Application Note

Cisco Router and Security Device Manager
Intrusion Prevention System

Introduction

This document explains how to use the Cisco® Router and Security Device Manager (Cisco SDM) to manage a Cisco Intrusion Protection System (IPS) on the router.

The Cisco IOS® IPS feature is an inline, signature-based solution for deep packet inspection that enables Cisco IOS Software to effectively mitigate network attacks. Cisco IOS IPS can be provisioned from the Cisco SDM. The IPS signatures can be loaded dynamically onto the Cisco router, and upon signature identification Cisco IOS IPS responds to misuse by dropping packets, resetting connections, and sending alarms.

The Cisco SDM allows you to download signature definition files (SDFs) from Cisco.com, import them onto a router, enable the IPS on router interfaces, tune IPS signatures, and deliver edited signatures to the router. You can specify that alerts are to be copied to a syslog server or you can configure the router to subscribe to the Security Device Event Exchange (SDEE) [1] protocol to report security events.

Deployment Scenarios

These deployment scenarios cover the following steps for a first-time IPS deployment:

1. Enable IPS with a customized SDF
2. Update IPS with a downloaded SDF
3. Tune IPS signatures

Prerequisites As a prerequisite, three Cisco recommended and tuned signature files (attack-drop.sdf, 128MB.sdf, and 256MB.sdf) are included with Cisco SDM (which examines the router memory and loads the best signature file to the router's flash memory), and a weekly compiled SDF can be manually downloaded from Cisco.com (http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup) and saved in a local management workstation. For a reference to all Cisco IOS Software security commands, see http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123tcr/123tsr/sec_01gt.pdf.

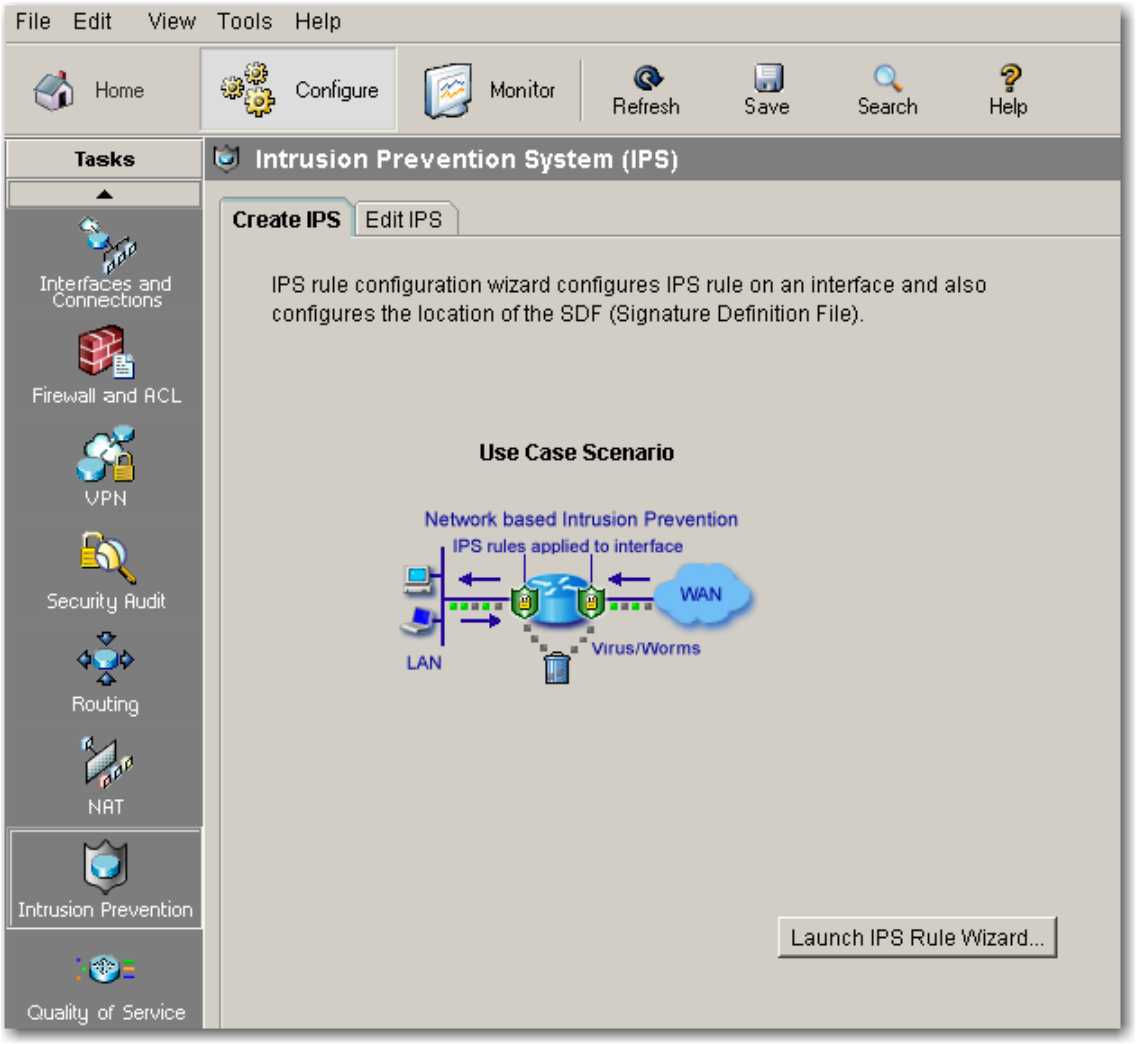
Scenario 1: Enable IPS with a Customized SDF

This scenario includes launching the Cisco SDM IPS wizard, importing the SDF onto the router, and enabling the IPS on the WAN interface. The router configuration has FastEthernet0/0 as its inside interface and FastEthernet0/1 as its outside interface. The IPS is applied to the inbound traffic to the outside interface. The SDF, 1841.sdf, is loaded from the SDF file server.

At Configure Mode, select Intrusion Prevention, click the Create IPS tab (Figure 1), and click Launch IPS Rule Wizard to launch the IPS wizard.

