Integrate Barracuda Web Security Gateway
EventTracker v8.x and above

Publication Date: February 28, 2017
Abstract

This guide helps you in configuring **Barracuda Web Security Gateway** with EventTracker to receive **Barracuda Web Security Gateway** events. In this document, you will find the detailed procedures required for monitoring **Barracuda Web Security Gateway**.

Audience

Administrators who are assigned the task to monitor and manage Barracuda Web Security Gateway events using EventTracker.
# Table of Contents

Abstract ................................................................................................................................. 1
Audience ................................................................................................................................. 1
Overview ................................................................................................................................. 3
Prerequisites .......................................................................................................................... 3
Integration of Barracuda Web Security Gateway events to EventTracker server ................ 3
   EventTracker Knowledge Pack ......................................................................................... 3
      Alerts ............................................................................................................................... 3
      Flex Reports .................................................................................................................. 4
Import Barracuda Web Security Gateway knowledge pack into EventTracker ................... 10
   Knowledge Objects .......................................................................................................... 11
   Templates .......................................................................................................................... 12
   Flex Reports ....................................................................................................................... 14
   Alerts ................................................................................................................................. 15
Verify Barracuda Web Security Gateway knowledge pack in EventTracker ....................... 17
   Knowledge Objects .......................................................................................................... 17
   Alerts ................................................................................................................................. 17
   Flex Reports ....................................................................................................................... 19
   Template ............................................................................................................................ 19
Create Flex Dashboards in EventTracker ............................................................................ 20
Schedule Reports .................................................................................................................. 20
Create Dashlets ..................................................................................................................... 23
Sample Flex Dashboards ...................................................................................................... 27
Overview

The Barracuda Web Security Gateway lets organizations benefit from online applications and tools without exposure to web-borne malware and viruses, lost user productivity, and misused bandwidth. The Barracuda Web Security Gateway uses a continually updated database to identify and block access to sites known to host spyware and viruses. It also detects installed spyware trying to access the Internet. Upon discovery, it blocks the spyware activity and notifies the administrator. By using dual-layer virus blocking, decompressing archives, and blocking file types, the antivirus engine in the Barracuda Web Security Gateway protects networks from aggressive viruses.

Prerequisites

- EventTracker v8.x should be installed.
- Barracuda Web Security Gateway version 610,710,810,910,1010.
- Barracuda Web Security Gateway firmware version 11.0.0.019.
- Windows Version 7 or later should be installed.
- An exception should be added into windows firewall on EventTracker machine for syslog port 514.

Integration of Barracuda Web Security Gateway events to EventTracker server

To enable syslog reporting on your Barracuda Web Security Gateway:

- Log into the web interface as admin and navigate to the Advanced > Syslog page.
- For both the Web Traffic Syslog and Web Interface Syslog, enter the IP address (192.168.1.1) of the EventTracker manager to which you want to direct messages.

EventTracker Knowledge Pack

Once logs are received into EventTracker; Alerts, Reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Windows.

Alerts

1. Barracuda-Content filtering: This alert is generated when any of the website contents that are being accessed by users are blacklisted or denied from accessing.
2. **Barracuda-Configuration changes**: This alert is generated when any configuration changes are done in the Barracuda web server gateway by different users or admins such as new user creation, group creation, backup scheduled, firmware updates etc.

3. **Barracuda-Malware detection**: This alert is generated when the web traffic content is infected by a malware or virus.

4. **Barracuda-Login and Logoff activity**: This alert is generated when login and logoff activity is done in the application.

5. **Barracuda-Login Failure**: This alert is generated when failed logon attempts are done in the application.

**Flex Reports**

1. **Barracuda-Clean policy allowed traffic**: This report provides all the allowed traffic content that pass through the barracuda web security gateway.

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Destination Url</th>
<th>Data size</th>
<th>Format</th>
<th>Version</th>
<th>TQ Flag</th>
<th>User Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/24/2017 04:23:48PM</td>
<td>192.168.137.1</td>
<td>215.58.220.35</td>
<td><a href="http://www.google.co.in/?gfe_rd=cr&amp;ei=PHyqiwLXwNurl8Aeiz2XoCg">http://www.google.co.in/?gfe_rd=cr&amp;ei=PHyqiwLXwNurl8Aeiz2XoCg</a> &amp;lfs=1064</td>
<td>2</td>
<td>0</td>
<td>MIKE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>02/24/2017 04:23:48PM</td>
<td>192.168.137.1</td>
<td>104.24.127.96</td>
<td><a href="http://analytics.planwallpaper.com/piwik.php?action_name=High0De1finition1and1high0xresolution04allpapergeneratesite78rec=18&amp;4001261h=118m=28s=358url=httpA">http://analytics.planwallpaper.com/piwik.php?action_name=High0De1finition1and1high0xresolution04allpapergeneratesite78rec=18&amp;4001261h=118m=28s=358url=httpA</a></td>
<td>2</td>
<td>0</td>
<td>Doe,John, CN=Users, DC=qq, DC=local</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Logs Considered:**

![Figure 1](#)

![Figure 2](#)
2. **Barracuda-Clean policy denied traffic**: This report provides all the denied traffic content that pass through the Barracuda web security gateway. The denial is based on the policies and rules written by the admins.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Destination URL</th>
<th>Content Type</th>
<th>Data size</th>
<th>Match flag</th>
<th>TQ flag</th>
<th>User Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/20/2017 11:02:31 AM</td>
<td>192.168.137.1</td>
<td>104.24126.96</td>
<td><a href="http://www.planwallpaper.com/static/assets/css/font-awesome.min.css">http://www.planwallpaper.com/static/assets/css/font-awesome.min.css</a></td>
<td>text/css</td>
<td>6043</td>
<td>2</td>
<td>0</td>
<td>[ZOE]</td>
</tr>
<tr>
<td>02/20/2017 11:02:32 AM</td>
<td>192.168.137.1</td>
<td>173.223.235.0</td>
<td><a href="http://www.msfncsi.com/rcsi.txt">http://www.msfncsi.com/rcsi.txt</a></td>
<td>text/plain 2</td>
<td>277</td>
<td>2</td>
<td>0</td>
<td>[cn=Administrator,cn=User,dc=Contoso,dc=Com]</td>
</tr>
<tr>
<td>02/20/2017 11:02:33 AM</td>
<td>192.168.137.1</td>
<td>96.43.137.99</td>
<td><a href="http://rules.emergingthreats.net/fwrules/%E6%96%B0%E5%85%B4-Block-IPs.txt">http://rules.emergingthreats.net/fwrules/新兴-Block-IPs.txt</a></td>
<td>text/plain</td>
<td>28206</td>
<td>2</td>
<td>0</td>
<td>[ANON]</td>
</tr>
</tbody>
</table>

**Figure 3**

**Logs Considered:**

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Event ID</th>
<th>Site / Computer</th>
<th>User</th>
<th>Domain</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/27/2017 10:06:17 AM</td>
<td>5555</td>
<td>PNPL-6-K/PNPL-6-K</td>
<td>N/A</td>
<td>N/A</td>
<td>Systag</td>
</tr>
<tr>
<td>Event Type: Information</td>
<td>Log Type: Application</td>
<td>Category ID: 0</td>
<td>Description:  Feb 20 10:06:21 PNPL-6-K <a href="http://rules.emergingthreats.net/fwrules/%E6%96%B0%E5%85%B4-Block-IPs.txt">http://rules.emergingthreats.net/fwrules/新兴-Block-IPs.txt</a> 277 BY BLOCKED CLEAN 20000 0 0 0 <a href="http://www.msfncsi.com/rcsi.txt">http://www.msfncsi.com/rcsi.txt</a> 277 BY BLOCKED CLEAN 20000 0 0 0 <a href="http://www.msfncsi.com">www.msfncsi.com</a> cact lookup failed [cn=Administrator,cn=User,dc=Contoso,dc=Com] - LDAP USER</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 4**

3. **Barracuda-Content filtering**: This report provides the details of the website contents that are being accessed by users which are blacklisted by the admins.
4. **Barracuda-Configuration changes:** This report provides all the configuration changes that are done in the Barracuda web server gateway by different users and admins such as new user creation, group creation, backup scheduled, firmware updates etc.
Logs Considered:

<table>
<thead>
<tr>
<th>LOG TIME</th>
<th>EVENT ID</th>
<th>SITE / COMPUTER</th>
<th>USER</th>
<th>DOMAIN</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2/27/2017 1:54:46 PM</td>
<td>5555</td>
<td>PNPL-G-KP / PNPL-S-K..</td>
<td>N/A</td>
<td>N/A</td>
<td>Syslog</td>
</tr>
<tr>
<td>Description: Feb 22 16:22:50 PNPL-G-KP web: [192.168.137.74] global] CHANGE backup_schedule: WF_Config_minute (00) [mike]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2/27/2017 1:54:46 PM</td>
<td>5555</td>
<td>PNPL-G-KP / PNPL-S-K..</td>
<td>N/A</td>
<td>N/A</td>
<td>Syslog</td>
</tr>
<tr>
<td>2/27/2017 1:54:46 PM</td>
<td>5555</td>
<td>PNPL-G-KP / PNPL-S-K..</td>
<td>N/A</td>
<td>N/A</td>
<td>Syslog</td>
</tr>
</tbody>
</table>

5. **Barracuda-Malware detection**: This report provides all the Malware Infected traffic details.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Destination Url</th>
<th>Data size</th>
<th>Virus stream details</th>
<th>Match flag</th>
<th>User Info</th>
<th>Referer Url</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/21/2017 12:44:22 PM</td>
<td>192.168.137.1</td>
<td>188.225.32.177</td>
<td>fo5.a1-downloader.org/g 2v9s1.php?id=y0 username=youdomain.com.zip</td>
<td>538</td>
<td>Trojan</td>
<td>2</td>
<td>ANON</td>
<td><a href="http://fo5.a1-downloader.org/g-Download.zip">http://fo5.a1-downloader.org/g-Download.zip</a> fo5.a1-...</td>
</tr>
</tbody>
</table>
6. **Barracuda-Inline Traffic details**: This report provides all internet traffic requests. It performs content filtering and scan downloads for spyware and viruses and also filter web based and non-web based applications. This is determined by the traffic that traverses via the automatic configured proxy (PAC).
Logs Considered:

![Table](image1.png)

**Figure 12**

7. **Barracuda-Login and Logoff activity**: This report provides all the login and logoff activities that are done in the Barracuda application.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Source IP</th>
<th>Action</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/23/2017 06:12:12 AM</td>
<td>192.168.137.74</td>
<td>LOGIN</td>
<td>zoe</td>
</tr>
<tr>
<td>02/23/2017 07:42:00 AM</td>
<td>192.168.137.1</td>
<td>LOGOFF</td>
<td>zoe</td>
</tr>
<tr>
<td>02/23/2017 08:35:19 AM</td>
<td>192.168.137.1</td>
<td>LOGIN</td>
<td>jack</td>
</tr>
<tr>
<td>02/23/2017 12:26:04 PM</td>
<td>192.168.137.1</td>
<td>LOGOFF</td>
<td>jack</td>
</tr>
<tr>
<td>02/23/2017 04:58:12 PM</td>
<td>192.168.137.74</td>
<td>LOGIN</td>
<td>glenn</td>
</tr>
<tr>
<td>02/23/2017 07:14:53 PM</td>
<td>192.168.137.74</td>
<td>LOGOFF</td>
<td>glenn</td>
</tr>
</tbody>
</table>

![Table](image2.png)

**Figure 13**

Logs Considered:

![Table](image3.png)

**Figure 14**
8. **Barracuda-Login Failure**: This report provides all the failed logon attempts that are done in the Barracuda application.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Source IP</th>
<th>User</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/17/2017 11:16:39 AM</td>
<td>192.168.137.1</td>
<td>admin</td>
</tr>
<tr>
<td>02/20/2017 10:49:41 AM</td>
<td>192.168.137.74</td>
<td>aaron</td>
</tr>
<tr>
<td>02/21/2017 12:12:34 PM</td>
<td>192.168.137.1</td>
<td>admin</td>
</tr>
<tr>
<td>02/22/2017 11:16:02 AM</td>
<td>192.168.137.74</td>
<td>admin</td>
</tr>
<tr>
<td>02/21/2017 12:54:45 PM</td>
<td>192.168.137.1</td>
<td>neeson</td>
</tr>
</tbody>
</table>

*Figure 15*

**Logs Considered:**

*Figure 16*

**Import Barracuda Web Security Gateway knowledge pack into EventTracker**

**NOTE**: Import knowledge pack items in the following sequence:

- Knowledge Objects
- Token templates
- Flex Reports
- Alerts
Knowledge Objects

1. Click Knowledge objects under Admin option in the EventTracker manager page.
2. Locate the All Barracuda Web Security Gateway group of Knowledge object.etko, and then click Import button.

3. Choose the Knowledge objects that needs to be imported and click upload.
4. Knowledge objects are now imported successfully.

![Figure 18: Knowledge objects import window](image1)

![Figure 19: Import success notification](image2)

**Templates**

1. Click the **Admin** menu, and then click **Parsing rule**.

![EventTracker logo](image3)
2. Select **Template** tab, and then click on 'Import' option.
3. Click on **Browse** button.

![Figure 20](image)

4. Locate **All Barracuda Web Security Gateway** group of template.ettd file, and then click the **Open** button.

![Figure 21](image)

5. Now select the check box and then click on 'Import' option. EventTracker displays success message.
6. Click on **OK** button.

**Flex Reports**

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.
3. Click the **Import** tab.
4. Click Reports option, and then click the browse button.
5. Locate the **All Barracuda Web Security gateway** group of flex reports.issch file, and then click the **Open** button.
6. Click the **Import** button to import the **scheduled** reports. EventTracker displays success message.

![Export Import Utility](image)

**Figure 24**

**Alerts**

1. Click **Alerts** option, and then click the browse button.
2. Locate the **All Barracuda Web Security Gateway.isalt** file, and then click the **Open** button.
2. To import alerts, click the **Import** button.

EventTracker displays success message.

3. Click **OK**, and then click the **Close** button.
Verify Barracuda Web Security Gateway knowledge pack in EventTracker

Knowledge Objects

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Knowledge Objects.
2. In the Knowledge Object tree, expand Barracuda Web Security Gateway group folder to see the imported Knowledge objects.

![Knowledge Objects](image)

Alerts

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Alerts.
2. In the Search field, type Barracuda Web Security Gateway, and then click Go button.
   Alert Management page will display the imported Barracuda Web Security Gateway alert.
3. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

4. Click the **OK** button, and then click the **Activate now** button.

**NOTE:**

You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.
Flex Reports

1. In the EventTracker Enterprise web interface, click the Reports menu, and then select Configuration.
2. In Reports Configuration pane, select Defined option.
3. In search box enter ‘Barracuda Web Security Gateway, and then click the Search button.
   EventTracker displays Flex reports of ‘Barracuda Web Security Gateway

![Reports Configuration]

Figure 31

Template

1. Logon to EventTracker Enterprise web interface.
2. Click the Admin menu, and then click Parsing Rules and click Template.
Create Flex Dashboards in EventTracker

**NOTE:** To configure the flex dashboards, schedule and generate the reports. Flex dashboard feature is available from EventTracker Enterprise v8.0.

**Schedule Reports**

1. Open **EventTracker** in browser and logon.

2. Navigate to **Reports>Configuration**.
3. Select **Barracuda Web Security Gateway** in report groups. Check **Defined** dialog box.

