Integrate WatchGuard XTM Firewall with EventTracker

EventTracker v9.0 and above

Publication Date: February 14, 2020
Abstract

This guide provides instructions to configure WatchGuard XTM Firewall forward relevant events to EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x and later, WatchGuard XTM Firewall v12.5.

Audience

Administrators who want to monitor the WatchGuard XTM Firewall using EventTracker.
Table of Contents

1. Overview .......................................................................................................................... 3
2. Prerequisites ...................................................................................................................... 3
3. Configuring syslog forwarding to EventTracker ............................................................... 3
4. EventTracker Knowledge Pack (KP) .................................................................................. 6
   4.1 Saved Searches ............................................................................................................. 6
   4.2 Alerts ............................................................................................................................ 7
   4.3 Reports .......................................................................................................................... 7
   4.4 Dashboards ................................................................................................................... 11
5. Importing knowledge pack into EventTracker ................................................................. 15
   5.1 Categories .................................................................................................................... 16
   5.2 Alerts ............................................................................................................................ 17
   5.3 Token Templates .......................................................................................................... 18
   5.4 Flex Reports ............................................................................................................... 19
   5.5 Knowledge Objects ...................................................................................................... 21
   5.6 Dashboards ................................................................................................................... 22
6. Verifying knowledge pack in EventTracker ....................................................................... 23
   6.1 Categories .................................................................................................................... 23
   6.2 Alerts ............................................................................................................................ 24
   6.3 Token Templates .......................................................................................................... 25
   6.4 Flex Reports ............................................................................................................... 25
   6.5 Knowledge Objects ...................................................................................................... 26
   6.6 Dashboards ................................................................................................................... 26
1. Overview

WatchGuard XTM Series appliances combine firewall/VPN with powerful security services and a suite of flexible management tools.

WatchGuard XTM Firewall forwards logs to EventTracker via syslog. EventTracker WatchGuard XTM Firewall report provides information about possible attacks, suspicious network traffic, device configuration changes, user login, and user authentication activities. By using these reports, one can track which user logged in successfully and login failed with reason. With the help of these reports one can inspect the endpoints to analyze the type of attack that happens, suspicious network traffic like IP spoofing, intrusion prevention traffic detected.

Dashboards display a graphical representation about user logon activities, device configuration changes, and attack detected. by using the geo-location dashboard one can track IPs traffic by country/ ISO code.

Alerts are triggered when a user performs any of the following: configuration changes on the endpoints, user login failed, user authentication failed, etc.

2. Prerequisites

- EventTracker v9.x and later should be installed.
- Fireware OS v12.5 or later should be deployed and configured.
- Users must have device Administrator access credentials for the WatchGuard XTM and EventTracker.
- Port 514 must be opened on WatchGuard XTM.
- An exception should be added into Windows Firewall on EventTracker machine for syslog port 514.

**NOTE:** Port 514 must not be used by other services of WatchGuard XTM.

3. Configuring syslog forwarding to EventTracker

To collect events from Fireware OS, you must configure your Firebox to send events to EventTracker. You can use Policy Manager or Fireware Web UI to make the changes. In this Integration Guide, one are using Web UI.

Follow the below steps to configure syslog forwarding to EventTracker.

1. Login to Fireware Web UI.
2. Select **System** from left side pane.
3. Select **Logging** and then click the **Syslog Server** tab.
4. In the Syslog Server section, enable the **Send log messages to the syslog server at this IP address** check box.

5. In the **IP Address** text box, type the IP address of the EventTracker machine.

6. In the **Port** text box, type 514.

7. From the **Log Format** drop-down list, select “Syslog”.

8. Select both check boxes **The serial number of the device** and **The syslog header**.

9. In the Syslog Settings section, ensure each log level is assigned a facility.

10. Click **Save**.

11. Go to **Diagnostic Log** under **System**.
12. In **Diagnostic Log Level**, select **Information** from the drop-down list for each log type.
13. Click **Save**.
4. EventTracker Knowledge Pack (KP)

Once logs are received in EventTracker; Categories, Alerts, Reports, and Dashboards can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker v9.x and later to support WatchGuard XTM monitoring:

**NOTE:** The EventTracker Knowledge Pack files for WatchGuard Firewall v12.5 and earlier version can be collected from the EventTracker support (support@eventtracker.com).

