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

目錄

簡介

在Cisco Router and Security Device Manager(SDM)2.2中，Cisco IOS® IPS配置整合到SDM應用程式中。您不再需要啟動單獨的視窗來配置Cisco IOS IPS。

在Cisco SDM 2.2中，一個新的IPS配置嚮導將引導您完成在路由器上啟用Cisco IOS IPS的必要步驟。此外，您仍然可以使用高級配置選項來啟用、禁用和調整使用Cisco SDM 2.2的Cisco IOS IPS。

思科建議您使用預調的簽名定義檔案(SDF)運行Cisco IOS IPS:attack-drop.sdf、128MB.sdf和256MB.sdf。這些檔案是為具有不同記憶體量的路由器建立的。這些檔案與Cisco SDM捆綁在一起，後者在您首次在路由器上啟用Cisco IOS IPS時建議使用SDF。這些檔案也可從http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup(僅限註冊客戶)下載。

使用出廠預設SDF啟用Cisco IOS IPS 中詳細說明了啟用預設SDF的流程。如果預設SDF不足，或者您想新增新簽名，則可以使用啟用預設SDF後附加其他簽名中介紹的步驟。

必要條件

需求

使用Cisco SDM 2.2需要Java Runtime Environment(JRE)1.4.2版或更高版本。Cisco推薦和最佳化的簽名檔案（基於DRAM）與Cisco SDM捆綁在一起（使用Cisco SDM載入到路由器快閃記憶體上）。

採用元件

本檔案中的資訊是根據Cisco路由器和安全裝置管理員(SDM)2.2。

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

使用出廠預設SDF啟用Cisco IOS IPS

CLI程式

完成以下步驟，以便使用CLI將採用Cisco IOS IPS的Cisco 1800系列路由器配置為在路由器快閃記憶體上載入128MB.sdf。

1. 配置路由器以啟用安全裝置事件交換(SDEE)事件通知。
   ```
   yourname#conf t
   ```

2. 輸入配置命令（每行一個），然後按Cntl+Z結束。
   ```
   yourname(config)#ip ips notify sdee
   ```

3. 建立用於與介面關聯的IPS規則名稱。
   ```
   yourname(config)#ip ips name myips
   ```

4. 配置IPS位置命令以指定Cisco IOS IPS系統將從哪個檔案讀取簽名。此範例使用快閃記憶體上的檔案：128MB.sdf。此命令的位置URL部分可以是通過FTP、HTTP、HTTPS、RTP、SCP和TFTP使用快閃記憶體、磁碟或協定以指向檔案的任何有效URL。
   ```
   yourname(config)#ip ips sdf location flash:128MB.sdf
   ```

   注意：如果通過Telnet會話配置路由器，或者建立簽名引擎時不會看到SDEE消息，則必須啟用**terminal monitor**命令。
5. 在要啟用Cisco IOS IPS以掃描流量的介面上啟用IPS。在本例中，我們在介面fastEthernet 0的兩個方向上都啟用了。
   ```
   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
```

首次將IPS規則應用於介面時，Cisco IOS IPS會從SDF locations命令指定的檔案啟動生成的特徵碼。SDEE消息會記錄到控制檯並傳送到系統日誌伺服器（如果已配置）。帶有*<number>*個引擎的*<number>*個*引擎的SDEE消息*指示簽名引擎構建過程。最後，當兩個數值相同時，所有的引擎都建立起來。**注意：**IP虛擬重組是一種介面功能，它會（在開啟時）自動重組通過該介面進入路由器的分段資料包。思科建議您在所有流量進入路由器的介面上啟用ip virtual-assembly。在上方範例中，除了在介面fastEthernet 0上開啟「ip virtual-assembly」外

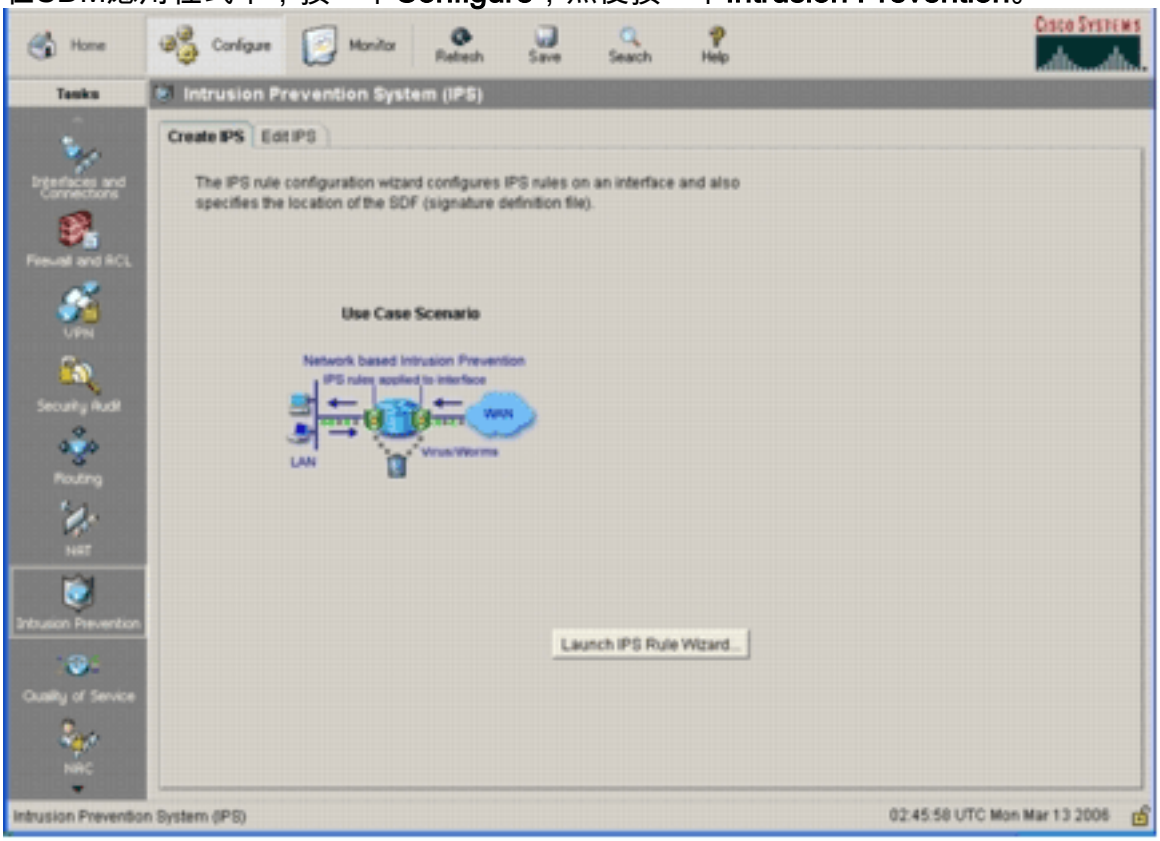
，我們還會在內部介面VLAN 1上設定該裝置。

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

SDM 2.2程式

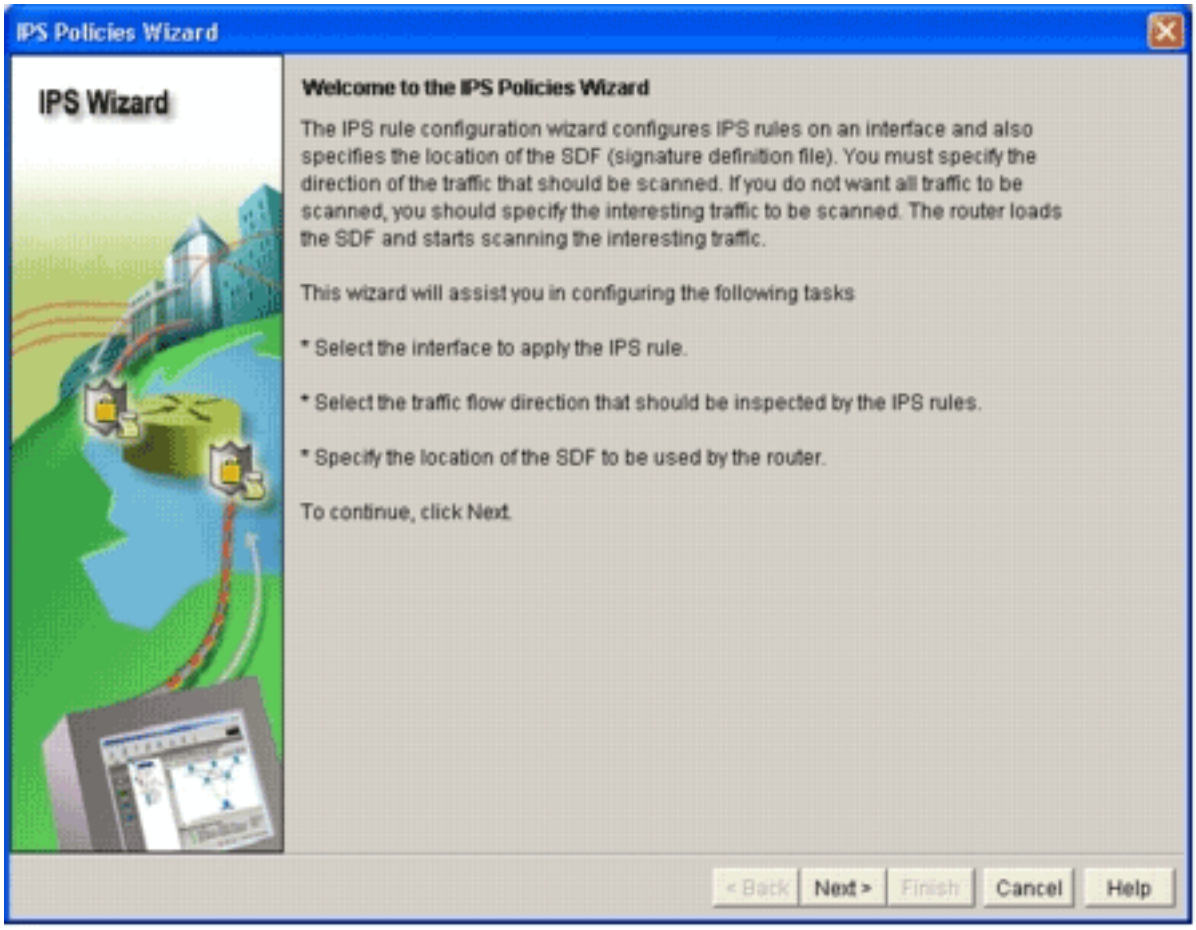
完成以下步驟，以便使用Cisco SDM 2.2配置帶有Cisco IOS IPS的Cisco 1800系列路由器。

