Managing Reports

Use the Report Manager application to view security and usage reports for devices and remote access IPsec and SSL VPNs.

This chapter contains the following topics:

Understanding Report Management

Use the Report Manager application to view security and usage reports for devices and remote access IPsec and SSL VPNs. These reports can provide useful information about your network.

The Report Manager aggregates information that is collected from monitored devices by the Event Manager service. Thus, to view reports about a device, you must also be monitoring the device in Event Viewer. Some statistics, such as VPN statistics, are obtained directly from the device through regular polling at five minute intervals. Aggregated data is kept for 90 days with data aggregated at 15-minute, hourly, daily, and monthly intervals; 15-minute aggregated data is kept for up to three days, hourly data up to one week. For more information about data aggregation, see Understanding Report Manager Data Aggregation, page 67-4.

You can use Report Manager to develop reports on the following:

- Adaptive Security Appliances (ASA) running ASA Software releases 8.0 and higher. ASA Software 7.x releases are also supported for VPN reports.

  Note VPN reports are not available for Cisco Catalyst 6500 Series ASA Services Modules (ASA-SM), which do not support any VPN configuration. Other types of reports are available for the ASA-SM.

- IPS devices running IPS software release 6.1 and higher (but not IOS IPS devices). This includes dedicated IPS modules installed in ASAs, routers, and switches.
- Remote access IPsec and SSL VPNs hosted on a supported ASA device.

Note Report Manager does not report on FWSM events even though Event Viewer works with FWSM.

The following topics explain Report Manager and its available reports in more detail, and also describe the other types of reports available in Security Manager:

Understanding the Types of Reports Available in Security Manager

Security Manager provides a variety of reporting capabilities. The following are the types of reports available:

- **Security and Usage Reports (Report Manager application)**—You can use the Report Manager application to view aggregated information collected by the Event Manager service from monitored devices. Some information is also obtained directly from the devices. These reports can provide information on network security and remote access IPsec and SSL VPN usage.
- **Activity (Configuration Session) Change Reports**—These reports provide detailed information about the policies changed within a specific activity (in Workflow mode) or configuration session (in non-Workflow mode). For more information, see Viewing Change Reports, page 4-16.
- **Out of Band Change Report**—These reports identify inconsistencies between the configuration that exists on a device and the configuration for the device maintained in Security Manager. You can use this information to proactively address these inconsistencies before deploying configurations, where the change will either be overwritten or the deployment will fail, depending on the behavior you select in the deployment job. For more information, see Detecting and Analyzing Out of Band Changes, page 8-46.
- **Audit Report**—This report provides information about changes to Security Manager and the objects contained in the database. The report includes information about the runtime environment, such as logins and authentication failures, changes to objects, such as activity changes and deployments, and changes to managed devices, such as inventory additions and deletions. For more information, see Generating the Audit Report, page 10-20.
- **Inventory Status**—This report provides information on policy deployment status. For more information, see Viewing Inventory Status, page 69-1.
- **Policy Discovery Status reports**—When you discover policies from a device, either while adding it to the inventory or when rediscovering policies on a managed device, the information about the policy discovery is maintained so that you can view it at a later time. For more information, see Viewing Policy Discovery Task Status, page 5-21.
- **Deployment Status reports**—When you deploy configurations to managed devices, information about the deployment is maintained so that you can view it at a later time. For more information, see Viewing Deployment Status and History for Jobs and Schedules, page 8-27.
- **Deployment and Discovery Status reports for troubleshooting**—You can export deployment and policy discovery status reports in a form suitable for sending to Cisco Technical Support (TAC) to help troubleshoot problems. You might also find these reports useful for your own purposes. For more information, see Generating Deployment or Discovery Status Reports, page 10-28.

- **Extranet VPN Configuration Summaries**—You can print, or generate a PDF file of, a summary of the configuration of an Extranet VPN. This summary can include the preshared key used for the connection. You can use this information to maintain a current record of connections between your network and the networks of partners or service providers. For more information, see Viewing a Summary of a VPN Topology's Configuration, page 24-58.
- **Policy Object Usage report**—This report shows you where a policy object is used, including instances where it is referred to by a policy or another policy object. You can use this information to help determine whether a proposed change to the object will provide the desired effect in all cases where it is used. The information is also helpful if you want to delete an object, because you cannot delete an object that is actively being used by a policy or another policy object. For more information, see Generating Object Usage Reports, page 6-14.
- **Policy Object Override report**—This report shows you all of the device-level overrides currently defined for a policy object, if the object is defined so that overrides are allowed. You can also create and delete overrides from this report. For more information, see Creating or Editing Object Overrides for Multiple Devices At A Time, page 6-19 and Policy Object Overrides Window, page 6-20.
- **Device Manager reports**—Security Manager includes read-only versions of individual device managers, such as the Adaptive Security Device Manager (ASDM), for most supported devices. You can start these device managers directly from Security Manager's Configuration Manager application and use any type of report available in those device managers. These reports are for a single device, and can augment the reports available through Report Manager. They can also provide status information for devices that are not directly supported by Event Viewer or Report Manager. For more information, see Starting Device Managers, page 69-4.

Preparing Devices for Report Manager Reporting

Before you can view reports about a device in Report Manager, you must configure the device to send events to Security Manager and configure Security Manager to monitor the device. Report Manager can provide reports only for devices you are monitoring in Event Viewer, so the device configuration for reporting is identical to the configuration for event monitoring.

Step 1 Configure the devices to send events to Security Manager. You can use Report Manager with the following types of devices:

- ASA 8.0 and higher—For the detailed configuration steps, see Configuring ASA and FWSM Devices for Event Management, page 66-25.
- IPS 6.1 and higher—For the detailed configuration steps, see Configuring IPS Devices for Event Management, page 66-26.

Step 2 Ensure that the devices are selected for event management as described in Selecting Devices to Monitor, page 66-31.

Step 3 Ensure that the Event Manager service is enabled as described in Starting, Stopping, and Configuring the Event Manager Service, page 66-27.

Understanding Report Manager Data Aggregation

Report Manager aggregates information that is collected from monitored devices by the Event Manager service. Thus, to view reports about a device, you must also be monitoring the device in Event Viewer.

Report Manager collects data using two techniques. First, the Event Manager service provides relevant events to Report Manager and then Report Manager decides if it should store those events based on the predefined reports and custom reports that are currently configured. Second, some statistics, such as VPN statistics, are obtained directly from the device through regular polling at five minute intervals.

Table 67-1 Report Manager Data Sources

Reports	Data Sources
FW Reports	
Top Sources Top Destinations Top Services	Built Syslogs: 302013,302015,302017,302020 Deny syslogs: 106001,106006,106007,106010,106011,106014,106015,106016,106017
Top Malware Sites Top Malware Ports Top Infected Hosts	BOTNET Syslogs: 338001,338002,338003,338004,338005,338006,338007,338008,338201,338202,338203,338204
IPS Reports	
All IPS Reports	All IPS Alerts
VPN Reports	

Top Bandwidth Users (Full-Client)
Top Duration Users (Full-Client)
Top Throughput Users (Full-Client)
	For ASA version 8.3 and earlier:
	`show vpn-sessiondb full svc`
	For ASA version 8.4.1 and later:
	`show vpn-sessiondb full anyconnect`

Top Bandwidth Users (IPSec-RA)
Top Duration Users (IPSec-RA)
Top Throughput Users (IPSec-RA)
	For ASA version 8.3 and earlier:
	`show vpn-sessiondb full remote`
	For ASA version 8.4.1 and later:
	`show vpn-sessiondb full ra-ikev1-ipsec`

Top Bandwidth Users (Clientless) Top Duration Users (Clientless) Top Throughput Users (Clientless)	For all ASA versions: `show vpn-sessiondb full webvpn`
User Report	All above show commands.
VPN Device Usage Report	All above show commands.

Report Manager aggregates this collected information at 15-minute, hourly, daily, and monthly intervals. Fifteen-minute aggregated data is kept a day, hourly data up to five days, and the other data for 90 days.

The aggregation schedule occurs at fixed times: 15-minute aggregation occurs at 00, 15, 30, and 45 minutes past the hour; hourly aggregation occurs on the hour (00 minutes); daily aggregation occurs at the change of day (when midnight is reached, the day is aggregated); monthly aggregation occurs at the change of the month.

The aggregation cycle has implications in what you will see in reports:

- Report data does not cover the immediate past. Instead, it covers the most recently completed whole time period of the selected duration. For example, a one-day report covers yesterday, it does not include data for today. In other words, a one day report is not the previous 24 hours starting from the time the report is generated.
- When configuring reports with a custom time period, you cannot select a time period of less than 15 minutes long. A report will always contain at least 15 minutes of aggregated data. Minute entries are rounded to the nearest aggregation time (that is, 00, 15, 30, or 45). You can configure minutes only for custom reports that start and end on the current day.

