CHAPTER 24

Cisco IOS IPS

The Cisco IOS Intrusion Prevention System (Cisco IOS IPS) allows you to manage intrusion prevention on routers that use Cisco IOS Release 12.3(8)T4 or later releases. Cisco IOS IPS lets you monitor and prevents intrusions by comparing traffic against signatures of known threats and blocking the traffic when a threat is detected.

Cisco SDM lets you control the application of Cisco IOS IPS on interfaces, import and edit signature definition files (SDF) from Cisco.com, and configure the action that Cisco IOS IPS is to take if a threat is detected.

IPS Tabs

Use the tabs at the top of the IPS window to go to the area where you need to work.

- Create IPS—Click to go to the IPS Rule wizard to create a new Cisco IOS IPS rule.
- Edit IPS—Click to edit Cisco IOS IPS rules and apply or remove them from interfaces.
- Security Dashboard—Click to view the Top Threats table and deploy signatures associated with those threats.
- IPS Migration—If the router runs a Cisco IOS image of release 12.4(11)T or later, you can migrate Cisco IOS IPS configurations created using earlier versions of the Cisco IOS.

IPS Rules

A Cisco IOS IPS rule specifies an interface, the type and direction of traffic that it is to examine, and the location of the signature definition file (SDF) that the router uses.

Create IPS

In this window you can launch the IPS Rule wizard.

The IPS Rule wizard prompts you for the following information:

- The interface on which to apply the rule
- The traffic on which to apply Cisco IOS IPS (inbound, outbound, or both)
- The location of the signature definition file (SDF)

For Cisco IOS 12.4(11) or later images, you are also prompted for the following information:

- Where you want to store files that contain changes to the IOS IPS configuration. A file that stores this type of information is referred to as a delta file.
- The public key to use to access the information in the delta files.
- The signature category. The basic signature category is appropriate for routers with less than 128 Mb of flash memory. The advanced signature category is appropriate for routers with more than 128 Mb of flash memory.

The use case scenario illustrates a configuration in which a Cisco IOS IPS rule is used. After you create the Cisco IOS IPS rule and deliver the configuration to the router, you can modify the rule by clicking the **Edit IPS** tab.

For more information on Cisco IOS IPS, see the documents at the following link:

http://www.cisco.com/en/US/products/ps6634/prod_white_papers_list.html

Click the **Launch IPS Rule Wizard** button to begin.

Create IPS: Welcome

This window provides a summary of the tasks to perform when you complete the IPS Rule wizard.

Click **Next** to begin configuring a Cisco IOS IPS rule.

Create IPS: Select Interfaces

Choose the interfaces on which you want to apply the Cisco IOS IPS rule by specifying whether the rule is to be applied to inbound traffic or outbound traffic. If you check both the inbound and the outbound boxes, the rule applies to traffic flowing in both directions.

For example: the following settings apply Cisco IOS IPS to inbound traffic on the BRI 0 interface, and both inbound and outbound traffic on the FastEthernet 0 interface.

Interface Name	Inbound	Outbound
BRI 0	Check	—
FastEthernet 0	Check	Check

Create IPS: SDF Location

Cisco IOS IPS examines traffic by comparing it against signatures contained in a signature definition file (SDF). The SDF can be located in router flash memory or on a remote system that the router can reach. You can specify multiple SDF locations so that if the router is not able to contact the first location, it can attempt to contact other locations until it obtains an SDF.

Use the **Add**, **Delete**, **Move Up**, and **Move Down** buttons to add, remove, and order a list of SDF locations that the router can attempt to contact to obtain an SDF. The router starts at the first entry, and works down the list until it obtains an SDF.

Cisco IOS images that support Cisco IOS IPS contain built-in signatures. If you check the box at the bottom of the window, the router will use the built-in signatures only if it cannot obtain an SDF from any location in the list.

Create IPS: Signature File

The Cisco IOS IPS signature file contains the default signature information present in each update to the file on Cisco.com. Any changes made to this configuration are saved in a delta file. For security, the delta file must be digitally signed. Specify the location of the signature file and provide the name and text of the public key that will be used to sign the delta file in this window.

This help topic describes the Signature File window that is displayed when the router runs Cisco IOS 12.4(11)T and later releases.

Specify the signature file you want to use with IOS IPS

If the signature file is already present on the PC, router flash memory, or on a remote system, click **Specify the signature file you want to use with IOS IPS** to display a dialog in which you can specify the signature file location.

Get the latest signature file from CCO and save to PC

Click **Get the latest signature file from CCO and save to PC** if the signature file is not yet present on the PC or in router flash memory. Click **Browse** to specify where you want to save the signature file, and then click **Download** to begin downloading the file. Cisco SDM downloads the signature file to the location that you specify.

Configure Public Key

Each change to the signature configuration is saved in the delta file. This file must be digitally signed with a public key. You can obtain a key from Cisco.com and paste the information in the Name and Key fields.

Note If you have already added a public key to the configuration using the Cisco IOS CLI, you must still provide a public key in this screen. After you have completed the Cisco IOS IPS Rule Wizard, you can go to **Edit IPS > Global Settings**. In the Global Settings screen, you can click **Edit** in the Edit IPS Prerequisites area, and then click **Public Key** to display the Public Key dialog. In that dialog, you can delete public keys that you do not need.

Follow these steps to place the public-key information in the Name and Key fields.

Step 1 Go to the following link to obtain the public key:

http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup

Step 2 Download the key to your PC.

Step 3 Copy the text after the phrase "named-key" into the Name field. For example, if the line of text including the name is the following:

```
named-key realm-cisco.pub signature
```

copy `realm-cisco.pub signature` to the Name field:

Step 4 Copy the text between the phrase `key-string`, and the word `quit` into the Key field. Example text follows:

```
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
```

Create IPS: Configuration File Location and Category

Specify a location for storing the signature information that the Cisco IOS IPS will use. This information consists of the signature file and the delta file that is created when changes are made to the signature information.

This help topic describes the Configuration File Location window that is displayed when the router runs Cisco IOS 12.4(11)T and later releases.

Config Location

Click the button to the right of the Config Location field to display a dialog that allows you to specify a location. After you enter information in that dialog, Cisco SDM displays the path to the location in this field.

Choose Category

Because router memory and resource constraints may prevent the use of all the available signatures, there are two categories of signatures—**basic** and **advanced**. In the Choose Category field, choose the category that will allow the Cisco IOS IPS to function efficiently on the router. The basic category is appropriate for routers with less than 128 MB of available flash memory. The advanced category is appropriate for routers with more than 128 MB of available flash memory.

Add or Edit a Config Location

Specify a location for storing the signature information and the delta file that the Cisco IOS IPS will use.

Specify config location on this router

To specify a location on the router, click the button to the right of the Directory Name field and choose the directory in which you want to store the configuration information.

Note If the router has a LEFS-based file system, you will be unable to create a directory in router memory. In this case, flash: is used as the config location.

Specify config location using URL

To specify a location on a remote system, specify the protocol and path of the URL needed to reach the location. For example, if you want to specify the URL http://172.27.108.5/ips-cfg, enter 172.27.108.5/ips-cfg.

Note Do not include the protocol in the path that you enter. Cisco SDM adds the protocol automatically. If you enter the protocol, Cisco SDM displays an error message.

In the No. of Retries and Timeout fields, specify how many times the router is to attempt to contact the remote system, and how long the router is to wait for a response before stopping the contacting attempts.

Directory Selection

Click the folder in which you want to store configuration information. If you want to create a new folder, click **New Folder**, provide a name for it in the dialog displayed, select it, and click **OK**.

Signature File

Specify the location of the signature file that the Cisco IOS IPS will use.

Specify Signature File on Flash

If the signature file is located on router flash memory, click the button to the right of the field. Cisco SDM displays the signature file names of the correct format for you to choose.

Specify Signature File using URL

If the signature file is located on a remote system, select the protocol to be used, and enter the path to the file. For example, if the signature file IOS-S259-CLI.pkg is located at 10.10.10.5, and the FTP protocol will be used , select **ftp** as the protocol, and enter

```
10.10.10.5/IOS-S259-CLI.pkg
```

Note Do not include the protocol in the path that you enter. Cisco SDM adds the protocol automatically. If you enter the protocol, Cisco SDM displays an error message. Additionally, when you use an URL, you must specify a filename that conforms to the IOS-Snnn-CLI.pkg file naming convention, such as the file used in the previous example.

Specify Signature File on PC

If the signature file is located on the PC, click **Browse**, navigate to the folder containing the file, and select the filename. You must choose an Cisco SDM-specific package of the format sigv5-SDM-S*xxx*.zip; for example, sigv5-SDM-S260.zip.

Create IPS: Summary

Here is an example of a Cisco IOS IPS summary display on a router running a Cisco IOS release earlier than 121.4(11)T.

```
Selected Interface: FastEthernet 0/1

IPS Scanning Direction: Both

Signature Definition File Location: flash//sdmips.sdf

Built-in enabled: yes
```

In this example, Cisco IOS IPS is enabled on the FastEthernet 0/1 interface, and both inbound and outbound traffic is scanned. The SDF is named sdmips.sdf and is located in router flash memory. The router is configured to use the signature definitions built in to the Cisco IOS image that the router uses.

Create IPS: Summary

The Summary window displays the information that you have entered so that you can review it before delivering the changes to the router.

