Integrate Palo Alto Firewall

EventTracker v8.x and above

Publication Date: December 26, 2017
Abstract

This guide provides instructions to configure Palo Alto Firewall to send crucial events to EventTracker Enterprise by means of syslog.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 8.x and later, and Palo Alto Appliance, PanOS version (2.0-8.1).

Audience

Palo Alto Firewall, who wish to forward its events to EventTracker Manager and monitor them using EventTracker Enterprise.
# Table of Contents

Abstract ........................................................................................................................................................................ 1  
Scope ........................................................................................................................................................................ 1  
Audience .................................................................................................................................................................. 1  
Overview ...................................................................................................................................................................... 4  
Prerequisites ................................................................................................................................................................ 4  
Enable Syslog Forwarding in Palo Alto Firewall version (2.0-7.0) ................................................................. 4  
  Defining Syslog Servers ........................................................................................................................................ 4  
    To define syslog server profile ........................................................................................................................... 4  
    To define configuration log settings .................................................................................................................. 6  
    To define system log settings ............................................................................................................................. 6  
    To define traffic log settings ............................................................................................................................... 7  
    To define threat log settings .............................................................................................................................. 9  
Enable Syslog Forwarding in Palo Alto Firewall version 8.0 ............................................................................. 11  
  Configure a Syslog server profile ....................................................................................................................... 11  
  Configure Log Forwarding ................................................................................................................................ 12  
    Assign the Log Forwarding profile to policy rules and network zones ............................................................ 12  
    Configure syslog forwarding for Traffic, Threat, and WildFire Submission logs ............................................ 13  
    Configure syslog forwarding for System, Config, HIP Match, and Correlation logs .................................... 13  
    Create a certificate to secure syslog communication over TLSv1.2 ............................................................... 13  
EventTracker Knowledge Pack ............................................................................................................................. 14  
  Categories .............................................................................................................................................................. 14  
  Alerts ...................................................................................................................................................................... 14  
  Flex Reports .......................................................................................................................................................... 15  
Import Palo Alto Firewall Knowledge Pack into EventTracker ........................................................................ 20  
  Import Category ..................................................................................................................................................... 21  
  Import Alerts .......................................................................................................................................................... 22  
  Import Knowledge Object ..................................................................................................................................... 23  
  Token Template ..................................................................................................................................................... 26  
  Import Flex Reports ............................................................................................................................................... 27
Integrate Palo Alto Firewall

Verify Palo Alto Firewall Knowledge Pack .................................................. 29
Verify Categories .......................................................................................... 29
Verify Alerts ................................................................................................. 29
Verify Knowledge Object .............................................................................. 30
Token Template ............................................................................................ 31
Verify Flex Reports ....................................................................................... 32
Create Dashboards in EventTracker ............................................................. 33
Schedule Reports .......................................................................................... 33
Create Dashlets ............................................................................................ 36
Sample Dashboards ....................................................................................... 40
Overview

Palo Alto Networks next-generation firewalls provide a flexible networking architecture that includes support for dynamic routing, switching, and VPN connectivity, enabling you to deploy the firewall into nearly any networking environment. When configuring the Ethernet ports on your firewall, you can choose from virtual wire, Layer 2, or Layer 3 interface deployments. In addition, to allow you to integrate into a variety of network segments, you can configure different types of interfaces on different ports.

The EventTracker Supports PanOS of Palo Alto firewall, it forwards the syslog messages to EventTracker manager. It enables capture of Palo Alto Networks PanOS Traffic events. The PanOS’s Firewall policy consists of specific traffic rules enabled, with traffic logging used to capture and send log data to the EventTracker. These Traffic events will be auto-identified, if enabled, and parsed into the EventTracker report tables for later review.

Prerequisites

- EventTracker 8.x and later should be installed.
- Palo Alto Appliance, PanOS version (2.0-8.1) should be installed.
- Proper access permissions to make configuration changes.
- Administrative access on the EventTracker Enterprise.
- Verify any firewalls between EventTracker Enterprise and Palo Alto firewall. If it is there make it off or add exception into that.
- Port 514 should be open in Palo Alto firewall (PanOS).

