Integrate Barracuda NextGen Firewall F-Series

EventTracker v8.x and above
Abstract

This guide provides instructions to configure Barracuda NG Firewall F-Series to send the syslog to EventTracker Enterprise. Once syslog is being configured to send to EventTracker Manager, alerts and reports can be configured into EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 8.x and later, Barracuda NG Firewall F-Series (F18, F80, F180, F280, F380, F400, F600, F800, F900, f1000).

Audience

Administrators who are responsible for monitoring Barracuda NG Firewall F-Series which are running using EventTracker Manager.
# Table of Contents

Abstract ........................................................................................................................................................................ 1  
Scope ........................................................................................................................................................................ 1  
Audience .................................................................................................................................................................. 1  
Prerequisites ............................................................................................................................................................ 3  
Configure Barracuda NextGen Firewall to send syslog to EventTracker ................................................................. 3  
Log into the Barracuda NextGen Firewall F-Series ................................................................................................ 3  
Enable the Syslog Service ........................................................................................................................................ 4  
EventTracker Knowledge Pack .................................................................................................................................... 6  
Alerts ........................................................................................................................................................................ 6  
Flex Reports ............................................................................................................................................................. 7  
Import Barracuda NG Firewall knowledge pack into EventTracker ......................................................................... 9  
Alerts ...................................................................................................................................................................... 10  
Token Templates ................................................................................................................................................... 11  
Flex Reports ........................................................................................................................................................... 12  
Verify Barracuda NG Firewall knowledge pack in EventTracker ............................................................................ 14  
Alerts ...................................................................................................................................................................... 14  
Token Template ................................................................................................................................................... 15  
Flex Reports ........................................................................................................................................................... 15  
Create Flex Dashboards in EventTracker ................................................................................................................. 16  
Schedule Reports ................................................................................................................................................... 16  
Create Dashlets .................................................................................................................................................... 19  
Sample Flex Dashboards ....................................................................................................................................... 22
Barracuda NG Firewall F-Series

The **Barracuda NextGen Firewall F-Series** is a family of hardware, virtual, and cloud-based appliances that protect and enhance your dispersed network infrastructure. They deliver advanced security by tightly integrating a comprehensive set of next-generation firewall technologies, including Layer 7 application profiling, intrusion prevention, web filtering, malware and advanced threat protection, antispam protection, and network access control.

In addition, the F-Series combines highly resilient VPN technology with intelligent traffic management and WAN optimization capabilities. This lets you reduce line costs, increase overall network availability, improve site-to-site connectivity, and ensure uninterrupted access to applications hosted in the cloud. Scalable centralized management helps you reduce administrative overhead while defining and enforcing granular policies across your entire dispersed network.

**Prerequisites**

- EventTracker v8.x should be installed.
- **Barracuda NG Firewall F-Series** (F18, F80, F180, F280, F380, F400, F600, F800, F900, f1000) should be installed and configured.
- An exception should be added into windows firewall on EventTracker machine for syslog port 514.

**Configure Barracuda NextGen Firewall to send syslog to EventTracker**

**Log into the Barracuda NextGen Firewall F-Series**

1. Launch NextGen Admin.
2. In the Log in window, select Firewall.
3. Enter the Management IP, Username, and Password.
4. Click **Sign In**. The Authentication Check window opens.

5. Click **Trust**.

6. The box wizard can only be used on hardware units. If you are deploying a virtual F-Series Firewall, you must configure the time zone and change the password manually.

Enable the Syslog Service

Enable the Barracuda NG Firewall to stream log files to external syslog devices like the Barracuda NG Control Center or a 3rd party syslog server. When using SSL for log file streaming, export the certificate and key for SSL based authentication.

1. Open the Syslog Streaming page (**Config** > **Full Config** > **Box** > **Infrastructure Services**).
2. Click Lock/Unlock.
3. Enable the Syslog service.
4. Enter your destination IP address and Port to where the syslog needs to be sent. This is highlighted in the above image.
5. Click **Send Changes** and then **Activate**.

**EventTracker Knowledge Pack**

Once logs are received into EventTracker, Categories, reports can be configured into EventTracker.

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

**Alerts**

- **Barracuda NG Firewall-Login failures**: This alert is generated when a login failure by a user is done on Barracuda Firewall console.
- **Barracuda NG Firewall-Attacks detection**: This alert is generated when any Security events has been triggered by a user.
- **Barracuda NG Firewall-IDS alerts**: This alert is generated when any IDS/IPS is detected.
- **Barracuda NG Firewall-Virus detection**: This alert is generated when any virus or malware is detected by the Barracuda NG firewall.
Flex Reports

- **Barracuda NG Firewall-Allowed traffic**- This report provides details about all the traffic that is allowed to pass by the NG Firewall.

- **Barracuda NG Firewall-Denied traffic**- This report provides details about all the traffic that is denied to pass by the NG Firewall.

- **Barracuda NG Firewall-Login success**- This report provides details on all successful logon that is done in the NG Firewall console.
- **Barracuda NG Firewall-Login failures**: This report provides details about all the login failures that is done in the NG Firewall console.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Device IP Address</th>
<th>UserName</th>
<th>Client IP address</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/29/2017 03:46:59 PM</td>
<td>PNPL-6-KP</td>
<td>192.168.105.1</td>
<td>katie</td>
<td>192.168.10.94</td>
<td>No Access from this ip address (192.168.1.125).</td>
</tr>
<tr>
<td>06/29/2017 03:47:21 PM</td>
<td>PNPL-6-KP</td>
<td>192.168.105.1</td>
<td>katie</td>
<td>192.168.10.94</td>
<td>No Access from this ip address (192.168.1.125).</td>
</tr>
</tbody>
</table>

- **Barracuda NG Firewall-IDS alerts**: This report provides details about all the IDS/IPS attacks that is attempted to compromise the NG Firewall.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Source IP Address</th>
<th>Threat List</th>
<th>Threat File</th>
<th>Origin</th>
<th>Risk</th>
<th>Hash</th>
<th>Threat Hits</th>
<th>Blocked</th>
<th>Start Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/29/2017 03:18:53 PM</td>
<td>PNPL-6-KP</td>
<td>192.168.105.1</td>
<td><a href="http://sei.leitfach.de/zoo/v0.50.74-g04ocod6iytnfz-thezoo-">http://sei.leitfach.de/zoo/v0.50.74-g04ocod6iytnfz-thezoo-</a> e4godf/namesbarman ese/equationgroup.pdf</td>
<td>httpsps</td>
<td>High</td>
<td>db1dfb7weg571a6e 3g3d3933</td>
<td>1</td>
<td>06/29/2017 17:22:40.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/29/2017 03:18:53 PM</td>
<td>PNPL-6-KP</td>
<td>192.168.105.1</td>
<td><a href="http://sei.leitfach.de/zoo/v0.50.74-g04ocod6iytnfz-thezoo-">http://sei.leitfach.de/zoo/v0.50.74-g04ocod6iytnfz-thezoo-</a> e4godf/namesbarman ese/equationgroup.pdf</td>
<td>httpsps</td>
<td>High</td>
<td>3bb277ygw23sec2oo 8avke</td>
<td>2</td>
<td>06/29/2017 15:02:00.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>06/28/2017 03:18:53 PM</td>
<td>PNPL-6-KP</td>
<td>192.168.105.1</td>
<td><a href="http://t010.17.33.114/vena/uno.zip">http://t010.17.33.114/vena/uno.zip</a></td>
<td>uno.zip</td>
<td>httpsps</td>
<td>Medium</td>
<td>16wh18e18d129i102 7g5v2x32</td>
<td>1</td>
<td>06/28/2017 13:01:80.</td>
<td></td>
</tr>
</tbody>
</table>

- **Barracuda NG Firewall-Attack detection**: This report provides details about on all the security events that is triggered by the user.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Source IP Address</th>
<th>Attack Detected</th>
<th>Count</th>
<th>Attack Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/26/2017 11:45:32 AM</td>
<td>BARRACUDA-NG</td>
<td>192.168.1.111</td>
<td>Address-Port Scan</td>
<td>13</td>
<td>13 unwanted requests for source IP 192.168.1.111 within 60 seconds</td>
</tr>
<tr>
<td>06/26/2017 11:45:32 AM</td>
<td>BARRACUDA-NG</td>
<td>192.168.1.65</td>
<td>Address-Port Scan</td>
<td>15</td>
<td>15 unwanted requests for source IP 192.168.1.65 within 60 seconds</td>
</tr>
</tbody>
</table>
**Barracuda NG Firewall-Virus detection** - This report provides details on all the Virus/malware that is detected by the Barracuda Anti-Virus scan.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Activity Type</th>
<th>User Name</th>
<th>Source IP Address</th>
<th>Destination IP Address</th>
<th>Protocol</th>
<th>Scan Type</th>
<th>Application Context</th>
<th>Action Info</th>
<th>Risk/Severity</th>
<th>Attack Count</th>
<th>Last Observed</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/29/2017 04:22:28 PM PNPL-6-KP LOUT</td>
<td>10.17.133.103</td>
<td>Leon</td>
<td>172.12.111.77</td>
<td>TCP</td>
<td>Virus Scan</td>
<td>Trojan - Host Scan</td>
<td>Critical</td>
<td>3</td>
<td>2</td>
<td>172.12.111.77</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Barracuda NG Firewall-Wifi authentication** - This report provides details about all Wifi authentication that are done by use.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Device IP Address</th>
<th>User Name</th>
<th>Client IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>06/29/2017 04:22:28 PM PNPL-6-KP LOUT</td>
<td>10.17.133.103</td>
<td>Leon</td>
<td>172.12.111.77</td>
<td></td>
</tr>
<tr>
<td>06/29/2017 04:22:29 PM PNPL-6-KP LOUT</td>
<td>10.17.133.103</td>
<td>Sophie</td>
<td>172.19.1.23</td>
<td></td>
</tr>
</tbody>
</table>