  Also, because hourly data is kept only up to five days, you can specify hours in a custom time period only for the past five days.
- You cannot generate a report for periods that are longer than the device has been monitored. For example, when you start the Event Manager service for the first time, you will not be able to generate a monthly report until after the month changes. This might be only a few days (for example, if you start the service on the twenty-ninth day of the month), or it might be almost a full month (for example, if you start the service on the first day of the month).

  The exception to this rule is the custom time period report. Custom time period reports are generated using daily aggregation data, so you can select any custom time period.

Note Be aware that your first month of aggregated data might be significantly less than one month's worth of data. If you compare monthly reports, this might appear as a significant discrepancy when in reality you are comparing 30 days of data to 15 days (as an example).

You can configure the default time interval for predefined system reports and configure time intervals in individual reports. The following topics explain the time controls:

- Configuring Default Settings for Reports, page 67-24
- Editing Report Settings, page 67-21

Understanding Report Manager Access Control

The user privileges assigned to your username control what you can do in Report Manager. If you use local users, or other types of non-ACS access control, then all users have access to Report Manager and all reports. However, the following access limits are imposed:

- You must have system administrator or network administrator privileges to configure default settings for the predefined system reports. See Configuring Default Settings for Reports, page 67-24.
- You must have system administrator or network administrator privileges to do the following to another user's schedules: see them, enable or disable them, view results generated from them, or delete them. See the following topics:
  - Viewing Report Schedules, page 67-28

  - Viewing Scheduled Report Results, page 67-30
  - Enabling and Disabling Report Schedules, page 67-30
  - Deleting Report Schedules, page 67-31
- You must have system administrator or network administrator privileges to see a list of all custom reports configured on the server and to delete another user's custom report. See Managing Custom Reports, page 67-27.

If you use ACS to control access to Security Manager, you can also control user access to Report Manager. When using ACS:

- You can control access to the Report Manager application using the View Report Manager privilege. Using this privilege, you could prevent certain users from accessing Report Manager, or create roles that allow access to Report Manager without allowing access to Event Viewer.
- Users can view reports on devices only if they have at least View privileges to the device.

For information on integrating Security Manager with Cisco Secure ACS, see the *Installation Guide for Cisco Security Manager*.

Overview of Report Manager

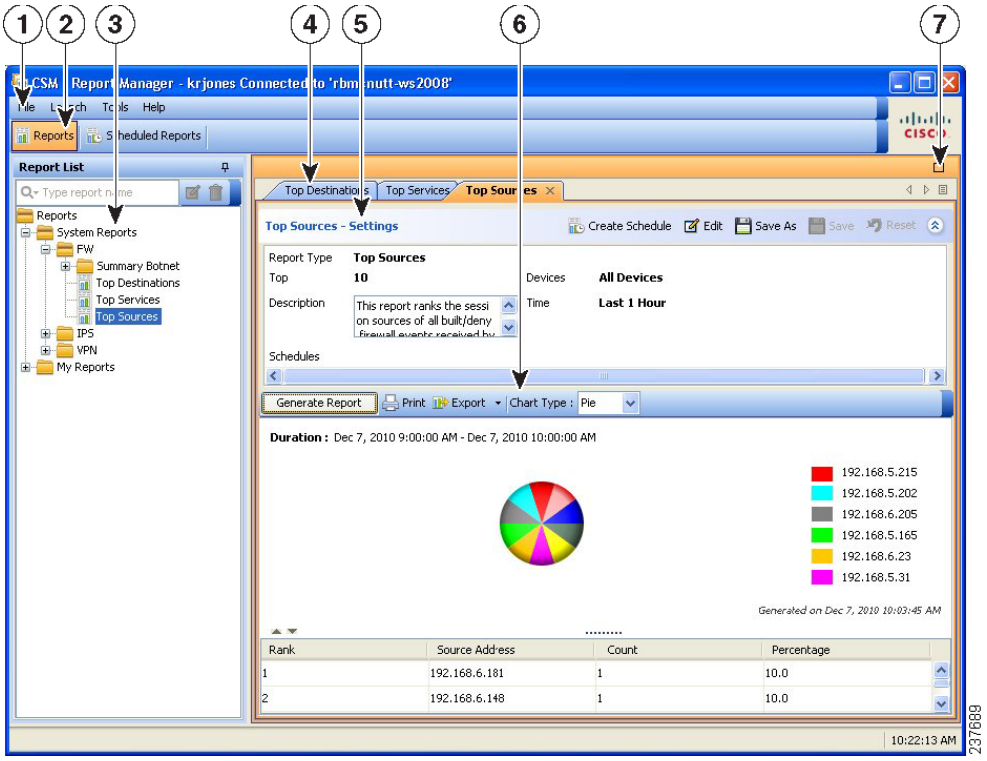
Use Report Manager to create security and usage reports for ASA and IPS devices, and for remote access IPsec and SSL VPNs hosted on ASA devices. For more information about supported devices and the reports you can generate using Report Manager, see Understanding Report Management, page 67-1.

To open Report Manager, do any of the following:

- Select **Start > All Programs > Cisco Security Manager Client > Report Manager** from the Windows Start menu (your exact command path might differ), or double-click the Report Manager icon on the desktop. You are prompted to log in. For more information about starting a Security Manager client application, see Logging In to and Exiting the Security Manager Client, page 1-11.
- Select **Launch > Report Manager** from the Configuration Manager or Event Viewer applications. Report Manager is opened using the same user account that you used to log into the other application.

The following illustration and subsequent list explain the basics of Report Manager.

Figure 67-1 Report Manager Main Window



The following list explains the main Report Manager window and its call-outs in more detail.

- **Menu Bar (1)**—General commands for performing actions in Report Manager. For a description of the commands, see Report Manager Menus, page 67-8.
- **Main Window Tabs (2)**—The main window area consists of the following tabs:
  - Reports—Use the Reports tab to generate reports on demand, to create custom reports, and to perform other report-oriented tasks. The illustration above, and most of the information in this topic, relates to the Reports tab. For information on the tasks you can perform from the Reports tab, see Working with Reports in Report Manager, page 67-18.
  - Scheduled Reports—Use the Scheduled Reports tab to view and manage report schedules. For more information on the Scheduled Reports tab, see Viewing Report Schedules, page 67-28. For information on the tasks you can perform from the Scheduled Reports tab, see Scheduling Reports, page 67-27.
- **Report List (3)**—The left pane of the Reports tab is a list of reports. The list is organized into folders; the System Reports are predefined reports, whereas the My Reports folder contains the custom reports that you create. Double-click a report to open it, select the report and select **File > Open**, or right-click the report and select **Open Report**. For more information about using the report list, see Understanding the Report List in Report Manager, page 67-9.
- **Report Pane (4, 5, 6, 7)**—The right pane of the Reports tab shows the open reports. Each open report is represented on separate tabs (you can have up to five open reports). Note that you can arrange reports horizontally or vertically in this space, or even make a report float to a separate window. For more information about how you can arrange or float reports, see Arranging Report Windows, page 67-25.

You can use the Maximize control (7) above the pane to make it take over the entire workspace (hiding the report list). After maximizing the pane, the control changes to a Restore control to return the main window to a two-pane view.

You can use the right and left arrows, and the Show List icon button, to scroll through the open reports or to go directly to a report. However, clicking the tab with the desired report name is the easiest way to go to a report.

The Report Pane includes these areas for each open report:

- Report Settings pane (5)—The top part of the report shows the report settings, which are the criteria used to generate the report. You can open and close the settings pane by clicking on the heading, or on the expand/collapse icon button. The heading includes a toolbar that has commands that you can perform on the report. For more information about the settings pane, see Understanding the Report Settings Pane, page 67-10.
- Generated Report Pane and Report Toolbar (6)—Below the settings pane is an additional toolbar used to generate and manipulate report data. Use these controls to generate the report using the criteria defined in the report settings, to print the report or to export it to PDF or CSV format, or to change the type of graphic displayed in the report.

  The bottom part of the report pane is the actual report. This area is empty until you click the Generate Report button. The top of the report shows a graphical representation of the information, the lower page shows the tabular data. For more information, see Understanding the Generated Report Pane and Toolbar, page 67-11 and Opening and Generating Reports, page 67-18.

Report Manager Menus

The following table describes the commands on the menus in Report Manager.

Table 67-2 Report Manager Menu Reference

Menu	Command	Description
File	Open	Opens the report selected in the report list on the Reports tab. See Opening and Generating Reports, page 67-18.
	Save	Saves changes made to the report settings. This command is available for custom reports only. See Saving Reports, page 67-25.
	Save As	Saves the report as a new report. Use this command to create new reports from existing reports. See Saving Reports, page 67-25.
	Close Report Close All Reports	Closes the active open report, or closes all open reports. See Closing Report Windows, page 67-26.
	Exit	Exits Report Manager.
Launch	Configuration Manager Event Viewer	Opens the indicated Security Manager application.

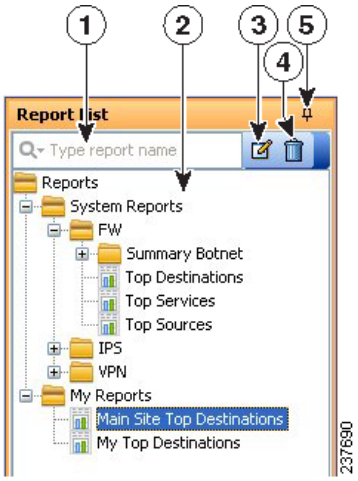
Table 67-2 Report Manager Menu Reference (Continued)

Menu	Command	Description
Tools	Default Report Settings	Configures the default settings for predefined system reports. See Configuring Default Settings for Reports, page 67-24.
	Custom Report List	Displays all custom reports configured on the server, not just those that you created. You can manage reports from this window. See Managing Custom Reports, page 67-27.
Help	Help about this page	Opens the online help to a topic relevant to the page currently displayed in the main window.
	About Report Manager	Displays copyright, version, and licensing information for the application.

Understanding the Report List in Report Manager

The left pane of the Reports tab in Report Manager displays a list of available reports, as shown in the following illustration.

Figure 67-2 Report Manager Report List



The Report List includes the following controls (illustration call-outs cited):

- **Quick Filter search box (1)**—Use the quick filter search box to search for reports in the list. The list is filtered as you type, although folders are not opened automatically. The default is to search for the text string anywhere in the report name. However, you can click the down arrow in the Quick Filter box to select a variety of options to change how your search string is evaluated.
- **List of reports (2)**—The list is organized into folders; the System Reports are predefined reports (explained in Understanding the Predefined System Reports in Report Manager, page 67-13), whereas the My Reports folder contains the custom reports that you create. Double-click a report to open it, or select the report and select **File > Open**. For more information, see Opening and Generating Reports, page 67-18.

- **Right-click shortcut menu (not shown)**—If you right-click on a report, you get a list of additional commands that you can perform, such as opening the report, creating a schedule, or saving the report as a new report.
- **Edit button (3)**—Click the Edit button to change the name of the selected custom report. You can edit custom reports only. For more information, see Renaming Reports, page 67-26.
- **Delete button (4)**—Click the Delete button to delete the selected custom report. You can delete custom reports only. For more information, see Deleting Reports, page 67-27
- **Push Pin button (5)**—Click the Push Pin icon to control whether the report list pane is opened or closed. If the pin is vertical, the report list remains open unless you maximize the report pane (the right pane). If the pin is horizontal, the report list collapses to the left margin, and you must click the Report List heading in the left margin to open the list.

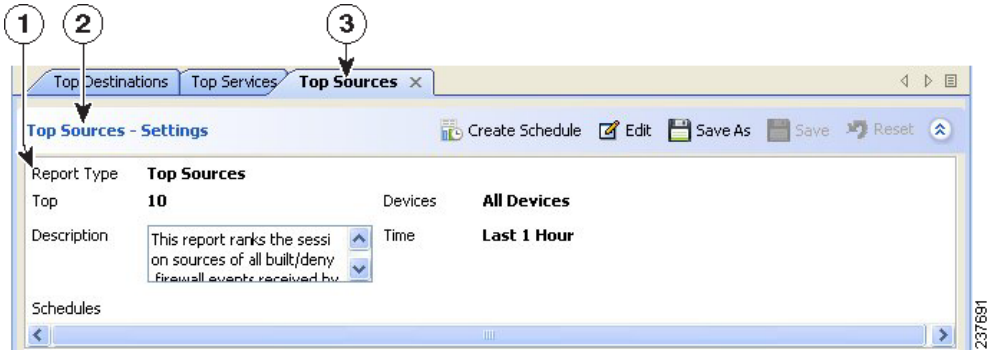
Related Topics

- Overview of Report Manager, page 67-6
- Understanding Report Management, page 67-1
- Working with Reports in Report Manager, page 67-18
- Viewing Report Schedules, page 67-28
- Scheduling Reports, page 67-27
- Arranging Report Windows, page 67-25

Understanding the Report Settings Pane

The top part of the right side of the Reports tab, with a report open, shows the report settings. These settings define the criteria that are used to generate a report. The following illustration shows an example of the report settings pane.

Figure 67-3 Report Manager Report Settings



The Report List includes the following controls (illustration call-outs cited):

- **Report tab (3)**—Although not part of the settings per se, each report appears on its own tab. The settings are the top part of the tab. If you right-click the tab itself, you get a menu of commands that allow you to arrange report windows. For more information, see Arranging Report Windows, page 67-25.

- **Heading and toolbar (2)**—The top of the settings pane includes the heading (for example, Top Sources - Settings) and a row of buttons for manipulating the settings. You can open or close the pane by clicking the heading or the up arrow button in the far right of the toolbar. The other buttons have the following functions:
  - Create Schedule button—Creates a new schedule for automatically generating reports based on these settings. For more information, see Configuring Report Schedules, page 67-28.
  - Edit button—Edits the report settings. For more information, see Editing Report Settings, page 67-21.
  - Save As button—Saves the report as a new report. If you edit the settings for a predefined system report, and you want to save your changes, you must use Save As to create a custom report. For more information, see Saving Reports, page 67-25 and Creating Custom Reports, page 67-20.
  - Save button—Saves changes to the settings. You can save changes for custom reports only. For more information, see Saving Reports, page 67-25.
  - Reset button—Resets the settings to the last saved values.
  - Expand/Collapse button (double up/down arrows)—Toggles between opening and closing the report setting pane.
- **Settings display (1)**—Below the heading and toolbar is a summarization of the report settings. Information includes the type of report, the devices included in the report, the time range, a description, the schedules defined for the report, and other properties unique to the report.

  To change the description, type your changes directly into the Description edit box.

Related Topics

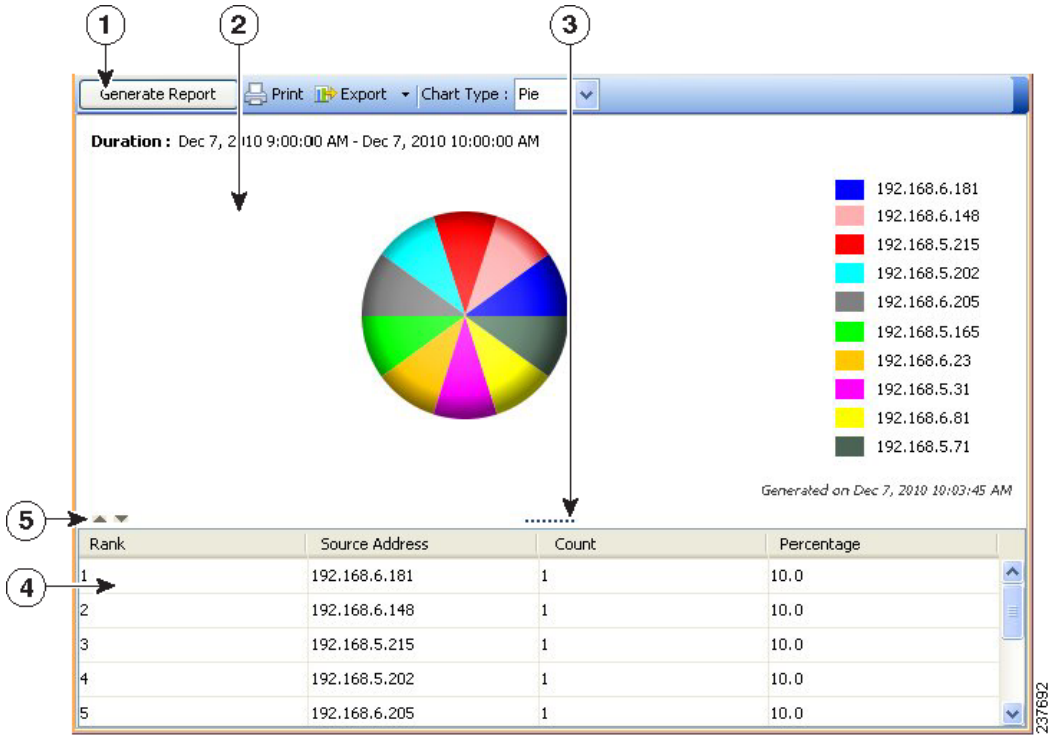
- Opening and Generating Reports, page 67-18
- Understanding the Generated Report Pane and Toolbar, page 67-11
- Overview of Report Manager, page 67-6
- Understanding Report Management, page 67-1
- Working with Reports in Report Manager, page 67-18
- Viewing Report Schedules, page 67-28
- Scheduling Reports, page 67-27

Understanding the Generated Report Pane and Toolbar

The bottom part of the right side of the Reports tab, with a report open, shows the generated report and report toolbar. This pane displays the results of clicking the Generate Report button.

The following illustration shows an example of the generated report pane and its associated report toolbar.

Figure 67-4 Report Manager Generated Report Pane and Toolbar



The Report List includes the following controls (illustration call-outs cited):

- **Report toolbar (1)**—The top of the generated report pane is a row of controls for generating and manipulating reports. The controls have the following functions:
  - Generate Report button—Generates a report based on the criteria defined in the report settings (in the upper pane). For more information, see Opening and Generating Reports, page 67-18.
  - Print button—Prints the generated report. For more information, see Printing Reports, page 67-23.
  - Export button—Exports the report. Click the down arrow in the button and select the type of file you want to create: **As PDF** (for Adobe Acrobat) or **As CSV** (for comma-separated values). For more information, see Exporting Reports, page 67-23.
  - Chart Type—Determines the type of graphical chart displayed in the upper part of the report, typically pie, bar, and XY (linear) graphs are available. In some cases, you do not have a choice of chart types. For more information, see Opening and Generating Reports, page 67-18.
- **Graphical view (2, 3, 5)**—The top part of the generated report shows a graphical, color-coded view of the report data, and includes a legend that explains the colors. Also included is the date and time the report was generated.

  At the bottom of the graphical view are the following controls:
  - Up and Down arrows (5)—These icon buttons, to the left of the graphic, allow you to open and close the graphical part of the report.

  - Window size control (3)—If you hover the mouse pointer over the vertical dashes below the graphic in the center of the window, you can click and move the pointer to change the size of the graphical portion of the report. The graphic is automatically resized as you increase or decrease the size of the area. In fact, you can hover over any part of the top of the table to access this control.

- **Tabular view (4)**—The bottom part of the report is a table that presents the data collected for the report and used to produce the graphic. The columns in the table vary according to the type of report.

  You can click a heading to sort the table by the column. There are three sort orders, and clicking the column heading cycles through these orders with an arrow indicating the sort order: ascending (up arrow), descending (down arrow), and no sort (empty). You can use Ctrl+click to create a second sort order on a separate column, which has an effect only if the first sort column repeats one or more entry. Numbers indicate whether the column is the first, second, third, and so on, sort criteria.

Related Topics

- Understanding the Report Settings Pane, page 67-10
- Overview of Report Manager, page 67-6
- Understanding Report Management, page 67-1
- Working with Reports in Report Manager, page 67-18
- Viewing Report Schedules, page 67-28
- Scheduling Reports, page 67-27

Understanding the Predefined System Reports in Report Manager

Report Manager includes several predefined system reports that you can use to analyze your network. You can customize these reports to focus on specific sets of devices and time periods or to focus on other configurable parameters.

This section contains the following topics:

- Understanding Firewall Traffic Reports, page 67-13
- Understanding Firewall Summary Botnet Reports, page 67-14
- Understanding VPN Top Reports, page 67-15
- Understanding General VPN Reports, page 67-16
- Understanding IPS Top Reports, page 67-16
- Understanding General IPS Reports, page 67-17

Understanding Firewall Traffic Reports

Report Manager includes predefined system reports that you can use to identify the top destinations, services, and sources for firewall ACL events. The statistics are based on the events collected by the Event Manager service (as displayed in Event Viewer).

The following reports are available in the **System Reports > FW** folder.

- **Top Destinations**—This report ranks the session destinations of all built/deny firewall events received by Security Manager. The report shows the destination IP address, the count of the number of events for each address, and the percentage of the count compared to the sum of all counts in the report.
- **Top Sources**—This report ranks the session sources of all built/deny firewall events received by Security Manager. The report shows the source IP address, the count of the number of events for each address, and the percentage of the count compared to the sum of all counts in the report.
- **Top Services**—This report ranks the destination services of all built/deny firewall events received by Security Manager. TCP and UDP services include the port number. The report shows the service, the count of the number of events for each service, and the percentage of the count compared to the sum of all counts in the report.

The parameters used to define the number of addresses or services to included in the report and the reporting time period are defined in the system defaults as described in Configuring Default Settings for Reports, page 67-24.

You can also edit the report settings and create custom versions of the reports. You can narrow the reports to focus on specific sets of source or destination addresses or services, or on just permit or deny actions, or limit the report to focus on a sub-set of firewall devices, as described in the following topics:

- Editing Report Settings, page 67-21
- Creating Custom Reports, page 67-20

Understanding Firewall Summary Botnet Reports

Report Manager includes predefined system reports that you can use to analyze botnet traffic filtering. The statistics are based on the botnet events collected by the Event Manager service (as displayed in Event Viewer) for blacklisted and gray-listed sites.

For more information about botnet, see Chapter 19, “Managing Firewall Botnet Traffic Filter Rules”.

The following reports are available in the **System Reports > FW > Summary Botnet** folder.

- **Top Infected Hosts**—This report ranks the top infected hosts for traffic originating from infected hosts to black- or gray-listed sites based on all botnet events received by Security Manager. The report shows the IP address of the infected host with the firewall interface name on which the event was detected in parentheses, the count of the number of connections logged to blacklisted or gray-listed sites for each address, the count of the number of connections that were blocked (dropped) by botnet traffic filtering, and the percentage of the count compared to the sum of all counts in the report.
- **Top Malware Ports**—This report ranks the top destination ports for traffic originating from infected hosts to black or gray-listed sites based on all botnet events received by Security Manager. The report shows the destination malware port, the count of the number of connections logged to blacklisted or gray-listed sites for each port, the count of the number of connections that were blocked (dropped) by botnet traffic filtering, and the percentage of the count compared to the sum of all counts in the report.
- **Top Malware Sites**—This report ranks the top botnet sites (black or gray-listed sites) for all inbound and outbound sessions based on all botnet events received by Security Manager. The report shows the following information:
  - IP Address—The IP address that is indicated as the malicious host in botnet events, either on the black list or the grey list.

- Malware Site—The domain name or IP address in the dynamic filter database to which the traffic was initiated.
- List Type—Whether the site is on the black list or the grey list.
- Connections Logged—The count of the number of connections logged or monitored for each site.
- Connections Blocked—The count of the number of connections that were blocked (dropped) by botnet traffic filtering for each site.
- Threat Level—The botnet threat level for the site, from very low to very high, or none.
- Category—The category of threat the site poses as defined in the botnet database, such as botnet, Trojan, spyware, and so on.

The parameters used to define the number of hosts, ports, or sites in the report and the reporting time period are defined in the system defaults as described in Configuring Default Settings for Reports, page 67-24. You can also edit the report settings and create custom versions of the reports, as described in the following topics:

- Editing Report Settings, page 67-21
- Creating Custom Reports, page 67-20

Understanding VPN Top Reports

Report Manager includes predefined system reports that you can use to identify the top remote access VPN users based on bandwidth usage, duration of connection to your network, and data throughput. Separate reports are provided based on the type of connection made by the user.

These reports are available in the **System Reports > VPN** folder in the **AnyConnect (SSL) Remote Access VPN**, **Cisco VPN Client (IPsec) Remote Access VPN**, and **Clientless SSL VPN**.

The following reports are available in each folder. Each report is specific to the connection type indicated by the folder name and also included in parentheses in the report name.

- **Top Bandwidth Users**—This report ranks the VPN users who consumed the most bandwidth. The report shows the usernames, the bandwidth in total number of bytes sent and received, and the percentage of reported bandwidth used by each user.
- **Top Duration Users**—This report ranks the VPN users who remained connected to the network for the longest time. The report shows the usernames, the connection duration time in *days hours:minutes:seconds* format, and the percentage of the reported duration by each user. The chart shows duration in seconds.
- **Top Throughput Users**—This report ranks the VPN users who sent and received data at the highest throughput rate. The report shows the usernames, the throughput for each user in kbps, and the percentage of reported throughput by each user. The throughput is calculated as 8.0*(bandwidth of the user in bytes)/(duration for which the user is connected in seconds*1000.0).

The parameters used to define the number of users included in the report and the reporting time period are defined in the system defaults as described in Configuring Default Settings for Reports, page 67-24. You can also edit the report settings and create custom versions of the reports, including focusing on specific users, as described in the following topics:

- Editing Report Settings, page 67-21
- Creating Custom Reports, page 67-20

Understanding General VPN Reports

Report Manager includes predefined system reports that you can use to analyze general remote access VPN usage in your network. These reports are not specific to the connection types used in the VPN.

The following reports are available in the **System Reports > VPN** folder.

- **User Report**—This report provides a summary of the bandwidth utilization, connection duration and throughput usage for each remote access VPN user. The report shows the usernames, the bandwidth in total number of bytes sent and received, the connection duration time in *days hours:minutes:seconds* format, and the throughput for each user in kbps. The throughput is calculated as 8.0*(bandwidth of the user in bytes)/(duration for which the user is connected in seconds*1000.0).

  Each username appears on a single row, even if the user connected to the VPN uses more than one type of connection. When a user uses more than one type of connection, the statistics for each connection type are added together in the report.

  The default report includes information for all connection technologies and all users. You can customize the report to focus on a single technology type or one or more specific users (see Editing Report Settings, page 67-21).

- **VPN Device Usage Report**—This report provides a summary of the usage statistics for each device that hosts remote access VPN connections. The report shows the device (using the Security Manager display name), the average number of users logged into the VPN at any given time during the reported time range, the total bandwidth of all users in the VPN in bytes (sent and received), the total connection duration time in *days hours:minutes:seconds* format, and the average throughput in kbps at any given time during this report period.

  The default report includes information for all connection technologies. You can customize the report to focus on a single technology type (see Editing Report Settings, page 67-21).

The parameter used to define the reporting time period is defined in the system defaults as described in Configuring Default Settings for Reports, page 67-24. You can also edit the report settings and create custom versions of the reports, as described in the following topics:

- Editing Report Settings, page 67-21
- Creating Custom Reports, page 67-20

Understanding IPS Top Reports

Report Manager includes predefined system reports that you can use to analyze top attackers, victims, and signatures for IPS alerts in your network.

The following reports are available in the **System Reports > IPS** folder.

- **Top Attackers**—This report ranks the attacker (source) addresses that generated the highest numbers of recorded IPS alerts. The report shows the attacker IP address, the count of the number of alerts for each address, and the percentage of the count compared to the sum of all counts in the report.

  The default report includes information for all attackers, victims, and signatures for both blocked and unblocked actions. You can customize the report to focus on subsets of attackers, victims, or signatures, or limit the analysis to blocked only or unblocked only actions (see Editing Report Settings, page 67-21).

- **Top Victims**—This report ranks the victim (destination) addresses that generated the highest numbers of recorded IPS alerts. The report shows the victim address, the count of the number of alerts for each address, and the percentage of the count compared to the sum of all counts in the report.

  The default report includes information for all attackers, victims, and signatures for both blocked and unblocked actions. You can customize the report to focus on subsets of attackers, victims, or signatures, or limit the analysis to blocked only or unblocked only actions (see Editing Report Settings, page 67-21).

- **Top Signatures**—This report ranks the signatures that fired the highest numbers of alerts. The report shows the signature ID number, the name of the signature, the count of the number of alerts for each signature, and the percentage of the count compared to the sum of all counts in the report.

  The default report includes information for all attackers, victims, and signatures for both blocked and unblocked actions. You can customize the report to focus on subsets of attackers, victims, or signatures, or limit the analysis to blocked only or unblocked only actions (see Editing Report Settings, page 67-21).

- **Top Blocked/Unblocked Signatures**—This report ranks the signatures that blocked the highest numbers of attacks. The report shows the signature ID number, the name of the signature, the count of the number of alerts for each signature, and the percentage of the count compared to the sum of all counts in the report.

  The default report shows blocked actions only. However, you can customize the report to show unblocked only or a combination of blocked and unblocked actions (see Editing Report Settings, page 67-21).

  If you want to see blocked or unblocked lists that are limited to specific attacker or victim addresses, or to a subset of signatures, use the Top Signatures report instead of the Top Blocked/Unblocked Signatures report. Customize the report to show blocked only or unblocked only signatures.

- **IPS Target Analysis**—This report provides the top targets by signature and frequency of attack. The report shows the signatures that generated the alerts, the number of alerts, and the victim IP address, and is based on an aggregated view of the Top Signatures and Top Victims reports. The report contains up to ten signatures and five attackers. The information is plotted on a scatter plot, which is the only graphical representation available for the report.

The parameters used to define the number of addresses or signatures to included in the report and the reporting time period are defined in the system defaults as described in Configuring Default Settings for Reports, page 67-24. You can also edit the report settings and create custom versions of the reports, as described in the following topics:

- Editing Report Settings, page 67-21
- Creating Custom Reports, page 67-20

Understanding General IPS Reports

Report Manager includes predefined system reports that you can use to analyze general IPS activity in your network.

The following reports are available in the **System Reports > IPS** folder.

- **Inspection/Global Correlation**—This report provides a comparison of alerts generated by global correlation against alerts generated by traditional IPS inspection. The report shows the number and percentage of alerts per IPS inspection method (either Global Correlation or Inspection).

- **IPS Simulation Mode**—This report provides a comparison of alerts in inline (IPS) and promiscuous (IDS or IPS simulation) modes. The report shows the number and percentage of alerts based on mode, either Non Simulation Count (inline) or Simulation Mode Count (promiscuous). The IPS sensor cannot directly block attacks that occur in promiscuous mode.

When working with IPS events, the Report Manager component of Cisco Security Manager reports events individually; the Event Viewer component of Cisco Security Manager displays alerts. In the Event Viewer component, the IPS Summarizer groups events into a single alert, thus decreasing the number of alerts that the IPS sensor sends out.

Tip Cisco IPS Manager Express (IME) and Cisco Security Manager do not summarize events in precisely the same way.

The parameter used to define the reporting time period is defined in the system defaults as described in Configuring Default Settings for Reports, page 67-24. You can also edit the report settings and create custom versions of the reports, as described in the following topics:

- Editing Report Settings, page 67-21
- Creating Custom Reports, page 67-20

Working with Reports in Report Manager

Use the Report Manager application to view security and usage reports for devices and remote access IPsec and SSL VPNs. The following topics explain the basics of creating reports. For information on working with report schedules, see Scheduling Reports, page 67-27.

This section contains the following topics:

Opening and Generating Reports

Reports are not static. When you open a report, it contains no data, although it does contain settings that define the data that shall be used to generate the report. Thus, to view a report, you need to open it and then generate it. This procedure explains the process.

Related Topics

- Overview of Report Manager, page 67-6
- Creating Custom Reports, page 67-20
- Arranging Report Windows, page 67-25
- Troubleshooting Report Manager, page 67-31

Step 1 In Report Manager, do one of the following to open a report:

- Double-click the name of the report in the report list (in the left pane).
- Select the report in the reports list and select **File > Open**.
- Right-click a report in the reports list and select **Open Report**.

The report opens with the report settings pane open and the report content area empty.

Tip You can have five reports at most open at one time. You can also collapse the report settings pane to provide more room for viewing the generated report by clicking on any area of the settings toolbar that is not a button that performs another function.

Step 2 (Optional) Verify that the report settings contain the desired values, for example, the desired time window for the report. The settings for system reports are based on the system defaults (which you can configure as described in Configuring Default Settings for Reports, page 67-24). The settings for custom reports are those that were last saved for the report.

If you need to change the settings, click the **Edit** button in the settings toolbar and make your changes in the Edit Settings dialog box. For more information, see Editing Report Settings, page 67-21.

Tip Be sure to save your changes if you want to make them permanent. If you change the settings for a system report and you want to preserve them, you must use Save As to create a new custom report; you cannot change the settings of a system report from the default settings.

Step 3 Click the **Generate Report** button below the settings pane to retrieve the report data from the reporting database and to display the resulting information. The information is displayed in two formats:

- Graphical—A graphical representation of the data is shown in the top part of the report. You can select different types of graphics from the **Chart** menu above the report data: pie, XY (for linear graphs), and bar. If there are more than 10 items in the report (for example, you configured a Top report to show 25 values), all values after the tenth are summarized in the chart as "others."

  Some reports, such as the IPS Target Analysis report, use scatter plots. For these reports, you do not have the option to select a different graphic type.

- Tabular—The table below the graphic lists the data used to generate the graphic. The table has different columns based on the type of report. Following are some typical columns; for more detailed information about the content of each report, see Understanding the Predefined System Reports in Report Manager, page 67-13.
  - Rank—The order of the information by magnitude. For example, for a firewall top destinations report, a rank of 1 indicates that the destination is the most used in the evaluated events.
  - (Name of reported characteristic)—There is always a column whose name is based on the characteristic targeted by the report, for example, Source/Destination (IP addresses), Service (protocol and port), or User (usernames).

  - Count—The number of times the item appears in an event or related statistic.
  - Percentage—The ratio of the reported characteristic to the total sum of that characteristic in the report. The ratio includes only those numbers included in a report, so for example, you could get a different percentage for the same item in a top 10 verses a top 25 report.

Step 4 (Optional) If desired, you can print the report or export it to a PDF or comma-separated values (CSV) file.

- To print the report, click the **Print** button and select your printer. For more information, see Printing Reports, page 67-23.
- To export the report, click the **Export** button and select the file type, PDF or CSV. For more information, see Exporting Reports, page 67-23.

Tip The report data is not preserved when you close the report. If you want to keep the displayed information, you must print or export the report.

Creating Custom Reports

You can create custom reports to target specific characteristics that require regular analysis or presentation. For example, you might want to create separate Top Destination firewall reports for different groups of firewall devices so that you can separately analyze activity in separate physical sites. You can also use custom reports to analyze sources, destinations, or services that otherwise do not make it into the top reports.

Tip It might take up to one hour for data to be available for a newly-created custom report. If you get the message that no records are found after creating the report, wait an hour and then ensure that the time span for the report is Last 1 Hour.

Related Topics

- Opening and Generating Reports, page 67-18
- Overview of Report Manager, page 67-6

Step 1 Select the report on which you want to base your custom report in the reports list. Open it by double-clicking it, by selecting it and selecting **File > Open**, or by right-clicking and selecting **Open Report**.

Step 2 Click the **Edit** (pencil) button in the settings toolbar to open the Edit Settings dialog box.

Note Do not click the Edit button above the reports list. That edit button allows you to change the name of the report only.

The Edit Settings dialog box is divided into two panes. The left pane lists the available settings pages; the right pane shows the settings for the page selected in the left pane.

Step 3 Configure the settings so that they define the desired report parameters. For more information, see Editing Report Settings, page 67-21.

Step 4 Click the **Save As** button in the settings toolbar, or select **File > Save As**.

Step 5 Enter the name of the report and optionally a description and click **OK**.

Report names can be up to 64 characters and contain alphanumeric characters, spaces, hyphens (-), and the underscore character (_). The description can be up to 1024 characters.

Editing Report Settings

You can change the settings that define the criteria used to generate a report. For custom reports, you can save your changes.

For predefined system reports, you cannot directly save your changes. Instead, you can use Save As to create a new custom report using the updated settings. You can also change the default settings used in all predefined system reports rather than editing report settings, as described in Configuring Default Settings for Reports, page 67-24.

Related Topics

- Opening and Generating Reports, page 67-18
- Overview of Report Manager, page 67-6
- Creating Custom Reports, page 67-20
- Understanding Report Manager Data Aggregation, page 67-4
- Arranging Report Windows, page 67-25

Step 1 In Report Manager, open the report whose settings you want to change. To open the report, double-click it, select it and select **File > Open**, or right-click it and select **Open Report**.

The report opens with the settings pane open at the top of the report. The settings pane shows the type of report, the devices included in the report, the time range, a description, the schedules defined for the report, and other properties unique to the report.

Step 2 (Optional) Change the Description by typing into the Description edit box in the report settings pane.

Step 3 Click the **Edit** (pencil) button in the settings toolbar to open the Edit Settings dialog box.

Note Do not click the Edit button above the reports list. That edit button allows you to change the name of the report only.

The Edit Settings dialog box is divided into two panes. The left pane lists the available settings pages; the right pane shows the settings for the page selected in the left pane.

Step 4 Edit the settings on the desired pages as follows:

- **Devices**—To change which monitored devices are included in the report. The default is **All Devices**.

  If you want the report to reflect a subset of monitored devices, select **Filter Devices** and then select the desired devices from the list. If a device is in italics, it means that the device is not currently selected for monitoring in Event Viewer; you can select these devices, and the report will include data for the device if it was monitored during the selected time period. You can select a folder to select all the devices in the folder.

The device list is pre-filtered to show devices of the appropriate type only. For example, if you are editing the settings for a firewall report, IPS devices do not appear in the list of selectable devices.

- **Time**—To change the time span used to select events and data to include in the report. The time is based on the Security Manager server time. You can select one of the following options to define the time span:
  - Last 1 Hour—The last full one hour on the zeros, for example, if the current time is 11:45 AM, the Last 1 Hour report shows data from 10:00 to 11:00.
  - Last 1 Day—The last full day, from midnight to midnight. For example, if the current day is Tuesday, the Last 1 Day report shows data from Monday.
  - Last 1 Week—The previous Monday through Sunday.
  - Last 1 Month—The previous month. For example, if the current date is September 29, the Last 1 Month report shows data from August.
  - Custom—Use the Start Date and End Date calendars to select the desired starting and ending times for the report. Click the down arrow, select the desired day and time, then click OK in the calendar widget. Reportable data is kept for 90 days, so you cannot select a date more than 90 days into the past. Additionally, you cannot specify a time if you select a start date more than five days into the past. If you select the current date for the start date, you can also specify minutes for both starting and ending dates, but because report data is aggregated every 15 minutes at 00, 15, 30, and 45 minutes past each hour, minute entries are rounded to the nearest of these figures. The allowed time selection is based on how data is aggregated, as explained in Understanding Report Manager Data Aggregation, page 67-4.
- **Criteria**—To change the other criteria used to define the report. The attributes available on the Criteria settings page are variable. In some cases, there are no selectable criteria. Following is a list of the possible criteria:
  - Top (All "Top" reports.)—The number of items targeted by the report to include. For example, the Top 10 firewall destinations returns the 10 most frequent destinations for firewall events in the configured time range. Select 10, 20, 25, or 50.
  - Service (Firewall reports except Botnet)—The services to include in the report. To specify services, click the Edit button next to the field and select the desired service policy objects. You can select multiple objects.
  - Source IP, Destination IP (Firewall reports except Botnet)—The source and destination IP address fields are separate, but they are functionally the same. They define the IP addresses for sources or destinations to include in the report. You can enter individual addresses, such as 10.100.10.10, or address ranges, such as 10.100.10.10-10.100.10.20. Both IPv4 and IPv6 addresses are accepted. Separate multiple addresses with commas.

    You can click the Edit button next to the field to open a dialog box where you can more easily create complex lists of addresses and address ranges. However, you cannot use network/host objects to define addresses.

    Note Do not specify values for all of the Service, Source IP, and Destination IP criteria in a single report. You can specify the criteria on which the report is based (for example, Service for the Top Services report) plus one other criteria. If you specify all three values, the report will always contain no data.
  - Permit/Deny (Firewall reports except Botnet)—The action reflected in the event, either permitting the matching traffic (Permit), denying the matching traffic (Deny), or either (All). The default is All.

- Signature ID (IPS top attackers, top signatures, top victims)—The signatures to include in the report. To specify signatures, click the Edit button next to the field and select the desired signatures. You can select a folder to select all signatures in the folder.

  Note In the predefined system reports, you cannot specify values for all three of the Signature ID, Attacker IP, and Victim IP criteria. You can specify a value for the key attribute of the report (for example, Victim IP for the top victims report) plus one of the other values. If you want to configure values for all three criteria, you must create a custom report.

- Attacker IP, Victim IP (IPS top attackers, top signatures, top victims)—The attacker and victim IP address fields are separate, but they are functionally the same. They define the IP addresses for attackers (sources) or victims (destinations) to include in the report. You can enter individual addresses, such as 10.100.10.10, or address ranges, such as 10.100.10.10-10.100.10.20. Both IPv4 and IPv6 addresses are accepted. Separate multiple addresses with commas.

  You can click the Edit button next to the field to open a dialog box where you can more easily create complex lists of addresses and address ranges. However, you cannot use network/host objects to define addresses.

- Blocked (IPS top attackers, top blocked/unblocked signatures, top signatures, top victims)—Whether the event resulted in dropped traffic (Blocked), traffic that was not dropped (Unblocked), or either (All).

- Username (VPN user report)—The names of the users to include in the report. The default, an empty list, includes all users. If you want the report to focus on specific users, use the Add (+), Edit (pencil), and Delete (trash can) buttons beneath the table to create the desired list of users.

- Technology (VPN device usage report)—The type of remote access technology to include in the report: All, Clientless (SSL VPN), Full Client (SSL VPN), IPsec RA (IPsec remote access VPN).

Step 5 Click **OK** in the Edit Settings dialog box to implement your changes.

You can now click the Generate Report button to retrieve the data defined by the settings and display it in the report. You can also use Save or Save As to permanently save the changes to the settings.

Printing Reports

After you generate a report as described in Opening and Generating Reports, page 67-18, you can print it.

To print the report, click the **Print** button above the report. You are prompted to select a printer.

Exporting Reports

After you generate a report as described in Opening and Generating Reports, page 67-18, you can export it to an Adobe Acrobat (PDF) or comma-separated values (CSV) file.

Exported files include the following information:

- The creation time of the report.
- The settings used to generate the report.

- (PDF only.) The graphical representation of the report data.
- The tabular report data. In PDFs, the information is represented as a table. In CSVs, the information is comma-separated, with the first row being the column headings.

To export the report, click the down arrow in the **Export** button above the report and select either **As PDF** or **As CSV**. You are prompted to select a folder for the report. A default file name is provided, but you can change the file name.

Configuring Default Settings for Reports

You can control the default settings that Report Manager uses for System reports. When you change the defaults, you automatically change the settings for all System reports, but the changes do not apply to any reports you saved as custom reports (in the My Reports folder). You must have system administrator or network administrator privileges to change these settings.

While viewing a report, you can edit any system report to specify different values for these settings, either to use temporarily while viewing the report, or to save as a custom report in the My Reports folder.

Tip If you change the settings in a system report, you can return the report to the default settings by clicking the **Reset** button in the Report Settings toolbar.

Step 1 In Report Manager, select **Tools > Default Report Settings** to open the Default Report Settings dialog box.

Step 2 Configure any of the following options:

- **Top**—The number of results listed in any of the "Top" reports, which list the most-often occurring items of the type targeted by the report. For example, if you select 20, the firewall Top Destinations report shows the 20 most often occurring traffic destinations in events reported to Security Manager. The default is 10.

  If you select more than 10, all items after the tenth are summarized as "others" in charts, although the detailed information for each additional item is listed in the report table.

- **Time Range**—The time window for events included in the report:
  - Last 1 Hour—The last full one hour on the zeros, for example, if the current time is 11:45 AM, the Last 1 Hour report shows data from 10:00 to 11:00.
  - Last 1 Day—The last full day, from midnight to midnight. For example, if the current day is Tuesday, the Last 1 Day report shows data from Monday.
  - Last 1 Week—The previous Monday through Sunday.
  - Last 1 Month—The previous month. For example, if the current date is September 29, the Last 1 Month report shows data from August.

  For more information on the implications of the time range setting, see Understanding Report Manager Data Aggregation, page 67-4.

- **Default Email Address**—The email address used as the default destination for scheduled reports.

If you decide you want to return to the installation default values, click **Restore Defaults**.

Step 3 Click **Apply** to save your changes, then click **Close** to close the dialog box.

Arranging Report Windows

You can open up to five report windows at one time. Reports are opened as tabbed windows in the right pane of the main Report Manager window, in the most recently used area ("tabbed group") if there is more than one area. The commands to arrange the windows appear if you right-click the tab for the report window as shown in the following illustration.

You have many options for arranging report windows based on your requirements. For example, you might want to compare two reports side-by-side, or remove a report from the main window without closing it.

You can use the following techniques to arrange the report windows to get the view that you desire:

- Floating a report—To remove a report from the main Report Manager window without closing it, right-click the report tab and select **Floating**. The report is moved to its own window.

  If you have already floated a report, you can select **Floating to** and choose one of the already-floated windows. The report becomes a new tab in that window.

- Docking a report—To move a floating report back to the main Report Manager window, right-click the report tab and select **Docking**.

- Arranging reports horizontally or vertically for side-to-side comparison—To create a vertical or horizontal arrangement of reports to allow for easy comparison, without floating the reports, right-click the report tab and select **New Horizontal Group** or **New Vertical Group**. These commands split the current tabbed group into the selected layout. You must have at least two reports open to use these commands. If you have more than two open reports, and you want all of them in separate windows, you need to use the command multiple times.

- Move reports to different tabbed groups—If you have several open reports, and you have arranged them into horizontal or vertical groups, you can move reports among the groups by right-clicking the report tab and selecting **Move to Next Tab Group** or **Move to Previous Tab Group**. The commands appear only if reports are arranged in a manner where such movement is possible:

- Change the orientation of groups—You can switch between horizontal and vertical layouts by right-clicking the report tab and selecting **Change Tab Groups Orientation**.

Saving Reports

If you edit the settings for a report, you must save it to make those changes permanent. However, to save changes to predefined system reports, you must save the report as a custom report.

Tip When you save a report, you are saving the settings that define the report. You are not saving the generated content of the report. If you want to save the generated content of the report, that is, the graphs and the report data, you must export the report rather than save it.

- To save changes to a custom report, do one of the following in Report Manager:
  - Select **File > Save** from the menu bar.
  - Click the **Save** button in the Report Settings toolbar.
- To save your changes as a new custom report, do one of the following to open the Save Report As dialog box:
  - Select **File > Save As** from the menu bar.
  - Click the **Save As** button in the Report Settings toolbar.
  - Right-click the report in the reports list and select **Save As**.

  Then, enter a name for the report and optionally a description of the report and click **OK**. The report is added to the My Reports folder in the reports list.

Note Report names can be up to 64 characters and contain alphanumeric characters, spaces, hyphens (-), and the underscore character (_). The description can be up to 1024 characters.

Renaming Reports

You can change the name of custom reports, but you cannot change the names of predefined system reports.

Related Topics

- Overview of Report Manager, page 67-6
- Understanding the Report List in Report Manager, page 67-9

Step 1 In Report Manager, select the report whose name you want to change from the reports list. You do not need to open the report; simply select it in the list.

Step 2 Click the **Edit** (pencil) button above the reports list to open the dialog box that allows you to change the report name.

Step 3 Enter the new name and click **OK**.

Report names can be up to 64 characters and contain alphanumeric characters, spaces, hyphens (-), and the underscore character (_).

Closing Report Windows

You can close any report by clicking the X icon on the report tab. For reports that you have floated, you can simply click the X icon in the window's title bar.

Tip When you close a report, none of the generated report data is preserved. If you want to preserve the generated data, you must print it or export it before you close the report window.

You can also use the following techniques to close the report windows without exiting Report Manager:

- Close a report—Select **File > Close Report** to close the currently-viewed report, or right-click the desired report tab and select **Close**.
- Close all reports—Select **File > Close All Reports**, or right-click any report tab and select **Close All**.
- Close all reports except one—Right-click the report tab of the report you want to keep open and select **Close Others**.

Deleting Reports

You can delete custom reports, but you cannot delete predefined system reports.

To delete a custom report, select it in the reports list and click the **Delete** (trash can) button above the reports list. You are asked to confirm your deletion.

Tip Deleting a report also deletes any schedules for that report.

If you need to delete another user's custom report, see Managing Custom Reports, page 67-27.

Managing Custom Reports

If you have system administrator or network administrator privileges, you can view a list of custom reports created by all Report Manager users on this Security Manager server.

To view the list of custom reports, select **Tools > Custom Report List** to open the Manage Custom Reports dialog box. The list shows the report name, the type of report, the type of device analyzed by the report, and the username of the person who created the custom report.

You can use the following controls to manage custom reports from this page:

- **Pagination controls**—If there are a lot of custom reports, use the pagination controls to move through the list. You can click the buttons to move to the first page, previous page, next page, or last page, or type the page number into the Page X of Y edit box. You can also click the down arrow in the edit box to change the edit box to work by record number rather than page number.
- **Delete button**—Click this button to delete the selected report. Any schedules (and schedule results) that use the report are also deleted.
- **Refresh button**—Click this button to update the list with the latest information.

Scheduling Reports

You can create schedules to regularly generate reports from Report Manager.

This section contains the following topics:

Viewing Report Schedules

You can view a list of report schedules that are configured in Report Manager. If you have system administrator or network administrator privileges, the list includes all schedules configured on the server, whether you configured them or another user configured them. Users with lesser privileges can see their own schedules only.

To view the list of report schedules, select the **Scheduled Reports** tab, and if necessary, the **Schedule List** sub-tab. The list shows the schedule name, description, the report that will be generated by the schedule, the frequency of report generation, the e-mail addresses to which reports are sent (if any), whether the schedule is enabled or disabled, and the username of the person who created the schedule.

You can use the following controls to manage report schedules from this page:

- **Pagination controls**—If there are a lot of schedules, use the pagination controls (below the table to the left) to move through the list. You can click the buttons to move to the first page, previous page, next page, or last page, or type the page number into the Page X of Y edit box. You can also click the down arrow in the edit box to change the edit box to work by record number rather than page number.
- **Add button**—Click this button to add a new schedule. For more information, see Configuring Report Schedules, page 67-28.
- **Edit button**—Click this button to edit the selected schedule. For more information, see Configuring Report Schedules, page 67-28.
- **Delete button**—Click this button to delete the selected schedule. For more information, see Deleting Report Schedules, page 67-31.
- **Refresh button**—Click this button to update the list with the latest information.
- **Enable button**—Click this button to enable the selected schedule. The button is active only if the selected schedule is disabled. For more information, see Enabling and Disabling Report Schedules, page 67-30.
- **Disable button**—Click this button to disable the selected schedule. The button is active only if the selected schedule is disabled. For more information, see Enabling and Disabling Report Schedules, page 67-30.

Configuring Report Schedules

You can create schedules to automatically generate reports at set times. The generated reports are e-mailed to identified recipients and are also stored and available for viewing from Report Manager. By scheduling reports, you can easily and efficiently create regular milestone views of network security and usage. This procedure explains how to set up a schedule for a report.

Related Topics

- Overview of Report Manager, page 67-6
- Opening and Generating Reports, page 67-18
- Viewing Report Schedules, page 67-28
- Troubleshooting Report Manager, page 67-31

Step 1 In Report Manager, do one of the following:

- On the Reports tab, open the report for which you are creating a new schedule by double-clicking the name of the report in the report list (in the left pane). Then, click the **Create Schedule** button in the report settings toolbar.

  Note You cannot edit an existing schedule from the Reports tab.

- On the Reports tab, right-click the report on which you are creating a schedule and select **Create Schedule**. If the report is not already open, it is opened.
- On the Scheduled Reports tab, Schedule List sub-tab, click the **Add** button below the list of schedules to create a new schedule. To edit an existing schedule, select it in the list and click the **Edit** button.

The Add or Edit Report Schedule dialog box opens.

Step 2 Configure the following options in the dialog box:

- **Schedule Name**—A name for the schedule, up to 64 characters.
- **Report Name**—Select the name of the report to be generated by the schedule. When you create a schedule from the report settings pane, the name is pre-selected and you cannot change it.
- **Schedule**—Select whether the report shall be generated daily, weekly (once per week), or monthly (once per month). Then, enter the day and time for generating the report:
  - Daily schedules—Select whether the schedule is for Monday through Friday (five days) or Monday through Sunday (all seven days). Enter the time of day (in 24-hour notation) to generate the report.
  - Weekly schedules—Select the day of the week and enter the time of day in 24-hour notation.
  - Monthly schedules—Select whether to generate the report on the first day of the month, the last day, or custom. If you select Custom, enter the day number. Then, enter the time of day in 24-hour notation.
- **Email To**—The email addresses that should be sent the report. Separate multiple addresses with commas. If you do not want reports e-mailed, ensure that the field is empty. Note that for e-mails to be sent successfully, you must configure SMTP on the Security Manager server as described in Configuring an SMTP Server and Default Addresses for E-Mail Notifications, page 1-25.

  If the report fails to generate for some reason, notification of the failure is sent to these e-mail addresses.
- **Export Report Format**—Whether to generate the report in Adobe Acrobat (PDF) or comma-separated value (CSV) format. The PDF includes graphics, the CSV does not. For more information on export formats, see Exporting Reports, page 67-23.
- **Description**—A description of the schedule.
- **Status**—Whether the schedule is enabled (reports will be generated) or disabled (reports will not be generated).

Step 3 Click **OK** to save the schedule. New schedules are added to the schedules list on the Schedules tab.

Viewing Scheduled Report Results

Typically, report schedules include e-mail addresses to which generated reports are sent. You can also view reports generated from schedules in Report Manager. If you have system administrator or network administrator privileges, you can view results generated by other users' schedules.

Tip Report Manager maintains a copy of the last report generated by the schedule. You cannot retrieve previously generated reports.

Related Topics

- Overview of Report Manager, page 67-6
- Opening and Generating Reports, page 67-18
- Viewing Report Schedules, page 67-28
- Troubleshooting Report Manager, page 67-31

Step 1 In Report Manager, select the **Scheduled Reports** tab.

Step 2 Select the **Results** sub-tab.

All results that you are authorized to see are listed on this tab. The list shows the schedule name, the name of the report that was generated, the frequency of report generation, the date and time of the last schedule run (when the report was generated), the status of the report generation (Success or Failed), a link to the generated report (in the Last Report column), and the username of the person who created the schedule.

Tip If the status of a report is Failed, click the link to see the reason for failure.

Step 3 Double-click the icon link to the report in the Last Report column to open it. While viewing the report, you can save it to your workstation.

If you cannot find the report you are looking for, click the **Refresh** button to update the list with the latest information.

Enabling and Disabling Report Schedules

You can enable or disable report schedules to change whether reports are generated based on the schedules. By disabling a schedule, you can prevent reports from being generated without deleting the schedule. If you have system administrator or network administrator privileges, you can enable or disable another user's schedule.

Related Topics

- Overview of Report Manager, page 67-6

- Viewing Report Schedules, page 67-28

Step 1 In Report Manager, select the **Scheduled Reports** tab, then if necessary, the **Schedule List** sub-tab. This tab lists all currently-defined schedules that you are authorized to see.

Step 2 Select the schedule whose status you want to change and click either the **Enable** or **Disable** button.

Deleting Report Schedules

You can delete report schedules if you no longer need them. If you have system administrator or network administrator privileges, you can delete another user's schedule.

Tip If you do not want to generate reports from a schedule, but you want to keep the schedule definition, you can disable the schedule. Disabled schedules do not generate reports.

Step 1 In Report Manager, select the Scheduled Reports tab, then if necessary, the Schedule List sub-tab. This tab lists all currently-defined schedules that you are authorized to see.

Step 2 Select the schedule and click the **Delete** button below the list. You are asked to confirm the deletion.

When you delete a schedule, any results of the schedule are also deleted from the server and they are removed from the Results tab.

Troubleshooting Report Manager

Following are some problems you might encounter when using the Report Manager application, and some ways to resolve the problems.

Problem: Report Manager does not open, you get the message "Not able to connect to server."

Solution: Report Manager requires that the csmReportServer, rptDbEngine, and rptDbMonitor processes be started. Report Manager also relies on the Event Management service VmsEventServer. Ensure that all services are started and running correctly on the Security Manager server.

To view the current state of the processes, log into the Security Manager web interface using http://*SecManServer*:1741, where *SecManServer* is the DNS name of the server. From the Security Management Suite home page, click the **Server Administration** link to open CiscoWorks Common Services at the Admin page. Click **Processes** in the TOC on the left side of the window to open the list of processes that displays their current states. Select these processes and click **Start** to start them. If necessary, you might want to stop them, and then restart them. Wait for the processes to fully restart, then try again to open Report Manager.

Problem: When generating a report, you get the message "No records found."

Solution: This message indicates that there were no event records in the event data storage location that relate to the report type and the configured settings, or that the required Report Manager aggregation cycle has not completed. Investigate the following:

- Ensure that devices of the appropriate type are selected for monitoring as described in Selecting Devices to Monitor, page 66-31.

- Ensure that these devices are appropriately configured for sending events to Security Manager, and that events from the device appear in Event Viewer. Ensure that the device and Security Manager are using the same syslog port. For information on configuring the devices, see Configuring ASA and FWSM Devices for Event Management, page 66-25 and Configuring IPS Devices for Event Management, page 66-26. To check the syslog port that Security Manager is using, view the setting on the **Tools > Security Manager Administration > Event Management** page in Configuration Manager.
- For IPS devices, ensure that the certificate has not expired. Check the certificates table by selecting **Manage > IPS > IPS Certificates** in Configuration Manager and regenerate the certificate if necessary.
- The report settings might specify a time period in which no aggregated data exists for the report. Data is aggregated every 15 minutes, 1 hour (on the hour), and 1 day (at midnight). Try changing the time parameters of the report. See Editing Report Settings, page 67-21. Consider the following:
  - To see a Last 1 Hour report, a change of hour must occur since initially starting the Event Manager service. For example, if you start the service at 10:05, hourly reports are available only after 11:00.
  - To see a Last 1 Day report, a change of day must occur since initially starting the Event Manager service. For example, if you start the service at 10:05, you must wait until after midnight to see a daily report.
  - To see a Last 1 Week report, at least one full day cycle must occur. Weekly reports are based on daily reports.
  - To see a Last 1 Month report, at least one full month must pass since starting the service.
  - To see a custom time period report, at least one daily cycle must occur.
- If you create a new custom report, it might take up to one hour for data to become available. Also, ensure that the time period is Last 1 Hour until the report is old enough to have data for other time periods.

Problem: You cannot get reports for a specific device.

Solution: Investigate the following:

- The device must have been selected for event management during the reporting time-frame as described in Selecting Devices to Monitor, page 66-31. Even if a device is selected, Report Manager might not support all devices that are supported for Event Viewer. For information on the supported device types, see Understanding Report Management, page 67-1.
- The report settings might exclude the device. Unless the report settings indicate that All Devices are considered in the report, check the device selection to ensure the device is included. See Editing Report Settings, page 67-21.
- The report settings might specify a time period in which no data exists for the device. Try changing the time parameters of the report. See Editing Report Settings, page 67-21.
- If your organization uses Cisco Secure ACS to control access to the application, you can view reports on a device only if you have at least View privileges to the device. Check whether you have the required permissions.

Problem: You cannot see data in certain IPS predefined reports after specifying values for each of signature, victim IP, and attacker IP.

Solution: The top attackers, top victims, and top signatures predefined reports include criteria for signature, victim IP address, and attacker IP address. However, you cannot configure all three criteria in a predefined report. Instead, you can configure the criteria on which the report is based (for example, victim IP address for the top victims report) plus one, and only one, of the remaining values. Note that this limitation does not apply to the other criteria, such as Blocked and Top.

Problem: You cannot see data in certain Firewall predefined reports after specifying values for each of service, source IP, and destination IP.

Solution: The top destinations, top services, and top sources predefined reports include criteria for service, source IP address, and destination IP address. However, you cannot configure all three criteria in a predefined report. Instead, you can configure the criteria on which the report is based (for example, service for the top services report) plus one, and only one, of the remaining values. Note that this limitation does not apply to the other criteria, such as Permit/Deny and Top.

Problem: Statistics for VPN reports are not available.

Solution: VPN statistics are partially obtained directly from the device rather than from events stored in the event data storage location. To obtain the statistics, Report Manager must be able to log into the device and use show commands. Ensure that the device properties for your VPN devices have the correct credentials for logging in.

Problem: Scheduled reports are not getting sent to recipients.

Solution: Ensure that the SMTP server is configured correctly and that a valid source e-mail address is configured for Security Manager. For more information, see Configuring an SMTP Server and Default Addresses for E-Mail Notifications, page 1-25.