Router and Security Device Manager in Cisco IOS Intrusion Prevention System Configuration Example

Document ID: 105627

Contents

Introduction

This document describes how to use Cisco Router and Security Device Manager (SDM) version 2.5 in order to configure Cisco IOS® Intrusion Prevention System (IPS) in 12.4(15)T3 and later releases.

The enhancements in SDM 2.5 related to IOS IPS are:

- Total compiled signature number displayed in the signature list GUI
- SDM signature files (zip file format; for example, sigv5−SDM−S307.zip) and CLI signature packages (pkg file format; for example, IOS−S313−CLI.pkg) can be downloaded together in one operation
- Downloaded signature packages can be pushed automatically to the router as an option

The tasks involved in the initial provisioning process are:

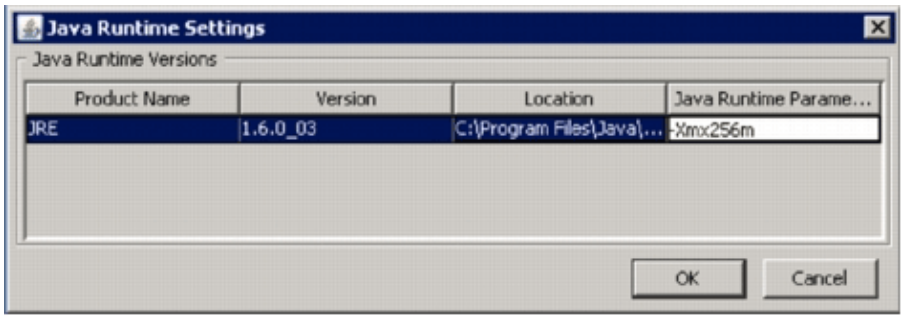
1. Download and install SDM 2.5.
2. Use SDM Auto Update in order to download the IOS IPS signature package to a local PC.
3. Launch the IPS Policies Wizard in order to configure IOS IPS.
4. Verify that the IOS IPS configuration and signatures are properly loaded

Cisco SDM is a web−based configuration tool that simplifies router and security configuration through smart wizards that help customers quickly and easily deploy, configure, and monitor a Cisco router without requiring knowledge of the command−line interface (CLI).

SDM version 2.5 can be downloaded from Cisco.com at http://www.cisco.com/pcgi−bin/tablebuild.pl/sdm (registered customers only) . The release note can be found at http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/software/release/notes/S

Note: Cisco SDM requires a screen resolution of at least 1024 x 768.

Note: Cisco SDM requires Java memory heap size to be no less than 256MB in order to configure IOS IPS. In order to change the Java memory heap size, open the Java control panel, click the **Java** tab, click **View** located under the Java Applet Runtime Settings, and then enter **−Xmx256m** in the Java Runtime Parameter column.



Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco IOS IPS in 12.4(15)T3 and later releases
- Cisco Router and Security Device Manager (SDM) version 2.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

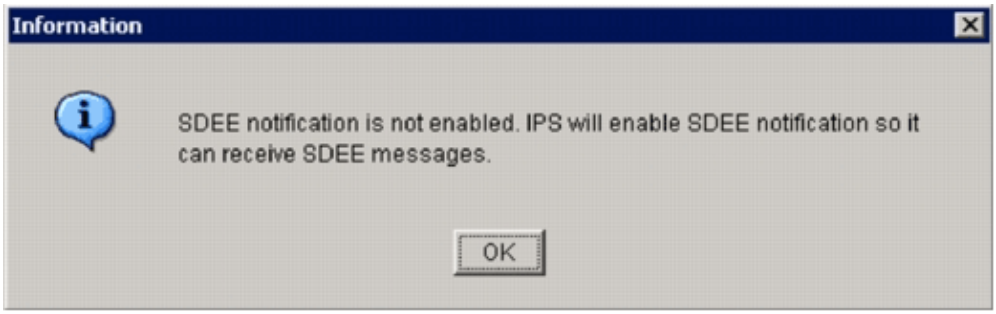
Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure

Note: Open a console or telnet session to the router (with `term monitor' on) in order to monitor messages when you use SDM to provision IOS IPS.