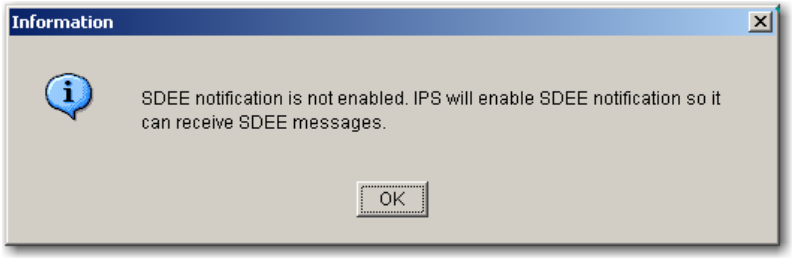
[1] A message protocol that can be used to report on security events, such as alarms generated when a packet matches the characteristics of a signature. SDEE is over HTTP.

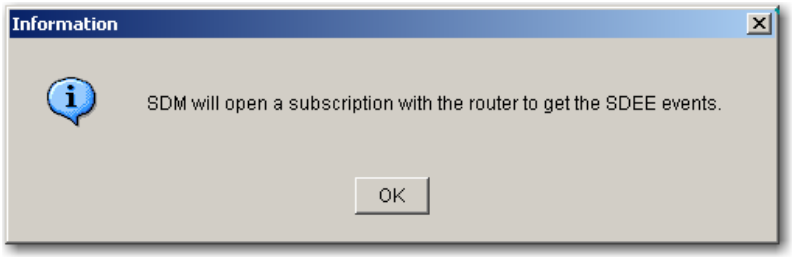
Figure 1. Configuring the Cisco SDM IPS



If SDEE is not enabled on the router, you are prompted to enable and subscribe to it (Figure 2). Click OK twice to continue.

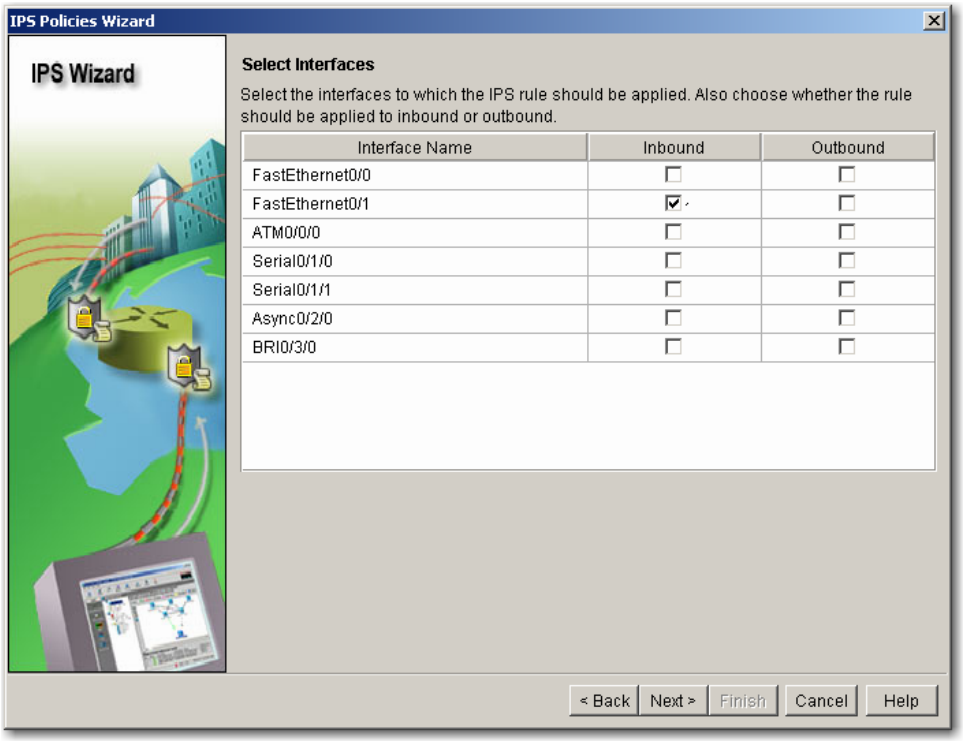
Figure 2. SDEE Notification and Subscription





At the Select Interfaces tab, in this case it is best to inspect the traffic from outside to inside at the outside interface FastEthernet0/1, so check Inbound IPS for FastEthernet0/1 (Figure 3) and click Next.

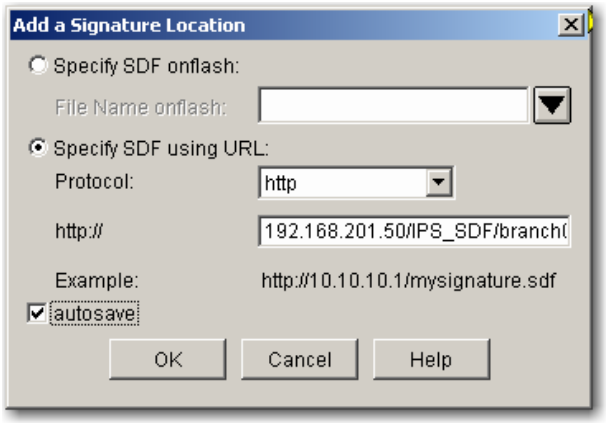
Figure 3. Select Interfaces Tab



At the Cisco SDM Location window, specify the location from which Cisco SDM should be loaded by Cisco IOS IPS. In the following scenario, click the Add… button. The Add a Signature Location window appears (Figure 4). Select the Specify SDF using URL button and perform the following steps:

