Router and Security Device Manager and Cisco IOS CLI in Cisco IOS IPS Configuration Example

Document ID: 105629

Contents

Introduction

In Cisco Router and Security Device Manager (SDM) 2.2, the Cisco IOS® IPS configuration is integrated within the SDM application. You are no longer required to launch a separate window in order to configure Cisco IOS IPS.

In Cisco SDM 2.2, a new IPS configuration wizard guides you through the steps necessary enable Cisco IOS IPS on the router. In addition, you can still use the advanced configuration options to enable, disable, and tune Cisco IOS IPS with Cisco SDM 2.2.

Cisco recommends that you run Cisco IOS IPS with the pretuned signature definition files (SDFs): attack−drop.sdf, 128MB.sdf, and 256MB.sdf. These files are created for routers with different amounts of memory. The files are bundled with Cisco SDM, which recommends SDFs when you first enable Cisco IOS IPS on a router. These files can also be downloaded from http://www.cisco.com/pcgi−bin/tablebuild.pl/ios−sigup (registered customers only) .

The process to enable the default SDFs is detailed in Enable Cisco IOS IPS with a Factory Default SDF. When the default SDFs are not sufficient or you want to add new signatures, you can use the procedure described in Append Additional Signatures after Enabling Default SDF.

Prerequisites

Requirements

Java Runtime Environment (JRE) Version 1.4.2 or later is required to use Cisco SDM 2.2. A Cisco−recommended and tuned signature file (based on DRAM) is bundled with Cisco SDM (loaded on router flash memory with Cisco SDM).

Components Used

The information in this document is based on the Cisco Router and Security Device Manager (SDM) 2.2.

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

Enable Cisco IOS IPS with a Factory Default SDF

CLI Procedure

Complete this procedure in order to use the CLI to configure a Cisco 1800 Series router with Cisco IOS IPS to load 128MB.sdf on the router flash.

1. Configure the router to enable Security Device Event Exchange (SDEE) event notification.

   ```
   yourname#conf t
   ```
2. Enter configuration commands (one per line), and then press Cntl+Z to end.

   ```
   yourname(config)#ip ips notify sdee
   ```
3. Create an IPS rule name that is used to associate to interfaces.

   ```
   yourname(config)#ip ips name myips
   ```
4. Configure an IPS location command to specify from which file the Cisco IOS IPS system will read signatures.

   This example uses the file on flash: 128MB.sdf. The location URL portion of this command can be any valid URL that uses flash, disk, or protocols via FTP, HTTP, HTTPS, RTP, SCP, and TFTP in order to point to the files.

   ```
   yourname(config)#ip ips sdf location flash:128MB.sdf
   ```

   Note: You must enable the **terminal monitor** command if you configure the router via a Telnet session or you will not see the SDEE messages when the signature engine is building.
5. Enable IPS on the interface where you want to enable the Cisco IOS IPS to scan traffic. In this case, we enabled on both directions on interface fastEthernet 0.

   ```
   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
```

The first time an IPS rule is applied to an interface, Cisco IOS IPS starts built signatures from the file specified by the SDF locations command. SDEE messages are logged to the console and sent to the syslog server if configured. The SDEE messages with <*number*> of <*number*> engines indicates the signature engine building process. Finally, when the two numbers are the same, all the engines are built.

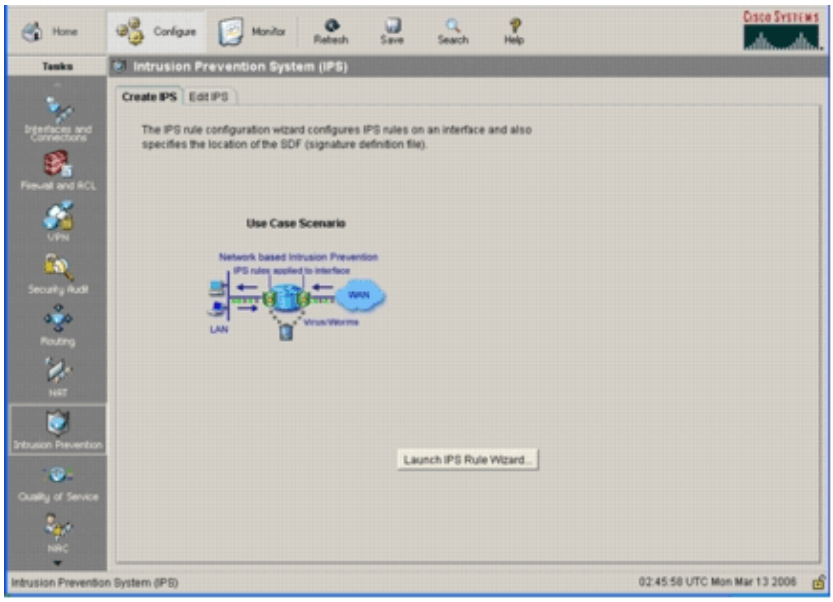
Note: IP virtual reassembly is an interface feature that (when turned on) automatically reassembles fragmented packets that come into the router through that interface. Cisco recommends that you enable ip virtual−assembly on all interfaces where traffic comes into the router. In the above example, besides turning on "ip virtual−assembly" on interface fastEthernet 0, we configure it on the inside interface VLAN 1 as well.

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

SDM 2.2 Procedure

Complete this procedure in order to use Cisco SDM 2.2 to configure a Cisco 1800 Series router with Cisco IOS IPS.

