Integrate Barracuda Web Application Firewall
EventTracker v9.0 and Above

Publication Date: June 14, 2019
Abstract
This guide provides instructions to configure the Barracuda Web Application Firewall to send the syslog events to EventTracker.

Scope
The configurations detailed in this guide are consistent with EventTracker version 9.x and later, and Barracuda Web Application Firewall.

Audience
Barracuda Web Application Firewall Admins, who wish to forward syslog events to EventTracker.
# Table of Contents

Abstract ..................................................................................................................................................... 1
Scope ........................................................................................................................................................ 1
Audience .................................................................................................................................................... 1
Overview ................................................................................................................................................... 3
Prerequisites ............................................................................................................................................. 3
Configuring Barracuda Firewall syslog .................................................................................................. 3
  Adding Export Log Server ................................................................................................................... 3
  Adding Export Log Settings .................................................................................................................. 5
  Logs Format ........................................................................................................................................... 8
EventTracker Knowledge Pack (KP) ........................................................................................................ 9
  Categories .............................................................................................................................................. 9
  Alerts .................................................................................................................................................... 10
Importing Barracuda Firewall Knowledge pack into EventTracker ....................................................... 11
  Category ............................................................................................................................................... 11
  Alerts ................................................................................................................................................... 12
Verifying Barracuda Firewall knowledge pack in EventTracker ............................................................ 14
  Categories ............................................................................................................................................ 14
  Alerts ................................................................................................................................................... 15
Overview

The Barracuda Web Application Firewall blocks an ever-expanding list of sophisticated web-based intrusions and attacks that target applications hosted on web servers and in the cloud.

Barracuda Web Application Firewall can be integrated with EventTracker using syslog. With the help of Barracuda Web Application Firewall KP items, we can monitor the network firewall logs, access logs, web firewall logs, system logs and audit logs on web applications. It also triggers the alert for authentication hijacking, buffer overflow attack, command injection attack, denial of service attack, and obfuscation attack.

Prerequisites

- **EventTracker v9.x or above** should be installed.
- **Barracuda Web Application Firewall** should be installed and proper access permissions to make configuration changes.

Configuring Barracuda Firewall syslog

Adding Export Log Server

1. Go to the **ADVANCED > Export Logs** page.
2. In the **Export Logs** section, click **Add Export Log Server**. The **Add Export Log Server** window appears, specify values for the following:
- **Name**: Enter a name.
- **Log Server Type**: Select **Syslog NG**.
- **IP Address**: Enter the EventTracker IP address.
- **Port**: Enter the Syslog server (514) port.
- **Connection Type**: Select the connection type to transmit the logs from the Barracuda Web Application Firewall to the EventTracker.
- **Validate Server Certificate**: Select **No**.
- **Client Certificate**: Select **No**.
- **Log Timestamp**: Select **Yes**.

3. Click **Add**.
Adding Export Log Settings

1. Go to the ADVANCED > Export Logs page.
2. In the Export Logs section, click Export Log Settings. The Export Log Settings window appears, specify values for the following:
3 In the syslog settings section of the **Export Log Settings** dialog box, follow the below-mentioned screenshot process.

4 Click **Save**.
Integrate Barracuda Web Application Firewall

Figure 4
Integrate Barracuda Web Application Firewall

Logs Format

1. From the **Web Firewall Logs Format** list box, select Custom Format.
2. In the **Web Firewall Logs Format** field, type the following custom event format:
   
   t=%t|ad=%ad|ci=%ci|cp=%cp|au=%au

3. From the **Access Logs Format** list box, select Custom Format.
4. In the **Access Logs Format** field, type the following custom event format:
   
   t=%t|p=%p|s=%s|id=%id|ai=%ai|ap=%ap|ci=%ci|cp=%cp|si=%si|sp=%sp|cu=%cu

5. From the **Audit Logs Format** list box, select Custom Format.
6. In the **Audit Logs Format** field, type the following custom event format:
   
   t=%t|trt=%trt|an=%an|li=%li|lp=%lp

7. From the **Network Firewall Logs Format** list box, select Default.
8. From **System Logs Format** list box, select Default.
9. Click **Save Changes**.