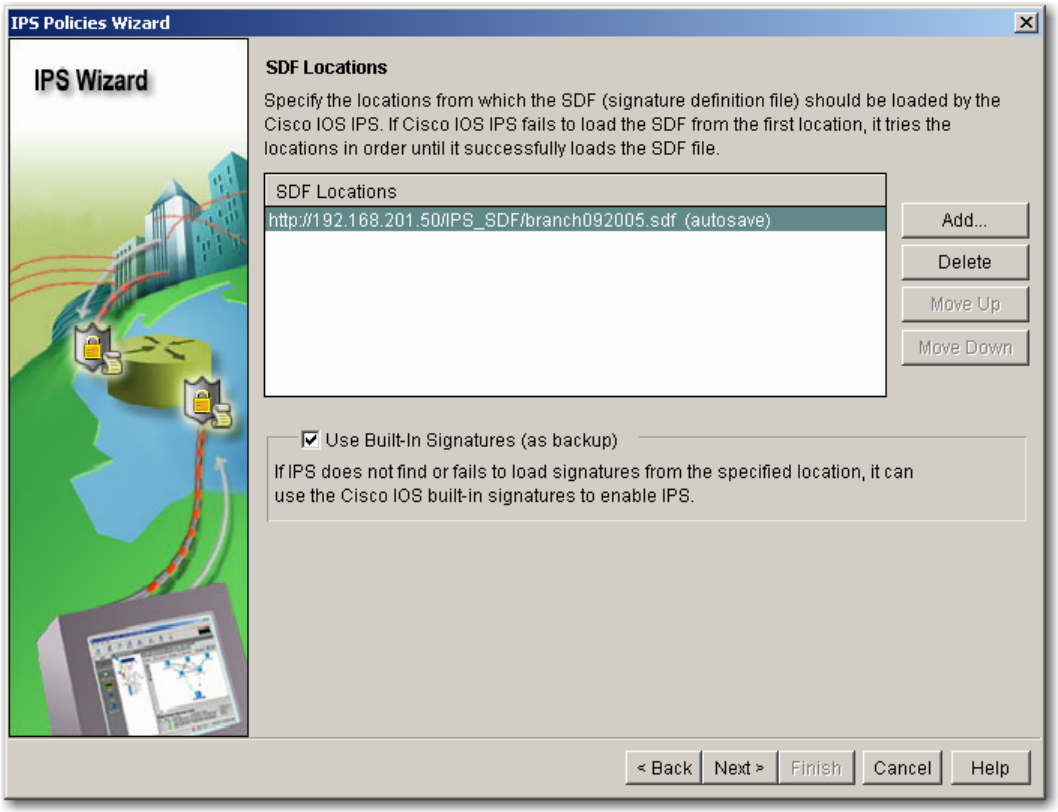
- In the Protocol box, enter http.
- In the http:// box, enter 192.168.201.50/IPS_SDF/branch092005.sdf.
- Check the autosave option.
- Click OK.

Figure 4. Specify SDF Location



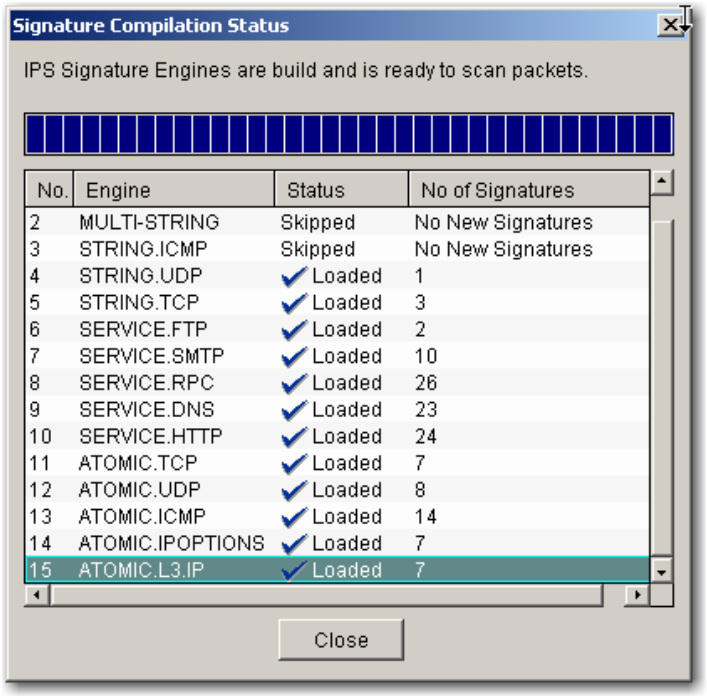
The SDF Locations window appears (Figure 5). Check the Use Built-in Signatures (as backup) option and click Next.

Figure 5. SDF Locations Window



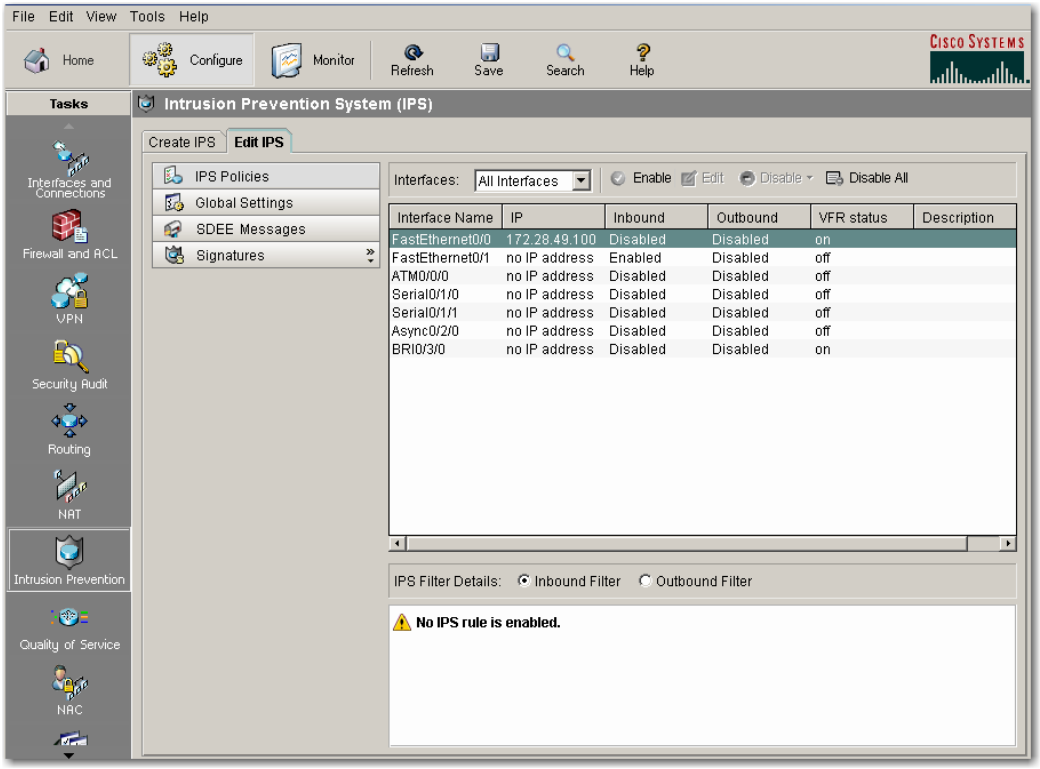
If you are satisfied with the configuration, click Finish to deliver the configuration. Click OK when the signatures are loaded onto the router memory, then the Signature Compilation Status window displays (Figure 6). Click OK to close the message window.