1. In the SDM application, click **Configure**, and then click **Intrusion Prevention**.

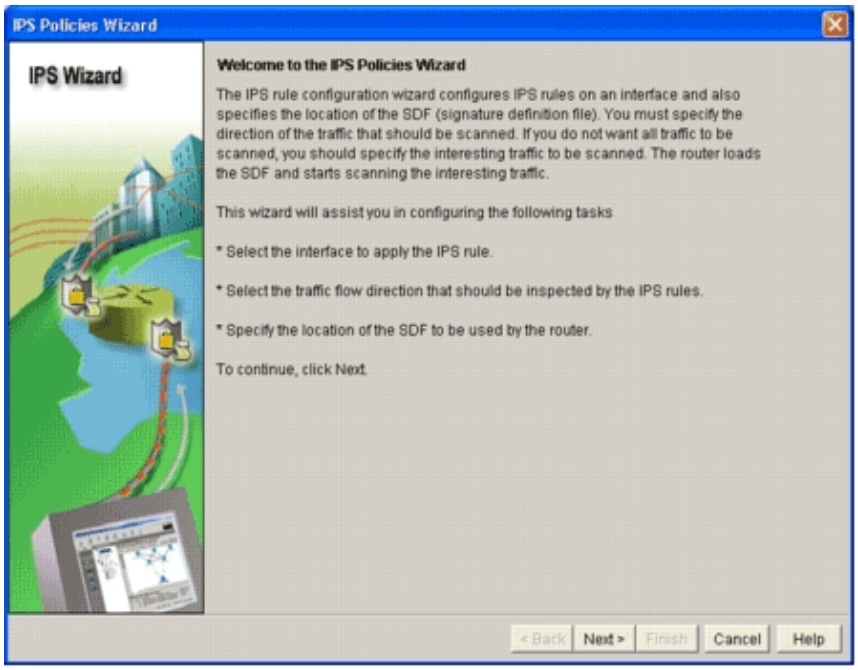


2. Click the **Create IPS** tab, and then click **Launch IPS Rule Wizard**.

   Cisco SDM requires IPS event notification via SDEE in order to configure the Cisco IOS IPS feature. By default, the SDEE notification is not enabled. Cisco SDM prompts you to enable IPS event notification via SDEE as shown in this image:

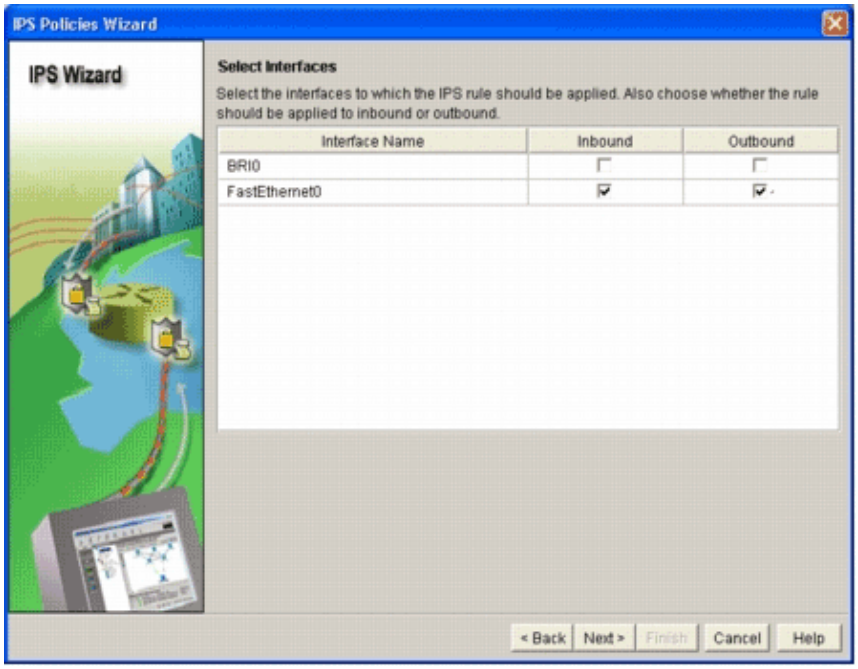
3. Click **OK**.

   The Welcome to the IPS Policies Wizard window of the IPS Policies Wizard dialog box appears.



4. Click **Next**.

   The Select Interfaces window appears.

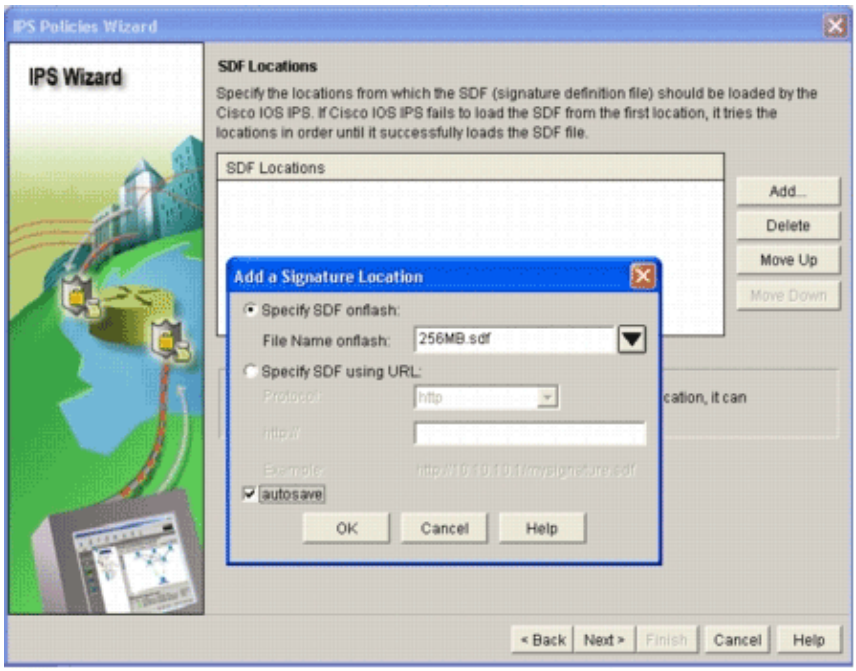


5. Choose the interfaces for which you want to enable IPS, and click either the **Inbound** or **Outbound** checkbox in order to indicate the direction of that interface.