### 4.1 Saved Searches

- **WatchGuard XTM: Authentication failure** - This category provides information related to user authentication failure.
- **WatchGuard XTM: Authentication success** - This category provides information related to user authentication success.
- **WatchGuard XTM: Configuration changed** - This category provides information related to a configuration change.
- **WatchGuard XTM: DHCP activity** - This category provides information related to DHCP activity.
- **WatchGuard XTM: Firewall allowed traffic** - This category provides information related to traffic allowed by the firewall.
- **WatchGuard XTM: Firewall denied traffic** - This category provides information related to traffic denied by firewall.
- **WatchGuard XTM: Interface status** - This category provides information related to change in interface status.
- **WatchGuard XTM: IPS attack detected** - This category provides information related to attacks detected by IPS.
- **WatchGuard XTM: PPOE session details** - This category provides information related to PPOE sessions.
- **WatchGuard XTM: Proxy policy allowed traffic** - This category provides information related to traffic allowed by proxy policy.
- **WatchGuard XTM: Proxy policy denied traffic** - This category provides information related to traffic denied by proxy policy.
- **WatchGuard XTM: Security services error** - This category provides information related to security services error.
- **WatchGuard XTM: VPN session details** - This category provides information related to VPN sessions.
4.2 Alerts

- **WatchGuard XTM: Attack detected**: This alert is generated when an attack is detected by the WatchGuard XTM firewall.
- **WatchGuard XTM: Authentication server unavailable**: This alert is generated when the authentication server is unavailable for authentication.
- **WatchGuard XTM: Customized certificate generation error**: This alert is generated when customized certificate generation error occurs.
- **WatchGuard XTM: Device configuration changed**: This alert is generated when a device configuration is changed by a user.
- **WatchGuard XTM: Feature expiration reminder**: This alert is generated when a feature is about to expire and so WatchGuard XTM generates a reminder event. EventTracker captures it and shows it on the Incident dashboard.
- **WatchGuard XTM: Feature key download failed**: This alert is generated when a feature key is downloaded.
- **WatchGuard XTM: Feature key expired**: This alert is generated when a feature key is expired.
- **WatchGuard XTM: Shutdown requested by system**: This alert is generated when the shutdown is requested by the system.
- **WatchGuard XTM: User authentication failed**: This alert is generated when a user tries to authenticate and it fails.
- **WatchGuard XTM: User logon failed**: This alert is generated when the user tries to login and it fails.

4.3 Reports

- **WatchGuard XTM-Device configuration change details**: This report provides information related to device configuration change when a user performs any changes in WatchGuard XTM. This report captures the changed item information in message details column and also shows the time and the firewall device configuration on which the changes have been done.
Sample Report

**WatchGuard XTM-Device configuration change details**

<table>
<thead>
<tr>
<th>Time</th>
<th>Computer</th>
<th>Message Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>07/29/2016 01:08:15 PM</td>
<td>WATCHTEST</td>
<td>Management user <a href="mailto:admin@Firebox.UB">admin@Firebox.UB</a> from 10.139.36.22 (modified</td>
</tr>
<tr>
<td>07/29/2016 01:08:29 PM</td>
<td>WATCHTEST</td>
<td>Administrative accounts were reset to the default settings</td>
</tr>
<tr>
<td>07/29/2016 01:08:37 PM</td>
<td>WATCHTEST</td>
<td>admin added feature key '33DB25CCF32949E5E'</td>
</tr>
<tr>
<td>07/29/2016 01:08:47 PM</td>
<td>WATCHTEST</td>
<td>admin removed feature key '33DB25CCF32949E5E'</td>
</tr>
<tr>
<td>07/29/2016 01:08:59 PM</td>
<td>WATCHTEST</td>
<td>Device default configuration was loaded in safe mode</td>
</tr>
<tr>
<td>07/29/2016 01:09:07 PM</td>
<td>WATCHTEST</td>
<td>Device auto restore from USB drive image initiated, reboot needed</td>
</tr>
<tr>
<td>07/29/2016 01:09:20 PM</td>
<td>WATCHTEST</td>
<td>System upgrade failed: 'LIVESECURITY' feature expired</td>
</tr>
<tr>
<td>07/29/2016 01:09:32 PM</td>
<td>WATCHTEST</td>
<td>Upload of log succeeded</td>
</tr>
<tr>
<td>07/29/2016 01:09:47 PM</td>
<td>WATCHTEST</td>
<td>Upload of log succeeded</td>
</tr>
<tr>
<td>07/29/2016 01:10:08 PM</td>
<td>WATCHTEST</td>
<td>The configuration file and feature key for the device were successfully updated after a request from admin from the Management Server at 10.139.44.58. Revision: dummy_config_rev_1. Comments: update tcp segment.</td>
</tr>
<tr>
<td>07/29/2016 01:10:17 PM</td>
<td>WATCHTEST</td>
<td>Device configuration file was successfully updated. Configuration file retrieved from the Management Server at 10.139.44.58.</td>
</tr>
<tr>
<td>07/29/2016 01:10:30 PM</td>
<td>WATCHTEST</td>
<td>During a system downgrade, the configuration rest failed</td>
</tr>
</tbody>
</table>