Figure 6. Signature Compilation Status Window



You are redirected to the Edit IPS tab in the Intrusion Prevention System (IPS) window. Figure 7 shows that IPS Inbound is enabled on FastEthernet0/1.

Figure 7. Updated IPS Signatures in IPS Policies



To verify the SDF location, click Global Settings (Figure 8). The Cisco SDM creates a new SDF, sdmips.sdf, in the router's flash memory as the primary IPS signature source file. You can enable and disable syslog notification, edit SDEE parameters and Engine Option (Figure 9), and control SDF locations at Global Settings.

Figure 8. Updated IPS Signatures in Global Settings

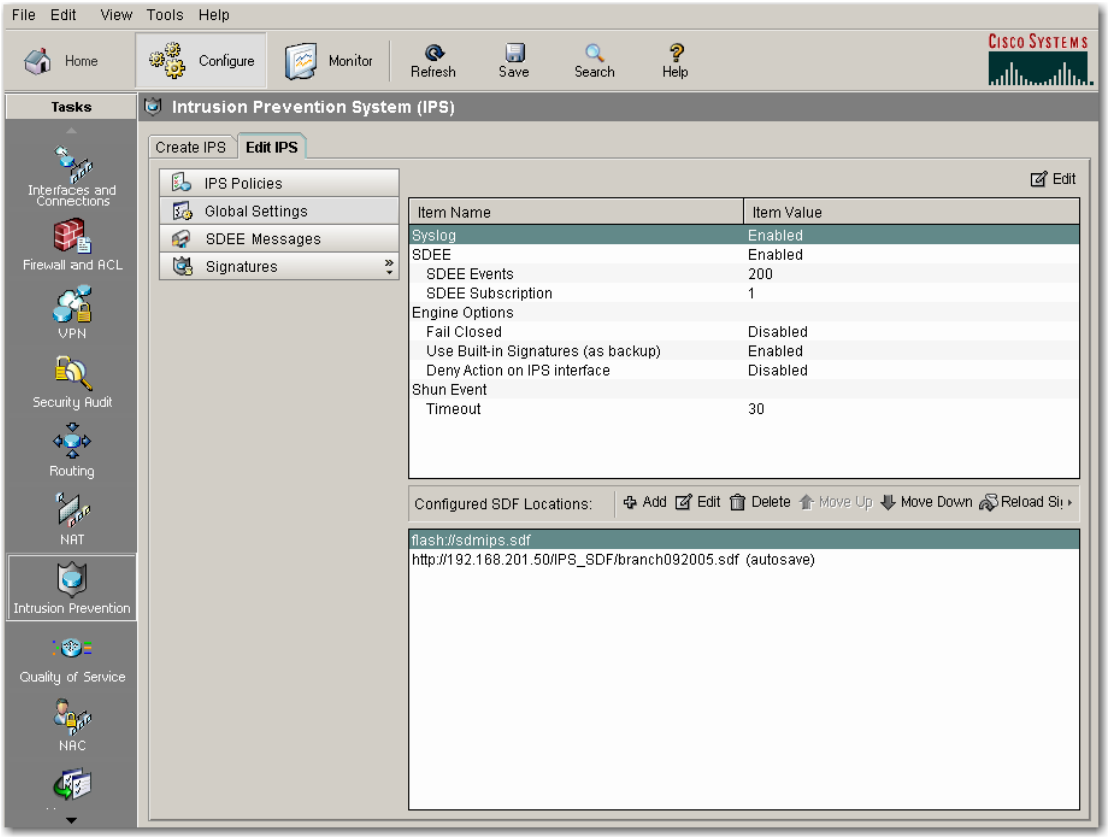
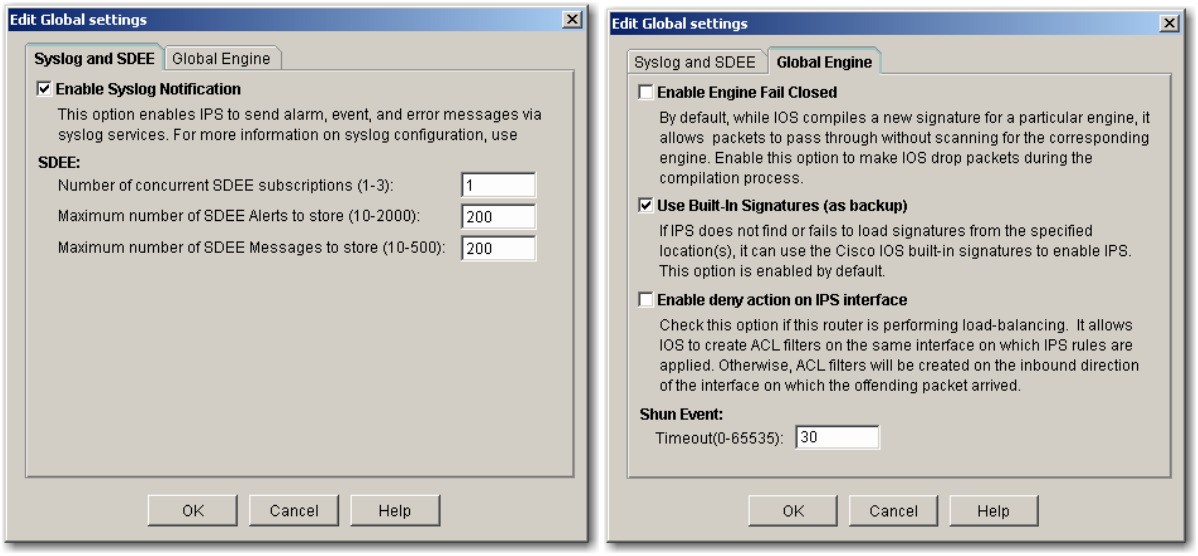