![Reports Configuration](image)

**Figure 34**

4. Click on ‘**schedule**’ to plan a report for later execution.
5. Click **Next** button to proceed.
6. In review page, check **Persist data in EventVault Explorer** option.
7. In next page, check column names to persist using PERSIST checkboxes beside them. Choose suitable Retention period.
8. Proceed to next step and click Schedule button.
9. Wait till the reports get generated.

Create Dashlets

1. Open EventTracker Enterprise in browser and logon.
2. Navigate to **Dashboard>Flex**.
   Flex Dashboard pane is shown.

3. Fill suitable title and description and click **Save** button.
4. Click 🗒️ to configure a new flex dashlet. Widget configuration pane is shown.
5. Locate earlier scheduled report in **Data Source** dropdown.
6. Select **Chart Type** from dropdown.
7. Select extent of data to be displayed in **Duration** dropdown.
8. Select computation type in **Value Field Setting** dropdown.
9. Select evaluation duration in **As Of** dropdown.
10. Select comparable values in **X Axis** with suitable label.
11. Select numeric values in **Y Axis** with suitable label.
12. Select comparable sequence in **Legend**.
13. Click **Test** button to evaluate. Evaluated chart is shown.
14. If satisfied, click **Configure** button.
15. Click ‘customize’ to locate and choose created dashlet.
16. Click to add dashlet to earlier created dashboard.

Sample Flex Dashboards

For below dashboard DATA SOURCE: Barracuda Web Security Gateway

- WIDGET TITLE: Barracuda-Clean policy allowed traffic
- CHART TYPE: Stacked Column
- AXIS LABELS [X-AXIS]: Destination IP
- LEGEND [SERIES]: User Info

Figure 42
For below dashboard **DATA SOURCE**: Barracuda Web Security Gateway

- **WIDGET TITLE**: Barracuda-Clean policy denied traffic  
  **CHART TYPE**: Stacked Column  
  **AXIS LABELS [X-AXIS]**: Destination IP  
  **LEGEND[SERIES]**: Destination Url

![Figure 43](image-url)
For below dashboard **DATA SOURCE: Barracuda Web Security Gateway**

- **WIDGET TITLE:** Barracuda-Configuration changes
- **CHART TYPE:** Donut
- **AXIS LABELS [X-AXIS]:** Object changed

![Barracuda-Configuration Changes Chart](image)
Integrate Barracuda Web Security Gateway

For below dashboard DATA SOURCE: Barracuda Web Security Gateway

- **WIDGET TITLE:** Barracuda-Content Filtering  
  **CHART TYPE:** Line  
  **AXIS LABELS [X-AXIS]:** Destination IP  
  **LEGEND [SERIES]:** Action Value

![Barracuda-Content Filtering](image)

**Figure 45**
For below dashboard **DATA SOURCE**: Barracuda Web Security Gateway

- **WIDGET TITLE**: Barracuda-Inline traffic content
- **CHART TYPE**: Stacked Column
- **AXIS LABELS [X-AXIS]**: Destination IP
- **LEGEND [SERIES]**: Reason

![Barracuda Inline Traffic Content Chart](image-url)

**Figure 46**
For below dashboard **DATA SOURCE: Barracuda Web Security Gateway**

- **WIDGET TITLE:** Barracuda-Logon and Logoff Activity
- **CHART TYPE:** Stacked Column
- **AXIS LABELS [X-AXIS]:** Action
- **LEGEND[SERIES]:** Source IP

![Barracuda Logon and Logoff Activity Chart](image)

Figure 47
For below dashboard **DATA SOURCE: Barracuda Web Security Gateway**

- **WIDGET TITLE:** Barracuda-Login Failed
- **CHART TYPE:** Stacked Column
- **AXIS LABELS [X-AXIS]:** Source IP
- **LEGEND[SERIES]:** User

![Barracuda-Login Failed Chart]

*Figure 48*