Configuring and Generating Reports

This chapter describes IME reports and how to configure and generate them. It contains the following topics:

Understanding IME Reporting

The IME lets you create different reports that you can customize using different filters. A report consists of a window with a bar or pie chart along with the tabular data used for the graphs. There are IME report types, user-defined reports, and demo reports that are predefined examples of reports.

The Reports window is divided in to two parts: the left-hand pane, the Report tree, shows the reports list in the form of a tree, and the right-hand pane, the Report Settings pane, contains the report. The Report tree contains a set of predefined reports, such as Basic Top Attacker, and place to store user-defined reports under the My Reports node. When you select a report in the list and click **Generate Report**, the corresponding report containing a graph and a table is displayed in the lower half of the Report Settings pane. The Reports Setting pane contains two tabs, General and Filter, which let you customize the report.

You can also save the reports as PDF or RTF files and print them in the IME. And you can set up automatic reporting and have the IME send you the reports you want automatically. The IME summarizes which reports were successfully generated and then attaches them as a PDF to the email. To set up automatic reporting, go to **Preferences > Tools > Reports**.

Note The Filter tab and Add Filter dialog box fields now support IPv6 and IPv4 addresses.

These are the IME report types:

- Top Attacker Reports—Shows top attacker IP addresses for a specified time. You specify the top number of attacker IP addresses. There are four predefined top attacker reports:
  - Basic Top Attacker
  - Top 10 Attackers Last 1 Hour
  - Top 10 Attackers Last 8 Hours with High Severity
  - Top 20 Critical Attackers Last 24 Hours

- Top Victim Reports—Shows top victim IP addresses for a specified time. You specify the top number of victim IP addresses. There are four predefined top victim reports:
  - Basic Top Victim
  - Top 10 Victims Last 1 Hour
  - Top 10 Victims Last 8 Hours with High Severity
  - Top 20 Victims with Action Denied Attacker
- Top Signature Reports—Shows top signatures fired for a specified time. You specify the top number of signatures. There are four predefined top signature reports:
  - Basic Top Signature
  - Top 10 Signatures Last 1 Hour
  - Top 10 Signatures Last 8 Hours with High Severity
  - Top 20 Critical Signatures Last 24 Hours
- Attacks Over Time Reports—Shows the attacks over a specified time. There are five predefined reports:
  - Basic Over Time Attack
  - Attacks Blocked in Last 24 Hours
  - Attacks Dropped in Last 24 Hours
  - Attacks Over Time Last 1 Hour
  - Critical Attacks Over Last 24 Hours
- Filtered Events vs. All Events Reports—Displays a set of events against the total events for a specified time period. There is one predefined report:
  - Negative Reputation Events
- Global Correlation Reports—Displays the global correlation reports since the sensor has been running. There are two predefined global correlation reports:
  - Reputation Filter
  - Global Correlation
- Specialized Reports—Displays the specialized reports. There is one predefined specialized report:
  - Obfuscated Traffic/Attacks—This report contains statistics on suspect and explicit traffic obfuscation activity. It combines a top attacker report with a top event report. Traffic obfuscation is way of getting attacks through the security device. With the strong obfuscation detection and cleansing capabilities of the Cisco IPS, you can detect traffic obfuscation and deal with potential threats.

Configuring and Generating Reports

Note The Filter tab and Add Filter dialog box fields now support IPv6 and IPv4 addresses.

You can customize your report by configuring the number of items you want in your report and what the time interval should be. You can also use DNS to resolve the IP addresses. You can also use filters to further refine the type of information you want your report to contain.

To configure and generate reports, follow these steps:

Step 1 In the Report tree, click **New**, and then in the New Report dialog box, enter the name of the new report, choose the type of report from the drop-down list, and then click **OK**. Your new report shows up under My Reports in the Report tree.

Step 2 Select your report, and on the **General** tab, configure the settings for your report:

a. In the Report Description field, enter a description for this report.

b. In the Top field, enter how many top events you want to see in this report.

c. Check the **Resolve Addresses Using DNS** check box, if you want to use DNS address resolution.

d. Configure the time interval for this report, either the duration or enter a custom time.

Step 3 On the **Filter** tab, from the Filter Name drop-down menu, choose the filter name, or to add a filter, click the **Note** icon.

Step 4 In the Manage Filter Rules dialog box, configure the filter fields for your report.

Step 5 Click **Generate Report**. Your report shows up in the bottom half of the Report Settings pane, displaying the statistics in graph and table form.

Step 6 To customize the display, choose Bar or Pie Chart in the **Display Type** drop-down menu.

Step 7 Click **Print** to print the report, or click **Save** to save the report in PDF or RFT format to your hard-disk drive.

Step 8 To see events for a single IP address, choose the IP address from the Events for drop-down list.

For More Information

- For the procedure for creating a filter, see Configuring Filters, page 3-16.
- For the procedure for configuring events for single IP addresses, see Working With a Single Event for Individual Top Attacker and Victim IP Addresses, page 3-14.
- For the procedure for configuring events for single signatures, see Working With a Single Event for a Top Signature, page 3-15.