This help topic describes the Summary window that is displayed when the router runs Cisco IOS 12.4(11)T and later releases. A sample Summary window display follows.

```
IPS rule will be applied to the outgoing traffic on the following interfaces.
     FastEthernet0/1
IPS rule will be applied to the incoming traffic on the following interfaces.
     FastEthernet0/0
Signature File location:
     C:\SDM-Test-folder\sigv5-SDM-S260.zip
Public Key:
       30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00B8BE84
  33251FA8 F79E393B B2341A13 CAFFC5E6 D5B3645E 7618398A EFB0AC74 11705BEA
  93A96425 CF579F1C EA6A5F29 310F7A09 46737447 27D13206 F47658C7 885E9732
  CAD15023 619FCE8A D3A2BCD1 0ADA4D88 3CBD93DB 265E317E 73BE085E AD5B1A95
  59D8438D 5377CB6A AC5D5EDC 04993A74 53C3A058 8F2A8642 F7803424 9B020301 0001

Config Location
     flash:/configloc/
Selected category of signatures:
     advanced
```

In this example, the Cisco IOS IPS policy is applied to the FastEthernet 0/0 and the FastEthernet 0/1 interfaces. The signature file is located on the PC. The config location is on router flash memory, in a directory named configloc.

Edit IPS

In this window you can view the Cisco IOS IPS buttons for configuring and managing Cisco IOS IPS policies, security messages, signatures, and more.

IPS Policies Button

Click to display the Edit IPS window, where you can enable or disableCisco IOS IPS on an interface and view information about how Cisco IOS IPS is applied. If you enableCisco IOS IPS on an interface, you can optionally specify which traffic to examine for intrusion.

Global Settings Button

Click to display the Edit IPS: Global Settings window, where you make settings that affect the overall operation of Cisco IOS IPS.

Auto Update

This button appears if the Cisco IOS image on the router is version 12.4(11)T or later. Auto Update allows you to configure the router to obtain the latest signature updates from the Cisco Security Center automatically. Refer to Edit IPS: Auto Update for more information.

SEAP Configuration

This button appears if the Cisco IOS image on the router is version 12.4(11)T or later. Signature Event Action Processing (SEAP) gives you greater control over IOS IPS by providing advanced filtering and overrides.

SDEE Messages Button

Secure Device Event Exchange (SDEE) messages report on the progress of Cisco IOS IPS initialization and operation. Click to display the Edit IPS: SDEE Messages window, where you can review SDEE messages and filter them to display only error, status, or alert messages.

Signatures Button

Click to display the Edit IPS: Signatures window where you can manage signatures on the router.

NM CIDS Button

This button is visible if a Cisco Intrusion Detection System network module is installed in the router. Click to manage the IDS module.

Edit IPS: IPS Policies

This window displays the Cisco IOS IPS status of all router interfaces, and allows you to enable and disable Cisco IOS IPS on interfaces.

Interfaces

Use this list to filter the interfaces shown in the interface list area. Choose one of the following:

- All interfaces—All interfaces on the router.
- IPS interfaces—Interfaces on which Cisco IOS IPS has been enabled.

Enable Button

Click to enable Cisco IOS IPS on the specified interface. You can specify the traffic directions to which Cisco IOS IPS is to be applied, and the ACLs used to define the type of traffic you want to examine. See Enable or Edit IPS on an Interface for more information.

Edit Button

Click to edit the Cisco IOS IPS characteristics applied to the specified interface.

Disable Button

Click to disable Cisco IOS IPS on the specified interface. A context menu shows you the traffic directions on which Cisco IOS IPS has been applied, and you can choose the direction on which you want to disable Cisco IOS IPS. If you disable Cisco IOS IPS on an interface to which it has been applied, Cisco SDM dissociates any Cisco IOS IPS rules from that interface.

Disable All Button

Click to disable Cisco IOS IPS on all interfaces on which it has been enabled. If you disable Cisco IOS IPS on an interface to which it has been applied, Cisco SDM dissociates any Cisco IOS IPS rules from that interface.

Interface Name

The name of the interface. For example: Serial0/0, or FE0/1.

IP

This column can contain the following types of IP addresses:

- Configured IP address of the interface.
- DHCP client—The interface receives an IP address from a Dynamic Host Configuration Protocol (DHCP) server.
- Negotiated—The interface receives an IP address through negotiation with the remote device.
- Unnumbered—The router will use one of a pool of IP addresses supplied by your service provider for your router and for the devices on your LAN.
- Not applicable—The interface type cannot be assigned an IP address.

Inbound IPS/Outbound IPS

- Enabled—Cisco IOS IPS is enabled for this traffic direction.
- Disabled—Cisco IOS IPS is disabled for this traffic direction.

VFR Status

Virtual Fragment Reassembly (VFR) status. The possible values are:

- On—VFR is enabled.
- Off—VFR is disabled.

Cisco IOS IPS cannot identify the contents of IP fragments, nor can it gather port information from the fragment in order to match it with a signature. Therefore, fragments can pass through the network without being examined or without dynamic access control list (ACL) creation.

VFR enables the Cisco IOS Firewall to create the appropriate dynamic ACLs, thereby protecting the network from various fragmentation attacks.

Description

A description of the connection, if added.

IPS Filter Details

If no filter is applied to traffic, this area contains no entries. If a filter is applied, the name or number of the ACL is shown in parentheses.

Inbound and Outbound Filter Buttons

Click to view the entries of the filter applied to inbound or outbound traffic.

Field Descriptions

Action—Whether the traffic is permitted or denied.

Permit source traffic.

Deny source traffic.

Source—Network or host address, or any host or network.

Destination—Network or host address, or any host or network.

Service—Type of service filtered: IP, TCP, UDP, IGMP, or ICMP.

Log—Whether or not denied traffic is logged.

Attributes—Options configured using the CLI.

Description—Any description provided.

Enable or Edit IPS on an Interface

Use this window to choose the interfaces on which you want to enable intrusion detection, and to specify the IPS filters for examining traffic.

Both, Inbound, and Outbound Buttons

Use these buttons to specify whether you are going to enable Cisco IOS IPS on both inbound and outbound traffic, only inbound traffic, or only outbound traffic.

Inbound Filter

(Optional) Enter the name or number of the access rule that specifies the inbound traffic to be examined. The ACL that you specify appears in the IPS Rules Configuration window when the interface with which it is associated is chosen. If you need to browse for the access rule or create a new one, click the **...** button.

Outbound Filter

(Optional) Enter the name or number of the access rule that specifies the outbound traffic to be examined. The ACL that you specify appears in the IPS Rules Configuration window when the interface with which it is associated is chosen. If you need to browse for the access rule or create a new one, click the **...** button.

... Button

Use this button to specify a filter. Click to display a menu with the following options:

- Choose an existing rule. See Select a Rule for more information.
- Create a new rule. See Add or Edit a Rule for more information.
- None (clear rule association). Use this option to remove a filter from a traffic direction to which it has been applied.

Enable fragment checking for this interface

(Enabled by default). Check if you want the Cisco IOS firewall to check for IP fragments on this interface. See VFR Status for more information.

Enable fragment checking on other interfaces

If fragment checking is enabled for outbound traffic, the router must examine the inbound traffic that arrives on the interfaces that send outbound traffic to the interface being configured. Specify these interfaces below.

If the Inbound radio button is chosen, this area does not appear.

Specify Signature File

The Specify Signature File box contains information about the SDF version that the router is using, and enables you to update the SDF to a more recent version. To specify a new SDF, click the **...** button next to the Signature File field and specify a new file in the displayed dialog.

Edit IPS: Global Settings

This window allows you to view and configure global settings for Cisco IPS. This help topic describes the information that you may see if the running Cisco IOS image is earlier than version 12.4(11)T.

Global Settings Table

This table in the Global Settings window displays the current global settings and their values. Click **Edit** to change any of these values.

Item Name	Item Value
Syslog	If enabled, then notifications are sent to the syslog server specified in System Properties.
SDEE	Security Device Event Exchange. If enabled, SDEE events are generated.
SDEE Events	Number of SDEE events to store in the router buffer.
SDEE Subscription	Number of concurrent SDEE subscriptions.

Engine Options	The engine options are: • Fail Closed—By default, while the Cisco IOS compiles a new signature for a particular engine, it allows packets to pass through without scanning for the corresponding engine. When enabled, this option makes the Cisco IOS drop packets during the compilation process. • Use Built-in Signatures (as backup)—If Cisco IOS IPS does not find signatures or fails to load them from the specified locations, it can use the Cisco IOS built-in signatures to enable Cisco IOS IPS. This option is enabled by default. • Deny Action on IPS Interface—We recommend this when the router is performing load balancing. When enabled, this option causes Cisco IOS IPS to enable ACLs on Cisco IOS IPS interfaces instead of enabling them on the interfaces from which attack traffic came.
Shun Events	This option uses the Shun Time parameter. Shun Time is the amount of time that shun actions are to be in effect. A shun action occurs if a host or network is added to an ACL to deny traffic from that host or network.

Configured SDF Locations

A signature location is a URL that provides a path to an SDF. To find an SDF, the router attempts to contact the first location in the list. If it fails, it tries each subsequent location in turn until it finds an SDF.

Add Button

Click to add a URL to the list.

Edit Button

Click to edit a specified location.