Barracuda Web Application Firewall events are automatically discovered. Events forwarded to EventTracker by Barracuda Web Application Firewall are displayed on the Log Search tab of EventTracker.
EventTracker Knowledge Pack (KP)

Once logs are received into EventTracker, Alerts and, categories can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker v9.x to support Barracuda Web Application Firewall monitoring:

Categories

- **Barracuda: Application platform exploits** - This category based report provides information related to application platform exploit.

- **Barracuda: Authentication hijacking** - This category based report provides information related to authentication hijacking.

- **Barracuda: Buffer overflow attack** - This category based report provides information related to buffer overflow attack.

- **Barracuda: Command injection attack** - This category based report provides information related to the command injection attack.

- **Barracuda: Cookie poisoning attack** - This category based report provides information related to a cookie poisoning attack.

- **Barracuda: Cross-site scripting attack** - This category based report provides information related to cross-site scripting attack.

- **Barracuda: Denial-of-service attack** - This category based report provides information related to the denial-of-service attack.

- **Barracuda: Directory traversal attack** - This category based report provides information related to directory traversal attack.

- **Barracuda: Error message interception** - This category based report provides information related to error message interception.

- **Barracuda: Firewall received messages** - This category based report provides information related to firewall received messages.

- **Barracuda: Firewall scan messages** - This category based report provides information related to firewall scan messages.
• **Barracuda: Firewall sending messages** - This category based report provides information related to firewall sending messages.

• **Barracuda: Forceful browsing attack** - This category based report provides information related to forceful browsing attack.

• **Barracuda: Form tampering attack** - This category based report provides information related to form tampering attack.

• **Barracuda: Malicious file execution attack** - This category based report provides information related to the malicious file execution attack.

• **Barracuda: Obfuscation attack** - This category based report provides information related to obfuscation attack.

• **Barracuda: Protocol exploit attack** - This category based report provides information related to protocol exploit attack.

• **Barracuda: SQL injection attack** - This category based report provides information related to the SQL injection attack.

• **Barracuda: Traffic allowed** - This category based report provides information related to traffic allowed.

• **Barracuda: Traffic denied** - This category based report provides information related to traffic denied.

**Alerts**

• **Barracuda: Authentication hijacking** - This alert is generated when authentication hijacking occurs.

• **Barracuda: Buffer overflow attack** - This alert is generated when a buffer overflow attack occurs.

• **Barracuda: Command injection attack** - This alert is generated when command injection attack occurs.

• **Barracuda: Cookie poisoning attack** - This alert is generated when a cookie poisoning attack occurs.

• **Barracuda: Cross-site scripting attack** - This alert is generated when cross-site scripting attack occurs.

• **Barracuda: Denial-of-service attack** - This alert is generated when a denial-of-service attack occurs.

• **Barracuda: Error message interception** - This alert is generated when error message interception occurs.
• **Barracuda: Malicious file execution attack** - This alert is generated when a malicious file execution attack occurs.

• **Barracuda: Obfuscation attack** - This alert is generated when the obfuscation attack occurs.

**Importing Barracuda Firewall Knowledge pack into EventTracker**

1. Launch the **EventTracker Control Panel**.

2. Double click **Export/Import Utility**, and then click the **Import** tab.

3. Import **Category and Alerts** as given below.

**Category**

1. Click **Category** option, and then click the browse button
2. Locate All Barracuda firewall group of Categories.iscat file, and then click the Open button.

3. Click the Import button to import the categories.

4. EventTracker displays a success message.

5. Click OK, and then click the Close button.

Alerts

1. Click the Alert option, and then click the browse button.
2. Locate All Barracuda firewall group of Alerts.isalt file, and then click the **Open** button.

3. Click the **Import** button to import the alerts.
   - EventTracker displays a success message.

4. Click **OK**, and then click the **Close** button.
Verifying Barracuda Firewall knowledge pack in EventTracker

Categories

1. Login to EventTracker.
2. Click the Admin menu, and then click Category.
3. Click the search, and then search with Barracuda.
Alerts

1. Login to EventTracker.
2. Click the Admin menu, and then click Alerts.

3. In the Search box, type ‘Barracuda’, and then click the search. Alert Management page will display all the imported alerts.

4. To activate the imported alerts, select the respective checkbox in the Active column. EventTracker displays a message box.
5. Click **OK**, and then click the **Activate Now** button.

**NOTE:** Specify appropriate **systems** in the **alert configuration** for better performance.