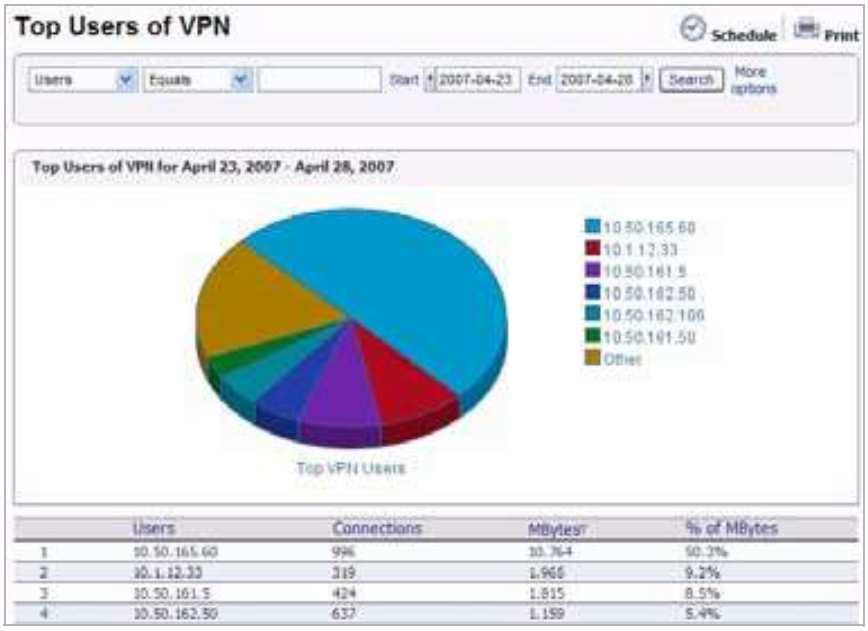
3. Expand the **VPN Usage** tree and click **Top Users Over Time**. The Top Users Over Time page displays.



4. The pie chart displays the VPN connections for the top VPN users.
5. The table contains the following information:
   - **Users**—the IP address of the user.
   - **Connections**—the number of VPN connections.
   - **MBytes**—the number of megabytes transferred.
   - **% of MBytes**—the percentage of megabytes transferred by this user, compared to all users. For example, if 10,000 megabytes of data was transferred during the period and 2000 kilobytes was transferred by the top user, the **% of MBytes** field will display 20%.
6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Users**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.

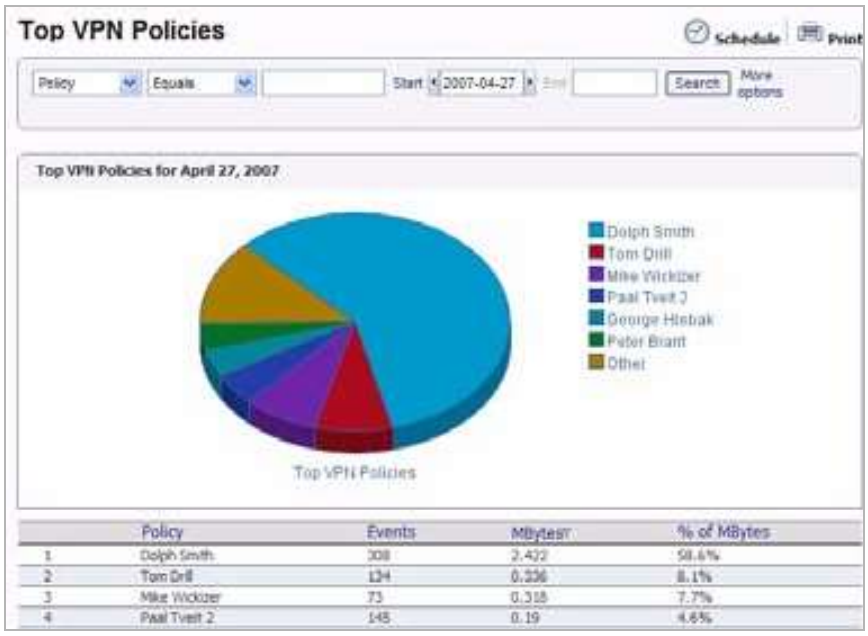
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing VPN Usage By Policy

The VPN Usage By Policy report contains information on VPN usage for a SonicWALL appliance, organized by policy.

To view the VPN Usage By Policy report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **VPN Usage** tree and click **By Policy**. The By Policy page displays.



4. The pie chart displays the amount of data transferred for each policy.
5. The table contains the following information:
   - **Policy**—the name of the policy.
   - **Events**—the number of VPN events.
   - **MBytes**—the number of megabytes transferred.
   - **% of MBytes**—the percentage of megabytes transferred for this policy, compared to all other policies. For example, if a total of 10,000 megabytes was transferred and 2,500 megabytes was transferred for one policy, the **% of Usage** field will display 25%.

Keysight, EX-1030
Page 411

6. The ViewPoint Reporting Module shows yesterday's report. To change the date of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Rows per Screen**

   See "Managing Report Settings" on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

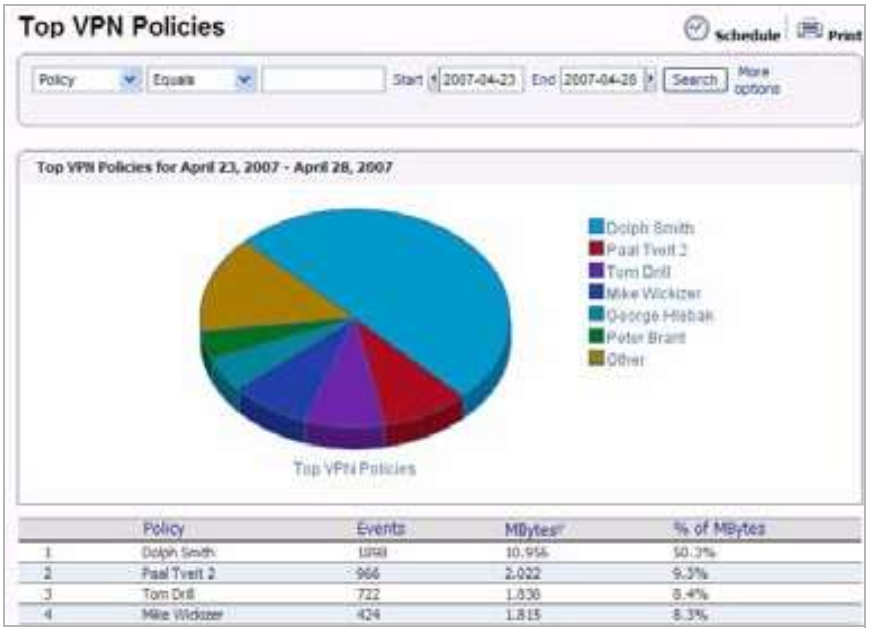
Viewing the Top VPN Policies Over Time

The By Policy Over Time report displays the top VPN Policies for the specified time period.

To view the By Policy Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.

3. Expand the **VPN Usage** tree and click **By Policy Over Time**. The By Policy Over Time page displays.



4. The pie chart displays the VPN connections for the top policies.
5. The table contains the following information:
   - **Policy**—the name of the policy.
   - **Events**—the number of VPN events.
   - **MBytes**—the number of megabytes transferred.
   - **% of MBytes**—the percentage of megabytes transferred for this policy, compared to all other policies for the period. For example, if a total of 100,000 megabytes was transferred and 3,000 megabytes was transferred for one policy, the **% of MBytes** field will display 3%.
6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.

7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing Hourly VPN Usage By Policy

The VPN Usage By Policy Hourly report contains information on hourly VPN usage for a SonicWALL appliance, organized by policy.

To view the VPN Usage By Policy Hourly report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **VPN Usage** tree and click **By Policy Hourly**. The By Policy Hourly page displays.



4. The table contains the following information:
   - **Hour**—the period of time.
   - **Events**—the number of VPN events.
   - **MBytes**—the number of megabytes transferred.
5. The ViewPoint Reporting Module shows yesterday’s report. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.

6. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart
   - **Hour Begin**
   - **Hour End**

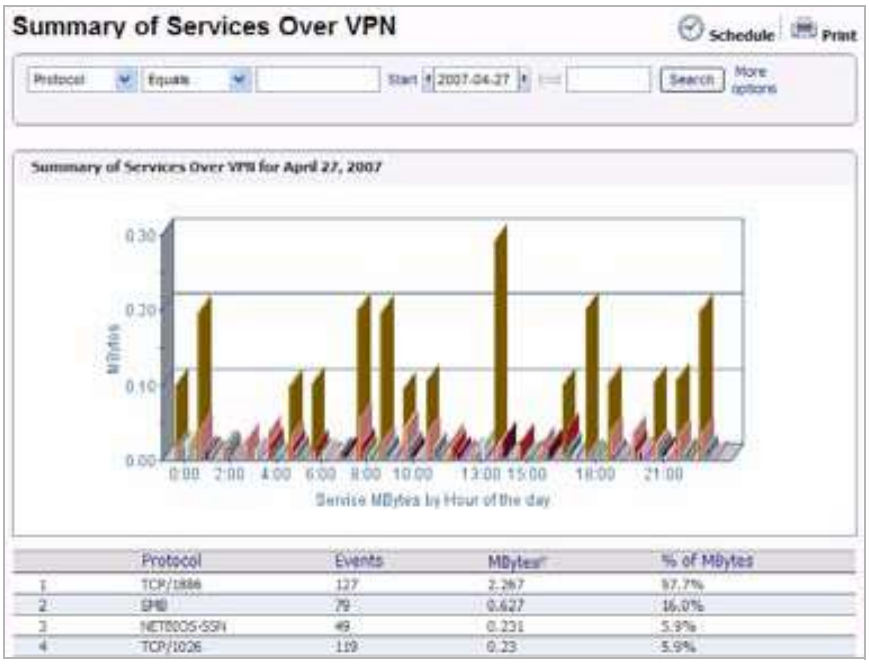
   See “Managing Report Settings” on page 154.
7. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

Viewing the VPN Services Summary Report

The Services Summary report displays the amount of traffic handled by each service during each hour of the specified day.

To view the Services Summary report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **VPN Usage** tree and click **By Service**. The By Service page displays.



4. The bar graph displays the amount of bandwidth used by each service during each hour of the day.

5. The table contains the following information:
   - **Protocol**—the service.
   - **Events**—the number of events or “hits.”
   - **MBytes**—the number of megabytes.
   - **% of MBytes**—the percentage of megabytes transferred by this service on the selected day, compared to all other services. For example, if 1,000 megabytes were transferred and 900 megabytes were handled by the HTTP service, the **% of Mbytes** field will display 90%.
6. The ViewPoint Reporting Module shows yesterday’s report. To change the date of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.
9. These settings will stay in effect for all similar reports during your active login session.

Viewing Attacks Reports

Attacks reports show the number of attacks that were directed at or through the selected SonicWALL appliance(s). These include denial of service attacks, intrusions, probes, and all other malicious activity directed at the SonicWALL appliance or computers on the LAN or DMZ.



Note All reports appear in the appliance’s time zone.

Select from the following:

- To view a summary of the attacks, see “Viewing the Attack Summary Report” on page 251.
- To view the attacks by attack category, see “Viewing the Attacks By Category” on page 253.
- To view the attacks by source IP address, see “Viewing the Errors Report” on page 254.
- To view a summary of the errors and exceptions, see “Viewing the Errors Report” on page 254.
- To view attacks over a period of time, see “Viewing Attack Reports Over Time” on page 256.
- To view errors and exceptions over a period of time, see “Viewing Errors Over Time” on page 258.

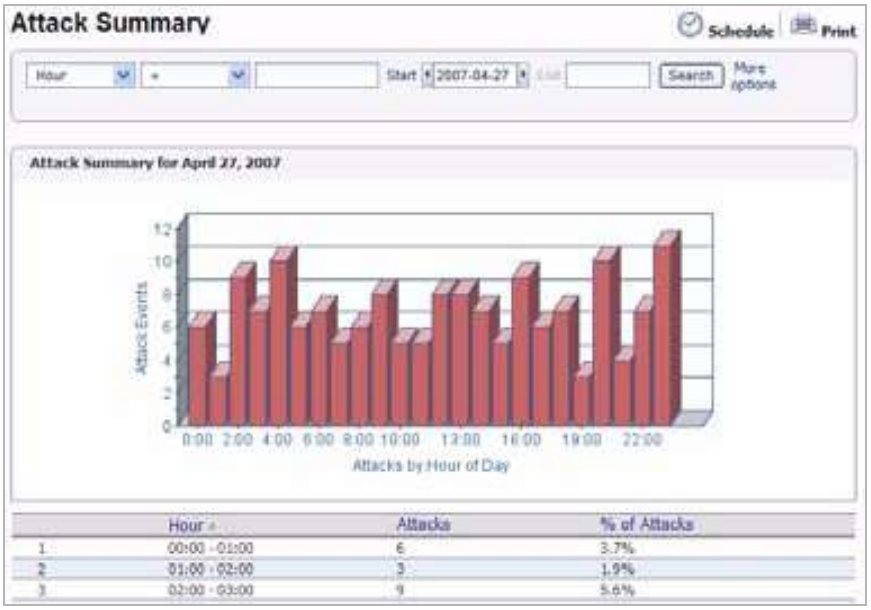
Viewing the Attack Summary Report

The Attack Summary report contains information on the number of attacks attempted on a SonicWALL appliance or all SonicWALL appliances during the specified day.

To view the Attack Summary report, perform the following steps:

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

3. Expand the **Attacks** tree and click **Summary**. The Summary page displays.



4. The bar graph displays the number of attacks attempted during each hour of the day. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Attacks**—the number of attack attempts.
   - **% of Attacks**—the percentage of attacks during this hour, compared to the day. For example, if 1,000 attacks occurred during the day and 100 attacks occurred during the 2:00 time period, the **% of Attacks** field will display 10%.
5. The ViewPoint Reporting Module shows yesterday's report. To change the date of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
6. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

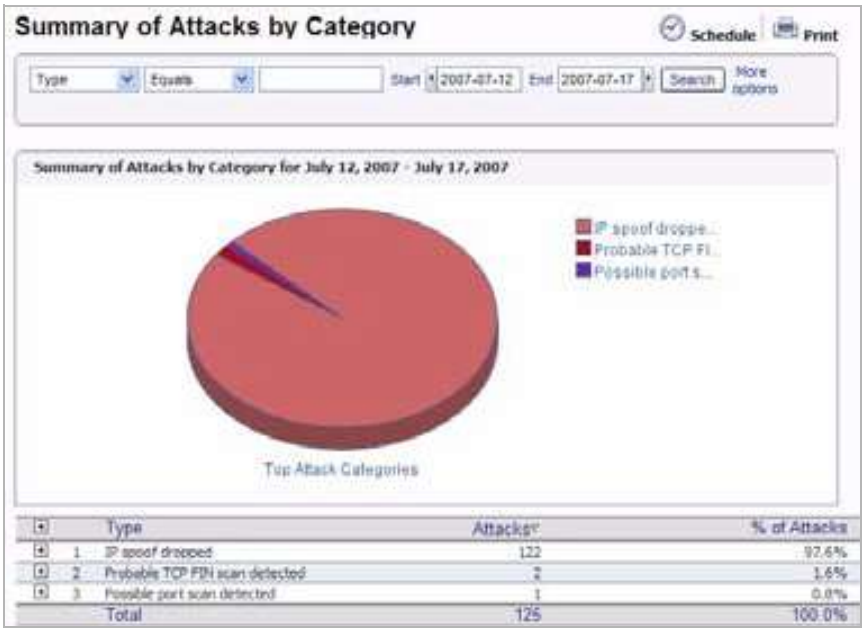
   See "Managing Report Settings" on page 154.
7. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

Viewing the Attacks By Category

The Attacks By Category report displays the attacks that occurred on the specified date, sorted by category.

To view the Attacks By Category report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Attacks** tree and click **By Category**. The By Category page displays.



4. The pie chart displays the percentage of each type of attack. To view source and destination information on the individual attacks, expand the category tree (indicated by a '+' sign).
5. The table contains the following information:
   - **Type**—the type of attack
   - **Source**—the IP address of the source
   - **Destination**—the IP address to the destination
     Click the highlighted source or destination IP address to access the Who is Source Website.

- **Attacks**—the number of attacks
- **% of Attacks**—the percentage of this type of attack, compared to all other attack types. For example, if 5,000 attacks occurred during the day and the IP Spoof makes up 500 of the attacks, its **% of Attacks** field will display 10%.

6. By default, the ViewPoint Reporting Module shows yesterday's report, a pie chart, and the ten top categories. To change the date of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Entries per Item**
   - **Rows per Screen**

   See "Managing Report Settings" on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.
9. These settings will stay in effect for all similar reports during your active login session.

Viewing the Errors Report

The Errors Summary report contains information on the number of dropped packets on a SonicWALL appliance or all SonicWALL appliances during the specified day.

To view the Errors report, perform the following steps:

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

3. Expand the **Attacks** tree and click **Errors**. The Errors page displays.



4. The bar graph displays the packets that were dropped during each hour of the day.
5. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Packets**—the number of dropped packets.
   - **% of Packets**—the percentage of packets dropped during this hour, compared to the day. For example, if 1,000 packets were dropped during the day and 100 packets were dropped during the 1:00 time period, the **% of Packets** field will display 10%.
6. The ViewPoint Reporting Module shows yesterday's report.To change the date of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

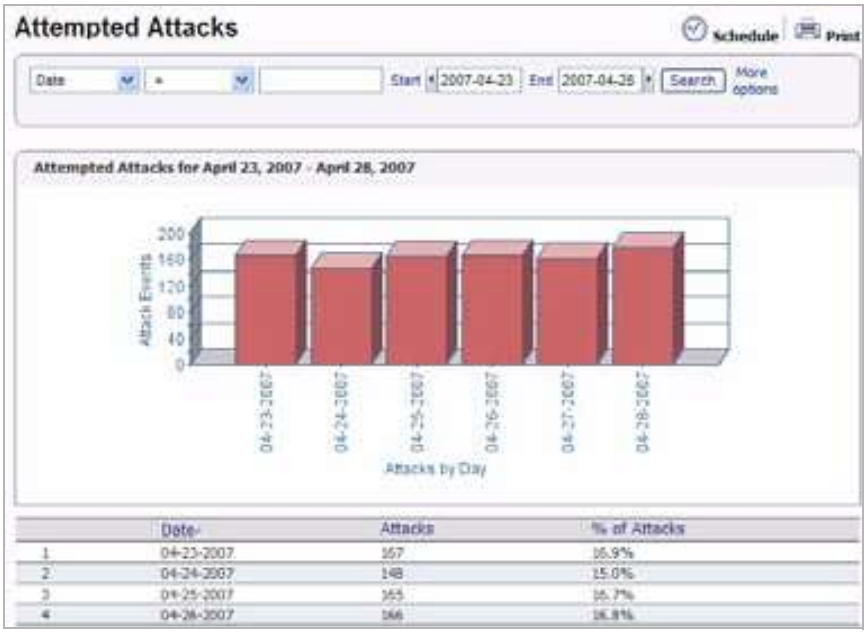
   See "Managing Report Settings" on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

Viewing Attack Reports Over Time

The Attacks Over Time report displays the daily number of attempted attacks during the specified time period.

To view the Attacks Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.
3. Expand the **Attacks** tree and click **Attacks Over Time**. The Attacks Over Time page displays.



4. The bar graph displays the number of attacks attempted each day of the time period.
5. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Attacks**—the number of attacks.
   - **% of Attacks**—the percentage of attacks on this day, compared to the time period. For example, if 10,000 attacks occurred during the time period and 1,000 attacks occurred on Thursday, its **% of Attacks** field will display 10%.
6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.

7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

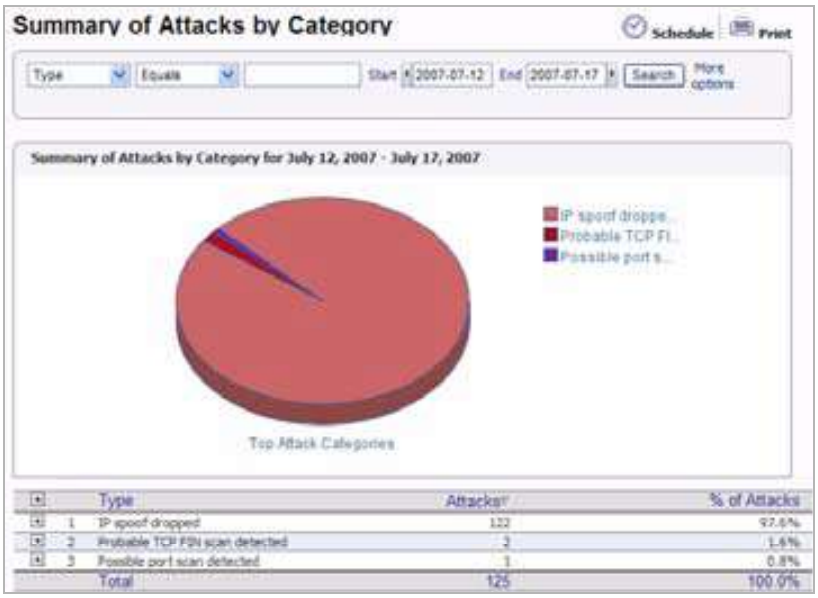
   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing the Attacks By Category Over Time

The Categories Over Time report displays the number of attacks in each attack category during the specified time period.

To view the Categories Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.
3. Expand the **Attacks** tree and click **Categories Over Time**. The Categories Over Time page displays.



4. The bar graph displays the number of attacks attempted each day of the specified time period. To view source and destination information on the individual attacks, expand the category tree (indicated by a ‘+’ sign).
5. The table contains the following information:
   - **Type**—the type of attack
   - **Source**—the IP address of the source

- **Destination**—the IP address to the destination
  Click the highlighted source or destination IP address to access the Whois Source Website.
- **Attacks**—the number of attacks
- **% of Attacks**—the percentage of this type of attack, compared to all other attack types. For example, if 5,000 attacks occurred during the day and the IP Spoof makes up 500 of the attacks, its **% of Attacks** field will display 10%.

6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Entries per Item**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

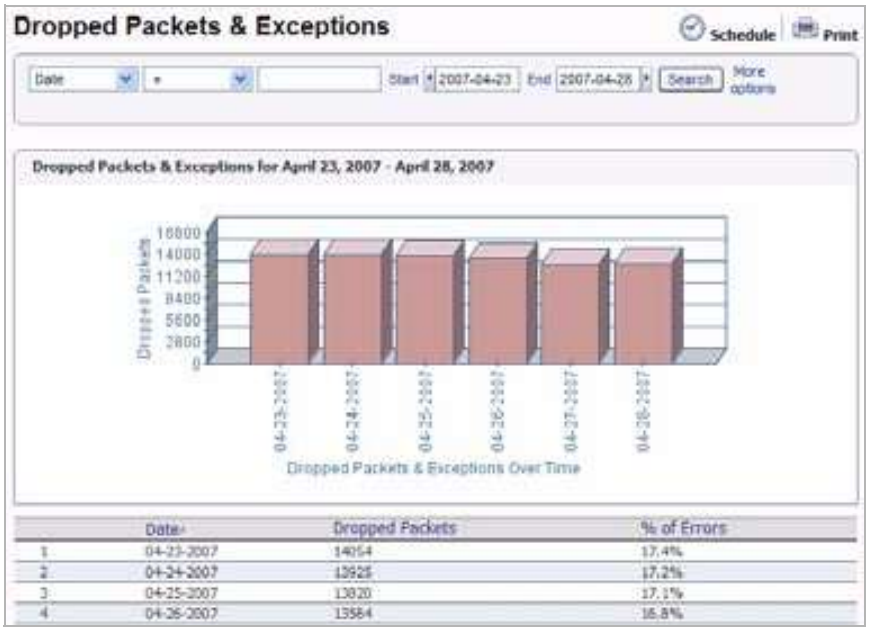
Viewing Errors Over Time

The Errors Over Time report displays the number of errors during the specified time period.

To view the Errors Over Time report, perform the following steps:

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

3. Expand the **Attacks** tree and click **Errors Over Time**. The Dropped Packets & Exceptions page displays.



4. The bar graph displays the number of packets that were dropped during each day of the specified time period.
5. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Dropped Packets**—the number of dropped packets.
   - **% of Errors**—the percentage of dropped packets on this day, compared to the time period. For example, if 10,000 packets were dropped during the time period and 1,000 packets were dropped on Wednesday, its **% of Attacks** field will display 10%.
6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing Virus Attacks Reports

Virus Attacks reports show the number of virus attacks that were directed at or through the selected SonicWALL appliance(s).

Note All reports appear in the appliance's time zone.

If the selected appliance is not licensed for SonicWALL Gateway Anti-Virus, a sample report is displayed, as shown below. You can click the **Click Here** link near the top to view the global dashboard report showing all viruses and similar attacks currently being monitored by SonicWALL, or click the link at the bottom of the page to read detailed information about SonicWALL Gateway Anti-Virus and other subscription services.



Select from the following reports:

- To view the top virus, see "Viewing the Top Viruses By Attack Attempts Report" on page 262.
- To view the virus attacks by top destinations, see "Viewing the Virus Attack Attempts Report" on page 263.

- To view virus attacks over time, see “Viewing the Virus Attack Attempts Report” on page 263.
- To view virus attacks over a period of time, see “Viewing the Virus Attacks By User Report” on page 265.
- To view virus attacks by top destinations over time, see “Viewing Anti-Spyware Reports” on page 266.

9. Expand the **Virus Attacks** tree and click **Summary**. The Summary page displays



10. The bar graph displays the number of virus attacks attempted during each hour of the day. The table contains the following information:
    - **Hour**—the hour of the day for which the summary is provided.
    - **Attempts**—the number of times the virus attempted to infect the device during a pre-set time interval (the hour of the day is the default).
    - **% of Attempts**—the percent of attempts the current virus entry comprises as a portion of the aggregate number of virus attempts on the device during a pre-set time interval (the hour of the day is the default).
11. The ViewPoint Reporting Module shows yesterday’s report. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
12. Under Report Display Settings you can set:

- **Display Type**: **Chart and Table**, or **Table Only**
- **Chart Type**: **Area**, **Bar** or **Plot** chart

See “Managing Report Settings” on page 154.

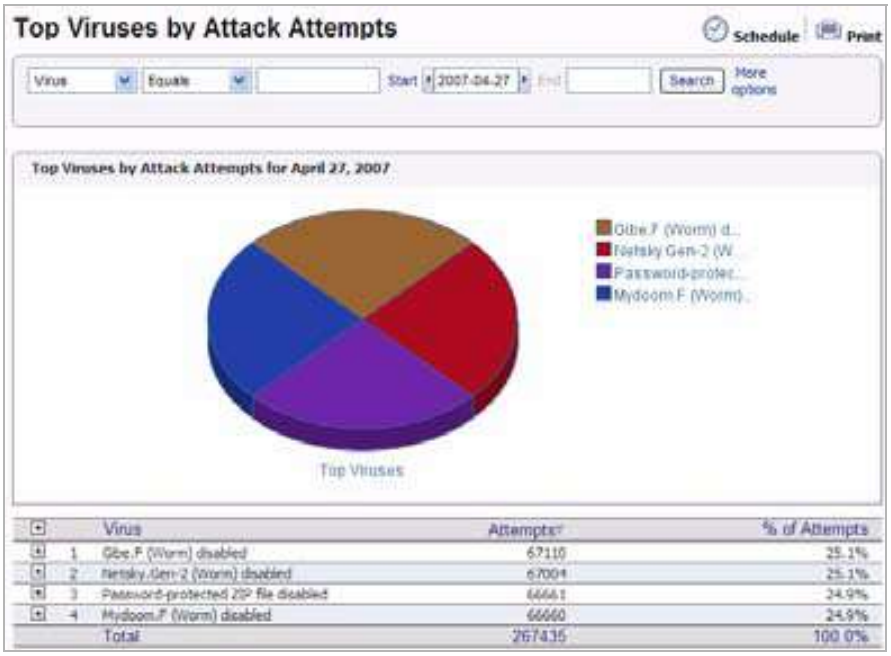
13. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing the Top Viruses By Attack Attempts Report

The Top Viruses By Attack Attempts report displays the top viruses for the specified date.