1. 在SDM應用程式中，按一下**Configure**，然後按一下**Intrusion Prevention**。



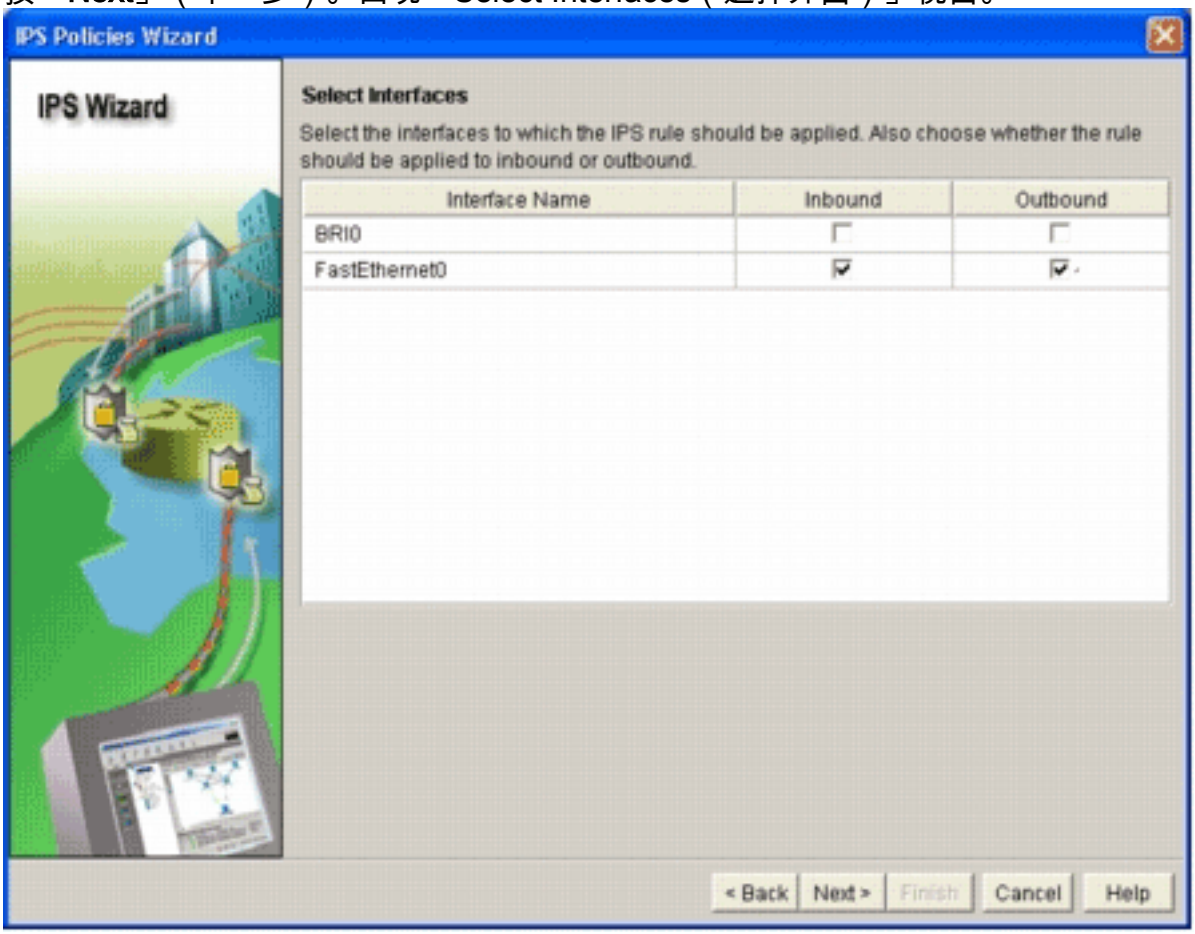
2. 按一下**Create IPS**頁籤，然後按一下**Launch IPS Rule Wizard**。Cisco SDM需要通過SDEE發出IPS事件通知，以便配置Cisco IOS IPS功能。預設情況下，SDEE通知未啟用。Cisco SDM提示您通過SDEE啟用IPS事件通知，如下圖所示：

