

Integrate Barracuda NextGen Firewall X

EventTracker v9.0 and Above

Abstract

This guide provides instructions to configure the Barracuda NextGen Firewall X to send the syslog events to the EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x and later, and Barracuda NextGen Firewall X Firewall.

Audience

Barracuda NextGen Firewall X Admins, who wish to forward syslog events to EventTracker.

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

This document is for informational purposes only. Netsurion 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 Netsurion, if its content is unaltered, nothing is added to the content and credit to Netsurion is provided.

Netsurion 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 Netsurion, 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.

© 2019 Netsurion. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

- 1. Overview..... 3
- 2. Prerequisites..... 3
- 3. Configuring Barracuda Firewall syslog 3
 - 3.1 Adding Export Log Server 3
- 4. EventTracker Knowledge Pack (KP) 4
 - 4.1 Categories 4
 - 4.2 Alerts..... 6
- 5. Importing Barracuda Firewall Knowledge pack into EventTracker..... 6
 - 5.1 Category..... 7
 - 5.2 Alerts..... 8
- 6. Verifying Barracuda Firewall knowledge pack in EventTracker 9
 - 6.1 Categories 9
 - 6.2 Alerts..... 10

1. Overview

The Barracuda NextGen Firewall X blocks an ever-expanding list of sophisticated web-based intrusions and attacks that target applications hosted on the web servers and in the cloud.

Barracuda NextGen Firewall X can be integrated with EventTracker using syslog. With the help of Barracuda NextGen Firewall X KP items, we can monitor the network firewall logs, access logs, web firewall logs, system logs and audit logs on web applications. It also triggers the alert for authentication hijacking, buffer overflow attack, command injection attack, denial of service attack, and obfuscation attack.

2. Prerequisites

- **EventTracker v9.x or above** should be installed.
- **Barracuda NextGen Firewall X** should be installed and proper access permissions to make configuration changes.

3. Configuring Barracuda Firewall syslog

3.1 Adding Export Log Server

1. Go to the **LOGS > Log Settings** page.
2. In the **Stream target** field, type the hostname or IP address of EventTracker. You can define only one target.
3. Select the **Protocol** and **Port**. The default port for **UDP** is **514**.
4. Select which log streams to enable.
5. Click **Save Changes**.

SYSLOG STREAMING

Stream target:
Hostname or IP address of receiver.

Protocol/Port: UDP
Note: Not all receivers support TCP.

Stream Firewall Log: ☐ Yes ☒ No

Stream HTTP Log: ☐ Yes ☒ No

Stream Network Log: ☐ Yes ☒ No

Stream VPN Log: ☐ Yes ☒ No

Stream Service Log: ☐ Yes ☒ No

Stream Authentication Log: ☐ Yes ☒ No

Figure 1

4. EventTracker Knowledge Pack (KP)

Once logs are received into EventTracker alerts and categories can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker v9.x to support Barracuda NextGen Firewall X monitoring:

4.1 Categories

- **Barracuda: Application platform exploits** - This category-based report provides information related to the application platform exploit.
- **Barracuda: Authentication hijacking** - This category-based report provides information related to the authentication hijacking.
- **Barracuda: Buffer overflow attack** - This category-based report provides information related to the buffer overflow attack.
- **Barracuda: Command injection attack** - This category-based report provides information related to the command injection attack.
- **Barracuda: Cookie poisoning attack** - This category-based report provides information related to a

cookie poisoning attack.

- **Barracuda: Cross-site scripting attack** - This category-based report provides information related to the cross-site scripting attack.
- **Barracuda: Denial-of-service attack** - This category-based report provides information related to the denial-of-service attack.
- **Barracuda: Directory traversal attack** - This category-based report provides information related to the directory traversal attack.
- **Barracuda: Error message interception** - This category-based report provides information related to the error message interception.
- **Barracuda: Firewall received messages** - This category-based report provides information related to the firewall received messages.
- **Barracuda: Firewall scan messages** - This category-based report provides information related to the firewall scan messages.
- **Barracuda: Firewall sending messages** - This category-based report provides information related to the firewall sending messages.
- **Barracuda: Forceful browsing attack** - This category-based report provides information related to the forceful browsing attack.
- **Barracuda: Form tampering attack** - This category-based report provides information related to the form tampering attack.
- **Barracuda: Malicious file execution attack** - This category-based report provides information related to the malicious file execution attack.
- **Barracuda: Obfuscation attack** - This category-based report provides information related to the obfuscation attack.
- **Barracuda: Protocol exploit attack** - This category-based report provides information related to the protocol exploit attack.
- **Barracuda: SQL injection attack** - This category-based report provides information related to the SQL injection attack.
- **Barracuda: Traffic allowed** - This category-based report provides information related to traffic the

allowed.

- **Barracuda: Traffic denied**- This category-based report provides information related to the traffic denied.