   Note: Cisco recommends that you enable both inbound and outbound directions when you enable IPS on an interface.
6. Click **Next**.

   The SDF Locations window appears.
7. Click **Add** in order to configure an SDF location.

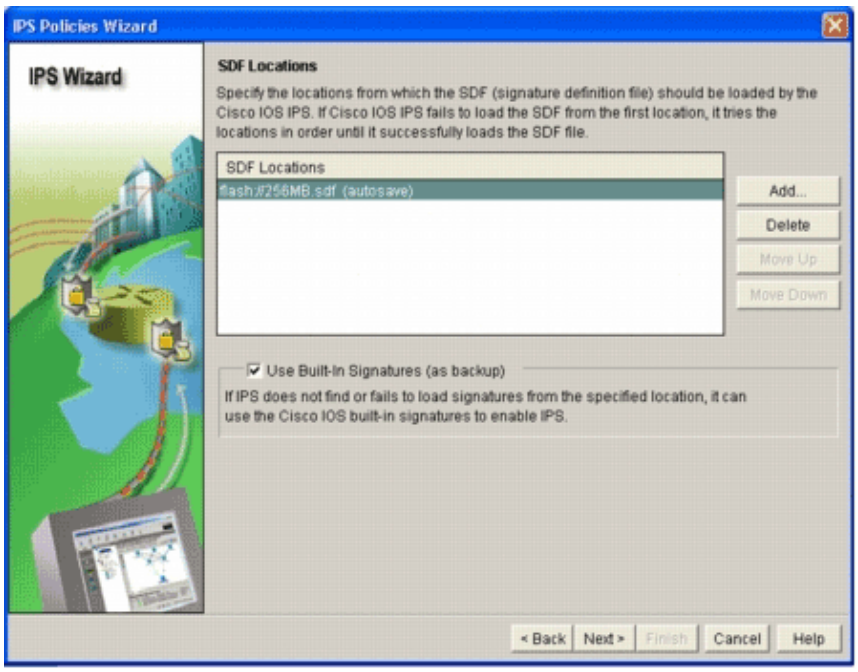
   The Add a Signature Location dialog box appears.



8. Click the **Specify SDF on flash** radio button, and choose 256MB.sdf from the **File Name on flash** drop−down list.
9. Click the **autosave** checkbox, and click **OK**.

   Note: The autosave option automatically saves the signature file when there is a signature change.

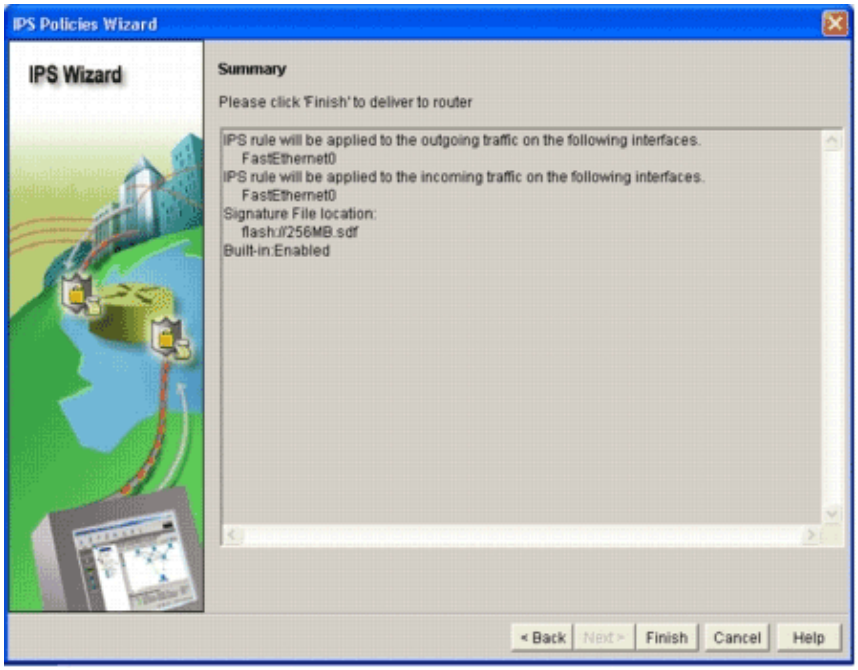
   The SDF Locations window displays the new SDF location.



   Note: You can add additional signature locations in order to designate a backup.
10. Click the **Use Built−In Signatures (as backup)** check box.

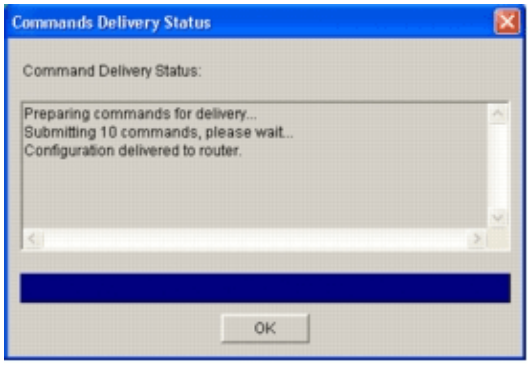
    Note: Cisco recommends that you do not use the built−in signature option unless you have specified one or more locations.
11. Click **Next** in order to continue.

The Summary window appears.



