Dell™ SonicWALL™ Analyzer

Administration Guide

Navigating Dell SonicWALL Analyzer Reporting

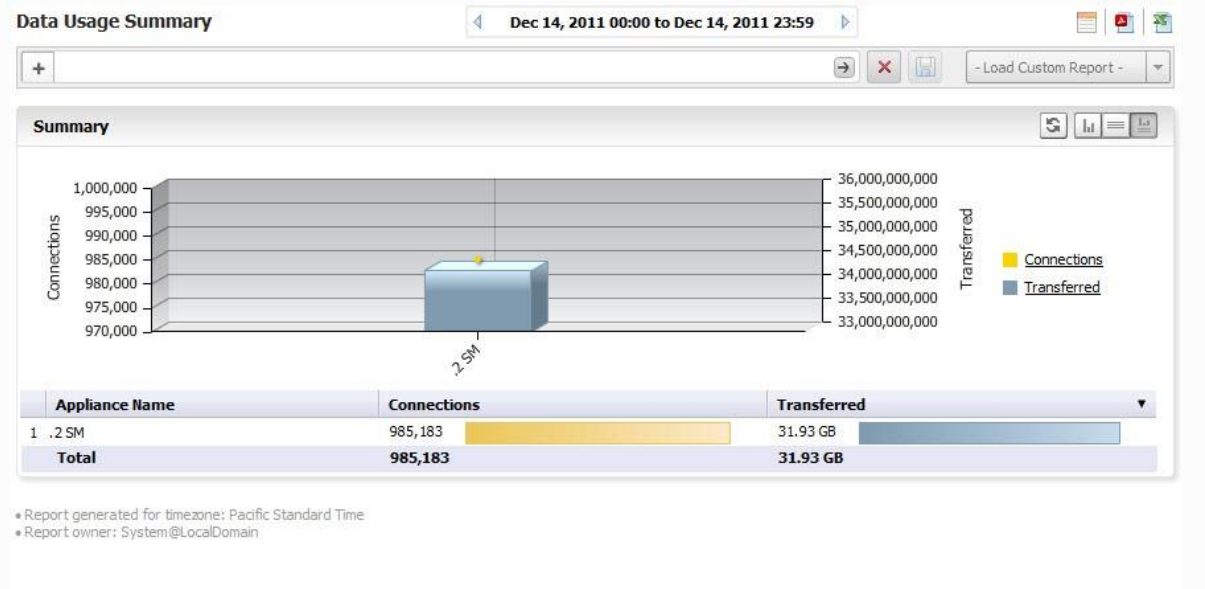
Dell SonicWALL Analyzer Reporting is a robust and powerful tool you can use to view detailed reports for individual SonicWALL appliances.

This section describes each view and what to consider when making changes. It also describes the Search Bar and display options for interactive reports, as well as other enhancements provided in Dell SonicWALL Analyzer. See the following sections:

Global Views

From the Global view of the Firewall Panel, Summary reports are available for all SonicWALL appliances connected to Dell SonicWALL Analyzer. The Summary provides a high level report for all appliances. More detail is available from the Unit view.

To open the Global view, click the **My Reports** view icon in the upper-left corner of the left pane.



Summary pages are available for the major functions on the middle pane. By default, they display both the Chart View and Grid View. You can use the toggle buttons to the right to display either view, or both.

NOTE: The selected Chart of Grid view remains in effect only for the specified screen. Changing screens defaults back to the Chart and Grid View.

Unit View

The Unit view provides a detailed report for the selected SonicWALL appliance.

Dell SonicWALL Analyzer provides interactive reports that create a clear and visually pleasing display of information. You can control the way the information is displayed by adjusting the settings through toggles that allow you to display a graphical chart, a grid view containing the information in tabular format, or both (default). Reports are scheduled and configured in the Universal Scheduled Reports settings. For more information, refer to Using the Universal Scheduled Reports Application on page 30.

The Reports tab provides a list of available Reports. Click on the type of report to expand the list items and view the available reports in that screen group.

TIP: At times, you might wish to see multiple screen groups at the same time. Ctrl-click to keep a previously-expanded topic from collapsing when you select a new report category. For example, you might want to view Data Usage, Applications, and Intrusions simultaneously, to see what detail sections are available. Control-click on these entries to see all the screen groups under these entries simultaneously.

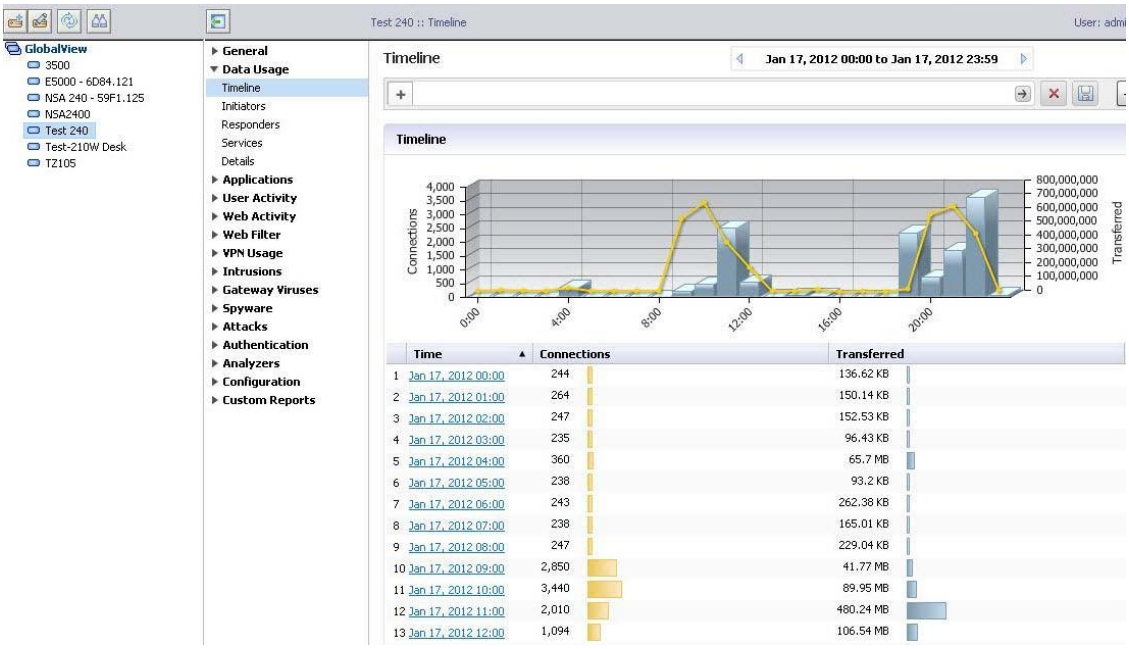
The reports available are usually the reports that appear as sections in the Details view. The Details entry is a shortcut to a view of all the available reports.

To access the Reports, use the following steps:

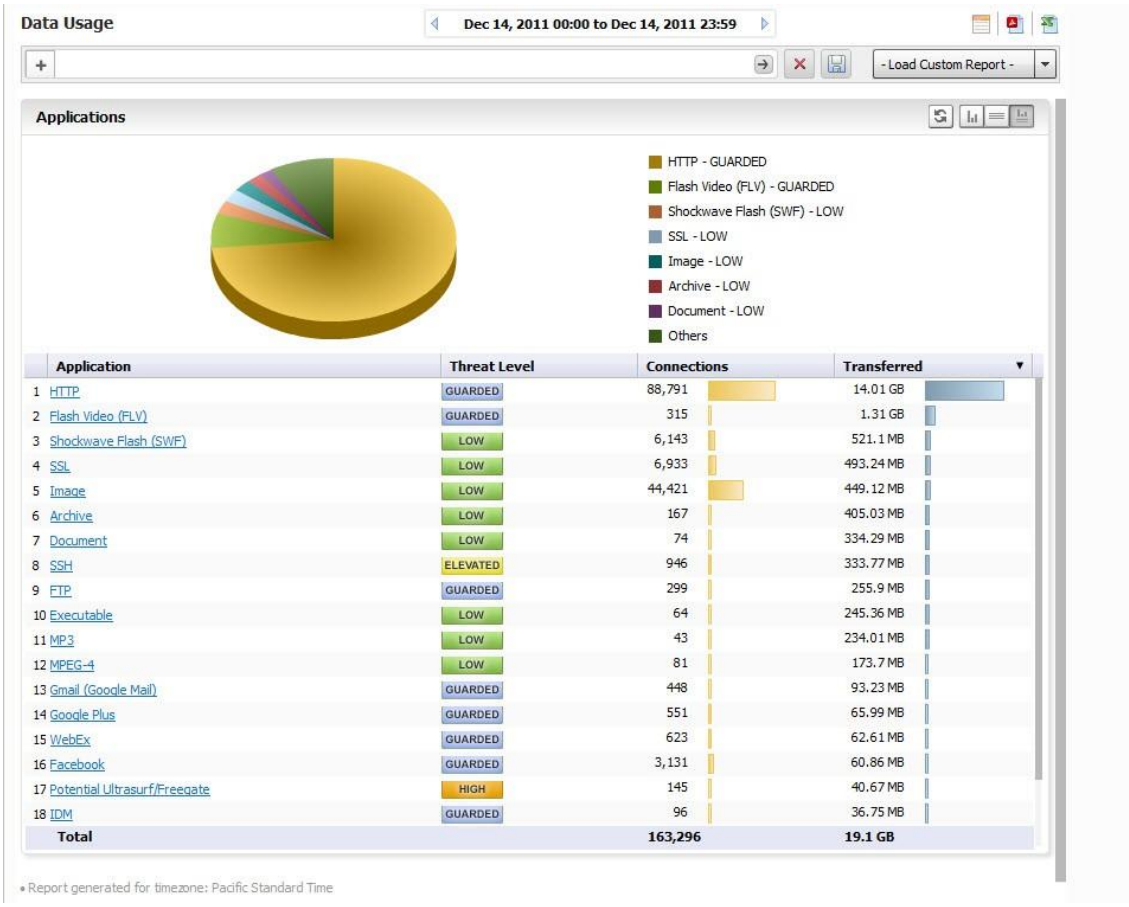
1 Click on the desired tab at the top of the Dell SonicWALL Analyzer interface.

2 To open the Unit view, click on a device in the TreeControl pane.

3 Click on the desired report in the list of reports in the middle pane.



The default view of a root-level report always shows the chart and grid view of the report. The Sections displayed in the Grid View depend on the Report item selected and the filters applied to it. Additional information can be displayed by mousing over certain elements of the Report.



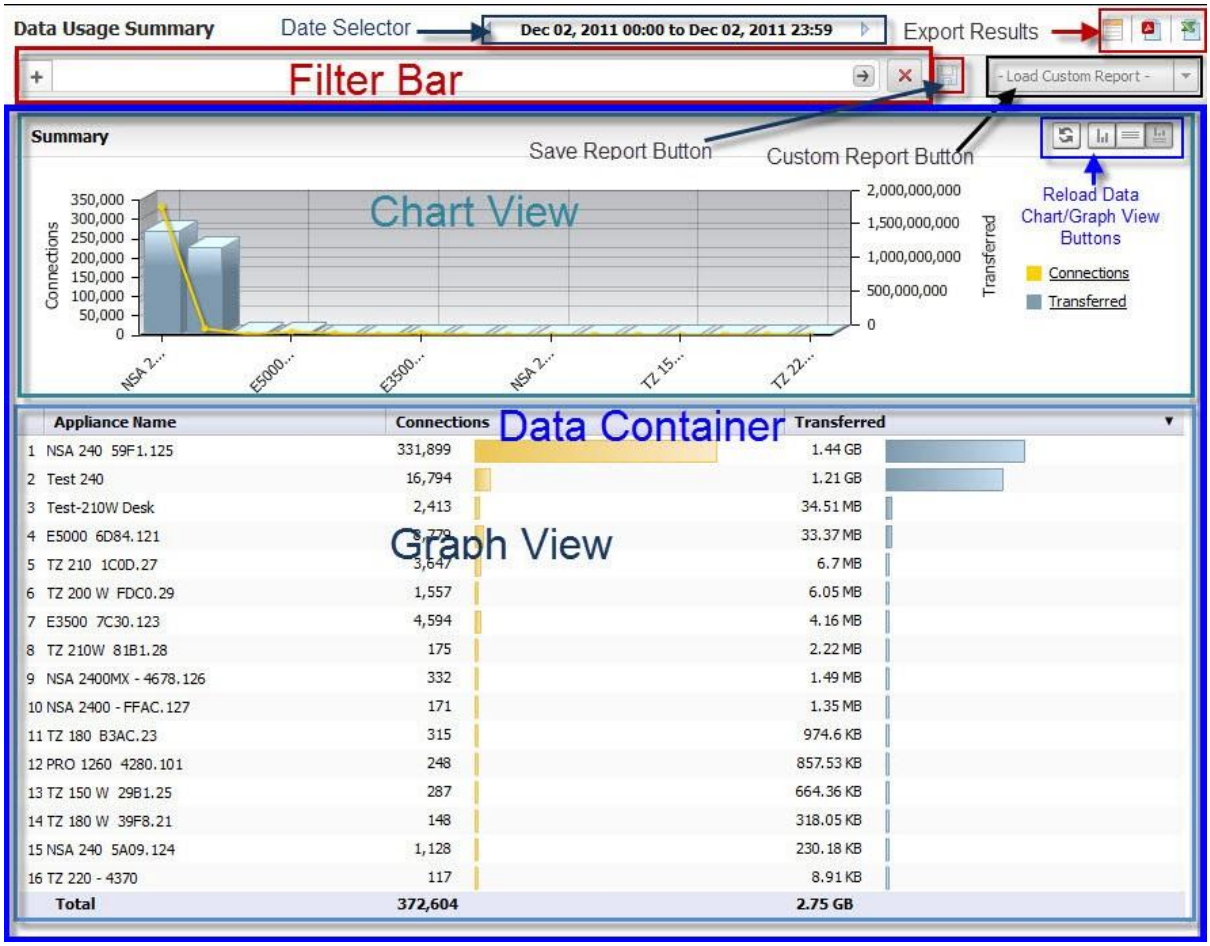
NOTE: As you navigate the Firewall panel with a single SonicWALL appliance selected and apply filter settings, your filter settings remain in effect throughout the session. To remove filter settings, click on the search bar **Remove Filters**. (Refer to the graphic in Layout of Reports Display on page 62.)

Layout of Reports Display

The Report Display is comprised of the following areas:

- The Filter Bar area, which includes the Time Bar, Export, and Custom Reports buttons, and data filter functions
- Report Data Container, containing the Chart and/or Grid Views

The figure that follows shows the layout of the Report.



The Report contains the following areas:

- The **Date Selector** Bar
- The **Filter** Bar

- Export Options, including:
  - **Schedule Report** button: brings up the Universal Scheduled Reports menus
  - **Export to CSV**
  - **Export to PDF**
- **Save** button
- **Load Custom Report** button
- **Report Data Container**. The **Report Data Container** consists of the Chart View and the Grid View, the **Show Chart**, **Show Grid**, and **Show Chart and Grid** toggle buttons, and the **Reload Data** button.

NOTE: The Chart view is clickable. You can drill down to Detail sections simply by clicking on areas of interest in the bar-chart or pie-chart.

The Date Selector

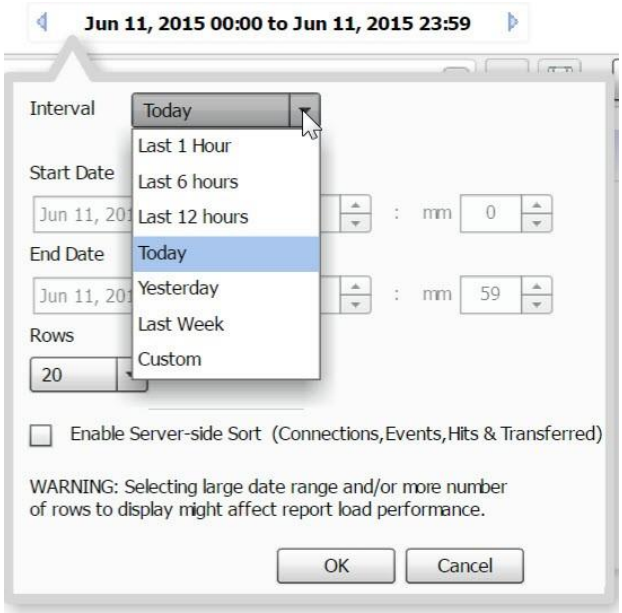
The **Date Selector** allows you to generate a report for only a specific date and time range. Use the right and left quick-link arrows to move backward and forward in time, a day at a time. Clicking the time field on the Date Selector brings up a drop-down menu that allows you to customize your time and date ranges.

Setting a Date or Date Range

By default, summary reports display only information for a single date. However, by using the **Time Selector** drop-down menu, you can fine-tune the time, date, or range of times and dates you want to see. Over-time reports display information over a date range.

Selecting a Date and Time

The **Time Selector** allows you to specify any time or date interval desired, whether by day, or in hour/minute intervals. To select a single date for a report, either use the Date Selector bar and the left and right arrows to page through reports by date, or click on the displayed date field in the Time Selector to display the drop-down schedule menu.



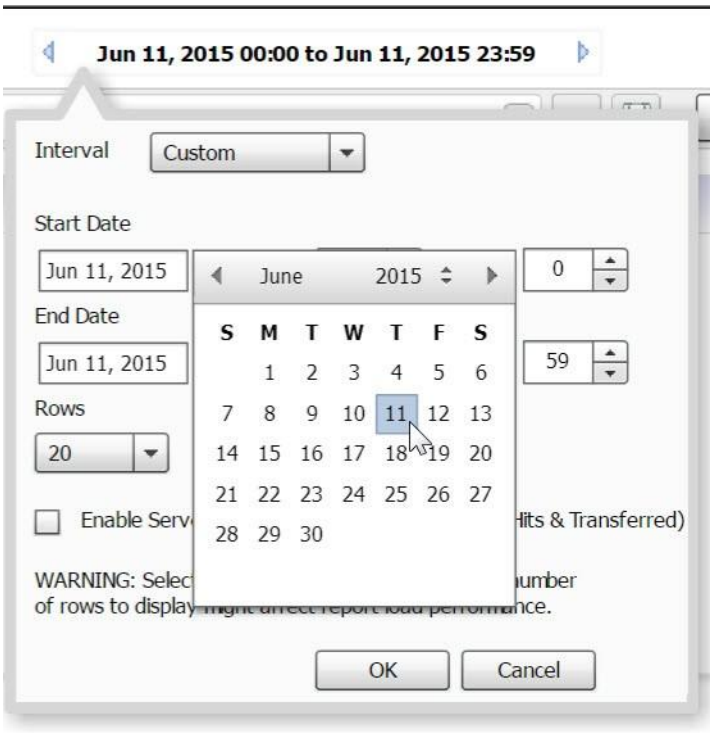
You can select from:

- Last 1 hour
- Last 6 hours
- Last 12 hours
- Today — 00:00 to 23:59
- Yesterday — 00:00 to 23:59
- Last Week — the previous 7 days, from 00:00 to 23:59
- Custom — a custom time and date range

In the drop-down schedule menu, you can specify a recent time snapshot, or click on Custom to select the starting and ending dates and times. The Custom option allows you to select a specific time and date or range from the Interval menu.