**Log Sample**

```
```

- **WatchGuard XTM-System management details**: This report provides information related to system management like the system is shut down, the system is restarted, the system is upgraded, the system is backed up, etc. This report has a column called message details which contains the information about what has been performed by the user or system. It also shows the time and on which firewall device it has happened.

- **WatchGuard XTM-User logon and logout success**: This report provides information related to user logons. This report captures at what time a user has logged in or logged out from a specific IP address and what IP address has been assigned to him.
Sample Report

WatchGuard XTM-User logon and logout success

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Username</th>
<th>User Type</th>
<th>Source Address</th>
<th>Status</th>
<th>Assigned Virtual Client IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>07/02/2016 06:10:11 PM</td>
<td>WATCHTEST</td>
<td><a href="mailto:root@nnvvt.com">root@nnvvt.com</a></td>
<td>SSL VPN</td>
<td>182.156.02.90</td>
<td>logged in</td>
<td>192.168.113.2</td>
</tr>
<tr>
<td>07/02/2016 06:10:20 PM</td>
<td>WATCHTEST</td>
<td><a href="mailto:mike@nnvvt.com">mike@nnvvt.com</a></td>
<td>SSL VPN</td>
<td>182.156.92.10</td>
<td>logged out</td>
<td>192.168.113.2</td>
</tr>
<tr>
<td>07/02/2016 06:10:58 PM</td>
<td>WATCHTEST</td>
<td><a href="mailto:john@nnvvt.com">john@nnvvt.com</a></td>
<td>management</td>
<td>182.156.92.18</td>
<td>logged in</td>
<td>192.168.113.2</td>
</tr>
<tr>
<td>07/02/2016 06:11:13 PM</td>
<td>WATCHTEST</td>
<td><a href="mailto:jack@nnvvt.com">jack@nnvvt.com</a></td>
<td>management</td>
<td>182.156.92.90</td>
<td>logged out</td>
<td>192.168.113.2</td>
</tr>
</tbody>
</table>

Log Sample


Jun 30 06:52:53 172.17.1.6 Jun 30 06:52:53 local-1-810 808502F579BAE local-810-Cluster (2016-06-30T10:52:53) sessiond[1588]: msg_id="3EOO-0002" SSL VPN user et_support@nnvvt.com from 182.156.92.138 logged in assigned virtual IP is 192.168.113.2

- **WatchGuard XTM-User authentication failed**: This report provides information related to the user authentication failure events. When a user tries to authenticate and it fails, it gives the reason why the authentication failed.

Sample Report

WatchGuard XTM-User authentication failure

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Username</th>
<th>User Type</th>
<th>Source Address</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>07/02/2016 06:10:11 PM</td>
<td>WATCHTEST</td>
<td><a href="mailto:root@nnvvt.com">root@nnvvt.com</a></td>
<td>SSL VPN</td>
<td>182.156.02.90</td>
<td>The user is in the wrong group</td>
</tr>
<tr>
<td>07/02/2016 06:10:29 PM</td>
<td>WATCHTEST</td>
<td><a href="mailto:mike@nnvvt.com">mike@nnvvt.com</a></td>
<td>SSL VPN</td>
<td>182.156.92.10</td>
<td>Both primary and secondary servers are unavailable</td>
</tr>
<tr>
<td>07/02/2016 06:10:58 PM</td>
<td>WATCHTEST</td>
<td><a href="mailto:john@nnvvt.com">john@nnvvt.com</a></td>
<td>management</td>
<td>182.156.92.18</td>
<td>RADIUS authentication method MSCHAP_V1 is not supported</td>
</tr>
<tr>
<td>07/02/2016 06:11:13 PM</td>
<td>WATCHTEST</td>
<td><a href="mailto:jack@nnvvt.com">jack@nnvvt.com</a></td>
<td>management</td>
<td>182.156.92.90</td>
<td>Domain not found</td>
</tr>
</tbody>
</table>