Enable Syslog Forwarding in Palo Alto Firewall version (2.0-7.0)

Defining Syslog Servers

To generate Syslog messages for system, configuration, traffic, or threat log entries, you must specify one or more Syslog servers. After you define the Syslog servers, you can use them for system and configuration log entries and for traffic and threat log.

To define syslog server profile

1. Under the Device tab, click Log Destinations > Syslog to open the Syslog Settings page.
2. Click **New** to open the **New Syslog Setting** page.
   - Specify the following information.

   a. **Name** - Enter a name for the Syslog server (up to 31 characters). The name is case-sensitive and must be unique. Use only letters, numbers, spaces, hyphens, and underscores.

   b. **Server** - Enter the IP address of the Syslog server i.e EventTracker Enterprise.

   c. **Port** - Enter the port number of the Syslog server (the standard port is 514).

   d. **Facility** - Choose a level from the drop-down list.
3. Click **OK** to submit the new trap destination.
4. You may activate your changes immediately or save them for future activation.

**To define configuration log settings**

1. Under the **Device** tab, click **Log Settings > Config** to open the **Config Log Settings** page.
2. Click **Edit** to change the log settings.
3. In **Syslog** field, select the syslog server profile that was created in the above step for the desired log-severity.
4. In **Syslog** field, select the syslog server profile that was created in the above step for the desired log-severity.
5. Click **OK** to change the log settings, or click **Cancel** to discard your changes.

![Figure 3](image)

6. You may activate your changes immediately or save them for future activation.

**To define system log settings**

1. Under the **Device** tab, click **Log Settings > System** to open the **System Log Settings** page.
2. Click **Edit** to change the log settings.
3. In **Syslog** field, select the syslog server profile that was created in the above step for the desired log-severity.
4. Click **OK** to change the log settings, or click **Cancel** to discard your changes.
5. You may activate your changes immediately or save them for future activation.

**To define traffic log settings**

1. Go to **Objects > Log forwarding**, click **Add** to create a new profile.

2. Select the syslog server profile that was created above in **Traffic Settings>Syslog** for forwarding traffic logs to the configured server.
3. Under the **Policies** tab, click **Security** to open the **Security Rules** page.

4. To view just the rules for specific zones, select a zone from the Source Zone and/or Destination Zone drop-down lists, and click **Filter by Zone**.

5. Click **Options**; specify any combination of the following options:
   a. Ensure **Send Traffic Log** at session end is enabled for action is set to **allow** (enabled by default).
   b. Ensure **Send Traffic Log** at session start for action is set to **deny**.
6. In **Actions** tab, select the above created syslog server profile in **Log Forwarding** drop-down menu.

![Figure 8](image-url)

7. Click **OK** to save changes.

**To define threat log settings**

1. Go to **Objects > Log forwarding** click **Add** to create a new profile.
2. Select the syslog server profile that was created above in Threat Settings>Syslog for forwarding threat logs to the configured server.

4. To view just the rules for specific zones, select a zone from the Source Zone and/or Destination Zone drop-down lists, and click Filter by Zone.
5. To view just the rules for specific zones, select a zone from the Source Zone and/or Destination Zone drop-down lists, and click Filter by Zone.
6. Select the rule for which the log forwarding needs to be applied.
7. Click **Options** to apply the security profiles to the selected rule.
8. In **Actions** tab, select the above created syslog server profile in **Log Forwarding** drop-down menu.

![Figure 12](image)

9. Click **OK** to save changes.

**NOTE:** This document does not describe all features and functionality within Palo Alto Networks (PanOS) regarding configuration and Syslog. For more information on these areas, see Palo Alto Networks (PanOS) Product Documentation.

