Integrate Barracuda Spam Firewall
Abstract

This guide provides instructions to configure Barracuda Spam Firewall to send the events to EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version 7.X and later, and Barracuda Spam Firewall 300 and later.

Audience

Barracuda Spam Firewall users, who wish to forward messages to EventTracker manager.
# Table of Contents

Abstract ................................................................................................................................. 1
Overview.................................................................................................................................. 3
Prerequisites............................................................................................................................. 3
Configuration............................................................................................................................ 3
Barracuda Syslog Server Configuration: .................................................................................. 3
EventTracker Knowledge Pack (KP) ....................................................................................... 4
    Alerts ................................................................................................................................. 4
    Categories......................................................................................................................... 5
    Reports .............................................................................................................................. 5
Import Barracuda Spam Firewall knowledge pack in EventTracker ........................................ 6
    Alerts ................................................................................................................................. 6
    Category ............................................................................................................................ 7
    Flex Reports ..................................................................................................................... 8
    Template .......................................................................................................................... 10
    Knowledge Object ........................................................................................................... 12
To Configure Flex Dashboard ................................................................................................. 14
Verify Barracuda Spam Firewall knowledge pack in EventTracker ........................................ 18
    Alerts ................................................................................................................................. 18
    Categories......................................................................................................................... 20
    Flex Reports ..................................................................................................................... 21
    Template .......................................................................................................................... 22
    Knowledge Objects .......................................................................................................... 23
Sample Report .......................................................................................................................... 24
Sample Dashboard .................................................................................................................. 25
Overview

The Barracuda Spam Firewall manages and filters all inbound and outbound email traffic to protect organizations from email-borne threats and data leaks. As a complete email management solution, the Barracuda Spam Firewall lets organizations encrypt messages and leverage the cloud to spool email if mail servers become unavailable.

With EventTracker you can monitor system logs like login activity (login failed and logout), configuration changes and messages containing virus and spam and quarantine messages. EventTracker will generate alerts for configuration changes, spam mails and virus mails. It will generate reports for login failed activity and configuration changes which will help you in compliance and security and generate reports for spam, virus and quarantine mails. Its dashboard provides us the graphical view for information of top mail recipients, top blocked messages and top spam and virus sender.

Prerequisites

- EventTracker 7.x and later should be installed.
- Barracuda Spam Firewall 300 and later should be installed.
- Administrative access on the EventTracker Enterprise and Barracuda Spam Firewall.
- An exception should be added into Windows Firewall on EventTracker machine for syslog port 514.
- An exception should be added into Firewall in between EventTracker and Barracuda Spam Firewall for syslog port 514.

Configuration

You must enable and configure logging on Barracuda Spam Firewall prior to configuring EventTracker.

Barracuda Syslog Server Configuration:

1. Login into web console of Barracuda Spam Firewall.
2. Go to the **ADVANCED > Advanced Networking** page.
   - In the **Syslog Configuration** section, fill IP address and port of EventTracker machine in **Mail Syslog** and **web interface Syslog**.
3. Click on **Add**
4. Click **Save** button for saving the configuration.

**EventTracker Knowledge Pack (KP)**

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

The following Knowledge Packs are available in EventTracker Enterprise to support Barracuda Spam Firewall.

**Alerts**

- **Barracuda Spam Firewall: Mail contains virus** - This alert is generated when spam firewall identifies mails which contains virus.
- **Barracuda Spam Firewall: Spam mails** - This alert is generated when spam firewall blocks spam messages.
- **Barracuda Spam Firewall: Configuration changes** - This alert is generated when the configuration changes in barracuda spam firewall.
- **Barracuda Spam Filter: User login failed** – This alert is generated when user login fails in barracuda spam filter.
Categories

- **Barracuda Spam Firewall: Configuration changes**: All logs generated by Barracuda spam virus firewall when configuration changes happen.
- **Barracuda Spam Firewall: Firewall received messages**: All logs generated by Barracuda spam virus firewall when a message was received and handled by the MTA.
- **Barracuda Spam Firewall: Firewall scan messages**: All logs generated by Barracuda spam virus firewall when a message was scanned and processing may have stopped or it may have been sent to the outbound processing for delivery.
- **Barracuda Spam Firewall: Firewall sending messages**: All logs generated by Barracuda spam virus firewall when a message is sent and status of outbound delivery.
- **Barracuda Spam Firewall: Login and logout activity**: All logs generated by Barracuda spam virus firewall when login or logout is happened on barracuda spam firewall web interface.
- **Barracuda Spam Filter: User login success**: This category provides information related to user login success into barracuda spam filter.
- **Barracuda spam filter - User login failed**: This category provides information related to user login failure into barracuda spam filter.

Reports

- **Barracuda Spam Firewall - Blocked messages**: This report provides information related to blocked messages which contains sender and recipient information, message id, mail direction (inbound or outbound), mail server IP, subject of the mails and reason code for why the mail transfer is blocked.
- **Barracuda Spam Firewall - Mails contains virus**: This report provides us the information related to mails containing virus which have information about sender and recipient, message id, mail direction and subject of the mails.
- **Barracuda Spam Firewall - spam mails**: This report provides us the information related to spam mails which contains sender and recipient information, mail direction, message id and subject of the message.
- **Barracuda Spam Firewall - quarantine messages**: This report provides us the information related to quarantine messages which contains sender and recipient information, mail direction, message id, subject of the message and reason code why it is in quarantine.
- **Barracuda Spam Firewall - Login failed activity**: This report provides information related to login failed which contains username and source IP address.
- **Barracuda Spam Firewall - Configuration changes**: This report provides information related to configuration changes in barracuda spam firewall which contains source IP, setting which is changed and the changes happened and information about who changed it.
• Barracuda Spam Filter - User login success: This report provides information related to user login success into barracuda spam filter.
• Barracuda spam filter - User login failed: This report provides information related to user login failure into barracuda spam filter.

