CHAPTER 10

# Using Trend Reports

**Note** To learn about supported services and platforms, see Supported Services and Platforms for Monitoring and Reports, page 1-5.

The following topics describe the reporting features available in Performance Monitor and explain how to use and save the historical trend reports that you generate.



## Understanding Reporting Options

You can configure and generate reports for all supported service types. Reports are organized in four broad categories and more than 30 narrow subcategories.

**Note** Only RAS VPN and site-to-site VPN services support all four of the high-level report categories. Subcategories are service-specific in most cases.

A subcategory measures trends over time for one narrow condition on a validated device or in a supported service. Subcategories are specific to categories; for example, subcategories in the Failure category are specific kinds of failures. The number of subcategories that you can select for a report ranges from one to four, depending on the subcategories you select.

The report categories are:

| Category Name | Reference |
|---|---|
| **Failure** | See Understanding Failure Report Subcategories, page 10-2. |
| **Performance** | See Understanding Performance Report Subcategories, page 10-3. |
| **Throughput** | See Understanding Throughput Report Subcategories, page 10-4. |
| **Usage** | See Understanding Usage Report Subcategories, page 10-5. |

# Understanding Failure Report Subcategories

Each generated line graph in a Failure report displays results for one device or service module or virtual server, depending on the service type and subcategory you select—as described in Table 10-1, which:

- Lists all subcategories for configuring Failure reports.
- Specifies which services support the subcategories.
- Describes the graphs displayed in Failure reports.

**Note** When you run historical reports, you might see a dip in the graph for any period of time during which the MCP process did not run on your CiscoWorks Server. See MCP Process Maintenance, page 3-16.

*Table 10-1 Failure Report Configuration Subcategories*

| Failure Report Subcategory | Relevant Services | Description |
|---|---|---|
| **Note** In all Failure report graphs, the horizontal axis represents time. The vertical axis represents either a percentile or a count, depending on the report. | | |
| % of Inbound Conn Failures | Remote Access VPN | Graph shows the trend of failed inbound connections over time as a percentage of all inbound connections for all remote access VPN devices. |
| % of Phase 1 Conn Failures | Remote Access VPN | Graph shows the trend of failed Phase-1 (IKE) connections over time as a percentage of all Phase-1 connections. |
| % of Phase 2 Conn Failures | Remote Access VPN | Graph shows the trend of failed Phase-2 (IPSec) connections over time as a percentage of all Phase-2 connections. |
| % Of Conns Dropped By All Virtual Servers | Load Balancing | Graph shows the trend of dropped virtual server connections over time as a percentage of all connections. |
| % Of Failed Conns Per Module | Load Balancing | Graph shows the trend of failed load-balancing connections over time as a percentage of all CSM service module connections. |
| % Of Inbound Conn Failures | Site-to-Site VPN | Graph shows the trend of failed inbound Phase-1 (IKE) and Phase-2 (IPSec) tunnels over time as a percentage of all inbound exchanges. |
| % Of Outbound Conn Failures | Site-to-Site VPN | Graph shows the trend of failed outbound Phase-1 (IKE) and Phase-2 (IPSec) tunnels over time as a percentage of all outbound exchanges. |
| % of Total Conn Failures | Site-to-Site VPN | Graph shows the trend of failed Phase-1 (IKE) and Phase-2 (IPSec) connections over time as a percentage of all inbound and outbound exchanges. |
| **Note** Trend reports are not usually useful when they are based on a small number of data points. The date range and trending type determine the number of data points. For example, there is only one data point if you apply the Daily trending type to less than 2 days' worth of data. It is not possible to graph a trend from only one data point. | | |

# Understanding Performance Report Subcategories

Each generated line graph in a Performance report displays results for one device or service module or virtual server, depending on the service type and subcategory you select—as described in Table 10-2, which:

- Lists all subcategories for configuring Performance reports.
- Specifies which services support the subcategories.
- Describes the graphs displayed in Performance reports.

