Integrate PoliWall Security Appliance

EventTracker Enterprise
Abstract

This guide provides instructions to configure PoliWall Security Appliance to send the syslog events to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 7.x and later, and PoliWall Security Appliance version 1.21.00.

Audience

Administrators, who are responsible for monitoring PoliWall Security Appliance using EventTracker Enterprise.

The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Prism Microsystems, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2016 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
Table of Contents

Abstract ........................................................................................................................................................................1
Scope ........................................................................................................................................................................1
Audience ...................................................................................................................................................................1
Introduction ..............................................................................................................................................................3
Pre-requisites ............................................................................................................................................................3
Syslog Configuration for PoliWall ...............................................................................................................................3
EventTracker Knowledge Pack (KP) ............................................................................................................................5
Alerts ........................................................................................................................................................................5
Reports .....................................................................................................................................................................5
Behavior Rules .......................................................................................................................................................10
Knowledge Objects ................................................................................................................................................11
Import PoliWall Knowledge Pack into EventTracker ...............................................................................................13
EventTracker Manager ..........................................................................................................................................15
  Knowledge Objects ............................................................................................................................................15
  Token Templates ................................................................................................................................................17
EventTracker Control Panel ..................................................................................................................................18
  Reports ...............................................................................................................................................................20
  Alerts ...............................................................................................................................................................21
  Parsing Rules ...................................................................................................................................................22
  Behavior Rules ...................................................................................................................................................23
Verify PoliWall knowledge pack in EventTracker ....................................................................................................25
  Knowledge Objects ............................................................................................................................................25
  Token Templates ................................................................................................................................................26
  Reports ...............................................................................................................................................................27
  Alerts ...............................................................................................................................................................27
  Parsing Rules ...................................................................................................................................................28
  Behavior Rules ...................................................................................................................................................29
Create Flex Dashboards in EventTracker .................................................................................................................30
  Schedule Reports ...............................................................................................................................................30
  Create Dashlets ................................................................................................................................................32
Sample Flex Dashboards ........................................................................................................................................36
Introduction

The Bandura’s PoliWall is an in-line appliance which reduces noise at the network perimeter, thereby decreasing workloads of systems deeper inside the network, making routers, firewalls, and IPS/IDS more effective.

EventTracker receives syslog data from PoliWall and helps in efficient visualization and analysis of allowed or blocked traffic by employing alerts, reports, dashboards and knowledge objects. EventTracker also utilizes IP VOID to identify blacklisted IP addresses in allowed traffic and generates alert to tip-off concerned IT Admin.

Pre-requisites

- EventTracker v7.x or later should be installed.
- An exception should be added into windows firewall on EventTracker machine for syslog port 514.
- PoliWall Security Appliance must be installed and configured.

Syslog Configuration for PoliWall

1. Login PoliWall web interface with valid credentials.
3. In **Syslog Servers** pane, click **Add IPv4 Server** button to configure desired syslog server.
4. In **Add** window, enter the IP address of EventTracker manager. (Port 514 is used by default)
5. Click **Add** to apply changes.

### EventTracker Knowledge Pack (KP)

Once logs are received into EventTracker, Alerts, Reports, Knowledge Objects and Behavior Rules can be configured into EventTracker.

The following Knowledge Packs are applicable in EventTracker v7.x and later to support PoliWall.

#### Alerts

1. **PoliWall: Threat detected**

   This alert is generated when malicious activity is detected in transient traffic. E.g. Spam, Malware.

2. **PoliWall: New IP detected in allowed traffic**

   This alert is generated when new source or destination IP address is detected in allowed traffic.

3. **PoliWall: Blacklisted IP detected in allowed traffic**

   This alert is generated when blacklisted source or destination IP address is detected in allowed traffic.

#### Reports

1. **PoliWall - Allowed traffic details**

   This report provides information related to inbound or outbound traffic permitted by PoliWall.
Sample report:

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Device Name/IP</th>
<th>Traffic Direction</th>
<th>Protocol Type</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Source Country</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Destination Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sep 22 03:40</td>
<td>10.1.44.88</td>
<td>inbound</td>
<td>UDP</td>
<td>188.135.2.252</td>
<td>84588</td>
<td>India</td>
<td>25.52.69.54</td>
<td>53</td>
<td></td>
</tr>
<tr>
<td>Sep 22 03:40</td>
<td>10.1.44.88</td>
<td>outbound</td>
<td>UDP</td>
<td>104.131.137.159</td>
<td>64119</td>
<td>211.75.101.61</td>
<td>53</td>
<td>United States</td>
<td></td>
</tr>
<tr>
<td>Sep 22 04:30</td>
<td>10.1.44.88</td>
<td>outbound</td>
<td>UDP</td>
<td>104.131.137.159</td>
<td>12568</td>
<td>82.230.175.157</td>
<td>53</td>
<td>United States</td>
<td></td>
</tr>
<tr>
<td>Sep 22 04:30</td>
<td>10.1.44.88</td>
<td>inbound</td>
<td>UDP</td>
<td>217.122.135.58</td>
<td>04569</td>
<td>India</td>
<td>25.52.69.54</td>
<td>53</td>
<td></td>
</tr>
</tbody>
</table>

Log Sample:

2. PoliWall - Blocked traffic details

This report provides information related to inbound or outbound traffic prohibited by PoliWall.
EventTracker: Integrating PoliWall

Sample report:

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Device Name</th>
<th>Traffic Direction</th>
<th>Protocol Type</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Source Country</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Destination Country</th>
<th>Reason</th>
<th>Block Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sep 22 11:32:29</td>
<td>10.1.44.88</td>
<td>out</td>
<td>TCP</td>
<td>199.171.235</td>
<td>80</td>
<td></td>
<td>169.135.238.78</td>
<td>61606</td>
<td>Australia</td>
<td>flow</td>
<td>no flow record</td>
</tr>
<tr>
<td>Sep 22 11:32:29</td>
<td>10.1.44.88</td>
<td>in</td>
<td>TCP</td>
<td>97.67.147.40</td>
<td>80</td>
<td>Brazil</td>
<td>58.96.60.240</td>
<td>61606</td>
<td>flow</td>
<td>no flow record</td>
<td></td>
</tr>
<tr>
<td>Sep 22 11:32:29</td>
<td>10.1.44.88</td>
<td>in</td>
<td>TCP</td>
<td>31.204.120.213</td>
<td>80</td>
<td>United States</td>
<td>116.193.45.159</td>
<td>61606</td>
<td>flow</td>
<td>no flow record</td>
<td></td>
</tr>
<tr>
<td>Sep 22 11:32:30</td>
<td>10.1.44.88</td>
<td>out</td>
<td>TCP</td>
<td>249.191.96.92</td>
<td>80</td>
<td>China</td>
<td>151.71.96.202</td>
<td>61606</td>
<td>flow</td>
<td>no flow record</td>
<td></td>
</tr>
</tbody>
</table>

Figure 5

Log Sample:

<table>
<thead>
<tr>
<th>Event Time</th>
<th>EVENT ID</th>
<th>SITE / COMPUTER</th>
<th>USER</th>
<th>DOMAIN</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sep 22 11:32:29</td>
<td>10.1.44.88</td>
<td>PNPL-15-KP</td>
<td>N/A</td>
<td>N/A</td>
<td>SYSLOG daemon</td>
</tr>
</tbody>
</table>

Description:
Sep 22 11:32:29 10.1.44.88 packet log: 2016-08-18T17:02:34.847455-6400, action=dropped, direction=outbound, group_id=SRPolkata, group=0, protocol=TCP, country=United States, as_num=30632, as_name=Lazearweb USA, INC., reason=flow, detail=No flow record, src=232.212.54.106, dst=153.113.198.83, src_port=80, dst_port=61606, flag=FIN,ACK

Figure 6

3. PoliWall - Threat traffic details

This report provides information related to malicious activity detected in inbound or outbound traffic.
Sample report:

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Device Name/IP</th>
<th>Traffic Direction</th>
<th>Protocol Type</th>
<th>Action Type</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Source Country</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Block Reason</th>
<th>Risk Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sep 22 11:32:29</td>
<td>10.1.44.88</td>
<td>inbound</td>
<td>TCP</td>
<td>dropped</td>
<td>21.154.107.164</td>
<td>38849</td>
<td>United States</td>
<td>240.52.115.71</td>
<td>23</td>
<td>Spam</td>
<td>100</td>
</tr>
<tr>
<td>Sep 22 11:32:30</td>
<td>10.1.44.88</td>
<td>inbound</td>
<td>TCP</td>
<td>dropped</td>
<td>159.247.109.176</td>
<td>38849</td>
<td>Canada</td>
<td>153.75.50.44</td>
<td>23</td>
<td>Spam</td>
<td>100</td>
</tr>
<tr>
<td>Sep 22 11:32:30</td>
<td>10.1.44.86</td>
<td>outbound</td>
<td>TCP</td>
<td>dropped</td>
<td>129.18.124.199</td>
<td>38849</td>
<td>United States</td>
<td>10.233.131.231</td>
<td>23</td>
<td>Spam</td>
<td>100</td>
</tr>
<tr>
<td>Sep 22 11:32:31</td>
<td>10.1.44.86</td>
<td>outbound</td>
<td>TCP</td>
<td>dropped</td>
<td>98.20.238.85</td>
<td>38849</td>
<td>United States</td>
<td>212.33.77.109</td>
<td>23</td>
<td>Spam</td>
<td>100</td>
</tr>
</tbody>
</table>

Log Sample:

4. PoliWall - Blacklisted IP activity details

This report provides information related to blacklisted source or destination IP address detected in allowed traffic.
Sample report:

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Analysis Date</th>
<th>AS Number</th>
<th>AS Owner</th>
<th>Blacklist Status</th>
<th>City</th>
<th>Continent</th>
<th>Country Code</th>
<th>IP Address</th>
<th>ISP</th>
<th>Longitude</th>
<th>Latitude</th>
<th>Region</th>
<th>Reverse DNS</th>
</tr>
</thead>
</table>
| 09/22/2016 03:49:29 PM | 7 minutes ago | AS50010   | Oman Qatar Telecom 
Telecommunications | BLACKLISTED | Unknown | Asia (Oman) | 188.135.2.252 | com         |     | 21 / 57   | Unknown | siip.ca.com |                     |


**Figure 9**

Log Sample:

<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>9/22/2016 4:11:16 PM</td>
<td>ES\WIN2K12R2VM3 / SC</td>
<td>N/A</td>
<td>N/A</td>
<td>EventTracker</td>
<td></td>
</tr>
</tbody>
</table>

**Event Type:** Warning

**Log Type:** Application

**Category Id:** 0

**Description:** Blacklisted IP detected in Poliwall traffic.

**ScanReport:**

- IPAddress: 82.230.176.157
- AnalysisDate: 8 minutes ago
- BlacklistStatus: BLACKLISTED 1/40
- ReverseDNS: b17-157.fbx.proxid.n...
- ASNNumber: AS12322
- ASOwner: Free SAS
- ISP: Free SAS
- Continent: Europe
- CountryCode: (FR) France
- Longitude: 48.86 / 2.35
- City: Unknown
- Region: Unknown

**SourceLog:**

Sep 22 04:05:30 10.1.44.88 packet_log: 2016-08-18T17:03:36.204166+04:00 action=allowed, direction=outbound, group_uid=GPI_DEF_EGRESS_GROUP, protocol=UDP, country=United States, as_num=30633, as_name=LeaseWeb USA, inc., reason=country, src=104.131.137.159, dst=82.230.176.157, src_port=65399, dst_port=93

**Figure 10**
Behavior Rules

1. **PoliWall allowed traffic destination IP activity**

   This behavior rule helps in identification of new destination IP addresses in inbound or outbound allowed traffic.

   ![NEW DESTINATION ADDRESS OBSERVED][5]

   ![Figure 11]

<table>
<thead>
<tr>
<th>DESTINATION ADDRESS</th>
<th>COUNT</th>
</tr>
</thead>
<tbody>
<tr>
<td>25.52.69.54</td>
<td>5</td>
</tr>
<tr>
<td>204.46.87.177</td>
<td>1</td>
</tr>
<tr>
<td>196.142.23.248</td>
<td>1</td>
</tr>
<tr>
<td>193.101.136.85</td>
<td>1</td>
</tr>
<tr>
<td>185.129.62.63</td>
<td>1</td>
</tr>
</tbody>
</table>

2. **PoliWall allowed traffic source IP activity**

   This behavior rule helps in identification of new source IP addresses in inbound or outbound allowed traffic.
Knowledge Objects

1. PoliWall Traffic

   This KO helps in advanced analysis and reporting of PoliWall allowed or blocked traffic.
EventTracker: Integrating PoliWall

2. PoliWall Threat

This KO helps in advanced analysis and reporting of PoliWall malicious traffic.
3. **PoliWall Blacklisted IP**

This KO helps in advanced analysis and reporting of blacklisted IP source or destination addresses detected in allowed traffic.

![PoliWall Blacklisted IP](image)

**Figure 15**

**Import PoliWall Knowledge Pack into EventTracker**

1. Contact EventTracker Support to acquire PoliWall Knowledge Pack.
2. Download ‘KP-PoliWall.zip’ from provided location and extract at the desired location.
3. Move ‘PoliWallblacklistIP.ps1’ script from 'Script' folder to the following path.

```
C:\Program Files (x86)\Prism Microsystems\EventTracker\RemedialActionScripts\PoliWall\n```

EventTracker Installation Path
PoliWall Script Folder Path

4. Import KP items in ‘KP’ folder in following sequence:

- Knowledge Objects
- Token Templates
- Reports
- Alerts
- Parsing Rules
- Behavior Rules
EventTracker Manager

Knowledge Objects and Token Templates can be imported using EventTracker Web Console.

- Login EventTracker Manager Web Console.

![Image](image1.png)

Figure 17

- Click Admin.

Knowledge Objects

1. Select Knowledge Objects from Admin drop-down.

2. Click 'Import' option.
3. In IMPORT pane and click on Browse button.

4. Locate All PoliWall group of knowledge objects.etko file, and then click the UPLOAD button.
5. Select all objects and click **Overwrite** button.

**Token Templates**

1. Select **Parsing Rules** from **Admin** drop-down.
2. Select **Template** tab.
3. Click **‘Import’** option and select **Browse** button.

4. Locate **All PoliWall group of token templates.ettd** file, and then click the **UPLOAD** button.
5. Select all objects and click ‘Import’ option.

EventTracker Control Panel

Alerts, Reports and Parsing Rules can be imported using EventTracker Control Panel’s Export/Import Utility.

- Launch EventTracker Control Panel.
• Double click **Export Import Utility**.

• Select **Import** tab.
Reports

1. Click **Reports** option, and then click the browse button.

2. Locate the All PoliWall group of reports.issch file, and then click **Open** button.

![Image of Export Import Utility](image)

Figure 24

3. To import categories, click the **Import** button.

EventTracker displays success message.
4. Click OK.

Alerts

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

2. Locate the **All PoliWall group of alerts.isalt** file, and then click the **Open** button.

3. To import alerts, click the **Import** button.
EventTracker displays success message.

Figure 27

4. Click **OK**.

**Parsing Rules**

1. Click **Token value** option, and then click the browse button.

Figure 28
2. Locate the **All PoliWall group of parsing rules.istoken** file, and then click the **Open** button.

3. To import tokens, click the **Import** button.

   EventTracker displays success message.

![Export Import Utility](image)

**Selected token values are imported successfully.**

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

**Behavior Rules**

1. Click **Behavior Rules** option, and then click the browse button.

2. Locate the **All PoliWall group of behavior rules.isrule** file, and then click **Open** button.
3. To import categories, click the **Import** button. EventTracker displays success message.

4. Click **OK**.
Verify PoliWall knowledge pack in EventTracker

- Login to EventTracker Manager Web Console.

![Admin drop-down menu](image)

**Figure 32**

- Click Admin.

**NOTE:** It is advised to select appropriate systems in alerts, reports and behavior rules to improve performance.

Knowledge Objects

1. Select **Knowledge Objects** from Admin drop-down.

2. Scroll down and select **PoliWall** in **Groups** pane. Imported **PoliWall** objects are shown along-side.
Token Templates

1. Select Parsing Rules from Admin drop-down.
2. Select Template Tab.
3. Scroll down and select PoliWall in Groups pane. Imported PoliWall templates are shown along-side.
Reports

1. Click the **Reports** menu, and then select **Configuration**.

![Figure 35](image)

2. In **Reports Configuration** pane, select **Defined** option.
3. Scroll down and select **PoliWall** in **Groups** pane. Imported **PoliWall** reports are shown along-side.

![Figure 36](image)

Alerts

1. Select **Alerts** from **Admin** drop-down.
2. In the **Search** field, type ‘**PoliWall**’, and then click **Go** button.
3. Alert Management page will display all the imported PoliWall alerts.

![Alert Management Page](image)

**Figure 37**

4. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

![Message Box](image)

**Figure 38**

5. 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.

### Parsing Rules

1. Select **Parsing Rules** from **Admin** drop-down.
2. Scroll down and select **PoliWall** in **Groups** pane. Imported **PoliWall** rules are shown along-side.
Behavior Rules

1. Select **Behavior Rules** from **Admin** drop-down.
2. Scroll down and find **PoliWall** rules.

Figure 39

Figure 40
Create Flex Dashboards in EventTracker

NOTE: Flex dashboard feature is available from EventTracker Enterprise v8.0 onwards.

Schedule Reports

1. Login EventTracker Manager Web Console.

![Figure 41](image)

2. Navigate to Reports>Configuration.
3. Scroll down and select PoliWall in report groups. Select Defined check box.

![Figure 42](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.
5. In next page, check column names to persist using PERSIST checkboxes beside them. Choose suitable Retention period.
6. Proceed to next step and click **Schedule** button.
7. 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.

![Protocol Type: TCP](image)

**Figure 48**

4. If satisfied, click **Configure** button.
5. Click ‘customize’ to locate and choose created dashlet.
6. Click to add dashlet to earlier created dashboard.
Sample Flex Dashboards

1. PoliWall Inbound Blocked Traffic by Protocol Type

- **Data Source:** PoliWall: Blocked traffic details
- **Chart Type:** Donut
- **Axis Labels [X-Axis]:** Source Country
- **Filter:** Traffic Direction
  - **Filter Direction:** inbound
- **Legend [Series]:** Protocol Type
  - **Select:** All

![Protocol Type: TCP](image)

09/21 04:08 - 09/21 16:08

*Figure 50*
2. PoliWall Outbound Blocked Traffic with Reason

- **Data Source:** PoliWall: Blocked traffic details
- **Chart Type:** Donut
- **Axis Labels (X-Axis):** Destination Country
- **Filter:** Traffic Direction
  - Filter Direction: outbound
- **Legend (Series):** Block Reason
  - Select: All

![Pie chart showing blocked traffic reasons and destination countries.](image)

*Figure 51*
3. PoliWall-Inbound Allowed Traffic by Country

- **Data Source:** PoliWall: Allowed traffic details
- **Chart Type:** Donut
- **Axis Labels [X-Axis]:** Source Country
- **Filter:** Traffic Direction
  - Filter Direction: inbound
- **Legend [Series]:** Device Name/IP
  - Select: All

![Chart: PoliWall-Inbound Allowed Traffic by Country](image)

*Figure 52*
4. **PoliWall-Outbound Allowed Traffic by Protocol Type**

- **Data Source:** PoliWall: Allowed traffic details
- **Chart Type:** Donut
- **Axis Labels [X-Axis]:** Destination Country
- **Filter:** Traffic Direction
  - **Filter Direction:** outbound
- **Legend [Series]:** Protocol Type
  - **Select:** All

![Protocol Type: UDP](image)

Figure 53
5. PoliWall Inbound Threats by Risk Score

- **Data Source:** PoliWall: Threat traffic details
- **Chart Type:** Donut
- **Axis Labels [X-Axis]:** Source Country
- **Filter:** Traffic Direction
  - **Filter Direction:** inbound
- **Legend [Series]:** Risk Score
  - **Select:** All

![Risk Score: 100](image)

09/21 04:08 - 09/21 16:08

**Figure 54**
6. PoliWall Outbound Threats with Country

- **Data Source**: PoliWall: Threat traffic details
- **Chart Type**: Donut
- **Axis Labels [X-Axis]**: Destination Country
- **Filter**: Traffic Direction
  - **Filter Direction**: outbound
- **Legend [Series]**: Block Reason
  - **Select**: All

![Figure 55](image-url)
7. **PoliWall Blocked IP with Country**

- **Data Source**: PoliWall: Blacklisted IP activity details
- **Chart Type**: Donut
- **Axis Labels [X-Axis]**: IP Address
- **Legend [Series]**: Country Code
  - Select: All

![Figure 56]

<~X~>