Import Barracuda Spam Firewall knowledge pack in EventTracker

1. Launch EventTracker Control Panel.
2. Double click Export Import Utility. Click Import tab.
   Import Alert/Category/Tokens/ Flex Reports/Knowledge Objects as given below.

Alerts

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

![Export Import Utility](image)

Figure 2

2. Locate All Barracuda Spam Firewall.isalt file, and then click the Open button.
3. To import alerts, click the **Import** button. EventTracker displays success message.

![Import Success Message](image)

**Figure 3**

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

### Category

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

![Category Options](image)

**Figure 4**

2. Locate **All Barracuda Spam Firewall group of Categories.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button. EventTracker displays success message.

   ![](image)

   Figure 5

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

**Flex Reports**

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

   ![Image]

   Figure 6

2. Locate the **All Barracuda Spam Firewall** group of **Flex Report.issch** file, and then click the **Open** button.
3. Click the **Import** button to import the scheduled reports. EventTracker displays success message.

![Export Import Utility](image)

**Selected reports configurations are imported successfully.**

**Figure 7**

4. Click the **OK** button. Click the **Close** button.
Template

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu and then click the **Parsing rule**.
3. Click the **Template** tab.
4. Click the **Import** button, it will open new window. ( **NOTE**: Make sure pop-up is enabled for EventTracker).

![Parsing Rule](image)

Figure 8

5. Locate and Choose .ETTD file and then click the **Open** button.
6. Select the template you want to upload.
7. Then click on the **Import configuration** icon.

EventTracker displays success message
Figure 11

8. Click **OK** and it will automatically close the window.

**Knowledge Object**

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu and then click the **Knowledge Objects**.
3. Click the **Import** button, it will open new window. (**NOTE**: Make sure pop-up is enabled for EventTracker.

![Figure 12: Knowledge Object Interface](image)

4. Choose the Knowledge object template (.EKTO) files and click on **UPLOAD** button.
5. Select Knowledge Object and click on **Overwrite or Merge** button.

EventTracker displays success message.
6. Click **OK** and it will automatically close the window.

**To Configure Flex Dashboard**

1. Schedule the flex reports (**Barracuda Spam Firewall-Allowed** messages) after importing them.
2. During scheduling, please check **Persist data** and select all the columns to persist.
3. Now, wait for report to run as per scheduled time.
4. After generating report, click on Dashboard > Flex.
5. Click on Add Dashboard button and fill Title and Description box and save it.
6. Now, create dashlet for Barracuda Spam Firewall by clicking on Configure flex dashlet icon.

7. Fill WIDGET TITLE, select DATA SOURCE, select CHART TYPE and select AXIS LABELS [X-AXIS].

8. After selecting and filling all options, click on the TEST button to check the Dashlet. If data are coming properly, then click on CONFIGURE button.
9. After creation of Dashlet for Barracuda Spam Firewall, click on **Customize flex dashlet**.

10. Select **Barracuda Spam Firewall-Top blocked mails** dashlet and click on **ADD** button.

11. Now, you can see the Dashlet on Dashboard.
Verify Barracuda Spam Firewall knowledge pack in EventTracker

Alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Alerts.
3. In Search field, type ‘Barracuda Spam’, and then click the Go button.
   Alert Management page will display all the imported Barracuda Spam Firewall alerts.
4. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

![Figure 23](image-url)

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

**NOTE:** You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.
Categories

1. Logon to EventTracker Enterprise.
2. Click Admin dropdown, and then click Categories.
3. In Category Tree to view imported categories, scroll down and expand Barracuda Spam Firewall group folder to view the imported categories.

![CATEGORY MANAGEMENT](image)

Figure 25
Flex Reports

1. Logon to EventTracker Enterprise.
2. Click the Reports.
3. Select the Configuration.
   In the Reports Configuration, select Defined by clicking the radio button. EventTracker displays Defined page.
4. Click the Barracuda Spam Firewall report group.
   EventTracker displays Flex reports of Barracuda Spam Firewall.

![Figure 26](image-url)
Template

1. Logon to EventTracker Enterprise, Go to Parsing rule.
2. Click on Template tab.
3. Check the template you had uploaded.

Figure 27
Knowledge Objects

1. Logon to EventTracker Enterprise.
2. Click on Knowledge Object option.
3. Check the Knowledge Object you had uploaded.
Sample Report

A sample report is shown below.

1. **Barracuda Spam Firewall-Login and logout activity**

   ![Barracuda Spam Firewall-Login and logout activity](image)

   Figure 29

2. **Barracuda Spam Firewall-Configuration changes**

   ![Barracuda Spam Firewall-Configuration changes](image)

   Figure 30
Sample Dashboard

1. Barracuda Spam Firewall-Top Blocked messages

![Figure 31](image1.png)

2. Barracuda Spam Firewall-Top Recipient

![Figure 32](image2.png)