



CHAPTER 9

Cisco IPS Modules

MARS can monitor Cisco IPS modules installed in Cisco switches and Cisco ASA appliances. To prepare these modules, you must perform the following tasks:

- Define the base module, either the router, switch, or Cisco ASA, as defined in [Chapter 17, “Cisco Routers”](#), [Chapter 15, “Cisco Switch Devices”](#), and [Cisco Firewall Devices \(PIX, ASA, and FWSM\)](#), page 19-1.
- Bootstrap the base module to enable SDEE traffic on the Cisco IPS module, to forward events to the MARS Appliance, and to enable MARS to access the SDEE events stored on the modules. Module access enables MARS to retrieve trigger packets and IP log information.
- Add the IPS feature set to the base module previously defined in the web interface.

The following topic also supports the configuration of the Cisco IPS modules:

- [Verify that MARS Pulls Events from a Cisco IPS Device](#), page 4-6

This chapter contains the following topics:

- [Enable SDEE on the Cisco IOS Device Running IOS IPS](#), page 9-1
- [Add an IPS Module to a Cisco Switch or Cisco ASA](#), page 9-2

Enable SDEE on the Cisco IOS Device Running IOS IPS

In addition to enabling either Telnet or SSH for configuration discovery on a Cisco IOS device, you must also ensure that SDEE is enabled on the device that supports the IOS IPS. SDEE is used to publish events to MARS about signatures that have fired.

To enable SDEE protocol on the Cisco IOS device running IOS IPS, perform the following steps:

-
- Step 1** Log in to the Cisco IOS device using the enable password.
- Step 2** Enter the following commands to enable MARS to retrieve the events from the IOS device:

```
Router(config)#ip http secure-server
Router(config)#ip ips notify sdee
Router(config)#ip sdee subscriptions 3
Router(config)#ip sdee events 1000
Router(config)#no ip ips notify log
```



Note The “no ips notify log” causes the IPS modules to stop sending IPS events over syslog.

Add an IPS Module to a Cisco Switch or Cisco ASA

You can enable in-line IPS functionality and signature detection in multi-purpose Cisco platforms. You can identify an IDS-M2 running in a Cisco Switch or an ASA-SSM running in a Cisco ASA. To represent either of these modules, you must define the settings for the module as part of the base platform, which must be previously defined under Admin > System Setup > Security and Monitor Devices.

To add an IPS module to a Cisco Switch or Cisco ASA, follow these steps:

- Step 1** Click **Admin > System Setup > Security and Monitor Devices**
- Step 2** From the list of devices, select the Cisco switch or Cisco ASA to which you want to add the IPS module and click **Edit**.
- Step 3** Click **Add Module**.

Device Type:

- Cisco ASA 7.0
- Cisco IPS 5.x

→	*Device Name:	<input type="text"/>
→	*Context Name:	<input type="text"/>
→	*Reporting IP:	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>
	SNMP RO Community:	<input type="text"/>

143172

- Step 4** Select **Cisco IPS 5.x** or **Cisco IPS 6.x** in the Device Type list.

For Cisco switches, you can also add a Cisco IPS 4.0 module. You configure these modules just as you would a standalone sensor. For instructions on configuring these modules, refer [Cisco IDS 4.0 and IPS 5.x Sensors, page 2-1](#).

Figure 9-1 Configure Cisco IPS 5.x or 6.x

Device Type:

→ *Device Name:

→ Reporting IP:

→ *Access Type: **SSL**

 Login:

 Password:

 Port:

→ Monitor Resource Usage:

 Pull IP Logs:

[Optional: for attack path calculation and mitigation enter monitoring networks information]

→ Monitored Networks:

Select a Network:

Define a Network:

 Network IP:

 Mask:

- Step 5** Enter the hostname of the sensor in the Device Name field.
- Step 6** Enter the administrative IP address in the Reporting IP field.
- Step 7** The Reporting IP address is the same address as the administrative IP address.
- Step 8** In the Login field, enter the username associated with the administrative account that will be used to access the reporting device.
- Step 9** In the Password field, enter the password associated with the username specified in the Login field.
- Step 10** In the Port field, enter the TCP port on which the webserver running on the sensor listens. The default HTTPS port is 443.



Note While it is possible to configure HTTP only, MARS requires HTTPS.

- Step 11** (Optional) For attack path calculation and mitigation, specify the networks being monitored by the sensor. To manually define the networks, select the **Define a Network** radio button.
- a. Enter the network address in the Network IP field.
 - b. Enter the corresponding network mask value in the Mask field.
 - c. Click **Add** to move the specified network into the Monitored Networks field.
 - d. Repeat as needed.

- Step 12** (Optional) To select the networks that are attached to the device, click the **Select a Network** radio button.
- a. Select a network from in the Select a Network list.
 - b. Click **Add** to move the specified network into the Monitored Networks field.
 - c. Repeat as needed.
- Step 13** Click **Test Connectivity** to verify the configuration.
- Step 14** To save your changes, click **Submit**.
- Step 15** To enable MARS to start sessionizing events from this module, click **Activate**.
-