1 To set up a custom time range, click in the Time Selector Bar. The Interval drop-down menu appears.

In the Interval menu, you can either set the date manually or by using the drop-down calendar. In the calendar, you can set the month by clicking the desired dates. If no data is available for a specific date, that date is not available (grayed out).



2 Set a specific start and ending time by specifying hours and minutes you want to monitor. The default for a date is an interval starting at hour 0 minute 0 (midnight) and ending at 23:59 (11:59 PM).

3 The Interval menu also lets you set how many lines of information appears in the graph view. Click the date, and when the Interval drop-down appears, specify the number of rows. Select **5**, **10**, **20**, **50**, or **100** from the **Rows** drop-down list to limit the display to a the specified number of lines, for easier viewing.

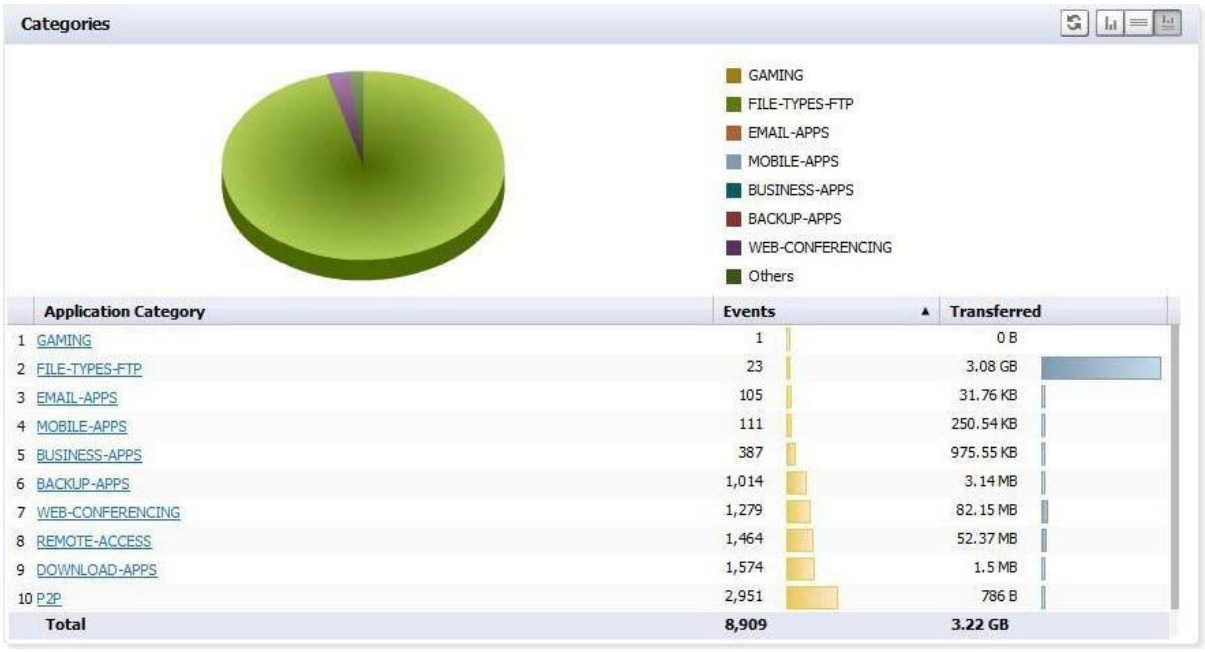
4 Click **OK** to generate the report.

Report data is sorted and ranked according to how many rows are displayed. By specifying a limited number of rows to be displayed in the graph section of the Report, rankings apply only to the data in those rows. If you reverse the sort order by clicking on the column bar, only the displayed items are re-sorted.

To re-sort according to all collected data in the database, click on the **Enable Server Side Sort** check box on the drop-down menu. The ranking of the grid items then reflects all data from the total entries.

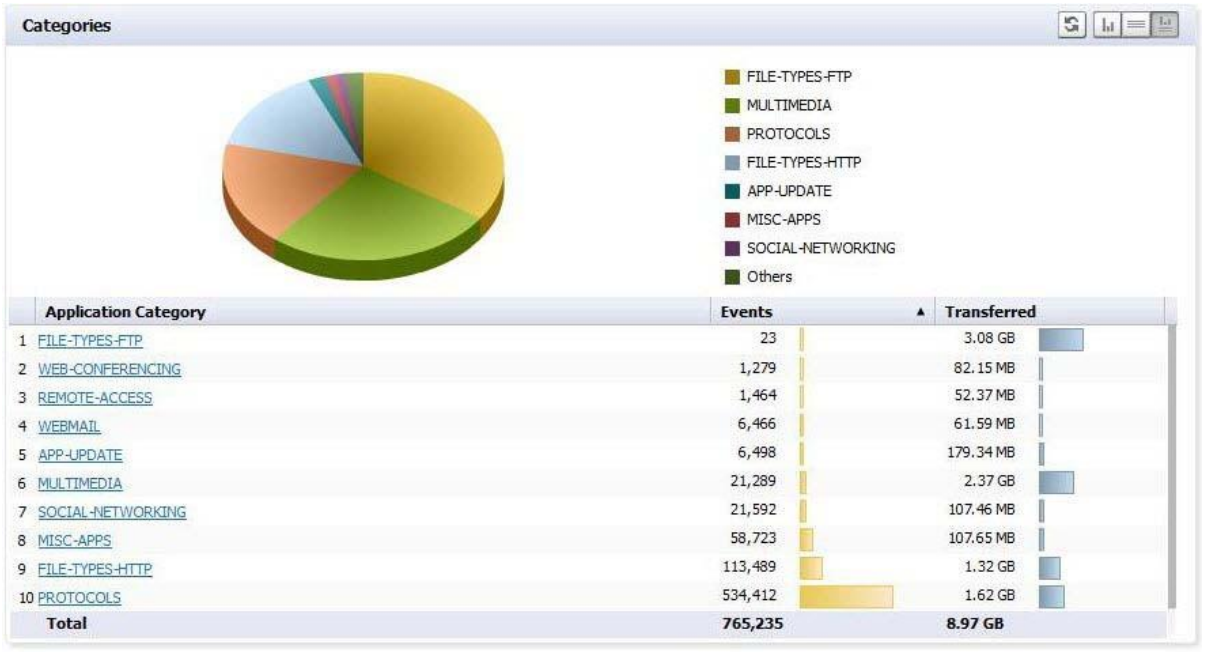
By default, Client-side Sort is used, which sorts only the currently viewable data, which was retrieved the first time the data base was clicked on.

For example, the image that follows shows data displayed only as it pertains to ten rows.



	Application Category	Events	Transferred
1	GAMING	1	0 B
2	FILE-TYPES-FTP	23	3.08 GB
3	EMAIL-APPS	105	31.76 KB
4	MOBILE-APPS	111	250.54 KB
5	BUSINESS-APPS	387	975.55 KB
6	BACKUP-APPS	1,014	3.14 MB
7	WEB-CONFERENCING	1,279	82.15 MB
8	REMOTE-ACCESS	1,464	52.37 MB
9	DOWNLOAD-APPS	1,574	1.5 MB
10	P2P	2,951	786 B
	Total	**8,909**	**3.22 GB**

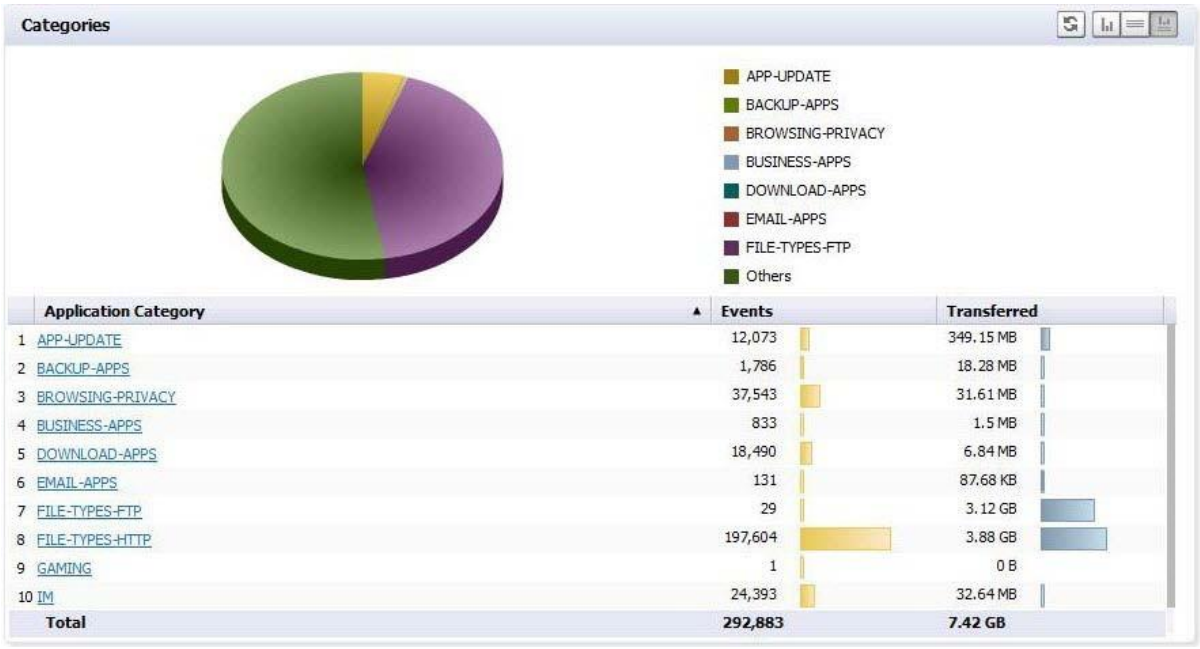
If you re-rank the column to see the lowest number of hits, it ranks only the items displayed in the ten rows you selected.



	Application Category	Events	Transferred
1	FILE-TYPES-FTP	23	3.08 GB
2	WEB-CONFERENCING	1,279	82.15 MB
3	REMOTE-ACCESS	1,464	52.37 MB
4	WEBMAIL	6,466	61.59 MB
5	APP-UPDATE	6,498	179.34 MB
6	MULTIMEDIA	21,289	2.37 GB
7	SOCIAL-NETWORKING	21,592	107.46 MB
8	MISC-APPS	58,723	107.65 MB
9	FILE-TYPES-HTTP	113,489	1.32 GB
10	PROTOCOLS	534,412	1.62 GB
	Total	**765,235**	**8.97 GB**

Use **Enable Server Side Sort** to sort data based on all underlying data records, not the client-side sort. Server side Sort retrieves current data from the back end database. Client-side sort merely rearranges the data already

retrieved. You can still constrain your display to 10 rows, but the display re-sorts based on the total data collected in the back-end database, and not just the data previously displayed.



	Application Category	Events	Transferred
1	APP-UPDATE	12,073	349.15 MB
2	BACKUP-APPS	1,786	18.28 MB
3	BROWSING-PRIVACY	37,543	31.61 MB
4	BUSINESS-APPS	833	1.5 MB
5	DOWNLOAD-APPS	18,490	6.84 MB
6	EMAIL-APPS	131	87.68 KB
7	FILE-TYPES-FTP	29	3.12 GB
8	FILE-TYPES-HTTP	197,604	3.88 GB
9	GAMING	1	0 B
10	IM	24,393	32.64 MB
	Total	**292,883**	**7.42 GB**

Export Results

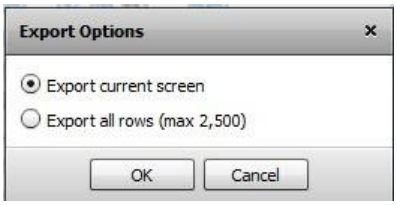
The **Export to PDF** and **Export to CSV** icons allow you to save a report in either PDF or Excel format.

These buttons provide the following export options:

- **Export to PDF** — This button allows you to save the displayed report data to a PDF file. The PDF can export a maximum of 2500 rows.
- **Export to CSV** — This button allows you to send the report to a file in Microsoft Excel Comma Separated Value (CSV) format. Excel can export a maximum of 10,000 rows.

TIP: To print a report, export it to PDF, using **Export to PDF**, then print out the PDF file.

If a very large Report file, such as a system log, is being exported, the number of lines that can be saved is limited. When you click the icon, you see a message like the following:



Select whether to print only the currently-displayed screen, or the maximum number of rows.

The Filter Bar

The Filter Bar provides filtering functions to narrow search results, to view subsets of report data.

The Filter Bar is at the top of the Report. It contains **Add Filter (+)** for adding filters and a **Go** button to apply filters, as well as the **Clear Filter** button to clear all filters.

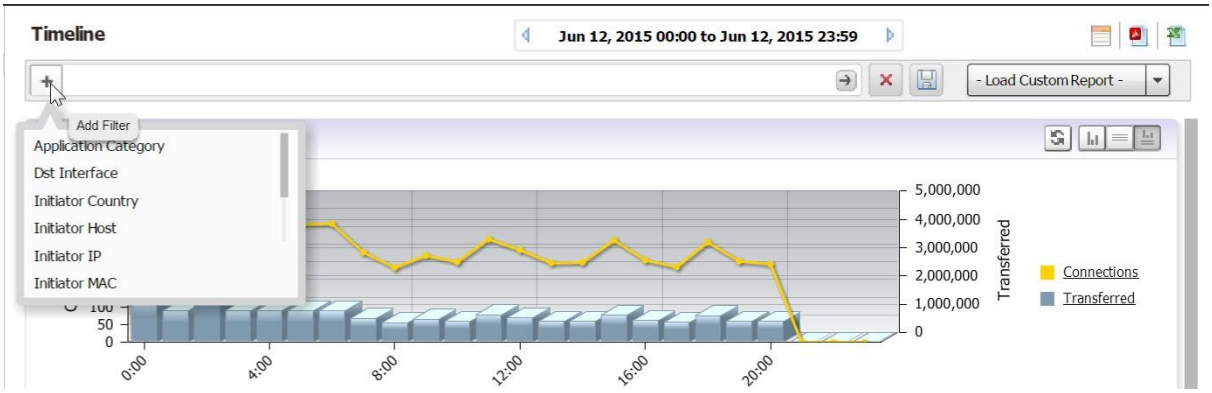
Using the Filter Bar allows you to view subsets of the report data, based on a set of pre-defined filters.

Adding Filters

Filters can be added in two ways, either explicitly through the Filter Bar, or implicitly by clicking on the hyperlinks in the grid sections of a displayed report. As hyperlinks are clicked, those link criteria are added to the Filter bar as if it was added explicitly. Refer to Adding Filters Implicitly on page 69 for more information.

Use the Filter Bar to add pre-defined filters from a drop-down menu and to specify parameters for those filters. Filter values are matched in the database during report generation.

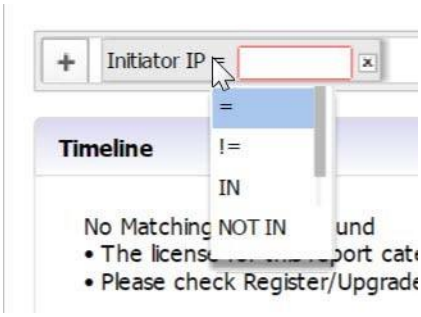
Click **Add Filter** (+) on the left to display a drop-down menu, which can then be used to fine-tune the report data by selecting categories.



Filters can also be added by right-clicking on a column entry and selecting the Filter option from the drop-down menu.

Filter criteria are context-dependant, meaning that Dell SonicWALL Analyzer finds the specific filter operators applicable to the entry. Many filter operators are used in connection with a text string or numeric filter input value that determines what data to include in the report. This control uses auto-complete to suggest a set of candidate values, or you can manually enter a different value. Manually-entered values should be checked for blanks, illegal characters and so on.

Operators are specified by clicking on the default operator to bring up the drop-down menu of available operators.



Depending on the selected field type, text string or numeric, several filter operators are available. The filter operators are used with a filter input value to restrict the information displayed in the Detail report.

The operators are defined as shown in Table 5.

Table 5. Filter Operators

Operator	Definition
=	Only data that exactly matches the filter input numerical value is included in the report
!=	Data values that are not equal to the input numerical value are included in the report
>	Data values that are greater than the input value are included in the report.
>=	Data values that are greater than or equal to the input value are included in the report.
<	Data values that are less than the input value are included in the report.
<=	Data values that are less than or equal to the input value are included in the report.
IN	Data values that are in the input value are included in the report.
NOT IN	Data values that are not in the input value are included in the report.
LIKE	Data values that are like the input value are included in the report.
NOT LIKE	Data values that are not like the input value are included in the report.
IS	Data values that are between the input values are included in the report. Separate the vales by using a hyphen with a space on either side, such as “172.30.72.16 - 172.30.72.19.”
IN RANGE	Subnet data that is in the specified range is included in the report.
NOT IN RANGE	Subnet data that is not in the specified range is included in the report.

You can also use wild-cards (*) in filters to match anything. For instance, you might want to match a User name. You would select LIKE as the operator, and use * in connection with a string. For example, “joh*” would match all users starting with “joh,” such as John, Johnny, Johan, and so on.

Using the Filter Bar

Use the Filter Bar to manually (explicitly) add filters.

To add a filter:

1 Click the **Add Filter (+)** menu and select a filter from the drop-down menu. Available Filter categories can differ, depending on the report, and could require parameters.

> **NOTE:** Some filter fields use operators with text or numeric values. Others might have pre-filled values. For example, the Initiator Country filter displays a pull-down list, allowing you to display results based on a selected country. You can create reports with filters on VLAN Interfaces by using the Interface Filter (Source or Destination), and using the VLAN interface name with ‘:’ replaced by ‘-’. VLAN Interfaces typically are as follows: X8:V100, X0:V20, and so on. When VLAN interface information is sent in the syslogs, the character ‘:’ is replaced with ‘-’. So, you must use values such as X8-V100, X0-V20 in the Interface filters.

2 Click **Go** (right arrow) to add a filter Each filter must be applied by clicking **Go** before you can select and apply the next filter. The filter bar shows all filters added, whether added from the menu bar or drop-down menu.

   As filters are added, items that have been filtered out disappear from the listings, reappearing only when the associated filter, or all filters, are removed.

3 To remove a filter, click the + next to the filter in the menu bar and click **Go** (right arrow). To clear all filters, click the Clear Filter (x) next to the filter fields.