3. 按一下「**OK**」（確定）。系統將顯示IPS策略嚮導對話方塊的「歡迎使用IPS策略嚮導」視窗



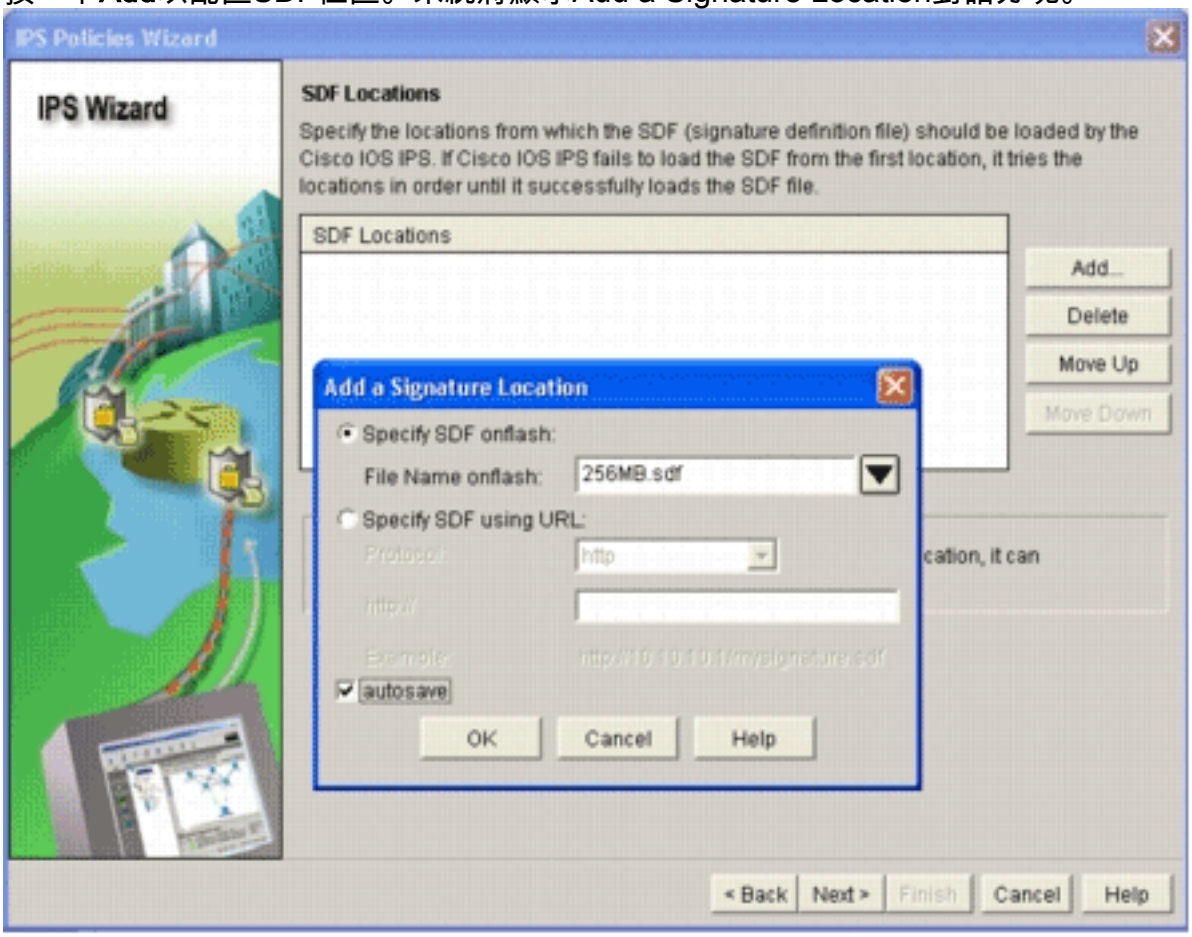
。

4. 按「**Next**」（下一步）。出現「Select Interfaces（選擇介面）」視窗。

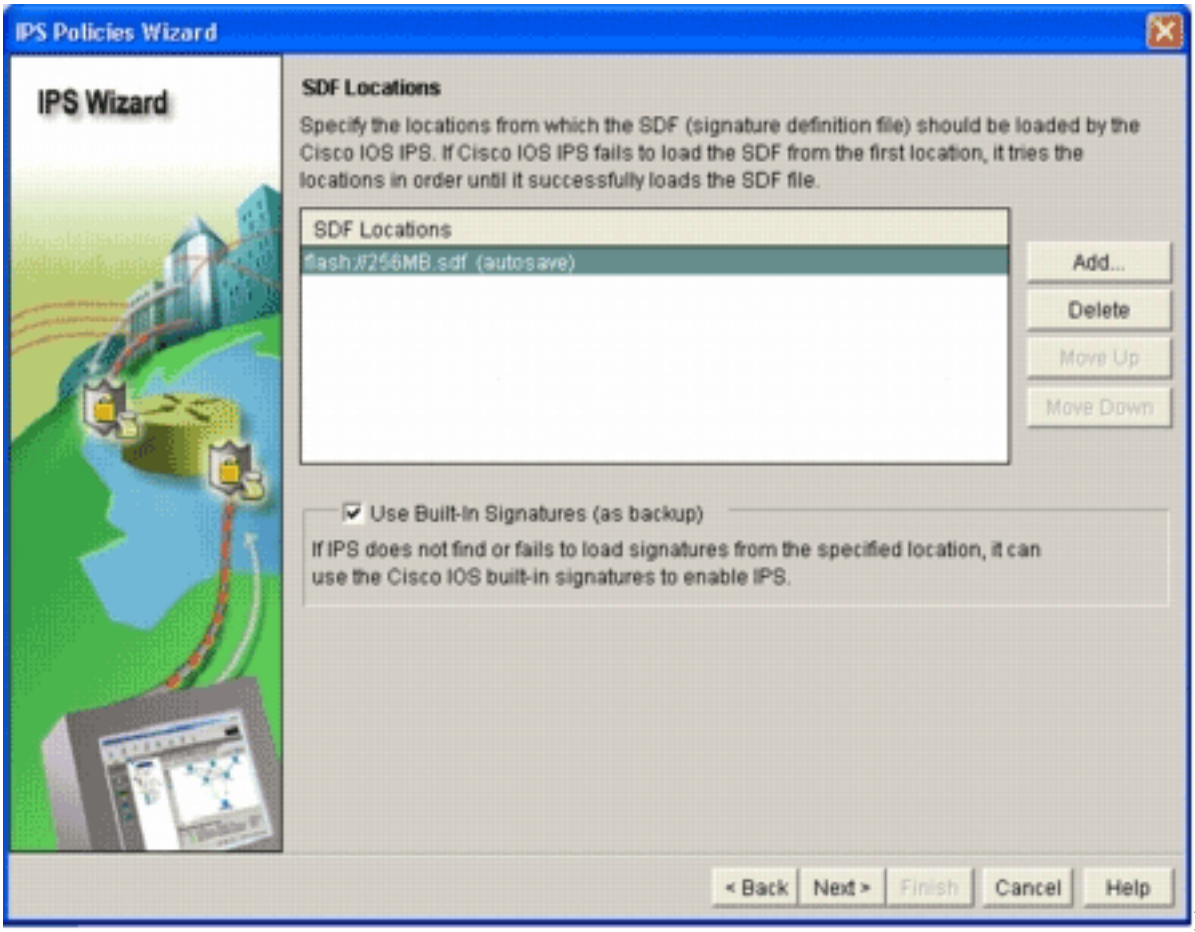


5. 選擇要為其啟用IPS的介面，然後按一下**Inbound**或**Outbound**覈取方塊以指示該介面的方向。
   注意：在介面上啟用IPS時，思科建議您同時啟用入站和出站方向。
6. 按「**Next**」（下一步）。出現「SDF位置」(SDF Locations)視窗。

7. 按一下**Add**以配置SDF位置。系統將顯示Add a Signature Location對話方塊。

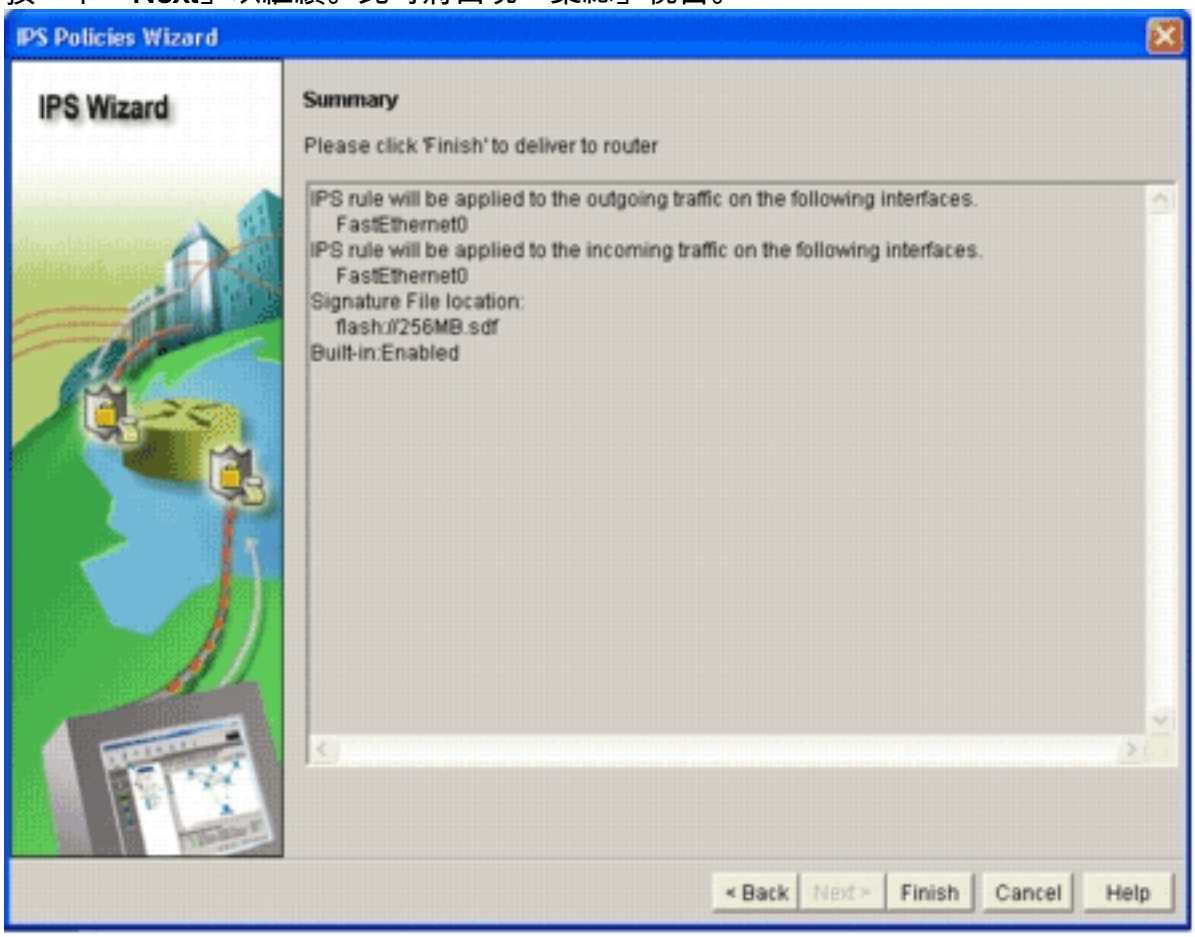


8. 按一下**Specify SDF on flash**單選按鈕，然後從**File Name on flash**下拉選單中選擇256MB.sdf。
9. 按一下**autosave**覈取方塊，然後按一下**OK**。**附註：** 自動儲存選項會在簽名更改時自動儲存簽名檔案。「SDF位置」(SDF Locations)視窗顯示新的SDF位置。