To view the Top Viruses, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.
3. Expand the **Virus Attacks** tree and click **By Virus**. The Top Viruses By Attack Attempts page displays.



4. The pie chart displays the percentage of virus attacks attempted in a given day.
5. The table contains the following information:
   - **Virus**—the name of the virus.
   - **Attempts**—the number of attack attempts.

- **% of Attempts**—the percentage of attempts as compared to the day.

6. The ViewPoint Reporting Module shows yesterday's report. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Entries per Item**
   - **Rows per Screen**

   See "Managing Report Settings" on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

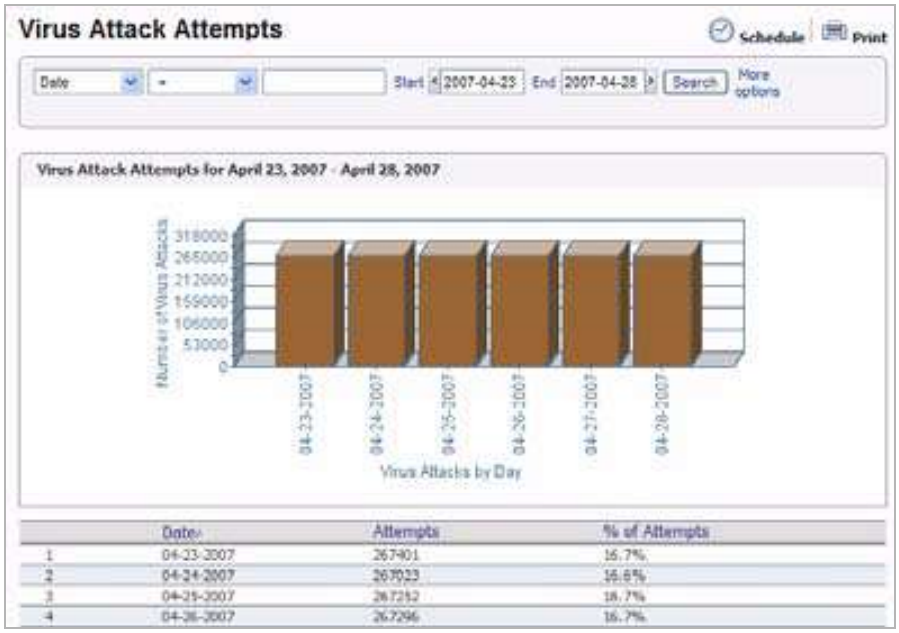
Viewing the Virus Attack Attempts Report

The Virus Attack Attempts report displays the number of virus attempts over the specified time range.

To view the Virus Attack Attempts report, perform the following steps:

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

3. Expand the **Virus Attacks** tree and click **Over Time**. The Virus Attack Attempts page displays.



4. The bar graph displays the number of virus attempts that were made during each day over a specified time period.
5. The table contains the following information:
   - **Date**—the date of when the sample was taken.
   - **Attempts**—the number of attempted virus attacks.
   - **% of Attempts**—the percentage of attempted virus attacks in a day compared to the time period. For example, if 5,000 attempts were made during the time period and 500 were made on one day, its **% of Attempts** field will display 10%.
6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.

7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Entries per Item**
   - **Rows per Screen**

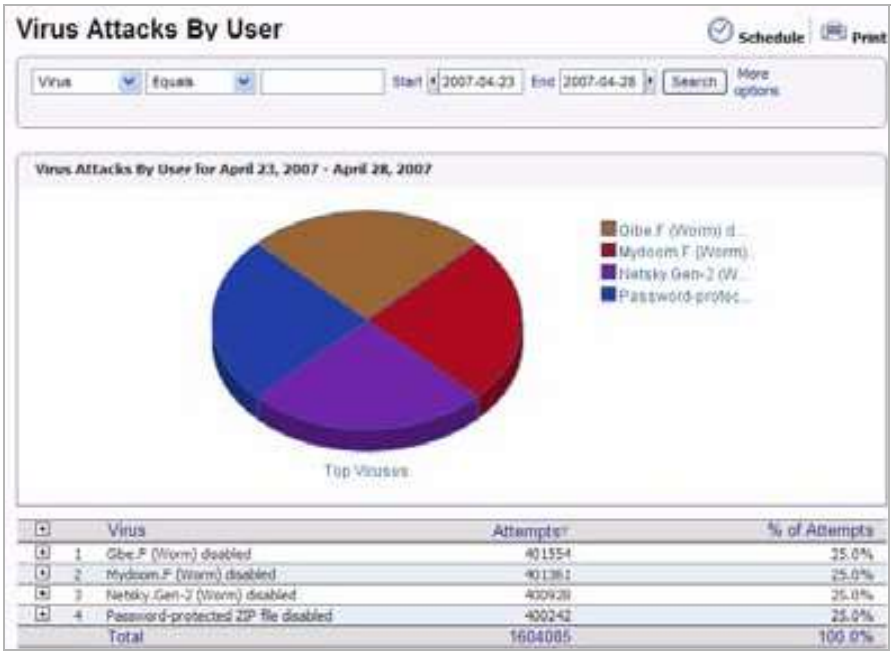
   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing the Virus Attacks By User Report

The Virus Attacks By User report displays the number of virus attack attempts over the specified time range.

To view the Virus Attacks By User report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.
3. Expand the **Virus Attacks** tree and click **By Viruses Over Time**. The Virus Attacks By User page displays.



Keysight, EX-1030
Page 431

4. The pie chart displays the percentage of virus attacks attempted in a given day.
5. The table contains the following information:
   - **Virus**—the name of the virus.
   - **Attempts**—the number of attack attempts.
   - **% of Attempts**—the percentage of attempts compared to the day.
6. The ViewPoint Reporting Module shows yesterday's report. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Entries per Item**
   - **Rows per Screen**

   See "Managing Report Settings" on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

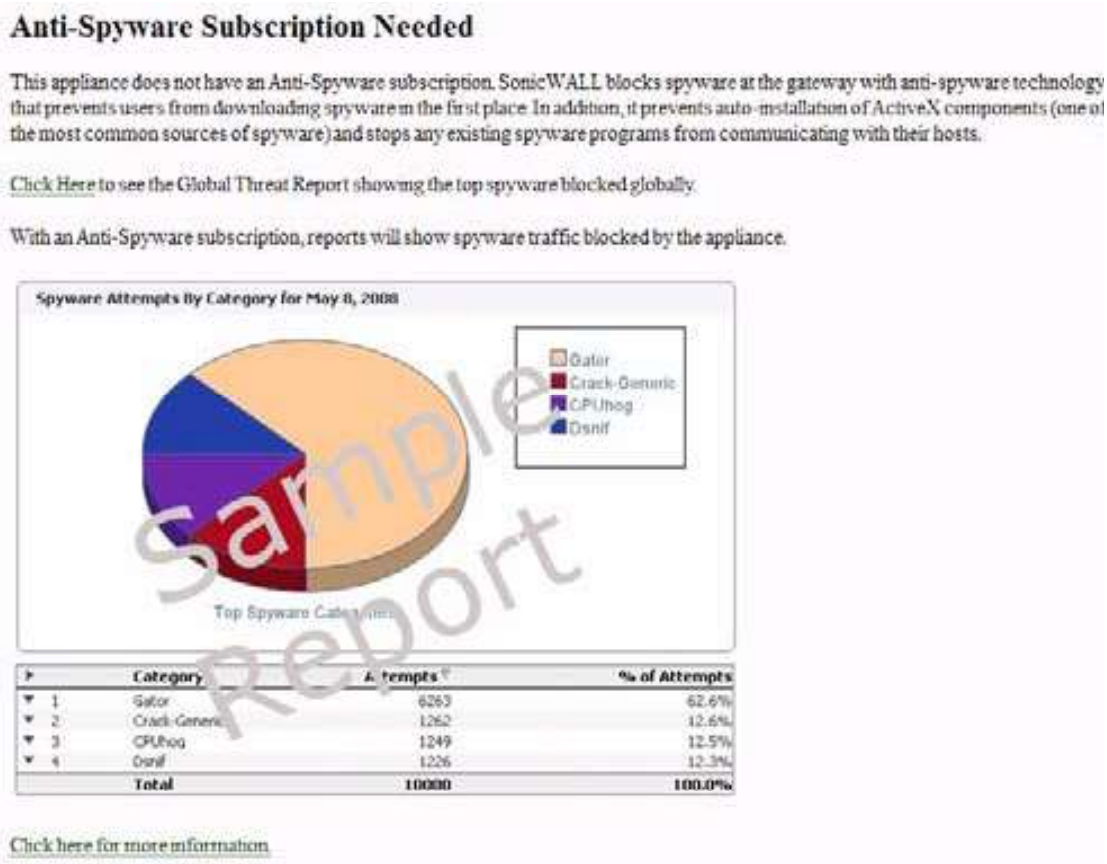
Viewing Anti-Spyware Reports

SonicWALL Anti-Spyware is included within the SonicWALL Gateway Anti-Virus (GAV), Anti-Spyware and Intrusion Prevention Service (IPS) unified threat management (UTM) solution. SonicWALL UTM delivers a comprehensive, real-time gateway security solution for your entire network.

Unlike other threat management solutions, SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service has the capacity to analyze files of any size in real-time without the need to add expensive hardware drive or extra memory. SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service includes a pro-active alerting mechanism that notifies network administrators when a new threat is discovered. Granular policy tools and an intuitive user interface enable administrators to configure a custom set of detection or prevention policies tailored to their specific network

environment. Network administrators can create global policies between security zones and group attacks by priority, simplifying deployment and management across a distributed network.

If the selected appliance is not licensed for SonicWALL Anti-Spyware, a sample report is displayed, as shown below. You can click the **Click Here** link near the top to view the global dashboard report showing all spyware and similar attacks currently being monitored by SonicWALL, or click the link at the bottom of the page to read detailed information about SonicWALL Anti-Spyware and other subscription services.



See the following sections to view Anti-Spyware reports:

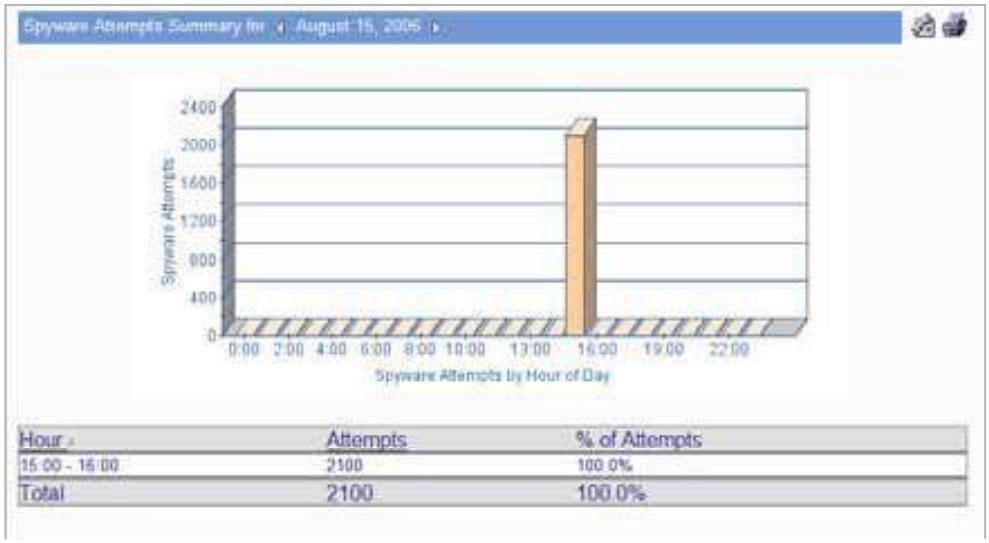
- “Viewing a Spyware Summary” on page 268
- “Viewing Spyware Attempts By Category” on page 269
- “Viewing Spyware Attempts Over Time” on page 270
- “Viewing Spyware Attempts By Category Over Time” on page 272

Viewing a Spyware Summary

The Anti-Spyware Summary report contains information on the number of spyware attempts by hour of the day.

To view a spyware Summary, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.
3. Expand the **Anti-Spyware** tree and click **Summary**. The Summary page displays.



4. The bar graph displays the number of virus attacks attempted during each hour of the day.
5. The table contains the following information:
   - **Hour**—the hour of the day for which the summary is provided.
   - **Attempts**—the number of times the spyware attempted to infect the device during a pre-set time interval (the hour of the day is the default).
   - **% of Attempts**—the percent of attempts the current spyware entry comprises as a portion of the aggregate number of spyware attempts on the device during a pre-set time interval (the hour of the day is the default).
6. The ViewPoint Reporting Module shows yesterday's report. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.

7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

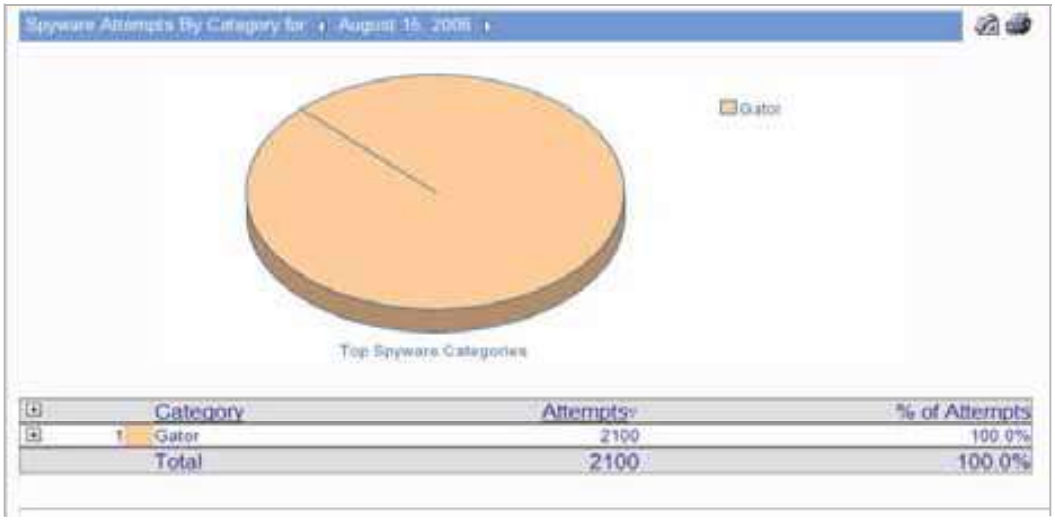
   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.
9. Note this page displays the number of spyware attempts that occurred during two-hour intervals during the past day.

Viewing Spyware Attempts By Category

These reports display the spyware activity by category including the actual category or classification of the spyware, the priority, and the event/attacks type. By using the category as criteria, you can display details about the type/message text and number of events.

To view spyware attempts by category, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Anti-Spyware** tree and click **By Category**. The By Category page displays.



Keysight, EX-1030
Page 435

4. The pie chart displays the percentage of spyware attempts by category.
5. The table contains the following information:
   - **Category**—the category of the spyware.
   - **Attempts**—the number of times the spyware attempted to infect the device using the category as a criteria.
   - **% of Attempts**—the percent of attempts the current spyware entry comprises as a portion of the aggregate number of spyware attempts using the category as a criteria.
6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Entries per Item**
   - **Rows per Screen**

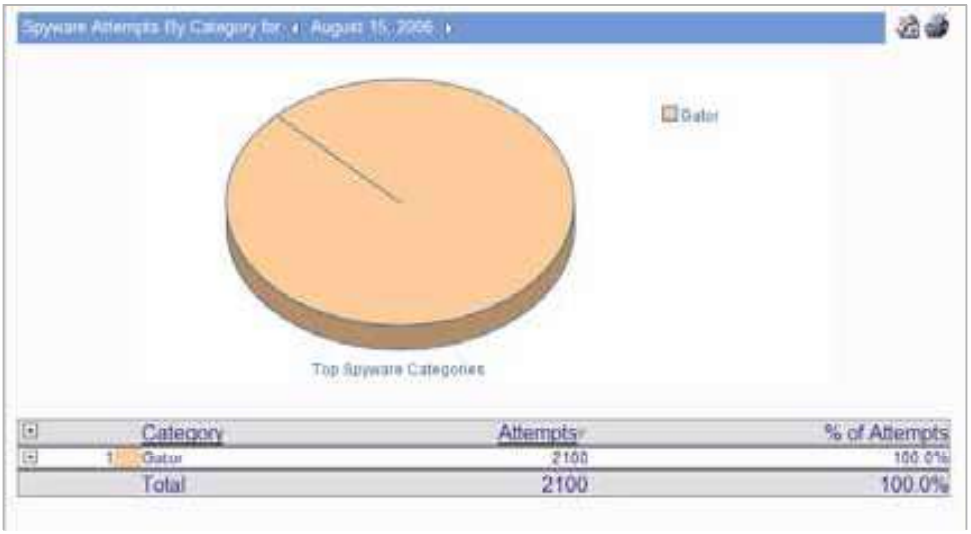
   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing Spyware Attempts Over Time

You can display spyware attempts over a set time interval. These reports are available at the unit and global levels similar to the other summary reports. To view spyware attempts using pre-set time intervals as the viewing criteria, perform the following steps:

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

3. Expand the **Anti-Spyware** tree and click **Over Time**. The Over Time page displays.



4. The bar graph displays the number of spyware attempts that were made during each day over a specified time period.
5. The table contains the following information:
   - **Date**—the date for which the summary is provided.
   - **Attempts**—the number of times the spyware attempted to infect the device during a specific date.
   - **% of Attempts**—the percent of attempts the current spyware entry comprises as a portion of the aggregate number of spyware attempts on the device during a pre-set time interval.
6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

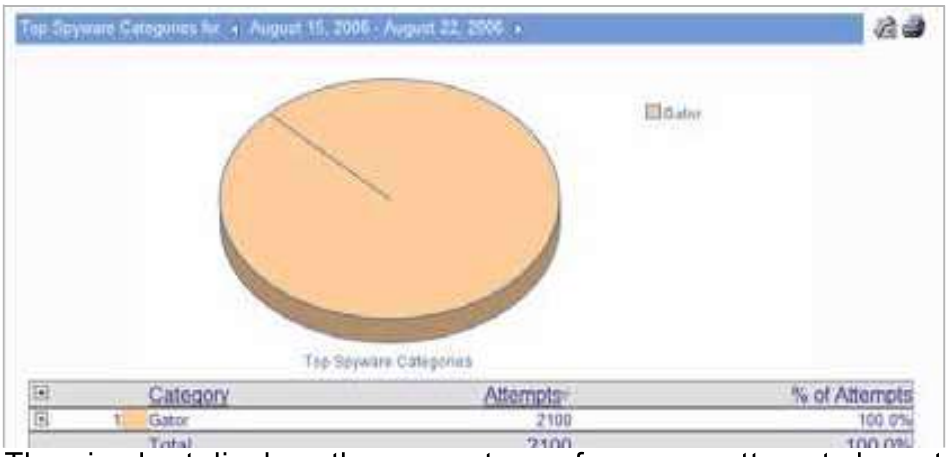
   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing Spyware Attempts By Category Over Time

You can generate reports that display the spyware activity by category, such as the category, priority, and events/attacks over time. Using the category over time statistic as criteria for report generation provides details about the type/message text and number of events.

To view Anti-Spyware attempts using categories over time intervals as the viewing criteria, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Anti-Spyware** tree and click **By Category Over Time**. The By Category Over Time page displays.



4. The pie chart displays the percentage of spyware attempts by category. The table contains the following information:
   - **Category**—the category of the virus.
   - **Attempts**—the number of times the spyware attempted to infect the device during a pre-set time interval.
   - **% of Attempts**—the percent of attempts the current spyware entry comprises as a portion of the aggregate number of spyware attempts on the device during a pre-set time interval.
5. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.

6. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Entries per Item**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.
7. To display a limited group of items, use the Search Bar fields.



Note The search bar fields use pattern matching with operators such as “contains”. For example, “john” will match john_smith or john42.

8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing Intrusion Prevention Reports

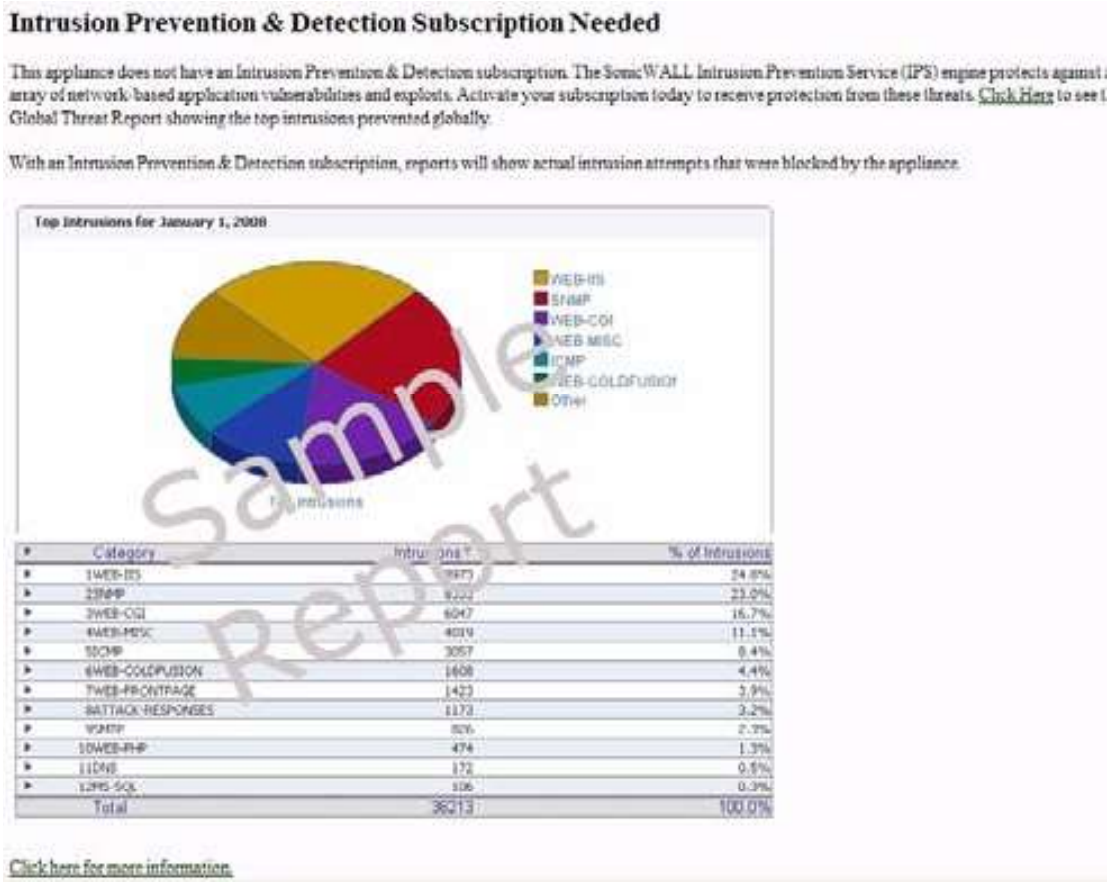
The Intrusion Prevention Service (IPS) reports show the number of attempted intrusions that occurred during the specified time period.



Note All reports appear in the appliance’s time zone.

If the selected appliance is not licensed for SonicWALL Intrusion Prevention Service, a sample report is displayed, as shown below. You can click the **Click Here** link near the top to view the global dashboard report showing all

intrusions and similar attacks currently being monitored by SonicWALL, or click the link at the bottom of the page to read detailed information about SonicWALL Intrusion Prevention Service and other subscription services.



Select from the following intrusion reports:

- To view a summary of the attacks, see “Viewing the Intrusion Prevention Summary Report” on page 275.
- To view the attacks by source IP address, see “Viewing the Errors Report” on page 254.
- To view a summary of the errors and exceptions, see “Viewing the Errors Report” on page 254.
- To view attacks over a period of time, see “Viewing Attack Reports Over Time” on page 256.
- To view errors and exceptions over a period of time, see “Viewing Errors Over Time” on page 258.

Viewing the Intrusion Prevention Summary Report

The Attack Summary report contains information on the number of attempted intrusions on a SonicWALL appliance or all SonicWALL appliances during the specified day.

To view the IPS Summary report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.
3. Expand the **Intrusion Prevention** tree and click **Summary**. The Summary page displays.



4. The bar graph displays the number of intrusions attempted during each hour of the day.
5. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Intrusions**—the number of intrusion attempts.
   - **% of Intrusions**—the percentage of intrusion attempts on this day, compared to the time period. For example, if 10,000 intrusion attempts occurred during the time period and 1,000 intrusion attempts occurred on Thursday, its **% of Intrusions** field will display 10%.

6. The ViewPoint Reporting Module shows yesterday's report. To change the date of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

   See "Managing Report Settings" on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

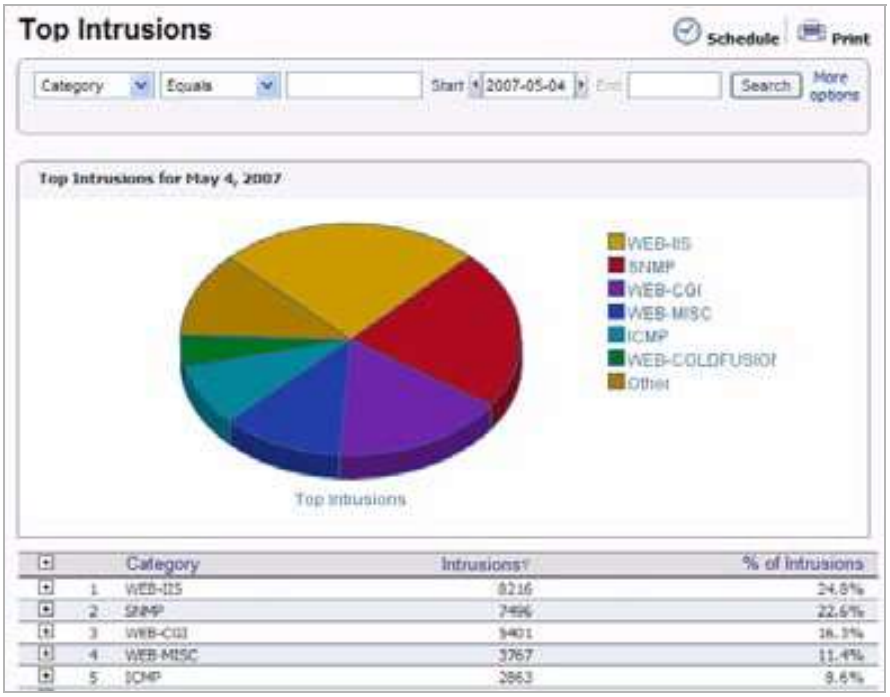
Viewing Intrusion Attempts By Category

These reports display the intrusion activity by category including the actual category or classification of the intrusion, the priority, and the event/attacks type. By using the category as criteria, you can display details about the type/message text and number of events.

To view intrusion attempts by category, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.

3. Expand the **Intrusion Prevention** tree and click **By Category**. The By Category page displays.



4. The pie chart displays a list of intrusions attempted by category. The table contains the following information:
   - **Category**—the category of the intrusion attempt.
   - **Intrusions**—the number of intrusion attempts.
   - **% of Intrusions**—the percentage of intrusion attempts as a portion of the aggregate number of intrusion attempts using the category as a criteria.
5. To change the date of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.

Keysight, EX-1030
Page 443

6. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Entries per Item**
   - **Rows per Screen**

   See “Managing Report Settings” on page 154.
7. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

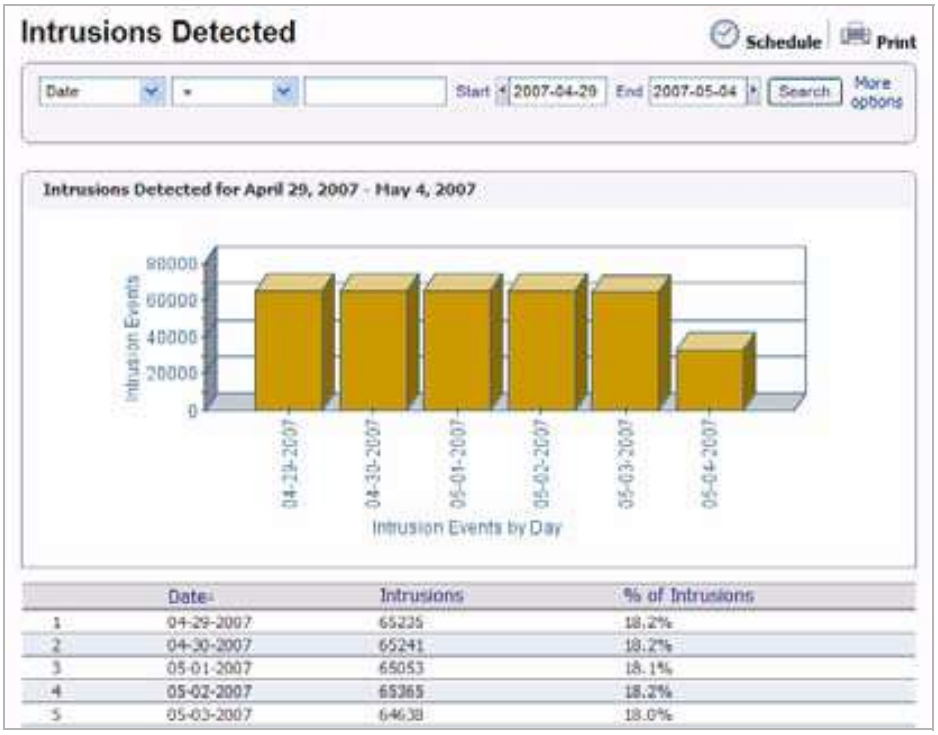
Viewing Intrusions Over Time

The Over Time report displays the daily number of intrusion attempts during the specified time period.

To view the Intrusions Over Time report, perform the following steps:

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

3. Expand the **Intrusion Prevention** tree and click **Intrusions Over Time.** The Intrusions Over Time page displays.



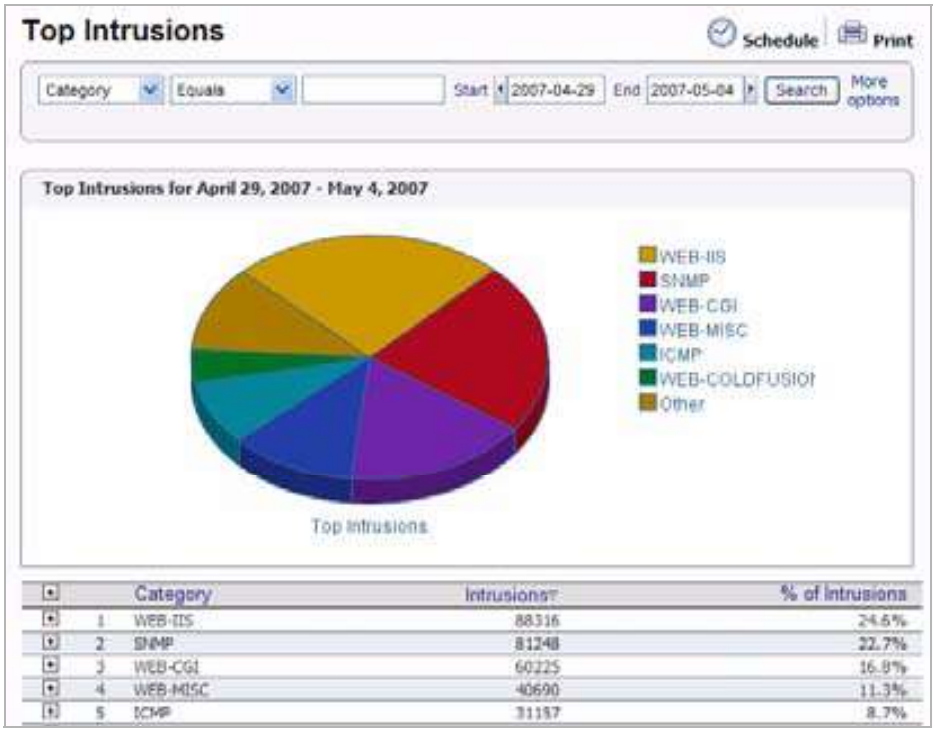
4. The bar graph displays the number of intrusions attempted each day of the specified time period.
5. The table contains the following information:
   - **Date**—when the sample was taken.
   - **Intrusions**—the number of intrusion attempts.
   - **% of Intrusions**—the percentage of intrusion attempts on this day, compared to the time period. For example, if 10,000 intrusion attempts occurred during the time period and 1,000 intrusion attempts occurred on Thursday, its **% of Intrusions** field will display 10%.
6. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
7. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar** or **Plot** chart

   See “Managing Report Settings” on page 154.
8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing Intrusion Reports By Category Over Time

You can generate reports that display the intrusion activity by category, such as the category, priority, and events/attacks over time. Using the category over time statistic as criteria for report generation provides details about the type/message text and number of events. To view intrusion attempts using categories over time intervals as the viewing criteria, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Intrusion Prevention** tree and click **By Category Over Time.** The By Category Over Time page displays.



4. The pie chart displays a list of intrusions attempted by category over time. The table contains the following information:
   - **Category**—the category of the intrusion attempt.
   - **Intrusions**—the number of attempted intrusions during a pre-set time interval.
   - **% of Intrusions**—the percentage of intrusion attempts the current intrusion entry comprises as a portion of the aggregate number of intrusion attempts on the device during a pre-set time interval.

5. The ViewPoint Reporting Module shows yesterday's report. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar, or click **More Options** for report display settings.
6. Under Report Display Settings you can set:
   - **Display Type**: **Chart and Table**, or **Table Only**
   - **Chart Type**: **Area**, **Bar**, **Pie** or **Plot** chart
   - **Number of Items**
   - **Entries per Item**
   - **Rows per Screen**

   See "Managing Report Settings" on page 154.
7. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

Viewing Application Firewall Reports

Application Firewall reports provide information on the applications, users, and Application Firewall policies that are handled by Application Firewall on the selected SonicWALL appliance(s). The Application Firewall feature is available on SonicWALL NSA and SonicWALL TZ 210 Series appliances in SonicOS Enhanced 5.0 and higher.

Application Firewall reports can be used to view Application Firewall usage by the day or over a period of days. Additionally, you can view the top applications, top users, or top policies for Application Firewall on a single SonicWALL NSA or SonicWALL TZ 210 series appliance.

Clickable reports (Graphs and Data) are supported, providing drill-down reporting information by clicking the graphical elements (such as pie chart slices) and data rows. For example, you can drill down to the User report level by clicking a user in one of the Top reports.



Note All reports appear in the appliance's time zone.

Select from the following:

- To view a summary of the daily Application Firewall usage, see "Viewing the Application Firewall Summary Report" on page 282.
- To view Application Firewall usage over time, see "Viewing the Application Firewall Over Time Report" on page 283.

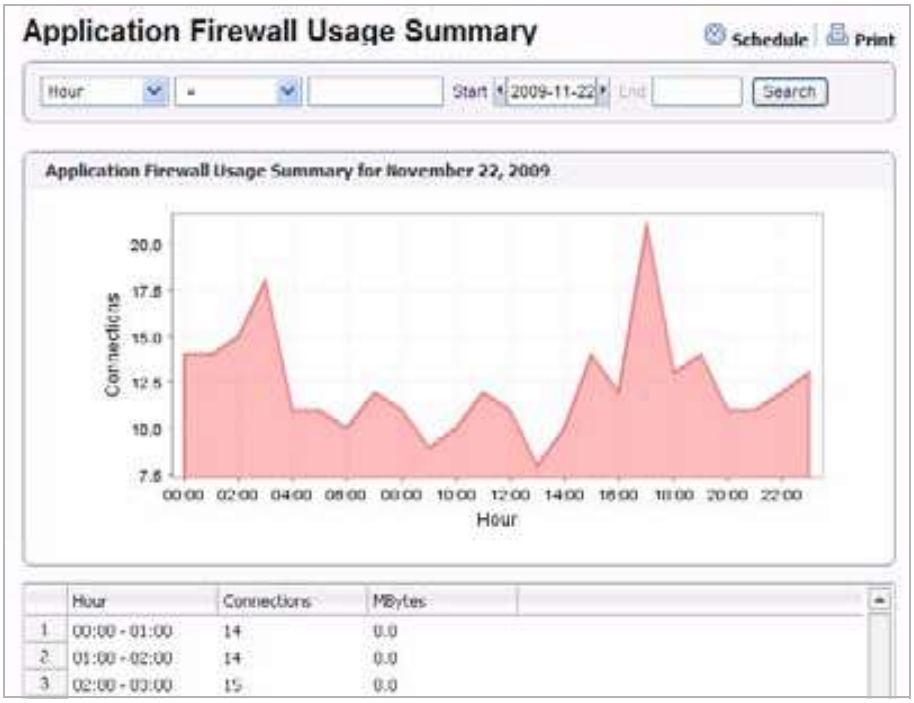
- To view the applications most often intercepted by Application Firewall, see “Viewing Application Firewall Top Applications” on page 284.
- To view the users whose traffic is most often intercepted by Application Firewall, see “Viewing Application Firewall Top Users” on page 285.
- To view the Application Firewall policies that are used the most, see “Viewing Application Firewall Top Policies” on page 286.

Viewing the Application Firewall Summary Report

The Application Firewall Summary report contains information on the number of connections incurring Application Firewall activity logged by a SonicWALL appliance during each hour of the specified day, or at the global level, for all SonicWALL appliances for the day.

To view the Application Firewall Summary report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.
3. Expand the **Application Firewall** tree and click **Summary**. The Summary page displays.



4. The table contains the following information:
   – **Hour**—when the sample was taken

Keysight, EX-1030
Page 448

- **Connections**—number of attempted connections logged (and possibly blocked) by Application Firewall
- **Mbytes**—megabytes of data transferred during the connections

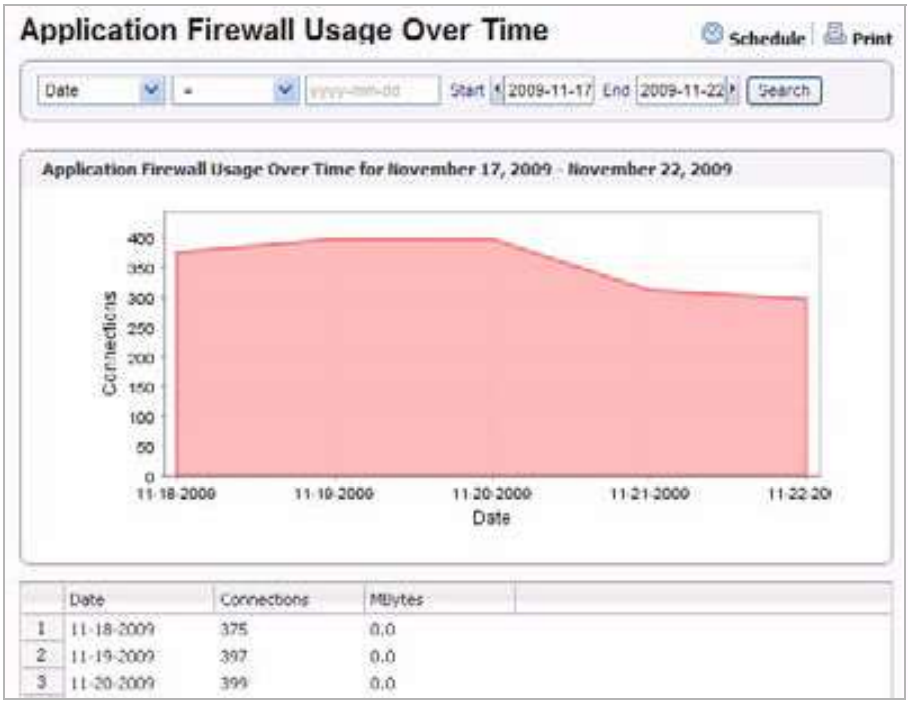
5. The ViewPoint Reporting Module shows yesterday's report. To change the date of the report, click the **Start** and **End** fields to access the drop-down calendars, select the desired dates, and then click **Search**. The ViewPoint Reporting Module displays the report for the selected day or date range.

Viewing the Application Firewall Over Time Report

The Application Firewall Over Time report displays the amount of Application Firewall usage handled by a SonicWALL appliance or a group of SonicWALL appliances for the specified time period.

To view the Application Firewall Over Time report, perform the following steps:

1. Click the **UTM** tab.
2. Select the global icon or a SonicWALL appliance.
3. Expand the **Application Firewall** tree and click **Over Time**. The Over Time page displays.



4. The table contains the following information:
   - **Date**—when the sample was taken

Keysight, EX-1030
Page 449

- **Connections**—number of attempted connections logged (and possibly blocked) by Application Firewall
- **Mbytes**—megabytes of data transferred during the connections

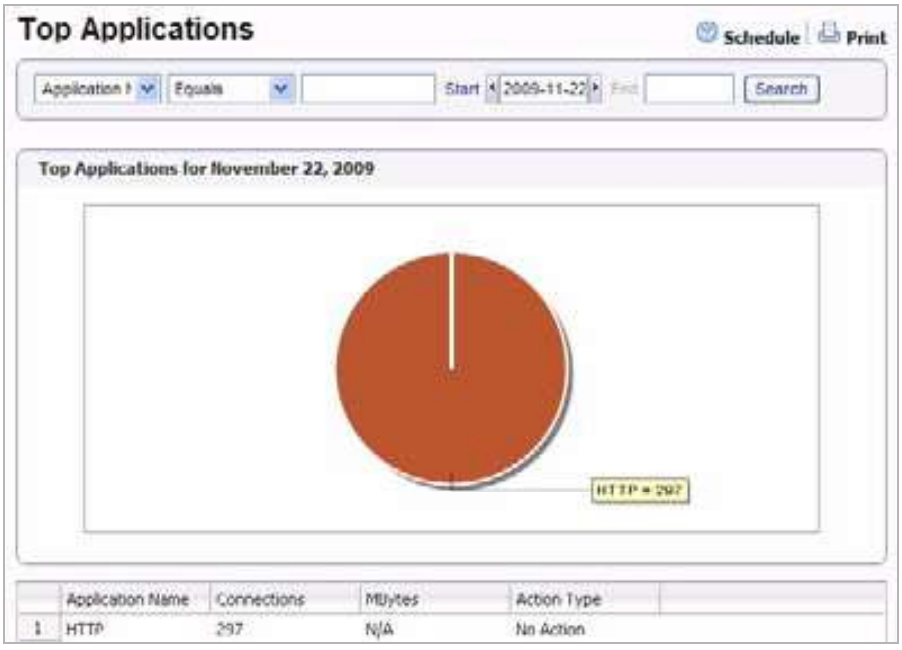
5. To change the date of the report, click the **Start** and **End** fields to access the drop-down calendars, select the desired dates, and then click **Search.** The ViewPoint Reporting Module displays the report for the selected date range.

Viewing Application Firewall Top Applications

The Top Applications report displays the applications that were most logged and/or blocked by Application Firewall on the specified date. The Top Applications report is available at the unit level.

To view the Top Applications report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Application Firewall** tree and click **Top Applications**. The Top Applications page displays.



4. The table contains the following information:
   - **Application Name**—the type of application, such as HTTP, FTP, and so on

- **Connections**—number of attempted connections logged (and possibly blocked) by Application Firewall
- **Mbytes**—megabytes of data transferred during the connections
- **Action Type**—either No Action, Logged, or Blocked

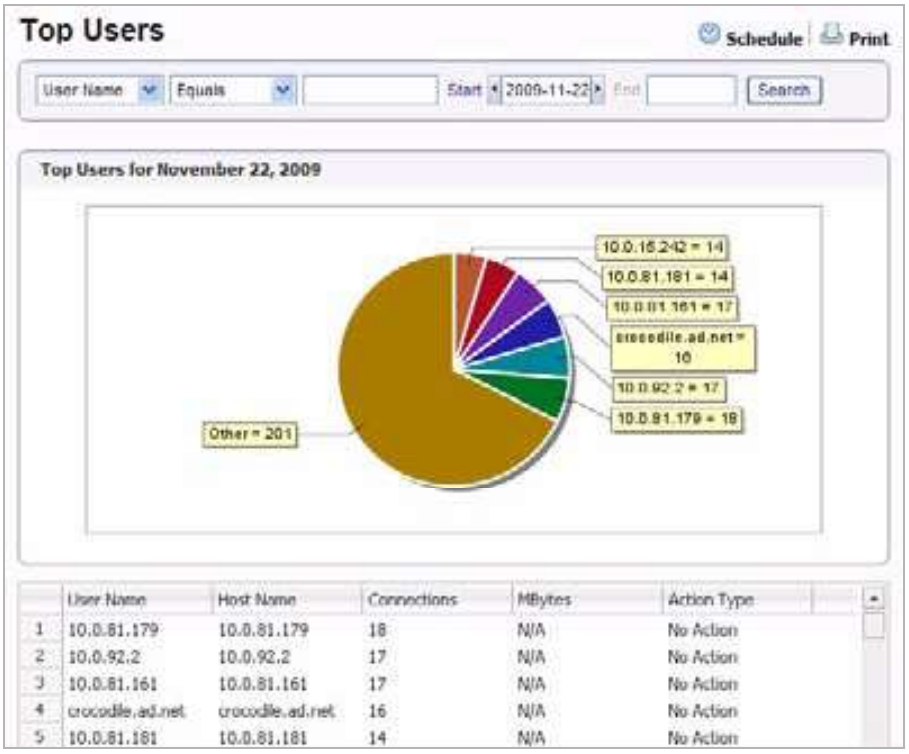
5. To change the date of the report, click the **Start** field to access the drop-down calendar, select the desired date, and then click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

Viewing Application Firewall Top Users

The Top Users report displays the users who made the most logged and/or blocked connections by Application Firewall on the specified date. The Top Users report is available at the unit level.

To view the Top Users report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Application Firewall** tree and click **Top Users**. The Top Users page displays.



4. The table contains the following information:
   - **User Name**—the user's name or IP address
   - **Host Name**—the host name or IP address of the computer that made the connection
   - **Connections**—number of attempted connections logged (and possibly blocked) by Application Firewall
   - **Mbytes**—megabytes of data transferred during the connections
   - **Action Type**—either No Action, Logged, or Blocked
5. To change the date of the report, click the **Start** field to access the drop-down calendar, select the desired date, and then click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

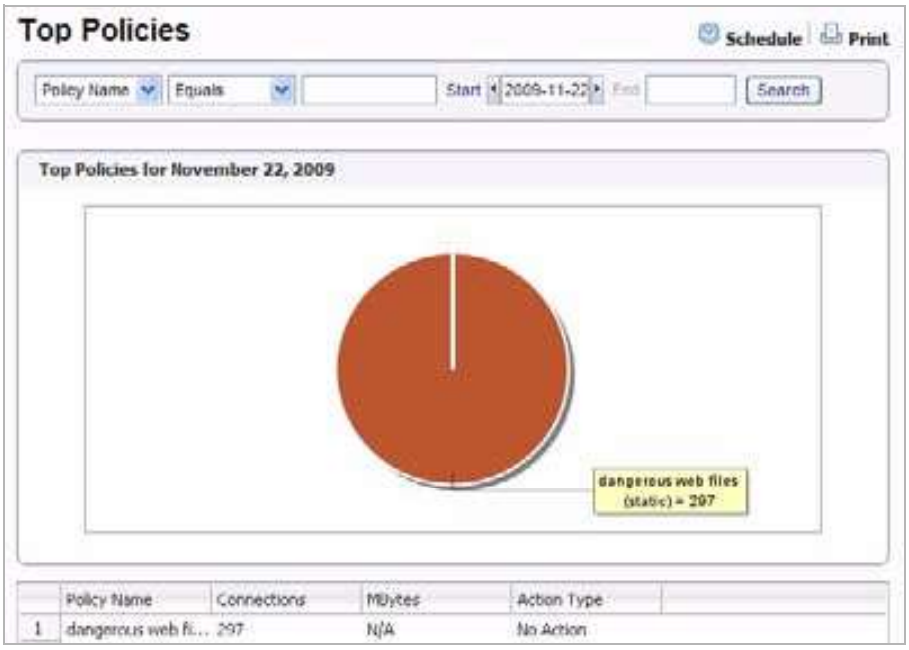
Viewing Application Firewall Top Policies

The Top Policies report displays the Application Firewall policies that were triggered the most on the specified date. The Top Policies report is available at the unit level.

To view the Top Policies report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.

3. Expand the **Application Firewall** tree and click **Top Policies**. The Top Policies page displays.



4. The table contains the following information:
   - **Policy Name**—the Application Firewall policy name
   - **Connections**—number of attempted connections logged (and possibly blocked) by Application Firewall
   - **Mbytes**—megabytes of data transferred during the connections
   - **Action Type**—either No Action, Logged, or Blocked
5. To change the date of the report, click the **Start** field to access the drop-down calendar, select the desired date, and then click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

Viewing Authentication Reports

The login reports show user logins, administrator logins, and failed login attempts for users and administrators. Authentication reports are available at the unit level.

Note All reports appear in the appliance's time zone.

Select from the following:

- "Viewing the User Login Report" on page 288
- "Viewing the Administrator Login Report" on page 289
- "Viewing the Failed Login Report" on page 289

Viewing the User Login Report

The user login report shows users that logged on to the SonicWALL appliance during the specified day to bypass content filtering or to remotely access local network resources.

To view the User Login report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Authentication** tree and click **User Login**. The User Login page displays.



4. The table contains the following information:
   - **User**—the user name.
   - **Time**—time the user logged in.
5. The ViewPoint Reporting Module shows yesterday's report. To change the date of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar.

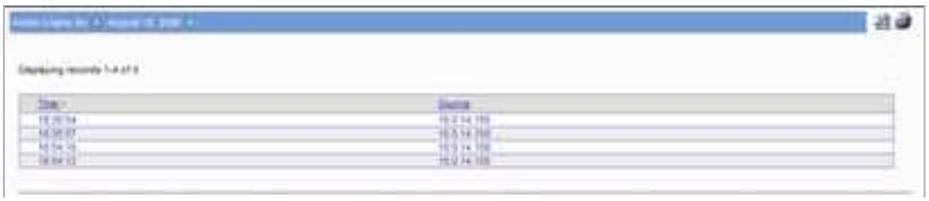
   See "Managing Report Settings" on page 154.
6. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

Viewing the Administrator Login Report

The administrator login report shows successful administrator logins during the specified day. This report is useful for identifying misuse and unauthorized management of a SonicWALL appliance.

To view the Admin Login report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Authentication** tree and click **Admin Login**. The Admin Login page displays.



4. The table contains the following information:
   - **User**—the user name.
   - **Time**—time the user logged in.
5. To change the date range of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar.

   See “Managing Report Settings” on page 154.
6. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date range.

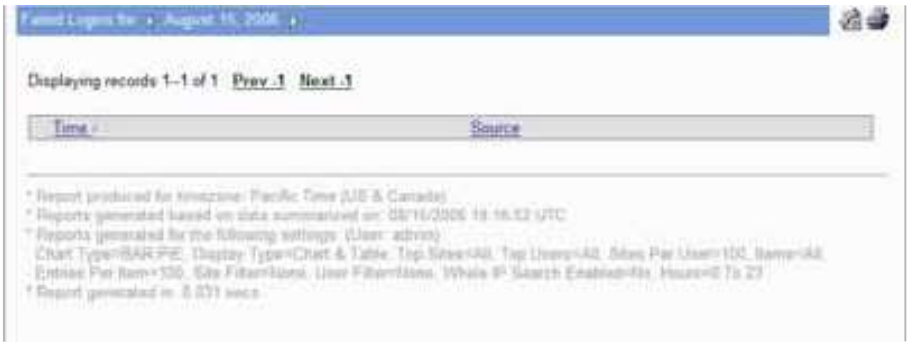
Viewing the Failed Login Report

The failed login report shows failed login attempts for users and administrators that attempted to log on to the SonicWALL appliance during the specified day. This report is useful for identifying unauthorized access attempts and potentially malicious activity.

To view the Failed Login report, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.

3. Expand the **Authentication** tree and click **Failed Login**. The page displays.



4. The table contains the following information:
   - **User**—the user name.
   - **Time**—time the user logged in.
   - **IP Address**—IP address of the user.
5. The ViewPoint Reporting Module shows yesterday's report. To change the date of the report, use the Search Bar and click the **Start** or **End** field to access the drop-down calendar.

   See "Managing Report Settings" on page 154.
6. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected date.

Viewing the Log

The Log Viewer contains detailed information on each transaction that occurred on the SonicWALL appliance. This information is stored for the time that you specified in the configuration settings.

It is necessary to enable the Log Viewer for UTM or SSL-VPN appliances for which you wish to generate Custom Reports. See "Using Custom Reports on UTM Appliances" on page 163.

Note The Log Viewer displays 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 that will be stored. For more information, see "Scheduling and Configuring Reports" on page 133.

Viewing the Log for a SonicWALL Appliance

To view the Log, perform the following steps:

1. Click the **UTM** tab.
2. Select a SonicWALL appliance.
3. Expand the **Log Viewer** tree and click **Search**. The Search page displays.



4. Select **Enable Log Viewer** and then click **Update** to turn on collection of raw data in the database and enable viewing of that log data. This can consume a large amount of space in your database. Review your database space constraints before enabling the log viewer. The maximum number of appliances for which Log Viewer can be enabled is controlled on the Console > Reports > Settings page. See "Controlling the Number of Appliances with Log Viewer Enabled" on page 72.

Note Custom Reports are available on appliances with Log Viewer enabled. See "Using Custom Reports on UTM Appliances" on page 163.

5. Under Select Search Criteria, select the date range to view data from in the **Start Date** and **End Date** fields.
6. Enter the starting time of events to view in the **Start Time** field.
7. Enter the ending time of events to view in the **End Time** field.
8. To limit the report to data originating from specific IP addresses or users, enter the source IP address or user name in the **Source IP/User** field. To view all IP addresses, enter **All.**
9. To view log entries for data originating from a particular port, enter the port number in the **Source Port** field.

10. To limit the report to data going to specific IP addresses or hosts, enter the destination IP address or host name in the **Destination IP/Hostname** field. To view log entries for data going to all IP addresses, enter **All.**
11. To view log entries for data going to a particular port, enter the port number in the **Destination Port** field.
12. Select the type of events to view from the **Message Category** list box.
13. To limit the report to messages containing a specific text string, enter the text in the **Message Text** field. Leave the field blank to view all messages.
14. Select the number of entries to display per page from the **Results Per Page** field.
15. Click **Generate Report**. The Log Viewer Results page displays.



16. Search through the entries to find the information for which you are searching. To view the next page of entries, click **Next.**
17. To generate another report, click **Search** again in the **Log Viewer** tree.

CHAPTER 16
SSL-VPN Reporting

This chapter describes how to manage SonicWALL ViewPoint SSL-VPN reporting by customizing and defining scheduled reports and summarization for SSL-VPN appliances.

For details about viewing specific SSL-VPN reports, see “Viewing SSL-VPN Reports” on page 299.

This chapter contains the following sections:

- “SSL-VPN Reporting Overview” section on page 293
- “Using and Configuring SSL-VPN Reporting” section on page 295

SSL-VPN Reporting Overview

This section provides an introduction to the SSL-VPN reporting feature. This section contains the following subsections:

- “What is SSL-VPN Reporting?” section on page 294
- “Benefits of SSL-VPN Reporting” section on page 294
- “How Does SSL-VPN Reporting Work?” section on page 295

After reading the ViewPoint SSL-VPN Reporting Overview section, you will understand the main steps to be taken in order to create and customize reports successfully.

What is SSL-VPN Reporting?

SSL-VPN reporting allows you to configure and design the way you view your reports and the manner in which you receive them. This feature offers various types of static and dynamic reporting in which you can customize the way information is reported.

SonicWALL ViewPoint SSL-VPN reporting provides a visual presentation of all your configured report settings and information. With SSL-VPN reporting, you are able to view your reports in new enhanced graphs, create granular, custom reports, create scheduled reports, and search for reports using the search bar tool.

Custom reports are also available in SSL-VPN reporting. SonicWALL SSL-VPN appliances provide a Resource Activity custom report for tracking the source, destination, and other information about resource activity passing through a SonicWALL SSL-VPN device.

The Custom Reports feature provides an intuitive, responsive interface for customizing the report layout and configuring content filtering prior to generating the report. Two types of reports are available: Detailed Reports and Summary Reports. Both provide detailed information, but are formatted to meet different needs. A Detailed Report displays the data in sortable, resizable columns, while a Summary Report provides top level information in graphs that you can click to drill down for detailed information.

Once you set up a Custom Report that meets your needs, you can save your settings as a template for reuse, set a schedule to run the report, export the report as a PDF or CSV (Excel) file, or print report pages.

Benefits of SSL-VPN Reporting

SSL-VPN reports provide visibility into the resource use by logged in users, leading to policies that enhance the user experience and the productivity of employees. The following capabilities contribute to the benefits of the SSL-VPN reporting feature:

- Custom reports can track events to the minute or second of the day for forensics and troubleshooting
- Interactive charts allow drill-down into specific details
- Table structure with ability to adjust column width of data grid
- Improved report navigation
- Report search
- Scheduled reports

How Does SSL-VPN Reporting Work?

SSL-VPN appliances send syslog data to the ViewPoint syslog collector, similar to SonicWALL UTM appliances. Once summarization takes place, you can create, schedule, view, and search for SSL-VPN reports from the ViewPoint central reporting interface.

SSL-VPN Custom Reports are based on raw syslog information contained in a database that is created daily from the raw syslog data sent from all managed or monitored appliances. This database is saved using a date/time suffix, and contains tables full of data for each appliance. All the syslog data received by SonicWALL ViewPoint is available in the database.

Note The raw syslog database required by Custom Reports is not enabled by default, as it is highly resource intensive. This functionality must be enabled per unit in the UTM > Log Viewer screen.

SSL-VPN Reporting supports scheduled reports to be sent on a daily, weekly, or monthly basis to any specified email address.

Using and Configuring SSL-VPN Reporting

This section describes how to use and configure SSL-VPN reporting. See the following subsections:

- "About Viewing Available SSL-VPN Report Types" section on page 295
- "Configuring SSL-VPN Scheduled Reports" section on page 296

About Viewing Available SSL-VPN Report Types

To view the available types of reports for SSL-VPN, perform the following steps:

1. Log into your ViewPoint management console.
2. Click the **SSL-VPN** tab.

   The SSL-VPN screen displays the following list of reports:

   Node Level reports:

   – **General**

   –Status: information about the appliance

- **Bandwidth**
  - Summary: total connections listed by hour
  - Top Users: connections listed by user
  - Over Time: connections listed by date
  - Top Users Over Time: connections listed by user for the selected date range
- **Custom Report**
  - Resource Activity: source, destination, and other information about resource activity
- **Resources**
  - Summary: connections per connection protocol (HTTPS, NetExtender, etc)
  - Top Users: connections listed by user
- **Authentication**
  - User Login: user, time, and source of successful authentication-daily. User Login reports now combine admin users with all other users in the same report.
  - Failed login: time and source host of failed logins for one day

Global Level Reports:

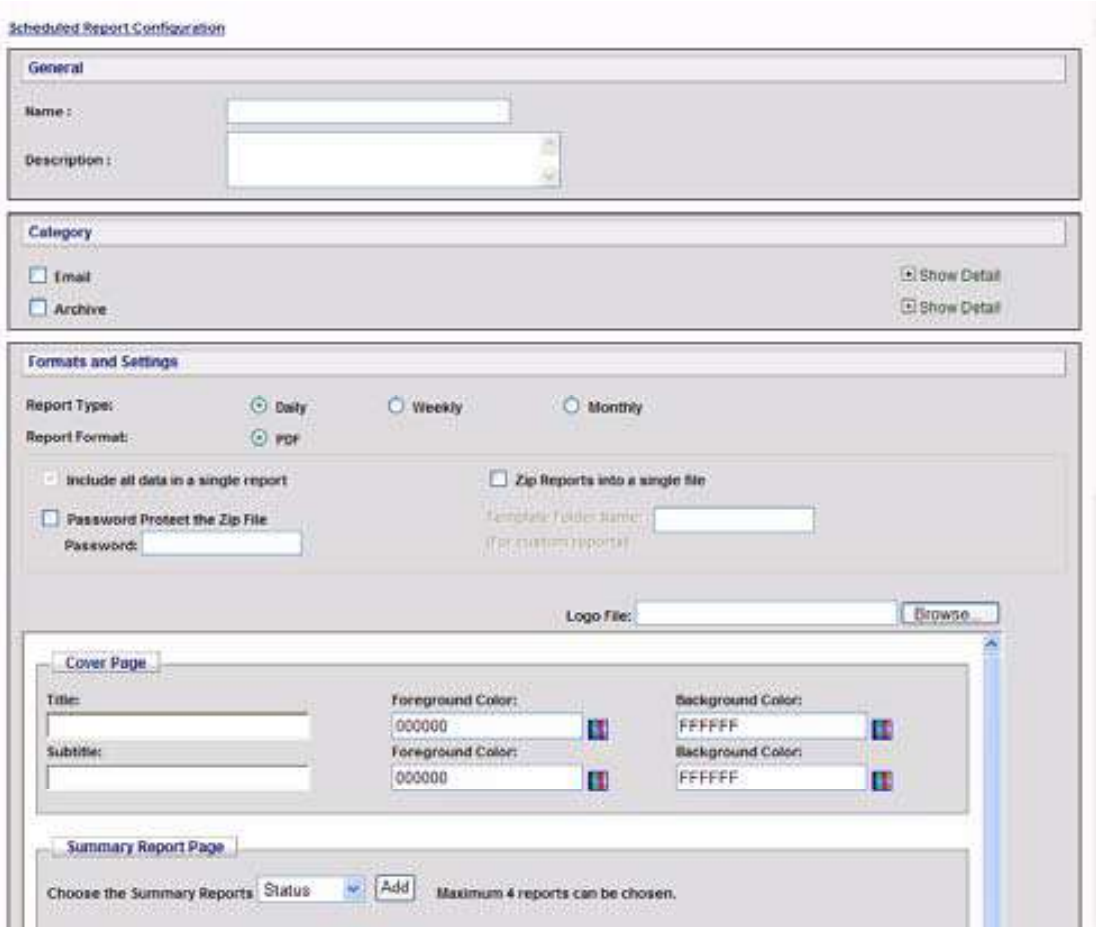
- **General**
  - Status: number of units in the system and their ViewPoint license status
- **Bandwidth**
  - Summary: connections per SSL-VPN appliance
  - Over Time: total connections by date for group

Configuring SSL-VPN Scheduled Reports

To configure SSL-VPN scheduled reports and summarization, perform the following tasks:

1. On the **SSL-VPN** tab, navigate to **Configuration > Scheduled Reports**.
2. Click the **Add** button.

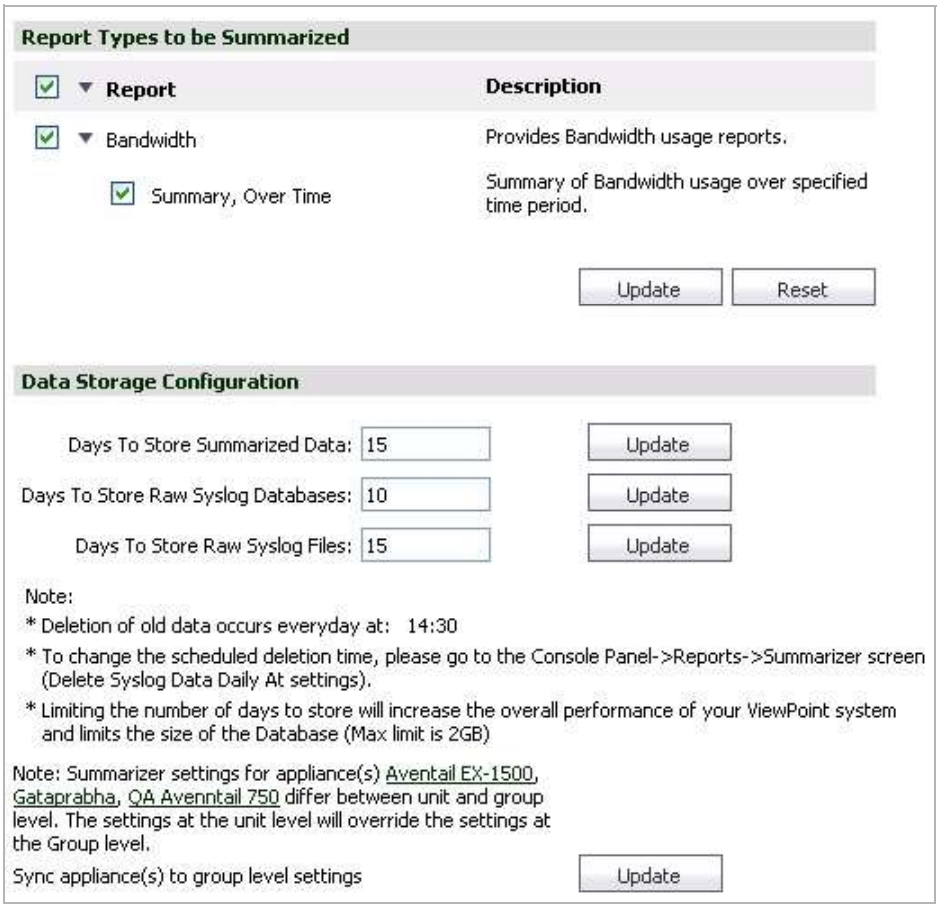
3. The Scheduled Report Configuration form displays. Fill out the fields accordingly. For more information, see the following sections:
   - “Configuring Scheduled Reports” on page 134
   - “Scheduling PDF Compliance Reports” on page 144



Configuring SSL-VPN Summarization

1. On the **SSL-VPN** tab, navigate to **Configuration > Summarizer Settings**. The reports that can be summarized for a SSL-VPN appliance are configurable at either global or unit level. The screen displays the configuration appropriate for the level. The report type lists can also be expanded for a detailed description of report content.

The report types you can summarize are shown below.



SSL-VPN reports generated in ViewPoint can be exported in PDF format, providing easy online transfer. For more information about the Summarizer and exporting reports in PDF format, see:

- “Selecting Reports for Summarization” on page 137
- “Configuring Data Storage Settings” on page 139
- “Using Summarize Now” on page 76
- “Scheduling PDF Compliance Reports” on page 144

Keysight, EX-1030
Page 464

CHAPTER 17
Viewing SSL-VPN Reports

This chapter describes the available reports for SonicWALL SSL-VPN appliances.

For information on how to configure scheduled reports and summarization, see:

- “Using and Configuring SSL-VPN Reporting” on page 295

Select from the following reports:

- “Viewing General Status Reports” section on page 299
- “Viewing SSL-VPN Bandwidth Reports” section on page 301
- “Using SSL-VPN Custom Reports” section on page 307
- “Viewing SSL-VPN Resources Reports” section on page 325
- “Viewing SSL-VPN Authentication Reports” section on page 330
- “Viewing the SSL-VPN Log” section on page 332

Viewing General Status Reports

The **General > Status** page contains information about the SSL-VPN appliance or group of SSL-VPN appliances.

To view the Status page, perform the following steps:

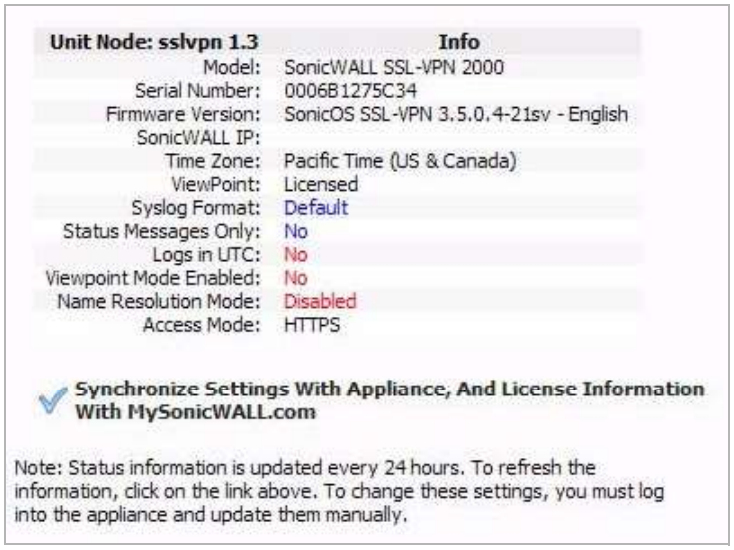
1. Click the **SSL-VPN** tab.
2. Select **MyReportsView** or an SSL-VPN appliance in the left pane.

3. In the center pane, expand the **General** tree and click **Status**. The Status page displays.

   When **MyReportsView** is selected, the Status page displays the license status of all SSL-VPN appliances.



   When a unit is selected, the Status page displays information about the SSL-VPN appliance, including model, serial number, firmware version, time zone, license status, log settings, and other settings.



4. In the unit view, to synchronize settings with the SSL-VPN appliance and license information with MySonicWALL, click **SynchronizeSettings With Appliance, And License Information With Mysonicwall.com**.

Viewing SSL-VPN Bandwidth Reports

Bandwidth reports display the amount of data transferred through one or more selected SSL-VPN appliances.

Bandwidth reports are an ideal starting point for viewing overall bandwidth usage. You can view bandwidth usage view by hour, day, or over a period of days. Additionally, you can view the top users of bandwidth.

From this information, you can determine network strategies. For example, if you need more bandwidth, you might need to upgrade network equipment, or you might simply need to curtail the bandwidth usage of a few employees.



Note All reports appear in the time zone of the selected appliance.

Select from the following:

- “Viewing SSL-VPN Bandwidth Summary Reports” on page 301
- “Viewing SSL-VPN Top Users of Bandwidth Reports” on page 303
- “Viewing SSL-VPN Bandwidth Usage Over Time Reports” on page 304
- “Viewing SSL-VPN Top Users of Bandwidth Over Time Reports” on page 306

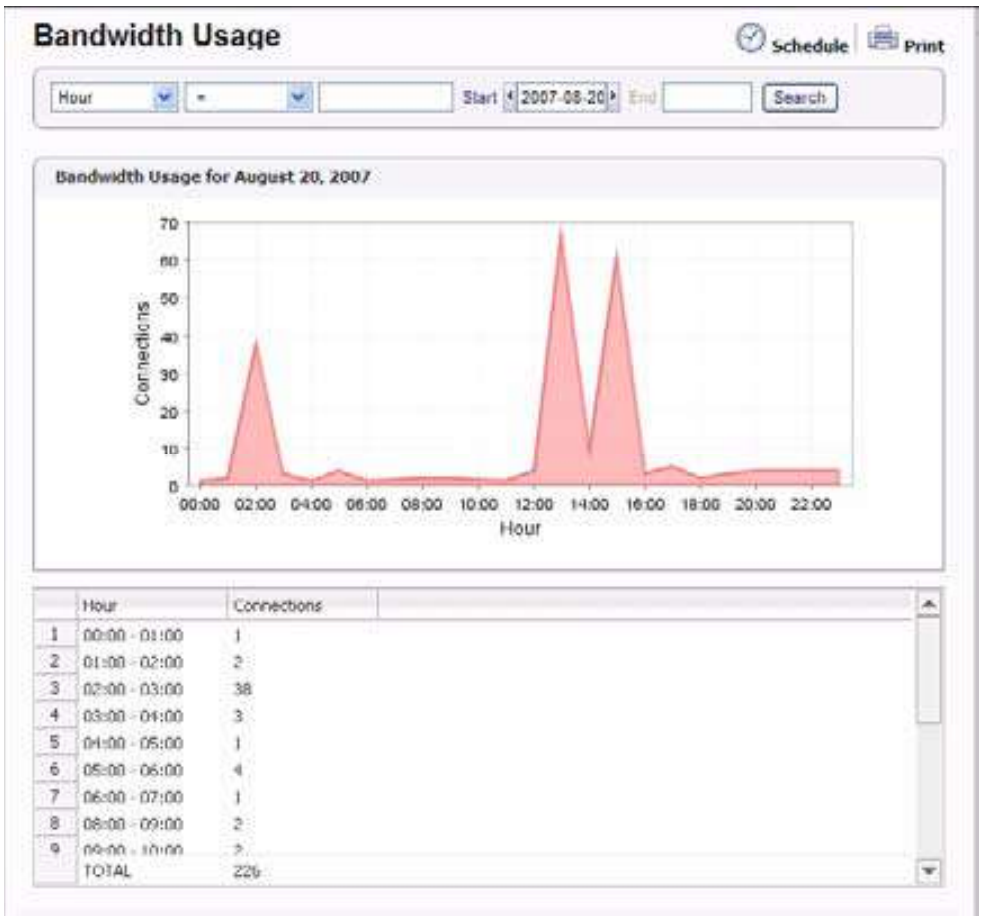
Viewing SSL-VPN Bandwidth Summary Reports

The Bandwidth Summary report shows the number of connections handled by a SSL-VPN appliance during each hour of the specified day, or at the global level, by each SSL-VPN appliance for the day.

To view the Bandwidth Summary report, perform the following steps:

1. Click the **SSL-VPN** tab.
2. Select the global icon or a SSL-VPN appliance.

3. Expand the **Bandwidth** tree and click **Summary**. The Summary page displays.



4. The graph displays the number of connections to the SSL-VPN appliance during each hour of the day.
5. The table contains the following information:
   - **Hour**—when the sample was taken.
   - **Connections**—number of connections to the SSL-VPN appliance
6. The ViewPoint Reporting Module shows yesterday's report. To change the date of the report, click the **Start** field to access the drop-down calendar.
7. After selecting a date, click **Search**. The ViewPoint Reporting Module displays the report for the selected day.

Note The date setting will stay in effect for all similar reports during your active login session.

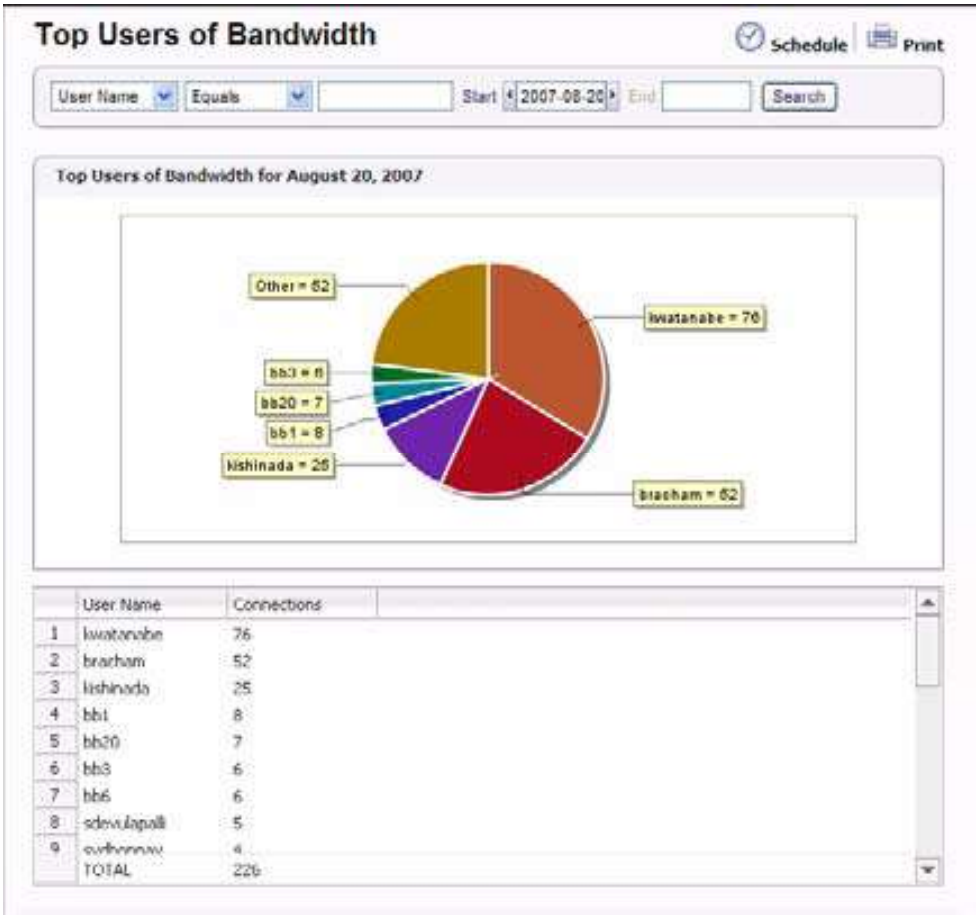
Keysight, EX-1030
Page 468

Viewing SSL-VPN Top Users of Bandwidth Reports

The Top Users report displays the users who used the most connections on the specified date.

To view the Top Users report, perform the following steps:

1. Click the **SSL-VPN** tab.
2. Select a SSL-VPN appliance.
3. Expand the **Bandwidth** tree and click **Top Users**. The Top Users page displays.



4. The pie chart displays the percentage of connections used by each user.

5. The table contains the following information for all users:
   - **Users**—the user name
   - **Connections**—number of connection events or “hits”
6. By default, the ViewPoint Reporting Module shows yesterday’s report, a pie chart for the top six users, and a table for all users. To change the date of the report, click the **Start** field to access the drop-down calendar.
7. To display a limited number of users, use the Search Bar fields.



Note The search bar fields use pattern matching with operators such as “contains”. For example, “john” will match john_smith, john42, or big_john.

8. When you are finished, click **Search**. The ViewPoint Reporting Module displays the report for the selected day.



Note The date setting will stay in effect for all similar reports during your active login session.

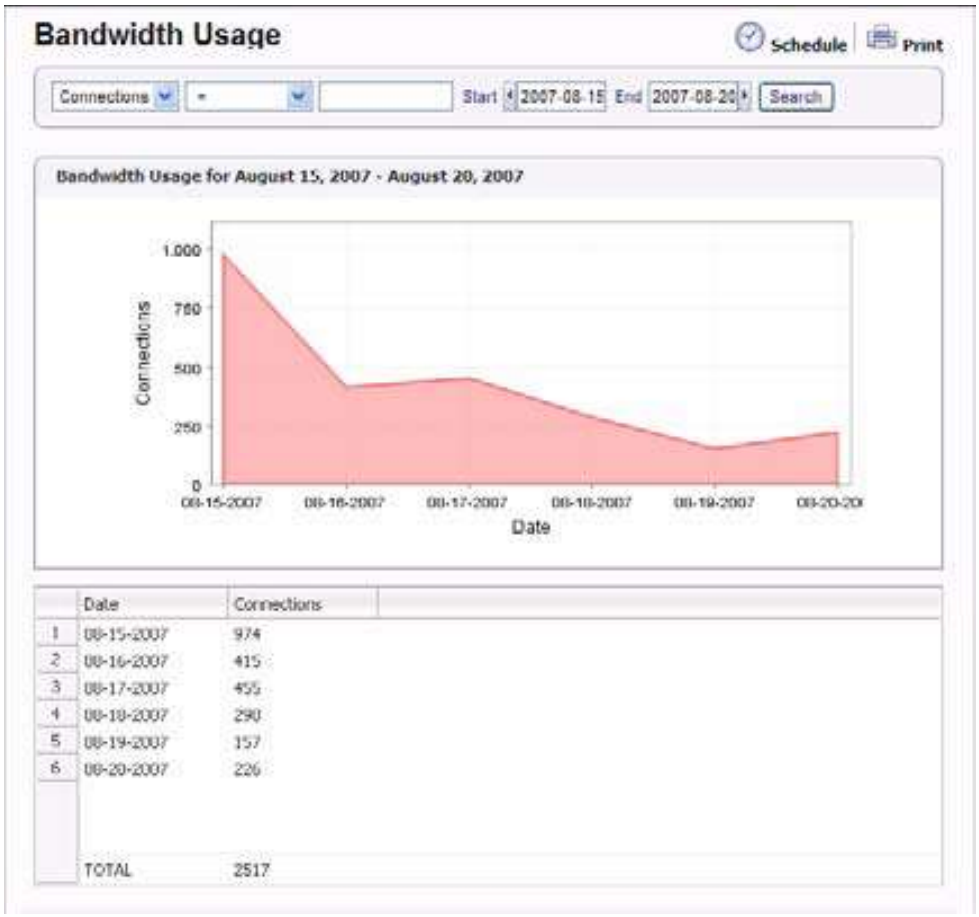
Viewing SSL-VPN Bandwidth Usage Over Time Reports

The Bandwidth Usage Over Time report displays the daily number of connections handled by a SSL-VPN appliance or a group of SSL-VPN appliances for the specified time period.

To view the Bandwidth Usage Over Time report, perform the following steps:

1. Click the **SSL-VPN** tab.
2. Select the global icon or a SSL-VPN appliance.

3. Expand the **Bandwidth** tree and click **Over Time**. The Over Time page displays.



4. The graph displays the number of connections during each day of the specified time period.
5. The table contains the following information:
   - **Date**—when the sample was taken
   - **Connections**—number of hits
6. To change the date of the report, use the Search Bar and click the **Start** or **End** fields to access the drop-down calendar.
7. When you are finished, click **Search.** The ViewPoint Reporting Module displays the report for the selected date range.

Note These date settings will stay in effect for all similar reports during your active login session.

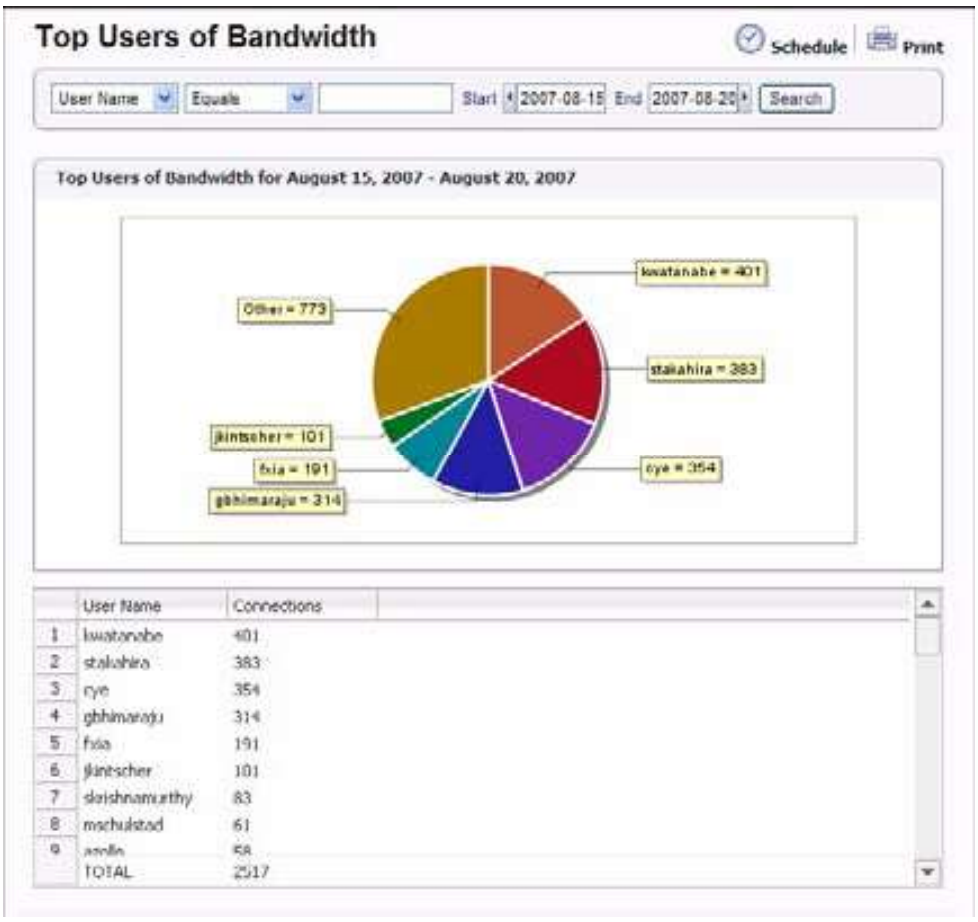
Keysight, EX-1030
Page 471

Viewing SSL-VPN Top Users of Bandwidth Over Time Reports

The Top Users Over Time report displays the users who used the most connections during the specified date range. This report is available at the unit level.

To view the Top Users Over Time report, perform the following steps:

1. Click the **SSL-VPN** tab.
2. Select a SSL-VPN appliance.
3. Expand the **Bandwidth** tree and click **Top Users Over Time**. The Top Users Over Time page displays.



4. The pie chart displays the percentage of connections used by the top users.

Keysight, EX-1030
Page 472