Delete Button

Click to delete a specified location.

Move Up an d Move Down Buttons

Use to change the order of preference for the URLs in the list.

Reload Signatures

Click to recompile signatures in all signature engines. During the time that signatures are being recompiled in a signature engine, the Cisco IOS software can not use that engine's signatures to scan packets.

Edit Global Settings

Edit settings that affect the overall operation of Cisco IOS IPS in this window, in the Syslog and SDEE and Global Engine tabs.

Enable Syslog Notification (Syslog and SDEE Tab)

Check this checkbox to enable the router to send alarm, event, and error messages to a syslog server. A syslog server must be identified in System Properties for this notification method to work.

SDEE (Syslog and SDEE Tab)

Enter the number of concurrent SDEE subscriptions, in the range of 1–3, in the **Number of concurrent SDEE subscriptions** field. An SDEE subscription is a live feed of SDEE events.

In the **Maximum number of SDEE alerts to store** field, enter the maximum number of SDEE alerts that you want the router to store, in the range of 10–2000. Storing more alerts uses more router memory.

In the **Maximum number of SDEE messages to store** field, enter the maximum number of SDEE messages that you want the router to store, in the range of 10–500. Storing more messages uses more router memory.

Enable Engine Fail Closed (Global Engine Tab)

By default, while the Cisco IOS software compiles a new signature for a particular engine, it allows packets to pass through without scanning for the corresponding engine. Enable this option to make the Cisco IOS software drop packets during the compilation process.

Use Built-in Signatures (as backup) (Global Engine Tab)

If Cisco IOS IPS does not find or fails to load signatures from the specified locations, it can use the Cisco IOS built-in signatures to enable Cisco IOS IPS. This option is enabled by default.

Enable Deny Action on IPS interface (Global Engine Tab)

This option is applicable if signature actions are configured to "denyAttackerInline" or "denyFlowInline." By default, Cisco IOS IPS applies ACLs to the interfaces from which attack traffic came, and not to Cisco IOS IPS interfaces. Enabling this option causes Cisco IOS IPS to apply the ACLs directly to the Cisco IOS IPS interfaces, and not to the interfaces that originally received the attack traffic. If the router is not performing load balancing, do not enable this setting. If the router is performing load balancing, we recommend that you enable this setting.

Timeout (Global Engine Tab)

This option lets you set the number of minutes, in the range of 0–65535, that shun actions are to be in effect. The default value is 30 minutes. A shun action occurs if a host or network is added to an ACL to deny traffic from that host or network.

Add or Edit a Signature Location

Specify the location from which Cisco IOS IPS should load an SDF. To specify multiple SDF locations, open this dialog again and enter the information for another SDF.

Specify SDF on this router

Specify the part of router memory in which the SDF is located by using the Location drop-down menu. For example: the menu could have the entries *disk0*, *usbflash1*, and *flash*. Then choose the filename by clicking the down arrow next to the File Name field or enter the filename in the File Name field.

Specify SDF using URL

If the SDF is located on a remote system, you can specify the URL at which it resides.

Protocol

Choose the protocol the router should use to obtain the SDF, such as *http* or *https*.

URL

Enter the URL in the following form:

path-to-signature-file

Note The protocol you chose from the Protocol menu appears to the right of the URL field. Do *not* reenter the protocol in the URL field.

The following URL is provided as an example of the format. It is *not* a valid URL to a signature file, and it includes the protocol to show the full URL:

`https://172.16.122.204/mysigs/vsensor.sdf`

Autosave

Check this option if you want the router to automatically save the SDF if the router crashes. This eliminates the need for you to reconfigure Cisco IOS IPS with this SDF when the router comes back up.

Edit IPS: SDEE Messages

This window lists the SDEE messages received by the router. SDEE messages are generated when there are changes to Cisco IOS IPS configuration.

SDEE Messages

Choose the SDEE message type to display:

- All— SDEE error, status, and alert messages are shown.
- Error—Only SDEE error messages are shown.
- Status—Only SDEE status messages are shown.
- Alerts—Only SDEE alert messages are shown.

View By

Choose the SDEE message field to search.

Criteria

Enter the search string.

Go Button

Click to initiate the search on the string entered in the Criteria field.

Type

Types are Error, Status, and Alerts. Click SDEE Message Text to see possible SDEE messages.

Time

Time message was received.

Description

Available description.

Refresh Button

Click to check for new SDEE messages.

Close Button

Click to close the SDEE Messages window.

SDEE Message Text

This topic lists possible SDEE messages.

IDS Status Messages

Error Message

```
ENGINE_BUILDING: %s - %d signatures - %d of %d engines
```

Explanation Triggered when Cisco IOS IPS begins building the signature microengine (SME).

Error Message

```
ENGINE_BUILD_SKIPPED: %s - there are no new signature
definitions for this engine
```

Explanation Triggered when there are no signature definitions or no changes to the existing signature definitions of an Intrusion Detection System SME.

Error Message

```
ENGINE_READY: %s - %d ms - packets for this engine will be
scanned
```

Explanation Triggered when an IDS SME is built and ready to scan packets.

Error Message

```
SDF_LOAD_SUCCESS: SDF loaded successfully from %s
```

Explanation Triggered when an SDF file is loaded successfully from a given location.

Error Message

```
BUILTIN_SIGS: %s to load builtin signatures
```

Explanation Triggered when the router resorts to loading the builtin signatures.

IDS Error Messages

Error Message

```
ENGINE_BUILD_FAILED: %s - %d ms - engine build failed - %s
```

Explanation Triggered when Cisco IOS IPS fails to build one of the engines after an SDF file is loaded. One message is sent for each failed engine. This means that the Cisco IOS IPS engine failed to import signatures for the specified engine in the message. Insufficient memory is the most probable cause of this problem. If this happens, the new imported signature that belongs to this engine is discarded by Cisco IOS IPS.

Error Message

```
SDF_PARSE_FAILED: %s at Line %d Col %d Byte %d Len %d
```

Explanation Triggered when an SDF file does not parse correctly.

Error Message

```
SDF_LOAD_FAILED: failed to %s SDF from %s
```

Explanation Triggered when an SDF file fails to load for some reason.

Error Message

```
DISABLED: %s - IDS disabled
```

Explanation IDS has been disabled. The message should indicate the cause.

Error Message

```
SYSERROR: Unexpected error (%s) at line %d func %s() file %s
```

Explanation Triggered when an unexpected internal system error occurs.

Edit IPS: Global Settings

Several Cisco IOS IPS configuration options are available with Cisco IOS 12.4(11)T and later images. These are described in this help topic. Screen controls and configuration options available prior to Cisco IOS 12.4(11)T, such as the Syslog and SDEE global settings are described in Edit IPS: Global Settings.

This help topic describes the Global Settings window that is displayed when the router runs Cisco IOS 12.4(11)T and later releases.

Engine Options

The engine options available with Cisco IOS 12.4(11)T and later images are the following:

- Fail Closed—By default, while the Cisco IOS compiles a new signature for a particular engine, it allows packets to pass through without scanning for the corresponding engine. When enabled, this option makes the Cisco IOS drop packets during the compilation process.
- Deny Action on IPS Interface—We recommend this when the router is performing load balancing. When enabled, this option causes Cisco IOS IPS to enable ACLs on Cisco IOS IPS interfaces instead of enabling them on the interfaces from which attack traffic came.

Edit IPS Prerequisites Table

This table displays the information about how the router is provisioned for Cisco IOS IPS. Click **Edit** to change any of these values. The sample data in the following table indicated that the config location is the directory configloc in flash memory, that the router is using the basic category of signatures, and that a public key has been configured to allow the router to access the information in the configloc directory.

Item Name	Item Value
Config Location	flash:/configloc/
Selected Category	basic
Public Key	Configured

Edit Global Settings

The Edit Global Settings dialog contains a Syslog and SDEE tab, and a Global Engine tab. Click the link below for the information that you want to see:

- Syslog and SDEE Tab
- Global Engine Tab

Syslog and SDEE Tab

The Syslog and SDEE dialog displayed when the router uses a Cisco IOS 12.4(11)T or later image allows you to configure syslog notification and parameters for SDEE subscriptions, events and messages.

Enable Syslog Notification

Check this checkbox to enable the router to send alarm, event, and error messages to a syslog server. A syslog server must be identified in System Properties for this notification method to work.

SDEE

Enter the number of concurrent SDEE subscriptions, in the range of 1–3, in the Number of concurrent SDEE subscriptions field. An SDEE subscription is a live feed of SDEE events.

In the Maximum number of SDEE alerts to store field, enter the maximum number of SDEE alerts that you want the router to store, in the range of 10–2000. Storing more alerts uses more router memory.

In the Maximum number of SDEE messages to store field, enter the maximum number of SDEE messages that you want the router to store, in the range of 10–500. Storing more messages uses more router memory.

Global Engine Tab

The Global Engine dialog displayed when the router uses a Cisco IOS 12.4(11)T or later image allows you to configure the settings described in the following sections.

Enable Engine Fail Closed

By default, while the Cisco IOS software compiles a new signature for a particular engine, it allows packets to pass through without scanning for the corresponding engine. Enable this option to make the Cisco IOS software drop packets during the compilation process.