**Note** When you run historical reports, you might see a dip in the graph for any period of time during which the MCP process did not run on your CiscoWorks Server. See MCP Process Maintenance, page 3-16.

*Table 10-2 Performance Report Configuration Subcategories*

| Performance Report Subcategory | Relevant Services | Description |
|---|---|---|
| **Note** In all Performance report graphs, the horizontal axis represents time. The vertical axis represents either a percentile value or a count, depending on the report. | | |
| Bandwidth Usage | Remote Access VPN | Graph shows trends for the average percentage of total bandwidth capacity used over time, calculated as the sum of inbound and outbound packets, factored against the interface speed. |
| CPU Usage | • Firewall<br>• Remote Access VPN<br>• Site-to-Site VPN<br>• SSL | Graph shows trends for the average percentage of total CPU capacity used over time. |
| CPU Usage Rev | Site-to-Site VPN | Graph shows trends for the average percentage of total CPU capacity used over time.<br>**Note** If the displayed report is empty when you select the CPU Usage Rev subcategory, use the CPU Usage subcategory instead. |
| FTP Fixup | Firewall | Graph shows trends for the average per-second activity and change rate over time for FTP Fixup—the PIX OS inspection function, as applied to FTP traffic. |
| HTTP Fixup | Firewall | Graph shows trends for the average per-second activity and change rate over time for HTTP Fixup—the PIX OS inspection function, as applied to HTTP traffic. |
| Memory Usage | • Firewall<br>• Site-to-Site VPN<br>• SSL | Graph shows trends for the average percentage of processor memory capacity used over time. |
| SSL Connections | SSL | Graph shows trends for the total number of active SSL connections over time. |
| TCP Fixup | Firewall | Graph shows trends for the average per-second activity and change rate over time for TCP Fixup—the PIX OS inspection function, as applied to TCP traffic. |

*Table 10-2 Performance Report Configuration Subcategories (continued)*

| Performance Report Subcategory | Relevant Services | Description |
|---|---|---|
| TCP Intercept | Firewall | Graph shows trends for the average per-second activity and change rate over time for TCP Intercept—a PIX OS feature that prevents denial-of-service (DOS) attacks against TCP servers. |
| Throughput | SSL | Graph shows trends for the sum in kbps of inbound and outbound octets through all public interfaces over time, factored against interface speed. |
| Total IfErrors | Firewall | Graph shows trends for the number of firewall interface errors over time. |
| Total Throughput | Firewall | Graph shows trends for the sum in kbps of inbound and outbound octets through all public interfaces over time, factored against interface speed. |
| URL Access | Firewall | Graph shows trends for the average number over time of URLs (web sites) accessed per second, based on the output of the PIX OS **show perfmon** command. |
| URL Request | Firewall | Graph shows trends for the average number over time of URLs (web sites) requested per second, based on the output of the PIX OS **show perfmon** command. |
| Xlates | Firewall | Graph shows trends for the average number over time of TCP and UDP NAT translations per second through the firewall.<br>**Note** A translation is a mapping of an internal address to an external address and can be one-to-one as with NAT, or many-to-one as with PAT. A single host can have multiple connections to various destinations, but only one translation. If you notice that the xlate count is much larger than the number of hosts on your internal network, it is possible that one of your internal hosts has been compromised. |

**Note** Trend reports are not usually useful when they are based on a small number of data points. The date range and trending type determine the number of data points. For example, there is only one data point if you apply the Daily trending type to less than 2 days' worth of data. It is not possible to graph a trend from only one data point.

# Understanding Throughput Report Subcategories

Each generated line graph in a Throughput report displays results for one device, service module, or virtual server, depending on the service type and subcategory you select—as described in Table 10-3, which:

- Lists all subcategories for configuring Throughput reports.
- Specifies which services support the subcategories.
- Describes the graphs displayed in Throughput reports.

**Note** When you run historical reports, you might see a dip in the graph for any period of time in which the MCP process did not run on your CiscoWorks Server. See MCP Process Maintenance, page 3-16.

*Table 10-3 Throughput Report Configuration Subcategories*

| Throughput Report Subcategory | Relevant Services | Description |
|---|---|---|
| **Note** In all Throughput report graphs, the horizontal axis represents time. The vertical axis represents either a percentile value or a count, depending on the report. | | |
| Throughput | • Remote Access VPN<br>• Site-to-Site VPN | Graph shows trends for the sum in kbps of inbound and outbound octets through all public interfaces over time, factored against interface speed. |
| Throughput Per Accelerator | Remote Access VPN | Graph shows trends for the sum, in kbps, of inbound and outbound octets across scalable encryption processor (SEP) accelerator cards over time, factored against SEP card speed.<br>**Note** Each line in the graph represents a separate SEP card. There are no SEP cards in a VPN 3005 Concentrator or a VPN 3015 Concentrator, so these devices are excluded from the report. You cannot select any other report subcategory when you select Throughput Per Accelerator. |
| Throughput Per Interface | • Remote Access VPN<br>• Site-to-Site VPN | Graph shows trends for the sum, in kbps, of inbound and outbound octets through the public interfaces of one device over time, factored against interface speed.<br>**Note** Each line in the graph represents a separate interface. You cannot select any other report subcategory when you select Throughput Per Interface. |
| % Of Crypto Packet Drop | Site-to-Site VPN | Graph shows the trend of dropped crypto packets as a percentage of all encrypted and decrypted packets over time. |
| % Of Crypto Packet Errors | Remote Access VPN | Graph shows the trend of encrypted packets with errors in Phase-1 (IKE) and Phase-2 (IPSec) tunnels as a percentage of all encrypted packets over time. |
| % Of Packets Dropped | • Remote Access VPN<br>• Site-to-Site VPN | Graph shows the trend of dropped packets in Phase-1 (IKE) and Phase-2 (IPSec) tunnels as a percentage of all inbound and outbound packets over time. |

# Understanding Usage Report Subcategories

Each generated line graph in a Usage report displays results for one device, service module, or virtual server, depending on the service type and subcategory you select—as described in Table 10-4, which:

- Lists all subcategories for configuring Usage reports.
- Specifies which services support the subcategories.
- Describes the graphs displayed in Usage reports.

**Note** When you run historical reports, you might see a dip in the graph for any period of time in which the MCP process did not run on your CiscoWorks Server. See MCP Process Maintenance, page 3-16.

*Table 10-4 Usage Report Configuration Subcategories*

| Usage Report Subcategory | Relevant Services | Description |
|---|---|---|
| **Note** In all Usage report graphs, the horizontal axis represents time. The vertical axis represents either a percentile or a count, depending on the report. | | |
| Number of Tunnels | Site-to-Site VPN | Graph shows trends for the combined number of Phase-1 (IKE) and Phase-2 (IPSec) tunnels for site-to-site VPNs over time. |
| Number of Users | Remote Access VPN | Graph shows trends for the aggregate number of active sessions on all RAS devices over time. |
| # Of Conns Per Module | Load Balancing | Graph shows trends for the average number of connections over time for each CSM module in a specific chassis.<br>**Note** Each line in the graph represents a separate service module. You cannot select any other report subcategory when you select # Of Conns Per Module. |
| # Of Conns Per Virtual Server | Load Balancing | Graph shows trends for the number of connections over time for each virtual server associated with a specific chassis.<br>**Note** Each line in the graph represents a separate virtual server. You cannot select any other report subcategory when you select # Of Conns Per Virtual Server. |
| **Note** Trend reports are not usually useful when they are based on a small number of data points. The date range and trending type determine the number of data points. For example, there is only one data point if you apply the Daily trending type to less than 2 days' worth of data. It is not possible to graph a trend from only one data point. | | |

# Configuring and Generating Reports

You can configure and generate historical reports for any supported service in your network.

**Procedure**

**Step 1** Select **Reports >** *Service Type* **> Configure Report**, where *Service Type* is the service you select in the options bar.

The Configure Report page displays an Object Selector, action buttons, lists, and reporting categories that apply to the service you select. See Using an Object Selector, page 3-10.

**Step 2** If the All tab is not active, click it to display a list of device groups and individual devices in the selection tree. Select the devices whose information you want to include in the report; select a device group to select all devices in the group and its descendants in the hierarchy.

You must select at least one device from the tree before you can configure a report. The following reporting subcategories require that you select *no more than* one device:

- Remote Access: Throughput: Throughput Per Accelerator.
- Remote Access: Throughput: Throughput Per Interface.
- Site-To-Site: Throughput: Throughput Per Interface.
- Load Balancing: Usage: # Of Conns Per Virtual Server.
- Load Balancing: Usage: # Of Conns Per Module.

- Load Balancing: Failure: % Of Conns Dropped By All Virtual Servers.
- Load Balancing: Failure: % Of Failed Conns Per Module.

**Step 3** Select a report category, then select a subcategory, and click **>>** (Add) to move it to the Selected List. Click **<<** (Remove) if you selected the wrong subcategory.

You can select more than one type of report, following these rules:

- You cannot select more than four subcategories for any report.
- You cannot select more than two subcategories for a report unless all of the subcategories you select measure units in percentages. In such cases, you can select as many as four subcategories.
- You cannot select more than two subcategories if either one of your selections measures units in percentages.
- In some cases, as specified in Understanding Reporting Options, page 10-1 and its subtopics, sometimes you can select only one subcategory.

There are more than 30 subcategories of reports. For a description of the report types, see:

- Understanding Failure Report Subcategories, page 10-2.
- Understanding Performance Report Subcategories, page 10-3.
- Understanding Throughput Report Subcategories, page 10-4.
- Understanding Usage Report Subcategories, page 10-5.

**Step 4** Select an interval from the Trending Type list. Trending options are:

- Hourly—The report shows monitored values at intervals of 1 hour for the range of calendar dates that you specify.
- Daily—The report shows monitored values at intervals of 1 day for the range of calendar dates that you specify.
- Weekly—The report shows monitored values at intervals of 1 week for the range of calendar dates that you specify.
- Monthly—The report shows monitored values at intervals of 1 month for the range of calendar dates that you specify.

**Step 5** Select the start (From) and end (To) dates for data to include in the report.

**Step 6** Do one of the following:

- To generate the report and view it in a new browser window, click **View**.
- To generate the report and configure one-time or recurring email distribution options for it, click **Email**. When configuring a recurring emai job, you can specify how many hours of data to include in the report.
- To generate the report and save it to a file, select a file format and click **Export**. The following formats are available:
  - CSV—Exports data in an ASCII list of comma-separated values that you can display in tabular form in most spreadsheet applications.
  - XML—Exports data in extensible markup language that you can review in a web browser or word processor or other application that displays XML files.
  - PDF—Exports data in portable document format, which you can review with the Adobe Acrobat Reader application or any other application that displays PDF files.

# Understanding Historical Reports

A generated report displays graphs that show historical trends for the subcategories you select, to which Performance Monitor applies the trending type and date range you specify. To understand a specific graph, see Understanding Reporting Options, page 10-1 and its subtopics.

The Details area in the Performance Monitor Report page lists your username, the trending type, and the range of dates for the relevant report.

### Related Topic

- Configuring and Generating Reports, page 10-6

# Viewing RAS VPN Top 10 User Reports

You can view an historical report of the top 10 RAS VPN users in your network across all RAS devices.

**Note** Performance Monitor does not display this information for Easy VPN RAS sessions.

### Procedure

**Step 1** Select **Reports > Remote Access > Top 10 Users**.

By default, the Top 10 Users page displays the 10 RAS users whose throughput levels are highest, with hourly data points for the last 24 hours. If fewer than 10 users have connected to your RAS VPN in the last 24 hours, there are fewer than 10 results displayed.

Information in the report is based on user activity rankings from every device.

**Step 2** If desired, modify the report criteria and click **Go** to see the results. You can:

- Change the trending type. Select one of the following:
  - Hourly—Shows monitored values at 1-hour intervals.
  - Daily—Shows monitored values at 1-day intervals.
  - Weekly—Shows monitored values at 1-week intervals.
  - Monthly—Shows monitored values at 1-month intervals.
- Specify a different range of reporting dates by entering different dates in the From and To fields.

### Related Topics

- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

# Viewing RAS VPN User Session Reports

You can view reports that describe the remote access VPN sessions over time of multiple users or of one user whom you specify.

**Tip** Some multi-user session queries return a high number of results. In cases where a query returns more than 10,000 results, the User Session Report page takes several minutes to load in your browser. If such a delay is unacceptable to you, we recommend that you select a specific device and adjust the Start and End times before you submit your query.

### Before You Begin

This feature requires that your VPN 3000 concentrators, ASA and PIX devices are configured to send Syslog messages to Performance Monitor.

- See Setting Up ASA Appliances, PIX Devices, and Firewall Services Modules, page 2-5, for help configuring your appliances and firewalls.
- See Setting Up VPN 3000 Concentrators, page 2-6, for help configuring your VPN concentrators.
- See Working with Notifications, page 12-1, for a list of the Syslog messages that Performance Monitor can process.

### Procedure

**Step 1** Select **Reports > Remote Access > User Session Report**.

The User Session Report page includes an Object Selector. See Using an Object Selector, page 3-10.

**Step 2** Decide whether to display session reports for multiple users or one user, then do one of the following:

- To display information that includes every user session, select **Search All Users**.
- To limit your search to the user sessions in a single cluster, select the cluster parent in the tree.
- To limit your search to the user sessions on a single device, select the device in the tree.
- To limit your search to the sessions of one user, enter the username in the User Name text box.

**Step 3** To define the interval in which Performance Monitor searches for sessions, do both of the following:

- In the Start Time area, select a calendar date and enter a time of day in HH:MM:SS format. The values in the Start Time area define the beginning of the interval in which Performance Monitor searches for session information.
- In the End Time area, select a calendar date and enter a time of day in HH:MM:SS format. The values in the End Time area define the end of the interval in which Performance Monitor searches for session information.

**Step 4** Do either or both of the following:

- To display the report in a new browser window, click **View**.
- To export the report, select a file format (CSV or XML), then click **Export**.

  If you select CSV, Performance Monitor might prompt you to accept a CiscoWorks Server certificate if you did not previously specify the server as a trusted source. If you accept the certificate, Performance Monitor displays the exported CSV data in your default spreadsheet application. If you decline the certificate, Performance Monitor prompts you for a filename and path to save the CSV file locally.

  If you select XML, an XML export opens a new browser window from which you can save the displayed result. Select **File > Save As** to save a local copy of the exported report.

The content of the report is explained in Table 10-5.

### User Session Report Format

*Table 10-5 User Session Report Format*

| Element | Description |
|---|---|
| Username column | Displays the authenticated username you entered as a search query, provided that you searched for one user and that a matching username was found.<br>If you searched for the sessions of all users in a specific timeframe, the Username column might contain all of the authenticated usernames associated with all of the sessions in that timeframe. |
| IP Address column | Displays the user IP address associated with the described session. The IP address for a specific user might vary between sessions, particularly in networks that use dynamic addressing. |
| State column | Displays the most recent status of the described user session—Active or Completed. |
| VPN Device Name column | Displays the DNS name of the VPN concentrator through which the described session took place (or is taking place, in the case of an active session). |
| Start Time column | Displays the date and time at which the described session began, in MM/DD/YYYY HH:MM:SS format. |
| End Time column | Displays the date and time at which the described session ended, in MM/DD/YYYY HH:MM:SS format.<br>If End Time values are red, the exact end time is unknown. The displayed value in such cases is the time at which Performance Monitor polling determined that the session was no longer active. |
| Duration column | Displays the duration of the session in days, hours, minutes, and seconds.<br>If the exact end time is unknown, values in the Duration column are red. The displayed value in such cases is the duration at which Performance Monitor polling determined that the session was no longer active. |
| Last Verified column | Displays the most recent time (in MM/DD/YYYY HH:MM:SS format) at which device polling provided information for the described session. |
| Bytes In column | Displays the total number of tunneled bytes that the user received through your network during the described session. |
| Bytes Out column | Displays the total number of tunneled bytes that the user sent through your network during the described session. |

# Viewing Site-to-Site VPN Top 10 Tunnel Reports

You can view an historical report of the top 10 site-to-site VPN tunnels in your network across all devices.

### Procedure

**Step 1** Select **Reports > Site-to-Site > Top 10 Tunnels**.

By default, the Top 10 Tunnels page displays the 10 tunnels with the highest throughput levels, applying hourly data points to the last 24 hours. If fewer than 10 tunnels have had measurable throughput in the last 24 hours, fewer than 10 results are displayed.

For an explanation of the columns in the table, see Table 10-6.

**Step 2** If desired, modify the report criteria and click **Go** to see the results. You can:

- Change the trending type. Select one of the following:
  - Hourly—Shows monitored values at 1-hour intervals.
  - Daily—Shows monitored values at 1-day intervals.
  - Weekly—Shows monitored values at 1-week intervals.
  - Monthly—Shows monitored values at 1-month intervals.
- Specify a different range of reporting dates by entering different dates in the From and To fields.

### Reference

*Table 10-6 Top 10 Tunnels Page*

| Element | Description |
|---|---|
| Device Name column | Displays the DNS name or IP address of the described device. |
| Local Endpoint column | Displays the IP address of the local endpoint device interface at which the tunnel terminates.<br>**Note** The identity of the "local" endpoint device might vary in Performance Monitor because its definition is always relative to the device that you monitor. |
| Remote Endpoint column | Displays the IP address of the remote endpoint device interface at which the tunnel terminates.<br>**Note** The identity of the "remote" endpoint device might vary in Performance Monitor because its definition is always relative to the device that you monitor. |
| Local Subnet column<br>Remote Subnet column<br>Protocol column | Taken together, the values in these three columns define the access list for one tunnel:<br>• Local Subnet—Displays the tunnel subnet and mask on the local endpoint device.<br>• Remote Subnet—Displays the tunnel subnet and mask on the remote endpoint device.<br>• Protocol—Displays the tunnel protocol and the port used, such as TCP 80. |
| Throughput (Kbps) column | Displays the sum of inbound and outbound octets through the tunnel since tunnel inception, in Kbps. |

### Related Topics

- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8

# Working with Scheduled Email Jobs

You can view and delete the scheduled email jobs through which Performance Monitor distributes historical reports.

### Procedure

**Step 1** Select **Reports** > *Service Type* > **Scheduled Email Jobs**, where *Service Type* is the service that you select in the options bar.

**Step 2** Select one job from the list.

**Step 3** Do one of the following:

- To display the job in the Email Job Details window, click **View**.
- To delete the job, click **Delete**. You cannot undo a job deletion.

### Reference

*Table 10-7 Email Jobs*

| Element | Description |
|---|---|
| Job Name column | Displays the name of the job, which consists of:<br>• Your CiscoWorks username—for example, Admin.<br>• The specified service type—for example, RAS.<br>• The value that you entered in the Job Name field in the Schedule Email Report window. |
| Recurring column | Displays either:<br>• Yes—the job is scheduled to recur.<br>• No—the job is scheduled to occur only once. |
| Next Schedule column | For recurring jobs only, displays the next date and time at which the job recurs. |
| Last Run Status column | Displays a message to indicate whether the email was sent successfully or if delivery failed. |
| Last Run Time column | Displays the most recent time (in MM/DD/YYYY HH:MM:SS format) at which this scheduled email job ran. |

### Related Topics

- Configuring and Generating Reports, page 10-6
- Optional Tasks in Performance Monitor Tables, page 3-9
- Common Elements in Tables, page 3-8