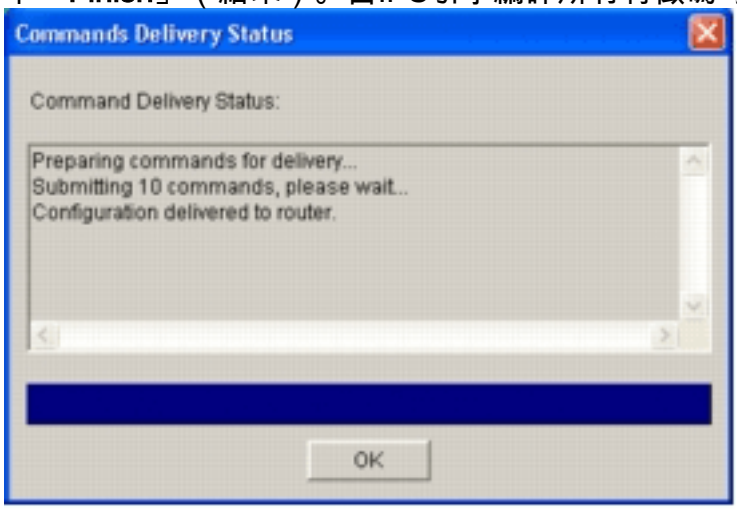


注意：您可以新增其他簽名位置以指定備份。

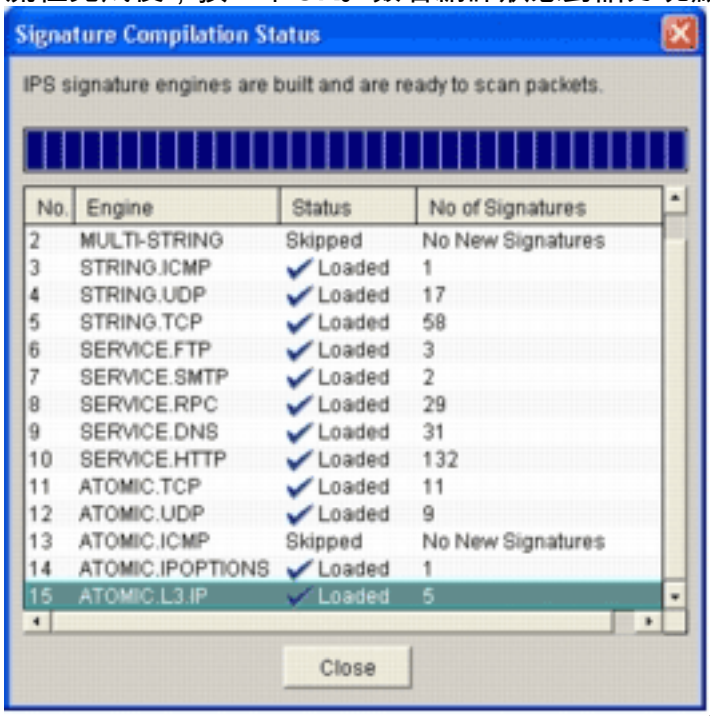
10. 按一下**Use Built-In Signatures(as backup)**覈取方塊。**注意**：思科建議您不要使用內建簽名選項，除非您已指定一個或多個位置。
11. 按一下「**Next**」以繼續。此時將出現「彙總」視窗。



12. 按一下「**Finish**」（結束）。當IPS引擎編譯所有特徵碼時，命令傳送狀態對話方塊會顯示狀態。

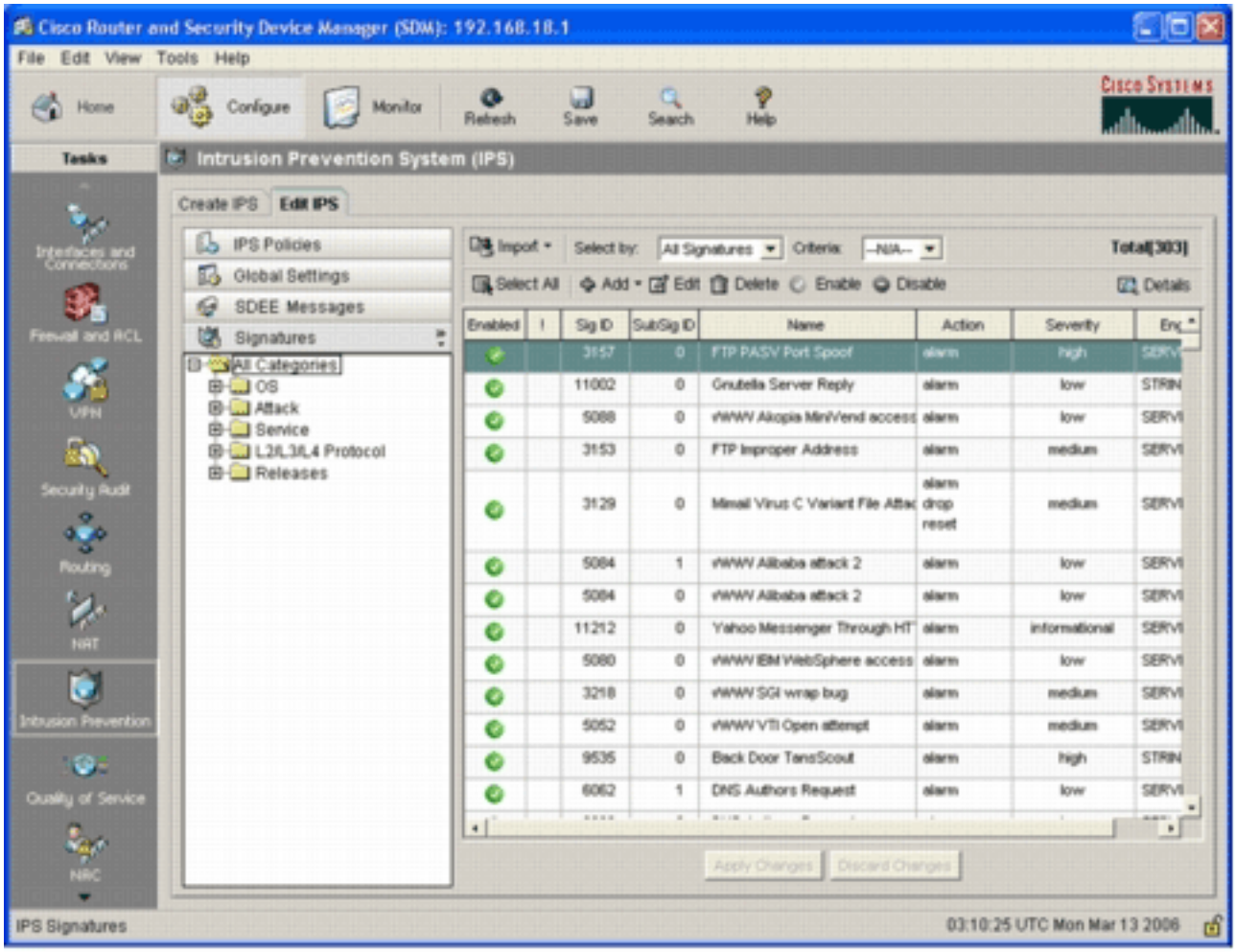


13. 流程完成後，按一下**OK**。簽名編譯狀態對話方塊顯示簽名編譯資訊。



此資訊顯示已編譯的引擎以及該引擎中的簽名數。對於在狀態列中顯示*Skipped*的引擎，沒有為該引擎載入簽名。

14. 按一下**關閉**以關閉「簽名編譯狀態」對話方塊。
15. 若要驗證路由器上當前載入了哪些簽名，請按一下**Configure**，然後按一下**Intrusion Prevention**。
16. 按一下**Edit IPS**頁籤，然後按一下**Signatures**。IPS特徵碼清單將顯示在「特徵碼」視窗中。



啟用預設SDF後附加其他簽名

CLI程式

沒有CLI命令可用於建立簽名或從分散式IOS-Sxxx.zip檔案中讀取簽名資訊。Cisco建議您使用SDM或Management Center for IPS Sensors來管理Cisco IOS IPS系統上的簽名。

對於已經準備好特徵碼檔案並希望將此檔案與在Cisco IOS IPS系統上運行的SDF合併的客戶，可以使用以下命令：

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

signature location命令定義的特徵碼檔案是路由器在重新載入或重新配置路由器IOS IPS時載入特徵碼檔案的位置。要使合併過程成功，還必須更新由signature file location命令定義的檔案。

1. 使用**show**命令檢查當前配置的簽名位置。輸出顯示了配置的簽名位置。此命令顯示當前運行簽名的載入位置。

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

   上次從flash:128MB.sdf載入簽名Cisco SDF版本S128.0趨勢SDF版本V0.0
2. 使用**copy** ***<url>*** ips-sdf命令以及上一步中的資訊來合併簽名檔案。

   ```
   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#
```

在您發出**copy**命令後，路由器將簽名檔案載入到記憶體中，然後構建簽名引擎。在控制檯SDEE消息輸出中，顯示每個特徵碼引擎的生成狀態。%IPS-6-ENGINE_BUILD_SKIPPED表示此引擎沒有新簽名。%IPS-6-ENGINE_READY表示存在新簽名，引擎已準備就緒。與以前一樣，「15個引擎中的15個」消息表示所有引擎均已構建。IPS-7-UNSUPPORTED_PARAM表示Cisco IOS IPS不支援某個引數。例如CapturePacket和ResetAfterIdle。**附註：** 這些消息僅供參考，不會影響Cisco IOS IPS簽名功能或效能。可以通過將日誌記錄級別設定為高於調試（級別7）來關閉這些日誌記錄消息。

3. 更新由signature location命令定義的SDF，這樣，當路由器重新載入時，它將具有帶有已更新簽名的合併簽名集。此範例顯示將合併的簽章儲存到128MB.sdf快閃檔案中後的檔案大小差異。

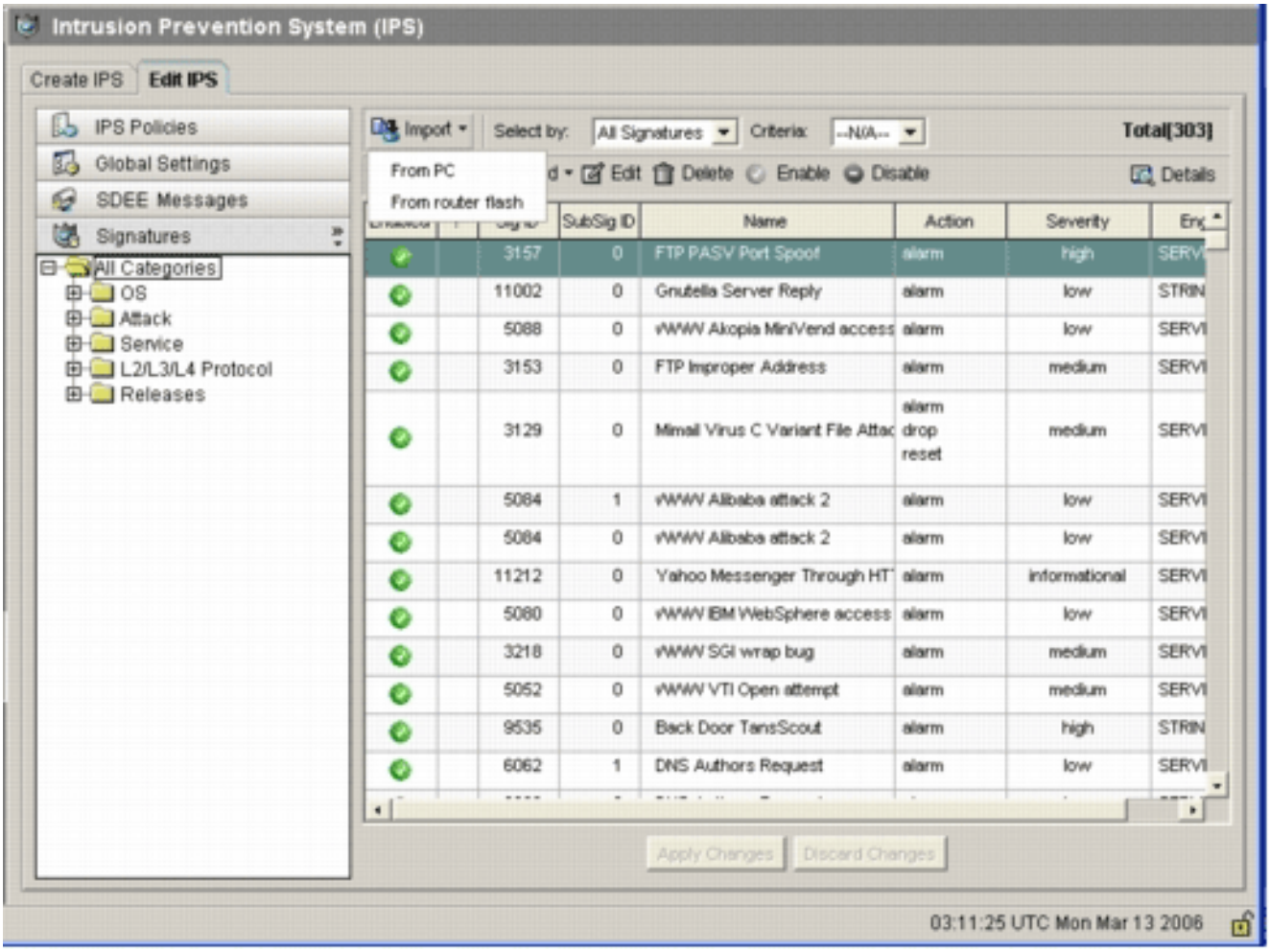
```
yourname#show flash:
-#- --length-- -----date/time------ path
4 504630 Aug 30 2005 22:58:34 +00:00 128MB.sdf
yourname#copy ips-sdf flash:128MB.sdf
yourname#show flash:
-#- --length-- -----date/time------ path
4 522656 Oct 26 2005 02:51:32 +00:00 128MB.sdf
```

警告：新的128MB.sdf現在包含客戶合併的簽名。內容與思科預設128MB.sdf檔案不同。思科建議您將此檔案更改為其他名稱以避免混淆。如果更改了名稱，則還需要更改簽名位置命令。

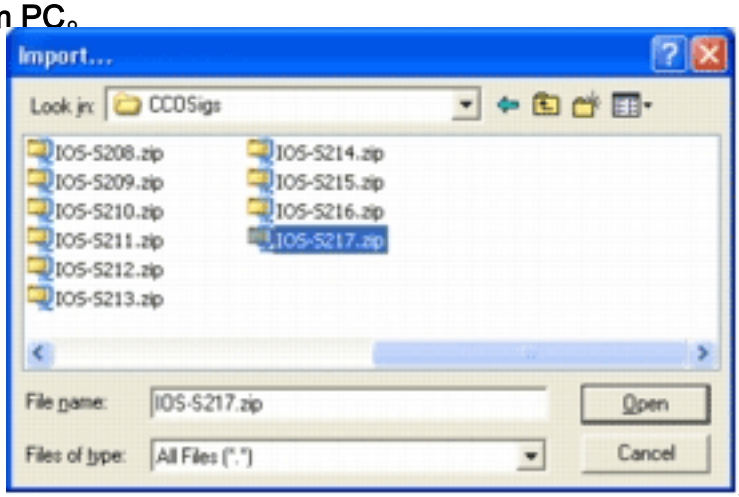
SDM 2.2程式

啟用Cisco IOS IPS後，可以將新簽名新增到運行具有Cisco SDM匯入功能的簽名集的路由器中。完成以下步驟以匯入新簽名：

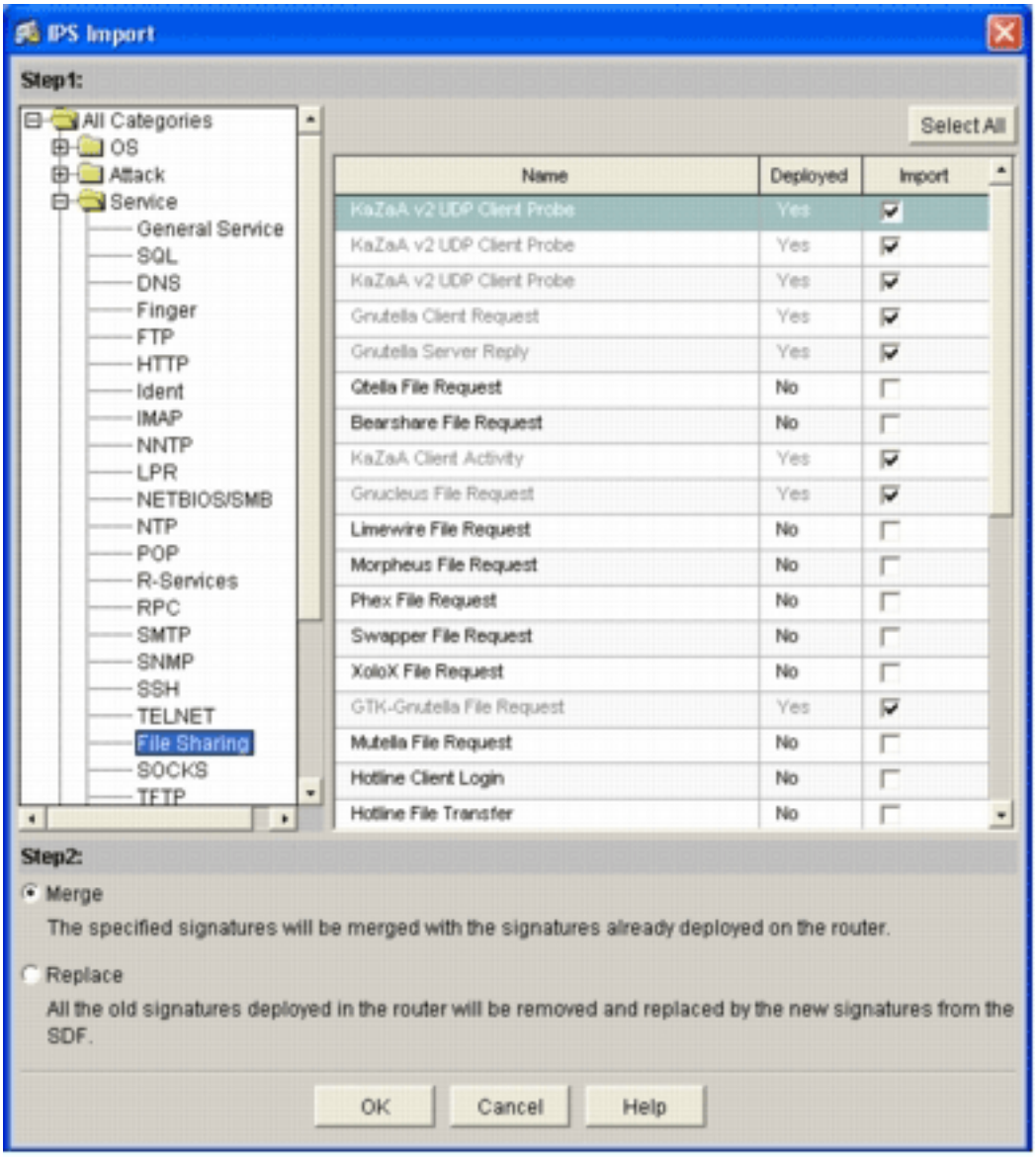
1. 選擇預設SDF或IOS-Sxxx.zip更新檔案以匯入其他簽名。
2. 按一下**Configure**，然後按一下**Intrusion Prevention**。
3. 按一下**Edit IPS**頁籤，然後按一下**Import**。