### Enable Syslog Forwarding in Palo Alto Firewall version 8.0

**Configure a Syslog server profile**

1. Select **Device** -> **Server Profiles** -> **Syslog**.
2. Click **Add** and enter a **Name** for the profile.
3. If the firewall has more than one virtual system (vsys), select the **Location** (vsys or **Shared**) where this profile is available.
4. For each syslog server, click **Add** and enter the information that the firewall requires to connect to it:
   - **Name**—Unique name for the server profile.
   - **Syslog Server**—Enter the **EventTracker Manager** IP Address.
   - **Transport**—Select UDP as the protocol for communicating with the syslog server.
Integrate Palo Alto Firewall

- **Port**—The port number on which to send syslog messages (default is UDP on port 514); you must use the same port number on the firewall and the syslog server.
- **Format**—Select the syslog message format to use: **BSD** (the default) or **IETF**. Traditionally, **BSD** format is over **UDP** and **IETF** format is over **TCP** or **SSL/TLS**.
- **Facility**—Select a syslog standard value (default is **LOG_USER**) to calculate the priority (PRI) field in your syslog server implementation. Select the value that maps to how you use the PRI field to manage your syslog messages.

5. Click **OK** to save the server profile.

Configure Log Forwarding

The profile defines the destinations for Traffic, Threat, WildFire Submission, URL Filtering, Data Filtering, Tunnel and Authentication logs.

1. Select **Objects** -> **Log Forwarding** and **Add** a profile.
2. Enter a **Name** to identify the profile

**Note:** If you want the firewall to automatically assign the profile to new security rules and zones, enter default. If you don’t want a default profile, or you want to override an existing default profile, enter a Name that will help you identify the profile when assigning it to security rules and zones.

3. **Add** one or more match list profiles.
   a) Enter a **Name** to identify the profile.
   b) Select the **Log Type**.
   c) In the **Filter** drop-down, select **Filter Builder**. Specify the following and then **Add** each query:
      - **Connector** logic (and/or)
      - **Log Attribute**
      - **Operator** to define inclusion or exclusion logic
      - **Attribute Value** for the query to match
   d) Select Panorama if you want to forward logs to Log Collectors or the Panorama management server.
   e) For each type of external service that you use for monitoring (SNMP, Email, Syslog, and HTTP), **Add** one or more server profiles.
4. Click **OK** to save the Log Forwarding profile.

Assign the Log Forwarding profile to policy rules and network zones.

Perform the following steps for each rule that you want to trigger log forwarding:

1. Select **Policies** -> **Security** and **edit** the rule.
2. Select **Actions** and select the **Log Forwarding profile** you created.
3. Set the **Profile Type** to **Profiles** or **Group**, and then select the **security profiles** or **Group Profile** required to trigger log generation and forwarding for:
Integrate Palo Alto Firewall

- **Threat logs**—Traffic must match any security profile assigned to the rule.
- **WildFire Submission logs**—Traffic must match a WildFire Analysis profile assigned to the rule.

4. For Traffic logs, select **Log At Session Start** and/or **Log At Session End**.
5. Click **OK** to save the rule.

### Configure syslog forwarding for Traffic, Threat, and WildFire Submission logs

1. Select **Objects** -> **Log Forwarding**, click **Add**, and enter a **Name** to identify the profile.
2. For each log type and each severity level or WildFire verdict, select the **Syslog** server profile and click **OK**.

### Configure syslog forwarding for System, Config, HIP Match, and Correlation logs

1. Select **Device** -> **Log Settings**.
2. For System and Correlation logs, click each **Severity level**, select the **Syslog** server profile, and click **OK**.
3. For Config, HIP Match, and Correlation logs, edit the section, select the **Syslog** server profile, and click **OK**.

### Create a certificate to secure syslog communication over TLSv1.2

Required only, if the syslog server uses client authentication. The syslog server uses the certificate to verify that the firewall is authorized to communicate with the syslog server.