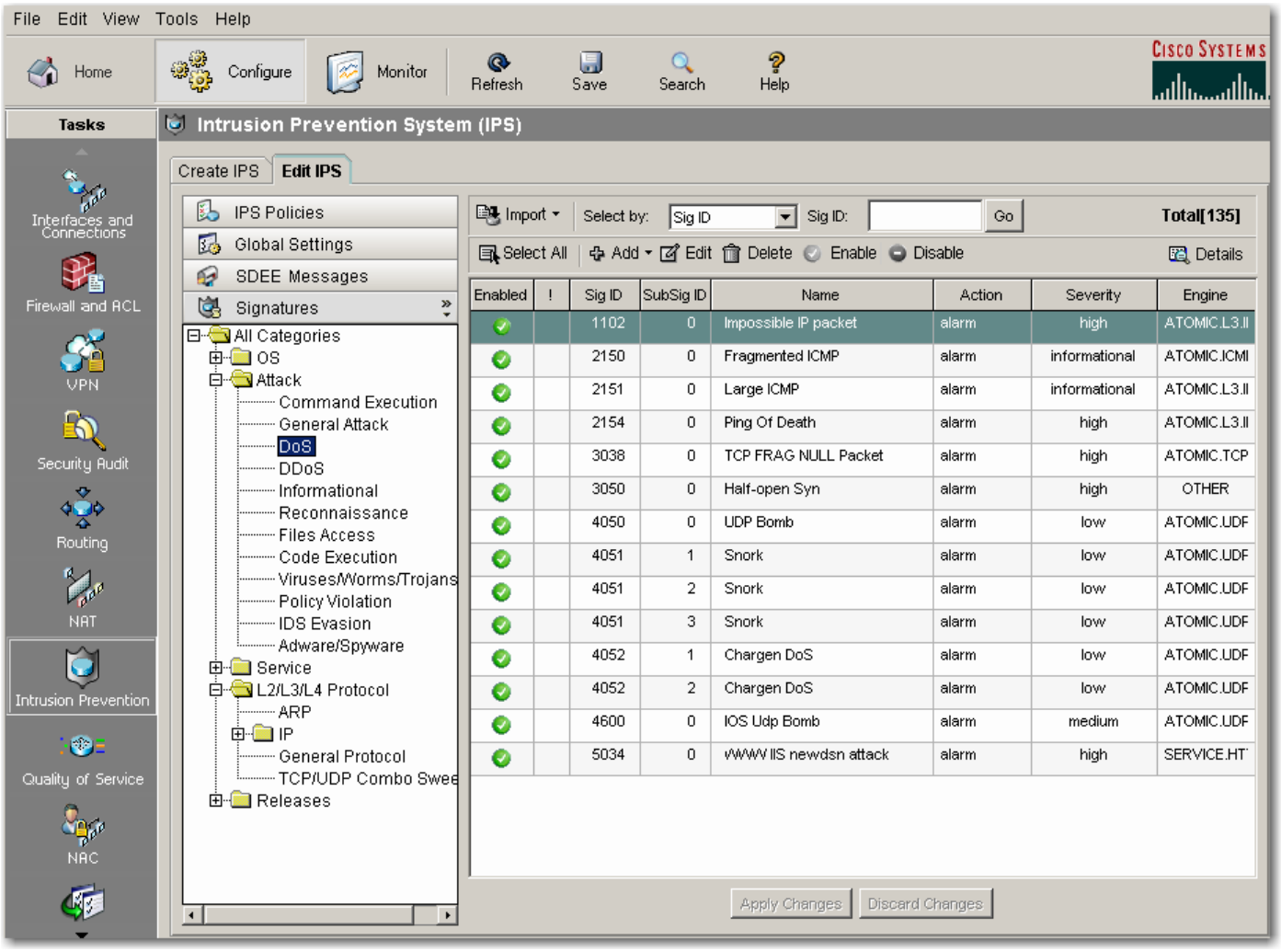
Figure 9. Tabs in the Edit Global Settings Window



Click Signatures in the Edit IPS tab to view the imported IPS signatures. In this example, there are 135 signatures in the SDF (Figure 10) shown on the upper panel of the signature list. The category tree enables you to filter the signature list on the right panel based on the type of signature you want to view.

Select the category of signature that you want to display; for example, select Attack from the category tree. The signature list panel displays the signatures for the Attack type. If a plus sign (+) appears to the left of the category branch, there are subcategories you can use to refine the filter. Click on the sign to expand the branch and select the subcategory you want to display. If the signature list is empty, there are no signatures available for that type.

Figure 10. DoS Attack Signatures Listing



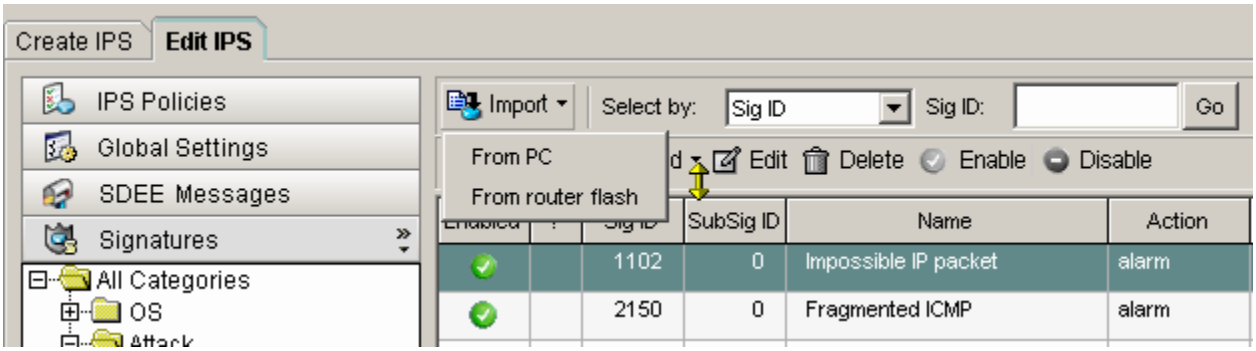
At the top of the Edit IPS tab, the Select by box enables you to filter the display by type of signature. First select a criterion in the Select by: list, then select the value for that criterion in the list to the right.

