# Configuring IOS IPS Routers

Some Cisco IOS routers, such as integrated services routers (ISRs), include native IPS capabilities based on IPS 5.1 software. You can configure some basic IPS inspection on these devices to supplement IPS sensor inspection or to support small networks.

This chapter contains the following topics:



# Understanding Cisco IOS IPS

You can use Cisco Security Manager with the Cisco IOS Intrusion Prevention System (IOS IPS) to manage intrusion prevention on Cisco routers that use supported Cisco IOS Software releases 12.4(11)T2 and later.

The Cisco IOS IPS acts as an in-line intrusion prevention sensor, watching packets and sessions as they flow through the router and scanning each packet to match any of the Cisco IOS IPS signatures. When it detects suspicious activity, it responds before network security can be compromised and logs the event through Cisco IOS syslog messages or Security Device Event Exchange (SDEE).

You can configure Cisco IOS IPS to choose the appropriate response to various threats. The Signature Event Action Processor (SEAP) can dynamically control actions that are to be taken by a signature event on the basis of parameters such as fidelity, severity, or target value rating. You can configure these actions in Security Manager through the Signatures and Event Actions policies.

When packets in a session match a signature, Cisco IOS IPS can take any of the following actions, as appropriate:

- Send an alarm to a syslog server or a centralized management interface.
- Drop the packet.
- Reset the connection.
- Deny traffic from the source IP address of the attacker for a specified amount of time.
- Deny traffic on the connection for which the signature was seen for a specified amount of time.

Cisco developed its Cisco IOS software-based intrusion-prevention capabilities and Cisco IOS Firewall with flexibility in mind, so that individual signatures could be disabled in case of false positives. Generally, it is preferable to enable both the firewall and Cisco IOS IPS to support network security policies. However, each of these features can be enabled independently and on different router interfaces.

For an overall understanding of the Cisco IOS IPS configuration process, see . Overview of Cisco IOS IPS Configuration , on page 4

This section contains the following topics:



# Understanding IPS Subsystems and Support of IOS IPS Revisions

Cisco Security Manager automatically supports minor revisions of IOS IPS. To identify minor revisions that are supported, the IPS subsystem version is needed.

The IPS subsystem version is a version number used to keep track of Cisco IOS IPS feature changes. The subsystem number is show in the device properties (right-click the device and select **Device Properties**). You can also use the command **show subsys name ips** at a command line on the router that is running Cisco IOS IPS to show the detailed Cisco IOS IPS subsystem version. The 3.x subsystems are equivalent to IPS 5.x. For a list of the supported subsystems by Cisco IOS Software release, see the *Supported Devices and Software Versions for Cisco Security Manager* on Cisco.com for this release of Security Manager.

An IPS subsystem version is minor if the version difference is limited at postfix. For example, a revision from 3.0.1 to 3.0.2 is considered minor. For another example, 3.0.1 to 3.1.1 is also considered a minor version change. However, minor revisions that include new features are not automatically supported by Cisco Security Manager.

# Cisco IOS IPS Signature Scanning with Lightweight Signatures

The addition of Cisco IOS IPS signature scanning with lightweight signatures in Cisco IOS Release 15.0(1)M is an enhancement to Cisco IOS IPS that allows loading of larger signatures sets, without consuming significant additional memory or reducing the memory consumed by an existing signature set, by loading equivalent lighter-weight signatures. These signatures are referred to as lightweight signatures.

Security Manager can discover and tune custom signatures with LWEs on ISRs and modular access routers. Security Manager supports the following features for signatures with LWEs on ISRs and modular access routers:

- New signature types
- Signature categories
- New default signature category recognition
- New engine update levels
- Licensing status—bypassed, expired, or not installed

# Router Configuration Files and Signature Event Action Processor (SEAP)

As of Cisco IOS Release 12.4(11)T, signature definition files (SDFs) are no longer used by Cisco IOS IPS. Thus, you cannot not use the deprecated built-in signature sets, 128.sdf, 256.sdf, and attack-drop.sdf, with Security Manager.

Instead, routers access signature definition information through a directory that contains three configuration files—the default configuration, the delta configuration, and the SEAP configuration. You configure the location using the **IPS > General Settings** policy.

SEAP is the control unit responsible for coordinating the data flow of a signature event. It allows for advanced filtering and signature overrides on the basis of the Event Risk Rating (ERR) feedback. ERR is used to control the level in which a user chooses to take actions in an effort to minimize false positives.