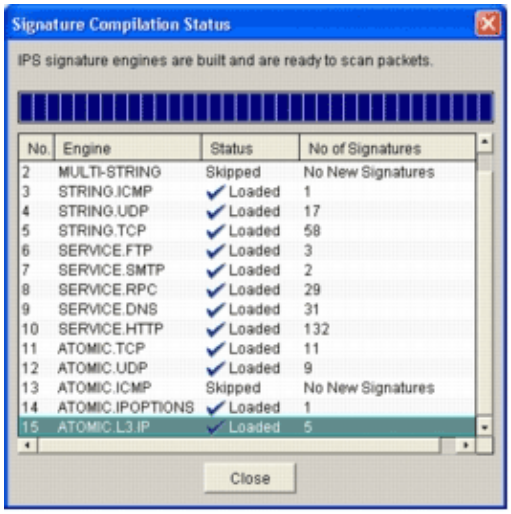
12. Click **Finish**.

The Commands Delivery Status dialog box displays the status as the IPS engine compiles all the signatures.



13. Once the process is complete, click **OK**.

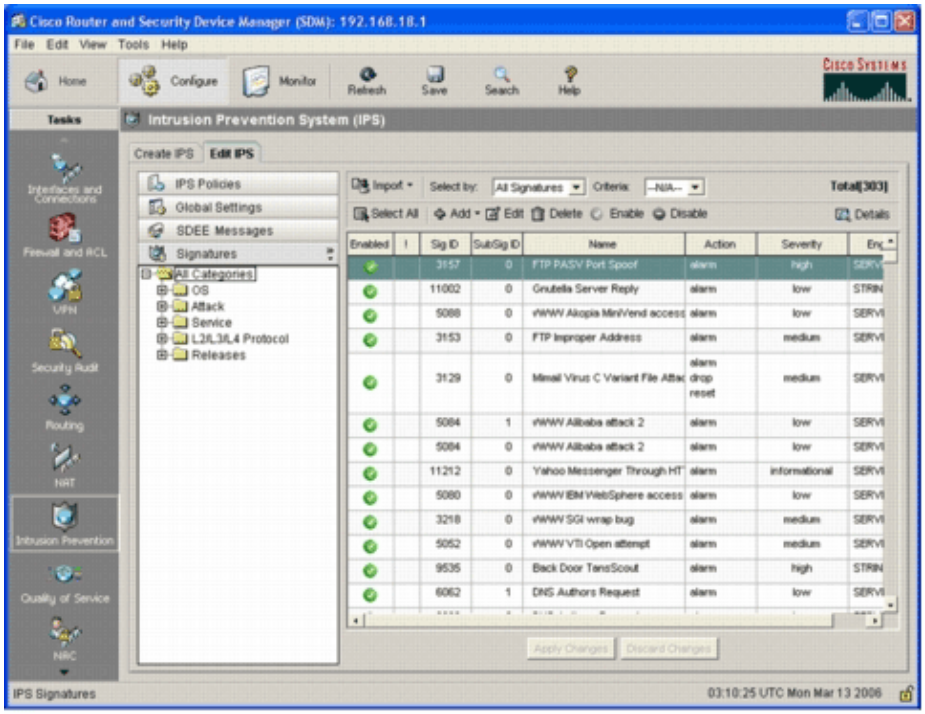
The Signature Compilation Status dialog box displays the signature compilation information.



This information shows which engines have been compiled and the number of signatures in that engine. For engines that display *Skipped* in the status column, there is no signature loaded for that engine.

14. Click **Close** in order to close the Signature Compilation Status dialog box.
15. In order to verify which signatures are currently loaded on the router, click **Configure**, and then click **Intrusion Prevention**.
16. Click the **Edit IPS** tab, and then click **Signatures**.

    The IPS signature list appears in the Signatures window.



Append Additional Signatures after Enabling Default SDF

CLI Procedure

There is no CLI command available to create signatures or read signature information from the distributed IOS−Sxxx.zip file. Cisco recommends that you use either SDM or the Management Center for IPS Sensors to manage the signatures on Cisco IOS IPS systems.

For customers who already have a signature file ready and want to merge this file with the SDF that runs on a Cisco IOS IPS system, you can use this command:

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

The signature file defined by the signature location command is where the router loads signatures files when it reloads or when the router IOS IPS is reconfigured. For the merging process to be successful, the file defined by the signature file location command must also be updated.

1. Use the **show** command in order to check the currently configured signature locations.

   The output shows the configured signature locations. This command shows from where the current running signatures are loaded.

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

Signatures were last loaded from flash:128MB.sdf

Cisco SDF release version S128.0

Trend SDF release version V0.0

2. Use the **copy** <*url*> **ips−sdf** command, along with the information from the previous step, in order to merge signature files.

```
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 signatur
        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=Fals
        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#
```

After you issue the **copy** command, the router loads the signature file into the memory and then builds the signature engines. In the console SDEE message output, the building status for each signature engine is displayed.

- %IPS−6−ENGINE_BUILD_SKIPPED indicates that there are no new signatures for this engine.
- %IPS−6−ENGINE_READY indicates that there are new signatures and the engine is ready. As before, the "15 of 15 engines" message indicates that all engines have been built.
- IPS−7−UNSUPPORTED_PARAM indicates that a certain parameter is not supported by Cisco IOS IPS. For example, CapturePacket and ResetAfterIdle.

Note: These messages are for information only and will have no affect on the Cisco IOS IPS signature capability or performance. These logging messages can be turned off by setting the logging level higher than debugging (level 7).

3. Update the SDF defined by the signature location command, such that when router reloads, it will have the merged signature set with updated signatures. This example shows the file size difference after the merged signature is saved to the 128MB.sdf flash file.