Log Sample


- **WatchGuard XTM-User authentication success**: This report provides information related to an authentication success event when a user tries to authenticate and it gets success. This report has the columns LogTime, Computer or Device name, Username, User Type and Source Address.

- **WatchGuard XTM-User login failed**: This report provides information related to user logon failure event i.e. when a user tries to login and it fails. It has the column LogTime, Computer or Device name, Username, User Type and Source Address and Assigned Virtual Client IP Address.
• **WatchGuard XTM-Attack detected**: This report provides information related to the attack detected by WatchGuard XTM. It contains the columns LogTime, Computer or Device name, Attack Type, Source Address and Target Address.

**Sample Report**

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Attack Name</th>
<th>Source Address</th>
<th>Target Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>07/23/2018 04:17:05 PM</td>
<td>WATCHTEST</td>
<td>IP4 source route</td>
<td>16.8.1.14</td>
<td></td>
</tr>
<tr>
<td>07/23/2018 04:17:21 PM</td>
<td>WATCHTEST</td>
<td>SYNF flood</td>
<td>216.3.21.4</td>
<td>10.0.1.1</td>
</tr>
<tr>
<td>07/23/2018 04:17:22 PM</td>
<td>WATCHTEST</td>
<td>ICMP flood</td>
<td>216.3.21.4</td>
<td>10.0.1.1</td>
</tr>
<tr>
<td>07/23/2018 04:17:44 PM</td>
<td>WATCHTEST</td>
<td>UDP flood</td>
<td>12.34.23.87</td>
<td>32.21.58.8</td>
</tr>
<tr>
<td>07/23/2018 04:17:56 PM</td>
<td>WATCHTEST</td>
<td>IPSec flood</td>
<td>12.34.23.67</td>
<td>32.21.56.8</td>
</tr>
<tr>
<td>07/23/2018 04:18:20 PM</td>
<td>WATCHTEST</td>
<td>RCE flood</td>
<td>12.34.23.67</td>
<td>32.21.56.8</td>
</tr>
<tr>
<td>07/23/2018 04:18:33 PM</td>
<td>WATCHTEST</td>
<td>IP scan</td>
<td>12.34.23.67</td>
<td>32.21.56.8</td>
</tr>
<tr>
<td>07/23/2018 04:18:47 PM</td>
<td>WATCHTEST</td>
<td>PORT scan</td>
<td>12.34.23.67</td>
<td>32.21.56.8</td>
</tr>
</tbody>
</table>

**Log Sample**

Feb 08 09:33:52 172.17.1.6 Feb 8 09:33:51 Crows-2-810 80850F5BE2E Crows-810-Cluster (2016-02-08T14:33:51) firewall- msg_id="3000-0150" Deny tun0 1-Trusted 820 tcp 20 62 192.168.16.79 172.16.14.34 51870 445 offset 5 A 2325226339 win 8003 signature_name="SMB Microsoft DLL Plantlying Remote Code Execution Vulnerability" signature_cat="Misc" signature_id="1130527" severity="4" msg="IPS detected" src_user="Leo@Production" (Allow SSLVPN-Users-00)

• **WatchGuard XTM-IP spoofing and blocked site traffic detected**: This report provides information related to IP spoofing and blocked site traffic detection. It has the column LogTime, Computer or Device name, Traffic Type, Source Address and Target Address.

• **WatchGuard XTM-Traffic details**: This report provides information related to inbound and outbound traffic. It has the columns LogTime, Computer or Device name, Status, In Interface Name, Out Interface Name, Source IP Address, Source Port, Destination IP Address, Destination Port, Application Behavior Name, Application Category ID, Application ID, Application Name, Category Name, Message, Policy Name.

