



CHAPTER 2

Configuring Network-based IDS and IPS Devices

Revised: June 27, 2008

Network intrusion detection and intrusion prevention systems are a critical source for identifying active attacks to MARS. This chapter explains how to bootstrap and add network-based IDS and IPS devices to MARS.

This chapter contains the following topics:

- [Cisco IDS 4.0 and IPS 5.x Sensors, page 2-1](#)

Cisco IDS 4.0 and IPS 5.x Sensors

Adding a Cisco IDS or IPS network sensor to MARS involves two parts:

1. [Bootstrap the Cisco Sensor, page 4-1](#)
2. [Add and Configure a Cisco IDS or IPS Device in MARS, page 2-2](#)
3. [Verify that MARS Pulls Events from a Cisco IPS Device, page 4-6](#)

The following topic supports Cisco IDS and IPS devices:

- [View Detailed Event Data for Cisco IPS Devices, page 4-2](#)



Note

If you've imported your sensor definitions using the seed file format, as specified in [Load Devices From the Seed File, page 1-45](#), you must define the networks monitored by the sensor.

Bootstrap the Cisco Sensor

Preparing a sensor to be monitored by MARS involves preparing the sensor so MARS can communicate with it and ensuring that the correct data is being generated.

This section contains the following topics:

- [Enable the Access Protocol on the Sensor, page 2-2](#)
- [Enable the Correct Signatures and Actions, page 4-2](#)

Enable the Access Protocol on the Sensor

The configuration of the sensor depends on the version of the software that is running on the sensor. The following topics identify the requirements of each version:

This section contains the following topics:

- [Cisco IDS 4.x Software, page 2-2](#)
- [Cisco IPS 5.x, 6.x, and 7.x Software, page 4-1](#)

Cisco IDS 4.x Software

For Cisco IDS 4.x devices, MARS pulls the logs using RDEP over SSL. Therefore, MARS must have HTTPS access to the sensor. To prepare the sensor, you must enable the HTTP server on the sensor, enable TLS to allow HTTPS access, and make sure that the IP address of MARS is defined as an allowed host, one that can access the sensor and pull events. If the sensors have been configured to allow access from limited hosts or subnets on the network, you can use the **accessList ipAddress ip_addressnetmask** command to enable this access.

Cisco IPS 5.x, 6.x, and 7.x Software

For Cisco IPS 5.x, 6.x, and 7.x devices, MARS pulls the logs using SDEE over SSL. Therefore, MARS must have HTTPS access to the sensor. To prepare the sensor, you must enable the HTTP server on the sensor, enable TLS to allow HTTPS access, and make sure that the IP address of MARS is defined as an allowed host, one that can access the sensor and pull events. If the sensors have been configured to allow access from limited hosts or subnets on the network, you can use the **access-listip_address/netmask** command to enable this access.

Enable the Correct Signatures and Actions

If the signature actions are correctly configured, MARS can display the trigger packet information for the first event that fires a signature on a Cisco IDS or IPS device. MARS is also able to pull the IP log data from Cisco IDS and IPS devices, however, this operation is system intensive. Therefore, you should select the set of signatures that generate IP log data carefully.

When configuring the active signatures on a Cisco IDS or IPS device, you must specify the alert action and the action that generates the desired data:

- To view trigger packets, you must enable the “produce-verbose-alert” action.
- To view IP logs, you must enable the alert or “produce-verbose-alert” action and the “log-pair-packets” action.



Caution

Configuring IP logging and verbose alerts on the sensor is system intensive and does affect the performance of your sensor. In addition, it affects the performance of your MARS Appliance. Because of these effects, you be cautious in configuring signatures to generate IP logs.

Add and Configure a Cisco IDS or IPS Device in MARS

To add and configure a Cisco IDS or IPS device in MARS, follow these steps:

-
- Step 1** Click **Admin > System Setup > Security and Monitor Devices > Add**.

- Step 2** Do one of the following:
- Select **Cisco IDS 4.0** from the Device Type list.

Figure 2-1 Configure Cisco IDS 4.0

Device Type: Cisco IDS 4.0

→ *Device Name:

→ *Reporting IP:

→ *Access Type: **SSL**

 Login:

 Password:

 Port:

143213

- Select **Cisco IPS 5.x** from the Device Type list.

Figure 2-2 Configure Cisco IPS 5.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:

143176

- Step 3** Enter the hostname of the sensor in the Device Name field.

The Device Name value must be identical to the configured sensor name.

- Step 4** Enter the administrative IP address in the Access IP field.
- Step 5** Enter the administrative IP address in the Reporting IP field.
The Reporting IP address is the same address as the administrative IP address.
- Step 6** In the Login field, enter the username associated with the administrative account that will be used to access the reporting device.
- Step 7** In the Password field, enter the password associated with the username specified in the Login field.
- Step 8** 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 9** To pull the IP logs from the sensor, select **Yes** in the Pull IP Logs box.
- Step 10** (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.
- Enter the network address in the Network IP field.
 - Enter the corresponding network mask value in the Mask field.
 - Click **Add** to move the specified network into the Monitored Networks field.
 - Repeat as needed.
- Step 11** (Optional) To select the networks that are attached to the device, click the **Select a Network** radio button.
- Select a network from in the Select a Network list.
 - Click **Add** to move the specified network into the Monitored Networks field.
 - Repeat as needed.
- Step 12** To verify the configuration, click **Test Connectivity**.
- Step 13** Click **Submit**.
-

Specify the Monitored Networks for Cisco IPS or IDS Device Imported from a Seed File

After you import a Cisco IPS or IDS device into MARS using a seed file, you must define the networks that are monitored by that sensor.

To define the networks monitored by a sensor, follow these steps:

-
- Step 1** Click **Admin > System Setup > Security and Monitor Devices**.
- Step 2** Select the check box next to the Cisco IPS or IDS device that was imported using a seed file. and click **Edit**.
- Step 3** (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.
- 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 4** (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 5** To save your changes, click **Submit**.
- Step 6** To enable MARS to start sessionizing events from this module, click **Activate**.
-

View Detailed Event Data for Cisco IPS Devices

In addition to the alert message, you can view the trigger packets and IP log data associated with incidents reported by Cisco IDS 4.x and Cisco IPS 5.x, 6.x, and 7.x devices, whether they are sensor appliances or modules. This information is useful when an in-depth understanding of the attack method is desired. MARS includes two event types that focus on these two data types:

- **Trigger packet data.** Identifies the data that was being transmitted on the network the instant an alarm was detected. You can use this information to help diagnose the nature of an attack. The trigger packet provides a single data packet—the data packet that caused the alarm to fire.
- **Packet data.** Identifies the data that was being transmitted on the network the instant an alarm was detected. You can use this information to help diagnose the nature of an attack. Although the amount of data contained in an IP log varies based on sensor configuration, by default an IP log contains 30 seconds of packet data. To view this data, you must enable the Pull IP Logs option on the Cisco IPS device under Admin > System Setup > Security and Monitor Devices.

For the correct signature settings required to generate this data, see [Enable the Correct Signatures and Actions, page 4-2](#).

If the IP log feature is enable for the reporting Cisco IPS device, these event types are combined as part of the incident data. You can view this data by drilling down in an incident, expanding the desired event type (either Packet Data or Trigger Packet Data), selecting an event, and clicking on the RAW Events for this Session icon under the Reporting Device column of that event. The source, destination, and other data displayed for these events matches that of the original alert. In addition, this data appears hexadecimal and binary format.

**Note**

The trigger packet and IP log data is stored using a base64-encoded format in the MARS database. Therefore, keyword search does not work on it if you just provide the search string.

Verify that MARS Pulls Events from a Cisco IPS Device

**Note**

If the Test Connectivity operation does not fail when configuring a Cisco IPS device in the MARS web interface, then communications are enabled. This task allows you to further verify the alerts are generated and pulled correctly.

It is common to create benign events on the network to verify the data flow. To verify the data flow between a Cisco IPS device and MARS, perform the following tasks:

1. On the Cisco IPS device, enable and alert on the signatures 2000 and 2004. The signatures monitor ICMP messages (pings).
2. Ping a device on the subnet on which the Cisco IPS device is listening. The events are generated and pulled by MARS.
3. Verify that the events appear in the MARS web interface. You can perform a query using the Cisco IPS device.
4. Once the dataflow is verified, you can disable the 2000 and 2004 signatures on the Cisco IPS device.