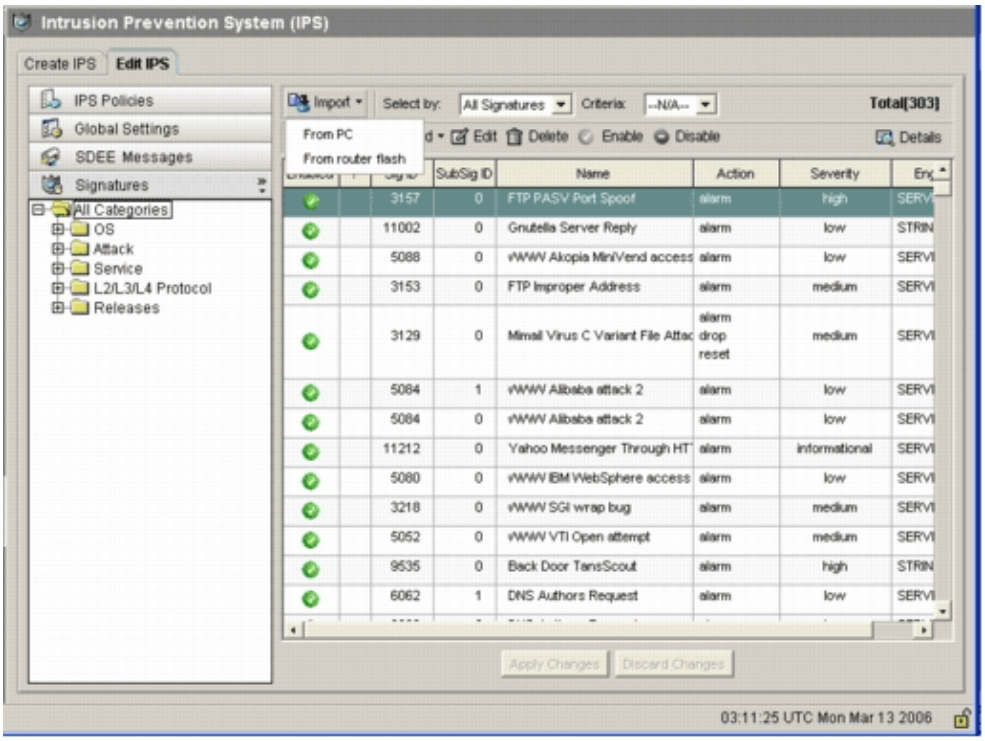
```
yourname#show flash:
-#- --length-- -----date/time------ path
4 504630 Aug 30 2005 22:58:34 +00:00 128MB.sdf
yourname#copy ips-sdf flash:128MB.sdf
yourname#show flash:
-#- --length-- -----date/time------ path
4 522656 Oct 26 2005 02:51:32 +00:00 128MB.sdf
```

Warning: The new 128MB.sdf now contains customer−merged signatures. The content is different from the Cisco default 128MB.sdf file. Cisco recommends that you change this file to a different name to avoid confusion. If the name is changed, the signature location command needs to be changed as well.

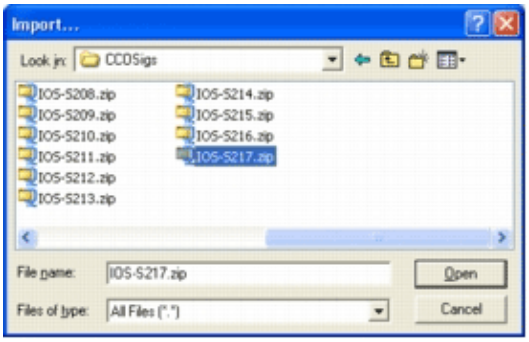
SDM 2.2 Procedure

After Cisco IOS IPS has been enabled, new signatures can be added into the router that runs a signature set with the Cisco SDM import function. Complete these steps in order to import new signatures:

1. Choose the default SDFs or the IOS−Sxxx.zip update file to import additional signatures.
2. Click **Configure**, and then click **Intrusion Prevention**.
3. Click the **Edit IPS** tab, and then click **Import**.



4. Choose **From PC** from the Import drop−down list.
5. Select the file from which you want to import signatures.

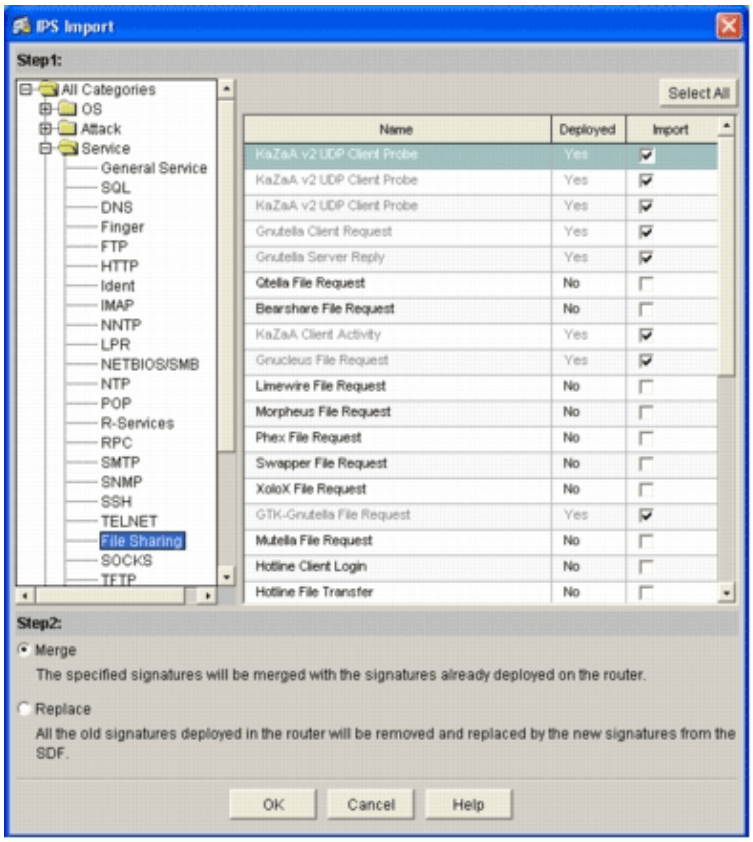


This example uses the latest update downloaded from Cisco.com and saved on the local PC hard disk.

6. Click **Open**.

Warning: Due to memory constraint, only a limited number of new signatures can be added on top of signatures that have already been deployed. If too many signatures are selected, the router might not be able to load all new signatures because of lack of memory.

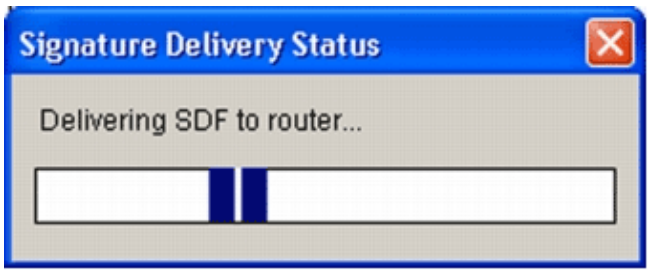
Once the signature file load completes, the IPS Import dialog box appears.



7. Navigate through the left tree view, and click the **Import** check box next to the signatures you want to import.
8. Click the **Merge** radio button, and then click **OK**.

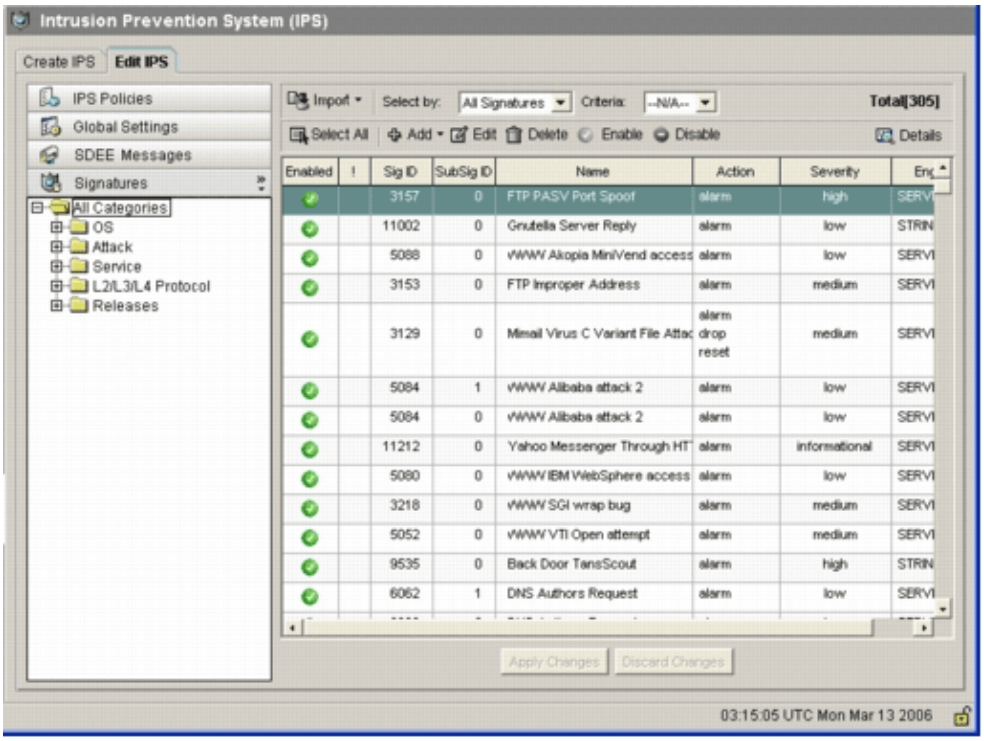
   Note: The Replace option replaces the current signature set on the router with the signatures you select to import.

   Once you click OK, the Cisco SDM application delivers the signatures to the router.



Note: High CPU utilization occurs during compilation and loading of signatures. After Cisco IOS IPS is enabled on the interface, the signature file starts to load. The router takes about five minutes to load the SDF. You can attempt to use the **show process cpu** command in order to view the CPU utilization from the Cisco IOS Software CLI. However, do not attempt to use additional commands or load other SDFs while the router is loading the SDF. This may cause the signature compilation process to take longer to complete (since the CPU utilization is close to 100−percent utilization at the time of loading the SDF). You might need to browse through the list of signatures and enable the signatures if they are not in *enabled* state.

The total signature number has increased to 519. This number includes all the signatures available in the IOS−S193.zip file that belong to the File Sharing subcategory.



For more advanced topics about how to use Cisco SDM to manage the Cisco IOS IPS feature, refer to the Cisco SDM documentation at this URL:

Select Signatures and Work with Signature Categories

In order to determine how to effectively select the correct signatures for a network, you must know a few things about the network that you are protecting. Updated signature category information in Cisco SDM 2.2 and later further assist customers to select the correct set of signatures to protect the network.

The category is a way to group signatures. It helps to narrow down signature selection to a subset of signatures that are relevant to each other. One signature could belong to only one category or it could belong to multiple categories.

These are the five top−level categories:

- OS Operation−system−based signature categorization
- Attack Attack−based signature categorization
- Service Service−based signature categorization
- Layer 2−4 Protocol Protocol−level−based signature categorization
- Releases Release−based signature categorization

Each of these categories is further divided into subcategories.

As an example, consider a home network with a broadband connection to the Internet and a VPN tunnel to the corporate network. The broadband router has Cisco IOS Firewall enabled on the open (non−VPN) connection to the Internet to prevent any connection from being originated from the Internet and connected to the home network. All traffic that originates from the home network to the Internet is permitted. Assume that the user uses a Windows−based PC and uses applications like HTTP (web browsing) and e−mail.

The firewall can be configured so that only the applications that the user needs are allowed to flow through the router. This will control the flow of unwanted and potentially bad traffic that can spread throughout the network. Consider that the home user does not need or use a specific service. If that service is allowed to flow

through the firewall, there is a potential hole that an attack can use to flow throughout the network. Best practices only allow services that are needed. Now, it is easier to select what signatures to enable. You need to enable signatures only for the services that you allow to flow through the firewall. In this example, services include e−mail and HTTP. Cisco SDM simplifies this configuration.

In order to use the category to select required signatures, choose **Service > HTTP**, and enable all the signatures. This selection process also works in the signature import dialog, where you can select all the HTTP signatures and import them into your router.

Additional categories that need to be selected include DNS, NETBIOS/SMB, HTTPS, and SMTP.

Update Signatures for Default SDF Files

The three per−built SDFs (attack−drop.dsf, 128MB.sdf, and 256MB.sdf) are currently posted on Cisco.com at http://www.cisco.com/pcgi−bin/tablebuild.pl/ios−sigup (registered customers only) . Newer versions of these files will be posted as soon as they are available. In order to update routers that run Cisco IOS IPS with these default SDFs, go to the website and download the latest versions of these files.

CLI Procedure

1. Copy the downloaded files to the location where the router is configured to load these files from. To find out where the router is currently configured, use the **show running−config | in ip ips sdf** command.

   ```
   Router#show running−config | in ip ips sdf
   ip ips sdf location flash://256MB.sdf autosave
   ```

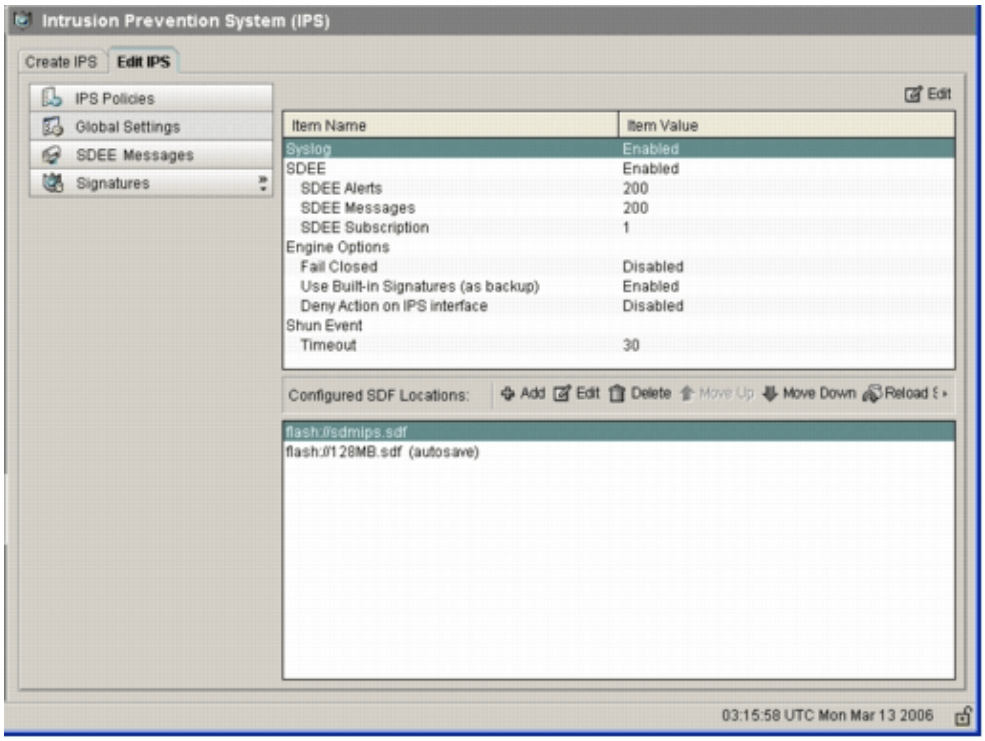
   In this example, the router uses 256MB.sdf on the flash. The file is updated when you copy the new downloaded 256MB.sdf to the router flash.
2. Reload the Cisco IOS IPS subsystem to run the new files.

   There are two ways to reload Cisco IOS IPS: reload the router or reconfigure Cisco IOS IPS to trigger the IOS IPS subsystem to reload signatures. In order to reconfigure Cisco IOS IPS, remove all the IPS rules from the configured interfaces, and then reapply the IPS rules back to the interfaces. This will trigger the Cisco IOS IPS system to reload.

SDM 2.2 Procedure

Complete these steps in order to update the default SDFs on the router:

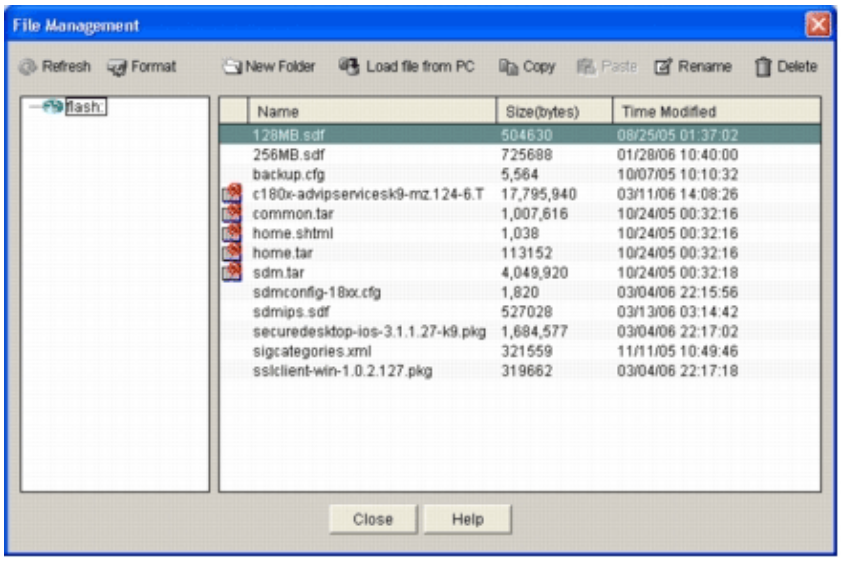
1. Click **Configure**, and then click **Intrusion Prevention**.
2. Click the **Edit IPS** tab, and then click **Global Settings**.



The top of the UI shows the global settings. The bottom half of the UI shows currently configured SDF locations. In this case, the 256MB.sdf file from flash memory is configured.

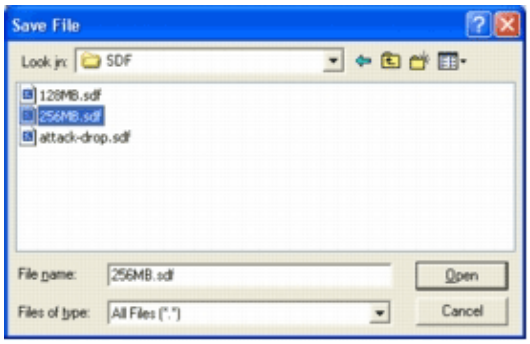
3. Choose **File Management** from the File menu.

   The File Management dialog box appears.



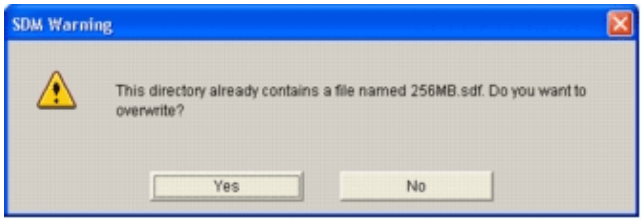
4. Click **Load file from PC**.

   The Save File dialog box appears.



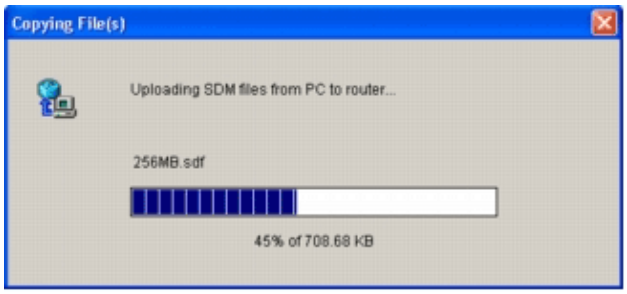
5. Choose the SDF that needs to be updated, and click **Open**.

   The SDM Warning message appears.

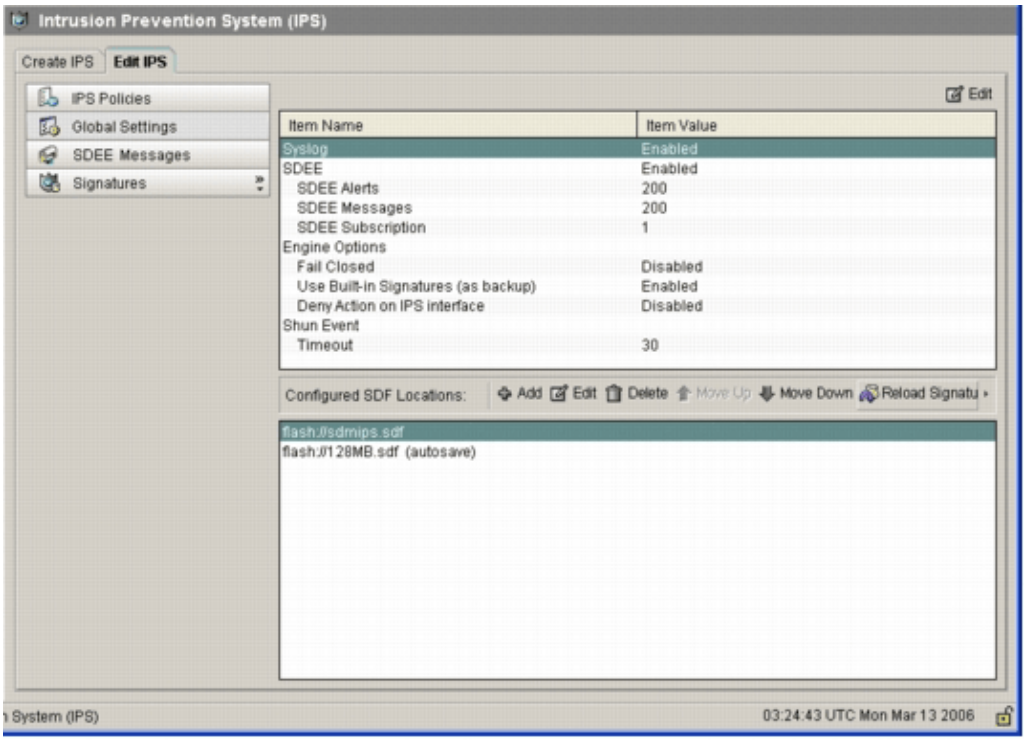


6. Click **Yes** in order to replace the existing file.

   A dialog box displays the progress of the upload process.



7. Once the upload process is complete, click **Reload Signatures** located on the SDF location toolbar. This action reloads the Cisco IOS IPS.



Note: The IOS−Sxxx.zip package contains all signatures that Cisco IOS IPS supports. Upgrades to this signature package are posted on Cisco.com as soon as they become available. In order to update signatures contained in this package, see Step 2.

Related Information

- **Cisco Intrusion Prevention System**
- **Security Product Field Notices (including CiscoSecure Intrusion Detection)**
- **Technical Support − Cisco Systems**

Updated: May 17, 2008 Document ID: 105629