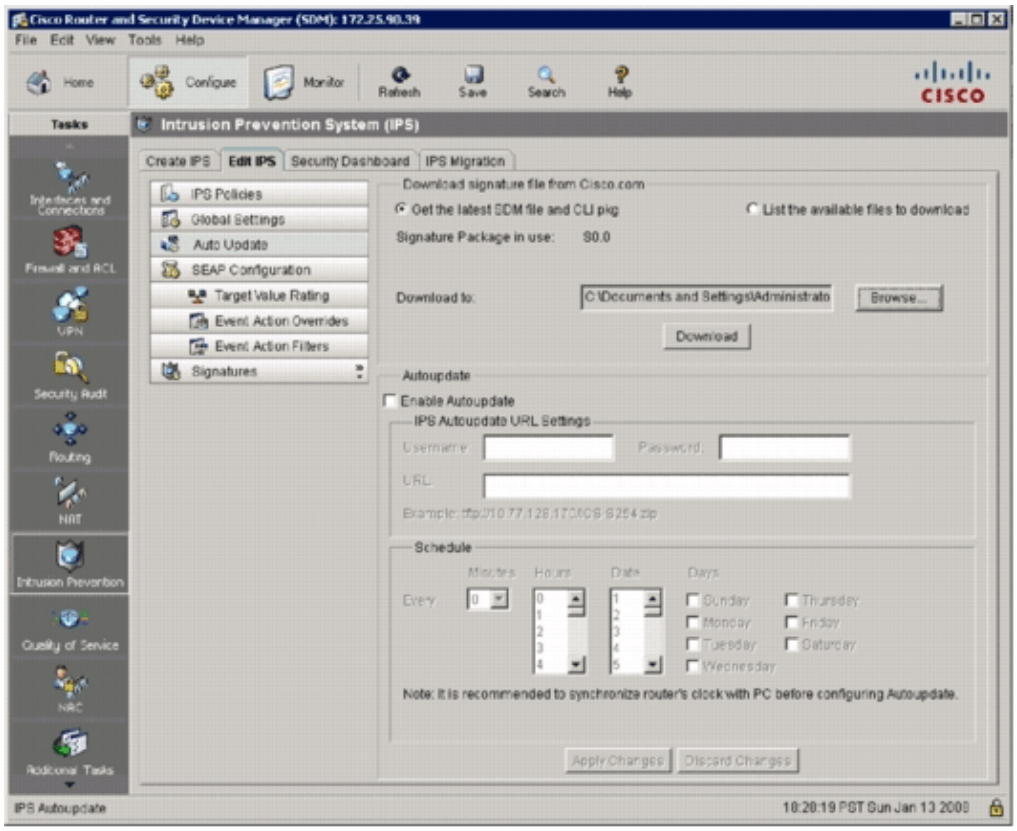
1. Download SDM 2.5 from Cisco.com at http://www.cisco.com/pcgi−bin/tablebuild.pl/sdm (registered customers only) and install it on a local PC.
2. Run SDM 2.5 from the local PC.
3. When the IOS IPS Login dialog box appears, enter the same user name and password that you use for SDM authentication to the router.

4. From SDM user interface, click **Configure**, and then click **Intrusion Prevention**.
5. Click the **Edit IPS** tab.
6. If SDEE notification is not enabled on the router, click **OK** in order to enable SDEE notification.



7. In the Download signature file from Cisco.com area of the Edit IPS tab, click the **Get the latest SDM file and CLI pkg** radio button, and then click **Browse** in order to select a directory on your local PC in which to save the downloaded files.

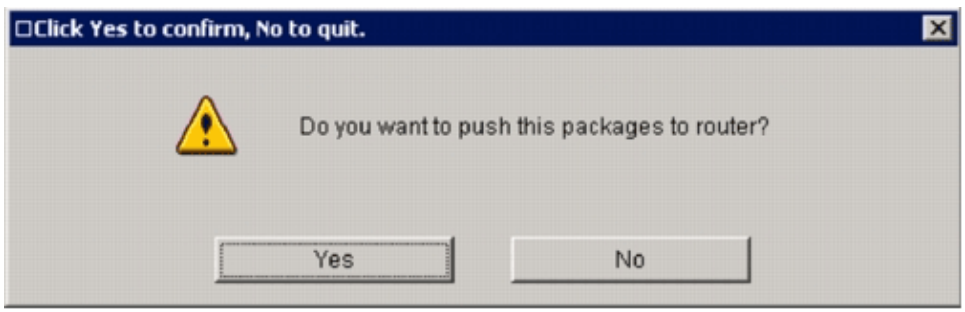
   You can choose the TFTP or FTP server root directory, which will be used later when you deploy the signature package to the router.
8. Click **Download**.



9. When the CCO Login dialog box appears, use your CCO registered user name and password.

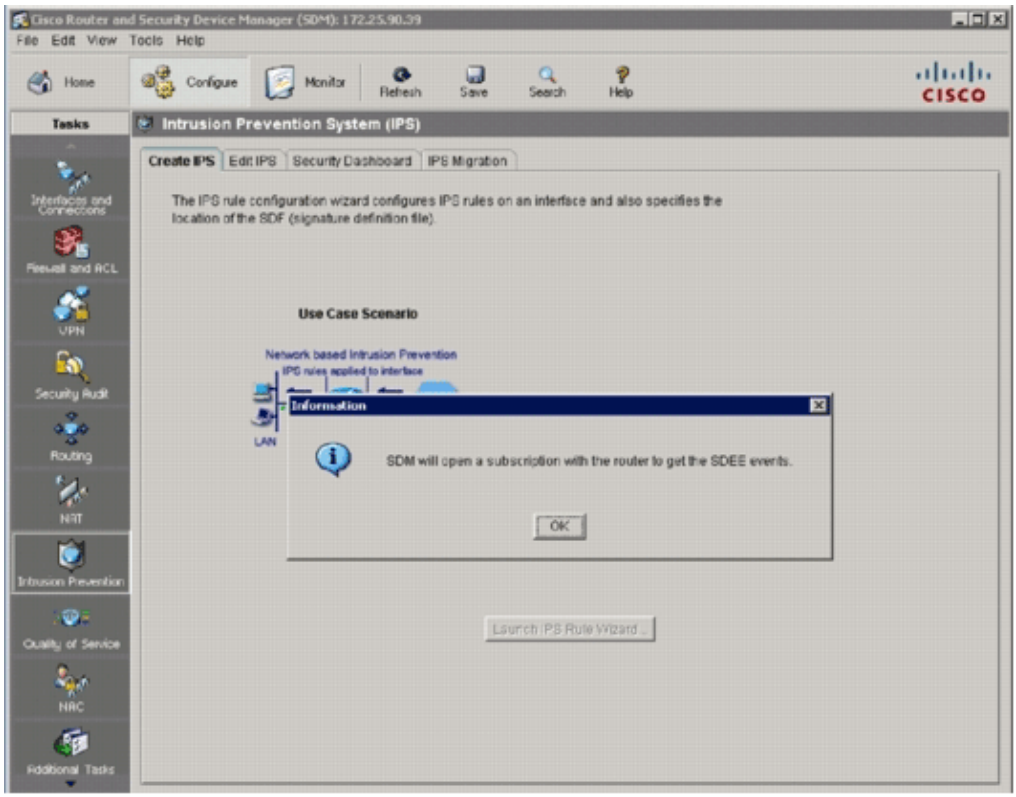
SDM connects to Cisco.com and starts to download both the SDM file (for example, sigv5−SDM−S307.zip) and the CLI pkg file (for example, IOS−S313−CLI.pkg) to the directory selected in step 7.