Adding Filters Implicitly

Dell SonicWALL Analyzer also allows adding filters directly to a drillable (hypertext-linked) column to create a "criteria control," where you can set a value for the filter. Adding a filter to a column allows you to restrict the display to view only the data related to the entry of interest.

In second-level reports with multiple subsections, filters can be added simply by clicking on the hyperlinked data in the report section.

To add a filter to a "drillable" column containing hypertext links:

1 Right-click on a hypertext column cell and select **Add Filter** from the resulting drop-down context menu.

   Because the filter is context-sensitive, it might suggest a set of candidate values, or you can manually enter a different value. A new filter is automatically added to the filter bar, and the report is updated accordingly.

   After being added, the filter is added to the filter area of the Search Bar and no longer appears in the drop-down list. The report displays only results restricted by that filter.

2 To remove the filter, click the x next to that filter, or clear all filters by clicking the red X button to the right of the field.

Saving/Viewing a Filtered Report

The **Save Report** pop-up menu allows you to save the currently-displayed report with a specified name of no more than 20 characters. You can also overwrite an already-saved report with the current report or overwrite the report to show a new date range.

Saved reports, even if created for a specific unit, are available for all units of that appliance type. For example, if a report for the X1 interface was created for a specific unit, this report is available from any unit: there is no need to create a X1 report for different units.

NOTE: Custom Reports created by a specific user are viewable by that user, and no one else. Domain Administrators can view all available reports.

To save a report, along with its filter criteria:

1 Click **Save Report**.

2 Assign it a file name for later reference.

3 To view a saved Custom Report, click **Custom Reports** to bring up a menu that contains a list of all saved Custom reports available for viewing. Selecting a Custom Report from this drop-down loads data for the selected report into the Report Data Container.

4 You can also load a saved report from the Report tab on the middle bar menu. Click **Custom Reports** on the Reports tab and select the desired report to load it into the Data Container.

5 Click on the appropriate **Export Results** icon to save a report to a PDF file or Excel spreadsheet. To print a copy of the report, click on the PDF icon and save it to a file, then print the PDF file.

TIP: Saved Reports can be modified or deleted by clicking **Custom > Manage Reports**.

Scheduling Reports

You can schedule a report to be created and sent to you in email, using the Universal Scheduled Reports function.

The **Schedule Reports** icon is located to the right side of the toolbar above **Load Custom Reports**.

Click this icon to bring up the Universal Scheduled Report Configuration Manager.

When the Configuration Manager menu comes up, it is pre-filled with the information about the current Reports page. Using this report, you can set up specific tasks, chose the format for the report, and other options. For more information on using Universal Scheduled Reports, refer to the section: Universal Scheduled Reports.

Report Data Container

The Report Data Container is the screen space where the report data is displayed.

Dell SonicWALL Analyzer provides interactive reporting to create a clear and visually pleasing display of information in the Report Data Container. The Root-level baseline report shows the Chart View, usually containing a timeline or a pie chart and a Graph View.

You can control the way the information is displayed by adjusting the settings through toggles or by configuring reports in the dashboard interface.

Reports have a Date Selector and Filter Bar at the top, with the Report Data Container below it.

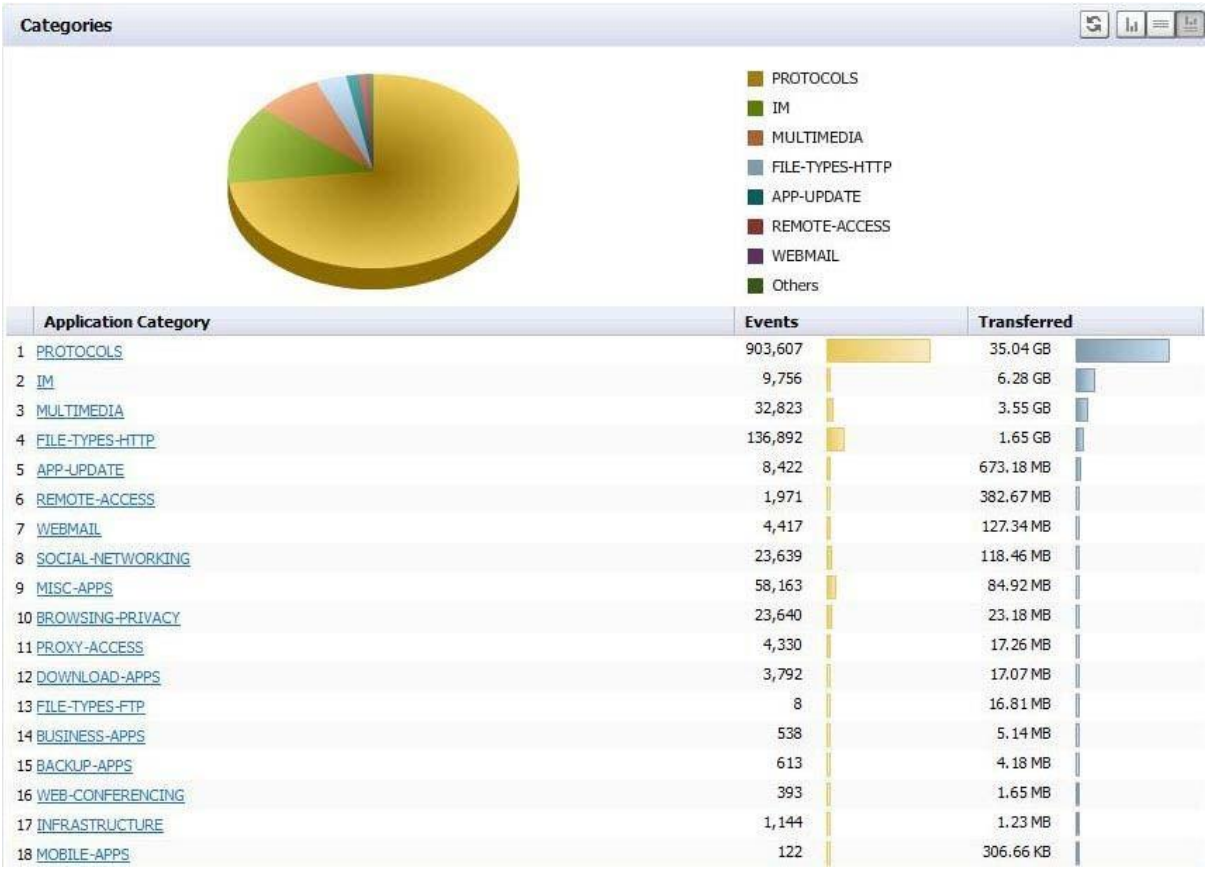
Detail-level reports are available either by “drilling down” on hyperlinks in the Root-level view, or, for some types of Reports, as a shortcut on the Report tab.

NOTE: Cell data in the report container can be copied by right-clicking the cell and selecting Copy Cell Data from the drop-down menu.

Layout of the Data Container

The Report Data Container is comprised of a number of Sections. Sections are usually arranged vertically stacked on top of each other. Each section has a “Title Bar” which contains the “Section” title on the left and a

group of buttons on the right. The Report itself might contain one or more Sections of data, which are different facets of the report data.



	Application Category	Events	Transferred
1	PROTOCOLS	903,607	35.04 GB
2	IM	9,756	6.28 GB
3	MULTIMEDIA	32,823	3.55 GB
4	FILE-TYPES-HTTP	136,892	1.65 GB
5	APP-UPDATE	8,422	673.18 MB
6	REMOTE-ACCESS	1,971	382.67 MB
7	WEBMAIL	4,417	127.34 MB
8	SOCIAL-NETWORKING	23,639	118.46 MB
9	MISC-APPS	58,163	84.92 MB
10	BROWSING-PRIVACY	23,640	23.18 MB
11	PROXY-ACCESS	4,330	17.26 MB
12	DOWNLOAD-APPS	3,792	17.07 MB
13	FILE-TYPES-FTP	8	16.81 MB
14	BUSINESS-APPS	538	5.14 MB
15	BACKUP-APPS	613	4.18 MB
16	WEB-CONFERENCING	393	1.65 MB
17	INFRASTRUCTURE	1,144	1.23 MB
18	MOBILE-APPS	122	306.66 KB

TIP: At times, you might wish to see multiple screen groups at the same time. Ctrl-click to keep a previously-expanded topic from collapsing when you select a new report category. For example, you might want to view Data Usage, Applications, and Intrusions simultaneously, to see what detail sections are available. Control-click on these entries to see all the screen groups under these entries simultaneously.

NOTE: Root level reports available in the Reports panel usually contain only one section.

The Report Data Container sections either appear as a chart view, a grid view, or both.

The default display mode is **Show Chart and Grid**. In this mode, the data is available for viewing as both a '**Chart**' and a '**Grid**'. This layout can be controlled by switching between three display mode options, any of which can be turned on/off at any time, using the utility toggle button group on the Section Title Bar.

The display modes available on this layout are:

- **Show Chart**: In this mode only the chart is visible and takes up all the available space inside the section container. Charts show a timeline or pie chart.
- **Show Grid**: In this mode only the Grid is visible. The Grid Display can contain more than one section.
- **Show Chart and Grid**: In this mode both the *chart* and the *grid* are visible and are vertically stacked.

  Switching between these modes is handled through the utility toggle buttons.

  Only one mode can be active at a time.

A ‘Reload Data’ button  is present on the title bar in *all the layouts* described previously. Clicking this button instructs the application to refresh the section data.

You can determine if you have reached the final section in a multi-section Grid View by checking if there is a message about the relevant time-zone at the bottom left of the report. If this message is present, there are no more Grid sections available.

Viewing Syslog Data of Generated Reports

Different types of section data are available under the root-level report. The section level reports are available through the Details entry on the middle pane Reports tab, for some Reports. You can also drill down from the root level report to the second level Detail views, containing multiple subsections, by right-clicking a hyperlink and selecting “Drilldown” from the drop-down menu. The syslog fields corresponding to the applied filter comes up.

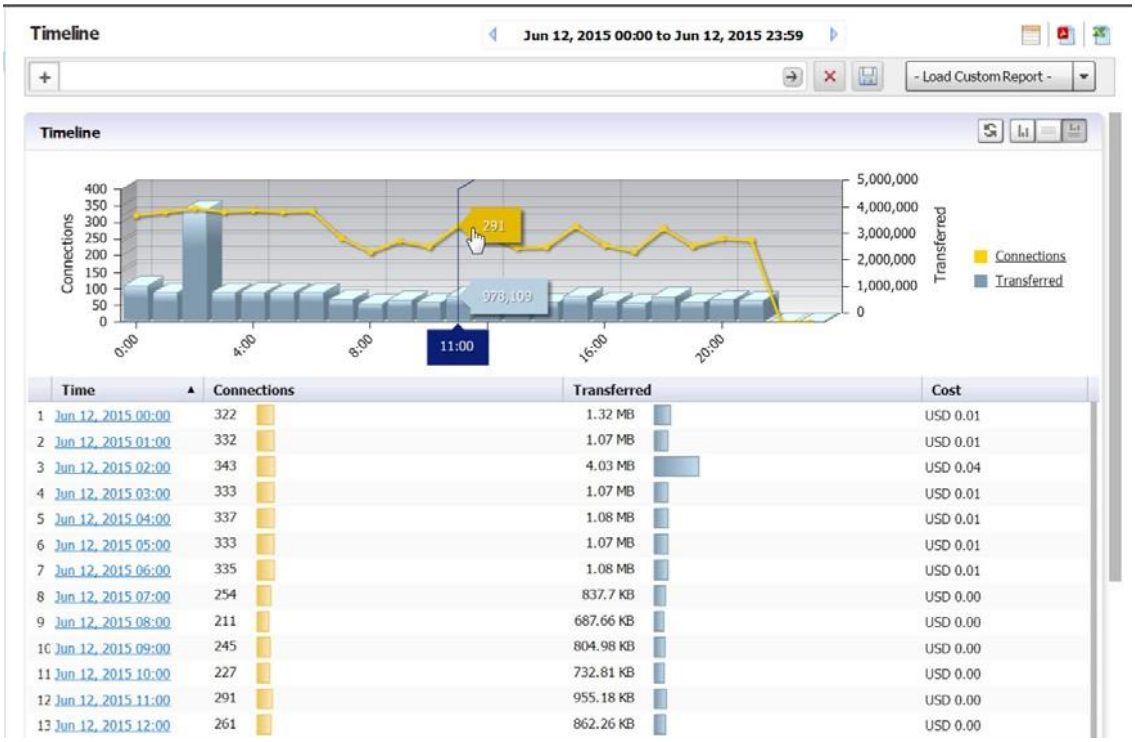
Drilling Down

Sections in the Grid display might contain drillable columns, containing hypertext links to bring up a Detail Report. A ‘drillable’ column appears as a column in the data grid, where the child values appear underlined and in blue, and act as a hyperlink to additional information. Click on any of these values to drill down to another report, using the value on which drill-down has been executed as a filter. When you click on a drillable link, this filter is added to the Filter Bar.

Drilling down navigates to a new Detail report, filtered by the data on which the drill-down was executed. Drillable reports can display multiple grid sections in the sub-reports, or bring up a System Analyzer view, depending on the item selected.

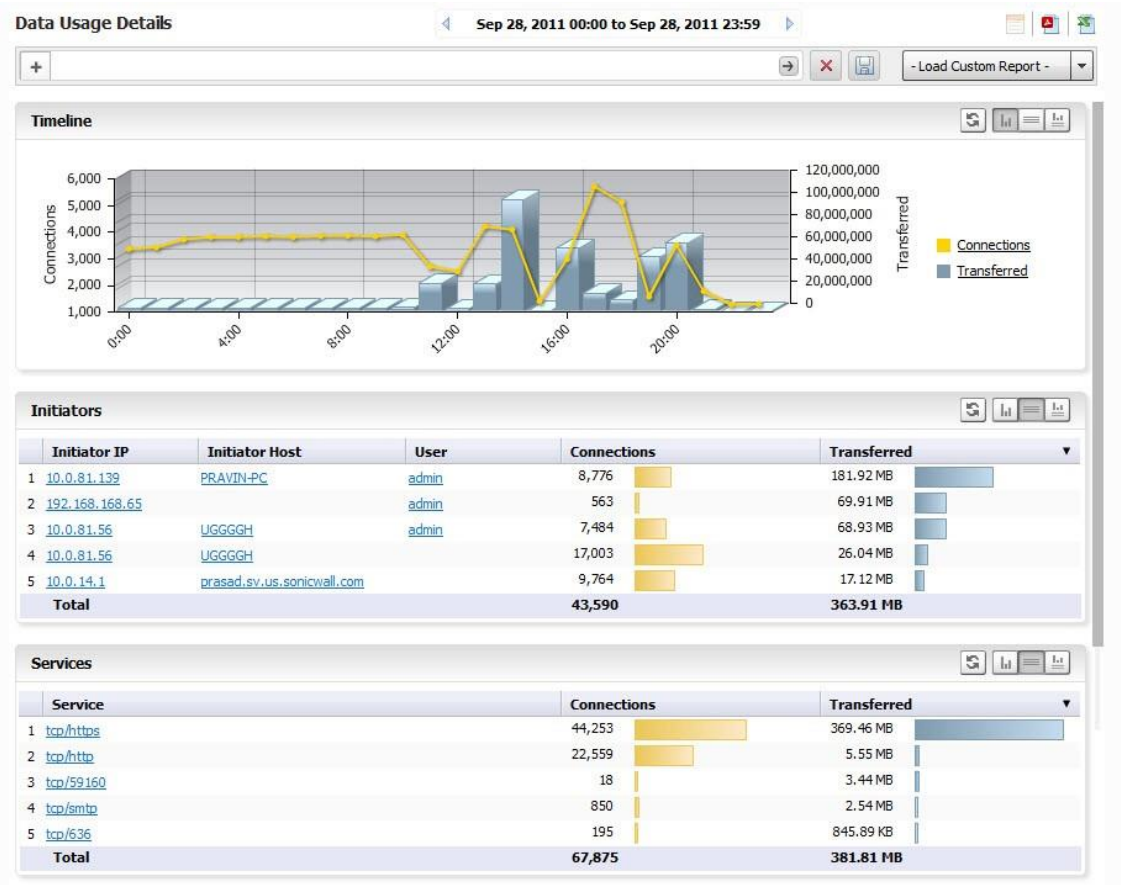
The following example illustrates how you can drill down through the **Data Usage** Report by clicking on a drillable entry to gain more information and filter the results.

1 Click on an appliance, then click **Data Usage** on the Reports tab. You see a timeline showing connections.

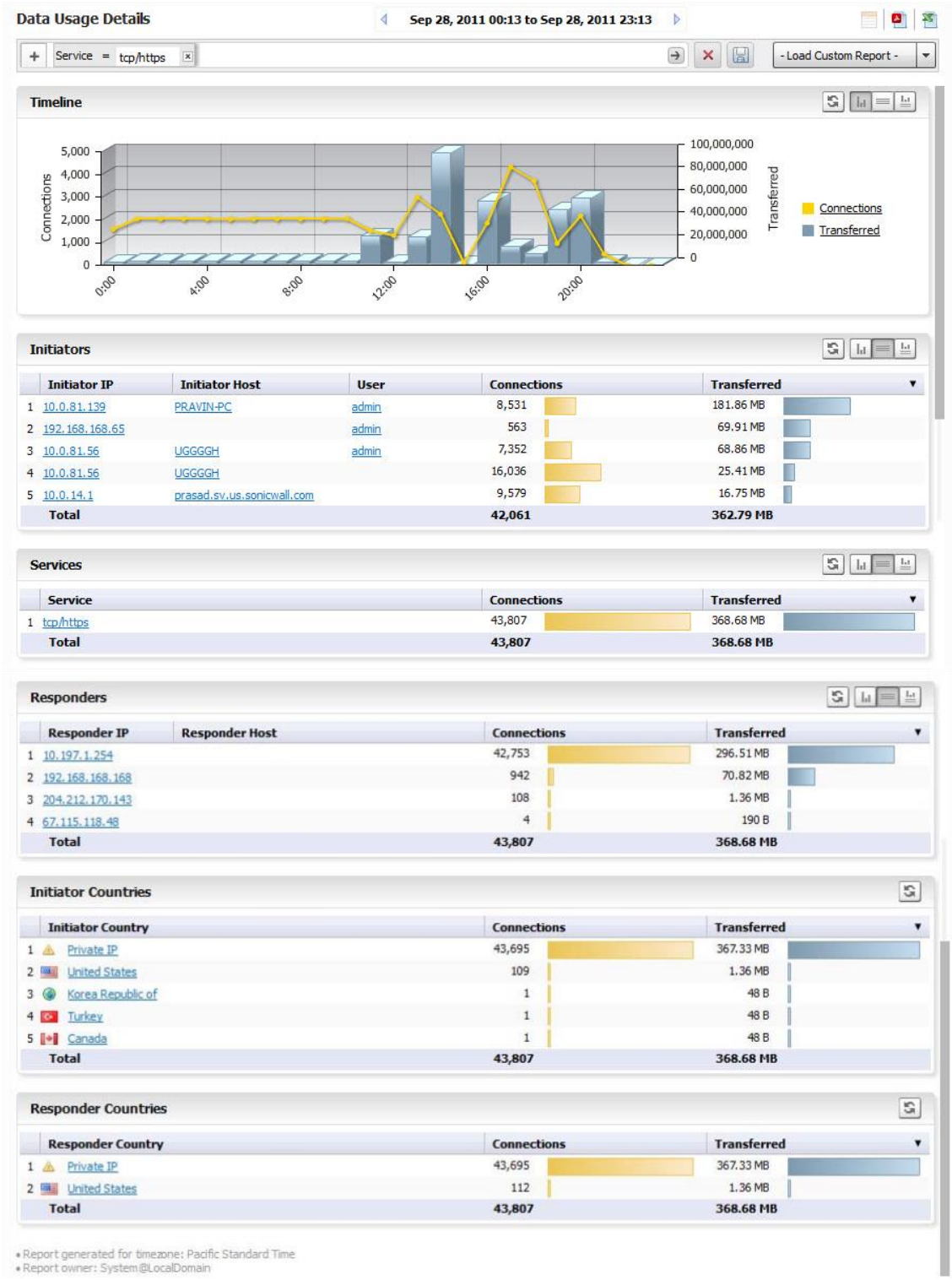


2 Click on a hyperlinked Time to go to the Detail view of the Report. The Detail view contains multiple sections, including Initiators, Responders, Service types, Initiator Countries, and Responder Countries. Depending on the number of entries, you might need to scroll down to see all the sections.

NOTE: You can also apply a filter through the Filter Bar or by right-clicking the entry. Select the filter and click Go. The Report shows the detail view applicable to that filter.

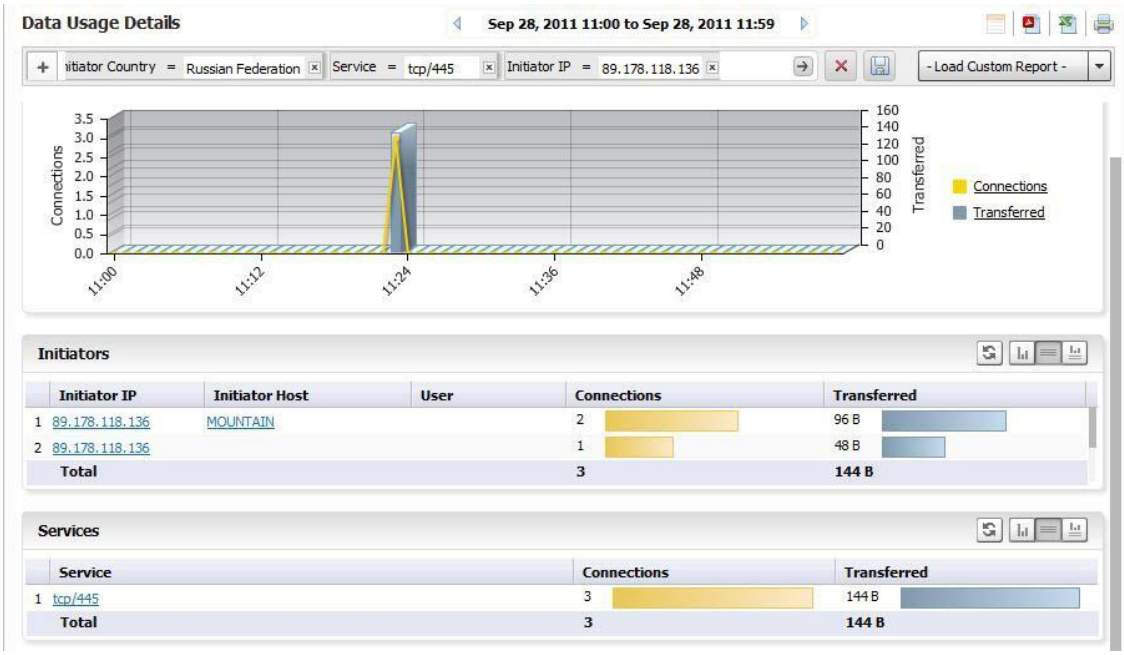


3 To further filter the output, to view only tcp/https usage, click on the tcp/https entry under **Services**. A **Detail** report, filtered to show only usage of tcp/https, comes up. Notice that a Service entry has been added to the Filter Bar.



Notice that the Report now focuses on the filter constraint from the drilled-down column.

Because this report also contains drill-down areas, you can drill down even further to add additional constraints to the results.



> **NOTE:** Many report categories contain a Details item in the list of reports. This link provides a shortcut directly to the Detail view of all sub-sections of the report. You can apply filters directly to the Detail view to further constrain the displayed information.

The Log Analyzer provides the most detailed Report information.

4 To view the Log Analyzer, go to the **Reports** tab after you have drilled down to the desired level of detail and click on **Analyzers > Log Analyzer**.

> **NOTE:** Because Log Analyzer Reports can contain a very large amount of data, you might wish to limit the amount of data displayed on the page. The amount of data in the report can also affect the loading speed.

The Log Analyzer contains information about each connection, including port and interface information, number of Bytes sent, and so on.

You can drill down through the Log Analyzer Report as well. Clicking on a column item adds an additional filter and narrows down your results, allowing you to zoom in on specific instances.

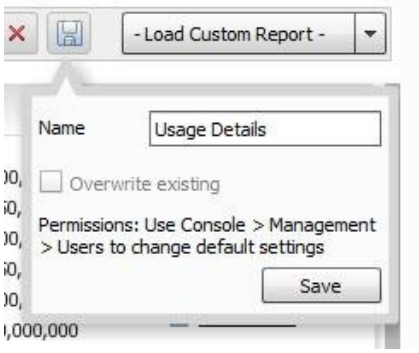
Some Log Analyzer reports can be reached as the final step of a drill-down process.

Click on a row to expand the log, additional information can be viewed here:

The bottom bar of the Log Analyzer contains a page bar, which allows you to navigate through the report by paging forward and backward, or going to the specific page of interest.

Custom Reports

Specific customized reports can be generated and saved by means of the **Save** icon. Click **Save** to bring up a drop-down allowing you to save a custom report.



This menu is pre-filled with a name reflecting the report it was based on. If an earlier report with this name was generated, you can choose to overwrite it or save a new copy, or assign it a different name.

The new Custom report is added to the drop-down menu accessed when you click **Load Custom Report**. It is also added to the Reports Tab list under Custom. When a specific Custom report is selected on the Load Custom Report drop-down menu, the button reflects the name of that report.

Custom Reports can also be accessed or deleted by going to **Reports > Custom > Manage Reports**.

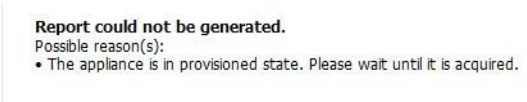
Troubleshooting Reports

One of the most common reasons when a report does not display is that no data is available for the selected appliance. There are several reasons why you might see this error. Analyzer displays the most likely reason(s) and gives you instructions for ways to resolve the problem.

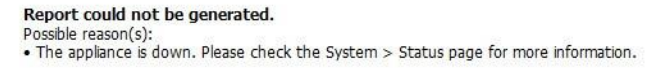
The most common examples are as follows:

Appliance is in a Provisioned State:

Analyzer is waiting for a handshake response signal from the appliance. Generally, the TreeControl menu also flags the appliance with a lightning bolt on a yellow background.



Appliance is Down



No Matching Records Found

There might be no data available for a variety of reasons. The most common causes are listed in this message, along with actions to take.

Managing Analyzer Reports on the Console tab

There are management settings for the Analyzer Reporting Module on the Analyzer **Console** tab. A Reports selection is available on the left menu bar, which allows you to set up certain tasks in the right Management pane that contains limited configuration screens, used for managing scheduled email report configuration, system debug-level logging, and show legacy reports.

In this pane, you can set Summarizer parameters and schedule emailing or archiving of reports.

Data deletion or storage specified in these menus takes place after completion of the current reports run.

Reports generated by pre 8.0 releases of Dell SonicWALL Analyzer can still be viewed, but require specific configuration. See Managing Legacy Reports on page 154.

7

Managing Firewall Reports

This chapter describes how to generate reports using the Dell SonicWALL Analyzer Reporting Module. The following section describes how to configure the settings for viewing reports:

Firewall Reporting Overview

The Reports available under the Firewall tab provide specific information on data gathered by the Dell SonicWALL Analyzer interface.

For a general introduction to reporting, see Dell SonicWALL Analyzer Reporting Overview on page 56.

The Firewall reports display either summary or unit views of connections, bandwidth, uptime, intrusions and attacks, and SMA usage, displayed in a Data Container. Information can be viewed in either chart (timeline or pie chart) form, or tabular (grid) format. The list of available reports allows you to navigate to a high-level or specific view.

All of the reports in Analyzer report on data gathered on a specific date or range of dates. Data can be filtered by time constraints and data filters.

Benefits of Firewall Reporting

Firewall Reports allow you to access both real-time and historical reports and view all activity on SonicWALL Internet security appliances. By monitoring network access, logins, and sites accessed, you can enhance system security, monitor Internet usage, and anticipate future bandwidth needs.

You can gain more information from the display, simply by hovering the mouse pointer over certain sections. Additionally, by clicking on selected sections of a pie chart or bar-graph timeline view, you can view more information or view different aspects of the information presented.

Firewall Reports Tab

The Firewall tab gives you access to the Firewall's reports section of the Dell SonicWALL Analyzer management interface. Reporting supports both graph and non-graph reports, and allows you to filter data according to what you wish to view. It supports multiple product-licensing models.

Firewall Reports provide the following features:

- Clickable reports with drill-down support on data rows
- Report data filtering through the Search Bar
- Log Analyzer

You can view Reports either as Summary reports for all or selected units on the Dell SonicWALL Analyzer network, or view detailed reports for individual units.

Viewing Available Firewall Report Types

To view the available types of reports for the Firewall appliances, complete the following steps:

1. Log in to your Analyzer management console.
2. Click the **Firewall** tab.
3. Select an appliance or global view from the TreeControl.
4. Expand the desired selection on the Reports list and click on it.

   NOTE: All Reports show a one-day period unless another interval is specified in the Time Bar.

The following types of reports are available:

Global Level Reports:

- Data Usage
  - Summary: connections, listed by appliance, for one day (default)
- Applications
  - Summary: connections, listed by application, for one day (default)
- Web Activity
  - Summary: hits, listed by appliance, for one day (default)
- Web Filter
  - Summary: access attempts, listed by appliance, for one day (default)
- VPN Usage
  - Summary: VPN connections, listed by appliance, for one day (default)
- Threats
  - Summary: connection attempts, listed by appliance, for one day (default)

  NOTE: Summary Reports are not drillable and no Detail view is available.
- Real-Time Viewer
  - Summary: Syslog

Unit Level Reports

Detail views are available for all Report items unless otherwise noted.

- Data Usage
  - Timeline: connections for one day (default)
  - Initiators: Top Initiators, listed by IP address, Initiator Host, Initiator MAC, User, Connections, and total Transferred, displayed as a pie chart

    - Responders: Top Responders, listed by IP address, Responder Host, Responder MAC, Connections, and total amount Transferred, displayed as a pie chart
    - Services: connections, listed by service protocol, displayed as a pie chart
    - Details: provides a shortcut to the Detail view normally reached by drilling down. Detail sections include: Initiator IPs, Initiator Host, Initiator MAC, Users, Connections, total amount transferred, Services, Responders, Initiator Countries, and Responder Countries. Additional filtering/drilldown takes you to the Log Analyzer
- Applications
    - Data Usage connections, listed by application and threat level
    - Detected: events, listed by application and threat level
    - Blocked: blocked events, listed by application and threat level
    - Categories: types of applications attempting access
    - Initiators: events displayed by Initiator IP and Initiator host
    - Timeline: events over one day
- User Activity
    - Details: a detailed report of activity for the specified user
- Web Activity
    - Categories: hits and browse time listed by information category
    - Sites: sites visited by IP, name, and category, with hits and browse time
    - Initiators: Initiator IP, Initiator Host, Initiator MAC, with User, Browse Time, Hits, and total amount transferred
    - Timeline: site hits with time of access and browse time
    - Details: provides a shortcut to an access timeline and Detail view normally reached by drilling down. Detail sections include: Categories, Sites, and Initiators.
- Web Filter
    - Categories: hits and browse time listed by information category
    - Sites: sites visited by IP, name, and category, with hits and browse time
    - Initiators: Initiator host and IP with category and user
    - Timeline: site hits with time of access and browse time
    - Details: provides a shortcut to an access timeline and Detail view normally reached by drilling down. Detail sections include: Categories, Sites, and Initiators.
- VPN Usage
    - Policies: lists connections by VPN Policy
    - Initiators: Initiator host and IP with category and user
    - Services: Top VPN Services by Service Protocol
    - Timeline: VPN connections over a 1 day period
- Intrusions
    - Detected: number of intrusion events by category
    - Blocked: blocked intrusions and number of attempts at access
    - Targets: number of intrusion events by target host and IP
    - Initiators: Initiator host and IP with category and use
    - Timeline: intrusions listed by time of day

    - Details: provides a shortcut to an access timeline and Detail view normally reached by drilling down. Detail sections include: Categories, Sites, and Initiators.
    - Alerts: provides a list of intrusion alerts
- Botnets
    - Initiators: Initiator host and IP with category and use
    - Responders:
    - Attacks:
    - Timeline: Intrusions listed by time of day
- Geo-IP
    - Responder Countries: Blocked traffic that is based on the traffic's country of origin or destination
    - Initiator Countries:
- Capture ATP
    - Status - files scanned in the last 30 days with applicable filters
    - Summary
    - Blocked - virus attacks blocked by Capture ATP and the number of attempts at access
- Gateway Viruses
    - Blocked: blocked virus attacks and number of attempts at access
    - Targets: targeted hosts and IP addresses
    - Initiators: initiating users, hosts, and IP addresses of the virus attack
    - Timeline: times when the virus attempted to gain access, displayed over time
    - Details: provides a shortcut to an access timeline and Detail view normally reached by drilling down. Detail sections include: Categories, Sites, and Initiators.
    - Alerts: provides a list of virus alerts
- Spyware
    - Detected: spyware detected by the firewall
    - Blocked: spyware blocked by the firewall
    - Targets: targeted hosts and IP addresses
    - Initiators: initiating users, hosts, and IP addresses of spyware download
    - Timeline: times when the spyware accessed the system, displayed over time
    - Details: provides a shortcut to an access timeline and Detail view normally reached by drilling down. Detail sections include: Categories, Sites, and Initiators.
    - Alerts: provides a list of spyware alerts
- Attacks
    - Attempts: type of attack and times access was attempted
    - Targets: host and IP address, and number of times access was attempted
    - Initiators: top attack initiators by IP and host
    - Timeline: time and number of attempts at access, displayed over time
- Authentication: authenticated users, their IP addresses, and type of login/logout
    - User Login
    - Admin Login
    - Failed Login

- Up/Down Status
    - Timeline: provides a timeline of unit availability. No Detail sections are available.
- Custom Reports: allows access to saved custom reports
- Analyzers
    - Log Analyzer: provides a detailed event-by event listing of all activity. The Log Analyzer is drillable, but no Detail sections are available.
- Flow Activity
    - Real-Time Viewer: real-time data displayed graphically.
    - Top Flows Dashboard: displays top flows per report type.
    - Flow Analytics: monitors applications, users, URLs, initiators, responders, threats, VoIP, VPNs, devices, and contents.
    - Flow Reports: real-time reports displayed graphically.

Understanding the Data Container

The Report contains a filter bar at the top, plus the actual Data Container. The default Data Container contains an interactive chart view that contains either a grid view, containing a text version of the information. One or more sections might be present in the grid view. Toggle buttons allow you to display the Chart view, Grid view, or Chart and Grid view.

Grid sections are arranged in columns. Columns can be rearranged to view them from the top down or bottom up, by clicking the up and down arrows in the column headings. You can narrow results by applying a filter to a column: right-click on a column heading and click **Add Filter**.

Hypertext-linked columns are drillable, meaning you can click on the hypertext entry to bring up a Detail view with more information on the desired entry. Detail views might have multiple sections.

The Detail views are usually reflected in the sub-headings under the Reports list that provide a shortcut directly to the Detail Report. To go to the full Detail view, click the Details entry in the Reports list. From the Detail view, you can access the system logs, for event-by-event information, or further filter the results. For more information on using the Log Analyzer to view and filter syslog reports, see Using the Log Analyzer on page 106.

Details views can contain multiple sections. To determine if you have reached the end of the list of sections, check for the time zone message that indicates the end of the Detail View.

Reports with hyperlinked columns can be filtered on the column or by drilling down on the hyperlinked entry.

You can also get to a filtered Detail view by clicking the section representing the desired information in the pie chart.

To save a filtered view for later viewing, click **Save** on the Filter Bar. The saved view now appears under Custom Reports.

To learn more about Custom reports, see Custom Reports on page 106.

How to View Firewall Reports

The Firewall Summary reports display an overview of bandwidth, uptime, intrusions and attacks, and SMA usage for managed SonicWALL Firewall appliances. The security summary report provides data about worldwide security threats that can affect your network. The summaries also display data about threats blocked by the SonicWALL security appliance.

The sections contain the following information:

- Node information — Information on the firewall(s) is displayed at the global or unit level.

- Syslog Categories — The types of syslog data selected to be collected for the selected appliance.
- Syslog Servers — The IP address and Port number of the syslog servers configured to collect data from the selected appliance.
    - Synchronize Appliance Information with Analyzer — Click the **Synchronize Appliance Information Now** link to refresh status data about the monitored appliances. This status information is normally updated every 24 hours.
- Getting Started With Analyzer — Click the **Open Getting Started Instructions In New Window** link to open the Analyzer installation and initial configuration instructions in a separate window.

Viewing Global Summary Reports

Summary reports for data usage, applications, web usage and filtering, VPN usage, and threats for managed SonicWALL appliances are available at the global level, through the TreeControl menu. Summary reports are available for:

- Data Usage
- App Control
- Web Usage
- Web Filtering
- VPN Usage
- Threats

Group-level Summary reports provide an overview of information for all Firewalls under the group node for the specified period. The report covers the connections and transfers by appliance for Data Usage, App Control, and VPN Usage, For Web Usage and Web Filters, hits are also included. Web filters and Threats list attempts at connection. Unless specified differently in the Date Selector, the Summary report covers a single day. Global Summary reports are not drillable.

The Dashboard Summary report displays statistics, alerts, graphical summary reports, and a list of available custom report templates. Displayed statistics can include total bandwidth, total attacks and other measurable information. The alerts list is displayed when the configured threshold has been reached. A wide range of graphical reports are also available for display.

You can configure the **Dashboard > Summary** report contents in the **Firewall > Configuration > Settings** page.

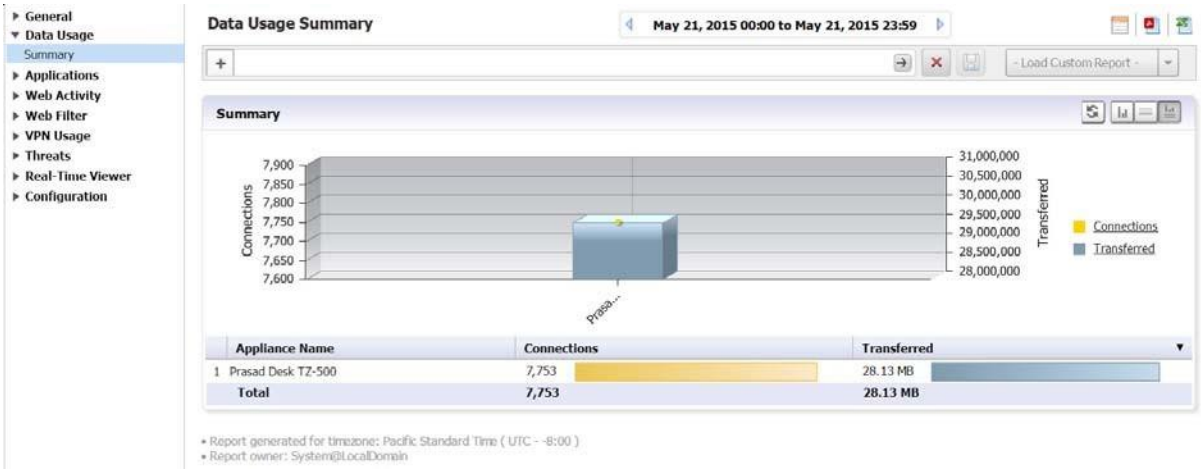
To view the Summary report, complete the following steps:

1 Click the **Firewall** tab.

2 Select the global icon.

3 Click **Data Usage > Summary**.

The timelines at the top of the page display the totals, and the grid section sorts the information by appliance or applications.



Unit level reports display status for an individual SonicWALL appliance.

Viewing Unit Level Status Reports

Unit level reports display status for an individual SonicWALL appliance. From this information, you can locate trouble spots within your network, such as a SonicWALL appliance that is having network connectivity issues caused by the ISP. You can also monitor web usage, including attempts to reach filtered sites, as well as incoming attacks on your network.

NOTE: Global reports are displayed in Analyzer's timezone. Reports for individual SonicWALL security appliances are displayed in the individual appliance's time zone.

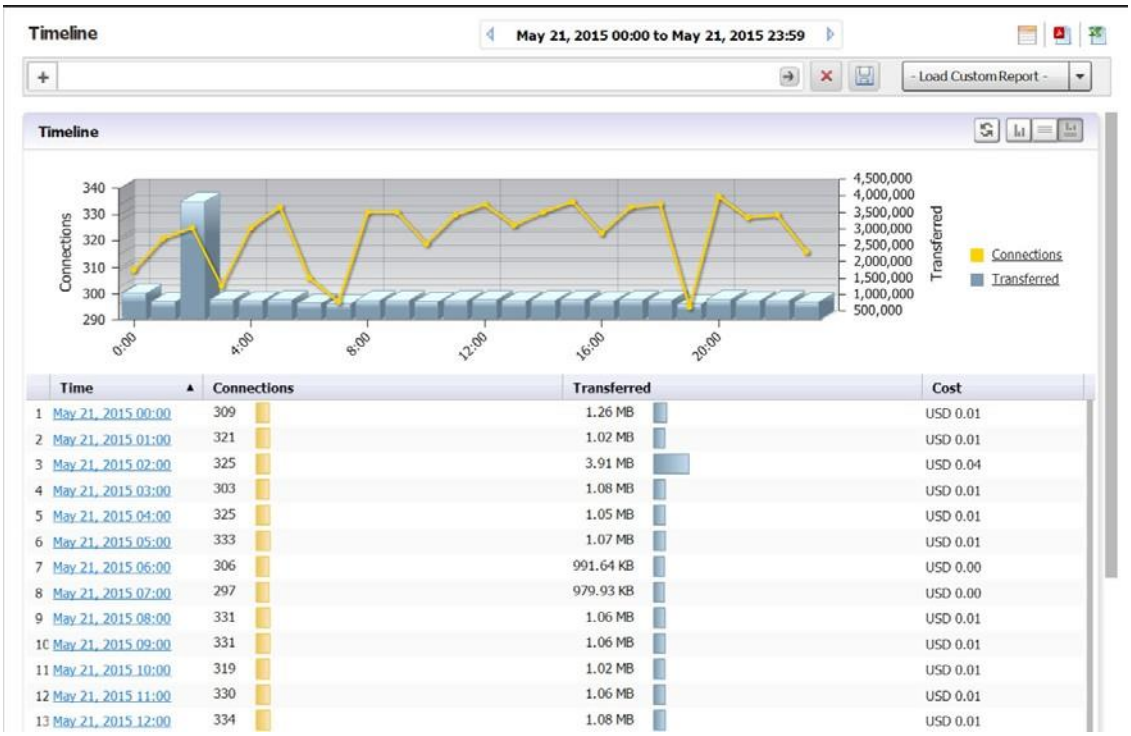
Viewing Data Usage Reports

The default Data Usage report displays a timeline for hours that the selected SonicWALL appliance was online and functional during the time period with connections, transferred connections, and cost displayed.

To view data usage reports, complete the following steps:

1. Click the **Firewall** tab.
2. Select the global icon or a SonicWALL appliance.

3 Click **Data Usage** > **Timeline**. (This is the default view when the Firewall Report interface comes up.)



This report is drillable. Click on an Initiator IP entry to break the Timeline report down into its Detail View report groups for the selected IP address. These groups also contain drillable hyperlinks that takes you to more specific Detail View information. The columns can also be filtered.

Viewing Applications Reports

Applications Reports provide details on the applications detected and blocked by the firewall, and their associated threat levels.

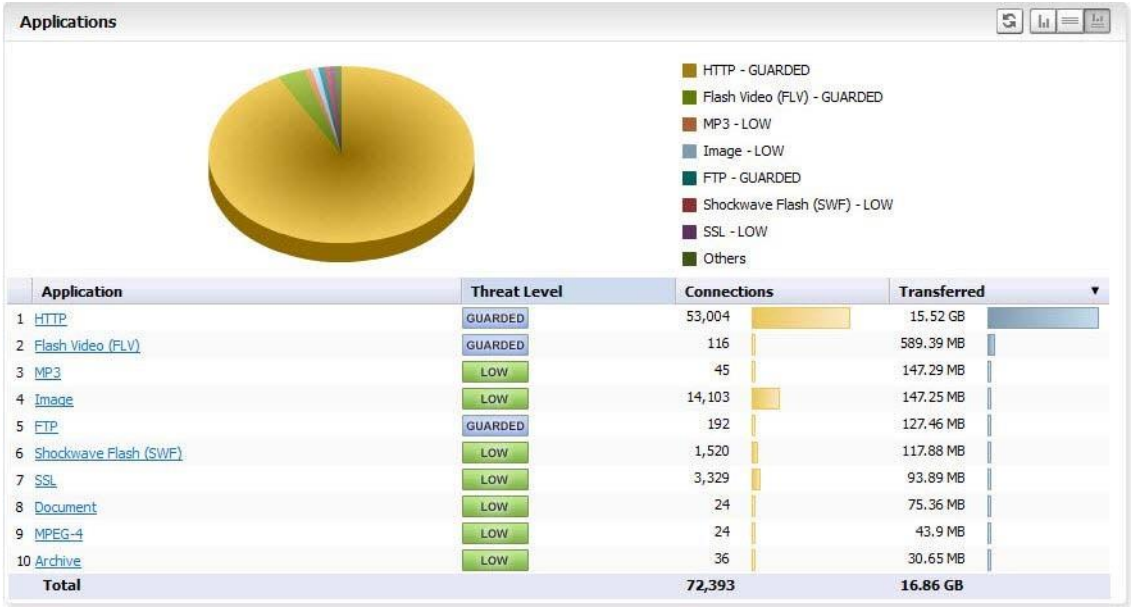
To view Application reports, complete the following steps:

1 Click the **Firewall** tab.

2 Select a SonicWALL appliance.

3 Click **Applications** > **Data Usage**.

The Applications Report displays a pie chart with the application and threat level it poses.



	Application	Threat Level	Connections	Transferred
1	HTTP	GUARDED	53,004	15.52 GB
2	Flash Video (FLV)	GUARDED	116	589.39 MB
3	MP3	LOW	45	147.29 MB
4	Image	LOW	14,103	147.25 MB
5	FTP	GUARDED	192	127.46 MB
6	Shockwave Flash (SWF)	LOW	1,520	117.88 MB
7	SSL	LOW	3,329	93.89 MB
8	Document	LOW	24	75.36 MB
9	MPEG-4	LOW	24	43.9 MB
10	Archive	LOW	36	30.65 MB
	Total		**72,393**	**16.86 GB**

You can drill down for additional Details views on connections over time (Timeline view), Data Usage, Detected applications, Blocked applications, Categories of applications, top initiators.

Viewing User Activity Logs

Web User Activity logs allow you to filter results to view only the activity of a specific user.

The User Activity Analyzer provides a detailed report listing activity filtered by user. If a user report has been saved previously, bringing up the User Activity Analyzer displays a list of saved reports under the Filter Bar.

If you wish to create a new report, use the Filter Bar to create a new report.

To view User Activity Logs, complete the following steps:

1 Click the **Firewall** tab.

2 Select a SonicWALL appliance.

3 Click on **User Activity > Details** to bring up the **User Activity Analyzer**. The User Activity Analyzer generates a Detail report based on the user name.

If no user activity reports were saved, only the Filter Bar displays, with the User filter pre-selected. You can enter a specific user name, or use the LIKE operator wildcards (*) to match multiple names.

4 Enter the name of the user into the field and click **Go** (arrow) to generate the report

The customized User Activity Details report displays a timeline of events, Initiators, Responders, Services, Applications, Sites visited, Blocked site access attempted, VPN access policy in use, user authentication, Intrusions, Initiator Countries, and Responder Countries associated with that particular user.

Data for a particular user cannot be available for all of these categories.

Viewing Web Activity Reports

Web Activity Reports provide detailed reports on browsing history.

To view Web Activity Reports, complete the following steps:

1. Click the **Firewall** tab.
2. Select a SonicWALL appliance.
3. Click **Web Activity > Categories**.

   The Web Activity Report displays a pie chart with the Top Categories of type of access, total browse time, and hits.

You can drill down for additional Details views on connections over time (Timeline view), Sites visited, Categories of sites, and Top Initiators. A Details entry links directly to the details view of all entries.

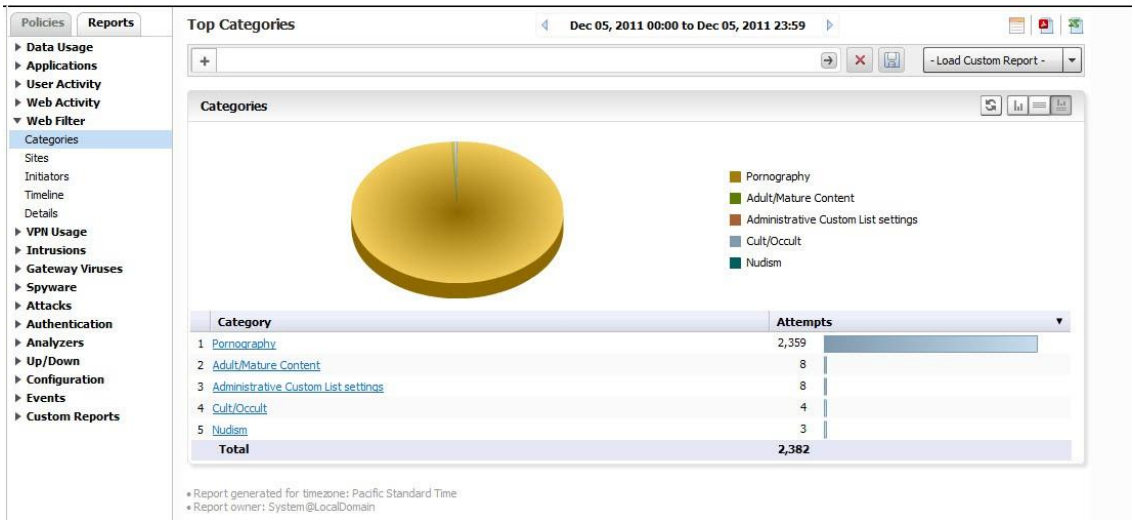
Viewing Web Filter Reports

Web Filter Reports provide detailed reports on attempts to access blocked sites and content.

To view Web Filter Reports, complete the following steps:

1. Click the **Firewall** tab.
2. Select the global icon or a SonicWALL appliance.
3. Click **Web Filter > Categories**.

   The Web Filter Report displays a pie chart with the Top Categories of blocked access and total attempts to access.



You can drill down for additional Details views on connections over time (Timeline view), Sites visited, Categories of sites, and Top initiators. A Details entry links directly to the details view of all entries.

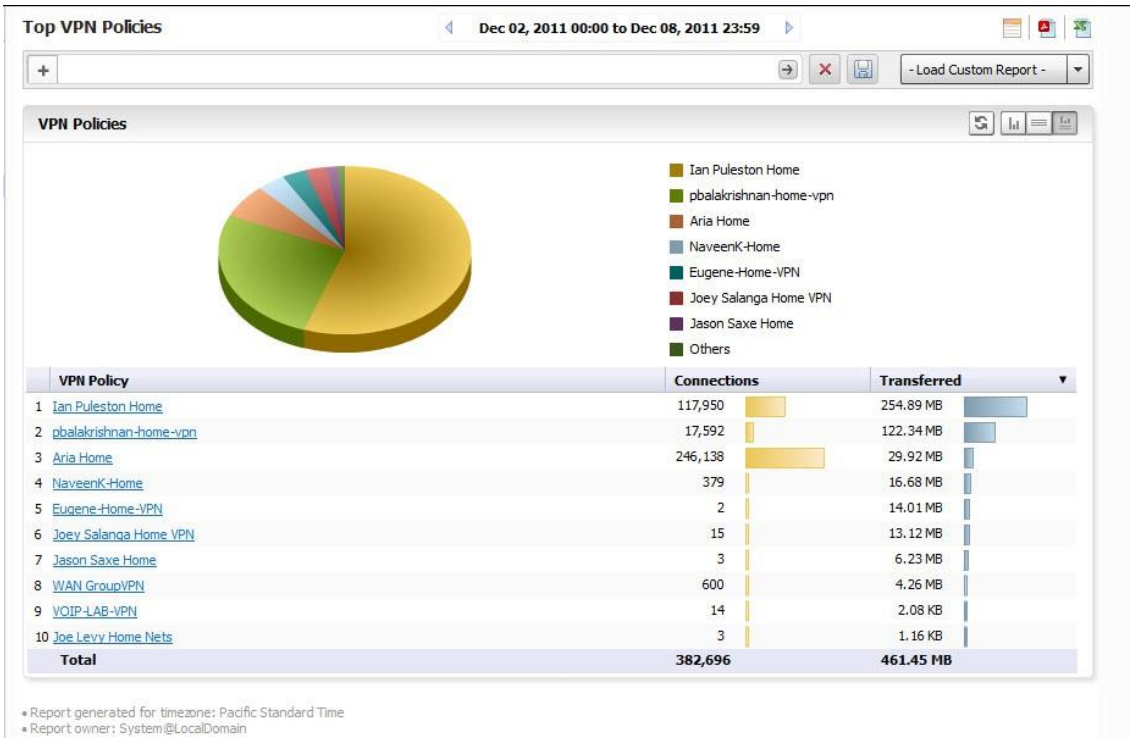
Viewing VPN Usage Reports

VPN usage reports provide details on the services and policies used by users of virtual private networks.

To view VPN Usage reports, complete the following steps:

1. Click the **Firewall** tab.
2. Select a SonicWALL appliance.
3. Click **VPN Usage > Policies**.

   The VPN Usage Report displays total connections for each VPN Policy item as a pie chart and tabular grid view.



You can drill down for additional Details views on Service protocols and Top initiators.

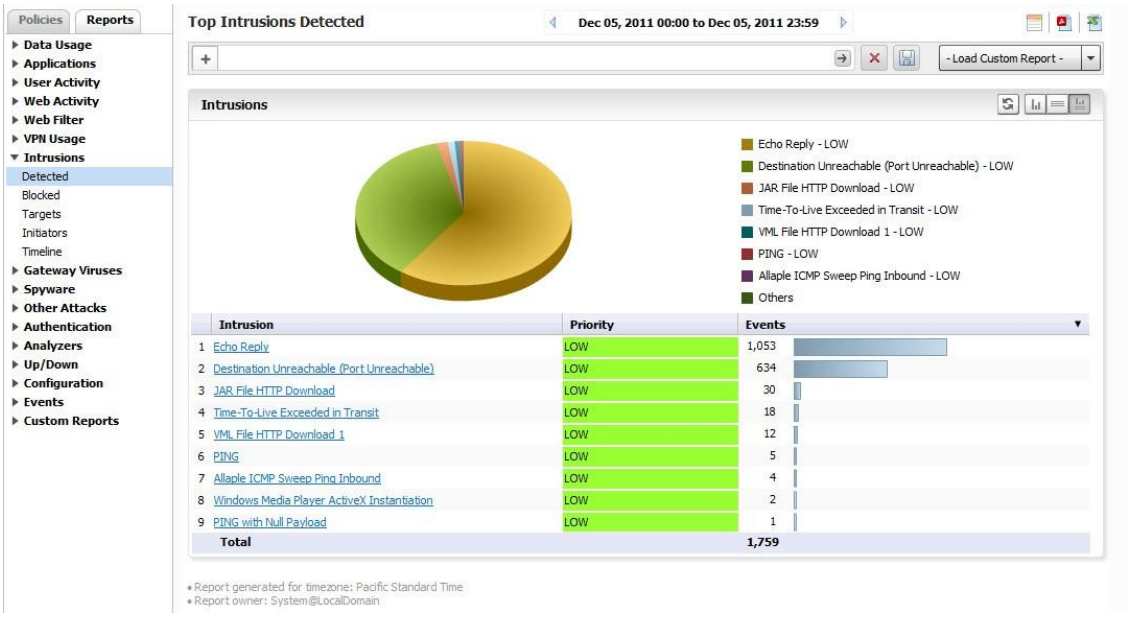
Viewing Intrusions Reports

Intrusion Reports provide details on types of intrusions and blocked access attempts.

To view Intrusion Reports, complete the following steps:

1. Click the **Firewall** tab.
2. Select a SonicWALL appliance.
3. Click **Intrusions > Detected**.

The Attacks report provides a pie chart and a list of the initiating IP addresses, hosts, and users, with number of attempts for each.



Drill down for additional Detail views of Intrusion Categories, Targets, Initiators, Ports affected, Target Countries, and Initiator Countries.

Viewing Botnet Reports

Botnet reports provide details on the botnet attempts that were blocked when attempting to access the firewall.

To view Botnet Reports, complete the following steps:

1 Click the **Reports** tab.

2 Select a SonicWALL appliance.

3 Click **Botnet > Initiators**.

The top botnet attacks report appears. The Initiators report provides a pie chart and a list of the initiating IP addresses, countries, hosts, and events, with number of attempts for each.

Drill down for additional detailed views of Attacks, Targets, Initiators, Ports affected, Initiator Countries, and Target Countries.

Viewing Geo-IP Reports

Geo-IP reports provide details on the botnet attempts that were blocked when attempting to access the firewall.

To view Geo-IP Reports, complete the following steps:

1 Click the **Reports** tab.

2 Select a SonicWALL appliance.

3 Click **Geo-IP > Initiator Countries**.

The top Geo-IP initiator report appears. The Initiators report provides a pie chart of threat initiator countries blocked and events, with number of attempts for each.

Drill down for additional detailed views of Initiator IPs, Hosts, Initiator MACs, Users, and Events.

Viewing Capture ATP Status

The Capture Advance Threat Protection (ATP) reports provide details on whether a file is malicious or not by transmitting the file to the cloud where the Dell SonicWALL Capture ATP service analyzes the file to determine if it contains a virus or other malicious elements.

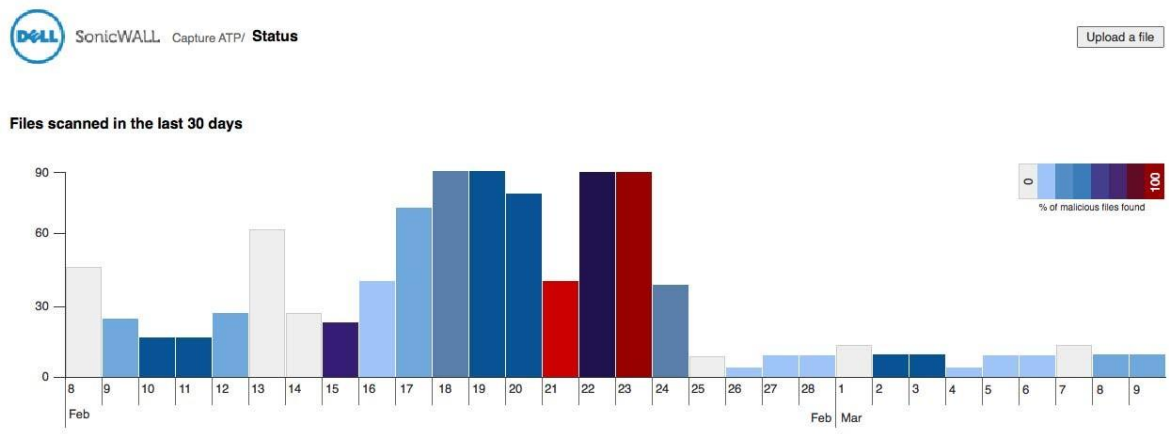
NOTE: A Capture ATP service license is required to use the Capture ATP features. Before you can enable Capture ATP, the Gateway Anti-Virus and Cloud Anti-Virus Database services must be enabled in Analyzer.

Topics:

- Viewing the graph and log table on page 90
- Filtering the log table on page 93

Viewing the graph and log table

The **Capture ATP > Status** page displays a graph and a log table that provide information for each file that has been scanned. Files can be uploaded to Capture ATP for scanning from this page by clicking the **Upload a file** button.



The graph shows the number of files scanned for each day. The X axis represents time and shows only the last 30 days. Each tick is one day. The Y axis represents the number of files scanned.

The percentage of malicious files found is represented by the color of each bar in the graph. The key shows the percentage that each color represents. Zero means no malicious files were found.

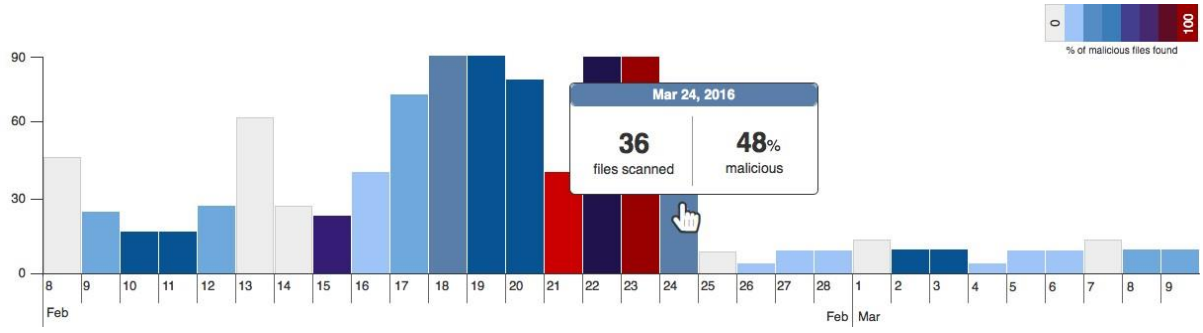
Below the graph, the log table shows information for each file that has been scanned. You can customize what is displayed in the log table, by clicking the Add filter… link. The graph, log table, and filters are bound, and any interactions on one will affect the others.

Viewing 1,859 files scanned.

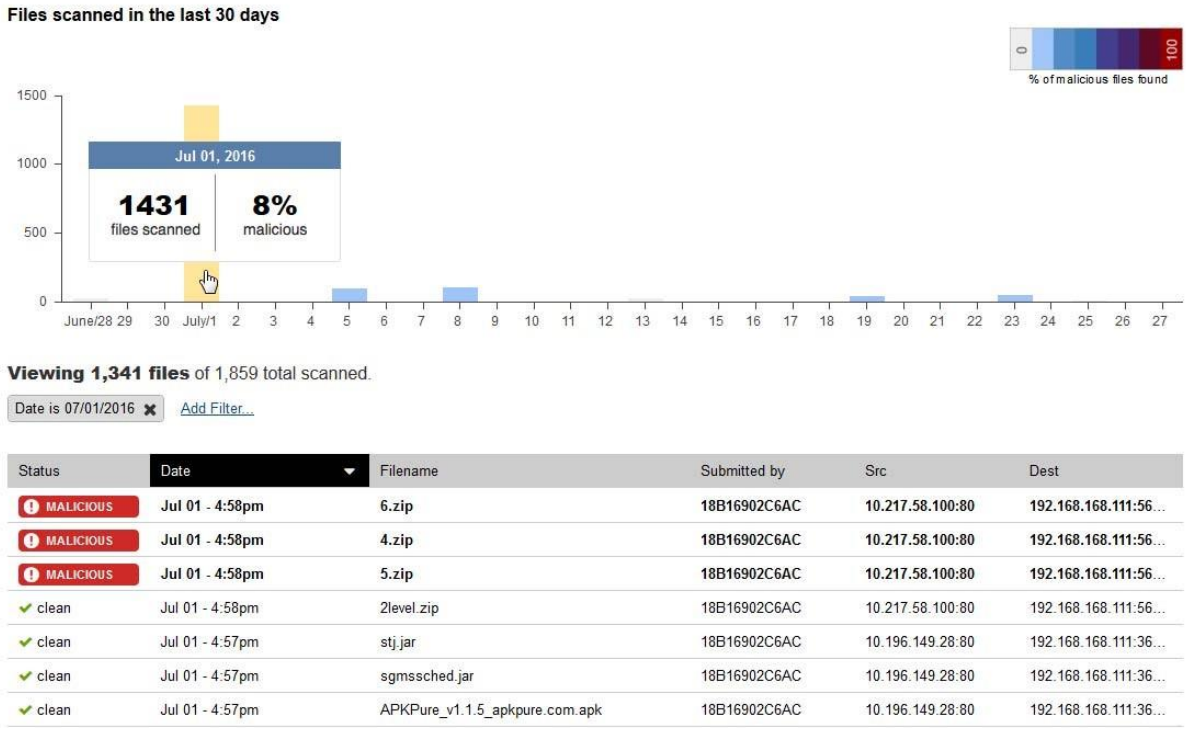
No filters applied. Add Filter...

Status	Date	Filename	Submitted by	Src	Dest
✔ clean	Jul 25 - 5:56pm	FileZilla_Server-0_9_57.exe	(uploaded)	127.0.0.1	127.0.0.1
✔ clean	Jul 24 - 10:08pm	s.jar	18B16902C6AC	10.217.58.100:80	192.168.168.9:3613
✔ clean	Jul 24 - 10:01pm	stj.zip	18B16902C6AC	10.217.58.100:80	192.168.168.9:2933
✔ clean	Jul 23 - 11:19am	vsjitdebugger.exe	18B16902C6AC	10.217.58.100:80	192.168.168.9:48726
✔ clean	Jul 23 - 11:19am	vssadmin.exe	18B16902C6AC	10.217.58.100:80	192.168.168.9:48727
✔ clean	Jul 23 - 11:19am	w32tm.exe	18B16902C6AC	10.217.58.100:80	192.168.168.9:48728
✔ clean	Jul 23 - 11:19am	waitfor.exe	18B16902C6AC	10.217.58.100:80	192.168.168.9:48729
✔ clean	Jul 23 - 11:19am	wecutil.exe	18B16902C6AC	10.217.58.100:80	192.168.168.9:48730
✔ clean	Jul 23 - 11:19am	wermgr.exe	18B16902C6AC	10.217.58.100:80	192.168.168.9:48731
MALICIOUS	**Jul 23 - 11:19am**	**test2.zip**	**18B16902C6AC**	**10.217.58.100:80**	**192.168.168.9:48716**
✔ clean	Jul 23 - 11:19am	test3.zip	18B16902C6AC	10.217.58.100:80	192.168.168.9:48717

When you hover over a bar, a popup shows the actual numbers of files scanned and malicious files found.



You can click on a single bar in the graph to set the filter for the log table to show the details of that bar only.



The log table allows you to scroll through the list of scanned files. If a scan fails, that row is dimmed. If a malicious file is found, that row is bolded. Clicking on any row opens the threat report. For more information about threat reports, see Viewing Threat Reports.

The heading for this page is dynamic and may appear in two states:

- When no filters are applied - Viewing n files scanned.
- When filters are applied - Viewing n files of n total scanned.

The columns for the log table are:

- The STATUS column displays these states:
  - scan pending - the scan is still in progress
  - clean - the scan has completed, but no judgment is confirmed yet
  - scan failed - the scan has failed
  - MALICIOUS - the scan has completed, and the judgment is malicious (the word MALICIOUS is displayed in small caps in a red tag with a warning symbol)
- The **Filename** column displays the name of the file.
- The **Date** column displays the date that the file was scanned.
- The **Submitted** by column displays the serial number of the firewall that submitted the file to Capture ATP.
- The **Src** column displays the source IP address where the file originated.
- The **Dest** column displays the destination IP address where the file was sent.

The columns can be sorted as follows:

- Currently, the Date column can be sorted in ascending or descending order.
- The default sort order is reverse chronological order with the most recent items on top.

- The heading for a sorted column has a black background with an arrow indicating the direction of the sort.
- Clicking the column heading sorts that column and toggles it in ascending or descending order.
- The selected sort order is persistent as filters are added or removed.

Filtering the log table

You can filter the entries in the log table by adding a filter that only displays certain criteria for a certain column, such as the status, date, or src, and so on.

To add a filter to the log table:

1 On the **Capture ATP > Status** page, click the **Add filter...** link.

The filter builder bar appears.

2 Select the criteria you want from the drop-down menus:

a From the first drop-down menu, select the column name, such as **Status**.

b From the second drop-down menu, select the operator: **is** or **is not**.

c From the third drop-down menu, select the appropriate criteria for the selected column.

3 Click **Add**.

The filter builder bar disappears, and a filter tag is created.

NOTE: Only one type of filter can be applied to the log table at a time.

The **Add Filter...** link reappears after the filter is added and the table results are updated immediately.

If you press **X**, the filter tag disappears and the filter is not applied to the log table.

Uploading a file for analysis

You can upload files to be scanned using the **Upload a File** button on the **Capture ATP > Status** page.

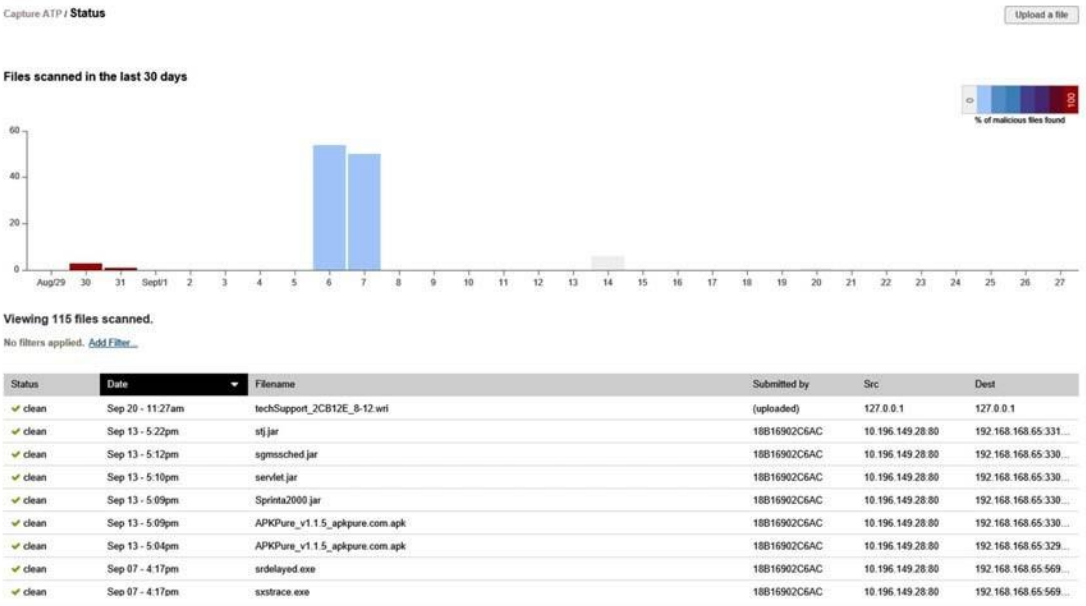
To upload a file for scanning, complete the following steps:

1 Click the **Firewall** tab.

2 Select a SonicWALL appliance.

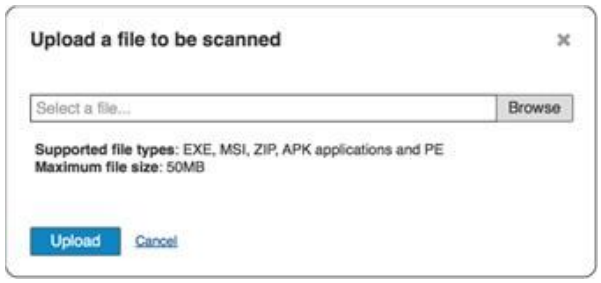
3 Click **Capture ATP > Status**.

The files scanned status report appears.



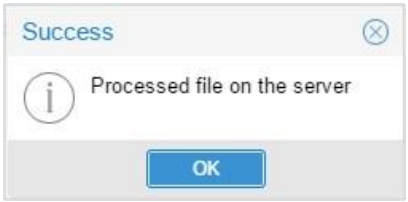
1 On the **Capture ATP > Status** page, click **Upload a File**.

The upload a file to be scanned dialog appears.

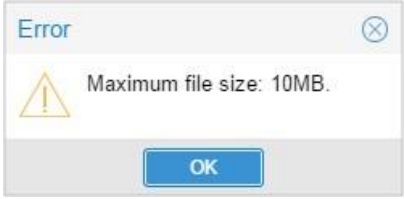


2 Click **Browse**, locate, and select the file you want to scan.

If the upload completes successfully, this message is shown:



If upload fails, an error message is displayed. If it fails because of file size limitations, you will see an error message similar to this:



Viewing threat reports

When you click on any row in the logs table on the **Capture ATP > Status** page, the Capture ATP threat report appears in a new browser window. The report format varies depending on whether a full analysis was performed or the judgment was based on preprocessing.

Topics:

Launching the threat report from the logs table

You can launch a threat report by clicking on any row in the logs table on the **Capture ATP > Status** page. Hovering your mouse pointer over a row highlights it, and you can click anywhere in the row to launch the threat report in a new browser window.

An exception exists for archives which do not contain any supported file types. In this case, no threat report is launched.

Viewing the threat report header

The report header is very similar among the various threat reports. This section describes the header components and variations.

Colored banner:

- The colored banner is red for a malicious file, and blue for a clean file.
- The top entry displays the date and time that the file was submitted to Capture ATP for analysis.
- Below the date and time, a summary of the result is displayed.

Lower banner:

- The lower part of the banner contains the connection information.
- On the left is the IP address (IPv4) and port number of the connection source. This is the address from which the file was sent.
- In the middle is the firewall identified by its serial number or friendly name.
- On the right is the IP address (IPv4) and port number of the connection destination. This is the address to which the file is being sent.

Viewing the threat report footer

The report footer is very similar among the various threat reports.

The File Identifiers are displayed at the left side of the footer. The following file identifiers are displayed, one per line:

- **MD5**
- **SHA1**
- **SHA256**

On the right side of the footer, the following information is displayed:

- **Serial Number** - This is the serial number of the firewall that sent the file. This is not displayed if the file was manually uploaded.
- **Capture ATP Version** - This is the software version number of the Capture ATP service running in the cloud.
- **Report Generated** - This is the timestamp in UTC format of when the report was generated.

Viewing the static file information

The static file information is displayed on the left side of the threat report, and is similar across all types of reports.

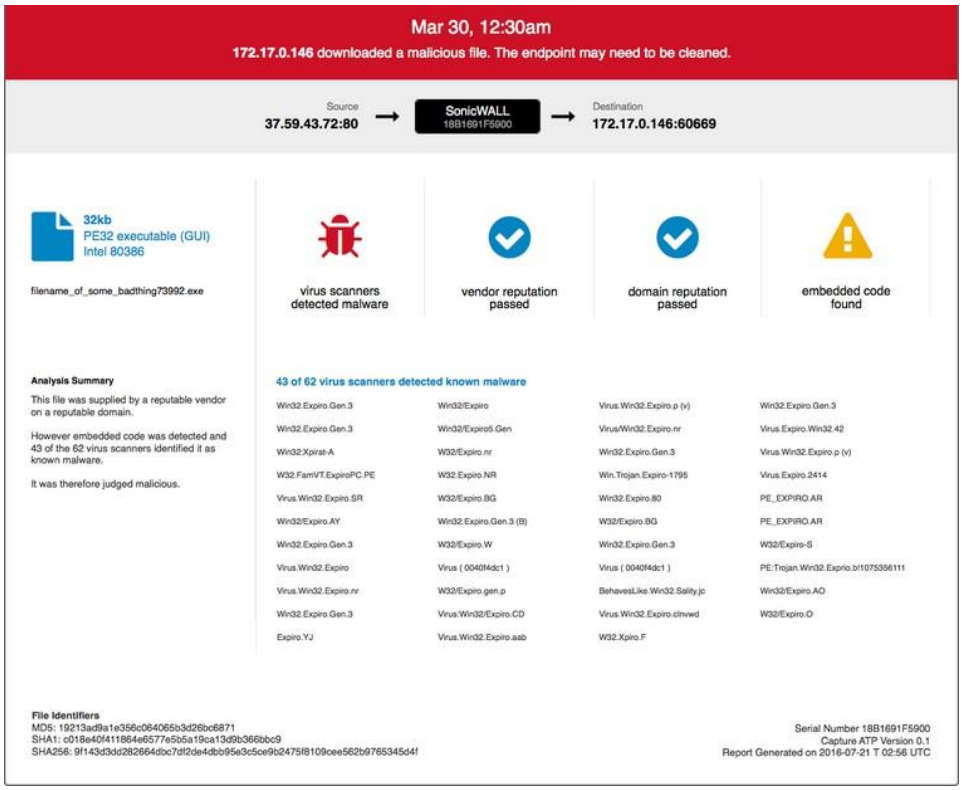
The file information includes:

- File size in kilobits (kb)
- File type
- File name as it was intercepted by the firewall

Viewing threat reports from preprocessing

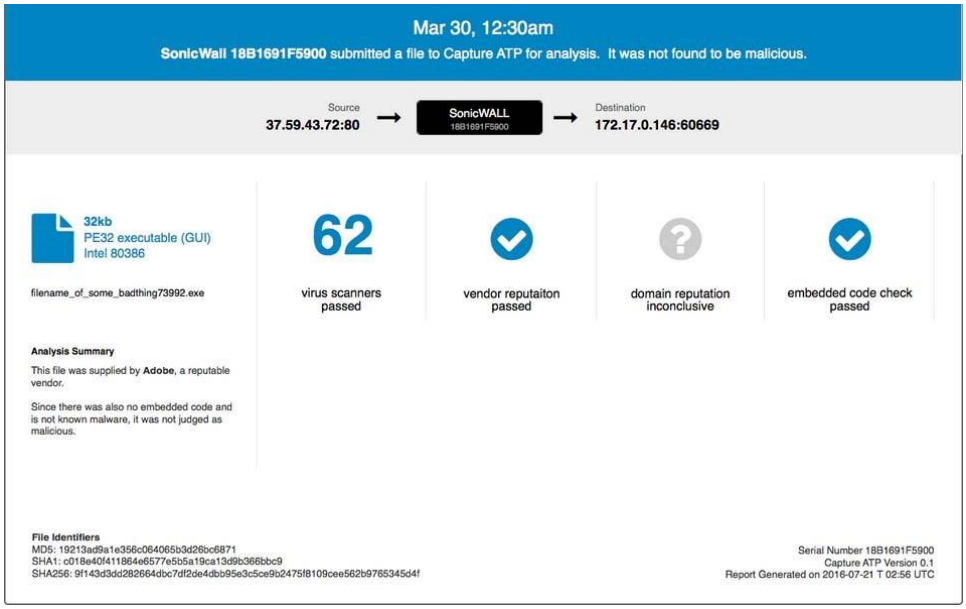
There are varying amounts of data on a preprocessor threat report, based on whether the file was found to be malicious or clean.

Preprocessor threat report for a malicious file:



The above threat report format is seen when the virus scans reveal malware in the file.

Preprocessor threat report for a clean file:



A clean threat report like the one shown above is seen in either of the following two cases:

Case one:

- Virus scans are inconclusive or all good.
- The file matches domain or vendor allow lists.

Case two:

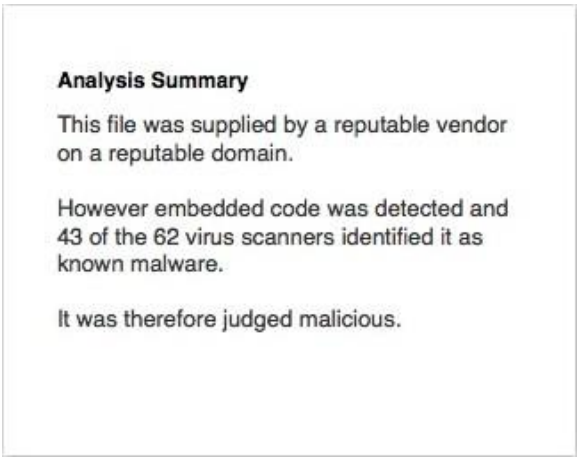
- Virus scans are inconclusive or all good.
- No embedded code is present in the file.

See the following topics for more information about preprocessor reports:

- Analysis summary and status boxes in preprocessor reports
- Malware names in preprocessor reports

Analysis summary and status boxes in preprocessor reports

Preprocessor threat reports contain an Analysis Summary section on the left side, which summarizes the findings based on the four phases of analysis during preprocessing.



The results from the four phases of preprocessing are displayed in the status boxes.

Each phase results in a true or false outcome. The following table shows what happens in the process depending on the result of each phase of the preprocessing.

Table 6. Four areas of preprocessor analysis

Preprocessor phase result	Virus scanners detect malware?	Vendor reputation - on Allow list?	Domain reputation - on Allow list?	Embedded code found in the file?
True	Malicious	**Non-malicious**	**Non-malicious**	Continue analysis
False	Continue analysis	Continue analysis	Continue analysis	**Non-malicious**

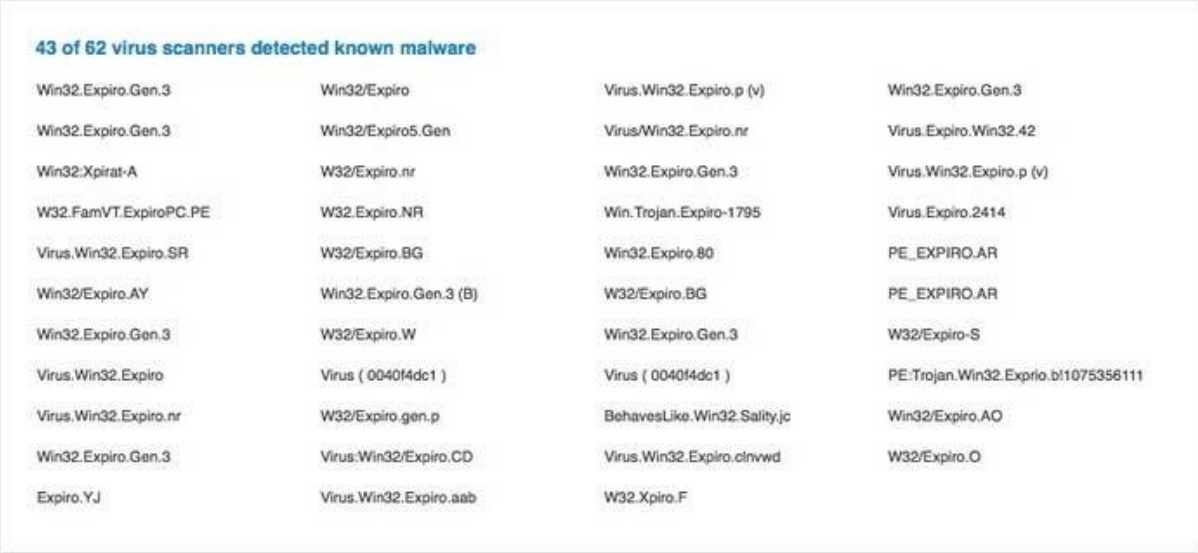
Some phase results trigger an immediate judgment of either Malicious or Non-malicious, as indicated in the above table. Otherwise, that phase ends with the “Continue analysis” state.

If all phases of preprocessing result in the “Continue analysis” state, the file is sent to the cloud for full analysis by Capture ATP.

NOTE: The vendor reputation filter is only applicable to PE files, and the domain reputation might not be available for files delivered over SMTP. In these cases, the “Continue analysis” state is the phase result.

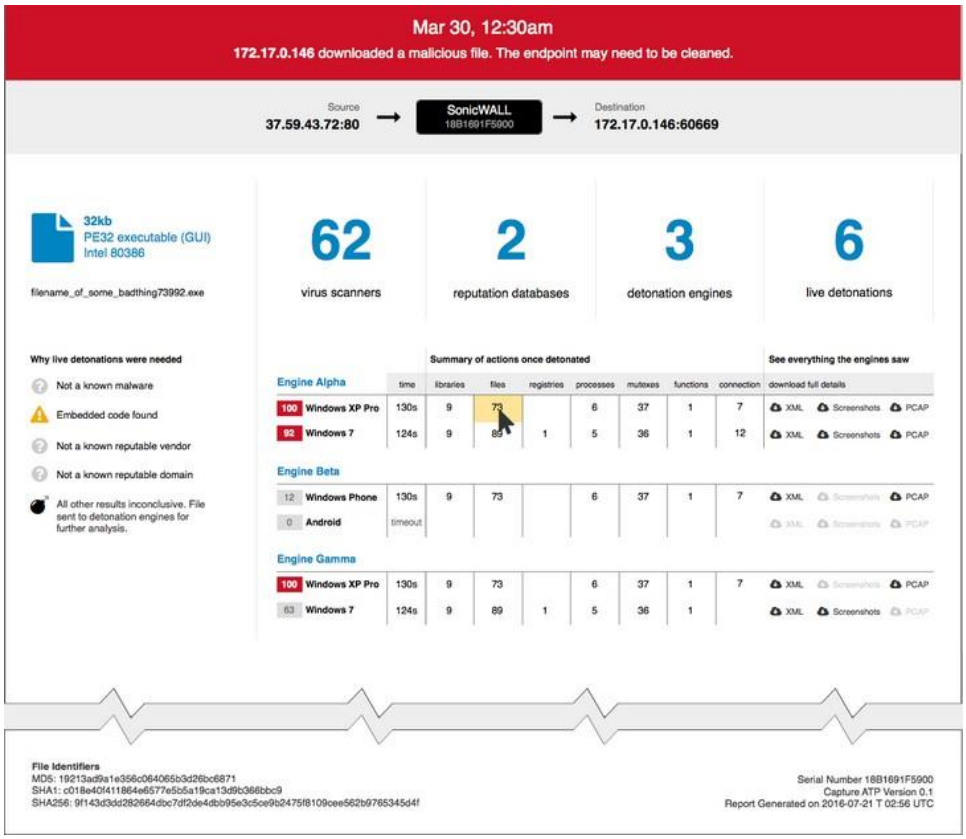
Malware names in preprocessor reports

If the virus scanners detect known malware in the file, all virus names are listed in the content area of the report.



Viewing threat reports from a full analysis

Full analysis threat reports provide the same set of information for both malicious and non-malicious files, although the banner color is different.



This Threat Report format is used when the following conditions occur:

- Virus scans are inconclusive or all good.
- Embedded code is present in the file.
- The file does not match domain or vendor allow lists.

See the following topics for more information about full analysis reports:

- Why live detonations were needed
- Status boxes in a full analysis threat report
- Analysis engine results tables

Why live detonations were needed

The left side of the full analysis threat report displays a summary of the preprocessing results as an explanation of why live detonations were needed. The term live detonations is used to indicate that one or more analysis engines and multiple environments were used to analyze the file in the cloud servers.

The set of preprocessing results which lead to full analysis of the file is shown below:

Status boxes in a full analysis threat report

The status boxes in full analysis threat reports display status from preprocessing results as well as information about the analysis performed in the cloud servers.

Virus scanners:

- This is the number of Anti-Virus vendors used, regardless of the judgment from each.
- SonicWALL Gateway Anti-Virus and Cloud Anti-Virus each count as one.
- Additional virus scanners from many AV products and online scan engines are included in the total.

Reputation databases:

- One is the vendors allowed list.
- One is the domains allowed list.

Detonation engines:

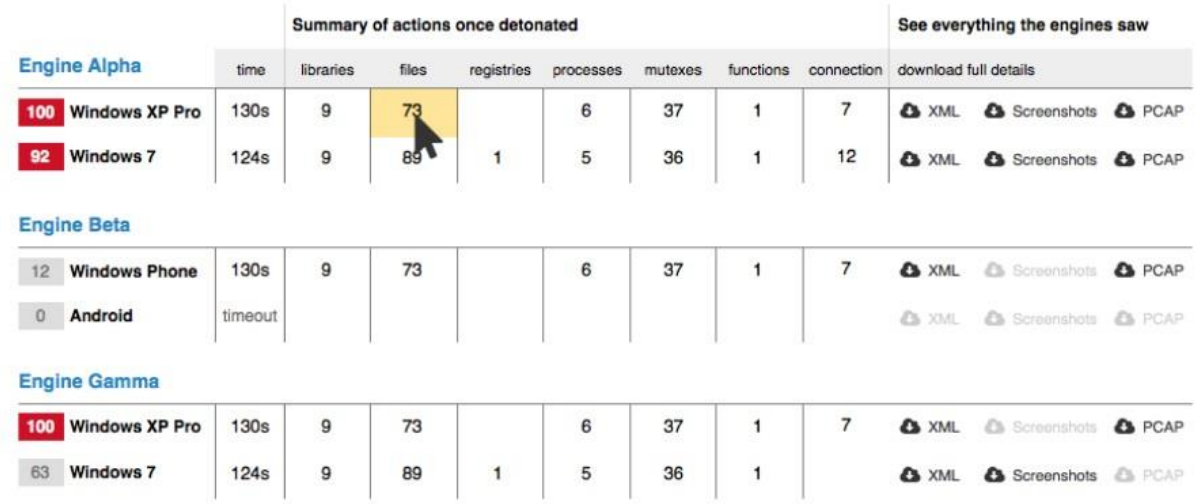
- This is the number of analysis engines used to analyze the file.
- One is the SonicWALL analysis engine.
- Additional analysis engines from third-party vendors are included in the count.

Live detonations:

- This is the total number of environments used across all analysis engines.
- The environment is comprised of the analysis engine and the operating system on which it was run.

Analysis engine results tables

Under the status boxes, the full analysis threat report displays multiple tables showing the results from each analysis engine.



		Summary of actions once detonated							See everything the engines saw
Engine Alpha	time	libraries	files	registries	processes	mutexes	functions	connection	download full details
100 Windows XP Pro	130s	9	73		6	37	1	7	XML Screenshots PCAP
92 Windows 7	124s	9	89	1	5	36	1	12	XML Screenshots PCAP
Engine Beta									
12 Windows Phone	130s	9	73		6	37	1	7	XML Screenshots PCAP
0 Android	timeout								XML Screenshots PCAP
Engine Gamma									
100 Windows XP Pro	130s	9	73		6	37	1	7	XML Screenshots PCAP
63 Windows 7	124s	9	89	1	5	36	1		XML Screenshots PCAP

The engines are designated by names from the Greek alphabet, such as Alpha, Beta, Gamma, and so on.

Each row represents a separate environment, and indicates the operating system in which the engine was executed.

The overall score from the analysis in each environment is displayed in a highlighted box to the left of the operating system. The color of the box indicates whether the score triggered a malicious or non-malicious judgment:

- A score in a red box indicates a malicious judgment
- A score in a grey box indicates a non-malicious judgment

For each environment, the columns provide the analysis duration and a summary of actions once detonated:

- **Time** - The time taken by the analysis, using 's' for seconds, 'm' for minutes, and timeout if the analysis did not complete.
- **Libraries** - Cumulative count of malware libraries that were read during the analysis.
- **Files** - Cumulative count of files that were created, read, updated or deleted during the analysis.
- **Registries** - Cumulative count of OS registries that were read during the analysis.

- **Processes** - Cumulative count of processes that were created during the analysis.
- **Mutexes** - Cumulative count of mutual exclusion objects that were used during the analysis to lock a resource for exclusive access.
- **Functions** - Cumulative count of functions executed during the analysis.
- **Connection** - Cumulative count of network connections that were created during the analysis.

You can click any cell in the Summary of actions table to jump to the full data available further down in the report. Blank cells are not clickable.

The last column provides access to the full details of the analysis by the different engines:

- **XML** - Clicking here lets you open or save an XML file which contains all the detailed data behind the above counts.
- **Screenshots** - Clicking here lets you open or save a zip file of all the screenshots produced by the analysis.
- **PCAP** - Clicking here lets you open or save a packet capture file in libpcap format with details about the connections opened during the analysis.

Viewing Gateway Viruses Reports

The Gateway Viruses reports provide details on the Top Viruses that were blocked when attempting to access the firewall.

To view Gateway Virus Reports, complete the following steps:

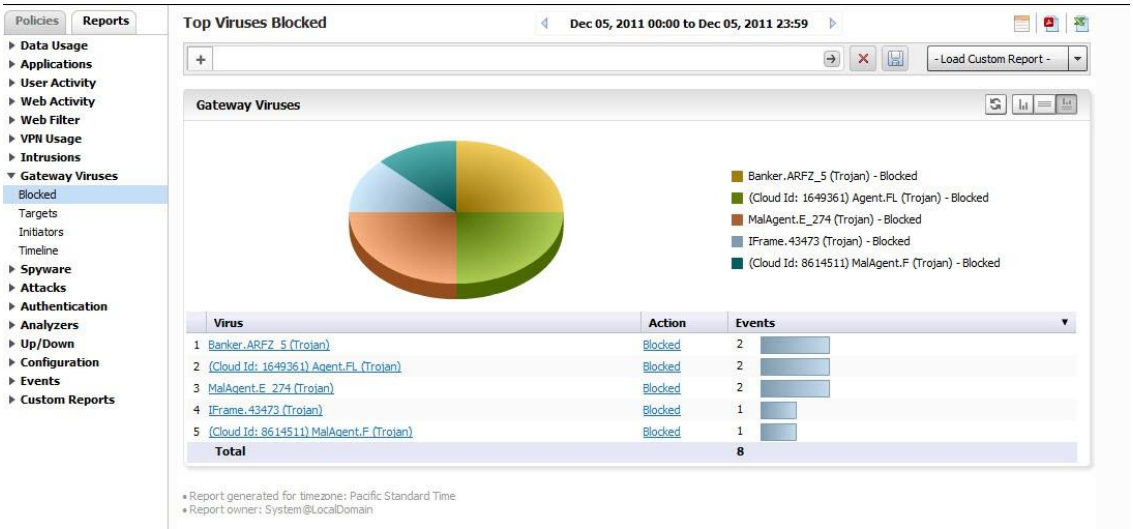
1 Click the **Firewall** tab.

2 Select a SonicWALL appliance.

3 Click **Gateway Viruses > Blocked**.

The Top Viruses report appears.

The report provides details on the viruses blocked, the targets, initiators, and a timeline of when they attempted access.



Drilling down provides a list of virus identity, Targets, Initiators, Target Countries, and Initiator Countries.

Viewing Spyware Reports

The Spyware report gives details of the spyware that was detected and/or blocked, the targets, initiators, and a timeline of when they attempted access.

To view Spyware Reports, complete the following steps:

1 Click the **Firewall** tab.

2 Select a SonicWALL appliance.

3 Click **Spyware > Detected**.

The report provides details on the types of spyware detected and blocked, targets.

Drilling down provides a list of virus identity, Targets, Initiators, Target Countries, and Initiator Countries.Drilling down lists countries of origin, and target countries.

Viewing Attacks Reports

The Attacks report lists attempts to gain access, target systems, initiators, and a timeline of when the attack occurred.

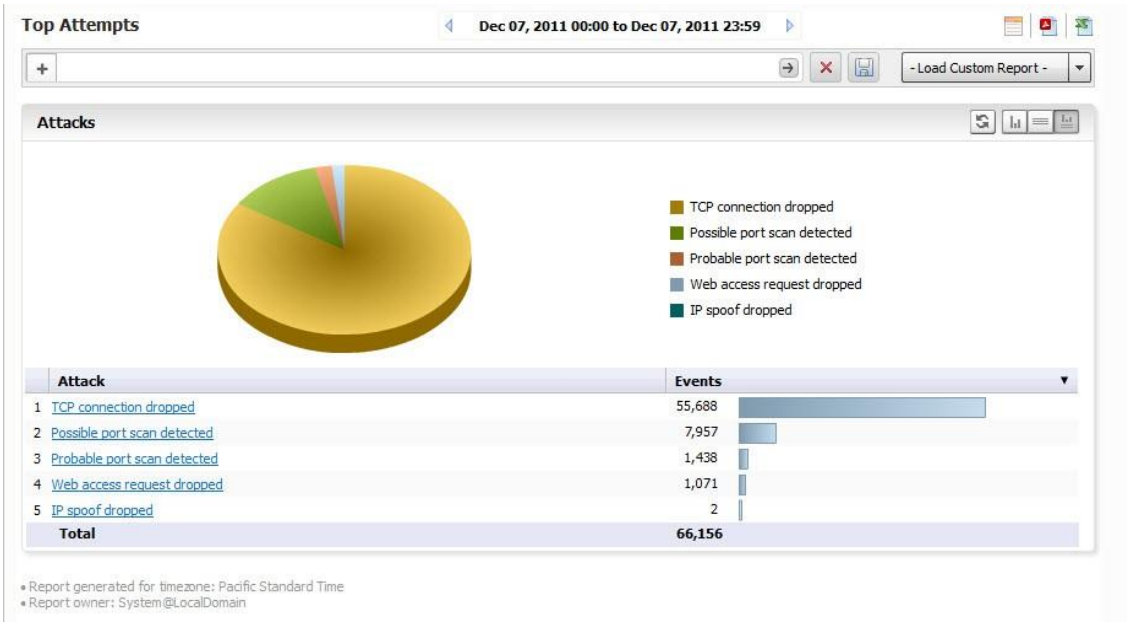
To view Attacks Reports, complete the following steps:

1 Click the **Firewall** tab.

2 Select a SonicWALL appliance.

3 Click **Attacks > Attempts**.

The Attacks report provides a pie chart and a list of the initiating IP addresses and hosts.



Drill down for additional Detail views of Intrusion Categories, Targets, Initiators, Ports affected, Target Countries, and Initiator Countries.

Viewing Authentication Reports

Authentication reports provide information on users attempting to access the Firewall.

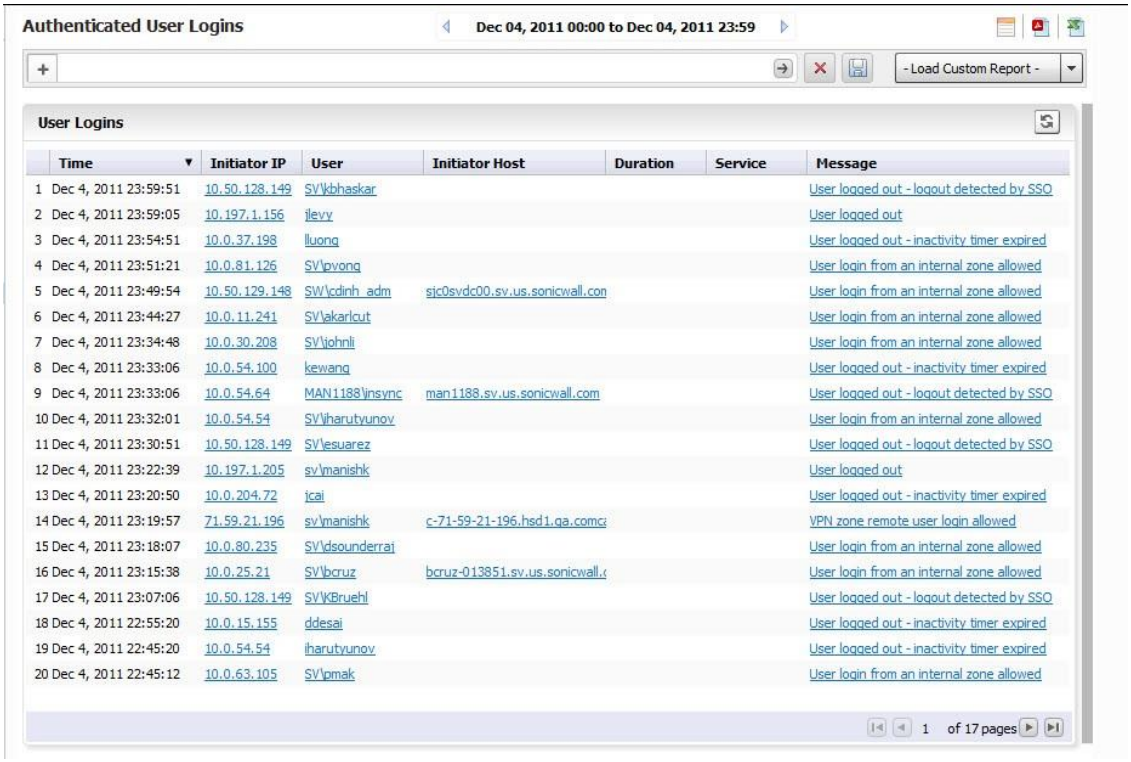
To view Authentication Reports, complete the following steps:

1 Click the **Firewall** tab.

2 Select a SonicWALL appliance.

3 Click **Authentication > User Login**.

The Authentication report displays a list of authenticated users, their IP addresses, service, time they were logged in, and type of login/logout. Additional Reports are available for Administrator logins and failed login attempts.



Clicking on hyperlinks provides additional filtering for the reports.

You can filter on the Service to view SMA and other appliances by drilling down to the syslog:

1 Go to the filter bar and click on the + and select **Service** from the drop-down menu. Click on the = operator, and click on the field next to it to bring up the drop-down menu. Select **SSLVPN** from the drop-down list.

2 Click **Go** to view a report for that service.

> **NOTE:** For the Duration and Service categories to be present, the Firewall appliance firmware must be at least version 5.6.0.

Custom Reports

You can configure a report with customized filters, then save it for later viewing and analysis. Saving a Report allows you to view it later, by loading it through the Custom Reports interface. Custom Reports can either be saved directly, or configured through Universal Scheduled Reports. You can either load the report through the Custom Report drop-down on the Search Bar, or click **Reports > Custom** and choose from the list of saved Custom reports.

Regularly scheduled Custom Reports can be configured through the Universal Scheduled Reports interface, accessible through the Custom Reports icon in the upper right corner. These reports can be set up to be emailed to you on a regular schedule.

Custom Reports are available at the unit level for all appliances visible on the Firewall tab. The Log Analyzer must be enabled for the appliance.

The Manage Reports screen (**Custom Reports > Manage Reports**) allows you to view what Custom Reports are available and delete reports from the system.

For more information on configuring and scheduling custom Reports refer to the Universal Scheduled Reports section.

Using the Log Analyzer

The Log Analyzer allows advanced users to examine raw data for status and troubleshooting. The Analyzer logs contain detailed information from the system logs on each transaction that occurred on the specified SonicWALL appliance. These logs can be filtered or drilled down to further narrow the focus of the information, allowing analysis of data about alerts, interfaces, bandwidth consumption, and so on. The Log Analyzer is only available at the individual unit level.

Because of space constraints, some column items, particularly the log event messages, might not be fully visible in the Reports pane. To view the full report, export the report to an Excel spreadsheet to view, sort, or organize messages.

Log information can be saved for later analysis and reloaded from Custom Reports.

To load a report for viewing, either:

- Click **Load Custom Report** and select from the drop-down list of saved Custom Reports.

- Click on **Analyzers > Log Analyzer** to view the current log.

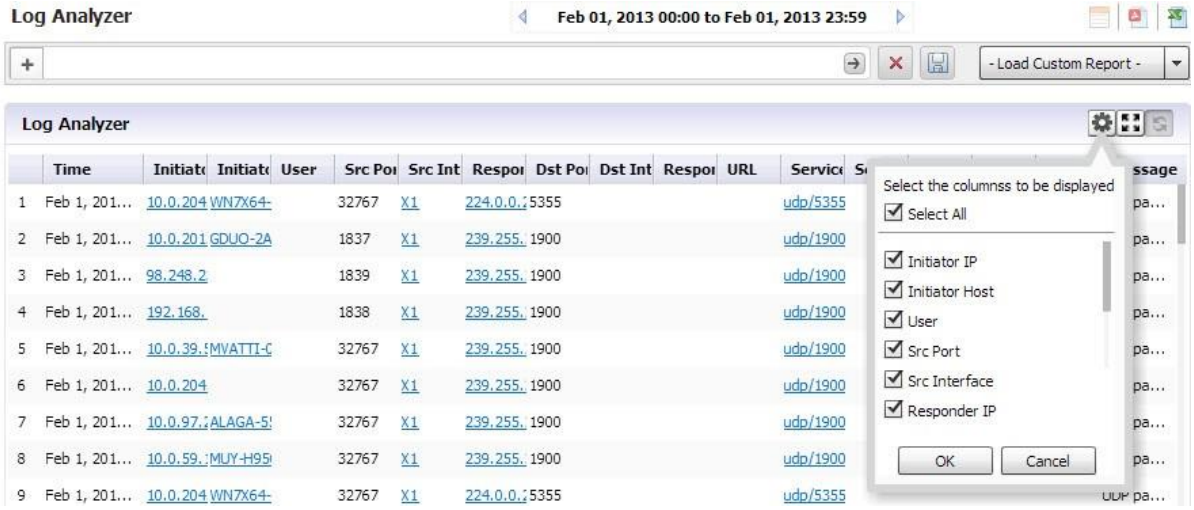
  NOTE: The Log Analyzer entries display raw log information for every connection. Depending on the amount of traffic, this can quickly consume a large amount of space in the database. It is highly recommended to be careful when choosing the number of days of information to be stored.

Viewing the Log Analyzer

The log displays information specific to either a particular report or overall system information, depending on the path used to reach the log, either from the individual report level or from the Log Analyzer entry on the Reports tab. Entries in the Analyzer log vary, according to the relevant report type. You can customize the log entries by using the following options:

Show/Hide Log Columns

Use the Show/Hide Columns function to hide columns that you do not want to display in the Analyzer Log. Just click the **Configure the Log Analyzer** icon, then select the columns that you want to display and deselect the ones that you do not want to display. By configuring the displayed columns, the Log Analyzer gives a more clean, concise, and meaningful way to view the logs, instead of displaying unnecessary columns that take up valuable real estate.



NOTE: “Serial number” column and “Time” column are not part of the list to be configured because they are necessary for any displays.

Row-Based Expansion

Instead of showing all the column information at once, the row-based expansion simplifies the screen and gives on-demand information through a single click.

Click on each row to drop-down the hidden column information.

NOTE: This feature is only available after you sort the columns using the show/hide function.

Full Screen Mode

Switch to full screen mode by clicking the **Full Screen Mode** toggle icon. This populates the entire browser screen with the Log Analyzer page, hiding the tree control and reports panels.

Session-Based Configurations

All column configurations for the Log Analyzer are recorded in each session. This is so that within the session, users can have the desired/configured tabular view of the Log Analyzer at all times.

Priority

The log event messages are color-keyed according to priority. Red is the highest priority, followed by yellow for Alerts. Messages without color keys are informational, only. The color categories are:

- Alert: Yellow
- Critical: Red
- Debug: White
- Emergency: Red
- Error: White
- Info: White
- Notice: White
- Warning: White

Color keys allow you to immediately focus on the priority level of the message, and filter data accordingly.

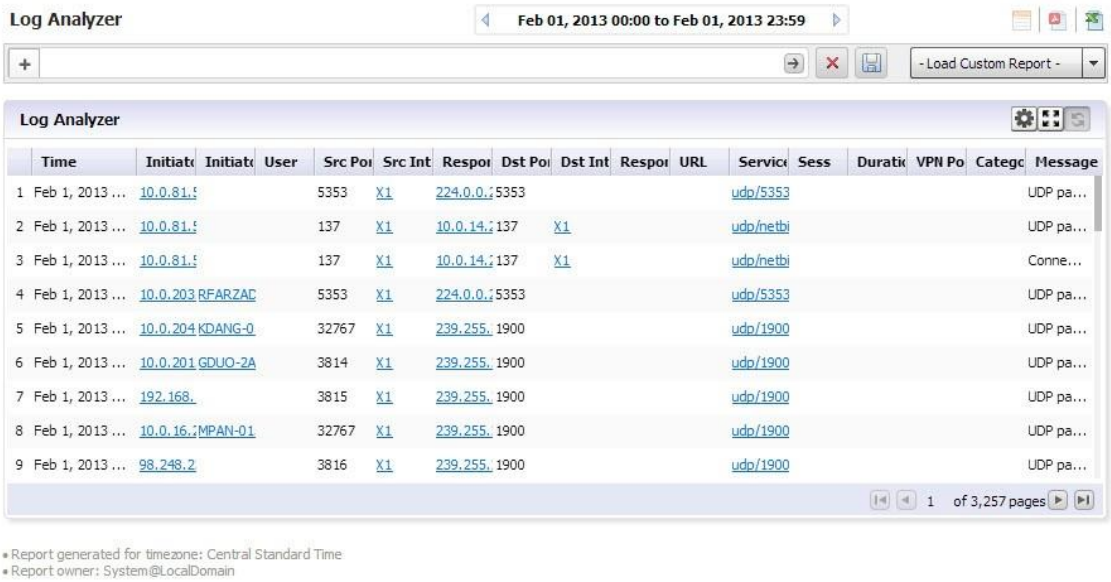
Filtering the Analyzer Log

The Log Analyzer allows you to add filters to view user-or incident-specific data. The Log Analyzer can be reached either by drilling down in individual reports, or from the Analyzers item under the Reports tab.

To view the Analyzer Log, complete the following steps:

1 Select a SonicWALL appliance from the TreeControl pane.

2 Click to expand the **Analyzer** tree and click on Log Analyzer. The saved Log Analyzer report page displays.



NOTE: Because system logs have a large number of entries, it is advisable to constrain the number of entries displayed on the page. Saved system logs are limited in the number of rows that are saved. If saving to PDF, a maximum of 2500 rows are saved. If saving to Excel, a maximum of 10,000 rows are saved.

3 To add a filter, click on the + in the Filter Bar and specify the desired filter item and parameters.

Available filters include filters for Application, Category, DST Interface, DST Port, Duration, Initiator Country, Host, or IP address, Interface, Message, Priority, Responder country, IP, or Name, Service, Session, Src Interface, Src Port, URL, User, or VPN Policy. This full list is available from the Log Analyzer Entry.

If you are viewing the log in the Log Analyzer view for a specific application entry, only those filters specific to that entry are available.

Log views are drillable, and adds filters as column entries are drilled. Click an entry of interest to add a filter and further constrain the information displayed.

Log Analyzer Use Case

In the following use case, we sort and filter the captured event information to evaluate threats targeted toward the X0 default interface.

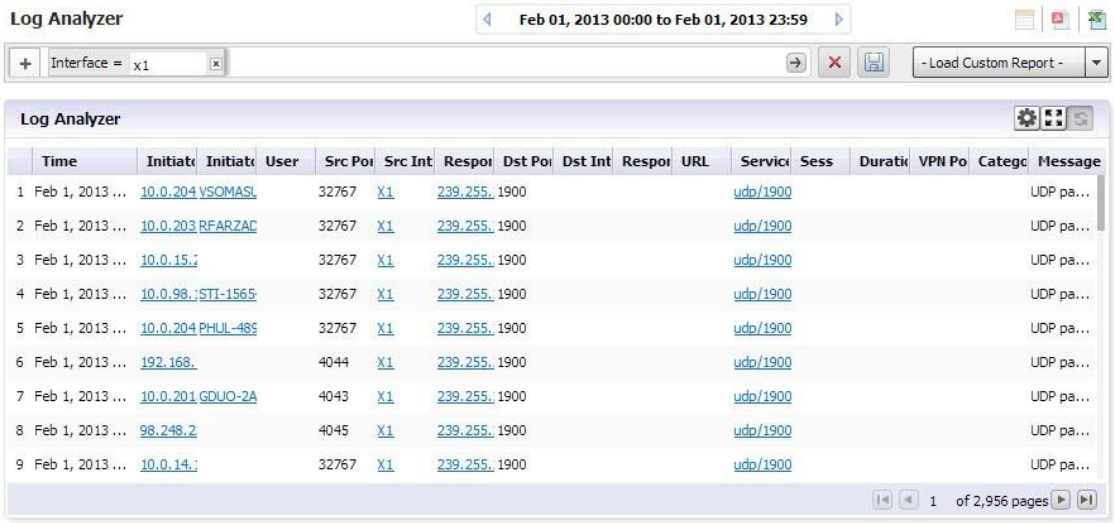
On the Reports tab, click **Analyzers > Log Analyzers**.

1 In the Log Analyzer, click on the + to add a filter, and select the **Interface** filter.

2 Type in X1 to specify the default interface filter.

3 Click **Go**.

The Log Analyzer is filtered on the X1 port interface.



This allows you to begin debugging, or further investigate the use of the database.

More information can also be found by using **Universal Scheduled Reports**.