Scenario 2: Update IPS Signatures

This scenario shows how to update the IPS signatures with the latest SDF. Downloading the SDF from Cisco is not covered in this scenario. To import an SDF from a PC, follow these steps:

1. Click Import in the Edit IPS/Signatures window and select From PC in the dropdown menu (Figure 11).

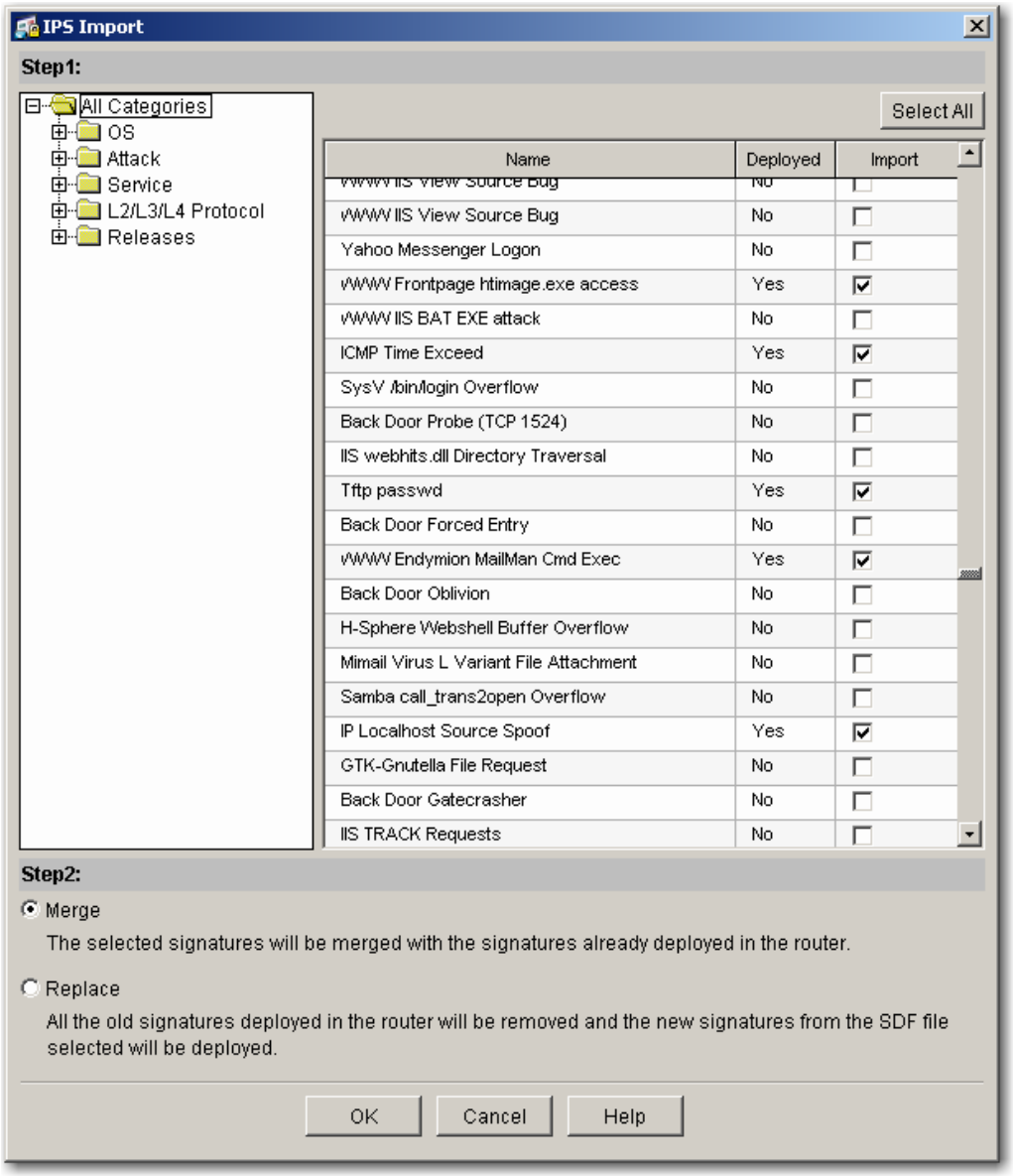
Figure 11. Import Signatures From PC



2. The Windows File Management window appears. Go to the directory and select the SDF, then click Open.

3. The IPS Import window appears (Figure 12).

Figure 12. IPS Import Window



The signature list displays the signatures available in the SDF. Review the signatures and choose the ones you want to import. If you want to import all the signatures, click Select All.

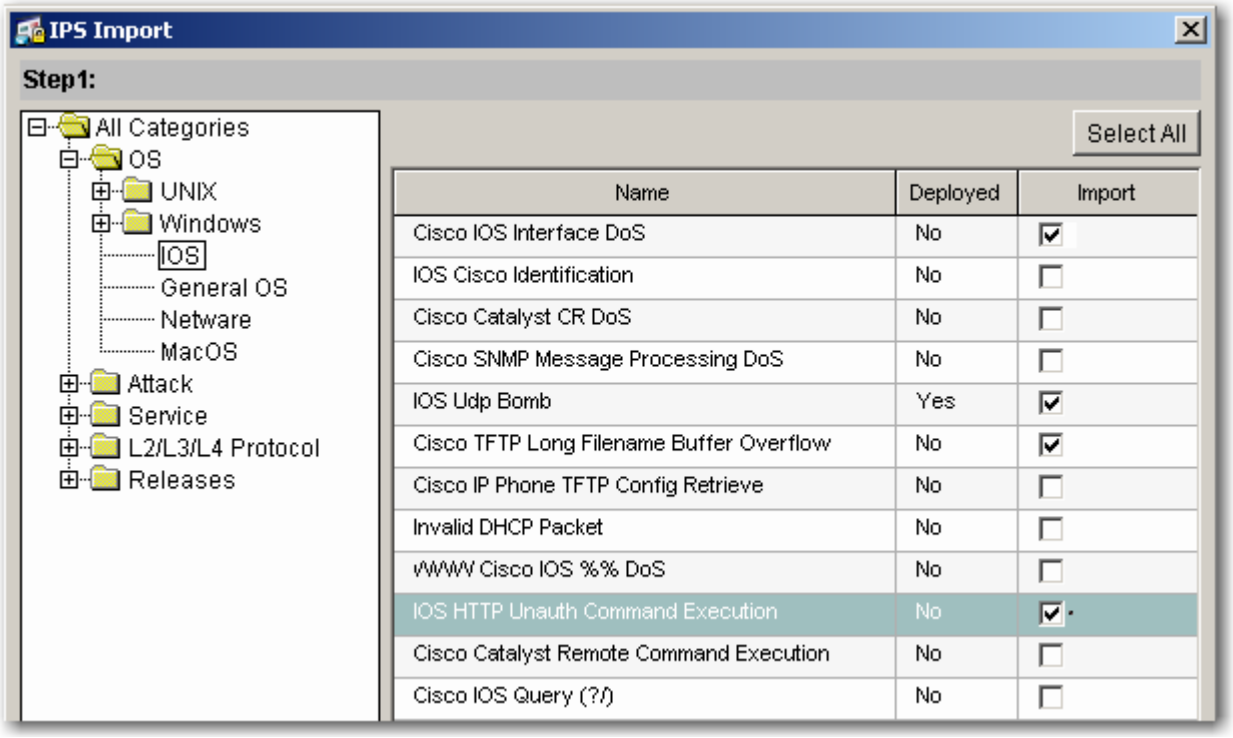
The signature list area has three columns:

- Name: This is the name of the signature, for example, Cisco IOS Interface DoS.
- Deployed: If the signature is already loaded on the router, this column says Yes; if not it says No.
- Import: To import the signature, check the box.

The second step is to decide whether to merge these signatures with the signatures already loaded on the router, or to replace the signatures on the router with these signatures.

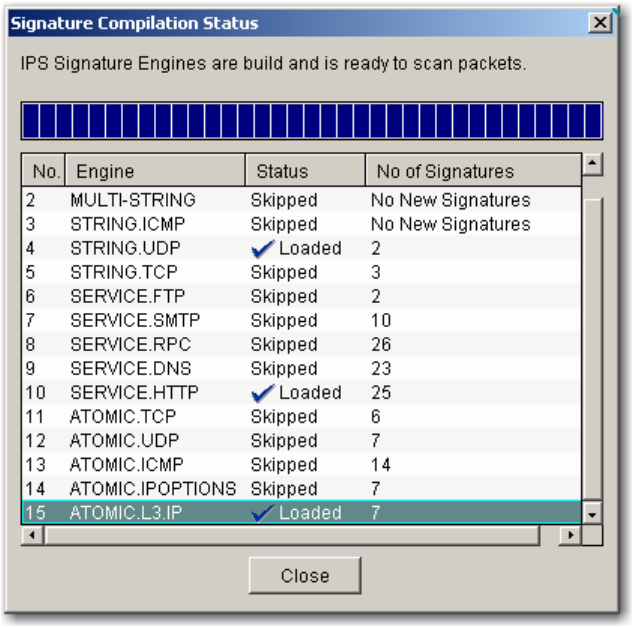
In this example, expand the All Categories list, expand OS, select IOS, check Cisco IOS Interface, check Cisco TFTP Long Filename Buffer Overflow, and check IOS HTTP Unauth Command Execution (Figure 13).

Figure 13. Manually Import Signatures



For the second step, select Merge and click OK. (Note: you can import only one category at a time; if you switch to another category, the current import selection is lost.) The Signature Delivery Status window appears. Click OK when command delivery is finished. The Signature Compilation Status window appears (Figure 14), showing that three signatures in three different engines have been loaded again. Click Close to close the window.

Figure 14. Signature Compilation Status



On the upper panel of the signature list on the Edit IPS/Signature window, there are total of 138 signatures imported.

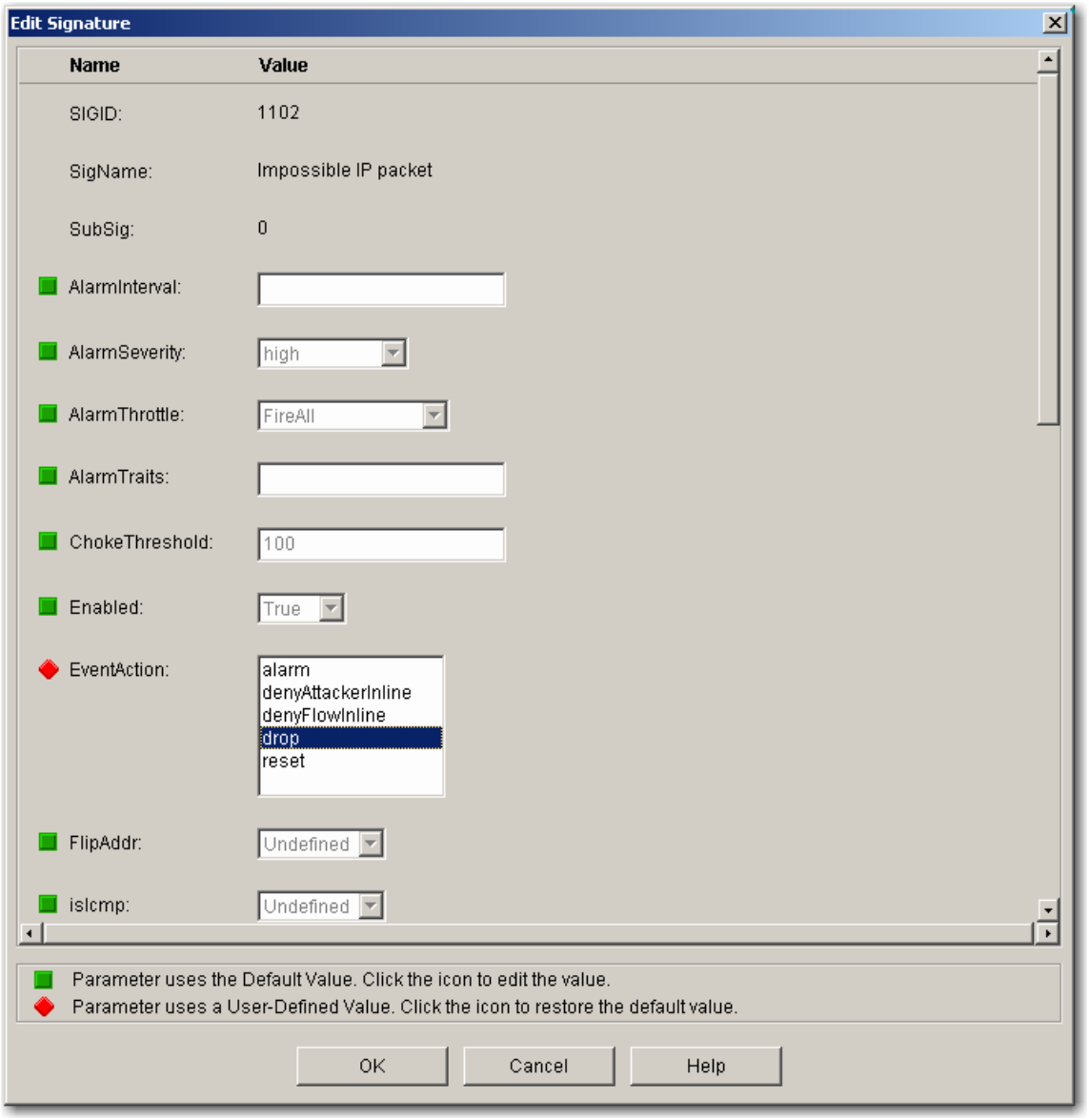
Scenario 3: Tuning IPS Signatures

Cisco SDM IPS allows you to edit, delete, enable, and disable signatures. The two ways to tune a signature are through the Edit Signature window or by right-clicking on Context Menu. This example shows how to edit signatures.

To change the action of the Attack/DoS signature with Sig ID = 1102 from “alarm” to “drop” using the Edit Signature window, take the following steps:

1. Expand All Categories, expand Attack, and select DoS.
2. Use the Select By filter to select the signature with Sig ID = 1102.
3. Click Edit in the toolbar. The Edit Signature window appears.
4. Enable EventAction by clicking the green button, which becomes a red diamond, and the choices become available.
5. Select the drop option (Figure 15).
6. Click OK to close the Edit Signature window.
7. Click Apply Changes to deliver the change to the router.

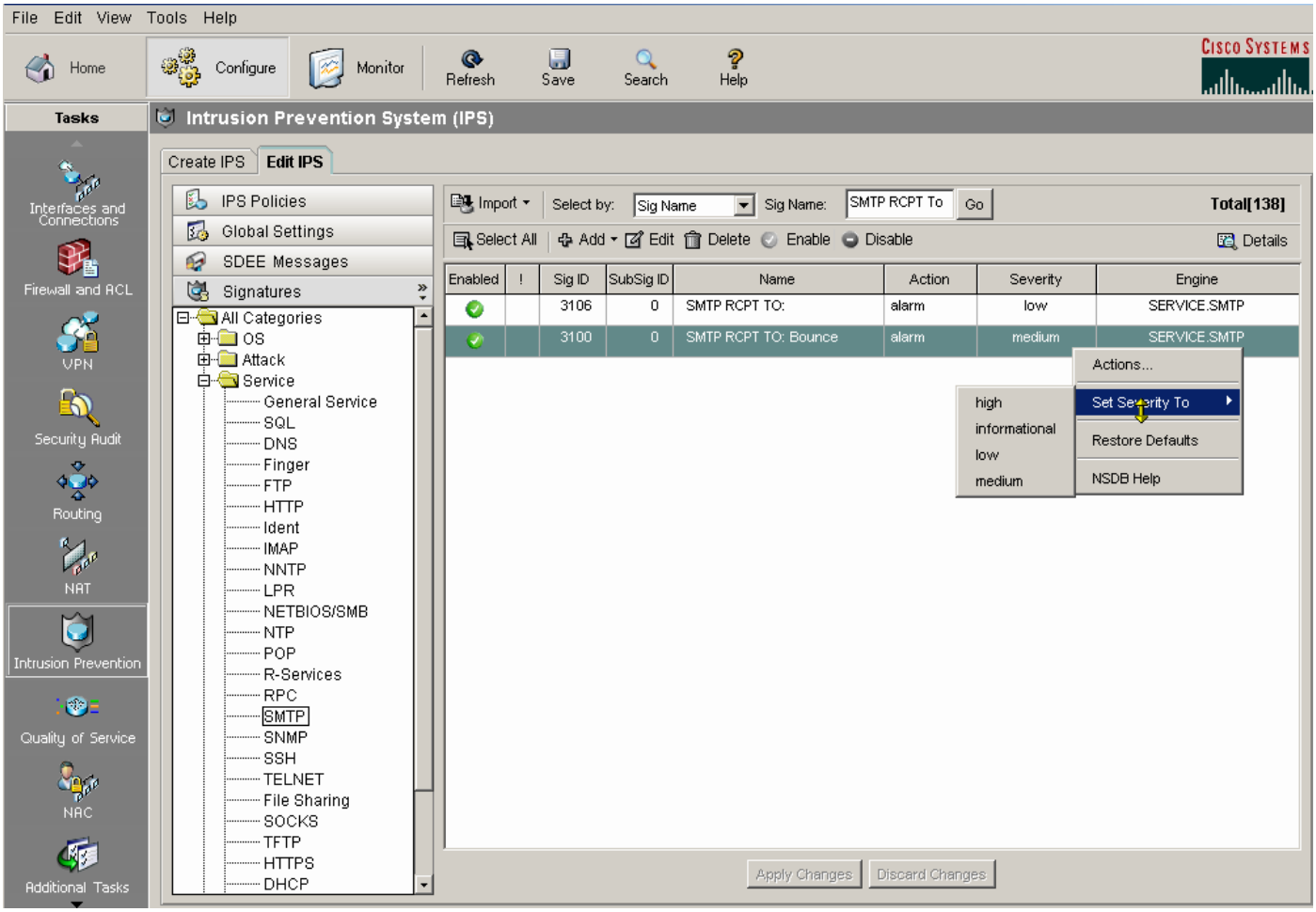
Figure 15. Edit Signature



To change the signature SMTP RCPT To: Bounce with Sig ID 3100 from medium severity to low severity, take the following steps:

1. Expand All Categories, expand Service, and select SMTP.
2. Use Select By filter to select the signature with Sig Name = SMTP RCPT To.
3. Select the signature with Sig ID 3100.
4. Left-click to bring up the popup menu.
5. Expand Set Severity To.
6. Select the low option (Figure 16).

Figure 16. Change Signature Severity in Context Menu



In summary, the Cisco SDM IPS can help you deploy, view, and tune Cisco IOS IPS signatures easily and quickly. For more information about Cisco IOS Firewall IPS commands, see: http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123tcr/123tsr/sec_01gt.pdf

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe