Integrate FortiGate Firewall
Abstract
This guide provides instructions to configure FortiGate Firewall to send crucial events to EventTracker Enterprise by means of syslog.

Scope
The configurations detailed in this guide are consistent with EventTracker version 7.X and later, and FortiGate Firewall with FortiOS version 4.0/5.0 or later.

Audience
FortiGate Firewall users, who wish to forward it’s events to EventTracker Manager and monitor them using EventTracker.

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

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

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

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

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

© 2017 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
# Table of Contents

Abstract ................................................................................................................................. 1
Scope ........................................................................................................................................ 1
Audience .................................................................................................................................. 1
Overview .................................................................................................................................. 3
Prerequisites ............................................................................................................................. 3
Enable Syslog Forwarding in FortiOS V4.0 ........................................................................... 3
Enable Syslog Forwarding in FortiOS V5.0 ........................................................................... 4
Import FortiGate Firewall Knowledge Pack .......................................................................... 5
  Import Categories .................................................................................................................... 6
  Import Alerts .......................................................................................................................... 7
  Import Flex Reports ............................................................................................................... 8
  Import Knowledge Object ..................................................................................................... 9
Verify FortiGate Firewall Knowledge Pack ........................................................................... 11
  Verify Categories .................................................................................................................. 11
  Verify Alerts .......................................................................................................................... 11
  Verify Flex Reports ............................................................................................................... 12
  Verify Knowledge Object ..................................................................................................... 13
EventTracker Knowledge Pack (KP) ....................................................................................... 14
  Categories ............................................................................................................................ 14
  Alerts ..................................................................................................................................... 21
  Reports ................................................................................................................................. 21
  Knowledge Objects .............................................................................................................. 22
Create Dashboards in EventTracker ...................................................................................... 23
  Schedule Reports .................................................................................................................. 23
Create Dashlets ...................................................................................................................... 25
Sample Dashboards ............................................................................................................... 29
Sample Reports ...................................................................................................................... 31
Overview

FortiGate Firewall is one of the fastest firewall providing protection in various areas with other key security features such as anti-virus, intrusion prevention system (IPS), web filtering, anti-spam and traffic shaping to deliver multi-layered security for the IT environment.

EventTracker collects and analyses firewall events and enlightens an administrator about security violations, user behavior, and traffic anomalies.

Prerequisites

- EventTracker should be installed.
- FortiGate Firewall with FortiOS V4.0/V5.0 should be installed.

Enable Syslog Forwarding in FortiOS V4.0

Syslog is a standard for forwarding log messages in an IP network. Syslog captures log information provided by network devices.

1. To send logs to syslog server, click Log & Report, click Log Config, and then click Log Setting.
2. In the Logging and Archiving section, select Syslog option.

![Figure 1](image-url)
After you select the check box, the **Syslog** options appear.

3. Enter the appropriate information for the following:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP/FDQN</td>
<td>Enter the domain name or IP address of the syslog server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter port number for communication with the syslog server, usually port 514.</td>
</tr>
<tr>
<td>Minimum log level</td>
<td>Select a log level the FortiGate unit will log all messages at and above that logging severity level.</td>
</tr>
<tr>
<td>Facility</td>
<td>Facility indicates to the syslog server the source of a log message. By default, the FortiGate reports facility as local7. You can change the Facility if you want to distinguish log messages from different FortiGate units.</td>
</tr>
<tr>
<td>Enable CSV Format</td>
<td>Select to have logs formatted in CSV format. When you enable CSV format, the FortiGate unit produces the log in Comma Separated Value (CSV) format. If you do not enable CSV format, the FortiGate unit produces plain text files.</td>
</tr>
</tbody>
</table>

4. Select the **Apply** button.

**Enable Syslog Forwarding in FortiOS V5.0**

Use this command to configure log settings for logging to a remote syslog server (available only in the CLI). You can configure the FortiGate unit to send logs to a remote computer running a syslog server. Using the CLI, you can send logs to up to three different syslog servers. Configure additional syslog servers using syslogd2 and syslogd3 commands.

**Syntax:**

```
Config log {syslogd | syslogd2 | syslogd3} setting
```

- Enter `enable` to enable logging to a remote syslog server.
  
  Example: `set status enable`

- Enter `enable` to enable the FortiGate unit to produce the log in Comma Separated Value (CSV) format. If you do not enable CSV format the FortiGate unit produces plain text files.
  
  Example: `set csv enable`

- Enter the facility type. Facility identifies the source of the log message to syslog.
• set facility {alert | audit | auth | authpriv | clock | cron | daemon | ftp | kernel | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 | lpr | mail | news | ntp | syslog | user | uucp}
  Example: set facility local3
• Enter the port number for communication with the syslog server.
  Example: set port 514
• Enable reliable delivery of syslog messages to the syslog server.
  Example: set reliable enable
• Enter the IP address of the syslog server that stores the logs.
  Example: set server 172.168.22.54
• Enter source IP address for syslogd, syslog2 and syslog3.
  Example: set source-ip 172.168.22.50

Import FortiGate Firewall Knowledge Pack

1. Launch EventTracker Control Panel.
2. Double click ExportImport Utility, and then click the Import tab.

Import Category/Alert as given below.
Import Categories

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

   ![Figure 3](image3.png)

2. Locate **FortiGate Firewall.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.
   EventTracker displays success message.

   ![Figure 4](image4.png)

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

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

2. Locate **FortiGate Firewall.isalt** file, and then click the **Open** button.

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

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

1. Click **Reports** option, and then click the ‘**browse**’ button.
2. Locate applicable **FortiGate Firewall.issch** file, and then click the **Open** button.

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

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

1. Click the Admin menu, and then click Knowledge Objects.
2. Click on ‘Import’ option.

3. In IMPORT pane click on Browse button.

4. Locate FortiGate.etko 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.
Verify FortiGate Firewall Knowledge Pack

Verify Categories

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Categories.
3. To view the imported categories, in the Category Tree, expand FortiGate group folder.

![Category Management](image)

Figure 13

Verify Alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Alerts.
3. In the Search box, type ‘FortiGate’, 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.

   ![Successfully saved configuration](image)

   **Figure 15**

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

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

---

**Verify Flex Reports**

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports** menu, and then **Configuration**.
3. Select **Defined** in report type.
4. In **Report Groups Tree** to view imported Scheduled Reports, scroll down and click **FortiGate Firewall** group folder.
Scheduled Reports are displayed in the Reports configuration pane.

**NOTE**: Please specify appropriate systems in report wizard for better performance.

**Verify Knowledge Object**

1. Click the Admin menu, and then click Knowledge Objects
2. Scroll down and select FortiGate in Objects pane.
   Imported FortiGate object details are shown.
EventTracker Knowledge Pack (KP)

EventTracker has separate KP items for FortiOS 4.0 and 5.0. Please check firmware version of our FortiGate device before using the following.

Categories

- **Event**: The event log records administration management as well as FortiGate system activity, such as when a configuration has changed, admin login, or high availability (HA) events occur. Event logs are an important log file to record because they record FortiGate system activity, which provides valuable information about how your FortiGate unit is performing.

Events which can be monitored using EventTracker:

- **FortiGate Admin login failed**: This category based report provides information related to admin login failed.
- **FortiGate Admin account locked**: This category based report provides information related to admin account locked.
- **FortiGate Admin account timed out**: This category based report provides information related to admin login timeout.
- **FortiGate Admin login success**: This category based report provides information related to admin login success.
- **FortiGate CPU usage is high**: This category based report provides information related to when CPU usage goes high.
- **FortiGate HA group deleted**: This category based report provides information related to HA group deleted.
- **FortiGate IPsec ESP transform success**: This category based report provides information related to IPsec ESP transform success.
- **FortiGate IPsec SA delete**: This category based report provides information when IPsec SA is deleted.
- **FortiGate IPsec SA install**: This category based report provides information related to IPsec SA installation.
- **FortiGate L2TP client connection finished**: This category based report provides information when L2TP (Layer Two Tunneling Protocol) client connection is finished.
- **FortiGate L2TP settings changed**: This category based report provides information when L2TP settings change.
- **FortiGate MAC address added**: This category based report provides information when MAC (Media Access Control) address is added to neighbor table successfully.
- **FortiGate MAC address deleted**: This category based report provides information when MAC address is deleted from neighbor table successfully.
- **FortiGate Performance statistics**: This category based report provides information related to performance statistics.
- **FortiGate PPPD authentication failed**: This category based report provides information when PPPD (Point-to-Point Protocol daemon) authentication is failed.
- **FortiGate PPTP maximum connection reached**: This category based report provides information related to maximum number of PPTP (Point-to-Point Tunneling Protocol) connections.
- **FortiGate Negotiate IPSec phase 1 error**: This category based report provides information related to negotiate IPSec phase 1 error.
- **FortiGate Negotiate IPsec phase 2 error**: This category based report provides information related to negotiate IPsec phase 2 error.
- **FortiGate SSL alerts**: This category based report provides information related to SSL (Secure Socket Layer) alerts.
- **FortiGate SSL certification**: This category based report provides information related to new SSL certification verification success.
- **FortiGate SSL new connection**: This category based report provides information related to SSL new connection.
• **FortiGate SSL exit failed**: This category based report provides information related to SSL exit failed.

• **FortiGate SSL VPN user login failed**: This category based report provides information related to SSL VPN user failed to log in.

• **FortiGate SSL VPN user login success**: This category based report provides information related to SSL VPN user succeeded to log in.

• **FortiGate SSL system busy**: This category based report provides information when SSL system is busy.

• **FortiGate SSL timeout**: This category based report provides information when SSL web application is timed-out.

• **FortiGate SSL tunnel error**: This category based report provides information when SSL tunnel error occurs.

• **FortiGate SSL tunnel established**: This category based report provides information when SSL tunnel is established.

• **FortiGate SSL tunnel shutdown**: This category based report provides information when SSL tunnel shuts down.

• **FortiGate SSL-VPN session discarded**: This category based report provides information when SSL-VPN web access session is discarded because of inactivity.

• **FortiGate SSL web app activated**: This category based report provides information when SSL web application is activated.

• **FortiGate SSL web app closed**: This category based report provides information when SSL web application gets closed.

• **FortiGate SSL web app blocked**: This category based report provides information when SSL web application is blocked.

• **FortiGate Virtual cluster deleted**: This category based report provides information when Virtual cluster is deleted.

• **FortiGate Virtual cluster member dead**: This category based report provides information when Virtual cluster detected member is dead.

• **FortiGate Web proxy error**: This category based report provides information when web proxy forwards server error message.

• **VoIP**: VoIP (Voice over Internet Protocol) activities that include SIP (Session Initiation Protocol) and SCCP (Signalling Connection Control Part) protocols.

Events which can be monitored using EventTracker:

• **FortiGate SCCP call end**: This category based report provides information when SCCP call is ended.

• **FortiGate SCCP call failed**: This category based report provides information when SCCP call is failed.
- **FortiGate SCCP call info**: This category based report provides information related to SCCP call information.
- **FortiGate SCCP call timeout**: This category based report provides information when SCCP call is timeout.
- **FortiGate SCCP register**: This category based report provides information related to SCCP register.
- **FortiGate SCCP unregister**: This category based report provides information when SCCP is unregistered.
- **FortiGate SIP authentication required**: This category based report provides information related to authentication required for SIP.
- **FortiGate SIP blocked**: This category based report provides information when SIP is blocked.
- **FortiGate SIP failed**: This category based report provides information when SIP is failed.
- **FortiGate SIP timeout**: This category based report provides information related to SIP timeout.

- **Webfilter**: Web Filter logs are an effective tool to help you determine if you need to update your web filtering settings within a web filter profile due to unforeseen threats or network congestion.

Events which can be monitored using EventTracker:

- **FortiGate Webfilter category block**: This category based report provides information related to FortiGuard webfilter category blocked.
- **FortiGate ActiveX script removed**: This category based report provides information related to removal of web script filter ActiveX.
- **FortiGate Web script filter**: This category based report provides information related to removal of web script filter applet.
- **FortiGate Webfilter category allow**: This category based report provides information related to FortiGuard webfilter category allowed.
- **FortiGate Webfilter command blocked**: This category based report provides information related to webfilter command blocked.
- **FortiGate Content type blocked**: This category based report provides information related to HTTP header content type blocked.
- **FortiGate Daily quota status**: This category based report provides information related to daily FortiGuard quota status.
- **FortiGate URL filter block**: This category based report provides information related to URL filter blocked.
- **FortiGate Webfilter error**: This category based report provides information related to FortiGuard webfilter error occurred.

- **IPS**: IPS logs, also referred to as attack logs, record attacks that occurred against your network. Attack logs contain detailed information about whether the FortiGate unit protected the network using anomaly-based defense settings or signature-based defense settings, as well as what the attack was.
Integrate FortiGate Firewall

Events which can be monitored using EventTracker

- **FortiGate Anomaly attack detected**: This category based report provides information related to anomaly attack detected (TCP - Transmission Control Protocol / UDP - User Datagram Protocol, ICMP - Internet Control Message Protocol, others).
- **FortiGate Anomaly attack dropped**: This category based report provides information related to anomaly attack dropped (TCP/UDP, ICMP, others).
- **FortiGate Anomaly attack reset**: This category based report provides information related to anomaly attack reset (TCP/UDP, ICMP, others).
- **FortiGate Signature attack detected**: This category based report provides information related to signature attack detected (TCP/UDP, ICMP, others).
- **FortiGate Signature attack dropped**: This category based report provides information related to signature attack dropped (TCP/UDP, ICMP, others).
- **FortiGate Signature attack reset**: This category based report provides information related to signature attack reset (TCP/UDP, ICMP, others).

- **Traffic**: Traffic logs record the traffic that is flowing through your FortiGate unit.

Events which can be monitored using EventTracker:

- **FortiGate Firewall traffic accepted**: This category based report provides information related to Firewall traffic being accepted.
- **FortiGate Firewall traffic deny**: This category based report provides information related to Firewall traffic denial.
- **FortiGate Firewall traffic timeout**: This category based report provides information related to Firewall traffic timed-out.
- **FortiGate ICMP message succeed**: This category based report provides information related to ICMP message succeeded.
- **FortiGate Multicast allowed message**: This category based report provides information related to multicast allowed message.
- **FortiGate Violation message**: This category based report provides information related to violation message.
- **FortiGate WAN optimization traffic**: This category based report provides information related to WAN optimization traffic.

- **Antivirus**: The logs provide a way to understand what viruses are trying to get in, as well as additional information about the virus itself. Events which can be monitored using EventTracker:

  - **FortiGate FortiGuard Analytics**: This category based report provides information related to FortiGuard analytics.
  - **FortiGate FortiGuard Analytics blocked**: This category based report provides information related to FortiGuard analytics blocked.
- **FortiGate FortiGuard Analytics monitored**: This category based report provides information related to FortiGuard analytics monitored.

- **FortiGate FortiGuard Analytics passthrough**: This category based report provides information related to FortiGuard analytics passthrough.

- **FortiGate Archive is corrupted**: This category based report provides information when archive is corrupted.

- **FortiGate Archive is encrypted**: This category based report provides information when archive is encrypted.

- **FortiGate Infected MIME pass**: This category based report provides information when MIME (Multipurpose Internet Mail Extension) pass is infected.

- **FortiGate MMS content checksum**: This category based report provides information related to MMS (Multimedia Messaging Service) content checksum.

- **FortiGate Multipart archive**: This category based report provides information related to multipart archive.

- **FortiGate Nested archive detected**: This category based report provides information related to nested archive detected.

- **FortiGate Oversized mime blocked**: This category based report provides information related to an oversized block.

- **FortiGate Oversized archive**: This category based report provides information when an archive is oversized.

- **FortiGate Oversized mime pass**: This category based report provide information related to when Multipurpose Internet Mail Extensions such as GIF graphics files and PostScript files passes.

- **FortiGate Switching protocols**: This category based report provides information when switching protocols are bypassed or blocked.

- **FortiGate Unhandled archive**: This category based report provides information related to an unhandled archive type.

- **FortiGate Virus file exempted**: This category based report provides information when virus file is exempted.

- **FortiGate Virus file intercepted**: This category based report provide information related to virus file interception.

- **FortiGate Virus infected file block**: This category based report provides information when Virus infected file is blocked.

- **FortiGate Virus infected file pass**: This category based report provides information when Virus infected file is passed.

- **FortiGate Worm blocked**: This category based report provides information when virus infected worm is blocked.

- **FortiGate Worm MIME monitored**: This category based report provides information when infected worm MIME is monitored.
- **Application-control:** The application control feature controls the flow of traffic from a specific application, and the FortiGate unit examines this traffic for signatures that the application generates.

Events which can be monitored using EventTracker:

- **FortiGate Application control SSH filter blocked:** This category based report provides information related to application control SSH filter blocked.
- **FortiGate App-control log message:** This category based report provides information related to an application control IM (VoIP basic) log message.

- **Data Leak Prevention:** Data Leak Prevention (DLP) logs, provide valuable information about the sensitive data trying to get through to your network as well as any unwanted data trying to get into your network.

Events which can be monitored using EventTracker:

- **FortiGate DLP Fingerprint:** This category based report provides information related to Fortinet DLP fingerprinting of document files and document file sources, multiple inspection modes (proxy and flow-based), enhanced pattern matching and data archiving.
- **FortiGate DLP warning:** This category based report provides information related to DLP warning.
- **FortiGate Data leak detected:** This category based report provides information related to data leak detected by a specified DLP sensor rule.
- **FortiGate Data leak blocked:** This category based report provides information related to data leak blocked by a specified DLP sensor rule.

- **Email filter:** Email filters logs, also referred to as spam filter logs, records information regarding the content within email messages. For example, within an email filter profile, a match is found that finds the email message to be considered spam.

Events which can be monitored using EventTracker:

- **FortiGate Content Archive:** This category based report provides information related to Content archive.
- **FortiGate Spam MM1 duplicate detected:** This category based report provides information when antispam MM1 duplicate is detected.
- **FortiGate Spam IMAP detected:** This category based report provides information when antispam IMAP banned-word is detected.
• **FortiGate POP3 spam blocked**: This category based report provides information when POP3 (Post Office Protocol) antispam is blocked.
• **FortiGate POP3 spam detected**: This category based report provides information when POP3 antispam is detected.
• **FortiGate POP3 spam exempted**: This category based report provides information when POP3 antispam is exempted.
• **FortiGate Endpoint filter detected**: This category based report provides information when endpoint filter is detected.
• **FortiGate SMTP spam blocked**: This category based report provides information when SMTP (Simple Mail Transfer Protocol) antispam is blocked.
• **FortiGate SMTP spam detected**: This category based report provides information when SMTP antispam is detected.
• **FortiGate SMTP spam exempted**: This category based report provides information when SMTP antispam is exempted.

**Alerts**

• **FortiGate:Virus Detected**: This alert is generated when antivirus detects an anomaly.
• **FortiGate:Attack Detected**: This alert is generated when an attack is detected by IPS.
• **FortiGate:Configuration Changed**: This alert is generated when firewall configuration is changed.
• **FortiGate:Administrator Logon Failed**: This alert is generated when administrator logon fails.

**Reports**

• **FortiGate-Attack Detected**: This report provides information related to attacks detected by IPS which includes Source Address, Source Port, Destination Address, Destination Port, Action, Attack Type, Attack Name, Referred URL and Attack Details fields.
• **FortiGate-Traffic Denied**: This report provides information related to traffic denied by firewall which includes Source Address, Source Port, Source Location, Destination Address, Destination Port, Destination Location, Service Name and Traffic Type fields.
• **FortiGate-Virus Detected**: This report provides information related to virus detected by antivirus which includes Source Address, Source Port, Destination Address, Destination Port, Service Name, Action, Virus Type, Virus Name and Referred URL fields.
• **FortiGate-VPN Logon Details**: This report provides information related to VPN logon success and failure which includes User Name, Tunnel Name, Source Address, Source Port, Destination Address, Destination Port, Action and Status fields.
- **FortiGate-Data Leak Detected**: This report provides information related to data breach detected by DLP which includes User Name, Source Address, Source Port, Destination Address, Destination Port, Host Name, File Type, File name and URL fields.

- **FortiGate-Suspicious Email Content Detected**: This report provides information related to hazardous attachment detected by Email filter which includes Source Address, Source Port, Destination Address, Destination Port, Service Name, Sender Address, Receiver Address and Mail Subject fields.

- **FortiGate-Traffic Allowed**: This report provides information related to traffic allowed by firewall which includes Source Address, Source Port, Source Location, Destination Address, Destination Port, Destination Location, Service Name and Traffic Type fields.

- **FortiGate-Suspicious Web Content Detected**: This report provides information related to hazardous web content detected by Web filter which includes Source Name, Source Address, Source Port, Destination Address, Destination Port, OS Version, OS Name, Host Name, Action, Service Name, Content Type and URL fields.

- **FortiGate-Administrator Logon Details**: This report provides information related to administrator logon success, logon failure and logout events which include Administrator Name, Administrator Address, Console Type, Action, Status and Reason fields.

- **FortiGate-Configuration Change Details**: This report provides information related to firewall configuration change which includes User Name, Console Type, Activity, Action, Configuration Path, Configuration Object and Configuration Attribute fields.

- **FortiGate-User Authentication Details**: This report provides information related to user authentication success and failure which includes User Name, Group Name, Source Address, Destination Address, and Console Type, Action, Status and Reason fields.

- **FortiGate-Policy Management Details**: This report provides information related to user policy management which includes User Name, Source Address, Destination Address, Message fields.

- **FortiGate-IDS (Intrusion Detection) Details**: This report provides information related to intrusion detection which includes Source Address, Destination Address, Services, Time, Date and Message fields.

- **FortiGate-Spam Filter Details**: This report provides information related to spam filters which include Source Address, Destination Address, Services, Time, Date, and Messages fields.

- **FortiGate-Password Change**: This report provides information related to user Password changed which includes Category, Subcategory, User Name and Messages fields.

### Knowledge Objects

- **FortiGate Firewall (For FortiOS 4.0)**: This KO assists in evaluation of all events generated by FortiGate firewall with FortiOS 4.0.

- **FortiGate Firewall (For FortiOS 5.0 or later)**: This KO assists in evaluation of all events generated by FortiGate firewall with FortiOS 5.0 or later.
Create Dashboards in EventTracker

Schedule Reports

1. Open EventTracker in browser and logon.

![Image of EventTracker interface]

2. Navigate to Reports>Configuration.

![Image of Reports Configuration]

3. Select FortiGate 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.

![Figure 25]

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.
Evaluating chart is shown.

Figure 26

16. If satisfied, Click **Configure** button.

![Configure button](image)

Figure 27

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

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

1. FortiGate Top Allowed Traffic Today

![FortiGate Top Allowed Traffic Today](image1)

**Figure 28**

2. FortiGate Top Denied Traffic Today

![FortiGate Top Denied Traffic Today](image2)

**Figure 29**
3. FortiGate Top Attacks Detected Today

Figure 30
Sample Reports

1. fortigate-VPN Logon Details

<table>
<thead>
<tr>
<th>LogTime</th>
<th>User Name</th>
<th>Tunnel Name</th>
<th>Source Address</th>
<th>Source Port</th>
<th>Destination Address</th>
<th>Destination Port</th>
<th>Action</th>
<th>Status</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/1/2015 02:21:47 PM</td>
<td>Derek</td>
<td>N/A</td>
<td>123.23.31.204</td>
<td>500</td>
<td>123.23.31.170</td>
<td>500</td>
<td>negotiate success</td>
<td>Progress Phase 1</td>
<td></td>
</tr>
<tr>
<td>10/1/2015 03:44:25 PM</td>
<td>Derek</td>
<td>N/A</td>
<td>123.23.31.204</td>
<td>500</td>
<td>125.33.112.23</td>
<td>500</td>
<td>negotiate failure</td>
<td>Progress Phase 1</td>
<td></td>
</tr>
<tr>
<td>10/1/2015 05:01:33 PM</td>
<td>Jack</td>
<td>Mobile_VPN</td>
<td>123.23.31.116</td>
<td>500</td>
<td>125.33.112.23</td>
<td>500</td>
<td>negotiate success</td>
<td>Progress Phase 1</td>
<td></td>
</tr>
<tr>
<td>10/1/2015 06:17:41 PM</td>
<td>Sara</td>
<td>Mobile_VPN</td>
<td>123.23.22.10</td>
<td>54</td>
<td>125.33.31.74</td>
<td>86</td>
<td>negotiate failure</td>
<td>Progress Phase 2</td>
<td></td>
</tr>
<tr>
<td>10/1/2015 07:34:10 PM</td>
<td>Jack</td>
<td>Mobile_VPN</td>
<td>123.23.31.117</td>
<td>501</td>
<td>123.23.31.171</td>
<td>501</td>
<td>negotiate success</td>
<td>Progress Phase 1</td>
<td></td>
</tr>
<tr>
<td>10/1/2015 08:50:57 PM</td>
<td>Martha</td>
<td>N/A</td>
<td>123.23.22.11</td>
<td>55</td>
<td>125.33.112.24</td>
<td>86</td>
<td>negotiate success</td>
<td>Progress Phase 2</td>
<td></td>
</tr>
<tr>
<td>10/1/2015 10:07:35 PM</td>
<td>Pascal</td>
<td>N/A</td>
<td>123.23.31.116</td>
<td>500</td>
<td>52.36.55.47</td>
<td>59</td>
<td>negotiate failure</td>
<td>Progress Phase 2</td>
<td></td>
</tr>
<tr>
<td>10/1/2015 11:24:13 PM</td>
<td>Sara</td>
<td>Mobile_VPN</td>
<td>123.23.22.17</td>
<td>56</td>
<td>125.33.112.25</td>
<td>97</td>
<td>negotiate success</td>
<td>Progress Phase 2</td>
<td></td>
</tr>
<tr>
<td>10/1/2015 12:45:51 AM</td>
<td>Pascal</td>
<td>Server_VPN</td>
<td>25.22.14.22</td>
<td>503</td>
<td>52.36.55.48</td>
<td>135</td>
<td>negotiate success</td>
<td>Progress Phase 2</td>
<td></td>
</tr>
<tr>
<td>10/1/2015 01:57:29 AM</td>
<td>John</td>
<td>Mobile_VPN</td>
<td>123.23.41.28</td>
<td>57</td>
<td>125.33.112.26</td>
<td>173</td>
<td>negotiate failure</td>
<td>Progress Phase 2</td>
<td></td>
</tr>
<tr>
<td>10/1/2015 03:14:07 AM</td>
<td>Sara</td>
<td>N/A</td>
<td>25.22.14.23</td>
<td>120</td>
<td>52.36.55.49</td>
<td>211</td>
<td>negotiate failure</td>
<td>Progress Phase 2</td>
<td></td>
</tr>
<tr>
<td>10/1/2015 04:30:48 AM</td>
<td>John</td>
<td>Mobile_VPN</td>
<td>123.23.41.28</td>
<td>199</td>
<td>125.33.112.27</td>
<td>248</td>
<td>negotiate failure</td>
<td>Progress Phase 1</td>
<td></td>
</tr>
<tr>
<td>10/1/2015 05:47:23 AM</td>
<td>Jack</td>
<td>N/A</td>
<td>25.22.14.24</td>
<td>270</td>
<td>52.36.55.50</td>
<td>267</td>
<td>negotiate failure</td>
<td>Progress Phase 2</td>
<td></td>
</tr>
<tr>
<td>10/1/2015 07:04:31 AM</td>
<td>Lee</td>
<td>Mobile_VPN</td>
<td>123.23.41.30</td>
<td>341</td>
<td>125.33.112.26</td>
<td>335</td>
<td>negotiate failure</td>
<td>Progress Phase 2</td>
<td></td>
</tr>
<tr>
<td>10/1/2015 09:20:39 AM</td>
<td>Pascal</td>
<td>Server_VPN</td>
<td>25.22.14.25</td>
<td>412</td>
<td>125.33.30.70</td>
<td>563</td>
<td>negotiate failure</td>
<td>Progress Phase 2</td>
<td></td>
</tr>
<tr>
<td>10/1/2015 09:37:17 AM</td>
<td>John</td>
<td>N/A</td>
<td>123.23.41.31</td>
<td>483</td>
<td>125.33.35.77</td>
<td>401</td>
<td>negotiate failure</td>
<td>Progress Phase 1</td>
<td></td>
</tr>
<tr>
<td>10/1/2015 12:10:35 PM</td>
<td>John</td>
<td>Mobile_VPN</td>
<td>123.23.41.32</td>
<td>625</td>
<td>125.33.112.27</td>
<td>82</td>
<td>negotiate success</td>
<td>Progress Phase 2</td>
<td></td>
</tr>
<tr>
<td>10/1/2015 01:27:11 PM</td>
<td>Sara</td>
<td>N/A</td>
<td>25.22.14.27</td>
<td>698</td>
<td>125.33.30.71</td>
<td>509</td>
<td>negotiate failure</td>
<td>Progress Phase 1</td>
<td></td>
</tr>
</tbody>
</table>