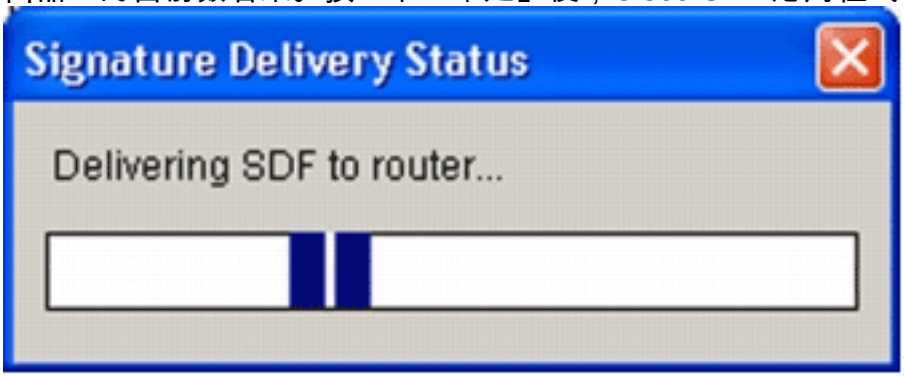
4. 從Import下拉選單中選擇**From PC**。



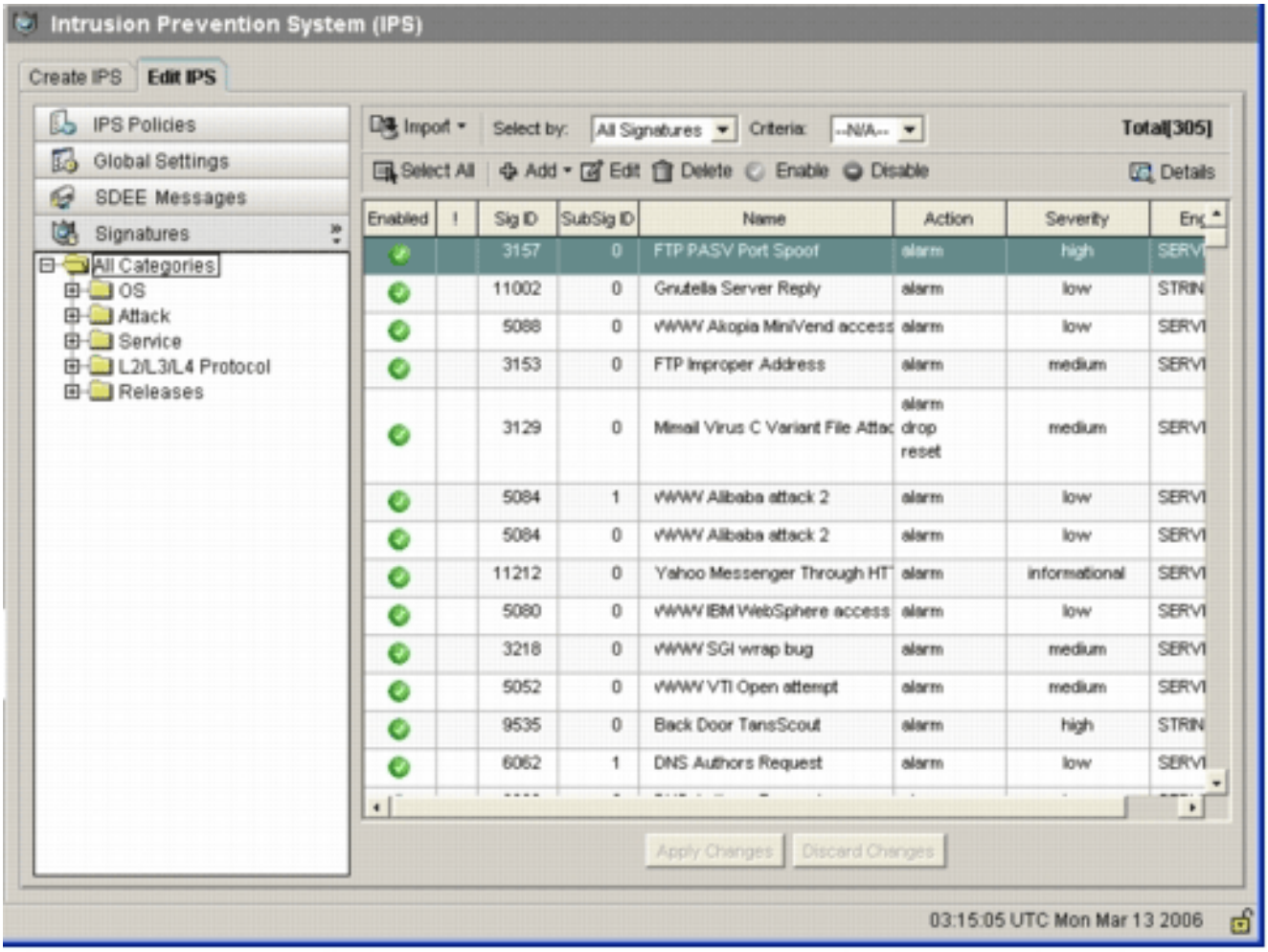
5. 選擇要從中匯入簽名的檔案。此示例使用從Cisco.com下載並儲存在本地PC硬碟上的最新更新。
6. 按一下「**Open**」。**警告**：由於記憶體限制，只能在已部署的簽名之上新增有限數量的新簽名。如果選擇了太多簽名，則由於記憶體不足，路由器可能無法載入所有新簽名。簽名檔案載入完成後，將出現IPS匯入對話方塊。



7. 在左側的樹檢視中進行導航，然後按一下要匯入的簽名旁邊的**Import**覈取方塊。
8. 按一下**Merge**單選按鈕，然後按一下**OK**。**注意：**Replace選項使用您選擇要匯入的簽名替換路由器上的當前簽名集。按一下「確定」後，Cisco SDM應用程式會將簽名傳送到路由器。



注意：在編譯和載入簽名期間出現CPU使用率較高。在介面上啟用Cisco IOS IPS後，開始載入簽名檔案。路由器大約需要5分鐘來載入SDF。您可以嘗試使用**show process cpu**命令從Cisco IOS軟體CLI檢視CPU使用率。但是，在路由器載入SDF時，請勿嘗試使用其他命令或載入其他SDF。這可能導致簽名編譯過程需要較長時間才能完成（因為在載入SDF時，CPU利用率接近100%的利用率）。 您可能需要瀏覽簽名清單，並在簽名未處於*enabled*狀態時啟用它們。簽名總數已增加到519。此數字包括屬於「檔案共用」子類別的IOS-S193.zip檔案中可用的所有簽名。



有關如何使用Cisco SDM管理Cisco IOS IPS功能的更多高級主題，請參閱以下URL中的Cisco SDM文檔：

選擇簽名和使用簽名類別

為了確定如何有效地為網路選擇正確的簽名，您必須瞭解要保護的網路的一些資訊。在Cisco SDM 2.2及更高版本中更新的特徵碼類別資訊進一步幫助客戶選擇正確的特徵碼集來保護網路。

類別是一種對簽名進行分組的方法。它有助於將簽名選擇縮小到彼此相關的簽名子集。一個簽名只能屬於一個類別或者可以屬於多個類別。

以下為五個頂級類別：

- 作業系統 — 基於作業系統的簽名分類
- 攻擊 — 基於攻擊的簽名分類
- 服務 — 基於服務的簽名分類
- 第2-4層協定 — 基於協定級別的簽名分類
- 版本 — 基於版本的簽名分類

這些類別中的每一類被進一步劃分為子類別。

例如，假設家庭網路具有到Internet的寬頻連線以及到企業網路的VPN隧道。寬頻路由器在與Internet的開放式（非VPN）連線上啟用了Cisco IOS防火牆，以防止任何連線從Internet發起並連線到家庭網路。所有從家庭網路到Internet的流量都允許通過。假設使用者使用基於Windows的PC並使用HTTP（Web瀏覽）和電子郵件等應用程式。

可以對防火牆進行配置，以便僅允許使用者需要的應用通過路由器。這將控制可能在整個網路中傳

播的不需要的和可能有害的流量。假設家庭使用者不需要或使用特定服務。如果允許該服務流經防火牆，則存在供攻擊用於流經網路的潛在漏洞。最佳實踐僅允許所需的服務。現在，更容易選擇要啟用的簽名。您只需要為允許通過防火牆的服務啟用簽名。在本示例中，服務包括電子郵件和HTTP。Cisco SDM簡化了此配置。

若要使用類別選擇所需的簽名，請選擇**Service > HTTP**，然後啟用所有簽名。此選擇過程還可用於特徵碼匯入對話方塊，您可以在其中選擇所有HTTP特徵碼並將其匯入路由器。

需要選擇的其他類別包括DNS、NETBIOS/SMB、HTTPS和SMTP。

更新預設SDF檔案的簽名

三個依照建的SDF（attack-drop.dsf、128MB.sdf和256MB.sdf）目前發佈在Cisco.com上，網址為http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup(僅限註冊客戶)。 這些檔案的較新版本將在可用時發佈。若要更新使用這些預設SDF執行Cisco IOS IPS的路由器，請前往網站並下載這些檔案的最新版本。

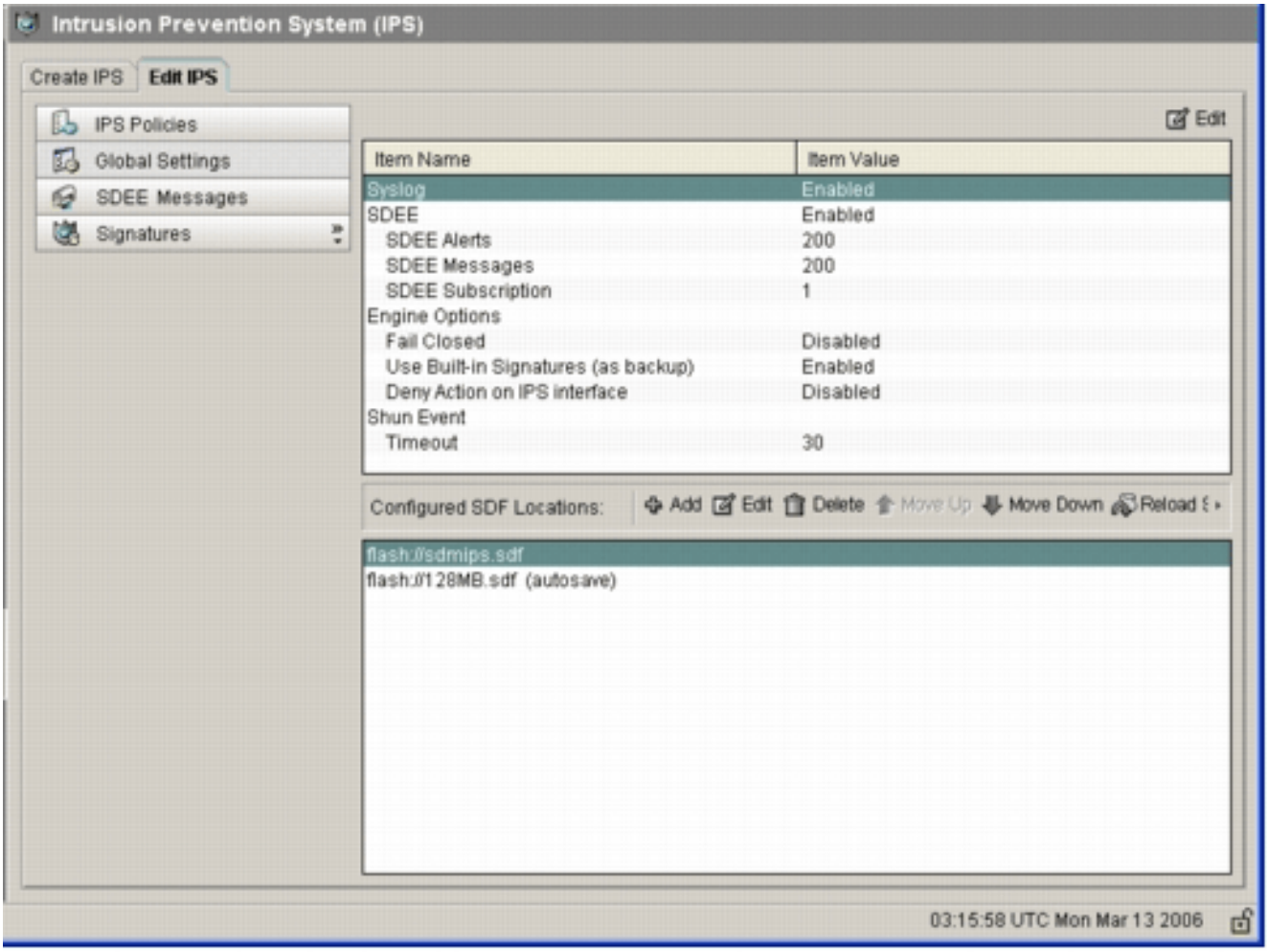
CLI程式

1. 將下載的檔案複製到路由器設定為從其中載入這些檔案的位置。要瞭解路由器當前配置的位置，請使用**show running-config |在ip ips sdf命令**中。
   ```
   Router#show running-config | in ip ips sdf
   ip ips sdf location flash://256MB.sdf autosave
   ```
   在本範例中，路由器在快閃記憶體上使用256MB.sdf。將新下載的256MB.sdf複製到路由器快閃記憶體時，檔案會更新。
2. 重新載入Cisco IOS IPS子系統以運行新檔案。重新載入Cisco IOS IPS有兩種方式：重新載入路由器或重新配置Cisco IOS IPS以觸發IOS IPS子系統來重新載入簽名。若要重新配置Cisco IOS IPS，請從已配置的介面刪除所有IPS規則，然後重新將IPS規則應用到介面。這將觸發Cisco IOS IPS系統重新載入。

SDM 2.2程式

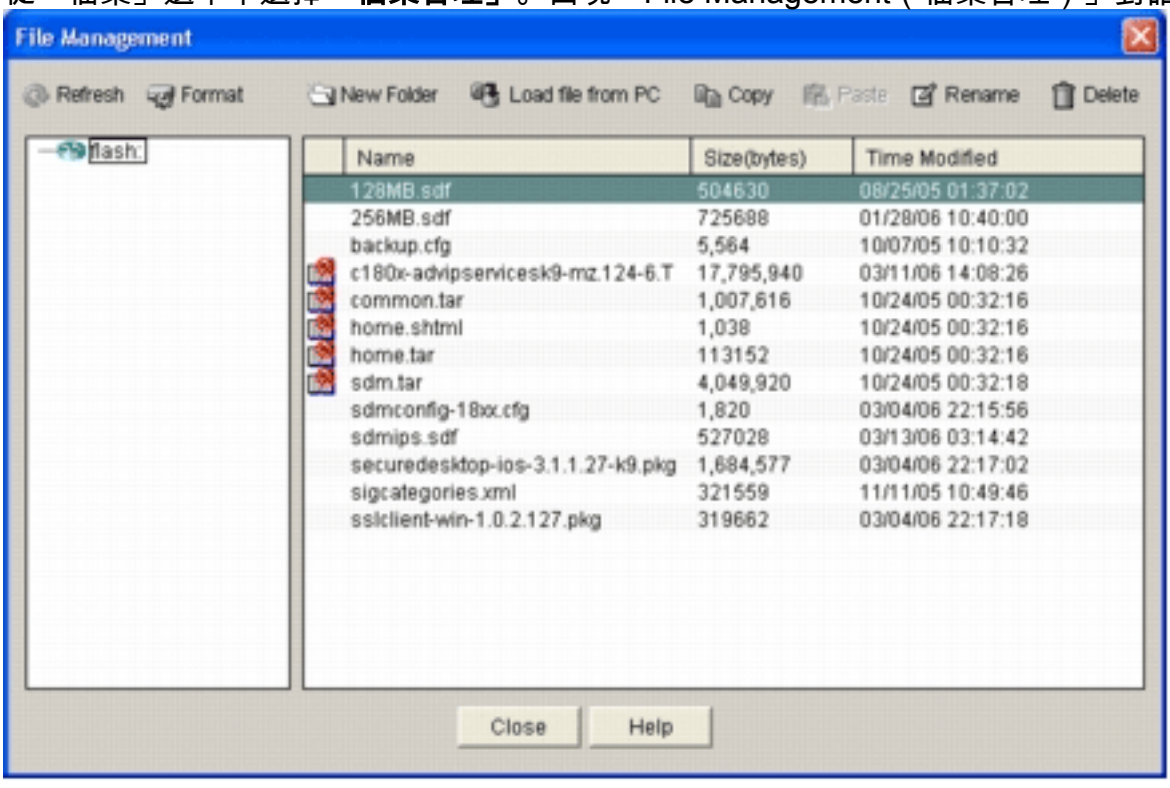
完成以下步驟，更新路由器上的預設SDF:

1. 按一下**Configure**，然後按一下**Intrusion Prevention**。
2. 按一下**Edit IPS**頁籤，然後按一下**Global Settings**。

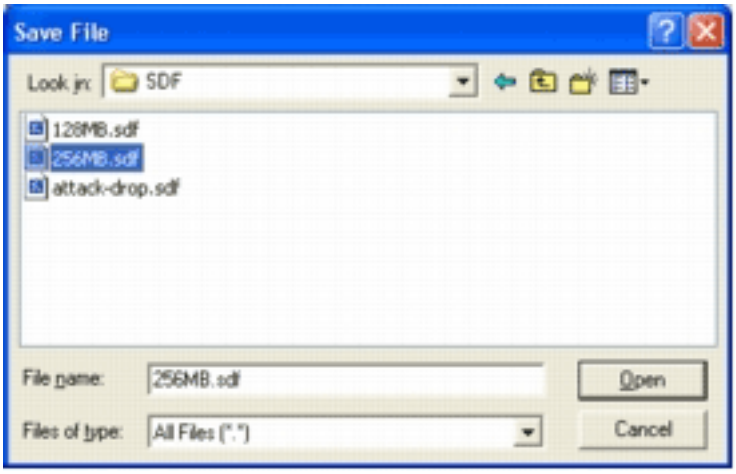


UI頂部顯示全域性設定。UI的下半部分顯示當前配置的SDF位置。在這種情況下，會配置快閃記憶體中的256MB.sdf檔案。

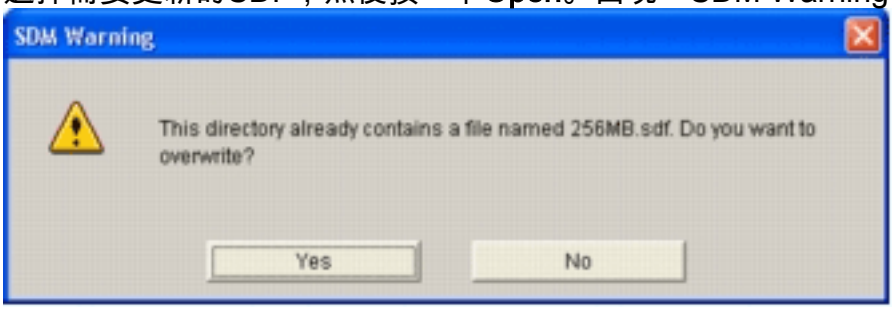
3. 從「檔案」選單中選擇**「檔案管理」**。出現「File Management（檔案管理）」對話方塊。



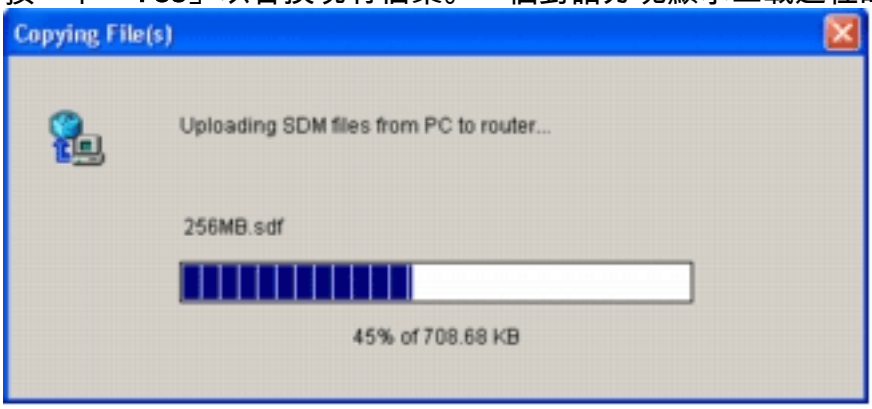
4. 按一下**Load file from PC**。將出現「儲存檔案」對話方塊。



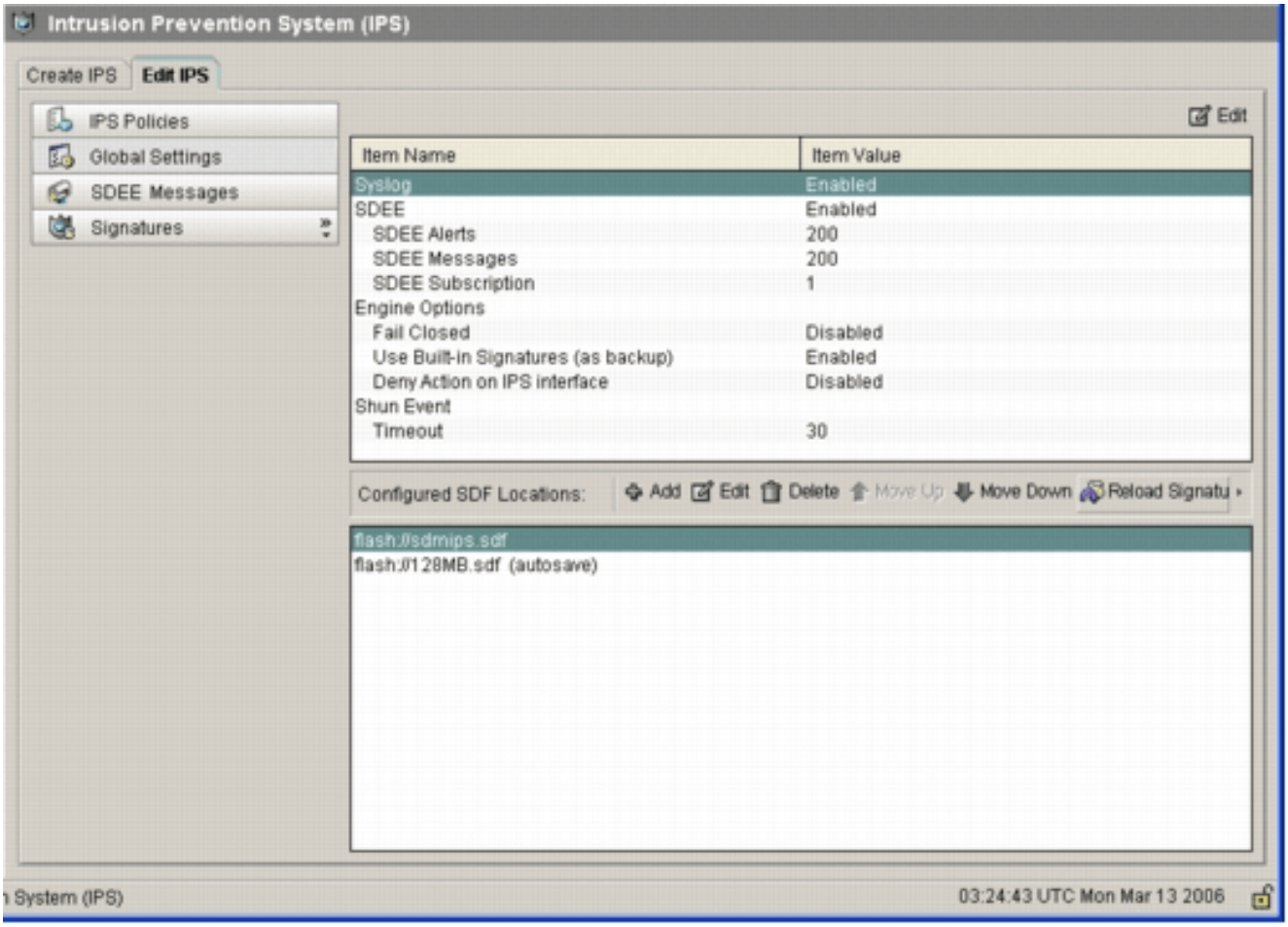
5. 選擇需要更新的SDF，然後按一下**Open**。出現「SDM Warning（SDM警告）」資訊。



6. 按一下「**Yes**」以替換現有檔案。一個對話方塊顯示上載過程的進度。



7. 上傳過程完成後，按一下SDF位置工具欄上的**Reload Signatures**。此操作將重新載入Cisco IOS IPS。



註：IOS-Sxxx.zip軟體包包含Cisco IOS IPS支援的所有簽名。此簽名包的升級一旦發佈，就會在Cisco.com上發佈。若要更新此程式包中包含的簽名，請參閱步驟2。

相關資訊

- 思科入侵防禦系統
- 安全產品現場通知（包括CiscoSecure Intrusion Detection）
- 技術支援 - Cisco Systems