Integrate Check Point Firewall

EventTracker v8.0 and above

Publication Date: September 10, 2019
Abstract

This guide helps you in configuring Check Point and EventTracker to receive Check Point events. You will find the detailed procedures required for monitoring Check Point.

Scope

The configurations detailed in this guide are consistent with EventTracker v8.x and later, Check Point Firewall R80.10 and later.

Audience

Check Point users, who wish to forward Events to EventTracker Manager and monitor events using EventTracker.
# Table of Contents

Abstract ............................................................................................................................... 1
Scope ..................................................................................................................................... 1
Audience ............................................................................................................................... 1

1. Overview ......................................................................................................................... 3

2. Integration of Check Point Firewall with EventTracker using Syslog .................................. 3
   2.1 Prerequisites ............................................................................................................. 3

3. EventTracker Knowledge Pack .......................................................................................... 6
   3.1 Categories .................................................................................................................. 6
   3.2 Alerts ......................................................................................................................... 7
   3.3 Reports ...................................................................................................................... 7

4. Import knowledge pack into EventTracker ......................................................................... 15
   4.1 To import Alerts ....................................................................................................... 15
   4.2 To import Token Templates ....................................................................................... 17
   4.3 To import Flex Reports ............................................................................................. 18

5. Verify knowledge pack in EventTracker ............................................................................ 19
   5.1 Verify Alerts ............................................................................................................. 19
   5.2 Verify Token Templates ............................................................................................ 20
   5.3 Verify Flex Reports ................................................................................................... 20

6. Create Dashboards in EventTracker .................................................................................. 22
   6.1 Schedule Reports ....................................................................................................... 22
   6.2 Create Dashlets ......................................................................................................... 23
   6.3 Sample Flex Dashboards .......................................................................................... 26
1. Overview

Check Point offers the perfect combination of proven security, easy deployment, and effective management by consolidating key security applications (firewall, VPN, intrusion prevention, and antivirus and more) into the same single, efficiently managed solution.

EventTracker’s built-in knowledge pack enables you to gather business intelligence providing increased security, performance, availability, and reliability of your systems.

Through alerts, knowledgebase solutions, and reports, EventTracker helps you correct problems long before a disastrous failure occurs.

2. Integration of Check Point Firewall with EventTracker using Syslog

Configure syslog for Check Point Firewall R80.10, two types of configuration need to configure.

- Gaia GUI portal
- Gaia CLISH

**Note:** There are some command options and parameters, which you cannot configure in the Gaia GUI Portal.

2.1 Prerequisites

- EventTracker v8.x should be installed.
- Administrative access to Check Point Firewall Smart Console.
- Check Point Firewall version R80.10 and later.
- Microsoft Windows Version 7 or later should be installed.
- An exception should be added into the Windows firewall on the EventTracker machine for syslog port 514.

To enable syslog reporting on your Check Point Firewall Gaia Portal GUI:

1. Click **System Management** in the main menu, and click the **System Logging** tab.
2. The **System Logging** page appears.
3. Click on the **Add** tab.
   - **IP Address**: Mention EventTracker IP address.
   - **Port**: Please mention syslog server (514) port number.
4. Click **Apply**.
5. Logs will now be forwarded to the EventTracker.

**To enable syslog reporting on your Check Point Firewall Gaia R80.10 CLISH:**

Below configuration runs on Check Point Firewall system.

1. Please login to Check Point Firewall R80.10 server console with admin privileges.
2. Enable expert mode by using `expert` command.
3. Add the below lines in the “/etc/rc.d/init.d/cpboot” file.

```
fw log -f -t -n -l 2> /dev/null | awk ‘NF’ | sed ‘/^$/d’ | logger -p local4.info -t CP_FireWall &
```
4. Please exit from the **expert** mode.
5. Configure syslog by using the below command.

   `> add syslog log-remote-address <Please mention EventTracker IP> level info`

6. Save config.
3. EventTracker Knowledge Pack

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

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

3.1 Categories

- **Check Point: Alerts**- All events logged by Check Point when an alert is issued by the Security Gateway.
- **Check Point: All firewall events**- All events generated by Check Point firewall.
- **Check Point: FTP activity**- All events generated by Check Point firewall related to FTP traffic passing through a security gateway.
- **Check Point: IMAP/POP3 activity**- All events generated by Check Point related to IMAP/POP3 traffic passing through a security gateway.
- **Check Point: Login failure**- All logs generated by Check Point related to all login failures that were reported by a firewall and/or Connectra.
- **Check Point: Network activity**- All events generated by Check Point related to traffic accepted by a firewall.
- **Check Point: Peer to peer activity**- All events logged by Check Point related to Peer to Peer.
- **Check Point: SMTP activity**- All events generated by Check Point firewall related to SMTP mail traffic passing through a security gateway.
- **Check Point: Traffic allowed**- All events generated by Check Point when traffic is allowed by the firewall.
- **Check Point: Traffic Blocked**- All events generated by Check Point when network traffic is blocked.
- **Check Point: Web activity**- All events generated by Check Point related to the web traffic passing through the security gateway.
- **Check Point: All identity awareness**- All Identity awareness events logged by Check Point.
- **Check Point: Failed login**- All identity awareness events logged by Check Point related to failed login.
- **Check Point: Login activity**- All events logged by Check Point identity awareness related to user login, logout and failed login.
- **Check Point: All IPS events**- All events generated by Check Point related to IPS.
- **Check Point: application control intrusion**- All logs generated by Check Point IPS application control protection.
- **Check Point: Critical intrusion not prevented**- All events generated by Check Point when any critical intrusion detected but not prevented.
- **Check Point: Protocol anomaly intrusion**- All logs generated by Check Point IPS Protocol anomaly protection.
- **Check Point: Administrator login**- All events logged by Check Point when administrator logs in to Check Point smartcenter server.
- **Check Point: All Check Point management events**- All Check Point management events.
• **Check Point: Audit activities** - All Check Point Audit logs.

• **Check Point: Object manipulation** - All events logged by Check Point when any object manipulation is done.

• **Check Point: Policy installation** - All events logged by Check Point when policy installation is performed.

• **Check Point: All VPN activity** - All events logged by Check Point IPSec VPN.

• **Check Point: Successful VPN login** - All events logged by Check Point VPN after a successful VPN connection.

• **Check Point: VPN login failure** - All events logged by Check Point when login fails to VPN server.

3.2 Alerts

• **Check Point: Configuration changes** - This alert is generated when any configuration changes are done.

• **Check Point: Interface status changed** - This alert is generated when the interface status is changed.

• **Check Point: Logon failure** - This alert is generated when an identity awareness event is logged related to a login failure.

• **Check Point: Upgrade and downgrade activity** - This alert is generated when any upgrade or downgrade checkpoint hotfixes or patches are done.

• **Check Point: User management activity** - This alert is generated when any user related changes are done for (e.g. user added to a group, user deleted)

• **Check Point: Critical attack not prevented** - This alert is generated when any critical intrusion is detected but not prevented.

• **Check Point: IPS alerts** - This alert is generated when an alert is generated related to IPS.

• **Check Point: Successful VPN login** - This alert is generated when a successful VPN connection is established.

3.3 Reports

• **Check Point-Login and logout activity**: This report provides us the information related to logon and logout activities which include username, system name, source address, and method when logon and logout happens on Check Point firewall.
Integrate Check Point Firewall

Logs Considered:

- **Check Point-Logon failure**: This report provides us the information related to logon failure which includes username, system name, source address and reason when logon fails on Check Point firewall.

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Client IP address</th>
<th>Protocol</th>
<th>Username</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/07/2017 03:23:50 PM</td>
<td>CONTOSO-CP</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>03/07/2017 03:24:31 PM</td>
<td>CONTOSO-CP</td>
<td>172.237.111.3</td>
<td>ssh</td>
<td>Richard</td>
<td>Accepted password</td>
</tr>
<tr>
<td>03/07/2017 04:11:00 PM</td>
<td>CONTOSO-CP</td>
<td></td>
<td>ssh</td>
<td>Richard</td>
<td>session closed</td>
</tr>
<tr>
<td>03/07/2017 04:13:47 PM</td>
<td>CONTOSO-CP</td>
<td></td>
<td></td>
<td>Richard</td>
<td>logged out</td>
</tr>
<tr>
<td>03/07/2017 03:23:51 PM</td>
<td>CONTOSO-CP</td>
<td>177.237.14.05</td>
<td></td>
<td>Tehet</td>
<td></td>
</tr>
</tbody>
</table>
Logs Considered:

<table>
<thead>
<tr>
<th>Event Type: Information</th>
<th>Event Type: Information</th>
<th>Event Type: Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Type: Application Category Id: 0</td>
<td>Log Type: Application Category Id: 0</td>
<td>Log Type: Application Category Id: 0</td>
</tr>
<tr>
<td>Description: Mar 8 01:03:35 CONTOSO-CP\xpand[11328]: HTTP login denied from 172.168.33.101</td>
<td>Description: Mar 8 11:30:10 CONTOSO-CP suh[45698]: Failed password for Hanna from 192.168.2.11 port 22 ssh2</td>
<td>Description: Mar 7 10:02:22 CONTOSO-CP\xpand[22326]: authentication failure: loginname= uid=0 euid=0 tty=sh user=host=172.236.1.101 user=Tony</td>
</tr>
</tbody>
</table>

**Figure 7**

- **Check Point-Allowed traffic:** This report provides us the information related to firewall allowed traffic which includes source address, source port, a destination address, destination port, and service name when a connection is accepted by Check Point firewall between source and destination.

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Firewall IP</th>
<th>Interface</th>
<th>Rule Id</th>
<th>Rule uid</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Protocol</th>
<th>Service Id</th>
<th>Source port</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/08/2017 08:21:01 PM</td>
<td>192.168.11.7</td>
<td>eth8</td>
<td>116</td>
<td>11111111-2222-3333-3808-02203F05349</td>
<td>192.168.11.13</td>
<td>192.168.11.255</td>
<td>udp</td>
<td>nbdtransport</td>
<td>38</td>
</tr>
</tbody>
</table>

**Figure 8**

Logs Considered:

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Event Type: Information</th>
<th>Event Type: Information</th>
<th>Event Type: Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/10/2017 4:22:27 PM</td>
<td>Log Type: Application Category Id: 0</td>
<td>Log Type: Application Category Id: 0</td>
<td>Log Type: Application Category Id: 0</td>
</tr>
</tbody>
</table>

**Figure 9**
• **Check Point- Denied traffic**: This report provides us the information related to firewall denied traffic which includes source address, source port, a destination address, destination port and service name when a connection is denied by Check Point firewall between source and destination.

![Figure 10](image)

**Logs Considered:**

![Figure 11](image)

• **Check Point-Configuration changes**: This report provides us the information related to any configuration changes that are done e.g. trapstate on or off, interface changes etc.
• **Check Point-Device maintenance messages:** This report provides us the information related to device maintenance messages such as shutting down for system reboot, boot image information, backup operations, etc.
Logs Considered:

![Check Point Firewall Logs](image)

- **Check Point-DHCP server activity**: This report provides us the information related to DHCP server activity.

![Logs Considered](image)

![EventTracker](image)
• **Check Point-Interface status changed**: This report provides us the information related to the interface status whether it is Up or Down.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Interface id</th>
<th>Interface state</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/07/2017 05:53:06 PM</td>
<td>CONTOSO-CP</td>
<td>eth-s1fc0c0</td>
<td>up</td>
</tr>
<tr>
<td>03/07/2017 05:50:00 PM</td>
<td>CONTOSO-CP</td>
<td>eth0-a2p5c0</td>
<td>down</td>
</tr>
<tr>
<td>03/07/2017 07:45:13 PM</td>
<td>CONTOSO-CP</td>
<td>enx78a7d1e46da</td>
<td>up</td>
</tr>
<tr>
<td>03/07/2017 08:00:00 PM</td>
<td>CONTOSO-CP</td>
<td>enp2a0-ac70b9</td>
<td>down</td>
</tr>
<tr>
<td>03/07/2017 10:29:57 PM</td>
<td>CONTOSO-CP</td>
<td>eno1-s3bg36</td>
<td>up</td>
</tr>
<tr>
<td>03/07/2017 10:51:05 PM</td>
<td>CONTOSO-CP</td>
<td>eth0-a2p5c0</td>
<td>down</td>
</tr>
</tbody>
</table>

**Figure 18**

**Logs Considered:**

<table>
<thead>
<tr>
<th>LOG TIME</th>
<th>EVENT ID</th>
<th>SITE / COMPUTER</th>
<th>USER</th>
<th>DOMAIN</th>
<th>CATEGORY</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/7/2017 5:53:06 PM</td>
<td>5555</td>
<td>PNPL-64P / PNPL-945</td>
<td>N/A</td>
<td>N/A</td>
<td>Category Id: 0</td>
<td>Sysdog</td>
</tr>
<tr>
<td>Description:</td>
<td>Mar 6 12:07:15 CP-HA2-ORL xpano[2228]: Interface enxs1a2p3c1 set to down</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LOG TIME</th>
<th>EVENT ID</th>
<th>SITE / COMPUTER</th>
<th>USER</th>
<th>DOMAIN</th>
<th>CATEGORY</th>
<th>SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/7/2017 5:53:06 PM</td>
<td>5555</td>
<td>PNPL-64P / PNPL-945</td>
<td>N/A</td>
<td>N/A</td>
<td>Category Id: 0</td>
<td>Sysdog</td>
</tr>
<tr>
<td>Description:</td>
<td>Mar 6 12:07:15 CP-HA2-ORL xpano[2228]: Interface enxs1a2p3c1 set to up</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 19**

• **Check Point-Upgrade and downgrade activity**: This report provides us the information related to the upgrade or downgrade activity that is done. For e.g. checkpoint hotfixes or patches are upgraded to remove.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Patch details</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/07/2017 05:30:39 PM</td>
<td>CONTOSO-CP</td>
<td>installer_available_install_packages_number 1</td>
</tr>
<tr>
<td>03/07/2017 05:56:00 PM</td>
<td>CONTOSO-CP</td>
<td>installer_packages:Check_Point_Hotfix_R77.20_%sk104443.tgz:tag:importance</td>
</tr>
<tr>
<td>03/07/2017 07:45:13 PM</td>
<td>CONTOSO-CP</td>
<td>installer_packages:Check_Point_SmartConsole_ R77.20_1124_Auto_Update.tgz 3</td>
</tr>
<tr>
<td>03/07/2017 08:00:00 PM</td>
<td>CONTOSO-CP</td>
<td>upgrade:package 8.7.111</td>
</tr>
<tr>
<td>03/07/2017 08:30:39 PM</td>
<td>CONTOSO-CP</td>
<td>Gale DB Upgrade successful</td>
</tr>
<tr>
<td>03/07/2017 10:29:57 PM</td>
<td>CONTOSO-CP</td>
<td>upgrade:package 8.7.111</td>
</tr>
<tr>
<td>03/07/2017 10:31:05 PM</td>
<td>CONTOSO-CP</td>
<td>installer_available_install_packages_number 1</td>
</tr>
</tbody>
</table>

**Figure 20**
Logs Considered:

**Check Point-User management activity:** This report provides us the information related to user management activity, which is any user-related changes done e.g. user added to a group, user deleted.

![Figure 21](image1)

![Figure 22](image2)

Logs Considered:

![Figure 23](image3)
4. Import knowledge pack into EventTracker

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

Import Alerts/Category/Tokens/Flex Reports as given below.

![EventTracker Control Panel](image)

**Figure 24**

4.1 To import Alerts

1. Click **Alerts** option, and then click the **browse** button.
2. Locate the **Check Point group of alerts.isalt file**, and then click the **Open** button.

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

4. Click **OK**, and then click the **Close** button.
4.2 To import Token Templates

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

![Figure 27](image)

4. Locate the Check Point group of Token **templates.ettd file**, and then click the Open button.

![Figure 28](image)

5. Now select the checkbox and then click on ‘**Import**’ option. EventTracker displays a success message.

![Figure 29](image)

6. Click on the **OK** button.
4.3 To import Flex Reports

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

![Figure 30](image)

2. Locate the **Check Point group of Reports.issch** file, and then click the **Open** button.

3. Click the **Import** button to import the scheduled reports. EventTracker displays a success message.

![Figure 31](image)

4. Click the **OK** button. Click the **Close** button.
5. Verify knowledge pack in EventTracker

5.1 Verify Alerts

1. Logon to EventTracker.
2. Click Admin dropdown, and then click Alert.
3. In the Search field, type ‘Check Point’, and then click the Go button.
   Alert Management page will display all the imported Check Point 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:

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.

5.2 Verify Token Templates

1. Logon to the **EventTracker** web interface.
2. Click the **Admin** menu, and then click **Parsing Rules** and click **Template**.

![Parsing Rule](image)

**Figure 34**

5.3 Verify Flex Reports

1. Logon to **EventTracker**.
2. Click the **Reports**.
3. Select the **Configuration**.
   
   In the **Reports Configuration**, select **Defined** from a radio button. EventTracker displays the **Defined** page.
4. Select **Check Point** folder from Reports Groups.
Here you can find imported defined reports.
6. Create Dashboards in EventTracker

6.1 Schedule Reports

1. Open EventTracker in browser and logon.

![Image](image.png)

Figure 36

2. Navigate to Reports>Configuration.

![Image](image.png)

Figure 37
3. During scheduling, please check **Persist data in the EventVault Explorer** option.

![Figure 38](image)

4. Check column names to persist using PERSIST checkboxes beside them. Choose a suitable Retention period.
5. Proceed to the next step and click the Schedule button.
6. Wait for the scheduled time or generate a report manually.

### 6.2 Create Dashlets

1. **EventTracker 8** is required to configure the flex dashboard.
2. Open **EventTracker** in browser and logon.
3. Navigate to Dashboard>Flex.
Flex Dashboard pane is shown.

4. Click + to add a new dashboard.
Flex Dashboard configuration pane is shown.
5. Fill the fitting title and description and click the **Save** button.
6. Click to configure a new flex dashlet.
   Widget configuration pane is shown.

   ![Widget Configuration](image)

   **Figure 42**

7. Locate earlier scheduled report in **Data Source** dropdown.
8. Select **Chart Type** from the dropdown.
9. Select the extent of data to be displayed in **Duration** dropdown.
10. Select computation type in **Value Field Setting** dropdown.
11. Select evaluation duration in **As Of** dropdown.
12. Select comparable values in **X-Axis** with a suitable label.
13. Select numeric values in **Y-Axis** with a suitable label.
14. Select a comparable sequence in **Legend**.
15. Click the **Test** button to evaluate.
16. If satisfied, click the **Configure** button.
6.3 Sample Flex Dashboards

- **WIDGET TITLE**: Check Point-Configuration changes
- **DATA SOURCE**: Check Point-Configuration changes
- **CHART TYPE**: Donut
- **AXIS LABELS [X-AXIS]**: Client IP address
• **WIDGET TITLE:** Check Point-Logon failure  
**DATA SOURCE:** Check Point-Logon failure  
**CHART TYPE:** Donut  
**AXIS LABELS [X-AXIS]:** Activity

![Check Point-Logon failure chart](image)

**Figure 45**

• **WIDGET TITLE:** Check Point-Interface status changed  
**DATA SOURCE:** Check Point-Interface status changed  
**CHART TYPE:** Donut  
**AXIS LABELS [X-AXIS]:** Interface Id  
**LEGEND [SERIES]:** Interface state

![Check Point-Interface status changed chart](image)

**Figure 46**
• **WIDGET TITLE:** Check Point-Device maintenance messages  
**DATA SOURCE:** Check Point-Device maintenance messages  
**CHART TYPE:** Donut  
**AXIS LABELS [X-AXIS]:** Device messages.

![Check Point-Device Maintenance Messages](image)

Figure 47

• **WIDGET TITLE:** Check Point-DHCP server activity  
**DATA SOURCE:** Check Point-DHCP server activity  
**CHART TYPE:** Donut  
**AXIS LABELS [X-AXIS]:** Dhcp messages.

![Check Point-DHCP Server Activity](image)

Figure 48
• **WIDGET TITLE**: Check Point-Upgrade and downgrade activity  
**DATA SOURCE**: Check Point-Upgrade and downgrade activity  
**CHART TYPE**: Donut  
**AXIS LABELS [X-AXIS]**: Patch details

![Figure 49](image1.png)

• **WIDGET TITLE**: Check Point-User management activity  
**DATA SOURCE**: Check Point-User management activity  
**CHART TYPE**: Donut  
**AXIS LABELS [X-AXIS]**: Patch details

![Figure 50](image2.png)
• **WIDGET TITLE:** Check Point-Traffic allowed  
**DATA SOURCE:** Check Point-Denied Traffic  
**CHART TYPE:** Donut  
**AXIS LABELS [X-AXIS]:** Source IP address

![Check Point Firewall Allowed Traffic](image1)

*Figure 51*

• **WIDGET TITLE:** Check Point-Denied Traffic  
**DATA SOURCE:** Check Point-Denied Traffic  
**CHART TYPE:** Donut  
**AXIS LABELS [X-AXIS]:** Source IP address

![Check Point Firewall Denied Traffic](image2)

*Figure 52*