Types of Logs

This section provides description about each type of log on the Barracuda Web Application Firewall.

Note: The number of logs stored in the system depends on the model of the Barracuda Web Application Firewall. The details are available here.

Web Firewall Logs

Web Firewall Logs are generated whenever suspicious activities, as specified in the access control lists, are detected. The log contains entries for every HTTP request that the Barracuda Web Application Firewall has denied. This data allows the administrator to identify the client that made the request, the method used and the result of the request. Using these logs, you can fine tune the security settings. For more information, refer to the **Tuning Security Rules Using Web Firewall Logs** article.

When a service is created, the default web firewall policy is associated with the service, and the threshold for logging error messages is initially set to 5-Notice. At that threshold, all violations/error messages (critical attack information to debug information) are logged on the **BASIC > Web Firewall Logs** page. You can change the log level, based on your requirements, by editing a service on the **BASIC > Services** page.

Note:

- Whenever a log is generated in **Web Firewall Logs** and **Access Logs**, a unique ID (UID) is associated with the log. You can select the filter option **ID** and enter a unique ID to search a specific log.
- The unique ID can be embedded in the custom response page. For more information, refer to the How to Create a Custom Response Page article.

Access Logs

Access Logs are generated for all user request patterns. Access logs allow you to monitor the web traffic that passes through the Barracuda Web Application Firewall for a specific user traffic pattern, or for a group of patterns. These logs provide information about website traffic and performance.

Access Logs are enabled by default. To disable **Access Logs**, edit the service on the **BASIC > Services** page and set **Enable Access Logs** to **Off**.

Audit Logs

Audit logs are generated whenever users log in or log out of the web interface of the Barracuda Web Application Firewall, except in a few rare cases. They are:

The **Login** action is not logged, when:

- Maintenance command is executed by a user or by the Barracuda Web Application Firewall, a new login session will be created in maintenance mode, but it won't be logged.

The **Logout** action is not logged, when:

- The Barracuda Web Application Firewall is restarted because critical processes have crashed, in which case the current existing sessions won't be logged out.
- The Maintenance command is executed by a user or by the Barracuda Web Application Firewall, in which case the current existing sessions won't be logged out.

System Logs

The **System Logs** provide a centralized collection point for all types of error reports, system alerts, diagnostic messages, and status messages of the Barracuda Web Application Firewall. Both hardware and software components of the Barracuda Web Application Firewall generate System Logs providing information about the problems and performance of a module. System Logs are required for security and troubleshooting. System logs are enabled by default, and are displayed on the **ADVANCED > System Logs** page.

Network Firewall Logs

The **Network Firewall Logs** are generated whenever network traffic passing through the interfaces (WAN, LAN and MGMT) matches configured Network ACL rule. Network Firewall log entries provide information about each packet the Barracuda Web Application Firewall allowed or denied based on the **Action** specified in the ACL rule. This data allows the administrator to identify where network traffic originated, was destined for, and the action applied.

Log Storage Capacity

Based on the available resources, each model has a predefined storage capacity for the logs.

Once the log storage is full, the oldest log is deleted and the new log is added. In high traffic environments, the logs may get rotated quickly. Setting up an external log server for long time log storage is highly recommended.

The log capacities mentioned are per log type, for firmware version 9.0 and later.

Hardware Model	Capacity per log type	Virtual Appliance Model	Capacity per log type
360	100,000	360V	100,000
460	1,000,000	460V	1,000,000
660	1,000,000	660V	1,000,000
860	2,000,000	760V	1,000,000
960	2,000,000	860V	2,000,000
		960V	2,000,000

AWS Instances	Capacity per log type	Azure Instances	Capacity per log type
Level 1	100,000	Level 1	100,000
Level 5	1,000,000	Level 5	1,000,000
Level 10	1,000,000	Level 10	1,000,000
Level 15	2,000,000	Level 15	2,000,000

Filtering Log Entries

You can use filters to quickly locate specific types of log entries. The applied filter can be saved locally on the Barracuda Web Application for later use. A filter can be created with a specific search criterion or multiple search criteria with AND/OR combination. The saved filters display when **Saved Filter** is selected from the filter list.

Whenever a log is generated in Web Firewall Logs and Access Logs, a unique ID (UID) is associated with the log. You can select the filter option **ID** and enter a unique ID to search a specific log.