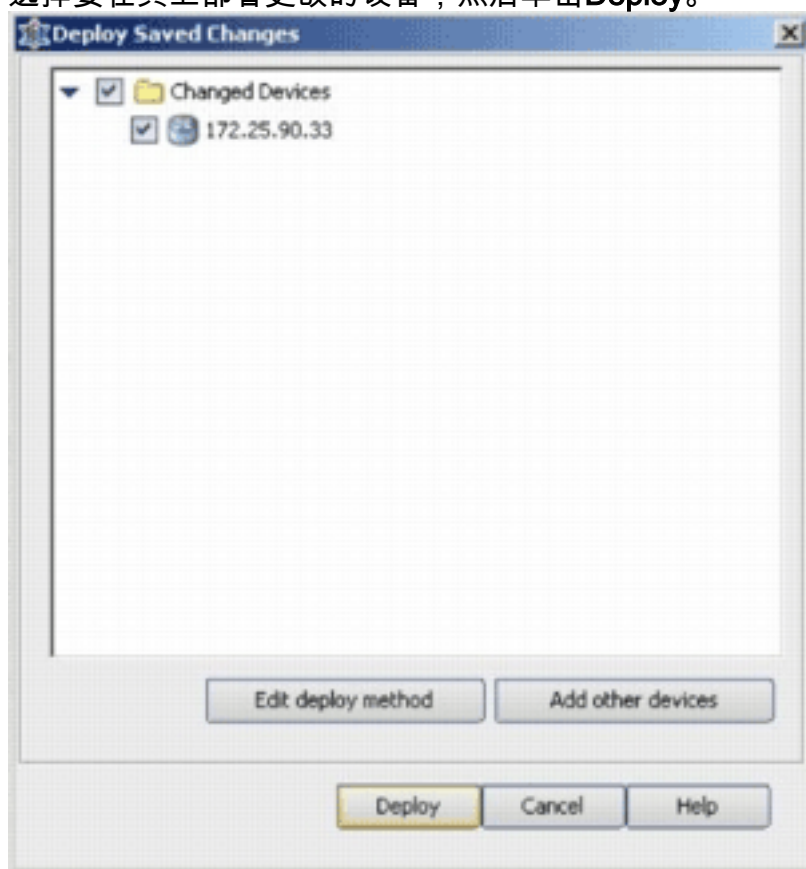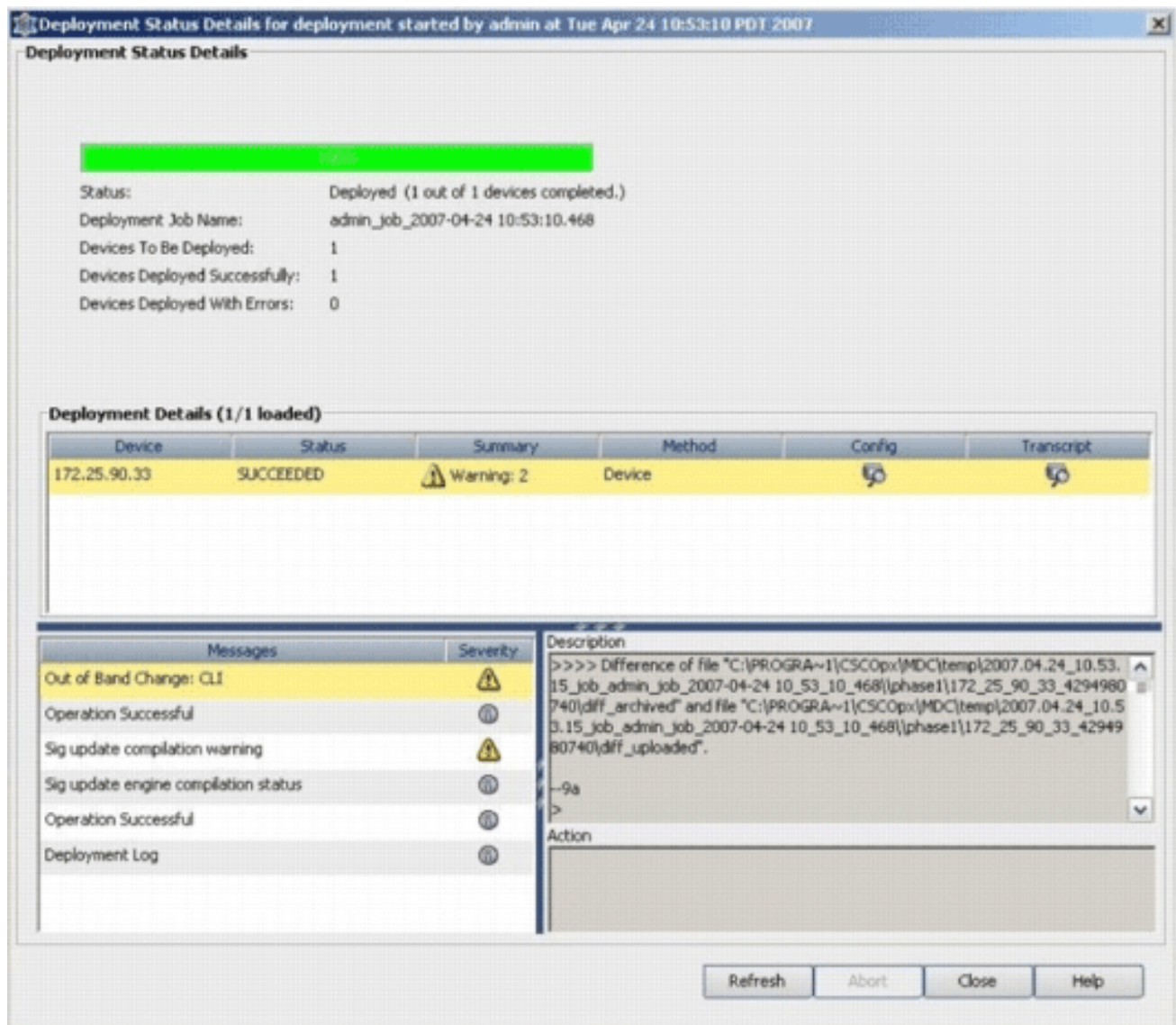26. 选择File > Submit and Deploy以在IOS路由器上部署IPS。

27. 选择要在其上部署更改的设备，然后单击**Deploy**。

28. 查看部署状态以验证是否存在错误。

相关信息

- Cisco IOS入侵防御系统(IPS)产品和服务页
- 采用 5.x 签名格式的 Cisco IOS IPS 入门
- IPS 5.x签名格式支持和可用性增强
- Cisco Intrusion Prevention System
- 安全产品的问题信息通告（Field Notice）(包括CiscoSecure Intrusion Detection)
- 技术支持 - Cisco Systems