How to Export Logs from the Barracuda Web Application Firewall

https://campus.barracuda.com/doc/4259935/

If the instance is deployed in the Azure Security Center, the Barracuda Web Application Firewall adds an Azure Event Hub server with the preset custom log format for “Web Firewall Logs Format”. If a Microsoft Azure Log Analytics server is added, some of the objects of the Web Firewall logs that are sent to the Log Analytics server will have incorrect values. Therefore, it is recommended not to use the Microsoft Azure Log Analytics server as an “Export Log” server when the instance is deployed in the Azure Security Center.

To add export log servers, navigate to the **ADVANCED > Export Logs** page, **Export Logs** section. You can configure a maximum of five (5) export log servers (i.e., Syslog NG, AMQP, AMQPS, and/or Azure Event Hub). All the logs (that is, system logs, web firewall logs, access logs, audit logs, and network firewall logs) are sent to the configured export log servers. See Steps To Add an Export Log Server .

If you are running syslog on a UNIX machine, be sure to start the syslog daemon process with the “-r” option so it can receive messages from external sources. Windows users require additional software to utilize syslog since the Windows OS does not include the syslog capability. Kiwi Syslog is a popular solution, but there are many others to choose from, both free and commercial.

Log messages are sent over UDP/TCP/SSL ports. If there are any firewalls between the Barracuda Web Application Firewall and the configured export log servers, ensure that the respective port is open on the firewalls.

Syslog Facility

Syslog receives different types of log messages. In order to differentiate and store them in distinct log files, log messages contain a logging priority and a logging facility in addition to the actual message and IP address.

All log messages are marked with one of the following facilities:

- local0
- local1
- |ocal2
- local3
- local4
- local5
- local6

- local7

For each configured syslog server, you can associate a specific facility (default = local0) with each log type, so your syslog server can segregate the log of each type into a different file.

Configure Facilities for Different Log Types

1. Navigate to the **ADVANCED > Export Logs** page.
2. In the **Export Logs** section, click **Export Log Settings**. The **Export Log Settings** window opens.
3. In the **Syslog Settings** section, select the appropriate facility (Local0 to Local7) from the drop-down list for each log type and click **Save**.

You can set the same facility for all log types. For example, you can set Local0 for System Logs, Web Firewall Logs, Access Logs, Audit Logs and Network Firewall Logs.

In the **Export Log Settings** window, you can do the following:

- Enable or disable the logs that needs to be exported to the configured export log server(s) in the **Export Log Settings** section.
- Set the severity level to export web firewall logs and system logs to the configured export log server(s) in the **Export Log Filters** section. The Barracuda Web Application Firewall exports the logs based on the selected severity level. For example, if Web Firewall Log Severity is set to 2-Critical, then logs with 0-2 (i.e., 0-Emergency, 1-Alert and 2-Critical) are sent to the external log server.

Configure Log Levels for Different Modules

1. Navigate to the **ADVANCED > Export Logs** page.
2. In the **Module Log Levels** section, specify values for the following fields:
   - **Name** – Enter a name for the new setting.
   - **Module** – Select a module name from the drop-down list.
   - **Log Level** – Select a log level for the module from the drop-down list. By default, the log level is set to *0-Emergency*. Note that the lower the level, the higher the priority and the more attention the log entry demands. For example, log levels 0-Emergency and 1-Alert are the highest priority situations, demanding more immediate response than 5-Notice or 6-Information.
   - **Comment** – (Optional). Enter comment about the new setting.
3. Click **Add** to add the above settings.

Module Log Level is an advanced feature, and available only when **Advanced Settings** is set to *Yes* on the **ADVANCED > System Configuration** page.