Ensure the following conditions are met:

- The private key must be available on the sending firewall; the keys can’t reside on a Hardware Security Module (HSM).
- The subject and the issuer for the certificate must not be identical.
- The syslog server and the sending firewall must have certificates that the same trusted certificate authority (CA) signed. Alternatively, you can generate a self-signed certificate on the firewall, export the certificate from the firewall, and import it in to the syslog server.

1. Select **Device** -> **Certificate Management** -> **Certificates** -> **Device Certificates** and click **Generate**.
2. Enter a **Name** for the certificate.
3. In the **Common Name** field, enter the IP address of the firewall sending logs to the syslog server.
4. In **Signed by**, select the trusted CA or the self-signed CA that the syslog server and the sending firewall both trust.
5. The certificate can’t be a **Certificate Authority** nor an **External Authority** (certificate signing request [CSR]).
6. Click **Generate**. The firewall generates the certificate and key pair.
7. Click the certificate **Name** to edit it, select the **Certificate for Secure Syslog** check box, and click **OK**.
EventTracker Knowledge Pack

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

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

Categories

- **Palo Alto Firewall-Allowed traffic**: This category based report provides information related to all the traffic that is allowed by the Palo Alto Firewall.
- **Palo Alto Firewall-Configuration success and failure**: This category based report provides information related to all the configuration success and failure.
- **Palo Alto Firewall-Denied traffic**: This category based report provides information related to all the traffic that is denied by the Palo Alto Firewall.
- **Palo Alto Firewall-Logon failures**: This category based report provides information related to all the logon failures that is attempted.
- **Palo Alto Firewall-Logon success**: This category based report provides information related to all the logon success that is done.
- **Palo Alto Firewall-Url filtering**: This category based report provides information related to all url filtering that is done in the traffic by the Palo Alto Firewall.
- **Palo Alto Firewall-Virus detected**: This category based report provides information related to all the virus that is detected in the traffic by the Palo Alto Firewall.
- **Palo Alto Firewall-Vpn activities**: This category based report provides information related to all the vpn activities that are done.
- **Palo Alto Firewall-VPN configuration changes**: This category based report provides information related to all the vpn configuration changes that are done.
- **Palo Alto Firewall-VPN login and logout activity**: This category based report provides information related to all the vpn login and logout activity that is done in Palo Alto Firewall.
- **Palo Alto Firewall-VPN login failures**: This category based report provides information related to all the vpn login failures that is attempted.
- **Palo Alto Firewall-Vulnerability detected**: This category based report provides information related to all the vulnerability that is detected in the traffic by the Palo Alto Firewall.

Alerts

- **Palo Alto Firewall: Configuration success and failure**: This alert is generated when any configuration success or failure is done in the Palo Alto Firewall.
- **Palo Alto Firewall: Logon failure**: This alert is generated when any logon failure is attempted in the Palo Alto Firewall.
- **Palo Alto Firewall: Virus detected**: This alert is generated when any virus is detected in the traffic by the Palo Alto Firewall.
- **Palo Alto Firewall: VPN configuration changes**: This alert is generated when any vpn configuration changes is done in the Palo Alto Firewall.
- **Palo Alto Firewall: VPN login failures**: This alert is generated when any vpn login failures is attempted in the Palo Alto Firewall.
- **Palo Alto Firewall: Vulnerability detected**: This alert is generated when any vulnerability is detected in the traffic by the Palo Alto Firewall.

**Flex Reports**

- **Palo Alto Firewall-Traffic details** - This report provides information related to traffic flow which includes session id, source address, source port, source location, destination address, destination port, destination location, protocol type, total bytes, bytes sent, bytes received, total packets, packets sent and packets received.

![Log Table](image)

**Logs Considered:**

![Log Examples](image)
- **Palo Alto Firewall - Threat details** - This report provides information related to threat detection which includes threat id, protocol type, action taken, source address, source port, source location, destination address, destination port and destination location.

