在Cisco IOS IPS中配置路由器、SDM和Cisco IOS CLI

目录

简介

在Cisco路由器和安全设备管理器(SDM)2.2中，Cisco IOS® IPS配置集成在SDM应用程序中。配置Cisco IOS IPS时，您不再需要启动单独的窗口。

在Cisco SDM 2.2中，新的IPS配置向导将引导您完成在路由器上启用Cisco IOS IPS所需的步骤。此外，您仍可以使用高级配置选项来启用、禁用和调整Cisco IOS IPS与Cisco SDM 2.2。

思科建议您使用预调整的签名定义文件(SDF)运行Cisco IOS IPS:attack-drop.sdf、128MB.sdf和256MB.sdf。这些文件是为具有不同内存量的路由器创建的。这些文件与Cisco SDM捆绑在一起，当您首次在路由器上启用Cisco IOS IPS时，Cisco SDM会建议使用SDF。这些文件也可从http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup下载(仅限注册客户)。

启用默认SDF的过程在使用出厂默认SDF启用Cisco IOS IPS中详细介绍。当默认SDF不足或您想添加新签名时，可以使用在启用默认SDF后附加附加签名中所述的过程。

先决条件

要求

使用Cisco SDM 2.2需要Java Runtime Environment(JRE)版本1.4.2或更高版本。Cisco推荐和调整的签名文件（基于DRAM）与Cisco SDM捆绑在一起（使用Cisco SDM加载在路由器闪存中）。

使用的组件

本文档中的信息基于Cisco路由器和安全设备管理器(SDM)2.2。

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

使用出厂默认SDF启用Cisco IOS IPS

CLI过程

要使用CLI配置Cisco 1800系列路由器（使用Cisco IOS IPS）以在路由器闪存上加载128MB.sdf，请完成此步骤。

1. 配置路由器以启用安全设备事件交换(SDEE)事件通知。
   ```
   yourname#conf t
   ```

2. 输入配置命令（每行一条），然后按Cntl+Z结束。
   ```
   yourname(config)#ip ips notify sdee
   ```

3. 创建用于关联到接口的IPS规则名称。
   ```
   yourname(config)#ip ips name myips
   ```

4. 配置IPS location命令以指定Cisco IOS IPS系统从哪个文件读取签名。本示例使用闪存上的文件：128MB.sdf。此命令的位置URL部分可以是任何使用闪存、磁盘或协议（通过FTP、HTTP、HTTPS、RTP、SCP和TFTP）以指向文件的有效URL。
   ```
   yourname(config)#ip ips sdf location flash:128MB.sdf
   ```

   注意：如果通过Telnet会话配置路由器，或者在生成签名引擎时看不到SDEE消息，则必须启用terminal monitor命令。
5. 在要启用Cisco IOS IPS以扫描流量的接口上启用IPS。在本例中，我们在接口fastEthernet 0上启用了两个方向。
   ```
   yourname(config)#interface fastEthernet 0
   yourname(config-if)#ip ips myips in
   *Oct 26 00:32:30.297: %IPS-6-SDF_LOAD_SUCCESS:
           SDF loaded successfully from opacl
   *Oct 26 00:32:30.921: %IPS-6-SDF_LOAD_SUCCESS:
           SDF loaded successfully from flash:128MB.sdf
   *Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING:
           OTHER - 4 signatures - 1 of 15 engines
   *Oct 26 00:32:30.921: %IPS-6-ENGINE_READY:
           OTHER - 0 ms - packets for this engines will be scanned
   *Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING:
           MULTI-STRING - 0 signatures - 2 of 15 engines
   *Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILD_SKIPPED:
           MULTI-STRING - there are no new signature definitions for this engine
   *Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING:
           STRING.ICMP - 1 signatures - 3 of 15 engines
   *Oct 26 00:32:30.941: %IPS-6-ENGINE_READY:
   ```

```
        STRING.ICMP - 20 ms - packets for this engine will be scanned
*Oct 26 00:32:30.945: %IPS-6-ENGINE_BUILDING:
        STRING.UDP - 17 signatures - 4 of15 engines
*Oct 26 00:32:31.393: %IPS-6-ENGINE_READY:
        STRING.UDP - 448 ms - packets for this engine will be scanned
*Oct 26 00:32:31.393: %IPS-6-ENGINE_BUILDING:
        STRING.TCP - 58 signatures - 5 of 15 engines
*Oct 26 00:32:33.641: %IPS-6-ENGINE_READY:
        STRING.TCP - 2248 ms - packets for this engine will be scanned
*Oct 26 00:32:33.641: %IPS-6-ENGINE_BUILDING:
        SERVICE.FTP - 3 signatures - 6 of 15 engines
*Oct 26 00:32:33.657: %IPS-6-ENGINE_READY:
        SERVICE.FTP - 16 ms - packets for this engine will be scanned
*Oct 26 00:32:33.657: %IPS-6-ENGINE_BUILDING:
        SERVICE.SMTP - 2 signatures - 7 of 15 engines
*Oct 26 00:32:33.685: %IPS-6-ENGINE_READY:
        SERVICE.SMTP - 28 ms - packets for this engine will be scanned
*Oct 26 00:32:33.689: %IPS-6-ENGINE_BUILDING:
        SERVICE.RPC - 29 signatures - 8 f 15 engines
*Oct 26 00:32:33.781: %IPS-6-ENGINE_READY:
        SERVICE.RPC - 92 ms - packets for this engine will be scanned
*Oct 26 00:32:33.781: %IPS-6-ENGINE_BUILDING:
        SERVICE.DNS - 31 signatures - 9 of 15 engines
*Oct 26 00:32:33.801: %IPS-6-ENGINE_READY:
        SERVICE.DNS - 20 ms - packets for this engine will be scanned
*Oct 26 00:32:33.801: %IPS-6-ENGINE_BUILDING:
        SERVICE.HTTP - 132 signatures - 10 of 15 engines
*Oct 26 00:32:44.505: %IPS-6-ENGINE_READY:
        SERVICE.HTTP - 10704 ms - packets for this engine will be scanned
*Oct 26 00:32:44.509: %IPS-6-ENGINE_BUILDING:
        ATOMIC.TCP - 11 signatures - 11 of 15 engines
*Oct 26 00:32:44.513: %IPS-6-ENGINE_READY:
        ATOMIC.TCP - 4 ms - packets for this engine will be scanned
*Oct 26 00:32:44.513: %IPS-6-ENGINE_BUILDING:
        ATOMIC.UDP - 9 signatures - 12 of 15 engines
*Oct 26 00:32:44.517: %IPS-6-ENGINE_READY:
        ATOMIC.UDP - 4 ms - packets for this engine will be scanned
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING:
        ATOMIC.ICMP - 0 signatures - 13 of 15 engines
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILD_SKIPPED:
        ATOMIC.ICMP - there are no new signature definitions for this engine
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING:
        ATOMIC.IPOPTIONS - 1 signatures - 14 of 15 engines
*Oct 26 00:32:44.517: %IPS-6-ENGINE_READY:
        ATOMIC.IPOPTIONS - 0 ms - packets for this engine will be scanned
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING:
        ATOMIC.L3.IP - 5 signatures - 15 of 15 engines
*Oct 26 00:32:44.517: %IPS-6-ENGINE_READY:
        ATOMIC.L3.IP - 0 ms - packets for this engine will be scanned
yourname(config-if)#ip ips myips out
yourname(config-if)#ip virtual-reassembly
```

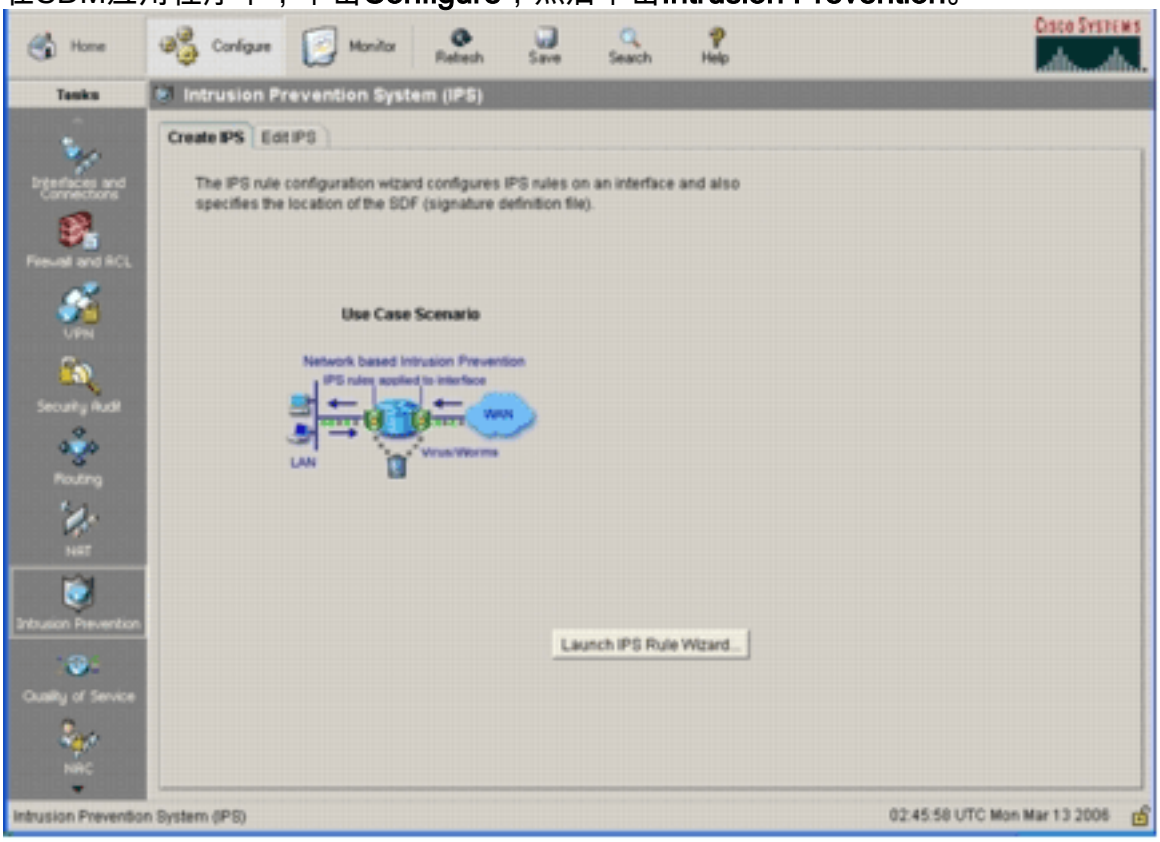
首次将IPS规则应用到接口时，Cisco IOS IPS会从SDF locations命令指定的文件启动构建签名。SDEE消息记录到控制台并发送到系统日志服务器（如果已配置）。SDEE消息的*<number>*个引擎的*<number>*表示签名引擎构建过程。最后，当两个数字相同时，所有引擎都建成。**注意：**IP虚拟重组是接口功能，（打开时）会自动重组通过该接口进入路由器的分段数据包。思科建议您在流量进入路由器的所有接口上启用ip virtual-assembly。在上例中，除了在接口fastEthernet 0上打开“ip virtual-assembly”外，我们还在内部接口VLAN 1上配置它。

```
yourname(config)#int vlan 1
yourname(config-if)#ip virtual-reassembly
```

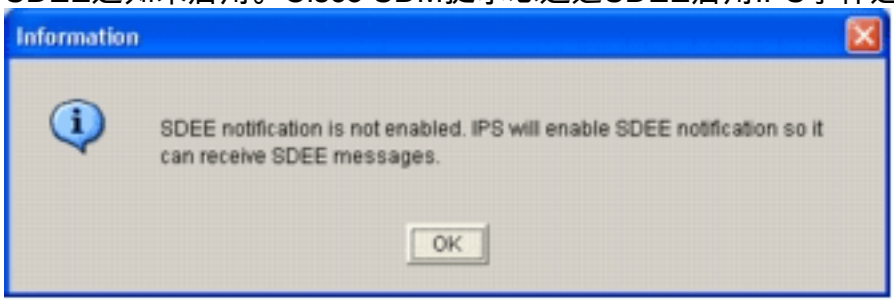
SDM 2.2程序

要使用Cisco SDM 2.2配置带Cisco IOS IPS的Cisco 1800系列路由器，请完成此步骤。

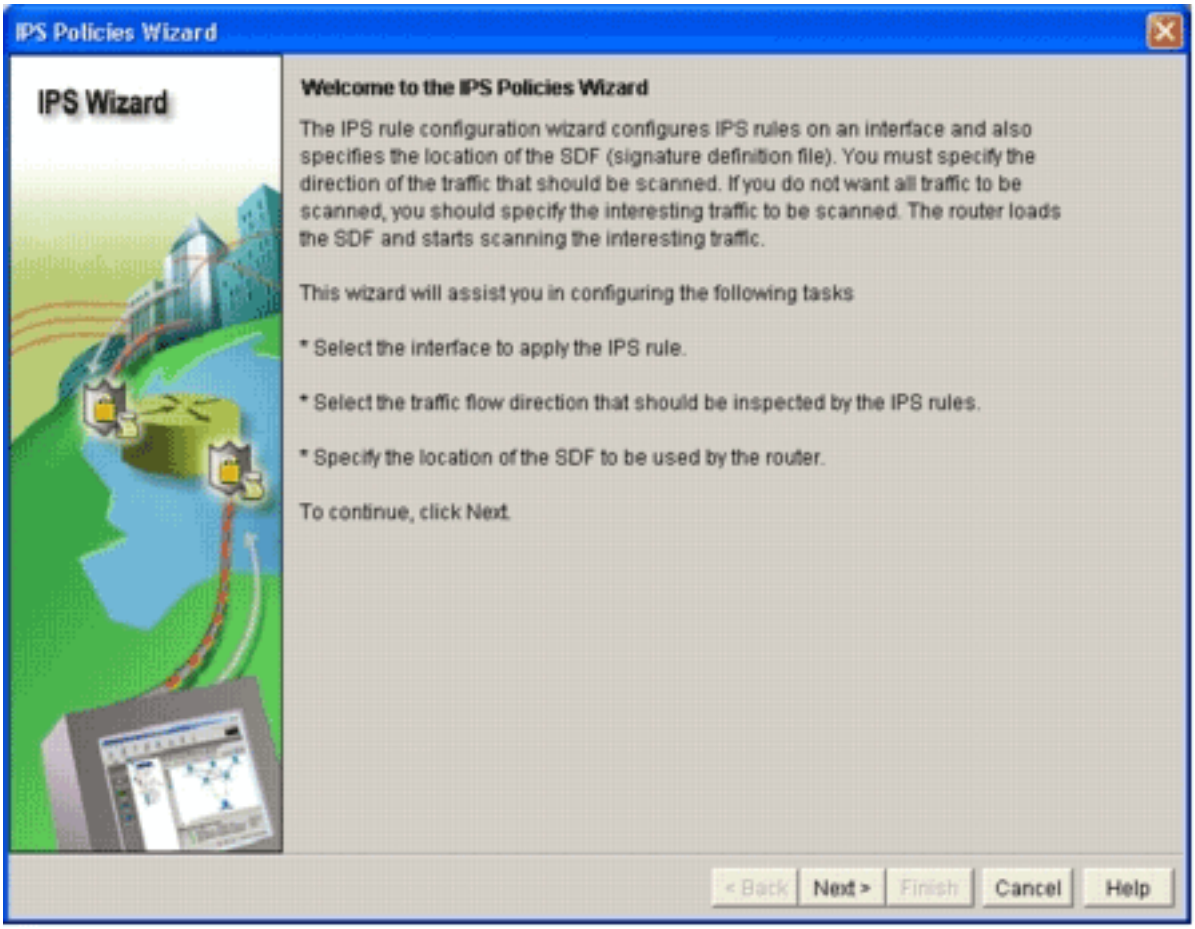
1. 在SDM应用程序中，单击**Configure**，然后单击**Intrusion Prevention**。



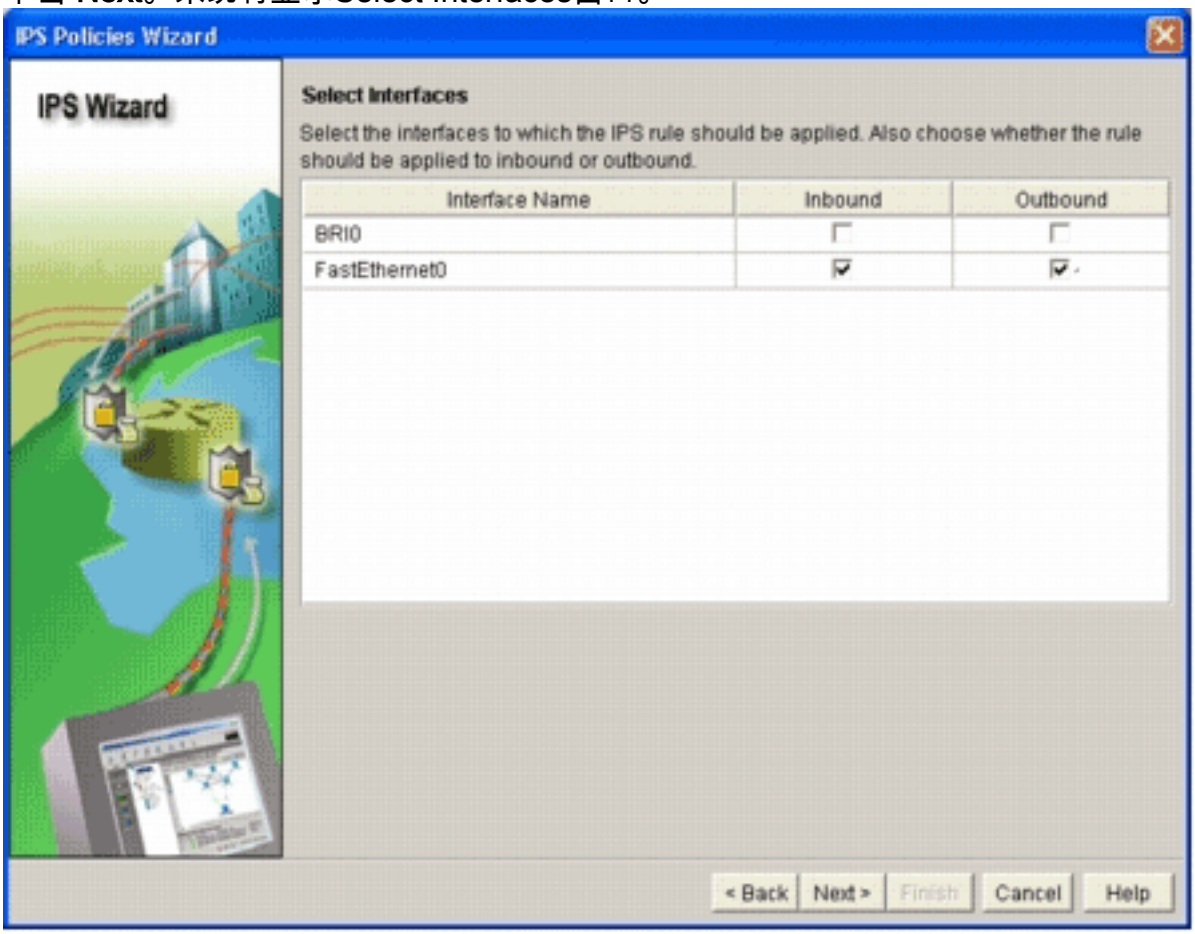
2. 单击“Create IPS（**创建IPS**）”选项卡，然后单击“**Launch IPS Rule Wizard（启动IPS规则向导）**”。Cisco SDM需要通过SDEE发出IPS事件通知才能配置Cisco IOS IPS功能。默认情况下，SDEE通知未启用。Cisco SDM提示您通过SDEE启用IPS事件通知，如下图所示：