2. Fortigate-Virus Detected

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Device Name</th>
<th>Source Address</th>
<th>Source Port</th>
<th>Destination Address</th>
<th>Destination Port</th>
<th>Service Name</th>
<th>Action</th>
<th>Virus Type</th>
<th>Virus Name</th>
<th>Virus Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/1/2015 09:00:30 PM</td>
<td>FGT45120374</td>
<td>10.260.31.44</td>
<td>66236</td>
<td>103.230.04.235</td>
<td>560</td>
<td>http</td>
<td>blocked infected</td>
<td>MyDoomFile is infected.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/1/2015 08:11:11 PM</td>
<td>FGT45120374</td>
<td>10.260.31.71</td>
<td>66236</td>
<td>124.31.102.25</td>
<td>441</td>
<td>https</td>
<td>blocked infected</td>
<td>MyDoomFile is infected.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10/1/2015 02:04:35 PM</td>
<td>FGT45120374</td>
<td>10.260.31.23</td>
<td>66236</td>
<td>103.230.04.248</td>
<td>22</td>
<td>http</td>
<td>blocked boodnet</td>
<td>ZeusFile is infected.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## 3. FortiGate-Traffic Denied

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Device Name</th>
<th>Source Address</th>
<th>Source Port</th>
<th>Source Location</th>
<th>Destination Address</th>
<th>Destination Port</th>
<th>Destination Location</th>
<th>Service Name</th>
<th>Traffic Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/09/2015 03:42:09 PM</td>
<td>FG123456789</td>
<td>176.29.117.125</td>
<td>53019</td>
<td>USA</td>
<td>123.231.70.68</td>
<td>53</td>
<td>Sri Lanka</td>
<td>TELNET</td>
<td>Local</td>
</tr>
<tr>
<td>10/09/2015 03:45:12 PM</td>
<td>FG123456789</td>
<td>176.29.117.125</td>
<td>53019</td>
<td>USA</td>
<td>123.231.70.68</td>
<td>53</td>
<td>Sri Lanka</td>
<td>TELNET</td>
<td>Local</td>
</tr>
<tr>
<td>10/09/2015 03:58:22 PM</td>
<td>FG123456789</td>
<td>176.29.117.125</td>
<td>54436</td>
<td>Reserved</td>
<td>123.231.70.73</td>
<td>53</td>
<td>Sri Lanka</td>
<td>TELNET</td>
<td>Local</td>
</tr>
<tr>
<td>10/09/2015 04:00:30 PM</td>
<td>FG123456789</td>
<td>176.29.117.125</td>
<td>54436</td>
<td>USA</td>
<td>123.231.70.73</td>
<td>53</td>
<td>Sri Lanka</td>
<td>TELNET</td>
<td>Local</td>
</tr>
<tr>
<td>10/09/2015 04:10:36 PM</td>
<td>FG123456789</td>
<td>192.168.3.98</td>
<td>114</td>
<td>Reserved</td>
<td>204.95.99.62</td>
<td>8020</td>
<td>United States</td>
<td>FTP</td>