**Sample Report**

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Status</th>
<th>In Interface Name</th>
<th>Out Interface Name</th>
<th>Source IP Address</th>
<th>Source Port</th>
<th>Destination IP Address</th>
<th>Destination Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>07/23/2018 04:43:34 PM</td>
<td>WATCHTEST</td>
<td>Allow</td>
<td>1-Trusted</td>
<td>6-External</td>
<td>192.168.30.242</td>
<td>58158</td>
<td>192.150.234.34</td>
<td>445</td>
</tr>
<tr>
<td>07/23/2018 04:42:26 PM</td>
<td>WATCHTEST</td>
<td>Allow</td>
<td>2-LAN</td>
<td>1-FPL</td>
<td>192.168.100.27</td>
<td>51994</td>
<td>22.239.26.09</td>
<td>123</td>
</tr>
</tbody>
</table>
Integrate WatchGuard XTM Firewall with EventTracker

Log Sample

<table>
<thead>
<tr>
<th>LogTime</th>
<th>In Interface Name</th>
<th>Out Interface Name</th>
<th>Source IP Address</th>
<th>Source Port</th>
<th>Destination IP Address</th>
<th>Destination Port</th>
<th>Policy Name</th>
<th>Signature Category</th>
<th>Signature ID</th>
<th>Signature Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>02/11/2020 04:24:50 PM</td>
<td>I-Trusted</td>
<td>G-External</td>
<td>192.168.90.9</td>
<td>1022</td>
<td>199.30.234.34</td>
<td>443</td>
<td>HTTP-00</td>
<td>Mac</td>
<td>1112404</td>
<td>EXPLOIT Apple QuickTime FLIC Animation File buffer overflow -1.2</td>
</tr>
</tbody>
</table>

- **WatchGuard XTM-IPS traffic detected**: This report provides information related to IPS traffic detection. It has the column LogTime, Computer or Device name, Status, Message, In Interface Name, Out Interface Name, Source IP Address, Source Port, Destination IP Address, Destination Port, Policy Name, Signature Category, Signature ID, Signature Name.

Sample Report

Log Sample

Feb 10 05:55:44 mspfirecluster Feb 10 05:55:50 MSP_M570_Member1 801102F65E96C MSP_M570_Cluster (2020-02-10T11:55:50) firewall: msg_id="3000-1510" Deny 1-ISP2 - CenturyLinkWAN - 500Mbps 2-LAN 454 tcp 20 55 66.115.169.211 204.26.117.170 55239 80 offset 8 A 3329469529 win 62977 signature_name="WEB SQL injection attempt" signature_cat="Web Attack" signature_id="1058468" severity="4" geo_src="USA" geo_dst="USA" msg="IPS detected" {vision.hga.int-00}

4.4 Dashboards

- **WatchGuard XTM Attack detected** – This dashboard will display the information on the attacks detected on endpoints.
Integrate WatchGuard XTM Firewall with EventTracker

- **WatchGuard XTM User authentication failed** – This dashboard will display the information on the user authentication failure.
• **WatchGuard XTM User logon and logout success** – This dashboard will display the information about user login success and user logout success.

![Figure 5](image1.png)

• **WatchGuard XTM User logon failure** – This dashboard will display the information about user login failures.

![Figure 6](image2.png)
• **WatchGuard XTM IPS traffic detected by geolocation** – This dashboard will display the information of IPS traffic detected by country codes.

![Figure 7](image)

• **WatchGuard XTM System management details** – This dashboard will display the information about system management details.

![Figure 8](image)
5. Importing knowledge pack into EventTracker

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

- Categories
- Alerts
- Token Template/ Parsing Rules
- Flex Reports
- Knowledge Objects
- Dashboards

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

![EventTracker Control Panel](image-url)
3. Click the Import tab.

5.1 Categories

1. Once you have opened “Export-Import Utility” via “EventTracker Control Panel”, click the Category option, and then click Browse ...
2. Navigate to the knowledge pack folder and select the file with the extension "iscat", like “Categories_WatchGuard XTM. iscat” and then click “Import”.