3. Click **OK**.系统将显示IPS策略向导对话框的欢迎使用IPS策略向导窗口。

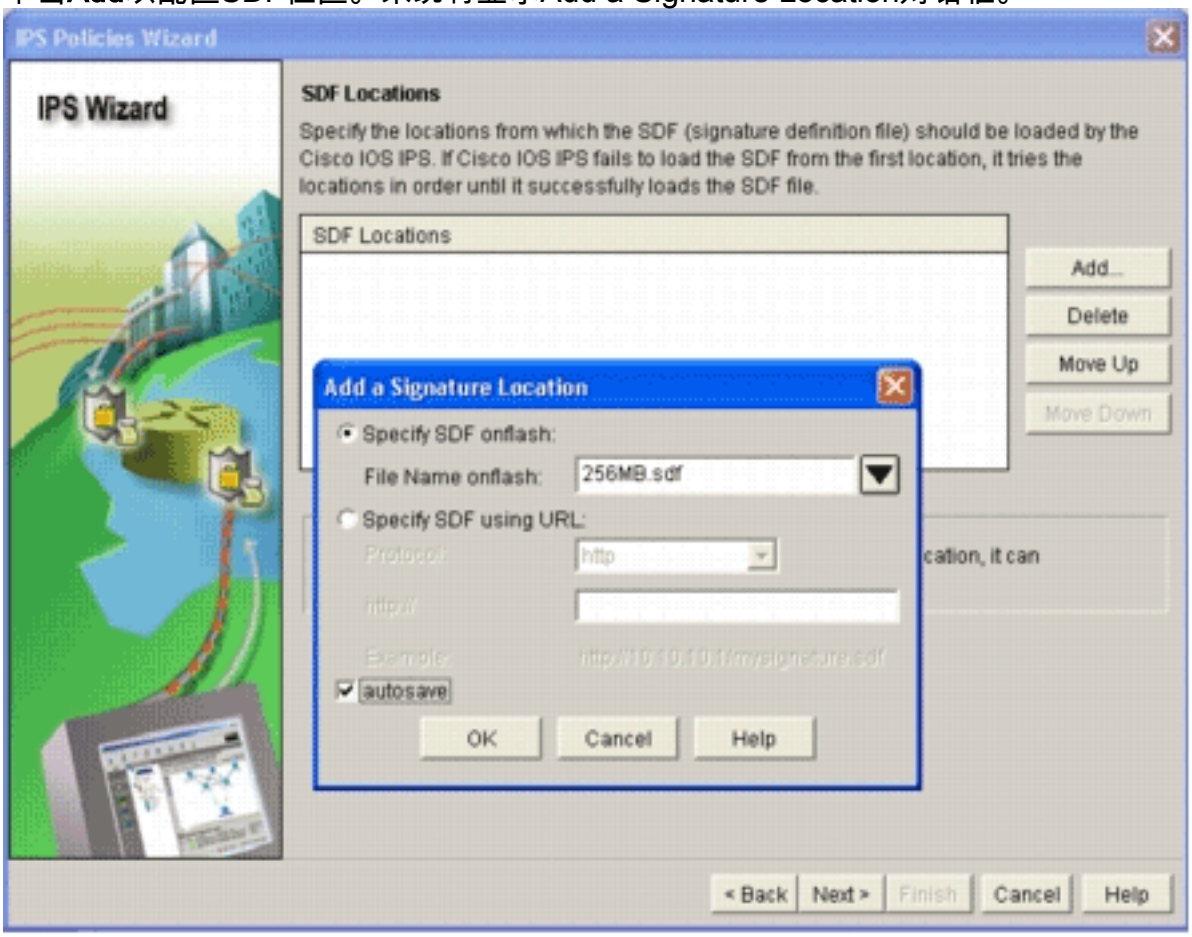


4. 单击 **Next**。系统将显示Select Interfaces窗口。

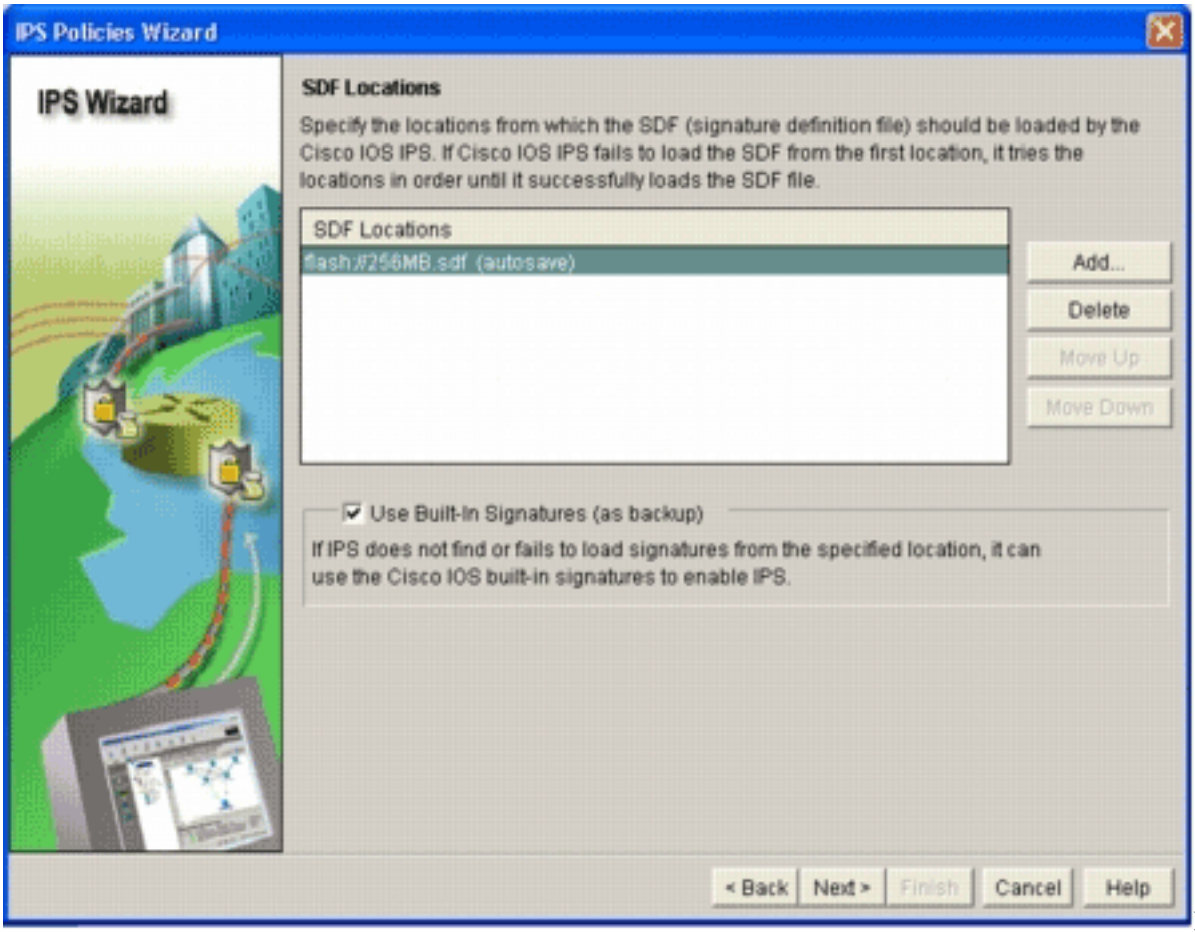


5. 选择要为其启用IPS的接口，然后单击**Inbound**或**Outbound**复选框以指示该接口的方向。**注意**：当在接口上启用IPS时，思科建议同时启用入站和出站方向。
6. 单击 **Next**。系统将显示SDF Locations窗口。