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Source Zone</th>
<th>Destination Zone</th>
<th>Source Address</th>
<th>Destination Address</th>
<th>Source Path</th>
<th>Destination Path</th>
<th>URL/FileName</th>
<th>Threat Category</th>
<th>Threat Type</th>
<th>Severity</th>
<th>Action</th>
<th>Source Location</th>
<th>Destination Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/05/2017 06:39:49 PM</td>
<td>PALOALTO 18.22.1.3</td>
<td>164.21.59.14</td>
<td>60</td>
<td>Internal</td>
<td>External</td>
<td>eth0</td>
<td>eth0</td>
<td>Internal</td>
<td>External</td>
<td>eth0</td>
<td>eth0</td>
<td>web-browsing</td>
<td>Traffic Block</td>
<td>Block</td>
<td>Medium</td>
<td>10.0.0.0</td>
<td>19.255.255.255</td>
</tr>
<tr>
<td>12/05/2017 06:30:49 PM</td>
<td>PALOALTO 77.28.86.1</td>
<td>223.19.48.23</td>
<td>109</td>
<td>Internal</td>
<td>External</td>
<td>eth0</td>
<td>eth0</td>
<td>Internal</td>
<td>External</td>
<td>eth0</td>
<td>eth0</td>
<td>web-browsing</td>
<td>Traffic Block</td>
<td>Block</td>
<td>Medium</td>
<td>19.8.0.0</td>
<td>10.255.255.255</td>
</tr>
<tr>
<td>12/05/2017 06:30:49 PM</td>
<td>PALOALTO 110.29.49.33</td>
<td>196.1.160.12</td>
<td>110</td>
<td>Internal</td>
<td>External</td>
<td>eth0</td>
<td>eth0</td>
<td>Internal</td>
<td>External</td>
<td>eth0</td>
<td>eth0</td>
<td>web-browsing</td>
<td>Traffic Block</td>
<td>Block</td>
<td>Medium</td>
<td>19.8.0.0</td>
<td>10.255.255.255</td>
</tr>
<tr>
<td>12/05/2017 06:30:49 PM</td>
<td>PALOALTO 333.19.94.35</td>
<td>127.1.10.13</td>
<td>99</td>
<td>Internal</td>
<td>External</td>
<td>eth0</td>
<td>eth0</td>
<td>Internal</td>
<td>External</td>
<td>eth0</td>
<td>eth0</td>
<td>web-browsing</td>
<td>Traffic Block</td>
<td>Block</td>
<td>Medium</td>
<td>10.0.0.0</td>
<td>19.255.255.255</td>
</tr>
<tr>
<td>12/05/2017 06:30:49 PM</td>
<td>PALOALTO 75.63.12.1</td>
<td>11.13.53.14</td>
<td>77</td>
<td>Internal</td>
<td>External</td>
<td>eth0</td>
<td>eth0</td>
<td>Internal</td>
<td>External</td>
<td>eth0</td>
<td>eth0</td>
<td>web-browsing</td>
<td>Traffic Block</td>
<td>Block</td>
<td>Medium</td>
<td>19.8.0.0</td>
<td>10.255.255.255</td>
</tr>
</tbody>
</table>

**Logs Considered:**

- **Palo Alto Firewall - Configuration success or failure** - This provides information related to changes happen in configuration of Palo Alto firewall which includes user, source IP, console type, and configuration path.
Integrate Palo Alto Firewall

Logs Considered:

- **Palo Alto Firewall-Logon failure**- This report provides information related to user logon failure in Palo Alto firewall which includes source IP, user and reason.
### Logs Considered:

- **Palo Alto Firewall - Logon success** - This report provides information related to user login success in Palo Alto firewall which includes source IP and user.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>UserName</th>
<th>Client IP Address</th>
<th>Module</th>
<th>Severity</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/06/2017 12:23:14 PM</td>
<td>PALOALTO</td>
<td>John</td>
<td>172.153.2.94</td>
<td>general</td>
<td>informational</td>
<td>Authentication profile not found for the user</td>
</tr>
<tr>
<td>12/06/2017 03:56:11 PM</td>
<td>PALOALTO</td>
<td>ubnt</td>
<td>127.0.0.125</td>
<td>general</td>
<td>medium</td>
<td>Authentication profile not found for the user</td>
</tr>
<tr>
<td>12/06/2017 03:56:11 PM</td>
<td>PALOALTO</td>
<td>root</td>
<td>201.178.191.192</td>
<td>general</td>
<td>informational</td>
<td>Authentication profile not found for the user</td>
</tr>
</tbody>
</table>
Integrate Palo Alto Firewall

Logs Considered:

<table>
<thead>
<tr>
<th>Time</th>
<th>Computer</th>
<th>User Name</th>
<th>Source IP Address</th>
<th>Status</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/07/2015 02:20:43 PM</td>
<td>Palo Alto</td>
<td>gilbert</td>
<td>108.185.246.31</td>
<td>succeeded</td>
<td></td>
</tr>
<tr>
<td>10/07/2015 02:20:43 PM</td>
<td>Palo Alto</td>
<td>fiona</td>
<td>108.185.246.31</td>
<td>succeeded</td>
<td>client logout</td>
</tr>
</tbody>
</table>

- **Palo Alto Firewall-VPN login and logout activity** - This report provides information related to VPN user login and logout activity which include user name, source IP, status and reason.

- **Palo Alto Firewall-VPN login failures** - This report provides information related to vpn logon failure in Palo Alto firewall which includes source IP, user and reason.
Logs Considered:

- **Palo Alto Firewall-VPN configuration changes**: This report provides information related to vpn configuration changes that is done in Palo Alto firewall which includes user, source IP, console type, and configuration path.

![Log Time Table]

Logs Considered:

![Log Time Table]

**Import Palo Alto Firewall Knowledge Pack into EventTracker**

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

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

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

• Categories
• Knowledge Objects
• Alerts
• Token Templates
• Flex Reports

1. Launch **EventTracker Control Panel**.

2. Double click **Export Import Utility**, and then click the **Import** tab.

![Figure 13](image)

**Import Category**

1. Click **Category** option, and then click the browse button.
2. Locate **Palo Alto_Categories.iscat** file, and then click the **Open** button.

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

4. EventTracker displays success message.

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

### Import Alerts

1. Click **Alert** option, and then click the **browse** button.
2. Locate **Palo Alto Alerts.isalt** file, and then click the **Open** button.

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

4. EventTracker displays success message.

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

**Import 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.

4. Locate Palo Alto_Knowledge objects.eto file, and then click the UPLOAD button.
5. Now select the check box and then click on ‘OVERWRITE’ option. EventTracker displays success message.

6. Click on OK button.
Token Template

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

2. Select **Template** tab, and then click on **‘Import’** option.

3. Click on **Browse** button.

   ![Figure 22](image)

4. Locate **Palo Alto Templates.ettd** file, and then click the **Open** button.

   ![Figure 23](image)

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

   ![Figure 24](image)
6. Click on OK button.

**Import Flex Reports**

1. Click Reports option, and then click the ‘browse’ button.
2. Locate applicable Palo Alto Reports.etcrx file, and then click the Open button.

![Import Flex Reports](image)

**Figure 25**

3. To import scheduled reports, click the Import button.
4. EventTracker displays success message.

Figure 27

5. Click OK, and then click the Close button.
Verify Palo Alto Firewall Knowledge Pack

Verify Categories

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Category.
3. In Category Tree to view imported categories, scroll down and expand ‘Palo Alto Firewall’ group folder to view the imported categories.

![Category Management](image)

Figure 28

Verify Alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Alerts.
3. In the Search box, type ‘Palo Alto Firewall’, and then click the Go button.

Alert Management page will display all the imported alerts.
4. To activate the imported alerts, select the respective checkbox in the **Active** column.

   EventTracker displays message box.

   ![Message Box]

   **Figure 30**

5. Click **OK**, and then click the **Activate Now** button.

**NOTE:** Please specify appropriate **systems** in **alert configuration** for better performance.

**Verify Knowledge Object**

1. Click the **Admin** menu, and then click **Knowledge Objects**
2. Scroll down and select **Palo Alto Firewall** in **Objects** pane.

