Basic Monitoring Tools

https://campus.barracuda.com/doc/12194191/

See the **BASIC > Dashboard** page for performance statistics on the Barracuda Web Security Gateway, to monitor the health of the system, and to make sure traffic is flowing as expected. Web requests by users on the network are tracked and presented as raw data in the web logs as described below, but that data is also packaged and presented in an easy-to-read format in the Reports module. Reports listed on the **BASIC > Reports** page should serve the needs of both managers and IT administrators regarding user productivity, bandwidth usage, infection/malware detection and more. See Reporting for details. For instructions about configuring and scheduling reports, click **Help** on the **BASIC > Reports** page.

Viewing performance statistics

The **BASIC > Dashboard** page provides an overview of the health and performance of your Barracuda Web Security Gateway. You can create and customize the layout and content of multiple dashboards as described in How to Customize the Dashboard Page. The following statistics are included on the default Dashboard:

- Filtering statistics (such as threats blocked by the filtering rules, blocked visits to known spyware websites, blocked downloads of spyware or viruses) for the past day and hour, as well as total statistics since installation (or last reset) of the Barracuda Web Security Gateway.
- Performance statistics, such as CPU temperature, throughput, system load and TCP connections. Statistics displayed in red signify that the value exceeds the normal threshold.
- **Operating Mode**: configured on the **BASIC > IP Configuration** page. Possible modes are:
  - *Active*: Traffic is logged and policies are applied.
  - *Audit*: In inline mode, traffic is logged only. Policies are not applied. In forward proxy deployment, traffic is logged and policies are applied, just like they are in *Active* mode.
  - *Safe*: Note that this mode is systematically set if the system load on your Barracuda Web Security Gateway is excessive because either the maximum number of TCP connections allowed on your model is exceeded, or the reporting engine is processing a large volume of data. ***Safe* mode cannot be triggered over the web interface and is not applicable if the Barracuda Web Security Gateway is deployed in WCCP configuration.** In *Safe* mode the device will pass web traffic through without filtering and logging. The Barracuda Web Security Gateway will send a notification email to the **System Alerts Email Address** that is specified on the **BASIC > Administration** page indicating the reason the device is experiencing a load issue. If the number of current TCP connections and/or the load on the reporting engine returns to normal range, the Barracuda Web Security Gateway will resume *Active* mode; otherwise the device will remain in *Safe* mode and traffic will not be filtered or logged. At this point it is recommended that you place the Barracuda Web Security Gateway in *Audit* mode and troubleshoot the problem. For further assistance, please contact Barracuda Networks Technical Support.

- **System Uptime** shows the time duration, in days, for which the system has been up and running continuously.
- **Throughput** gauges the total volume of traffic that is passing through the Barracuda Web Security Gateway and is measured in Mb/s.
- **TCP Connections** indicates number of concurrent TCP connections used by the Barracuda Web Security Gateway to service Internet traffic. TCP Connection usage can be monitored while in Audit mode as well as in Active mode without affecting production traffic. A single user typically requires 1 to 1.5 active TCP connections; however, the peak number of TCP connections can significantly increase with heavy Web browsing or with bandwidth-intensive Internet applications such as voice, instant messaging (IM) or other streaming media applications.
- **Cloud Control** indicates whether or not this Barracuda Web Security Gateway is connected to the Barracuda Cloud Control (BCC) management tool. For general information about Barracuda Cloud Control, see Overview. For details about connecting the Barracuda Web Security Gateway to the BCC, see How to Set Up Barracuda Cloud Control.
- **System Load** represents an estimate of CPU and disk load on the system. It is not unusual for the load to reach 100%, especially when the incoming queue is large. 100% load for long periods of time indicates trouble in the system, especially if the incoming queue continues to increase in size. If the System Load exceeds 50% for more than 5 minutes, the Operating Mode will automatically shift to Safe mode (unless the Barracuda Web Security Gateway is deployed in WCCP configuration) and will pass traffic without filtering or logging until normal operation can be resumed. See the online help for the **BASIC > Dashboard** page for more information.
- **Cache Hit Ratio** indicates the percentage of requests handled by the cache.
- **Subscription** status for Energize Updates, Instant Replacement, and Premium Support.
- Lists of infected clients and blocked web requests.
- A set of bar graphs that illustrate an hourly breakdown of requests made by your users in the last 24 hours, and a set of bar graphs that illustrate a daily breakdown of requests made by your users in the last 30 days. Both sets of graphs illustrate the following data:
  - Number of requests blocked
  - Number of requests received
  - Number of kilobytes per second used by the requests allowed

  Each bar graph is accompanied by two Top Ten lists: domains represented in the graph and web content categories represented in the graph.
- LAN, WAN and Auxiliary (AUX) port connection details are associated with icons in the Link Status section, displaying connectivity where applicable (version 6.0.1 and higher). Hover the mouse over the LAN icon, for example, to see LAN connection details (MAC address, IP address, throughput). If the AUX port is configured, the icon will be displayed with details for that port in addition to icons for either or both the WAN and LAN. On the Barracuda Web Security Gateway Vx, only the LAN port icon and details are displayed.

To customize one or more dashboards, displaying only the data that matters to the administrator, see How to Customize the Dashboard Page.