7. 单击**Add**以配置SDF位置。系统将显示Add a Signature Location对话框。

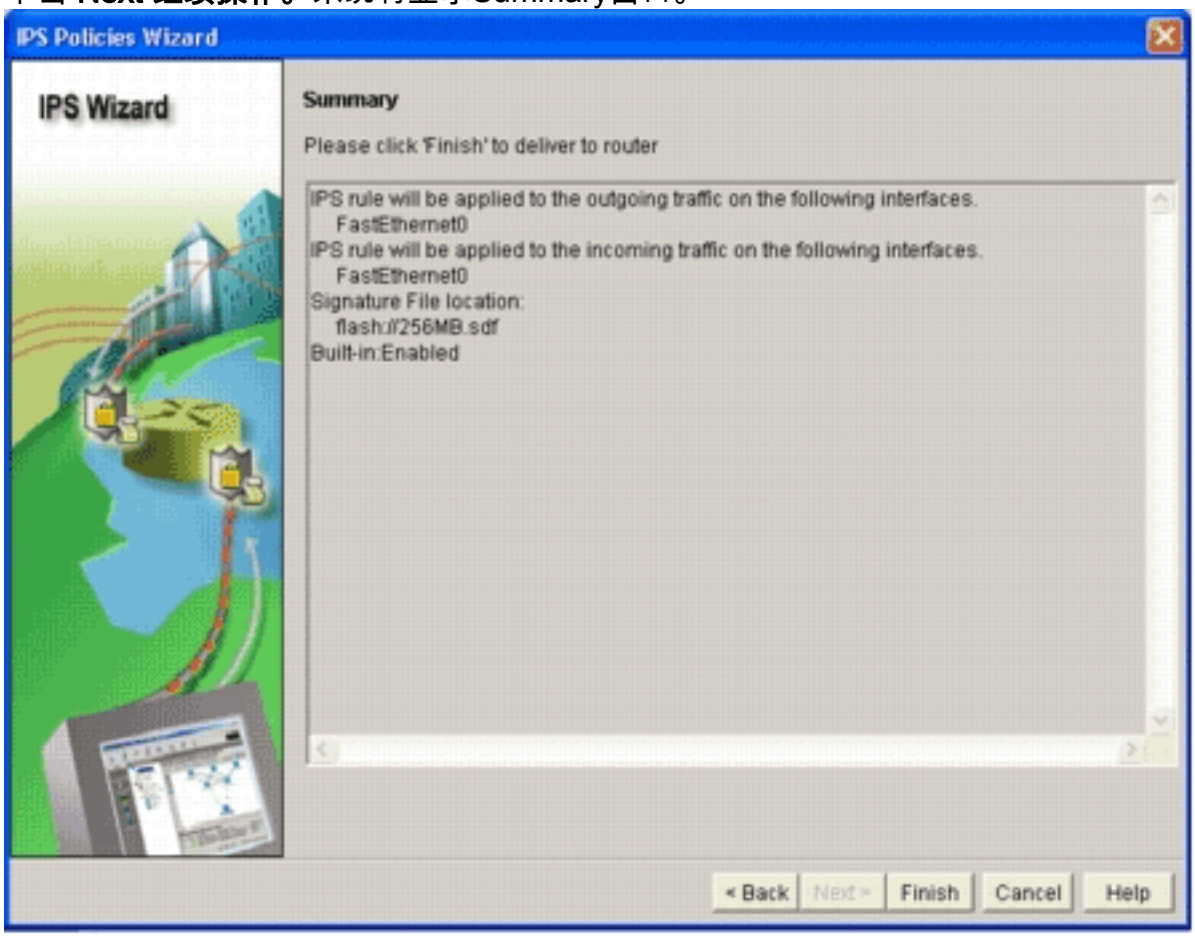


8. 单击“**Specify SDF on flash”单选**按钮，然后从“File Name on flash”下拉列**表中选择** 256MB.sdf。
9. 单击“自动**保存”**复选框，然后单击“**确定”。注意：** 当签名发生更改时，autosave选项会自动保存签名文件。“SDF位置”窗口显示新的SDF位置。

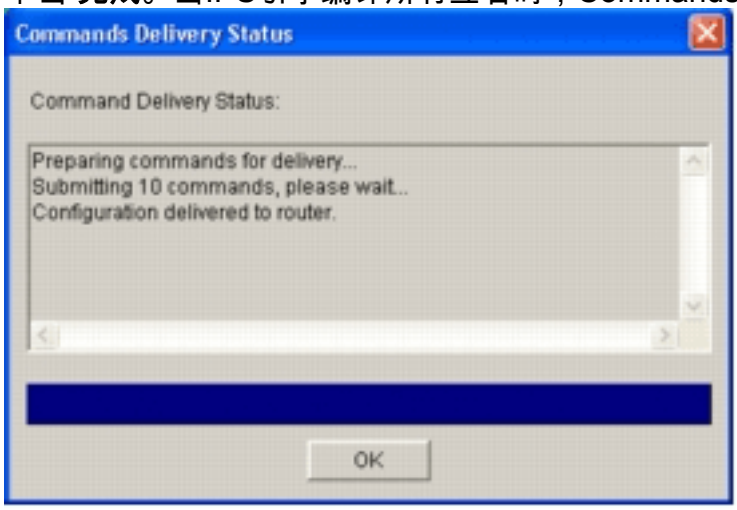


注意：您可以添加其他签名位置以指定备份。

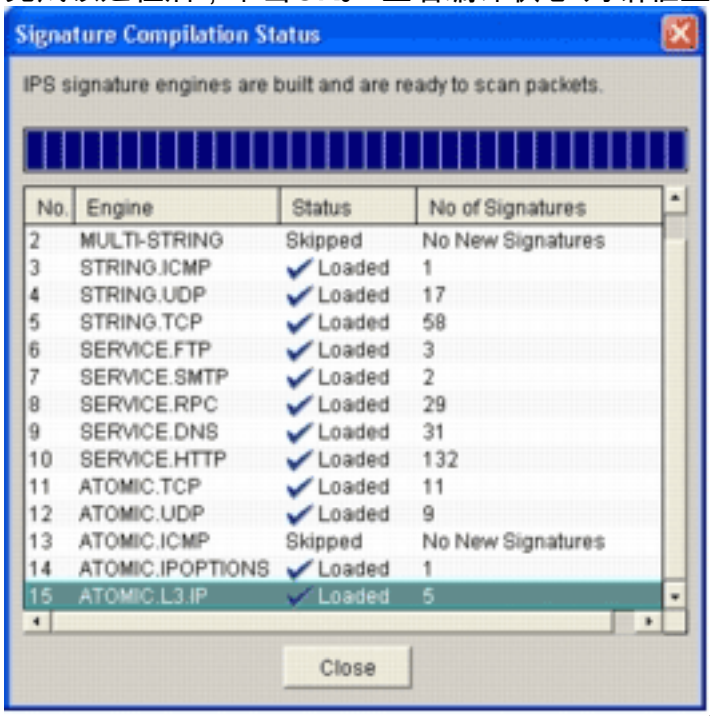
10. 单击“**使用内置签名（作为备份）**”复选框。**注意：**除非已指定一个或多个位置，否则思科建议不要使用内置签名选项。
11. 单击 **Next 继续操作。**系统将显示Summary窗口。



12. 单击 **完成**。当IPS引擎编译所有签名时，Commands Delivery Status对话框显示状态。

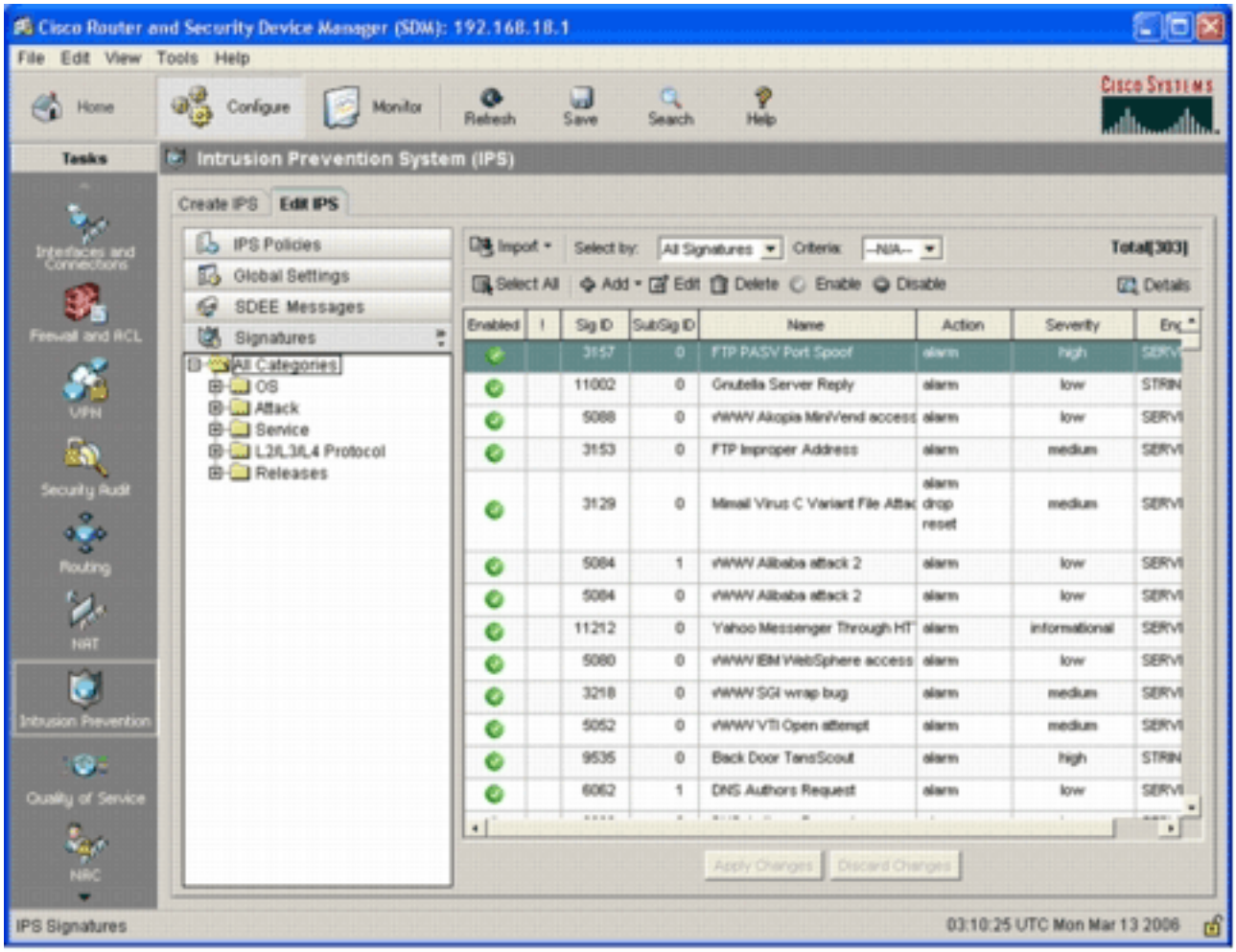


13. 完成该过程后，单击**OK**。“签名编译状态”对话框显示签名编译信息。



此信息显示已编译的引擎以及该引擎中的签名数。对于在状态列中显示“已跳过”的引擎，没有为该引擎加载签名。

14. 单击**关闭**以关闭“签名编译状态”对话框。
15. 要验证路由器上当前加载的签名，请单击**Configure**，然后单击**Intrusion Prevention**。
16. 单击“Edit IPS（**编辑IPS**）”选项卡，然后单击“**Signatures（签名）**”。IPS签名列表显示在“签名”窗口中。