**Import Barracuda NG Firewall knowledge pack into EventTracker**

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

- Alerts
- Token templates
- Flex Reports

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

- Alerts
- Token templates
- Flex Reports
1. Launch EventTracker Control Panel.

2. Double click Export Import Utility.

3. Click the Import tab.

Alerts

1. Click Alerts option, and then click the browse button.

2. Locate the Barracuda NG Firewall alerts.isalt file, and then click the Open button.
3. To import alerts, click the **Import** button. EventTracker displays success message.

![Figure 8](image)

4. Click **OK**, and then click the **Close** button.

**Token Templates**

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab, and then click on ‘**Import**’ option.
3. Click on **Browse** button.

![Figure 9](image)

4. Locate **Barracuda NG Firewall.ettd** file, and then click the **Open** button.
5. Now select the check box and then click on ‘Import’ option. EventTracker displays success message.

   Template(s) imported successfully

   ![Figure 10](image)

6. Click on OK button.

**Flex Reports**

1. Click **Reports** option, and then click the browser '...' button.
2. Locate the **Barracuda NG Firewall.etcrx** file, and then click the **Open** button.
3. Click the **Import** button to import the **scheduled** reports. EventTracker displays success message.
Verify Barracuda NG Firewall knowledge pack in EventTracker

1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Alerts.
2. In the Search field, type Barracuda NG Firewall, and then click Go button.
   Alert Management page will display the imported Barracuda NG Firewall 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.

## Token Template

1. Logon to **EventTracker Enterprise** web interface.
2. Click the **Admin** menu, and then click **Parsing Rules** and click **Template**.
3. Click on **Barracuda NG Firewall** group option.

![Parsing Rule](image)

**Figure 16**

## 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 NG Firewall', and then click the **Search** button. EventTracker displays Flex reports of 'Barracuda NG Firewall'
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.

![EventTracker dashboard](image-url)
2. Navigate to **Reports>Configuration**.
3. Select **Barracuda NG Firewall** in report groups. Check **Defined** dialog box.

![Figure 19](image)

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

- REPORT: Barracuda NG Firewall-Allowed traffic
  WIDGET TITLE: Barracuda NG Firewall-Allowed traffic
  CHART TYPE: Stacked Column
  AXIS LABELS [X-AXIS]: Source IP Address
  LEGEND[SERIES]: Activity Type

![Sample Flex Dashboard Chart](image)
• REPORT: Barracuda NG Firewall-Denied traffic
  WIDGET TITLE: Barracuda NG Firewall-Denied traffic
  CHART TYPE: PIE
  AXIS LABELS [X-AXIS]: Source IP Address
  LEGEND[SERIES]: Rule Description
- **REPORT**: Barracuda NG Firewall-Login success
  - **WIDGET TITLE**: Barracuda NG Firewall-Login success
  - **CHART TYPE**: Donut
  - **AXIS LABELS [X-AXIS]**: User Name
  - **LEGEND[SERIES]**: Action

06/29 16:58 - 06/30 16:58
• REPORT: Barracuda NG Firewall-Login failures
  WIDGET TITLE: Barracuda NG Firewall-Login failures
  CHART TYPE: Pie
  AXIS LABELS [X-AXIS]: User Name
  LEGEND[SERIES]: Reason

  ![](image1)

• REPORT: Barracuda NG Firewall-IDS alerts
  WIDGET TITLE: Barracuda NG Firewall-IDS alerts
  CHART TYPE: Pie
  AXIS LABELS [X-AXIS]: Threat File
  LEGEND: Risk

  ![](image2)
• REPORT: Barracuda NG Firewall-Wifi authentication  
  WIDGET TITLE: Barracuda NG Firewall-Wifi authentication  
  CHART TYPE: Stacked Column  
  AXIS LABELS [X-AXIS]: User Name  
  LEGEND[SERIES]: Client IP Address