   Imported Palo Alto Firewall details are shown.
Token Template

1. Logon to EventTracker Enterprise web interface.
2. Click the Admin menu, and then click Parsing Rules and click Template.
3. Click on Palo Alto Firewall group option.
Verify Flex Reports

1. Logon to EventTracker Enterprise.
2. Click the Reports menu, and then Configuration.
4. In Report Groups Tree to view imported Scheduled Reports, scroll down and click Palo Alto Firewall group folder.

Scheduled Reports are displayed in the Reports configuration pane.
NOTE: Please specify appropriate systems in report wizard for better performance.

Create Dashboards in EventTracker

Schedule Reports

1. Open EventTracker in browser and logon.
2. Navigate to Reports>Configuration.

3. Select Palo Alto Firewall in report groups. Check defined dialog box.

4. Click on ‘schedule’ to plan a report for later execution.
5. Choose appropriate time for report execution and in Step 8 check **Persist data in Eventvault explorer** box.
6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.

7. Proceed to next step and click **Schedule** button.

8. Wait for scheduled time or generate report manually.

### Create Dashlets

1. **EventTracker 8** is required to configure 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 fitting title and description and click **Save** button.
6. Click 🔄 to configure a new flex dashlet.
   Widget configuration pane is shown.

![Widget Configuration](image)

7. Locate earlier scheduled report in **Data Source** dropdown.
8. Select **Chart Type** from dropdown.
9. Select 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 suitable label.
13. Select numeric values in **Y Axis** with suitable label.
14. Select comparable sequence in **Legend**.
15. Click **Test** button to evaluate.
   Evaluated chart is shown.
16. If satisfied, Click **Configure** button.

17. Click ‘customize’ 🛠️ to locate and choose created dashlet.

18. Click ✖️ to add dashlet to earlier created dashboard.
Sample Dashboards

- REPORT: Palo Alto Firewall-Traffic details
  WIDGET TITLE: Palo Alto Firewall-Traffic details
  CHART TYPE: Pie
  AXIS LABELS [X-AXIS]: Source IP Address
  LEGEND [SERIES]: Action Taken
Integrate Palo Alto Firewall

- REPORT: Palo Alto Firewall-Threat details
- WIDGET TITLE: Palo Alto Firewall-Threat details
- CHART TYPE: Donut
- AXIS LABELS [X-AXIS]: Url/FileName
- LEGEND [SERIES]: Threat type
- **REPORT: Palo Alto Firewall- Configuration success or failure**
  WIDGET TITLE: Palo Alto Firewall- Configuration success or failure
  CHART TYPE: Donut
  AXIS LABELS [X-AXIS]: Status
  LEGEND [SERIES]: User Name

- **REPORT: Palo Alto Firewall-Logon failure**
  WIDGET TITLE: Palo Alto Firewall-Logon failure
  CHART TYPE: Pie
  AXIS LABELS [X-AXIS]: Source IP Address
  LEGEND [SERIES]: User Name
- REPORT: Palo Alto Firewall-Logon success
  WIDGET TITLE: Palo Alto Firewall-Logon success
  CHART TYPE: Pie
  AXIS LABELS [X-AXIS]: Source IP Address
  LEGEND [SERIES]: User Name
- REPORT: Palo Alto Firewall-VPN login failures
  WIDGET TITLE: Palo Alto Firewall-VPN login failures
  CHART TYPE: Stacked Column
  AXIS LABELS [X-AXIS]: User Name
  LEGEND [SERIES]: Reason

EventTracker
Actionable Security Intelligence
• REPORT: Palo Alto Firewall-VPN configuration changes
  WIDGET TITLE: Palo Alto Firewall-VPN configuration changes
  CHART TYPE: Pie
  AXIS LABELS [X-AXIS]: Status
  LEGEND [SERIES]: User Name