启用默认SDF后附加其他签名

CLI过程

没有CLI命令可用于创建签名或从分布式IOS-Sxxx.zip文件读取签名信息。Cisco建议您使用SDM或IPS传感器管理中心来管理Cisco IOS IPS系统上的签名。

对于已准备好签名文件并希望将此文件与在Cisco IOS IPS系统上运行的SDF合并的客户，可以使用以下命令：

```
yourname#show running-config | include ip ips sdf
ip ips sdf location flash:128MB.sdf
yourname#
```

由signature location命令定义的签名文件是路由器在重新加载或重新配置路由器IOS IPS时加载签名文件的位置。要使合并过程成功，还必须更新由signature file location命令定义的文件。

1. 使用**show**命令检查当前配置的签名位置。输出显示已配置的签名位置。此命令显示当前运行签名的加载位置。

   ```
   yourname#show ip ips signatures
   Builtin signatures are configured
   ```

   上次从闪存加载签名：128MB.sdf思科SDF版本S128.0趋势SDF版本V0.0
2. 使用**copy <*url*> ips-sdf**命令以及上一步中的信息来合并签名文件。

   ```
   yourname#copy tftp://10.10.10.5/mysignatures.xml ips-sdf
   Loading mysignatures.xml from 10.10.10.5 (via Vlan1): !
   [OK - 1612 bytes]
   *Oct 26 02:43:34.904: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from opacl
   ```

```
No entry found for lport 55577, fport 4714 No entry found for lport 51850, fport
4715
*Oct 26 02:43:34.920: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from
        tftp://10.10.10.5/mysignatures.xml
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: OTHER - 4 signatures - 1 of 15 engines
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: OTHER - there are no new signature
        definitions for this engine
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: MULTI-STRING - 0 signatures -
        2 of 15 engines
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: MULTI-STRING - there are
        no new signature definitions for this engine
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: STRING.ICMP - 1 signatures -
        3 of 15 engines
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: STRING.ICMP - there are
        no new signature definitions for this engine
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: STRING.UDP - 17 signatures -
        4 of 15 engines
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: STRING.UDP - there are
        no new signature definitions for this engine
*Oct 26 02:43:34.924: %IPS-6-ENGINE_BUILDING: STRING.TCP - 59 signatures -
        5 of 15 engines
*Oct 26 02:43:36.816: %IPS-7-UNSUPPORTED_PARAM: STRING.TCP 9434:0 CapturePacket=False -
        This parameter is not supported
*Oct 26 02:43:37.264: %IPS-6-ENGINE_READY: STRING.TCP - 2340 ms - packets for this
        engine will be scanned
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.FTP - 3 signatures -
        6 of 15 engines
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.FTP - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.SMTP - 2 signatures -
        7 of 15 engines
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.SMTP - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.RPC - 29 signatures -
        8 of 15 engines
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.RPC - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.292: %IPS-6-ENGINE_BUILDING: SERVICE.DNS - 31 signatures -
        9 of 15 engines
*Oct 26 02:43:37.292: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.DNS - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.296: %IPS-6-ENGINE_BUILDING: SERVICE.HTTP - 132 signatures -
        10 of 15 engines
*Oct 26 02:43:37.296: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.HTTP - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILDING: ATOMIC.TCP - 11 signatures -
        11 of 15 engines
*Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.TCP - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILDING: ATOMIC.UDP - 9 signatures -
        12 of 15 engines
*Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.UDP - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.ICMP - 0 signatures -
        13 of 15 engines
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.ICMP - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.IPOPTIONS - 1 signatures -
        14 of 15 engines
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.IPOPTIONS - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.L3.IP - 5 signatures -
        15 of 15 engines
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.L3.IP - there are
```

```
        no new signature definitions for this engine
yourname#
```

发出**copy**命令后，路由器会将签名文件加载到内存中，然后构建签名引擎。在控制台SDEE消息输出中，显示每个签名引擎的构建状态。%IPS-6-ENGINE_BUILD_SKIPPED表示此引擎没有新签名。%IPS-6-ENGINE_READY表示有新签名，且引擎已就绪。与以前一样，“15个引擎中的15个”消息表示所有引擎都已构建。IPS-7-UNSUPPORTED_PARAM表示Cisco IOS IPS不支持某个参数。例如，CapturePacket和ResetAfterIdle。**注意：** 这些消息仅供参考，对Cisco IOS IPS签名功能或性能没有影响。通过将日志记录级别设置为高于调试级别（级别7），可以关闭这些日志记录消息。

3. 更新由signature location命令定义的SDF，这样当路由器重新加载时，它将具有包含更新签名的合并签名集。此示例显示将合并签名保存到128MB.sdf闪存文件后的文件大小差异。

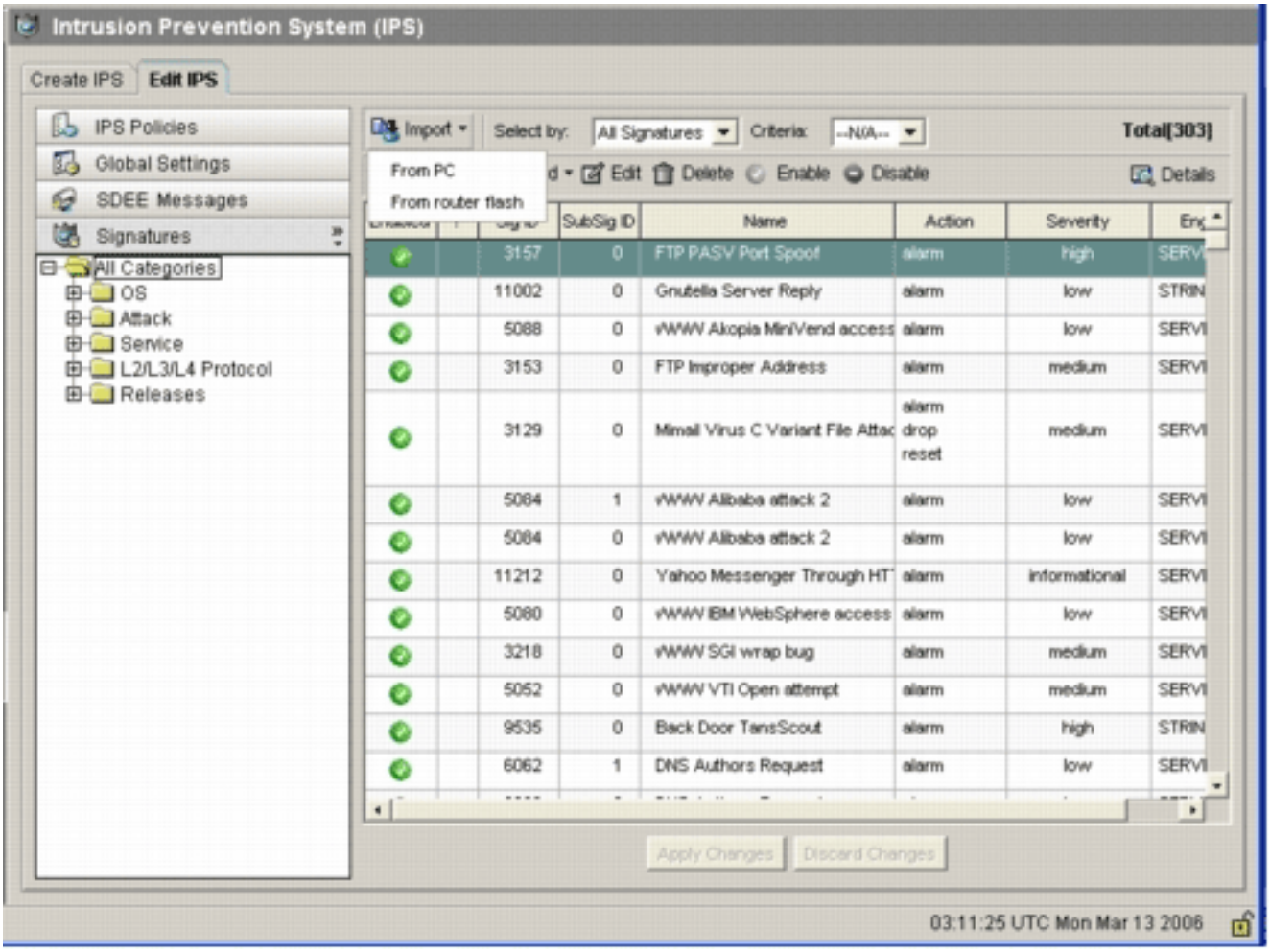
```
yourname#show flash:
-#- --length-- -----date/time------ path
4 504630 Aug 30 2005 22:58:34 +00:00 128MB.sdf
yourname#copy ips-sdf flash:128MB.sdf
yourname#show flash:
-#- --length-- -----date/time------ path
4 522656 Oct 26 2005 02:51:32 +00:00 128MB.sdf
```

警告：新的128MB.sdf现在包含客户合并的签名。内容与思科默认128MB.sdf文件不同。思科建议您将此文件更改为其他名称以避免混淆。如果名称更改，则还需要更改signature location命令。

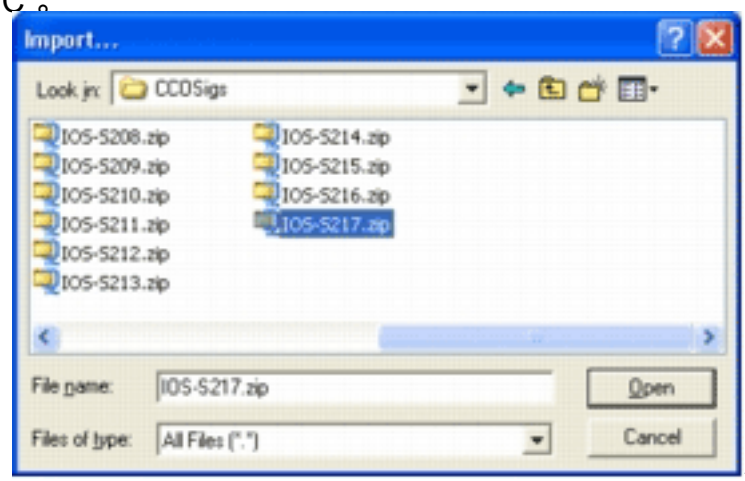
SDM 2.2程序

启用Cisco IOS IPS后，可以向运行具有Cisco SDM导入功能的签名集的路由器中添加新签名。要导入新签名，请完成以下步骤：

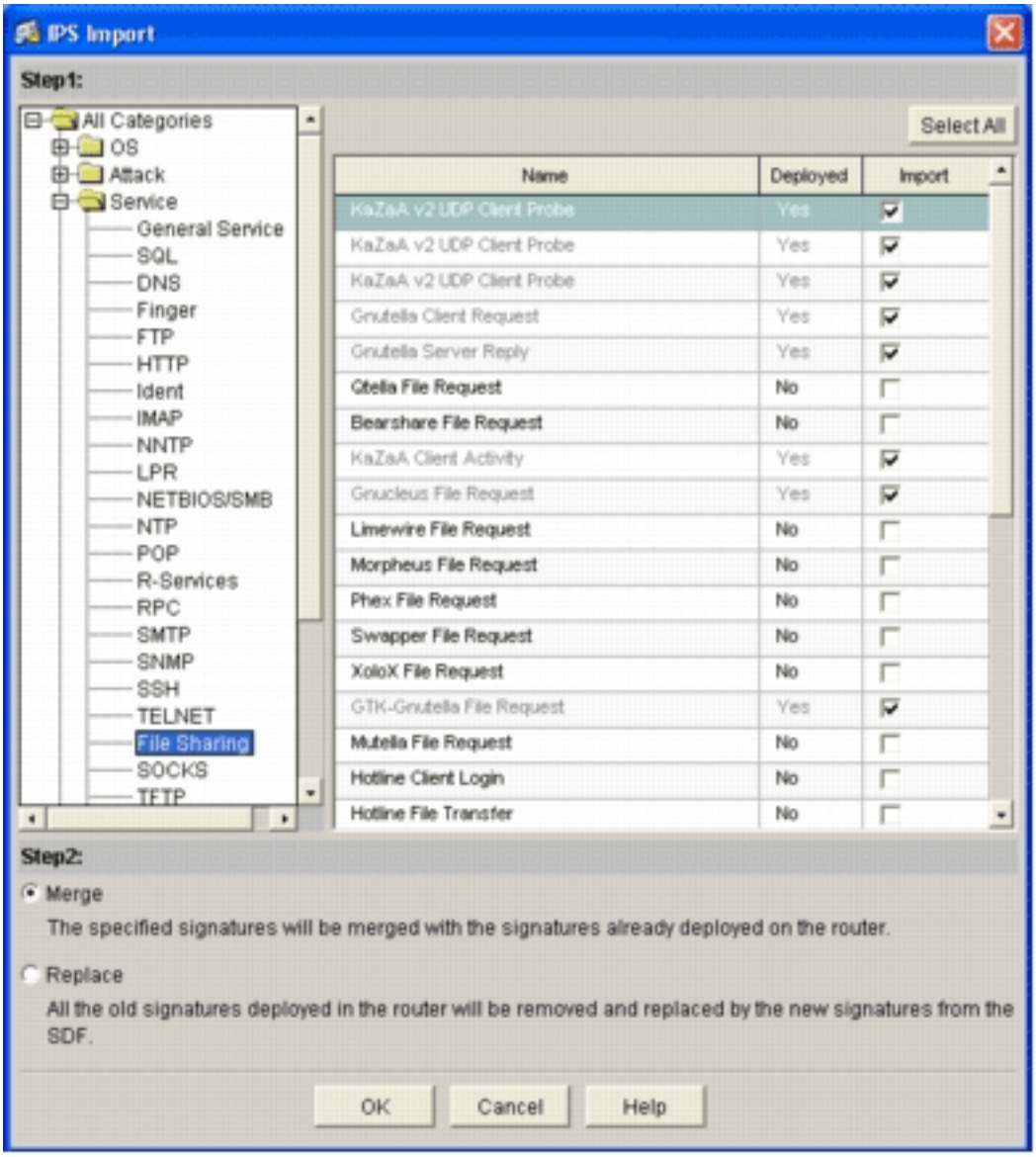
1. 选择默认SDF或IOS-Sxxx.zip更新文件以导入其他签名。
2. 单击**Configure**，然后单击**Intrusion Prevention**。
3. 单击“Edit IPS（**编辑IPS**）”选项卡，然后单击“**Import(导入)**”。



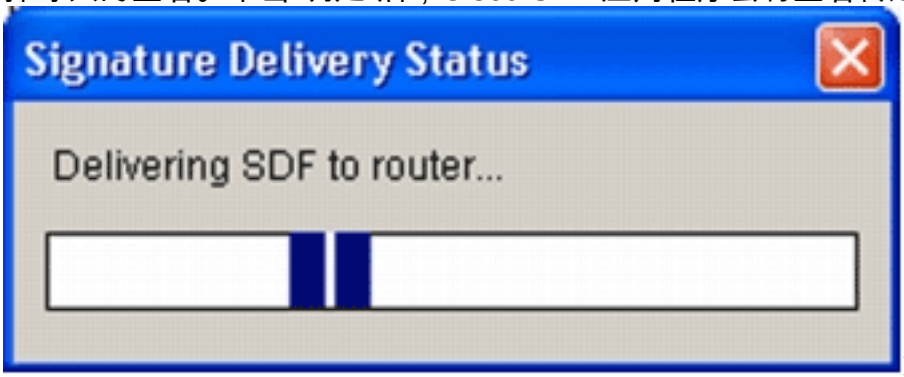
4. 从“导入”下拉列表中选择“从PC”。



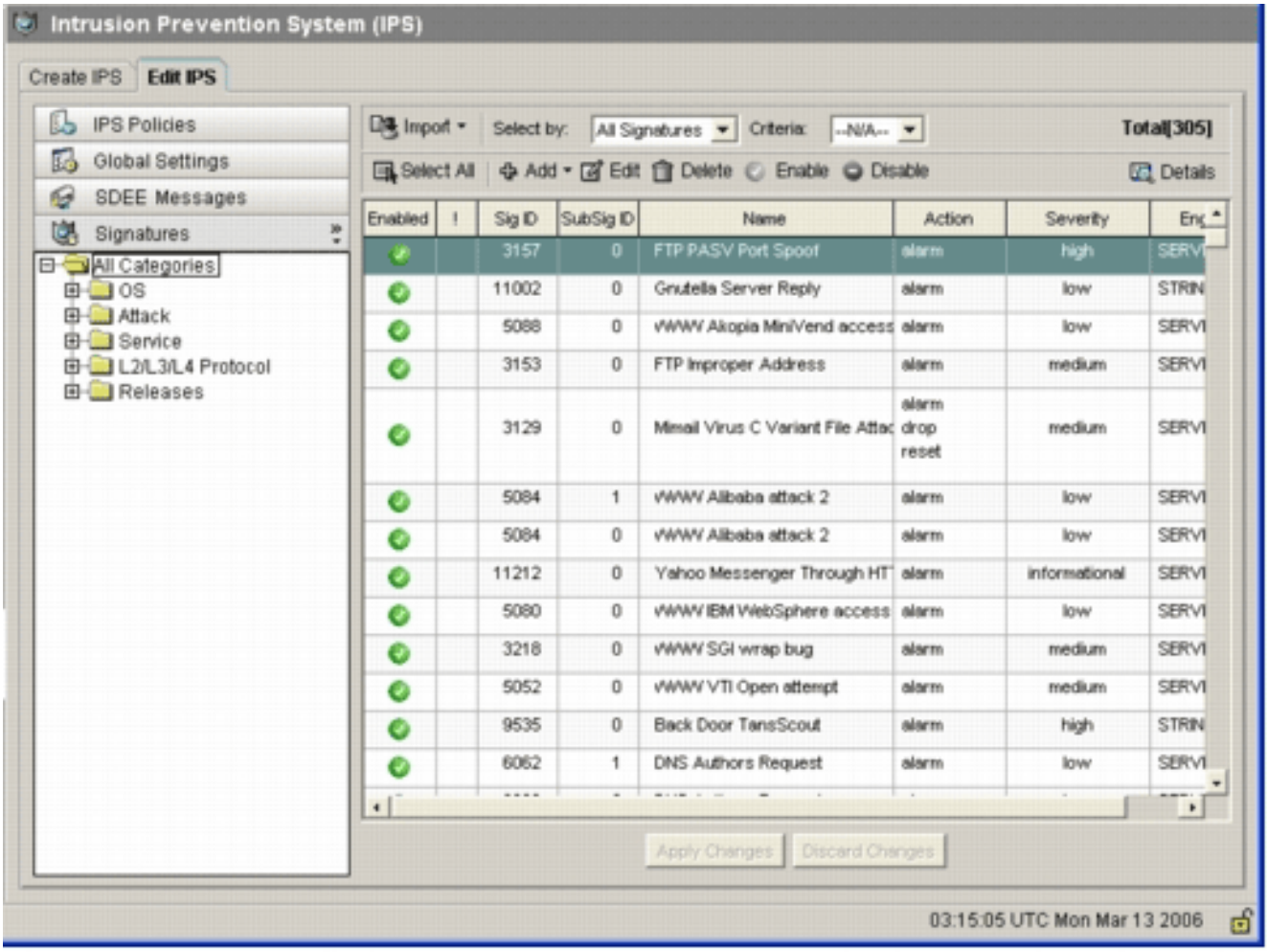
5. 选择要从中导入签名的文件。本示例使用从Cisco.com下载并保存到本地PC硬盘的最新更新。
6. 单击 **Open**（打开）。**警告**：由于内存限制，在已部署的签名之外，只能添加数量有限的新签名。如果选择的签名太多，则路由器可能无法加载所有新签名，因为内存不足。签名文件加载完成后，将显示IPS Import对话框。



7. 在左侧树视图中导航，然后单击要导入的签名旁边的**Import**复选框。
8. 单击“合**并**”单选按钮，然后单击“**确定**”。**注意**：替换选项将路由器上的当前签名集替换为您选择导入的签名。单击“确定”后，Cisco SDM应用程序会将签名传送到路由器。



注意：在编译和加载签名时，CPU使用率较高。在接口上启用Cisco IOS IPS后，签名文件开始加载。路由器加载SDF大约需要五分钟。您可以尝试使用**show process cpu**命令，以从Cisco IOS软件CLI查看CPU利用率。但是，在路由器加载SDF时，请勿尝试使用其他命令或加载其他SDF。这可能导致签名编译过程需要更长的时间才能完成（因为加载SDF时CPU利用率接近100%）。 如果签名未处于启用状态，则可能需要浏览签名列表并启*用*签名。总签名号已增加到519。此编号包括IOS-S193.zip文件中属于文件共享子类别的所有可用签名。



有关如何使用Cisco SDM管理Cisco IOS IPS功能的更多高级主题，请参阅Cisco SDM文档，网址为：

选择签名并使用签名类别

要确定如何有效选择网络的正确签名，您必须了解有关您所保护的网络的一些信息。Cisco SDM 2.2及更高版本中更新的签名类别信息进一步帮助客户选择正确的签名集以保护网络。

类别是对签名进行分组的方法。它有助于将签名选择范围缩小到彼此相关的签名子集。一个签名只能属于一个类别，也可以属于多个类别。

以下是五个顶级类别：

- OS — 基于操作系统的签名分类
- 攻击 — 基于攻击的签名分类
- 服务 — 基于服务的签名分类
- 第2-4层协议 — 基于协议级别的签名分类
- 版本 — 基于版本的签名分类

这些类别中的每个类别进一步划分为子类别。

例如，假设家庭网络具有到Internet的宽带连接和到企业网络的VPN隧道。宽带路由器在与互联网的开放（非VPN）连接上启用了Cisco IOS防火墙，以防止任何连接从互联网发起并连接到家庭网络。允许从家庭网络发往Internet的所有流量。假设用户使用基于Windows的PC并使用HTTP（Web浏览）和电子邮件等应用。

可以配置防火墙，以便仅允许用户需要的应用通过路由器。这将控制可能传播到整个网络的有害和

潜在有害流量的流动。请考虑家庭用户不需要或使用特定服务。如果允许该服务通过防火墙，则攻击可能会利用漏洞在整个网络中传播。最佳实践仅允许所需的服务。现在，选择要启用的签名更加容易。您只需要为允许通过防火墙的服务启用签名。在本例中，服务包括电子邮件和HTTP。Cisco SDM简化了此配置。

要使用类别选择所需的签名，请选择**Service > HTTP**，然后启用所有签名。此选择过程也在签名导入对话框中运行，您可以在其中选择所有HTTP签名并将其导入路由器。

需要选择的其他类别包括DNS、NETBIOS/SMB、HTTPS和SMTP。

更新默认SDF文件的签名

每个构建的三个SDF（attack-drop.dsf、128MB.sdf和256MB.sdf）当前发布在Cisco.com上，网址为http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup(仅限注册客户)。 这些文件的更新版本将在可用时立即发布。要使用这些默认SDF更新运行Cisco IOS IPS的路由器，请访问网站并下载这些文件的最新版本。

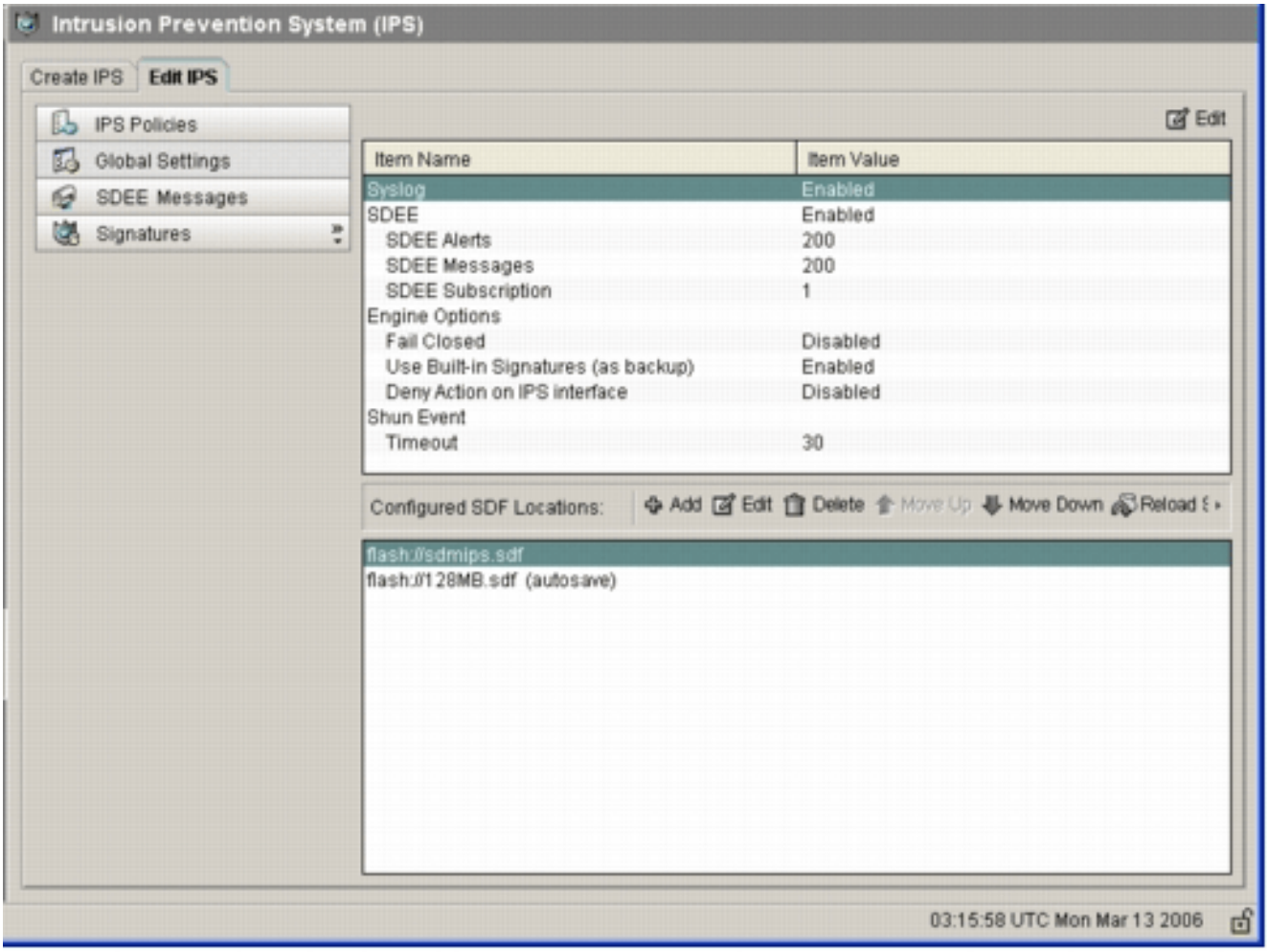
CLI过程

1. 将下载的文件复制到路由器配置为从加载这些文件的位置。要确定路由器当前配置的位置，请使用**show running-config | ip ips sdf**命令。
   ```
   Router#show running-config | in ip ips sdf
   ip ips sdf location flash://256MB.sdf autosave
   ```
   在本例中，路由器在闪存上使用256MB.sdf。将新下载的256MB.sdf复制到路由器闪存时，文件会更新。
2. 重新加载Cisco IOS IPS子系统以运行新文件。重新加载Cisco IOS IPS有两种方法：重新加载路由器或重新配置Cisco IOS IPS以触发IOS IPS子系统重新加载签名。要重新配置Cisco IOS IPS，请从已配置的接口中删除所有IPS规则，然后将IPS规则重新应用回接口。这将触发Cisco IOS IPS系统重新加载。

SDM 2.2程序

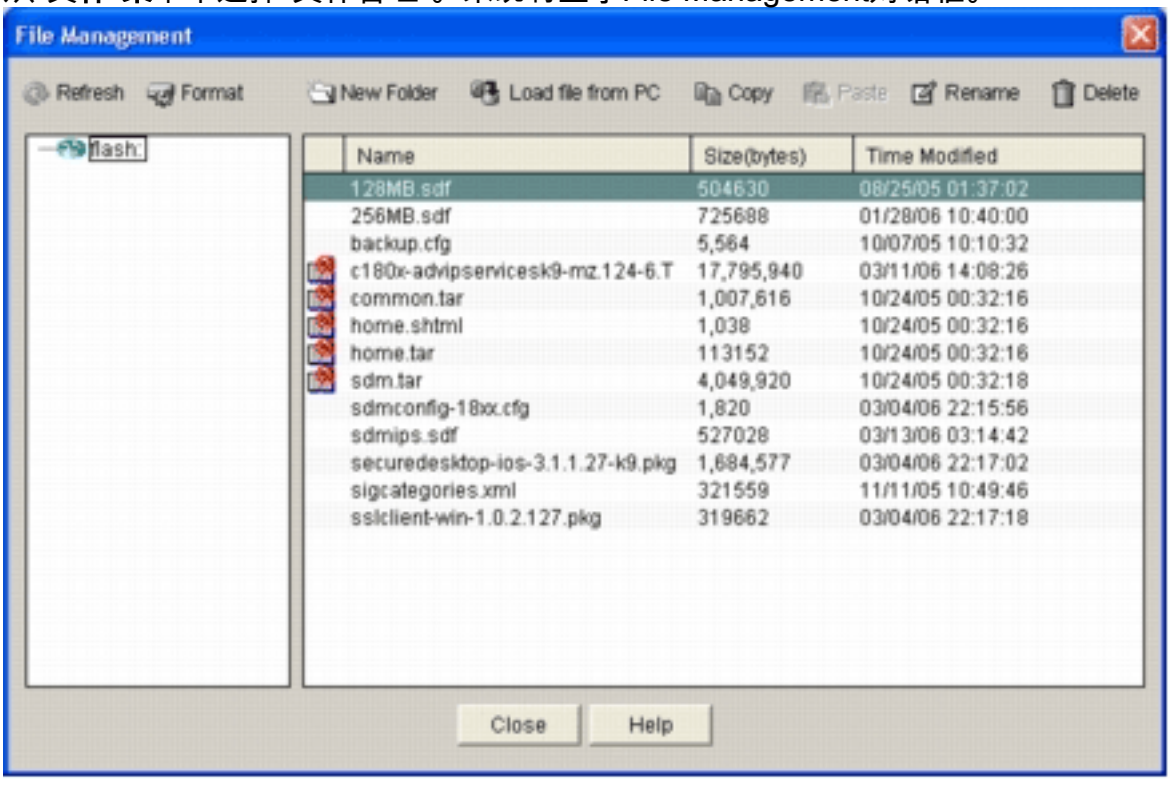
要更新路由器上的默认SDF，请完成以下步骤：

1. 单击**Configure**，然后单击**Intrusion Prevention**。
2. 单击“Edit IPS（**编辑IPS**）”选项卡，然后单击“**Global Settings(全局设置)**”。

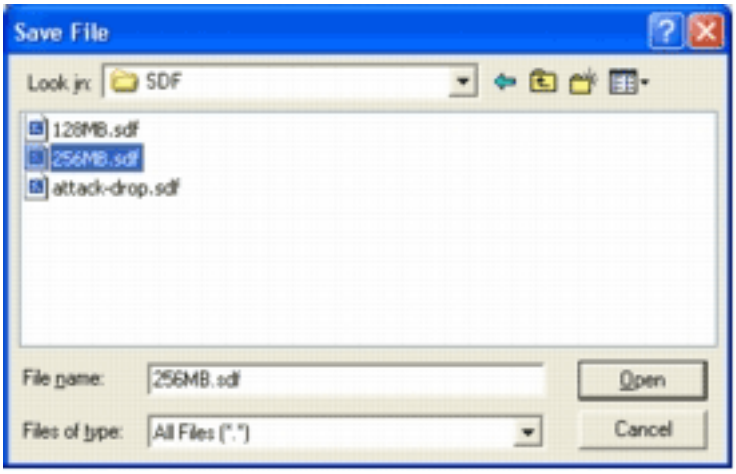


UI顶部显示全局设置。UI的下半部分显示当前配置的SDF位置。在这种情况下，从闪存配置256MB.sdf文件。

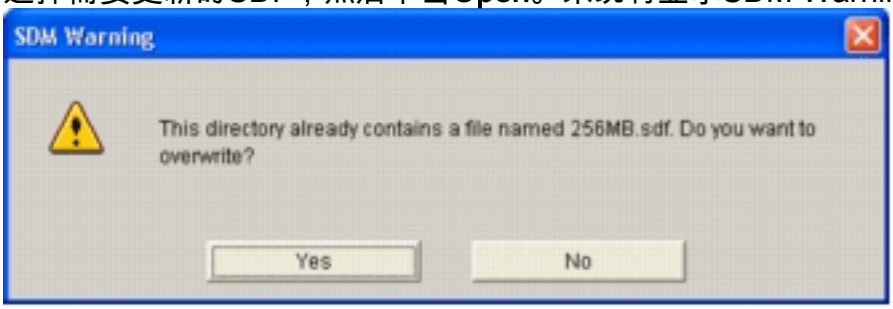
3. 从“文**件”菜**单中选择“文件管理”。系统将显示File Management对话框。



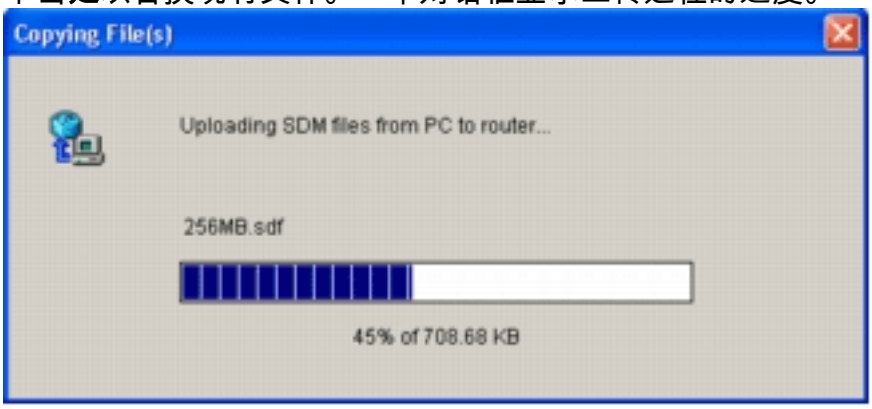
4. 单击**从PC加载文件**。系统将显示“保存文件”对话框。



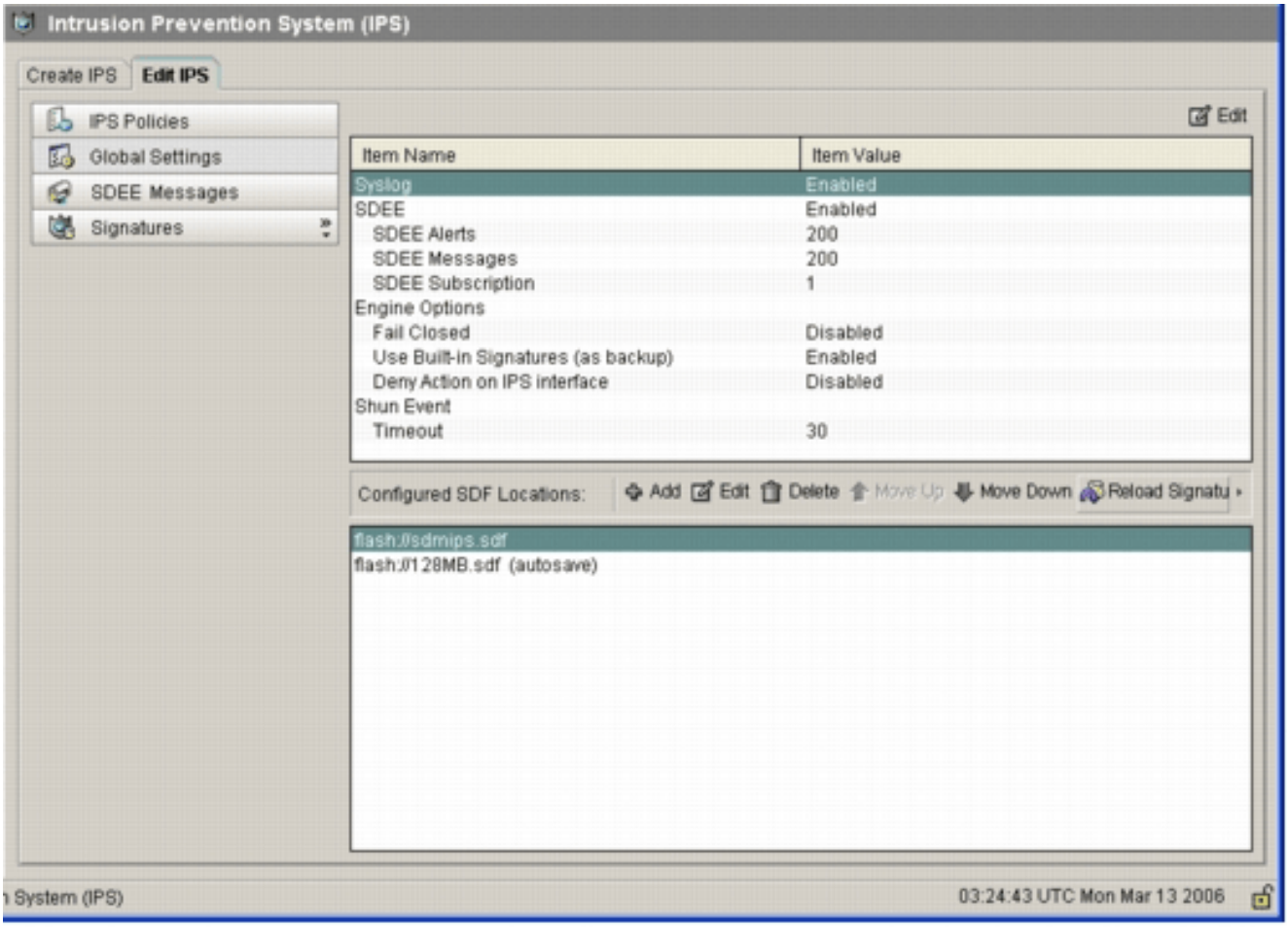
5. 选择需要更新的SDF，然后单击**Open**。系统将显示SDM Warning（SDM警告）消息。



6. 单击**是**以替换现有文件。一个对话框显示上传过程的进度。



7. 完成上传过程后，单击SDF位**置工**具栏上的重新加载签名。此操作将重新加载Cisco IOS IPS。



注意：IOS-Sxxx.zip软件包包含Cisco IOS IPS支持的所有签名。此签名包的升级一经发布，即会发布到Cisco.com上。要更新此包中包含的签名，请参阅步骤2。

相关信息

- 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