Logs for Web Traffic and Syslog

Web Traffic Log

The **BASIC > Web Log** page displays a list of system logs for your Barracuda Web Security Gateway. On a regular basis you should view the Web Log page to monitor the web and spyware traffic (both HTTP and non-HTTP) passing through your Barracuda Web Security Gateway. The page also has a button used to clear all traffic logs as needed. Use this page to view the following information about each entry in this log:

- Date and time the Barracuda Web Security Gateway processed the request.
- IP address of the client that originated the request.
- IP address of the requested website or application
- For search engine requests, the search keyword(s) entered by the user
- Type of file contained in the request, as designated by the HTTP header. For a list of common MIME types, see the help page for the MIME Type Blocking feature.
- The user name or group that sent the request.
- The action taken by the Barracuda Web Security Gateway (Allowed, Detected, Warned, Monitored, Blocked).
- The reason the Barracuda Web Security Gateway performed the action.
- Detailed information about the actions.
- Number of bytes of data processed for this request.

You can perform the following operations on the **Web Log** page:

- Apply filters to locate specific log entries
- Refresh to update the log. The most recent entry is at the top of the list.
- Clear the log to purge all the current entries.
- Export the displayed entries to a CSV file.

Application log

The **BASIC > Application Log** page displays the log of web application traffic blocked by the Barracuda Web Security Gateway. Note that the Barracuda Web Security Gateway Vx virtual machine does not block applications. Use this page to view the following information about each entry in this log:

- Date and time the Barracuda Web Security Gateway blocked the request.
- IP address of the client that initiated the request.
- Name of the application that was blocked.

You can perform the following operations in the **Application Log** page:

- Customize the appearance of the display
- Update the contents displayed in this page

- Clear the contents of the traffic log itself
- Filter the entries displayed
- Export the displayed entries to a CSV file

Using a Syslog Server to Centrally Monitor System Logs

Syslog is a standard UNIX/Linux tool for sending remote system logs and is available on all UNIX/Linux systems. The Barracuda Web Security Gateway provides syslog data for both web traffic and system events. Use the **ADVANCED > Syslog** page to specify servers to which the Barracuda Web Security Gateway sends each type of syslog data.

Syslog servers are also available for Windows platforms from a number of free and premium vendors. Barracuda Networks has tested with a Windows freeware syslog server from Kiwi Enterprises (www.kiwisyslog.com). Barracuda Networks makes no guarantees that your Barracuda Web Security Gateway will be completely compatible with this syslog server. **Note that syslog support is not available on the Barracuda Web Security Gateway 210.**

For details about syslog output from the Barracuda Web Security Gateway, see Syslog and the Barracuda Web Security Gateway.

Warned Activity List

The **BASIC > Warned Activity** page displays the list of all warned activity that is in effect for the client machines protected by the Barracuda Web Security Gateway system. Use this page to view the following information about each entry in this log:
Date and time that the warned activity was triggered.

- IP address of the client machine that triggered the warned activity.
- Username that triggered the warned activity. This field indicates whether the user account is from the local, LDAP or NTLM realm.
- The URL that the user was attempting to access when the warned activity triggered.
- The domain names that triggered the warned activity.
- The Web content category that triggered the warned activity.

You can perform the following operations in the **Warned Activity** page:

- View details about a warned activity
- Clear all warned activity

A warned activity remains in effect until it times out (as configured in the **BLOCK/ACCEPT > Configuration** page) or until it is explicitly removed by the Administrator (using the **BASIC > Warned Activity** page). If the user attempts to access the same website after a warned activity times out or is deleted, the user must click the **Proceed** button to re-acknowledge the warning and then access the website again.

List of Infected Clients

The **BASIC > Infection Activity** page displays outbound activity monitored by the Barracuda Web Security Gateway to sites/IP addresses that are known to be malicious, and displays a list of clients in the network that are infected with a virus or with spyware. Check this page for activity by client hostname or IP address to determine if further investigation should be performed on the client. The data in the log includes:

- **Spyware** – Names of the threats blocked by the Barracuda Web Security Gateway.
- **Count** – Number of times that the Barracuda Web Security Gateway blocked this threat.
- **Last Seen** – Date and time this threat type was last detected on this client.
- **Port** – The port over which the infection was detected.

Remote Devices Tracking by Time

The Barracuda Web Security Gateway maintains a log of remote user and mobile devices seen by the Barracuda Web Security Agent (WSA). Logged data includes the date and time when a remote user logged in or a mobile device was synchronized with Barracuda Web Security Gateway settings. See the **ADVANCED > Remote Devices** page to view and configure. Logged fields include:

- **Username**– Username created for the device user login.
- **Domain**– Domain the user is logged into
- **Device Name**– Name given to the mobile device for identification
- **Device Type**– Mobile device type, for example: iPad, iPhone, etc.
- **IP Address**– IP address of the mobile device
- **Last Seen**– Date and time of the last user login or device synchronization with the Barracuda Web Security Gateway

See also the **Remote Devices** section of the **Dashboard** page for a simple list of username and number of devices per user.

Task Manager

The **ADVANCED > Task Manager** page provides a list of system tasks that are in the process of being performed and also displays any errors encountered when performing these tasks.
Some of the tasks that the Barracuda Web Security Gateway tracks include:

- Linked management setup
- Configuration restoration

If a task takes a long time to complete, you can click **Cancel** next to the task name and then run the

task at a later time when the system is less busy. The **Task Errors** section will list an error until you manually remove it from the list. Note that the errors are not phased out over time.