Figure 10

Figure 11
Integrate WatchGuard XTM Firewall with EventTracker

EventTracker displays a success message:

![Success Message](image1)

**Figure 12**

### 5.2 Alerts

1. Once you have opened “Export-Import Utility” via “EventTracker Control Panel”, click Alert option, and then click **Browse ...**.
2. Navigate to the knowledge pack folder and select the file with the extension “.isalt”, e.g. “Alerts_WatchGuard XTM.isalt” and then click “Import”.

![Import Details](image2)

**Figure 13**
Integrate WatchGuard XTM Firewall with EventTracker

EventTracker displays a success message.

Figure 14

5.3 Token Templates

For importing “Token Template”, navigate to the EventTracker manager web interface.

1. Click Parsing Rules under the Admin option in the EventTracker manager web interface.

Figure 15

2. Click the “Template” tab and then click “Import Configuration”.

Figure 16
3. Now, click “Browse” and navigate to the knowledge packs folder (type C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs” in the navigation bar) where “.ettd”, e.g. “Templates_WatchGuard XTM.ettd” file is located. Wait for a few seconds, as templates will be loaded. Once you see the templates, click desired templates and click “Import”.

![Import Screen](image)

5.4 Flex Reports

1. In the EventTracker control panel, select “Export/ Import utility” and select the “Import tab”. Click Reports option, and choose “New (*.etcrx)”: 
2. Once you have selected “New (*.etcrx)”, a new pop-up window will appear. Click “Select File” and navigate to the knowledge pack folder and select file with the extension “.etcrx”, e.g. “Reports_WatchGuard XTM.etcrx”.

3. Wait while reports are being populated in the below tables. Now, select all the relevant reports and then click Import.
EventTracker displays a success message.

5.5 Knowledge Objects

1. Click **Knowledge objects** under the **Admin** option in the EventTracker web interface.

2. Click the “import object” icon.
3. A pop-up box will appear, click “Browse” in that and navigate to the knowledge packs folder (type “C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs” in the navigation bar) with the extension “.etko”, e.g. “KO_WatchGuard XTM.etko” and then click “Upload”.

![Figure 25](image)

4. Wait while EventTracker populates all the relevant knowledge objects. Once the objects are displayed, select the required ones and click “Import”.

![Figure 26](image)

5.6 Dashboards

1. Login to the EventTracker web interface.
2. Navigate to Dashboard → My Dashboard.

![Figure 27](image)
4. Select the **Browse** and navigate to the knowledge pack folder (type “C:\Program Files (x86)\Prism Microsystems\EventTracker\Knowledge Packs” in the navigation bar) where “.etwd”, e.g. “Dashboard_WatchGuard XTM.etwd” is saved and click “Upload”.

5. Wait while EventTracker populates all the available dashboards. Now, choose “Select All” and click “Import”.

### 6. Verifying knowledge pack in EventTracker

#### 6.1 Categories

1. Login to the **EventTracker web interface**.
2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree** to view imported categories, click “**Search**” and search with the “**WatchGuard XTM**.”
You will see the below results.

![Category Tree](image)

**Figure 31**

### 6.2 Alerts

1. In the EventTracker web interface, click the Admin dropdown, and then click Alerts.
2. In the search box enter **WatchGuard XTM** and then click Search.

EventTracker displays an alert related to **WatchGuard XTM**:

![Alerts](image)

**Figure 32**
6.3 Token Templates

1. In the EventTracker web interface, click the Admin dropdown, and then click “Parsing Rules”.
2. In the “Template” tab, click on the “WatchGuard XTM” group folder to view the imported Token.

![Parsing Rules](image)

Figure 33

6.4 Flex Reports

1. In the EventTracker web interface, click the Reports menu, and then select the Report Configuration.

![Report Configuration](image)

Figure 34

2. In Reports Configuration pane, select the Defined option.
3. Click on the “WatchGuard XTM” group folder to view the imported reports.

![Report Configuration](image)

Figure 35
6.5 Knowledge Objects

1. In the EventTracker web interface, click the Admin dropdown, and then click Knowledge Objects.
2. In the Knowledge Object tree, expand the “WatchGuard XTM” group folder to view the imported Knowledge objects.

![Knowledge Objects](image)

Figure 36

6.6 Dashboards

1. In the EventTracker web interface, Click Home and select “My Dashboard”.

![Dashboard](image)

Figure 37

2. In “WatchGuard XTM” dashboard you should be now able to see something like this: