Integrate pfSense

EventTracker Enterprise
Abstract

This guide provides instructions to configure pfSense 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 pfSense 2.3.1.

Audience

Administrators, who are responsible for monitoring pfSense using EventTracker Enterprise.
Table of Contents

Abstract.................................................................................................................................................. 1
Scope.................................................................................................................................................. 1
Audience............................................................................................................................................. 1
Introduction ........................................................................................................................................... 3
Pre-requisites........................................................................................................................................ 3
Integration Method for pfSense............................................................................................................ 3
EventTracker Knowledge Pack (KP)....................................................................................................... 6
  Categories .......................................................................................................................................... 6
  Alerts ................................................................................................................................................ 6
  Flex Reports ................................................................................................................................... 6
Import pfSense knowledge pack into EventTracker ............................................................................. 7
  Category ............................................................................................................................................. 8
  Alerts ................................................................................................................................................ 10
  Templates ....................................................................................................................................... 11
  Knowledge Object ............................................................................................................................ 12
  Flex Reports ................................................................................................................................... 13
Verify pfSense knowledge pack in EventTracker ................................................................................ 14
  Category ............................................................................................................................................. 14
  Alerts ................................................................................................................................................ 14
  Template ....................................................................................................................................... 15
  Knowledge Object ............................................................................................................................ 16
  Flex Reports ................................................................................................................................... 17
Create Flex Dashboards in EventTracker ............................................................................................ 17
  Schedule Reports ............................................................................................................................. 17
  Create Dashlets .............................................................................................................................. 20
Sample Flex Dashboards ..................................................................................................................... 24
Introduction

pfSense is an open source firewall/router computer software distribution based on FreeBSD. It is installed on a physical computer or a virtual machine to make a dedicated firewall/router for a network and is noted for its reliability and offering features often only found in expensive commercial firewalls. pfSense is commonly deployed as a perimeter firewall, router, wireless access point, DHCP server, DNS server, and as a VPN endpoint.

EventTracker collects the logs, helps administrator to analyze the events and generate the reports for the defined firewall rules and monitors the configured alerts.

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.
- pfSense version 2.3.1 must be installed and configured.

Integration Method for pfSense

1. Log into the pfSense Web interface.

2. Go to Status -> System Logs
3. Click the **Settings** tab.

4. Enable the checkbox “**Enable syslogging to remote syslog server**”.

**NOTE:**

**Source Address:** Chooses which interface on pfSense to use for initiating log messages. If the target syslog server is across an IPsec tunnel, this should be a local interface address inside of a Phase 2 definition for the IPsec tunnel.
**IP Protocol:** Selects IPv4 or IPv6 to be used for sending log messages when multiple possibilities exist.

**Enable Remote Logging:** When checked, send syslog entries to the defined servers.

**Remote Syslog Servers:** List of remote syslog servers. It can be an IP address (IPv4 or IPv6), hostname, or IP: port if syslog is on a non-default port. (E.g. EventTracker manager IP address and port (10.150.26.33:514)

**Remote Syslog Contents:** Select the items which will be sent via remote syslog. **Everything** is the preferred choice.

5. Type the IP of the logging server in the box next to Remote syslog server i.e. EventTracker manager.

6. Check the boxes for the log entries to forward.

7. Click Save.

---

**Figure 5**
EventTracker Knowledge Pack (KP)

Once logs are received in to EventTracker, Alerts and Reports can be configured into EventTracker.

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

Categories

- **pfSense-Traffic allowed and blocked details**
  
  This category provides information related to traffic blocked or passed by the rule configured on the firewall.

Alerts

- **pfSense - IPsec tunnel down**
  
  This alert is generated when IPsec tunnel goes down.

Flex Reports

- **pfSense: Traffic allowed and blocked details**
  
  This report provides the information related to protocols (TCP, UDP, ICMP, and ICMPv6), protocol numbers, traffic passed or blocked on the interface and direction of the traffic (inbound or outbound).

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Computer</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Interface</th>
<th>Direction</th>
<th>Action</th>
<th>Protocol</th>
<th>Protocol Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jul 05 09:14:49</td>
<td>PFSENSE-PW1</td>
<td>192.168.1.121</td>
<td>80</td>
<td>172.16.17.32</td>
<td>443</td>
<td>80</td>
<td>in</td>
<td>block</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Jul 05 09:14:49</td>
<td>PFSENSE-PW1</td>
<td>192.168.1.121</td>
<td>80</td>
<td>172.16.17.32</td>
<td>443</td>
<td>80</td>
<td>in</td>
<td>block</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Jul 05 09:14:49</td>
<td>PFSENSE-PW1</td>
<td>192.168.1.121</td>
<td>80</td>
<td>172.16.17.32</td>
<td>443</td>
<td>80</td>
<td>in</td>
<td>block</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Jul 05 09:14:49</td>
<td>PFSENSE-PW1</td>
<td>192.168.1.121</td>
<td>80</td>
<td>172.16.17.32</td>
<td>443</td>
<td>80</td>
<td>in</td>
<td>block</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Jul 05 09:14:49</td>
<td>PFSENSE-PW1</td>
<td>192.168.1.121</td>
<td>80</td>
<td>172.16.17.32</td>
<td>443</td>
<td>80</td>
<td>in</td>
<td>block</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Jul 05 09:14:49</td>
<td>PFSENSE-PW1</td>
<td>192.168.1.121</td>
<td>80</td>
<td>172.16.17.32</td>
<td>443</td>
<td>80</td>
<td>in</td>
<td>block</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>

Figure 6
Import pfSense knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence

- Categories
- Alerts
- Templates
- Knowledge Objects
- Flex Reports

1. Launch EventTracker Control Panel.
2. Double click Import Export Utility.
3. Click the **Import** tab.

4. **Import knowledge pack as specified in the sequence.**

**Category**

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

2. Locate the **All pfSense group of categories.iscat** file, and then click **Open** button.
To import categories, click the **Import** button.

EventTracker displays success message.

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

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

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

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

   EventTracker displays success message.

   ![Figure 11](image1)

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

   ![Figure 12](image2)
Templates

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

2. Select Template tab, and then click on 'Import' option.

3. Locate the All pfSense group of templates.ettd file, and then click the Open button.
4. To import tokens, click the **Import** button.

EventTracker displays success message.

![Export Import Utility](image)

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

**Knowledge Object**

1. Click the **Admin** menu, and then click **Knowledge Objects**.
2. Click on the **Import** option.
3. In **IMPORT** pane click on **Browse** button.

![IMPORT Window](image)

**Figure 20**

4. Locate All **pfSense group of knowledge object.etko** file, and then click the **UPLOAD** button.

**Flex Reports**

1. Click **Report** option, and then click the browse button.
2. Locate the All **pfSense group of flex reports.issch** file, and then click the **Open** button.

![Export Import Utility](image)

**Figure 17**
3. Click the **Import** button to import the scheduled reports, EventTracker displays success message.

![Figure 18](image)

**Verify pfSense knowledge pack in EventTracker**

**Category**

1. In the **EventTracker Enterprise**, web interface.
2. Click the **Admin** dropdown, and then click **Categories**.
3. In the **Category Tree**, expand **pfSense** group folder to see the imported categories.

![Figure 21](image)

**Alerts**

1. In the **EventTracker Enterprise**, web interface, click the **Admin** dropdown, and then click **Alerts**.
2. In the **Search** field, type **pfSense**, and then click **Go** button.

   Alert Management page will display all imported **pfSense** alert.
3. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

![Message Box](image)

**Figure 23**

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.

**Template**

1. Logon to **EventTracker Enterprise**.

2. Click the **Admin** menu, and then click **Parsing Rules**.
Knowledge Object

1. Click the Admin menu, and then click Knowledge Objects.

2. Scroll down and select pfSense in Objects pane. Imported pfSense object details are shown.
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.

   EventTracker displays Defined page.

3. In search box enter ‘pfSense’, and then click the Search button.

   EventTracker displays Flex reports of pfSense

![Figure 26](image)

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 **pfSense** in report groups. Check **Defined** dialog box.

4. Click on ‘**schedule**’ to plan a report for later execution.
REPORT WIZARD

TITLE: PSense-TRAFFIC ALLOWED AND BLOCKED DETAILS
LOGS

Review cost details and configure the publishing options.

DISK COST ANALYSIS

Estimated time for completion: 00:00:00@HH:MM:SS
Number of file(s) to be processed: 2
Available disk space: 256 GB
Required disk space: 50 MB

- Enable publishing options (Configure SMTP Server in manager configuration screen to use this option)
- Deliver results via E-mail
- Notify results via E-mail

To E-mail: [Enter email addresses separated by commas]

Update status via RSS: Select Feed

Show in: [Select option]

- Persist data in Eventwaist Reporter

Figure 29
5. 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.
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: pfSense: Traffic allowed and blocked details**

1. **pfSense: Traffic blocked by IPs**

   **WIDGET TITLE:** Traffic blocked by IPs
   **CHART TYPE:** Donut
   **AXIS LABELS [X-AXIS]:** Source IP
   **Label Text:** Source IP
   **FILTER:** Action
   **FILTER Values:** block

   ![pfSense: Traffic blocked by IPs](image)

   **Figure 36**
2. **pfSense: Traffic blocked by Port**

   **WIDGET TITLE:** Traffic blocked by Port  
   **CHART TYPE:** Donut  
   **AXIS LABELS [X-AXIS]:** Destination Port  
   **Label Text:** Destination Port  
   **FILTER:** Action  
   **FILTER Values:** block

![PFSENSE TRAFFIC BLOCKED BY PORT](image)

   **Figure 37**

3. **pfSense: Traffic blocked by Protocols**

   **WIDGET TITLE:** Traffic blocked by Protocols  
   **CHART TYPE:** Donut  
   **AXIS LABELS [X-AXIS]:** Protocol  
   **Label Text:** Protocols  
   **FILTER:** Action  
   **FILTER Values:** block
Figure 38
4. **pfSense: Traffic blocked by Interface**

   **WIDGET TITLE:** Traffic blocked by Interface  
   **CHART TYPE:** Donut  
   **AXIS LABELS (X-AXIS):** Interface  
   **Label Text:** Interface  
   **FILTER:** Action  
   **FILTER Values:** block  

   ![PFSENSE TRAFFIC BLOCKED BY INTERFACE](image)

   Figure 39
5. **pfSense: Traffic allowed by IPs**

**WIDGET TITLE:** Traffic allowed by IPs  
**CHART TYPE:** Donut  
**AXIS LABELS [X-AXIS]:** Source IP  
**Label Text:** Source IP  
**FILTER:** Action  
**FILTER Values:** Pass