Enable Deny Action on IPS interface

This option is applicable if signature actions are configured to "denyAttackerInline" or "denyFlowInline." By default, Cisco IOS IPS applies ACLs to the interfaces from which attack traffic came, and not to Cisco IOS IPS interfaces. Enabling this option causes Cisco IOS IPS to apply the ACLs directly to the Cisco IOS IPS interfaces, and not to the interfaces that originally received the attack traffic. If the router is not performing load balancing, do not enable this setting. If the router is performing load balancing, we recommend that you enable this setting.

Edit IPS Prerequisites

The Edit IPS Prerequisites dialog contains tabs for the following categories of information. Click on a link for the information that you want to see:

- Config Location Tab
- Category Selection Tab
- Public Key Tab

Config Location Tab

If a config location has been configured on the router, you can edit it. If none has been configured, you can click Add and configure one. The Add button is disabled if a config location is already configured. The Edit button is disabled when no config location has been configured. See Create IPS: Configuration File Location and Category for more information.

Category Selection Tab

If you specify a signature category, SDM configures the router with a subset of signatures appropriate for a specific amount of router memory. You can also remove an existing category configuration if you want to remove category constraints when selecting signatures.

Configure Category

Click **Configure Category** and choose either **basic** or **advanced**. The basic category is appropriate for routers with less than 128 MB of available flash memory. The advanced category is appropriate for routers with more than 128 MB of available flash memory.

Delete Category

If you want to remove the category configuration, click **Delete Category**.

Public Key Tab

This dialog displays the public keys configured for Cisco IOS IPS. You can add keys or delete keys from this dialog. To add a key, click **Add** and configure the key in the dialog displayed.

To remove a key, select the key name and click **Delete**.

Add Public Key

You can copy the name of the key and the key itself from the following site on Cisco.com:

http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup

Copy the key name and paste it into the Name field in this dialog. Then copy the key from the same location and paste it into the Key field. For detailed instructions that explain exactly which parts of the text to copy and paste, see Configure Public Key.

Edit IPS: Auto Update

Signature file updates are posted on Cisco.com. Cisco SDM can download the signature file update that you specify, or it can automatically download the latest signature file update on a defined schedule.

This help topic describes the Auto Update window that is displayed when the router runs Cisco IOS 12.4(11)T and later releases.

Before Configuring Autoupdate

Before configuring autoupdate, you should synchronize the router clock with the clock on your PC. To do this, complete the following steps:

Step 1 Go to **Configure** > **Additional Tasks** > **Router Properties** > **Date/Time**.

Step 2 In the Date/Time window, click **Change Settings**.

Step 3 Check the **Synchronize with my local PC clock** option, and then click the **Synchronize** button.

Step 4 Close the dialog.

Download signature file from Cisco.com

To have Cisco SDM download a specific signature file from Cisco.com to your PC, specify the file that you want Cisco SDM to download, and specify the location where the file will be saved. Signature Package in use displays the version that the Cisco IOS IPS is currently using. A CCO login is required to download signature files and obtain other information from the Cisco.com the Cisco IOS IPS web pages.

To download the latest signature file, click **Get the latest file**. Click **Browse** to specify where you want the file saved, and then click **Download** to save the file to your PC.

To browse the available files before downloading, click **List the available files to download**. Then click the button to the right of the List of signature packages field. Click **Refresh** in the context menu to browse the list of available files. To view the readme file, click **Show readme**. Choose the file that you want, and then use the **Browse** and **Download** buttons to save it to your PC.

Autoupdate

Click **Enable Autoupdate** if you want Cisco SDM to automatically obtain updates from a remote server that you specify.

IPS Autoupdate URL Settings

Enter the username and password required to log in to the server, and enter the URL to the update file in the IPS Autoupdate URL Settings fields. A sample URL follows:

```
tftp//:192.168.0.2/jdoe/ips-auto-update/IOS_update.zip
```

Schedule

Specify a schedule for when you want the router to obtain the update from the server. You can specify multiple values in each column to indicate a range or to indicate multiple time values. To specify that you want to obtain the update from the server at 1:00 a.m. every day, Sunday through Thursday, choose the values in the following table.

Minute	Hour	Date	Day
0	1	Select 1 and select 31.	Check the boxes for Sunday through Thursday.

Click **Apply Changes** to send the changes that you make in the Auto Update fields to the router. Click **Discard Changes** to remove the data that you have entered in these fields.

Edit IPS: SEAP Configuration

Cisco IOS IPS available with Cisco IOS release 12.4(11)T or later implements Signature Event Action Processing (SEAP). This window describes SEAP features that you can configure. To begin configuration, click on one of the buttons under the SEAP Configuration button.

You can configure SEAP settings for Cisco IOS IPS when the router runs Cisco IOS 12.4(11)T and later releases.

Edit IPS: SEAP Configuration: Target Value Rating

The target value rating (TVR) is a user-defined value that represents the user's perceived value of the target host. This allows the user to increase the risk of an event associated with a critical system and to de-emphasize the risk of an event on a low-value target.

Use the buttons to the right of the Target Value Rating and Target IP Address columns to add, remove, and edit target entries. Click **Select All** to highlight all target value ratings automatically. Click **Add** to display a dialog in which you can create a new TVR entry. Click **Edit** to change the IP address information for an entry.

Target Value Rating Column

Targets can be rated as High, Low, Medium, Mission Critical, or No Value. Once a target entry has been created, the rating cannot be changed. If you need to change the rating, you must delete the target entry and recreate it using the rating that you want.

Target IP Address Column

The target IP address can be a single IP address or a range of IP addresses. The following example shows two entries. One is a single IP address entry and the other is an address range.

Target Value Rating	Target IP Address
High	192.168.33.2
Medium	10.10.3.1-10.10.3.55

Apply Changes

When you have entered the information that you want in the Target Value Rating window, click **Apply Changes**. The **Apply Changes** button is disabled when there are no changes to send to the router.

Discard Changes

To clear information that you have entered in the Target Value Rating window but have not sent to the router, click **Discard Changes**. The Discard Changes button is disabled when there are no changes made that are awaiting delivery to the router.

Add Target Value Rating

To add a TVR entry, choose the target value rating and enter a Target IP Address or range of IP addresses.

Target Value Rating (TVR)

Targets can be rated as High, Low, Medium, Mission Critical, or No Value. Once a rating has been used for one target entry, it cannot be used for additional entries. Therefore, enter into the same entry all the targets that you want to give the same rating.

Target IP Addresses

You can enter a single target IP address or a range of addresses, as shown in the examples that follow:

```
192.168.22.33
10.10.11.4-10.10.11.55
```

The IP addresses that you enter are displayed in the Target Value Rating window.

Edit IPS: SEAP Configuration: Event Action Overrides

Event action overrides allow you to change the actions associated with an event based on the Risk Rating RR of that event. You do this by assigning an RR range for each event action. If an event occurs and its RR falls within the range that you defined, the action is added to the event. Event action overrides are a way to add event actions globally without having to configure each signature individually.

Use Event Action Overrides

Check the Use Event Action Overrides box to enable Cisco IOS IPS to use event action overrides. You can add and edit event action overrides whether or not they are enabled on the router.

Select All

The Select All button works with the Enable, Disable and Delete buttons. If you want to enable or disable all event action overrides, click **Select All** and then click **Enable** or **Disable**. To remove all event action overrides, click **Select All**, and then click **Delete**.

Add and Edit Buttons

Click **Add** to display a dialog in which you can enter the information for an event action override. Choose an event action override, and click **Edit** to change the information for an event action override.

Delete

Click **Delete** to remove the event action overrides that you selected, or to remove all event action overrides if you clicked **Select All**.

Enable and Disable

The Enable and Disable buttons allow you to enable or disable event action overrides. Choose one event action override, or click **Select All** to enable or disable all event action overrides.

Apply Changes

When you have entered the information that you want in the Event Action Overrides window, click **Apply Changes**. The **Apply Changes** button is disabled when there are no changes to send to the router.

Discard Changes

If you want to clear information that you have entered in the Event Action Overrides window but have not sent to the router, click **Discard Changes**. The **Discard Changes** button is disabled when there are no changes made that are awaiting delivery to the router.

Add or Edit an Event Action Override

To add an event action override, choose the event action, enable or disable it, and specify the RR range. If you are editing, you cannot change the event action.

Event Action

Choose one of the following event actions:

- Deny Attacker Inline—Does not transmit this packet and future packets from the attacker address for a specified period of time (inline only).
- Deny Connection Inline—Does not transmit this packet and future packets on the TCP Flow (inline only)
- Deny Packet Inline—Does not transmit this packet.
- Produce Alert—Writes an <evIdsAlert> to the log.
- Reset TCP Connection—Sends TCP resets to hijack and terminate the TCP flow.

Enabled

Click **Yes** to enable the event action override, or **No** to disable it. You can also enable and disable event action overrides in the Event Action Override window.

Risk Rating

Enter the lower bound of the RR range in the Min box, and the upper bound of the range in the Max box. When the RR value of an event falls within the range that you specify, Cisco IOS IPS adds the override specified by the Event Action. For example, if Deny Connection Inline is assigned a RR range of 90-100, and an event with an RR of 95 occurs, Cisco IOS IPS responds by denying the connection inline.

Edit IPS: SEAP Configuration: Event Action Filters

Event action filters let Cisco IOS IPS perform individual actions in response to an event without requiring it to perform all actions or remove the entire event. Filters work by removing actions from an event. A filter that removes all actions from an event effectively consumes the event. Event action filters are processed as an ordered list. You can move filters up or down in the list to have the router process one filter before it processes other filters.

The Event Action Filters window displays the configured event action filters, and allows you to reorder the filters list so that Cisco IOS IPS processes the filters in the order that you want.

Use Event Action Filters

Check **Use Event Action Filters** to enable the use of event action filters. You can add, edit, and remove event action filters, and rearrange the list to specify the order that the router processes the filters whether or not event action filtering is enabled.

Event Action Filter List Area

For a description of the columns in the Event Action Filter List area, see Add or Edit an Event Action Filter.

Event Action Filter List Buttons

The Event Action Filter List buttons allow you to create, edit, and remove event action filters, and to place each event action filter in the order you want it to be in the list. The buttons are described in the following sections.

Select All

The **Select All** button works with the **Enable**, **Disable**, and **Delete** buttons. To enable or disable all event action filters, click **Select All**, and then click **Enable** or **Disable**. To remove all event action filters, click **Select All**, and then click **Delete**.

Add

Click the **Add** button to add an event action filter to the end of the list. A dialog is displayed that enables you to enter the data for the filter.

Insert Before

To insert a new event action filter before an existing one, select the existing filter entry and click **Insert Before**. A dialog is displayed that enables you to enter the data for the filter.

Insert After

To insert a new event action filter after an existing one, select the existing filter entry and click **Insert Before**. A dialog is displayed that enables you to enter the data for the filter.

Move Up

Choose an event action filter and click the **Move Up** button to move the filter up in the list.

Move Down

Choose an event action filter and click the **Move Down** button to move the filter down in the list.

Edit

Click the **Edit** button to edit an event action filter you have chosen.

Enable

Click the **Enable** button to enable an event action filter you have chosen. To enable all event action filters, click **Select All** first, and then click **Enable**.

Disable

Click the **Disable** button to disable an event action filter you have chosen. To disable all event action filters, click **Select All** first, and then click **Disable**.

Delete

Click the **Delete** button to delete an event action filter you have chosen. If you want to delete all event action filters, click **Select All** first, and then click **Delete**.

Apply Changes

When you have entered the information that you want in this window, click **Apply Changes**. The Apply Changes button is disabled when there are no changes to send to the router.

Discard Changes

If you want to clear information that you have entered in this window but have not sent to the router, click **Discard Changes**. The Discard Changes button is disabled when there are no changes awaiting delivery to the router.

Add or Edit an Event Action Filter

The following information describes the fields in the Add and the Edit Event Action Filter dialogs.

Name

SDM provides event action filter names beginning with Q00000, incrementing the numerical portion of the name by 1 each time you add an event action filter. You can also enter a name that you choose. If you are editing an event action filter, the Name field is read-only.

Enabled

Click **Yes** to enable the event action filter, or click **No** to disable it. You can also enable and disable event action filters in the Event Action Filter window.

Signature ID

For Signature ID, enter a range of signature IDs from 900 to 65535, or enter a single ID in that range. If you enter a range, use a dash (-) to separate the upper and lower bounds of the range. For example, enter 988-5000.

Subsignature ID

For Subsignature ID, enter a range of subsignature IDs from 0 to 255, or enter a single subsignature ID in that range. If you enter a range, use a dash (-) to separate the upper and lower bounds of the range. For example, enter 70-200

Attacker Address

For Attacker Address, enter a range of addresses from 0.0.0.0 to 255.255.255.255, or enter a single address in that range. If you enter a range, use a dash (-) to separate the upper and lower bounds of the range. For example, enter 192.168.7.0-192.168.50.0.

Attacker Port

For Attacker Port, enter a range of port numbers from 0 to 65535, or enter a single port number in that range. If you enter a range, use a dash (-) to separate the upper and lower bounds of the range. For example, enter 988-5000.

Victim Address

For Victim Address, enter a range of addresses from 0.0.0.0 to 255.255.255.255, or enter a single address in that range. If you enter a range, use a dash (-) to separate the upper and lower bounds of the range. For example, enter 192.168.7.0-192.168.50.0.

Victim Port

For Victim Port, enter a range of port numbers from 0 to 65535, or enter a single port number in that range. If you enter a range, use a dash (-) to separate the upper and lower bounds of the range. For example, enter 988-5000.

Risk Rating

For Risk Rating, enter an RR range between 0 and 100.

Actions to Subtract

Click any actions that you want to subtract from matching events. To subtract more than one action from matching events, hold down the **Ctrl** key when you choose additional events. All the events that you choose for this filter will be listed in the Event Action Filters window.

Stop on Match

If you want the Cisco IOS IPS to stop when an event matches this event action filter, click **Yes**. If you want the Cisco IOS IPS to evaluate matching events against the other remaining filters, click **No**.

Comments

You can add comments to describe the purpose of this filter. This field is optional.

Edit IPS: Signatures

Cisco IOS IPS prevents intrusion by comparing traffic against the signatures of known attacks. Cisco IOS images that support Cisco IOS IPS have built-in signatures that can be used, and you can also have Cisco IOS IPS import signatures for the router to use when examining traffic. Imported signatures are stored in a signature definition file (SDF).

This window lets you view the configured Cisco IOS IPS signatures on the router. You can add customized signatures, or import signatures from SDFs downloaded from Cisco.com. You can also edit, delete, enable, and disable signatures.

Cisco IOS IPS is shipped with an SDF that contains signatures that your router can accommodate. To learn more about the SDF shipped with Cisco IOS IPS, and how to have Cisco IOS IPS use it, click IPS-Supplied Signature Definition Files.

Signature Tree

The signature tree enables you to filter the signature list on the right according to the type of signature that you want to view. First choose the branch for the general type of signature that you want to display. The signature list displays the configured signatures for the type that you chose. If a plus (+) sign appears to the left of the branch, there are subcategories that you can use to refine the filter. Click the + sign to expand the branch and then choose the signature subcategory that you want to display. If the signature list is empty, there are no configured signatures available for that type.

For example: If you want to display all attack signatures, click the **Attack** branch folder. If you want to see the subcategories that you can use to filter the display of attack signatures, click the + sign next to the Attack folder. If you want to see Denial of Service (DoS) signatures, click the **DoS** folder.

Import Button

Click to import a signature definition file from the PC or from the router. When you have specified the file, Cisco IOS IPS displays the signatures available in the file, and you can choose the ones that you want to import to the router. For more information about how to choose the signatures to import, see Import Signatures.

Note You can only import signatures from the router if the router has a DOS-based file system.

SDFs are available from Cisco. Click the following URL to download an SDF from Cisco.com (requires login):

http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup

Cisco maintains an alert center that provides information on emerging threats. See Cisco Security Center for more information.

View By and Criteria List

The View By and Criteria drop-down lists enable you to filter the display according to the types of signatures that you want to view. First choose the criteria in the View By drop-down list, then choose the value for that criteria in the Criteria drop-down list.

For example: If you choose **Engine** in View By, Criteria changes to Engine, and you can choose among the available engines, such as **Atomic.ICMP** and **Service.DNS**.

If you choose **Sig ID**, or **Sig Name**, you must enter a value in the criteria field.

Total [*n*] New [*n*] Deleted [*n*]

This text gives you the count of new signatures and deleted signatures.

Select All

Click to choose all signatures in the list.

Add

Click **Add** if you want to do any of the following:

- **Add New**—Choose this option to add a new signature, and provide signature parameters in the displayed dialog.
- **Clone**—The clone option is enabled if a signature is specified that does not belong to a hardcoded engine. It is disabled if the signature uses one of the the Cisco IOS hardcoded engines.

Edit

Click to edit the parameters of the specified signature.

Delete

Click **Delete** to mark the specified signature for deletion from the list. To view signatures you have deleted, click **Details**. For more information on the status and handling of these signatures, see Signatures marked for deletion.

Note You can display and monitor TrendMicro OPACL signatures, but you cannot edit, delete, enable, or disable them. If a TrendMicro OPACL signature is specified, the **Edit**, **Delete**, **Enable** and **Disable** buttons are disabled. The Cisco Incident Control Server assumes control of these signatures.

Enable

Click **Enable** to enable the specified signature. An enabled signature is designated with a green checkmark. A signature that was disabled and then enabled has a yellow Wait icon in the ! column indicating that the change must be applied to the router.

Disable

Click **Disable** to disable the specified signature. A signature that is disabled is designated with a red icon. If the signature is disabled during the current session, a yellow Wait icon appears in the ! column indicating that the change must be applied to the router.

Summary or Details Button

Click to display or hide the signatures marked for deletion.

Signature List

Displays the signatures retrieved from the router, and any signatures added from an SDF.

Note Signatures that are set to import and are identical to deployed signatures will not be imported and will not appear in the signature list.

The signature list can be filtered using the selection controls.

Enabled	Enabled signatures are indicated with a green icon. If enabled, the actions specified when the signature is detected is carried out. Disabled signatures are indicated with a red icon. If disabled, the actions are disabled and are not be carried out.
Alert (!)	This column may contain the yellow Wait icon.  This icon indicates new signatures that have not been delivered to the router or modified signatures that have not been delivered to the router.
Sig ID	Numerical signature ID. For example: the sigID for ICMP Echo Reply is 2000.
SubSig ID	Subsignature ID.
Name	Name of the signature. For example: ICMP Echo Reply.
Action	Action to take when the signature is detected.
Filter	ACL associated with the corresponding signature.
Severity	Severity level of the event. Severity levels are informational, low, medium, and high
Engine	Engine to which the signature belongs.

Right-click Context Menu

If you right-click a signature, Cisco SDM displays a context menu with the following options:

- Actions—Click to choose the actions to be taken when the signature is matched. See Assign Actions for more information.
- Set Severity to—Click to set the severity level of a signature to: high, medium, low, or informational.
- Restore Defaults—Click to restore the signature's default values.
- Remove Filter—Click to remove a filter applied to the signature.
- NSDB help (need CCO account)—Click to display help on the Network Security Data Base (NSDB).

Signatures marked for deletion

This area is visible when the **Details** button is clicked. It lists the signatures that you deleted from the Signature List, and signatures that are marked for deletion because imported signatures are set to replace signatures already configured on the router. See How to Import Signatures for more information.

Signatures marked for deletion remain active in the Cisco IOS IPS configuration until you click **Apply Changes**. If you exit the Signatures window and disable Cisco IOS IPS, the marked signatures will be deleted if Cisco IOS IPS is re-enabled.

Undelete All Button

Click to restore all signatures in the signatures marked deleted list.

Undelete Button

Click to restore specified signatures marked for deletion. When clicked the signatures are unmarked, and returned to the list of active signatures.

Apply Changes Button

Click to deliver newly imported signatures, signature edits, and newly enabled or disabled signatures to the router. When the changes are applied, the yellow Wait icon is removed from the ! column. These changes are saved to your router flash memory in the file sdmips.sdf. This file is created automatically the first time you click **Apply Changes**.

Note If you are attempting to import signatures, and these signatures are all identical to deployed signatures, then the **Apply Changes** button is disabled.

Discard Changes Button

Click to discard accumulated changes.

Note If you are attempting to import signatures, and these signatures are all identical to deployed signatures, then the **Discard Changes** button is disabled.

Victim Port

For Victim Port, enter a range of port numbers from 0 to 65535, or enter a single port number in that range. If you enter a range, use a dash (-) to separate the upper and lower bounds of the range. For example, enter 988-5000.

Risk Rating

For Risk Rating, nter an RR range between 0 and 100.

Actions to Subtract

Click any actions that you want to subtract from matching events. To subtract more than one action from matching events, hold down the **Ctrl** key when you choose additional events. All the events that you choose for this filter will be listed in the Event Action Filters window.

Stop on Match

If you want the Cisco IOS IPS to stop when an event matches this event action filter, click **Yes**. If you want the Cisco IOS IPS to evaluate matching events against the other remaining filters, click **No**.

Comments

You can add comments to describe the purpose of this filter. This field is optional.

Edit IPS: Signatures

Cisco IOS IPS prevents intrusion by comparing traffic against the signatures of known attacks. Cisco IOS images that support Cisco IOS IPS have built-in signatures that Cisco IOS IPS can use, and you can also have Cisco IOS IPS import signatures for the router to use when examining traffic. Imported signatures are stored in a signature definition file (SDF).

This help topic describes the Signatures window displayed when the router runs Cisco IOS 12.4(11)T and later releases.

The Signatures window lets you view the configured Cisco IOS IPS signatures on the router. You can add customized signatures, or import signatures from SDFs downloaded from Cisco.com. You can also edit, enable, disable, retire, and unretire signatures.

Signature Tree

The signature tree enables you to filter the signature list on the right according to the type of signature that you want to view. First choose the branch for the general type of signature that you want to display. The signature list displays the configured signatures for the type that you chose. If a plus (+) sign appears to the left of the branch, there are subcategories that you can use to refine the filter. Click the + sign to expand the branch and then choose the signature subcategory that you want to display. If the signature list is empty, there are no configured signatures available for that type.

For example: If you want to display all attack signatures, click the **Attack** branch folder. If you want to see the subcategories that you can use to filter the display of attack signatures, click the + sign next to the Attack folder. If you want to see Denial of Service (DoS) signatures, click the **DoS** folder.

Import Button

Click to import a signature definition file from the PC or from the router. When you have specified the file, Cisco IOS IPS displays the signatures available in the file, and you can choose the ones that you want to import to the router. For more information about how to choose the signatures to import, see Import Signatures.

Note You can only import signatures from the router if the router has a DOS-based file system.

SDFs are available from Cisco. Click the following URL to download an SDF from Cisco.com (requires login):

http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup

Cisco maintains an alert center that provides information on emerging threats. See Cisco Security Center for more information.

View By and Criteria List

The View By and Criteria drop-down lists enable you to filter the display according to the types of signatures that you want to view. First choose the criteria in the View By drop-down list, then choose the value for that criteria in the Criteria drop-down list.

For example: If you choose **Engine** in View By, Criteria changes to Engine, and you can choose among the available engines, such as **Atomic.ICMP** and **Service.DNS**.

If you choose **Sig ID**, or **Sig Name**, you must enter a value in the criteria field.

Total [*n*]

This text gives you the total number of signatures on the router.

Select All

Click to choose all signatures in the list.

View By and Criteria List

The View By and Criteria drop-down lists enable you to filter the display according to the types of signatures that you want to view. First choose the criteria in the View By drop-down list, then choose the value for that criteria in the Criteria drop-down list.

For example: If you choose **Engine** in View By, Criteria changes to Engine, and you can choose among the available engines, such as **Atomic.ICMP** and **Service.DNS**.

If you choose **Sig ID**, or **Sig Name**, you must enter a value in the criteria field.

Total [*n*]

This text gives you the total number of signatures on the router.

Select All

Click to choose all signatures in the list.

Disable

Click **Disable** to disable the specified signature. A signature that is disabled is designated with a red icon. If the signature is disabled during the current session, a yellow Wait icon appears in the ! column indicating that the change must be applied to the router.

Retire

Click **Retire** to prevent a signature from being compiled for scanning.

Unretire

Click **Unretire** to allow the signature to be compiled for scanning.

Signature List

Displays the signatures retrieved from the router, and any signatures added from an SDF.

Note Signatures that are set to import and are identical to deployed signatures will not be imported and will not appear in the signature list.

The signature list can be filtered using the selection controls.

Enabled	Enabled signatures are indicated with a green icon. If enabled, the actions specified when the signature is detected is carried out. Disabled signatures are indicated with a red icon. If disabled, the actions are disabled and are not be carried out.
Alert (!)	This column may contain the yellow Wait icon.  This icon indicates new signatures that have not been delivered to the router or modified signatures that have not been delivered to the router.
Sig ID	Numerical signature ID. For example: the sigID for ICMP Echo Reply is 2000.
SubSig ID	Subsignature ID.
Name	Name of the signature. For example: ICMP Echo Reply.
Action	Action to take when the signature is detected.
Severity	Severity level of the event. Severity levels are informational, low, medium, and high
Fidelity Rating	The fidelity rating of the signature.
Retired	A value of true or false. True if signature has been retired. False if not. Retired signatures are not compiled.
Engine	Engine to which the signature belongs.

Right-click Context Menu

If you right-click a signature, Cisco SDM displays a context menu with the following options:

- Actions—Click to choose the actions to be taken when the signature is matched. See Assign Actions for more information.
- Fidelity Rating—Click to enter a fidelity rating for the signature.
- Set Severity to—Click to set the severity level of a signature to: high, medium, low, or informational.
- Restore Defaults—Click to restore the signature's default values.

- NSDB help (need CCO account)—Click to display help on the Network Security Data Base (NSDB).

Apply Changes

Click **Apply Changes** to deliver newly imported signatures, signature edits, and newly enabled or disabled signatures to the router. When the changes are applied, the yellow Wait icon is removed from the ! column. These changes are saved to your router flash memory in the file sdmips.sdf. This file is created automatically the first time you click **Apply Changes**.

Note If you are attempting to import signatures, and these signatures are all identical to deployed signatures, then the **Apply Changes** button is disabled.

Discard Changes

Click **Discard Changes** to discard accumulated changes.

Note If you are attempting to import signatures, and these signatures are all identical to deployed signatures, then the **Discard Changes** button is disabled.

Edit Signature

Use the fields in Edit Signature dialog to edit the selected signature. The changes that you make are stored in a delta file that is saved to router flash memory. The elements of signatures are described in the following sections.

This help topic describes the Edit Signatures window displayed when the router runs Cisco IOS 12.4(11)T and later releases.

Signature ID

The unique numerical value assigned to this signature. This value allows the Cisco IOS IPS to identify a particular signature.

Subsignature ID

The unique numerical value assigned to this subsignature. A subsignature ID is used to identify a more granular version of a broad signature.

Alert Severity

Choose one of the following to categorize the severity of the alert: High, Medium, Low, or Informational.

Sig Fidelity Rating

The signature fidelity rating is a value set by the author of the signature to quantify the confidence that the signature will produce true positives. This value is set before a signature is deployed and can be adjusted when signature performance data is available.

Promiscuous Delta

The promiscuous delta is a factor that is subtracted from the risk rating (RR) of an event when the router is operating in promiscuous mode. The Promiscuous Delta is subtracted from the RR every time an alert is triggered when the system is deployed in promiscuous mode.

Note Even though the promiscuous delta can be reconfigured on a signature basis, it is not recommended that you change any of the predefined promiscuous-delta settings.

Sig Description

The signature description includes the signature name and release, any alert notes available from the Cisco Security Center, user comments, and other information.

Engine

The signature engine associated with this signature. One commonly-used engine is named Atomic IP.

The Engine box contains fields that allow you to tune a wide variety of signature parameters. For example, you can specify the action to be taken if this signature is matched and an event is generated, you can specify the layer 4 protocol to inspect for events matching this signature, and you can specify IP parameters, such as header length and type of service.

Event Counter

The controls in the Event Counter box allow you to specify the parameters described in the following sections.

Event Count

The number of times an event must occur before an alert is generated.

Event Count Key

The type of information to use to count an event as occurring. For example, if you choose **both attacker and victim addresses and ports**, each time you have these 4 pieces of information for an event, the count increments by 1. If you choose **attacker address**, only that piece of information is needed.

Event Interval

The number of seconds between events being sent to the log. If you select **Yes**, an additional field is displayed allowing you to enter the number of seconds.

Alert Frequency

The purpose of the alert frequency parameter is to reduce the volume of the alerts written to the log,

Summary Mode

There are four modes: Fire All, Fire Once, Summarize, and Global Summarize. The summary mode is changed dynamically to adapt to the current alert volume. For example, you can configure the signature to Fire All, but after a certain threshold is reached, it starts summarizing.

Summary Key

The type of information to use to determine when to summarize. For example, if you choose **both attacker and victim addresses and ports**, each time you have these 4 pieces of information for an event, summarization occursY. If you choose **attacker address**, only that piece of information is needed.

Specify Global Summary Threshold

You can optionally specify numerical thresholds to use for determining when to summarize events to the log. If you choose **Yes**, you can specify a global summary threshold, and a summary interval.

Status

You can specify whether the signature should be enabled, disabled, or retired in the Status box. Additionally, the Status box can display the signatures that you have obsoleted.

File Selection

This window allows you to load a file from your router. Only DOSFS file systems can be viewed in this window.

The left side of window displays an expandible tree representing the directory system on your Cisco router flash memory and on USB devices connected to that router.

The right side of the window displays a list of the names of the files and directories found in the directory that is specified in the left side of the window. It also shows the size of each file in bytes, and the date and time each file and directory was last modified.

You can choose a file to load in the list on the right side of the window. Below the list of files is a Filename field containing the full path of the specified file.

Note If you are choosing a configuration file to provision your router, the file must be a CCCD file or have a .cfg extension.

Name

Click **Name** to order the files and directories alphabetically based on name. Clicking **Name** again will reverse the order.

Size

Click **Size** to order the files and directories by size. Directories always have a size of zero bytes, even if they are not empty. Clicking **Size** again will reverse the order.

Time Modified

Click **Time Modified** to order the files and directories based on modification date and time. Clicking **Time Modified** again will reverse the order.

Assign Actions

This window contains the actions that can be taken upon a signature match. Available actions depend on the signature, but the most common actions are listed below:

- **alarm**—Generate an alarm message. Same as **produce-verbose-alert**.
- **deny-attacker-inline**—Create an ACL that denies all traffic from the IP address considered to be the source of the attack by the Cisco IOS IPS system. Same as **denyAttackerInline**.
- **deny-connection-inline**—Drop the packet and all future packets on this TCP flow. Same as **produce-alert** and **denyFlowInline**.
- **deny-packet-inline**—Do not transmit this packet (inline only). Same as **drop**.
- **denyAttackerInline**—Create an ACL that denies all traffic from the IP address considered to be the source of the attack by the Cisco IOS IPS system. Same as **deny-attacker-inline**.
- **denyFlowInline**—Create an ACL that denies all traffic from the IP address that is considered the source of the attack belonging to the 5-tuple (src ip, src port, dst ip, dst port and l4 protocol). denyFlowInline is more granular than denyAttackerInline. Same as **produce-alert** and **deny-connection-inline**.
- **drop**—Drop the offending packet. Same as **deny-packet-inline**.

- **produce-alert**—Generate an alert. Same as **denyFlowInline** and **deny-connection-inline**.
- **produce-verbose-alert**—Generate an alert which includes an encoded dump of the offending packet. Same as **alarm**.
- **reset**—Reset the connection and drop the offending packet. Same as **reset-tcp-connection**.
- **reset-tcp-connection**—Send TCP RESETS to terminate the TCP flow. Same as **reset**.

Import Signatures

Use the Import IPS window to import signatures from an SDF or other file on your PC. The information in this window tells you which signatures are available from the SDF, and which of them are already deployed on your router.

How to Import Signatures

To import signatures, follow these steps:

Step 1 Use the signature tree, View By drop-down list, and Criteria List drop-down list to display the signatures you want to import.

In the signature list, uncheck the **Import** checkbox for the signatures that you *do not* want to import. If you want to uncheck the **Import** checkbox for all of the signatures, click the **Unselect All** button, which changes to the **Select All** button

Step 2 Check the checkbox **Do not import signatures that are defined as disabled** if you want to avoid importing signatures that may degrade router performance when used.

Step 3 Click the **Merge** button to merge the imported signatures with the signatures that are already configured on the router, or the **Replace** button to replace the already configured signatures.

See Merge Button and Replace Button for more information.

Step 4 Click the **Apply Changes** button in the Edit IPS window to deploy the imported signatures.

You can make changes to the imported signatures before deploying them. Signatures that set to import and are identical to deployed signatures will not be imported. If all imported signatures are identical to deployed signatures, then the **Apply Changes** button is disabled.

Signature Tree

If you need a description of the signature tree, click this link: Signature Tree. You can use the signature tree in this window to assemble the signatures that you want to import, category by category.

For example: you may want to add signatures from the OS category, and from the Service category. You can do this by choosing the **OS** branch of the tree, and any branch from that part of the tree that you want, such as the UNIX branch or the Windows branch. When the types of signatures that you want to import are displayed, you can make your selections in the signature list area. Then you can choose the **Service** branch, and choose any of the service signatures that you want.

View By and Criteria List

The View By and Criteria list boxes enable you to filter the display according to the types of signatures that you want to view. First choose the criteria in the View By list, then choose the value for that criteria in the list to the right (the criteria list).

For example: If you choose **Engine** in the View By list, the criteria list is labeled Engine, and you can choose among the available engines, such as **Atomic.ICMP**, and **Service.DNS**.

If you choose **Sig ID**, or **Sig Name**, you must enter a value in the criteria list.

Signature List Area

The signature list displays the signatures available in the SDF based on the criteria you chose in the signature tree. The text of signatures already found on the target router is blue.

The signature list area has these columns:

- Sig ID—Unique numerical value assigned to this signature. This value allows Cisco IOS IPS to identify a particular signature.

- Name—Name of the signature. For example: *FTP Improper Address*.
- Severity—High, medium, low, or informational.
- Deployed—Displays *Yes* if the signature is already deployed on the router. Displays *No* if the signature is not deployed on the router.
- Import—Contains a checkbox for each signature. If you want to import the signature, check this box.

Note All of the signatures imported from an SDF or a zip file with the name IOS-S*xxx*.zip can be displayed in the signature list. When signatures are imported from a zip file with a different name, only the signatures found through the View By and Criteria List drop-down lists are displayed.

Merge Button

Click to merge the signatures that you are importing with the signatures that are already configured on the router.

Replace Button

Click to replace the signatures that are already configured on the router with the signatures that you are importing. Signatures already configured on the router but that are *not* found in the list of signatures being imported are marked for deletion and listed under **Signatures Marked for Deletion** in **Edit IPS > Signatures**. See Signatures marked for deletion for more information.

Add, Edit, or Clone Signature

This window contains fields and values described in the Field Definitions section. The fields vary depending on the signature, so this is not an exhaustive list of all the fields you might see.

Field Definitions

The following fields are in the Add, Edit, and Clone Signature windows.

- **SIGID**—Unique numerical value assigned to this signature. This value allows Cisco IOS IPS to identify a particular signature.

- **SigName**—Name assigned to the signature.
- **SubSig**—Unique numerical value assigned to this subsignature. A subsig ID is used to identify a more granular version of a broad signature.
- **AlarmInterval**—Special Handling for timed events. Use AlarmInterval Y with MinHits X for X alarms in Y second interval.
- **AlarmSeverity**—Severity of the alarm for this signature.
- **AlarmThrottle**—Technique used for triggering alarms.
- **AlarmTraits**—User-defined traits further describing this signature.
- **ChokeThreshold**—Threshold value of alarms-per-interval that triggers autoswitch AlarmThrottle modes. If ChokeThreshold is defined, Cisco IOS IPS automatically switches AlarmThrottle modes if a large volume of alarms is seen in the ThrottleInterval.
- **Enabled**—Identifies whether or not the signature is enabled. A signature must be enabled in order for Cisco IOS IPS to protect against the traffic specified by the signature.
- **EventAction**—Actions Cisco IOS IPS will take if this signature is triggered.
- **FlipAddr**—True if the source and destination addresses, and their associated ports, are swapped in the alarm message. False if no swap occurs (default).
- **MinHits**—Specifies the minimum number of signature hits that must occur before the alarm message is sent. A hit is the appearance of the signature on the address key.
- **SigComment**—Comment or description text for the signature.
- **SigVersion**—Signature version.
- **ThrottleInterval**—Number of seconds defining an Alarm Throttle interval. This is used with the AlarmThrottle parameter to tune special alarm limiters.
- **WantFrag**—True enables inspection of fragmented packets only. False enables inspection of non-fragmented packets only. Choose “undefined” to allow for inspection of both fragmented and non-fragmented packets.

Cisco Security Center

The Cisco Security Center provides information on emerging threats, and links to the Cisco IOS IPS signatures available to protect your network from them. Signature reports and downloads are available at this link (requires login):

http://tools.cisco.com/MySDN/Intelligence/searchSignatures.x

IPS-Supplied Signature Definition Files

To ensure that the router has as many signatures available as its memory can accommodate, Cisco SDM is shipped with one of the following SDFs:

- 256MB.sdf—If the amount of RAM available is greater than 256 MB. The 256MB.sdf file contains 500 signatures.
- 128MB.sdf—If the amount of RAM available is between 128 MB and 256 MB. The 128MB.sdf file contains 300 signatures.
- attack-drop.sdf—If the amount of available RAM is 127 MB or less. The attack-drop.sdf file contains 82 signatures.

If your router runs Cisco IOS version 12.4(11)T or later, you must use an SDF file that has a name of the format sigv5-SDM-S*xxx*.zip; for example, sigv5-SDM-S260.zip.

Note The router must be running Cisco IOS Release 12.3(14)T or later releases to be able to use all the available signature engines in 256MB.sdf and 128MB.sdf files. If the router uses an earlier release, not all signature engines will be available.

To use an SDF in router memory, determine which SDF has been installed and then configure Cisco IOS IPS to use it. The procedures that follow show you how to do this.

Determine Which SDF File Is in Memory

To determine which SDF file is in router memory, open a Telnet session to the router, and enter the **show flash** command. The output will be similar to the following:

```
System flash directory:
```

```
File  Length   Name/status
  1   10895320  c1710-k9o3sy-mz.123-8.T.bin
  2   1187840  ips.tar
  3   252103   attack-drop.sdf
  4   1038     home.shtml
  5   1814     sdmconfig-1710.cfg
  6   113152   home.tar
  7   758272   es.tar
  8   818176   common.tar
[14028232 bytes used, 2486836 available, 16515068 total]
16384K bytes of processor board System flash (Read/Write)
```

In this example, the attack-drop.sdf file is in router memory. On some routers, such as routers with a disk file system, use the **dir** command to display the contents of router memory.

Configuring IPS to Use an SDF

To haveCisco IOS IPS use the SDF in router memory, do the following:

Step 1 Click **Global Settings**.

Step 2 In the Configured SDF Locations list, click **Add**.

Step 3 In the dialog box displayed, click **Specify SDF on flash**, and enter the name of the SDF file.

Step 4 Click **OK** to close the dialog box.

Security Dashboard

The Security Dashboard allows you to keep your router updated with signatures for the latest security threats. You must have Cisco IOS IPS configured on your router before you can deploy signatures using the Security Dashboard.

Top Threats Table

The Top Threats table displays the latest top threats from Cisco if the status of the associated signatures indicates that they are available for deployment or are under investigation. Some of the top threats in the table are associated with signatures that can be deployed to your router. The text of signatures already found on your router is blue.

To obtain the latest top threats, click the **Update top threats list** button.

Note You cannot update the top threats by using the Cisco SDM **Refresh** button or your browser's Refresh command.

The top threats table has the following columns:

- **Device Status** indicates if the signature associated with the threat is already enabled on your router. The following symbol may appear in the Device Status column:

Signature is already enabled on your router.

Signature is not available on your router or is available but *not* enabled on your router.

- **Sig ID** is a unique number identifying the signature associated with the threat.
- **SubSig ID** is a unique number identifying the subsignature. If the signature associated with the threat does not have a subsignature, **SubSig ID** is 0.
- **Name** is the name given to the threat.
- **Urgency** indicates if the level of the threat is high (Priority Maintenance) or normal (Standard Maintenance).
- **Threat Status** indicates if the signature associated with the threat is available or if the threat is still under investigation.
- **Deploy** contains checkboxes that can be checked if the signature associated with the threat is available to deploy.

Select SDF

Click the **Browse** button and choose the Cisco IOS SDF file to use. The Cisco IOS SDF file must be present on your PC. The format that the filename has depends on the version of Cisco IOS the router is running.

- If the router is running a Cisco IOS image earlier than 12.4(11)T, the SDF must have a name with the format IOS-S*xxx*.zip, where *xxx* is a three-digit number. For example: a Cisco IOS IPS SDF file may be named IOS-S193.zip.
- If the router is running a Cisco IOS image of version 12.4(11)T or later, the SDF must have a name with the format sigv5-SDM-S*xxx*.zip; for example, sigv5-SDM-S260.zip

The location of a Cisco IOS SDF file you choose is shown in the SDF file location field. The SDF file location field is read-only.

After the first time you download a Cisco IOS SDF file, Cisco SDM remembers the location of the file. The next time you load the Security Dashboard, Cisco SDM will select the latest Cisco IOS SDF file based on the three-digit number in the file's name.

Note The Cisco IOS SDF file with the highest three-digit number in its name is the latest Cisco IOS SDF file.

Deploying Signatures From the Top Threats Table

Before attempting to deploy signatures from the Top Threats table, ensure that you have:

- Configured Cisco IOS IPS on your router
- Downloaded the latest Cisco IOS file to your PC

To deploy signatures from the Top Threats table, follow these steps:

Step 1 Click the **Update top threats list** button to ensure that you have the latest top threats list.

Step 2 In the Deploy column, check the checkbox for each top-threat signature you want to deploy from the Top Threats table.

Only top threats with the status **Signature available** can be chosen. Available signatures with a red icon in their Applied column are automatically set to deploy.

Step 3 Click the **Browse** button and choose the latest Cisco IOS file if you need to ensure that you are using the latest signature file.

You may need to do this if the location of the latest SDF file has changed since it was last set in the Security Dashboard, or if the format of its name is not IOS-S*xxx*.zip, where *xxx* is a three-digit number

Step 4 Click the **Deploy signatures** button to deploy the chosen signatures to your router.

A warning is shown if any of the chosen signatures are not found in the Cisco IOS file. However, all found signatures can still be deployed. After being deployed on your router, the signatures are automatically enabled and added to the router active signatures list.

IPS Migration

If you have an existing the Cisco IOS IPS configuration that you want to migrate to Cisco IOS IPS available in Cisco IOS 12.4(11)T or later releases, you can use the IPS Migration wizard to do the migration.

Note If the router uses a Cisco IOS image of version 12.4(11)T or later, you must migrate a configuration created before this release if you want to use Cisco IOS IPS on your router. If you do not migrate the configuration, the configuration commands will not be changed, but Cisco IOS IPS will not operate.

Click the **Launch IPS Migration Wizard** button to begin the migration process.

Migration Wizard: Welcome

The Migration Wizard Welcome window lists the tasks that the wizard helps you to complete. If you do not want to run the IPS migration wizard, click **Cancel**.

The IPS Migration wizard is available when the router runs Cisco IOS 12.4(11)T and later releases.

Migration Wizard: Choose the IOS IPS Backup Signature File

The backup file contains the Cisco IOS IPS information that will be migrated. This may be a Signature Definition File (SDF), such as attack-drop.sdf, or 128MB.sdf. If you made changes to the signature information, such as disabling signatures or changing the attributes of specific signatures, the records of your changes are kept in a separate file. If you used Cisco SDM to make changes, Cisco SDM saves them in a file named sdmips.sdf, which it saves to router flash memory. If you made changes manually, you may have given the file another name and may have saved a backup copy on your PC.

Click the **...** button next to the backup file field to display a dialog that allows you to browse for this backup file on router flash memory or on your PC.

Signature File

Specify the location of the backup signature file in this dialog.

Specify signature file on flash

If the backup signature file is located on flash memory, click the down arrowhead button next to this field and choose the file.

Specify signature file on the PC

If the backup signature file is located on the PC, click the **Browse** button next to this field and navigate to the file.

Java Heap Size

Cisco SDM displays the Java Heap Size window when the Java heap size is too low to support an SDM feature. Complete the following procedure to set the heap size to the value stated in the window.

Step 1 Exit Cisco SDM.

Step 2 Click **Start > Control Panel > Java**.

Step 3 Open the Java Runtime Settings dialog. The location of this dialog varies by release.

a. Click the **Advanced** tab. Locate the Java Runtime Settings dialog and proceed to Step 4. If the dialog is not available from the Advanced tab, proceed to b.

b. Click the **Java** tab. Locate the Java Runtime Settings dialog. Click the **View** button if necessary to display the dialog, and proceed to Step 4.

Step 4 In the Java Runtime Parameters column, enter the value stated in the window. For example if the window states that you must use the value `-Xmx256m`, enter that value in the Java Runtime Parameters column. The following table shows sample values.

Product Name	Version	Location	Java Runtime Parameters
JRE	1.5.0_08	C:\Program Files\java\jre1.5.0_08	-Xmx256m

Step 5 Click **OK** in the Java Runtime Settings dialog.

Step 6 Click **Apply** in the Java Control Panel, and then click **OK**.

Step 7 Restart Cisco SDM.