Once both files are downloaded, SDM prompts you to push the downloaded signature package to the router.



10. Click **No** since IOS IPS has not been configured on the router yet.
11. After SDM downloads the latest IOS CLI signature package, click the **Create IPS** tab in order to create initial IOS IPS configuration.
12. If you are prompted to apply changes to the router, click **Apply Changes**.
13. Click **Launch IPS Rule Wizard**.

    A dialog box appears to inform you that SDM needs to establish a SDEE subscription to the router to retrieve alerts.

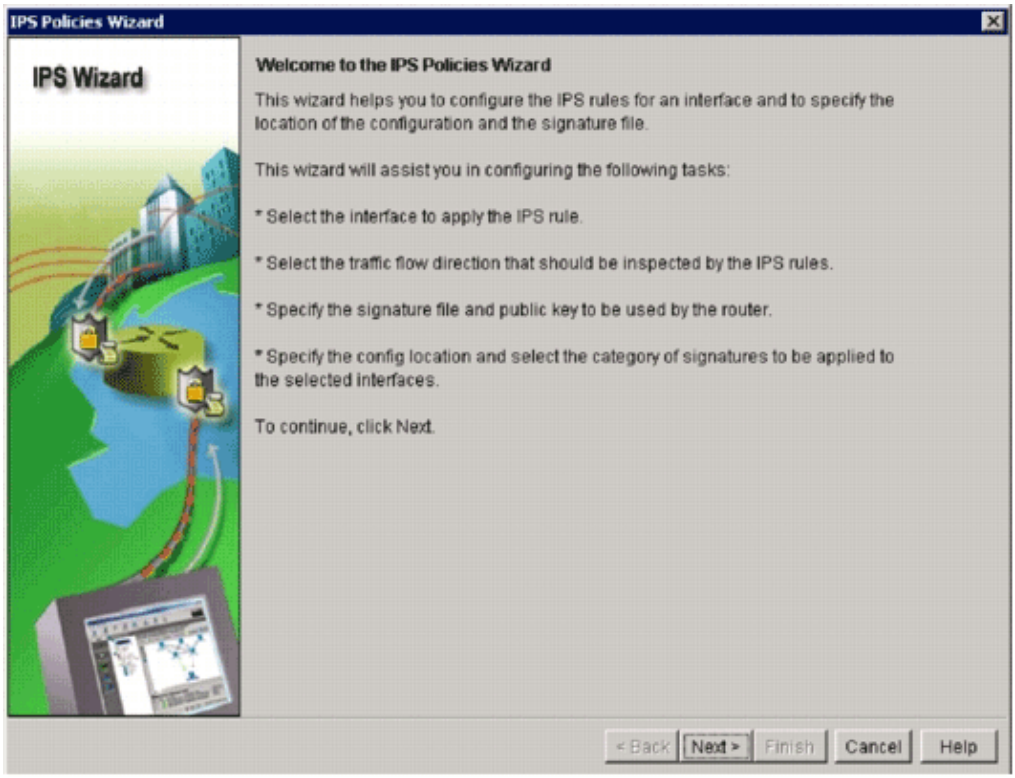


14. Click **OK**.

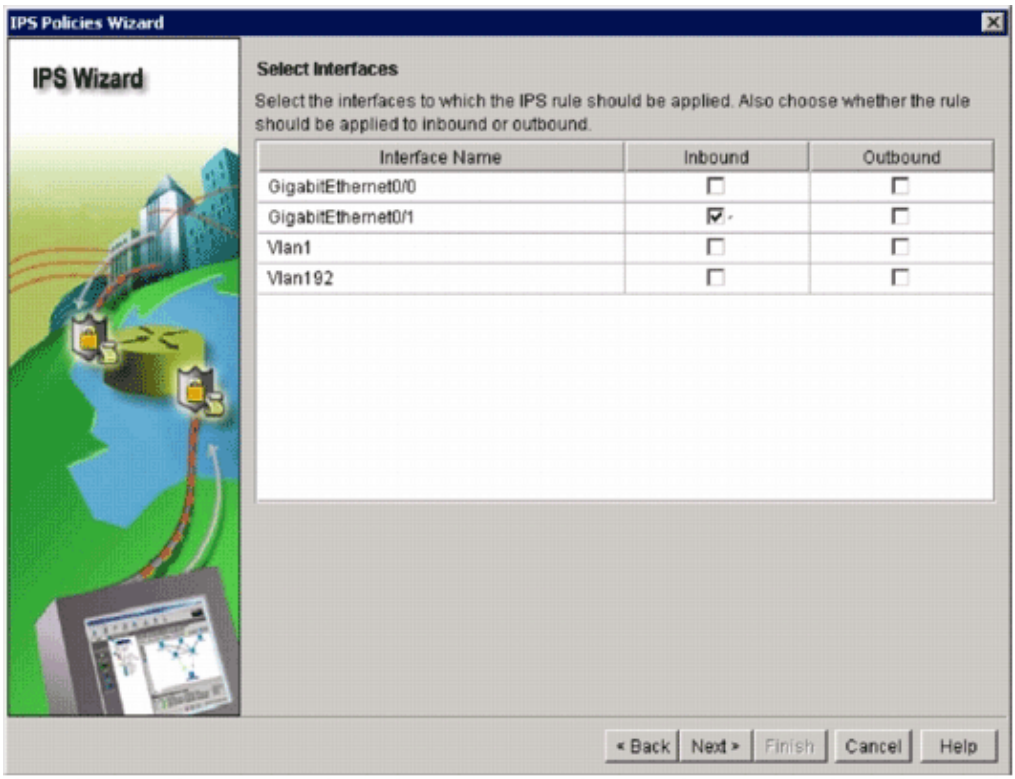
    The Authentication Required dialog box appears.

15. Enter the user name and password that you used for SDM to authenticate to the router, and click **OK**.

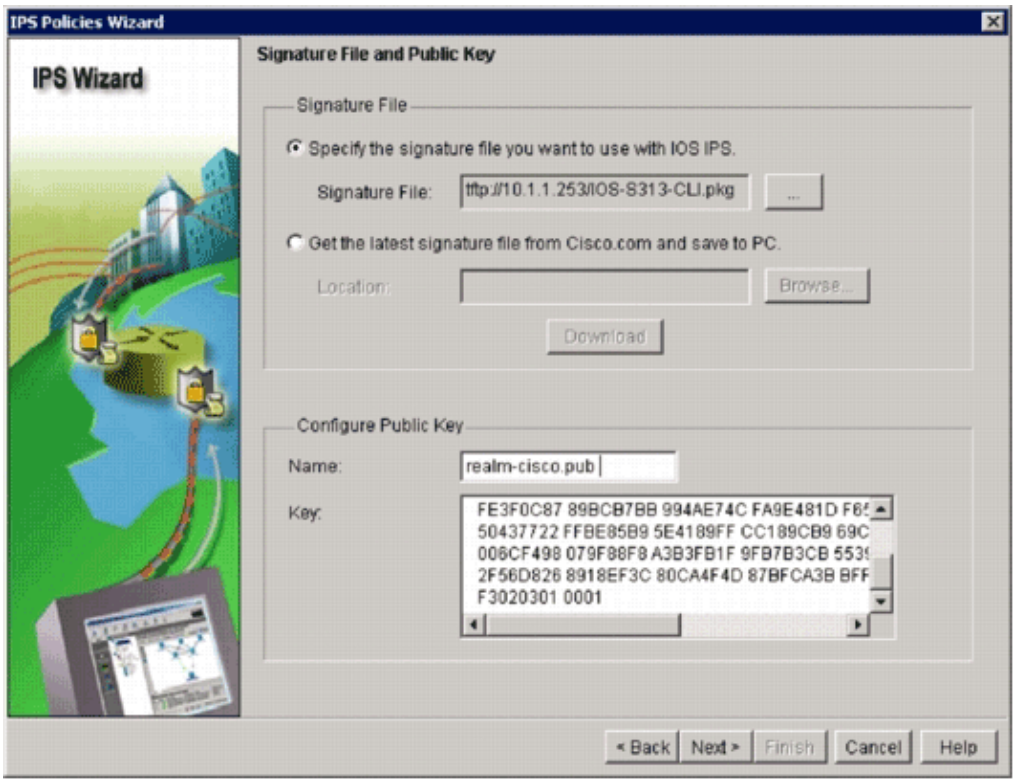
The IPS Policies Wizard dialog box appears.



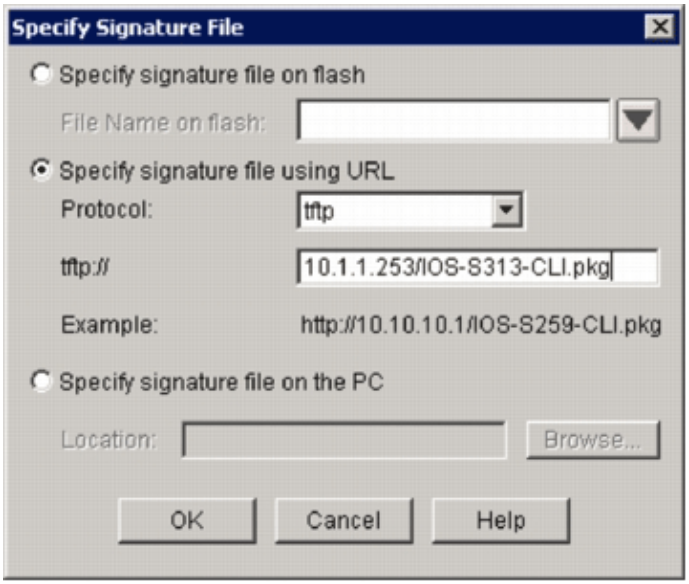
16. Click **Next**.



17. In the Selected Interfaces window, choose the interface and the direction to which that IOS IPS will be applied, and then click **Next** to continue.



18. In the Signature File area of the Signature File and Public Key window, click the **Specify the signature file you want to use with IOS IPS** radio button, and then click the **Signature File** button (...) in order to specify the location of the signature package file, which will be the directory specified in step 7.



19. Click the **Specify signature file using URL** radio button, and choose a protocol from the Protocol drop−down list.

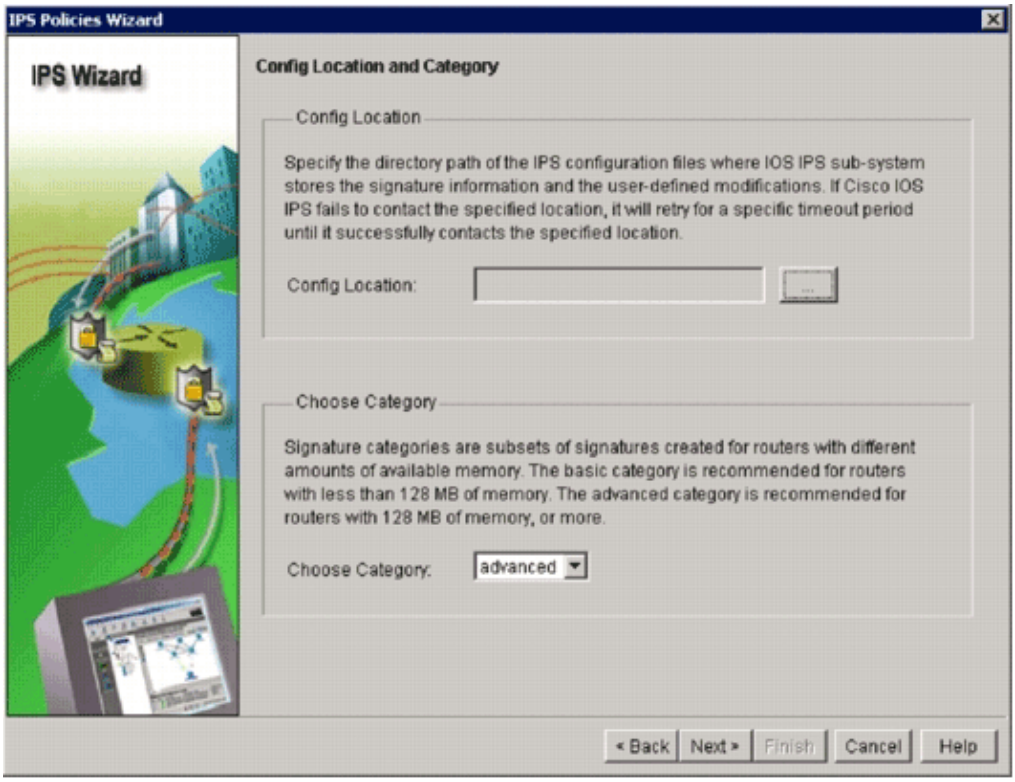
    Note: This example uses TFTP in order to download the signature package to the router.
20. Enter the URL for the signature file, and click **OK**.
21. In the Configure Public Key area of the Signature File and Public Key window, enter **realm−cisco.pub** in the Name field, and then copy this public key and paste it into the Key field.

```
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
```

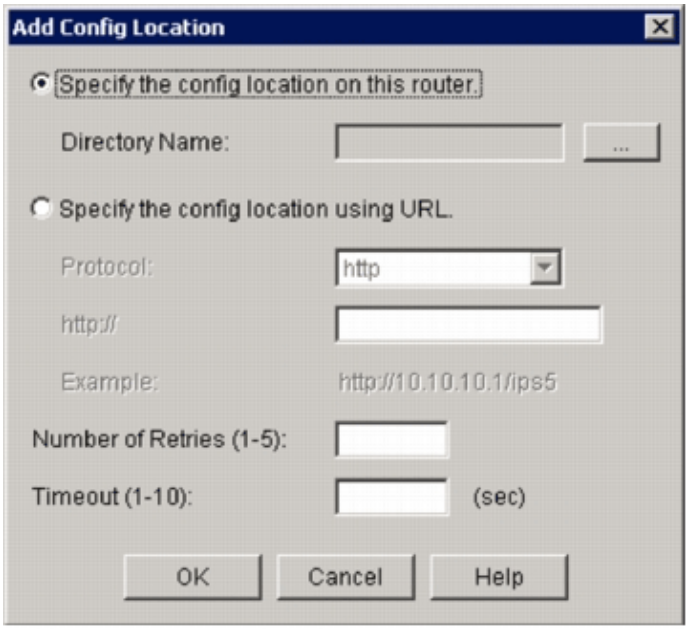
Note: This public key can be download from Cisco.com at: http://www.cisco.com/pcgi−bin/tablebuild.pl/ios−v5sigup (registered customers only) .

22. Click **Next** to continue.



23. In the Config Location and Category window, click the **Config Location** button (...) in order to specify a location where the signatures definition and configuration files will be stored.

    The **Add Config Location** dialog box appears.



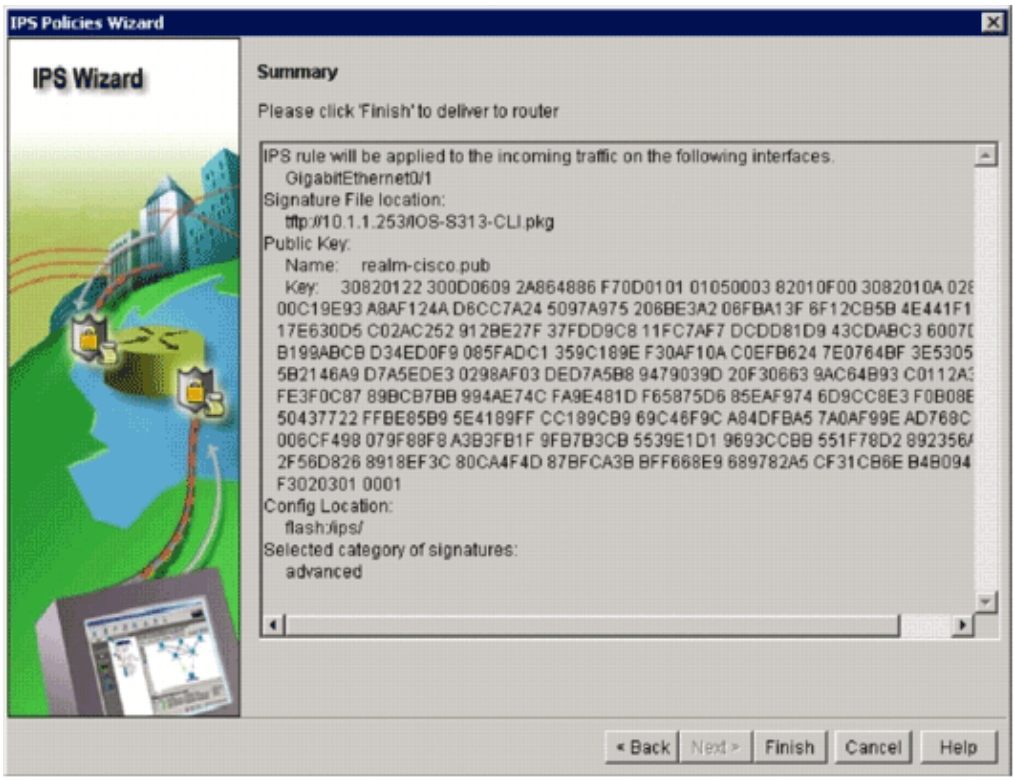
24. In the Add Config Location dialog box, click the **Specify the config location on this router** radio button, and then click the **Directory Name** button (...) in order to locate the configuration file.

    The Choose Folder dialog box appears in order to allow you to select an existing directory or create a new directory on the router flash to store the signature definition and configuration files.

25. Click **New Folder** located at the top of the dialog box if you want to create a new directory.
26. Once you select the directory, click **OK** in order to apply changes, and then click **OK** in order to close the Add Config Location dialog box.
27. On the IPS Policies Wizard dialog box, select the signature category according to the amount of memory installed on the router. There are two signature categories you can choose in SDM: Basic and Advanced.

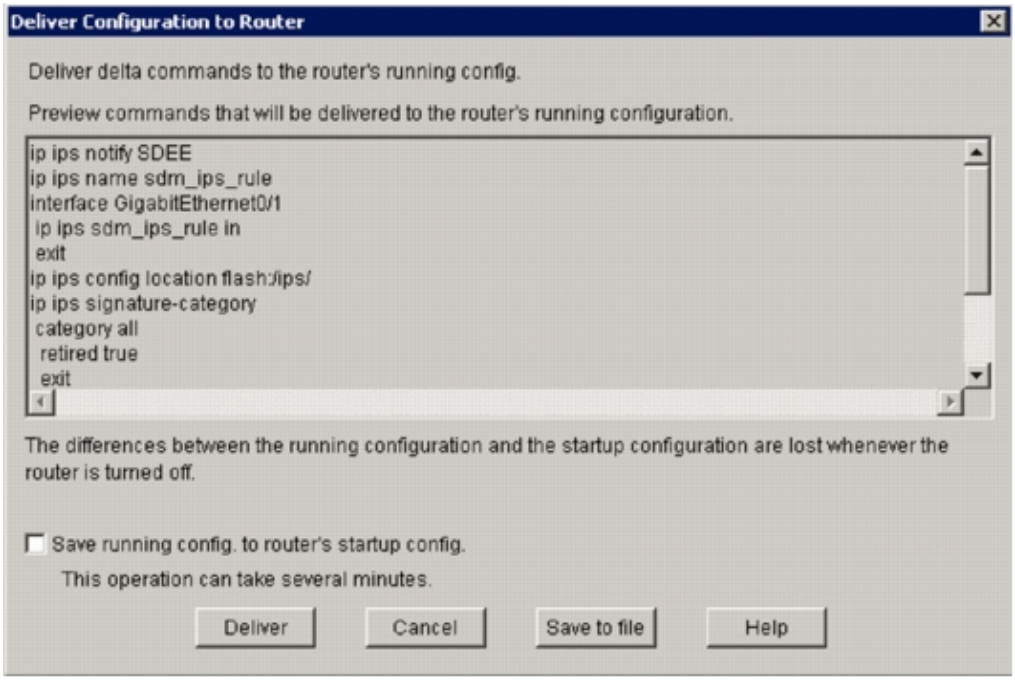
    If the router has 128MB DRAM installed, Cisco recommends that you choose the Basic category in order to avoid memory allocation failures. If the router has 256MB or more DRAM installed, you can choose either category.
28. Once you select a category to use, click **Next** in order to continue to the summary page.

    The summary page provides a brief description about the tasks IOS IPS initial configuration.



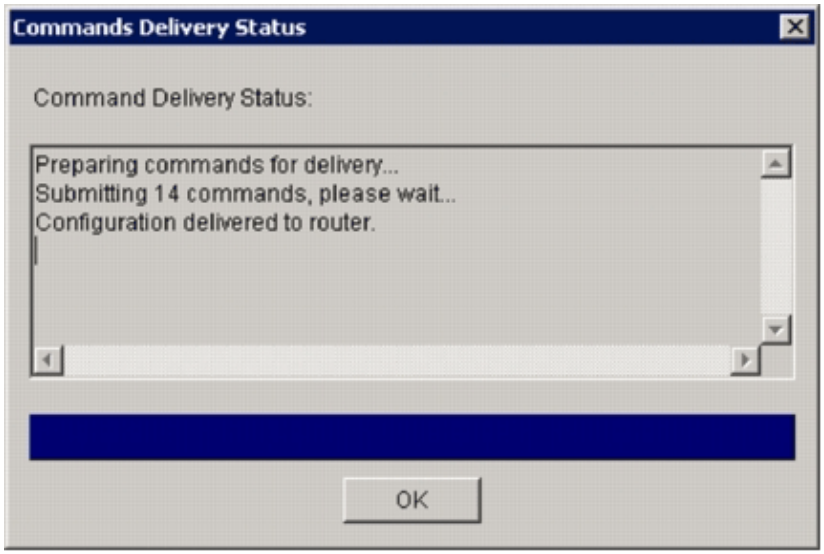
29. Click **Finish** on the summary page in order to deliver the configurations and signature package to the router.

    If the preview commands option is enabled on the Preferences settings in SDM, SDM displays the Deliver Configuration to Router dialog box that shows a summary of CLI commands that SDM deliver to the router.



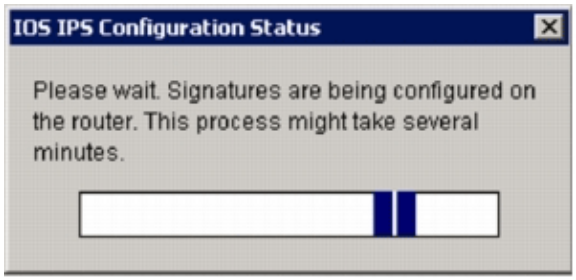
30. Click **Deliver** in order to proceed.

    The Commands Delivery Status dialog box appears to show the commands delivery status.

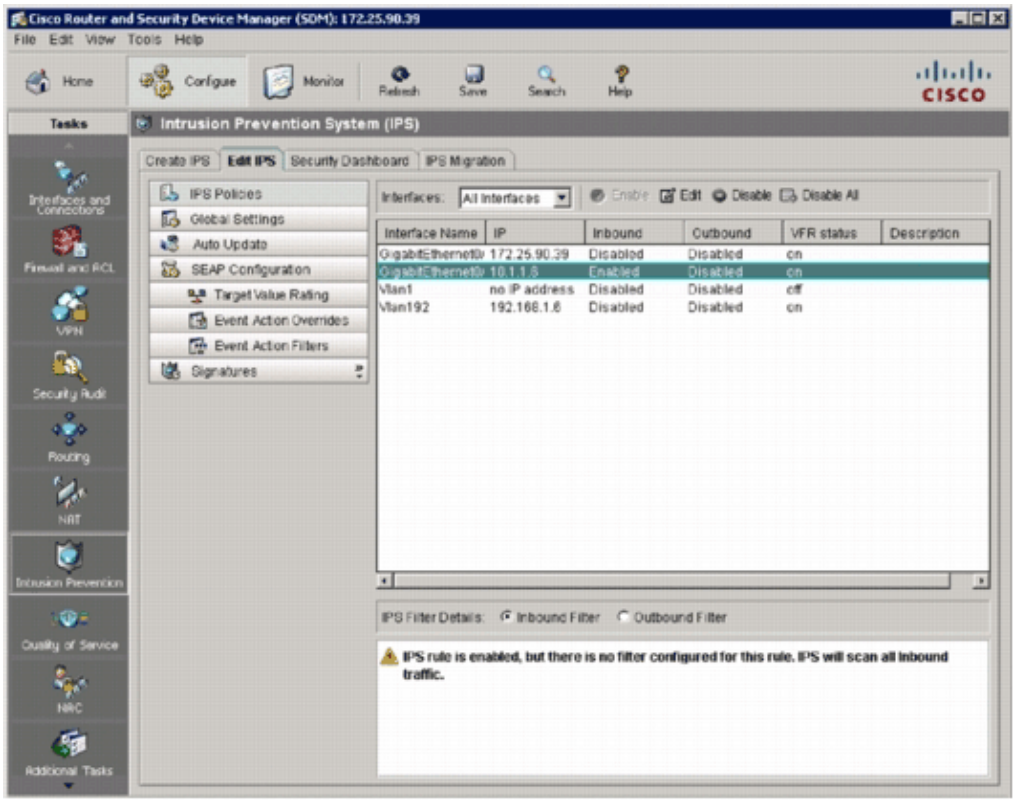


31. When the commands are delivered to the router, click **OK** in order to continue.

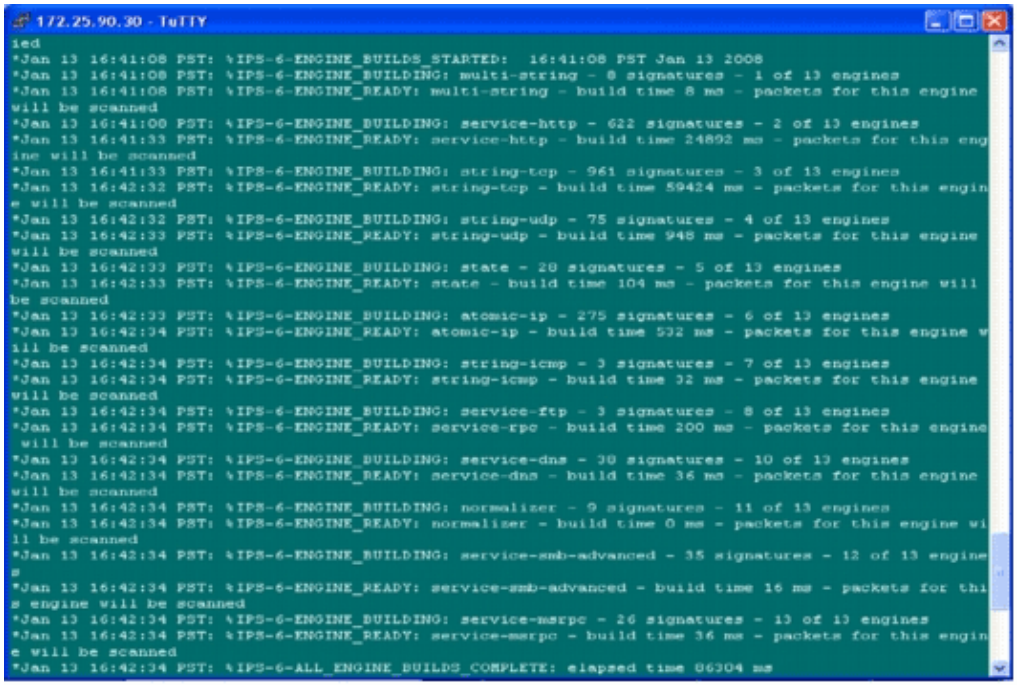
    The IOS IPS Configuration Status dialog box shows that the signatures are being loaded on the router.



32. When the signatures are loaded, SDM displays the **Edit IPS** tab with the current configuration. Check which interface and in what direction the IOS IPS is enabled in order to verify the configuration.



The router console shows that the signatures have been loaded.

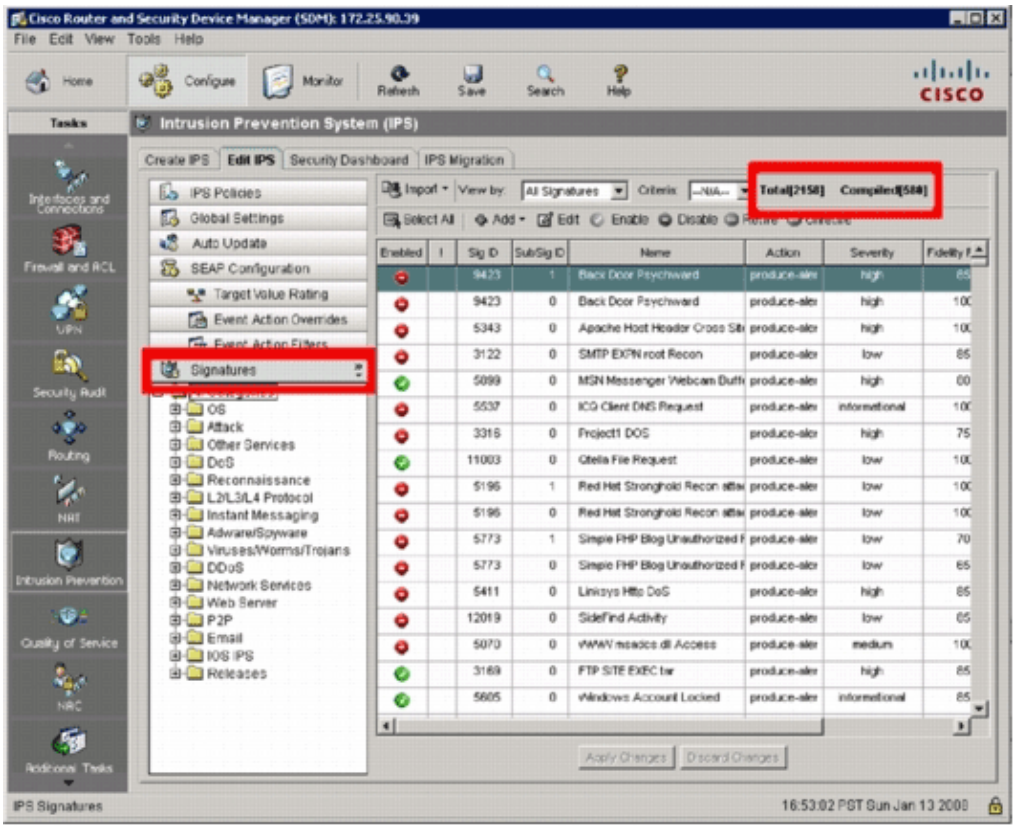


33. Use the **show ip ips signatures count** command in order to verify the signatures are loaded properly.

```
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
```

The initial provisioning of IOS IPS using SDM 2.5 is complete.

34. Verify the signature numbers with SDM as shown in this image.



Related Information

- **Cisco IOS IPS on Cisco.com**
- **Cisco IOS IPS Signature package**
- **Cisco IOS IPS Signature files for SDM**
- **Getting Started with Cisco IOS IPS with 5.x Signature Format**
- **Cisco IOS IPS Configuration Guide**
- **Cisco IDS Event Viewer**
- **Technical Support & Documentation − Cisco Systems**

Updated: May 17, 2008 Document ID: 105627