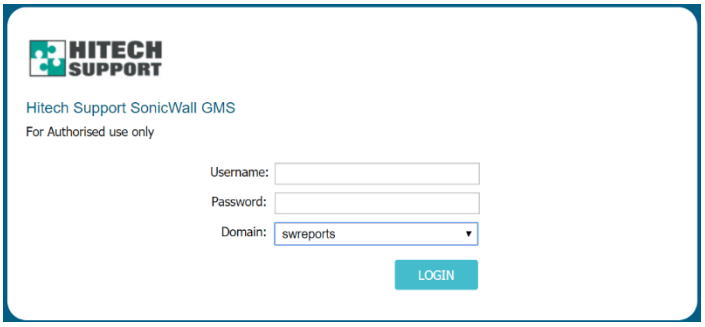
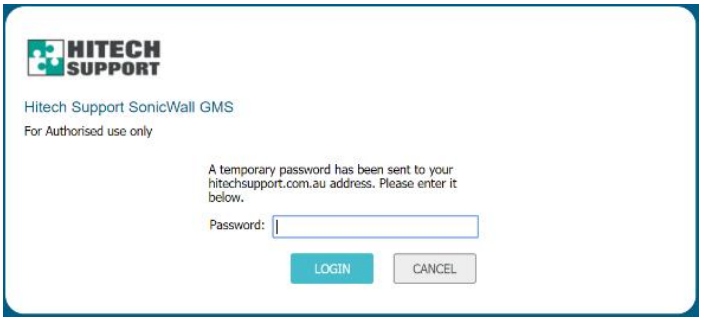
How to access the reporting server

Navigate to https://swreports.hitechsupport.com.au and enter your username and password.

Note: if you are logging in for the 1st time, contact Hitech Support to setup your login and multi-factor authentication. Please call 02 8883 4355 or email support@hitechsupport.com.au

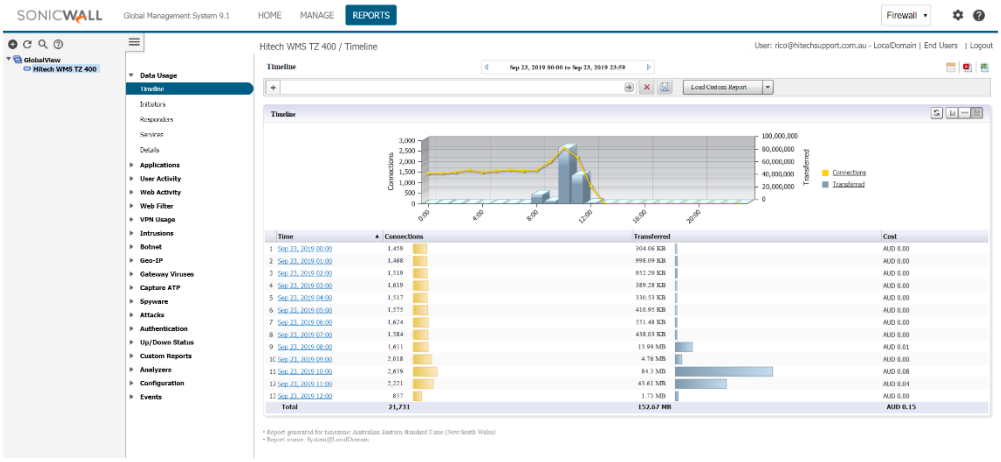


Enter the temporary password that was sent to you mobile phone via SMS



Enter your username and password again on the next screen

After you have logged in, click on the Reports tab to load the reporting interface screen.



You can select the firewall you would like to report on in the left most column – the firewall panel. Selecting an indivdual firewall will give the most detailed reports. Selecting the parent group will report on all firewalls underneath, however, it will have limited amount of reports available.

Using the SGMS Report server

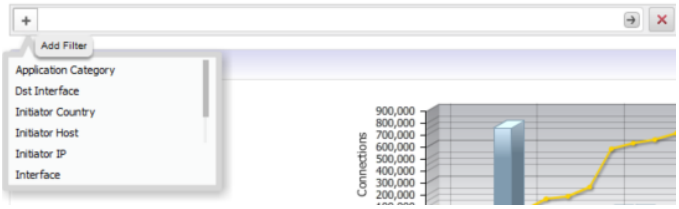
The reporting server comes with a number of simple, pre-defined reports by the software vendor. You can create your own custom reports to suit your requirements using filters and by 'drilling down' on the hyperlinks in the report.

Reports can also have the following features:

- Filters can be saved as a custom report template for reuse and scheduling;
- Moving the mouse pointer over the chart displays sample value for the intervals;
- You can sort data by clicking on the column headers.

Filter bar

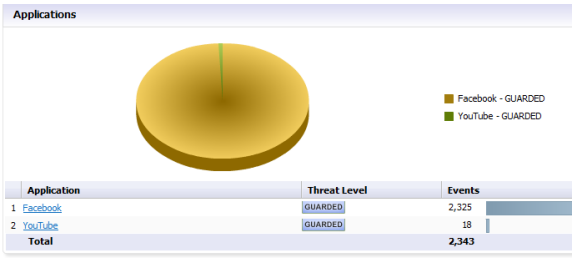
The filter bar is used to narrow the results of a report, and allows further detail to be shown. The Filter bar has pre-defined filters from a pull-down menu, which are context dependant.



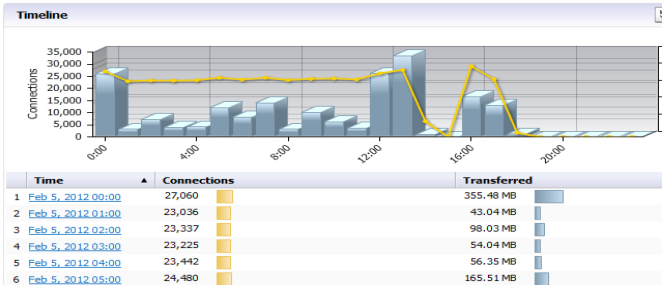
Built in reports

Data usage

The WMS reports shows the data usage specific to the WMS hotspot while these SGMS data usage reports displays information on everything that passes through the SonicWall firewall including the top users, host or IP addresses using the most data, and the top destinations of where data is being downloaded from.



- **Timeline.** Displays the data used and the amount of connections opened every hour over the period specified. The initial report is calculated on traffic going through any interface on the firewall.



- **Initiators.** Shows the top IP addresses, hosts or users that are using the most data. The initial report shows both internal and external (from the internet) initiators.
- **Responders.** Similarly, Responders shows the top destination of where data is being download from.
- **Services**. Displays the services that are being used the most from a data usage point of view.
- **Details**. This is a combination of the first four reports on one report.

Applications

This requires a Gateway Antivirus/IPS license to be present on the firewall. This shows the applications sending or receiving traffic through the firewall.

- **Data usage**. Displays the amount of traffic from each application over the time period.
- **Detected**. Displays the applications that have been detected.
- **Blocked**. Displays the amount of matches to an application firewall rule where a blocking action has been specified.
- **Categories.** Displays the categories of the most common applications detected or blocked.
- **Initiators.** Shows the top IP addresses, hosts or users that are using the applications.

User Activity

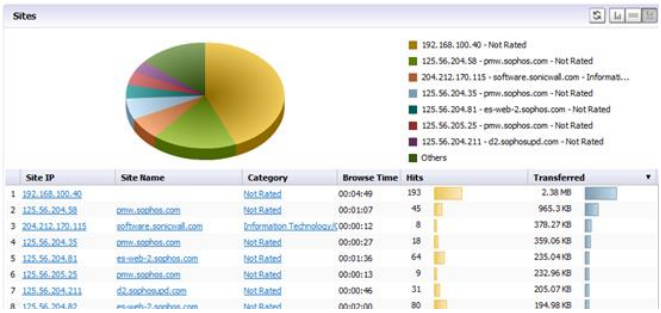
This displays detailed activity for user(s) that are specified in the report filter criteria. This report is only useful when some type of user authentication is being performed to the firewall, such as in a staff LAN where the SonicWall SSO agent has been deployed.

Web Activity

These reports display detailed information about web browsing activities.

- **Categories.** Displays hits and browse time grouped by category. Note: unless a SonicWall Content Filter subscription has been purchased, the categories will be blank.

- **Sites**. Displays the top sites



- **Initiators.** Shows the top IPs, hosts or users that are performing web browsing.