Logging

https://campus.barracuda.com/doc/96026556/

The Barracuda CloudGen Firewall generates log events for system processes on the box layer and for each configured service. To limit the size of a single log file, the Barracuda CloudGen Firewall creates a new log file for each service every four hours. All log files are stored in plain text in the system's `/var/phion/logs` directory and can be viewed and filtered conveniently with the Log Viewer in the Barracuda Firewall Admin application. For information on how to view and filter log file entries, see the LOGS Tab.

The `/var/phion/logcache` directory contains the **L**og **A**ccess **F**iles (`*.laf`) for internal log file processing only. These are BDB (Berkeley DB) files that are suitable for fast access to large log files. Intervention via the command line is generally not recommended. To view the contents of the `.laf` files, use the `showbdb` utility.

DO NOT write, rename or put any files into this directory. Editing the contents of this directory may cause logs to be displayed incorrectly.

Configure Log File Handling

1. Go to **CONFIGURATION > Full Configuration > Box > Infrastructure Services > Log Configuration** .
2. Click **Lock**.
3. Set the parameters for **Generate Log Data** and **Store Log Data**.
4. Click **Send Changes** and **Activate**.

The following table displays how the log daemon saves log files, when the parameters are set:

Generate Log Data	Store Log Data	Result
yes	yes	Logs are sent to the syslog service and written to disk.
yes	no	Logs are sent to the syslog service but not written to disk.
no	yes	Logs are neither sent to the syslog service nor written to disk. If you want to activate the writing of log files to disk only, you must set parameters **Generate Log Data** AND **Store Log Data** to **yes** and disable syslog streaming in the **Infrastructure Services > Syslog Streaming** configuration.
no	no	Logs are neither sent to the syslog service nor written to disk.

Format and Types

Log file entries are divided into the following segments:

- **Time** – The time when an event has taken place. This indicator marks individual log entries.
- **Type** – Shows the following types of the log files.
  - **Warning** – Uncritical log event (e.g. login to the system)
  - **Error** – Log event error (e.g. system calls or clock skew)
  - **Fatal** – System critical log events.
  - **Notice** – Normal system log events.
  - **Security** – Security relevant log events.
  - **Panic** – Marks critical log events compromising the system's functionality and stability.
- **TZ** – Displays the UTC time zone offset compared to the local box time.
- **Message** – Description of the log event.

Viewing Log File Entries

The Barracuda Firewall Admin application offers a graphical log file interpreter for viewing and filtering log files. For a list of all available log files in the log file tree, see Available Log Files and Structure .

Log File Propagation

Log files are by default stored on the local filesystem of the unit. In addition, log files can be sent to external Syslog servers. Firewall log events can be forwarded to the Barracuda Firewall Control Center for central log consolidation for centralized management. For more information, see How to Configure Syslog Streaming and How to Enable the Firewall Audit Log Service.