<td>Pass-through</td>
</tr>
<tr>
<td>10/09/2015 04:17:45 PM</td>
<td>FG123456789</td>
<td>176.29.117.126</td>
<td>472</td>
<td>USA</td>
<td>152.66.23.41</td>
<td>802</td>
<td>China</td>
<td>TCP</td>
<td>Forward</td>
</tr>
<tr>
<td>10/09/2015 04:24:54 PM</td>
<td>FG123456789</td>
<td>192.168.3.70</td>
<td>1115</td>
<td>USA</td>
<td>254.95.99.63</td>
<td>74</td>
<td>UK</td>
<td>UDP</td>
<td>Forward</td>
</tr>
<tr>
<td>10/09/2015 04:32:02 PM</td>
<td>FG123456789</td>
<td>176.29.117.127</td>
<td>124</td>
<td>USA</td>
<td>72.66.23.42</td>
<td>142</td>
<td>France</td>
<td>TCP</td>
<td>Forward</td>
</tr>
<tr>
<td>10/09/2015 04:38:13 PM</td>
<td>FG123456789</td>
<td>192.168.3.47</td>
<td>752</td>
<td>USA</td>
<td>142.25.33.52</td>
<td>210</td>
<td>Germany</td>
<td>UDP</td>
<td>Forward</td>
</tr>
<tr>
<td>10/09/2015 04:56:18 PM</td>
<td>FG123456789</td>
<td>176.29.117.111</td>
<td>1380</td>
<td>USA</td>
<td>72.66.23.43</td>
<td>278</td>
<td>France</td>
<td>TCP</td>
<td>Forward</td>
</tr>
<tr>
<td>10/09/2015 04:58:28 PM</td>
<td>FG123456789</td>
<td>192.168.3.48</td>
<td>2005</td>
<td>Reserved</td>
<td>142.25.33.53</td>
<td>346</td>
<td>Germany</td>
<td>UDP</td>
<td>Forward</td>
</tr>
<tr>
<td>10/09/2015 05:00:34 PM</td>
<td>FG123456789</td>
<td>176.29.117.112</td>
<td>2020</td>
<td>USA</td>
<td>72.66.23.44</td>
<td>414</td>
<td>France</td>
<td>TCP</td>
<td>Forward</td>
</tr>
<tr>
<td>10/09/2015 05:07:42 PM</td>
<td>FG123456789</td>
<td>192.168.3.49</td>
<td>3364</td>
<td>Reserved</td>
<td>142.25.33.54</td>
<td>482</td>
<td>Germany</td>
<td>UDP</td>
<td>Forward</td>
</tr>
<tr>
<td>10/09/2015 05:14:50 PM</td>
<td>FG123456789</td>
<td>176.29.117.113</td>
<td>3692</td>
<td>USA</td>
<td>72.66.23.45</td>
<td>550</td>
<td>France</td>
<td>TCP</td>
<td>Forward</td>
</tr>
<tr>
<td>10/09/2015 05:21:53 PM</td>
<td>FG123456789</td>
<td>192.168.3.50</td>
<td>4520</td>
<td>USA</td>
<td>204.95.99.67</td>
<td>810</td>
<td>UK</td>
<td>FTP</td>
<td>Forward</td>
</tr>
<tr>
<td>10/09/2015 05:29:06 PM</td>
<td>FG123456789</td>
<td>176.29.117.129</td>
<td>417</td>
<td>Reserved</td>
<td>152.66.23.46</td>
<td>886</td>
<td>India</td>
<td>TCP</td>
<td>Pass-through</td>
</tr>
<tr>
<td>10/09/2015 05:36:14 PM</td>
<td>FG123456789</td>
<td>192.168.3.75</td>
<td>120</td>
<td>USA</td>
<td>204.95.99.68</td>
<td>754</td>
<td>UK</td>
<td>FTP</td>
<td>Forward</td>
</tr>
</tbody>
</table>