Signatures once stored in NVRAM are now stored in the delta configuration file.

# Cisco IOS IPS Limitations and Restrictions

Cisco IOS IPS routers do not support all the features that are supported by dedicated IPS sensor appliances and service modules. In addition, routers that support IOS IPS might not allocate as much memory to IPS functionality as an IPS sensor does. The following limitations and restrictions are important:

- When configuring an IOS IPS device, select only the signatures that you need. If you select all signatures that are available in Security Manager, you might exceed the memory available on the IOS IPS router and deployment can fail, the device might fail to load all of the signatures, or performance might be significantly degraded. If you encounter deployment failures, select a reduced set of signatures and then redeploy the configuration to the device.
- Security Manager-managed routers being configured to use IOS-IPS for the first time cannot use the auto-update process for signature updates. You must first update the router before you use the auto-update process. Follow these steps:
  1. Push an E3 signature, for example, S317.
  2. Push an intermediate signature, for example, S470.
  3. Push the first E4 signature, for example, S485.
  4. Push subsequent E4 signatures until you reach the desired level. Note that each delta should be less than 10 MB in size.

After you have updated the router, you can use the auto-update process to update the signatures. The auto-update process will be successful as each incremental change will not exceed the memory available on the router. For information on configuring automatic updates, see Automating IPS Updates.

- Virtual sensors are not supported by IOS IPS.
- When using event action filters with an IOS IPS router, only a subset of IPS actions are available for removal from an event that meets the criteria of the event action filter. For more information on available event actions, see Filter Item Dialog Box and Understanding IPS Event Actions.
- IOS IPS is based on IPS Software 5.1. Therefore, features introduced in later versions of IPS Software are typically not available in IOS IPS. For example, you cannot configure the following features:
  - Global correlation.

- Anomaly detection.
- OS identification in the event action network identification policy.

# Overview of Cisco IOS IPS Configuration

There are a wide variety of devices on which you can configure the Intrusion Prevention System. From a configuration point-of-view, you can separate the devices into two groups: dedicated appliances and service modules (for routers, switches, and ASA devices) that run the full IPS software; and IPS-enabled routers running Cisco IOS Software 12.4(11)T and later (Cisco IOS IPS).

The following procedure is an overview of IPS configuration on a Cisco IOS IPS router. For dedicated IPS devices, including IPS service modules installed in a router, see Overview of IPS Configuration.

Cisco IOS IPS is a more limited feature meant for branch offices and small to medium sized networks, or to distribute IPS throughout a network. You typically cannot employ as many signatures in a Cisco IOS IPS router compared to a dedicated appliance. You also cannot configure advanced features such as global correlation, because Cisco IOS IPS is based on IPS Software version 5.1. When configuring Cisco IOS IPS devices, you are mostly configuring standard router policies, because the device is a router that is running a few IPS features. In comparison, the platform policies for IPS appliances and service modules are specific to IPS software.

**Tip** Before configuring Cisco IOS IPS, read *Cisco IOS Intrusion Prevention System Deployment Guide* on Cisco.com.

**Step 1** Install and connect the device to your network. Install the device software and perform basic device configuration. Install the licenses required for all of the services running on the device. The amount of initial configuration that you perform influences what you will need to configure in Security Manager. For information about required basic settings, see:

- Setting Up SSL on Cisco IOS Routers
- Setting Up SSH
- Configuring Licenses on Cisco IOS Devices
- Initial Preparation of a Cisco IOS IPS Router, on page 5
- Selecting a Signature Category for Cisco IOS IPS , on page 6

**Step 2** Add the device to the Security Manager device inventory (see Adding Devices to the Device Inventory). When you add the device be sure to make the following selections:

- When adding from Network or Export File, ensure that you select **IPS Policies** for policy discovery.
- When adding from Configuration File or by Manual Definition, ensure that you select **IPS** from the **Options** list, or the device will not be IPS-capable from Security Manager's point of view.

**Step 3** Configure the IPS general settings to specify the location of the IPS files on the router. For more information, see Configuring General Settings for Cisco IOS IPS , on page 7.

**Step 4** Configure the IPS interface rules to enable IPS and to identify the interfaces on which traffic will be subject to IPS inspection. For more information, see Configuring IOS IPS Interface Rules , on page 9.

**Step 5** Configure IPS signatures and event actions. Event action policies are easier to configure than creating custom signatures, so try to use event action filters and overrides to modify signature behavior before trying to edit specific signatures. For more information, see the following topics:

- Configuring Event Action Rules
- Configuring Signatures

**Step 6** Maintain the device:

- Update and redeploy configurations as necessary.
- Apply updated signature and engine packages. For information about checking for updates, applying them, and setting up regular automated updates, see Managing IPS Updates.

# Initial Preparation of a Cisco IOS IPS Router

Before you add a Cisco IOS IPS router to the Security Manager inventory, you need to perform some preparatory steps. The white paper Getting Started with Cisco IOS IPS with 5.x Format Signatures provides a step-by-step explanation of a basic configuration. Although you could do some of the steps after adding the router to Security Manager, such as configuring interface rules, you should do at least the basic steps.

The following procedure explains the steps you are required to complete in the CLI. These steps are required because Security Manager either cannot complete them, or it is simply easier to do it in the CLI (as a one-time configuration). The white paper includes additional steps that you can complete in the CLI, and Security Manager can discover your configuration when you add the device to the inventory. The more you do in CLI, the less you will have to configure in Security Manager.

**Tip** You also must complete the basic router configuration steps as explained in Setting Up SSL on Cisco IOS Routers, Setting Up SSH, and Configuring Licenses on Cisco IOS Devices. The following steps apply to the IPS configuration only.

**Step 1** Create a directory for IPS files on flash. For example, the following command creates a directory named ips:

**Example:**

```
router# mkdir ips
Create directory filename [ips]?
Created dir flash:ips
```

At this point, you can optionally configure the router to use this directory for IPS, or you can do it later in Security Manager (in the IPS > General Settings policy). Use the following commands to configure it in CLI:

**Example:**

```
router# configure terminal
router(config)# ip ips config location flash:ips
```

**Step 2** Configure the Cisco IOS IPS crypto key. The crypto key is used to verify the digital signature for the main signature file (sigdef-default.xml) whose contents are signed by a Cisco private key to guarantee its authenticity and integrity at every release.

You can obtain the CLI required for the key from http://download-sj.cisco.com/cisco/ciscosecure/ids/sigup/5.0/ios/realm-cisco.pub.key.txt (login to Cisco.com is required).

**Tip** Configuring the key through the CLI is probably the easiest way to do it. Alternatively, you can configure it in Security Manager by assigning the IOS_IPS_PUBLIC_KEY pre-defined FlexConfig object to the router's FlexConfig policy. For more information about FlexConfigs, see Managing Flexconfigs.

a) Open the text file and copy its contents to the clipboard (select all text then press Ctrl+C).
b) If necessary, enter **configure terminal** at the router CLI prompt.
c) Paste the copied text file at the router prompt.
d) Exit configuration mode.
e) Enter the **show run** command to confirm that the key was correctly configured.

**Step 3** Syslog is configured for IPS notifications by default. If you want to use SDEE for notifications, enable SDEE:

**Example:**

```
router# configure terminal
router(config)# ip ips notify sdee
```

**Step 4** Select a signature category to compile. For detailed information, see Selecting a Signature Category for Cisco IOS IPS , on page 6.

# Selecting a Signature Category for Cisco IOS IPS

Cisco IPS appliances and Cisco IOS IPS with IPS 5.x format signatures operate with signature categories. All signatures are grouped into categories; the categories are hierarchical. An individual signature can belong to more than one category. Top-level categories help to define general types of signatures. Subcategories exist beneath each top-level signature category. (For a list of supported top-level categories, use your router CLI help (?) with the **category** command.)

Router memory and resource constraints prevent a router from loading all Cisco IOS IPS signatures. Thus, it is recommended that you load only a selected set of signatures that are defined by the categories. Because the categories are applied in a "top-down" order, you should first retire all signatures, followed by "unretiring" specific categories. Retiring signatures enables the router to load information for all signatures, but the router does not build the parallel scanning data structure.

Retired signatures are not scanned by Cisco IOS IPS, so they do not fire alarms. If a signature is irrelevant to your network or if you want to save router memory, you should retire signatures, as appropriate.

Security Manager does not manage the signature category command. You cannot configure it directly with a policy. However, you can configure the FlexConfig policy to include a FlexConfig object that configures the command. There is a pre-defined object, IOS_IPS_SIGNATURE_CATEGORY, that you can use. If you want to configure a different category than basic, make a copy of the object and edit it. For information on how to use FlexConfigs, see Managing Flexconfigs.

**Tip** If you do not use the **category** command to select a subset of IPS signatures that the device will attempt to compile, Security Manager will configure the category command to enable the IOS IPS Basic category to prevent the device resources from being overloaded. You can change the category manually on the device to select another set of signatures to compile. We recommend that you configure the category before adding the device to Security Manager; however, this is not possible if you add the device through manual definition.

The following example shows how to first retire all signatures, then to configure the basic category and unretire the basic signatures:

```
Router> enable
Router# configure terminal
Router(config)# ip ips signature-category
Router(config-ips-category)# category all
Router(config-ips-category-action)# retired true
Router(config-ips-category-action)# exit
Router(config-ips-category)# category ios_ips basic
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# exit
```

# Configuring General Settings for Cisco IOS IPS

Use the General Settings page to specify the global settings used for Cisco IOS IPS properties defined for a particular router. The default settings are appropriate for most situations; however, you must specify an IPS configuration file location. If storing the configuration file on the router, you must first create the directory as described in Initial Preparation of a Cisco IOS IPS Router, on page 5.

### Navigation Path

- (Device view) Select **IPS > General Settings** from the Policy selector.
- (Policy view) Select **IPS (Router) > General Settings**, then select an existing policy or create a new one.

### Related Topics

- Overview of Cisco IOS IPS Configuration , on page 4
- Understanding Cisco IOS IPS , on page 1

### Field Reference

***Table 1: General Settings Page***

| Element | Description |
|---|---|
| Block Traffic when IPS engine is unavailable | Whether to block all inspected traffic if the IPS engine is not available, for example, when the signature engine is being built or if it fails to build.<br><br>If you select this option, any traffic specified for inspection is dropped if IPS cannot process it (also known as fail-closed mode). Otherwise, traffic is allowed to pass in accordance with the other rules in place on the router (the default). |

| Element | Description |
|---|---|
| Apply Deny Action On | Where to apply ACL entries to drop traffic for Deny Attacker Inline or Deny Flow Inline events. Select one of the following values:<br>• **Ingress Interface** (the default)—Enforce the deny action on the interface attached to the network from which the traffic originated.<br>• **IPS enabled interfaces**—Enforce the deny action on the interface on which the triggered IPS rule is applied.<br>Enabling this option causes IOS IPS to apply the ACLs directly to the 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. |
| SDEE Properties | |
| Maximum Subscriptions | The maximum number of concurrent SDEE subscriptions allowed, in the range of 1-3. An SDEE subscription is a live feed of SDEE events.<br>The default is 1. |
| Maximum Alerts | 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.<br>The default is 200. |
| Maximum Messages | 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.<br>The default is 200. |
| IPS Config Location Properties | |
| IPS Config Location | The location where the router will save IOS IPS specific configuration files. These configuration files are automatically updated every time the IOS IPS configuration is changed or updated from Security Manager. When the router reboots, the IOS IPS configuration is retrieved and restored from these configuration files.<br>To specify a location on the router, enter the name of the directory. The directory must already exist; Security Manager does not create it. For example, flash:ips.<br>**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.<br>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 save the config files to an HTTP server, then enter http://172.27.108.5/ips-cfg.<br>Supported servers for saving the IOS IPS configuration files are: http://, https://, ftp://, rcp://, scp://, and tftp://. |
| Max retries | When storing configuration files on a remote system, how many times the router is to attempt to contact the remote system.<br>The default is 1. |

| Element | Description |
|---|---|
| Timeout seconds between retries | When storing configuration files on a remote system, how long the router is to wait before attempting to contact the configuration location again.<br>The default is 1. |

# Configuring IOS IPS Interface Rules

**Note** From version 4.17, though Cisco Security Manager continues to support IOS and IPS features/functionality, it does not support any bug fixes or enhancements.

Use the IPS Interface Rules policy to enable IPS inspection on Cisco IOS IPS routers and to specify the interfaces that will be subject to IPS inspection. You can identify a subset of the traffic on the interface that is subject to inspection by configuring an ACL and by specifying the traffic direction relative to the interface.

**Related Topics**

- Overview of Cisco IOS IPS Configuration , on page 4
- Understanding Cisco IOS IPS , on page 1

**Step 1** Do one of the following to open the Interface Rules policy you want to modify:

- (Device view) Select **IPS > Interface Rules** from the Policy selector.
- (Policy view) Select **IPS (Router) > Interface Rules** from the Policy selector. Select an existing policy or create a new one.

The policy shows any existing interface rules, including the rule name, the name of the ACL that defines which traffic is inspected (if any), and the interface and traffic direction that is inspected. If no ACL is specified, all traffic on the interface in the specified direction is inspected.

Although the rules are numbered, the sequence of rules has no effect on IPS processing.

**Step 2** Select **Enable IPS** to enable the deployment of IOS IPS configuration to the device.

If Enable IPS is unchecked, IPS rules are removed from all the router interfaces, which disables IPS. Also, no signature or event action policy will be deployed.

**Step 3** Configure the interface rules. The rules identify the interfaces, and traffic direction on the interface, that will be inspected by IPS. The rules can optionally include an ACL to identify a subset of traffic for inspection.

- To add a rule, click the **Add Row (+)** button and fill in the Add IPS Rule dialog box. For detailed information, see IPS Rule Dialog Box , on page 10.
- To edit a rule, select it and click the **Edit Row (pencil)** button.
- To delete a rule, select it and click the **Delete Row (trash can)** button.

# IPS Rule Dialog Box

**Note** From version 4.17, though Cisco Security Manager continues to support IPS features/functionality, it does not support any bug fixes or enhancements.

Use the Add or Edit IPS Rule dialog box to identify the traffic flows to be inspected using the active signature policy.

### Navigation Path

From the Interface Rules policy, click the **Add Row** button to add a new rule, or select a rule and click the **Edit Row** button. For information on opening the Interface Rules policy, see Configuring IOS IPS Interface Rules , on page 9.

### Field Reference

***Table 2: Add or Edit IPS Rule Dialog Box***

| Element | Description |
|---|---|
| Rule Name | The unique name for this IPS rule.<br>IPS rule names are not case sensitive. You cannot use a rule name that contains the same characters as another one previously defined but using a different case. For example MYRULE and MyRule are the same. |
| ACL Name | The name of the ACL policy object that defines which traffic should be subject to IPS inspection. If you do not specify an ACL, all traffic on the interface/direction pairs listed in the Interface Pairs table is subject to inspection.<br>**Tip** If you create an ACL, permit entries identify traffic that is subject to inspection, whereas deny entries identify traffic that is exempt from inspection. Remember that there is an implicit deny any any rule at the end of the ACL, so if your intention is simply to identify exempt traffic, be sure to add a permit any any rule at the end of the ACL.<br>Enter the name of the ACL policy object, or click **Select** to select it from a list or to create a new object. |
| Interface Pairs table | The interfaces and traffic direction pairs that are subject to IPS inspection.<br>• To add a pair, click the **Add Row (+)** button and fill in the Adding Pair dialog box. See Pair Dialog Box , on page 11.<br>• To edit a pair, select it and click the **Edit Row (pencil)** button.<br>• To delete a pair, select it and click the **Delete Row (trash can)** button. |

# Pair Dialog Box

Use the Adding or Editing Pair dialog box to identify the interface and traffic direction pair to add to a Cisco IOS IPS interface rule. For information on configuring interface rules, see Configuring IOS IPS Interface Rules , on page 9.

## Navigation Path

From the Add or Edit IPS Rule dialog box, click the **Add Row** button to add a new pair, or select a pair and click the **Edit Row** button. For information on opening the Add or Edit IPS Rule dialog box, see IPS Rule Dialog Box , on page 10.

## Field Reference

*Table 3: Adding or Editing Pair Dialog Box*

| Element | Description |
|---|---|
| Direction | The traffic direction, with respect to the interface, on which IPS inspection should be performed. Select one of the following:<br>• **In** (default)—The IPS rule should be applied to inbound traffic.<br>• **Out**—The IPS rule should be applied to outbound traffic.<br>• **Both**—The IPS rule should be applied to both inbound and outbound traffic. |
| Interfaces | The interface on which to apply this IPS rule. Enter the name of an interface or interface role object, or click **Select** to select the interface or interface role from a list or to create a new interface role.<br>If you use interface roles, the rule is applied to all interfaces on the device that are defined by the role. The interfaces that match the role cannot conflict with an existing rule. You cannot specify the same interface for more than one interface rule. |