Barracuda Web Application Firewall

The IBM® Security QRadar® DSM for Barracuda Web Application Firewall collects syslog LEEF and custom events from Barracuda Web Application Firewall devices.

The following table identifies the specifications for the Barracuda Web Application Firewall DSM:

Table 1. Barracuda Web Application Firewall DSM specifications

Specification	Value
Manufacturer	Barracuda
DSM name	Web Application Firewall
RPM file name	DSM-BarracudaWebApplicationFirewall-*QRadar_version-build_number*.noarch.rpm
Supported versions	V7.0. and later
Protocol type	Syslog
QRadar recorded event types	System Web Access Audit
Automatically discovered?	If LEEF-formatted payloads, the log source is automatically discovered. If custom-formatted payloads, the log source is not automatically discovered.
Included identity?	Yes
More information	Barracuda Networks website (https://www.barracudanetworks.com)

To collect syslog events from Barracuda Web Application Firewall, use the following steps:

1. If automatic updates are not enabled, download the most recent version of the following RPMs on your QRadar Console:
   - Barracuda Web Application Firewall DSM RPM
   - DSMCommon RPM
2. Configure your Barracuda Web Application Firewall device to send syslog events to QRadar.
3. Add a Barracuda Web Application Firewall log source on the QRadar Console. The following table describes the parameters that require specific values that are required for Barracuda Web Application Firewall event collection:

Table 2. Barracuda Web Application Firewall log source parameters

Parameter	Value
Log Source type	Barracuda Web Application Firewall

Table 2. Barracuda Web Application Firewall log source parameters (continued)

Parameter	Value
Protocol Configuration	Syslog

Configuring Barracuda Web Application Firewall to send syslog events to QRadar

Configure your Barracuda Web Application Firewall appliance to send syslog events to IBM Security QRadar.

Before you begin

Verify that firewalls between the Barracuda appliance and QRadar allow UDP traffic on port 514.

Procedure

1. Log in to the Barracuda Web Application Firewall web interface.
2. Click the **Advanced** tab.
3. From the **Advanced** menu, select **Export Logs**.
4. Click **Add Syslog Server**.
5. Configure the parameters:

Option	Description
Name	The name of the QRadar Console or Event Collector
Syslog Server	The IP address of your QRadar Console or Event Collector.
Port	The port that is associated with the IP address of your QRadar Console or Event Collector. If syslog messages are sent by UDP, use the default port, 514.
Connection Type	The connection type that transmits the logs from the Barracuda Web Application Firewall to the QRadar Console or Event Collector. UDP is the default protocol for syslog communication.
Validate Server Certificate	**No**

6. In the **Log Formats** pane, select a format from the list box for each log type.
   - If you are using newer versions of Barracuda Web Application Firewall, select **LEEF 1.0 (QRadar)**.
   - If you are using older versions of Barracuda Web Application Firewall, select **Custom Format**.
7. Click **Save Changes**.