4.2 Alerts

- **Barracuda: Authentication hijacking**- This alert is generated when the authentication hijacking occurs.
- **Barracuda: Buffer overflow attack**- This alert is generated when a buffer overflow attack occurs.
- **Barracuda: Command injection attack**- This alert is generated when the command injection attack occurs.
- **Barracuda: Cookie poisoning attack**- This alert is generated when a cookie poisoning attack occurs.
- **Barracuda: Cross-site scripting attack**- This alert is generated when cross-site scripting attack.
- **Barracuda: Denial-of-service attack**- This alert is generated when a denial-of-service attack occurs.
- **Barracuda: Error message interception**- This alert is generated when the error message interception occurs.

5. Importing Barracuda Firewall Knowledge pack into EventTracker


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



Figure 2

3. Import **Category and Alerts** as given below.

5.1 Category

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

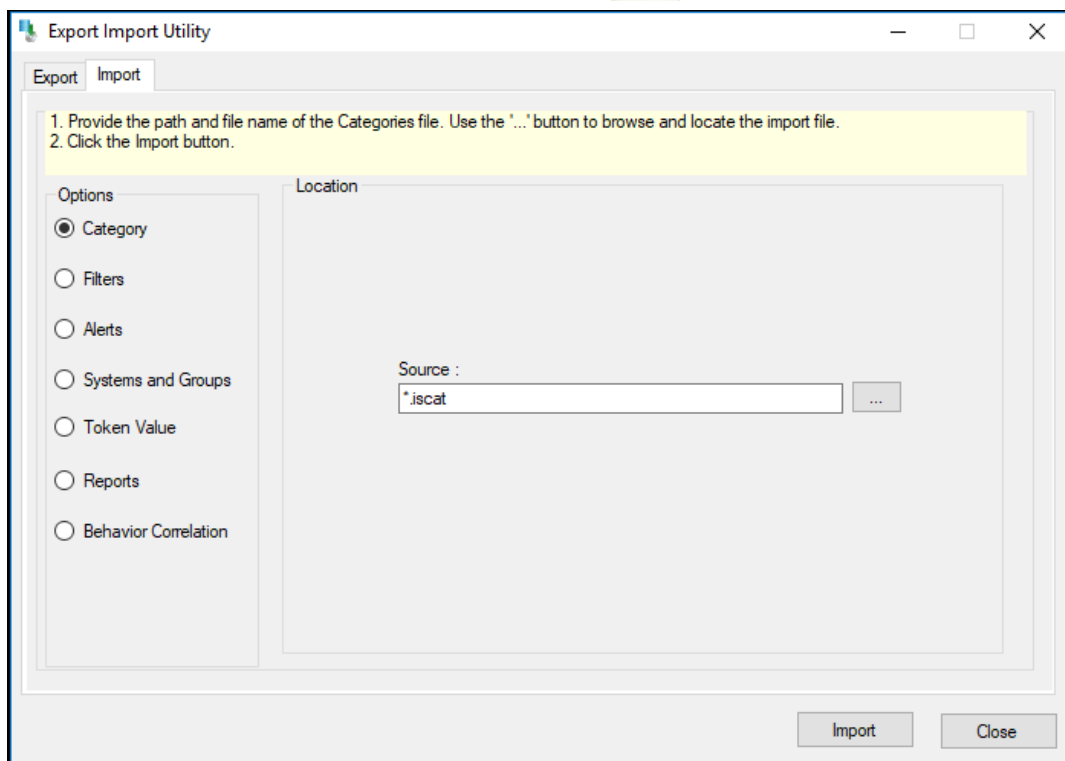


Figure 3

2. Locate **All Barracuda firewall group of Categories.iscat** file, and then click the **Open** button.
3. Click the **Import** button to import the categories.
4. EventTracker displays a success message.

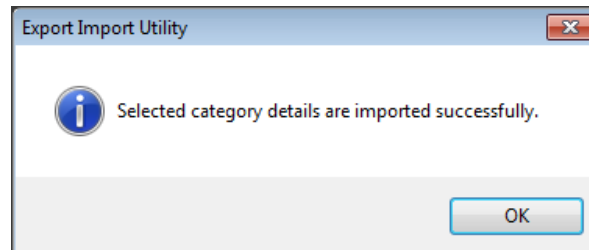



Figure 4

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

5.2 Alerts

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

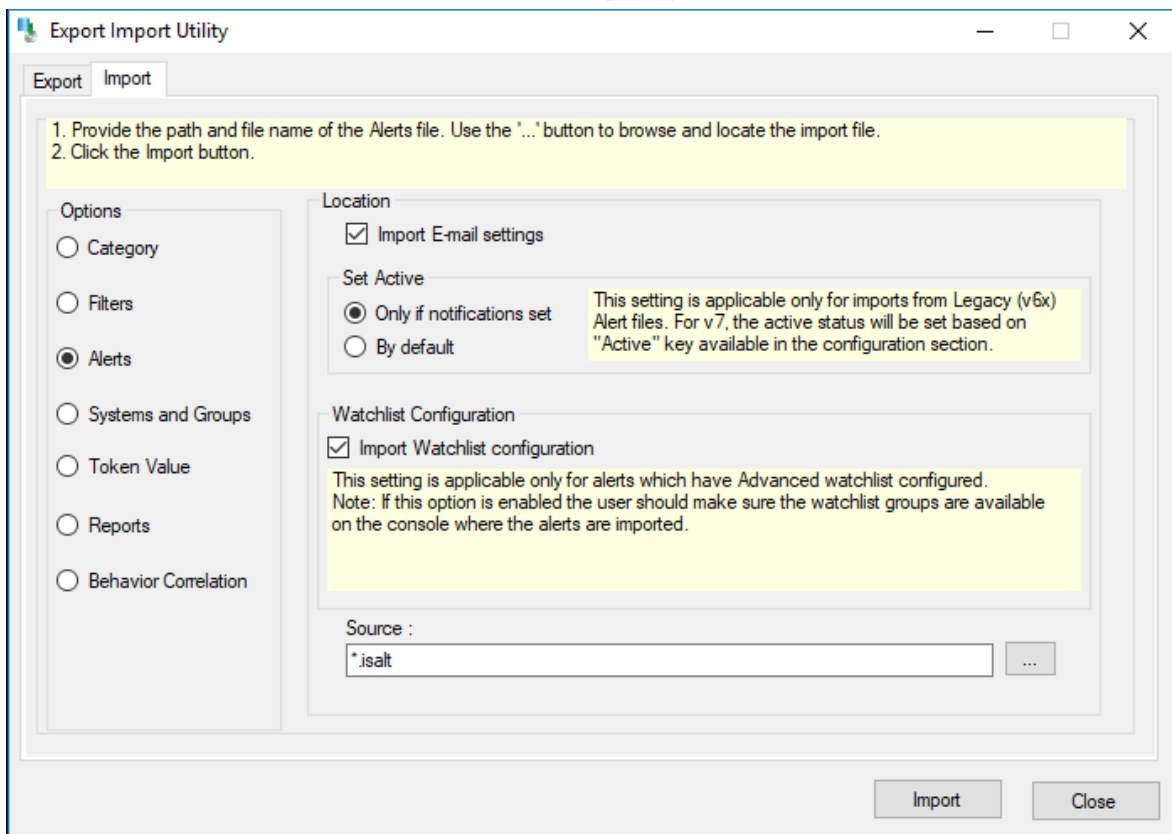


Figure 5

2. Locate **All Barracuda firewall group of Alerts.isalt** file, and then click the **Open** button.
3. Click the **Import** button to import the alerts.

EventTracker displays a success message.

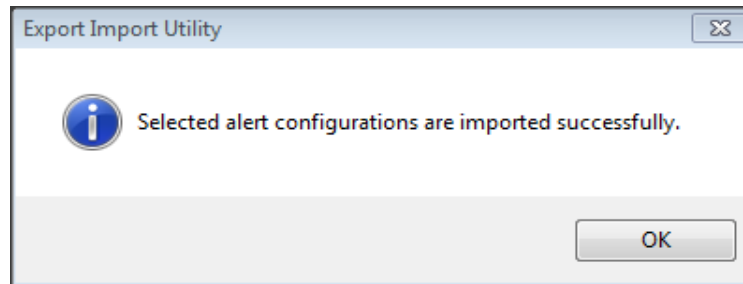


Figure 6

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

6. Verifying Barracuda Firewall knowledge pack in EventTracker

6.1 Categories

1. Login to **EventTracker**.
2. Click the **Admin** menu, and then click **Category**.

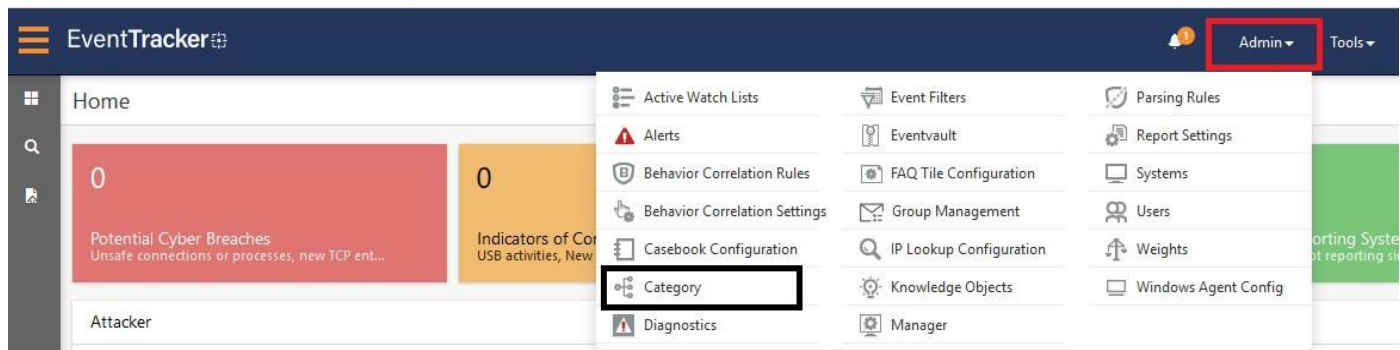


Figure 7

3. Click the **search**, and then **search** with **Barracuda**.

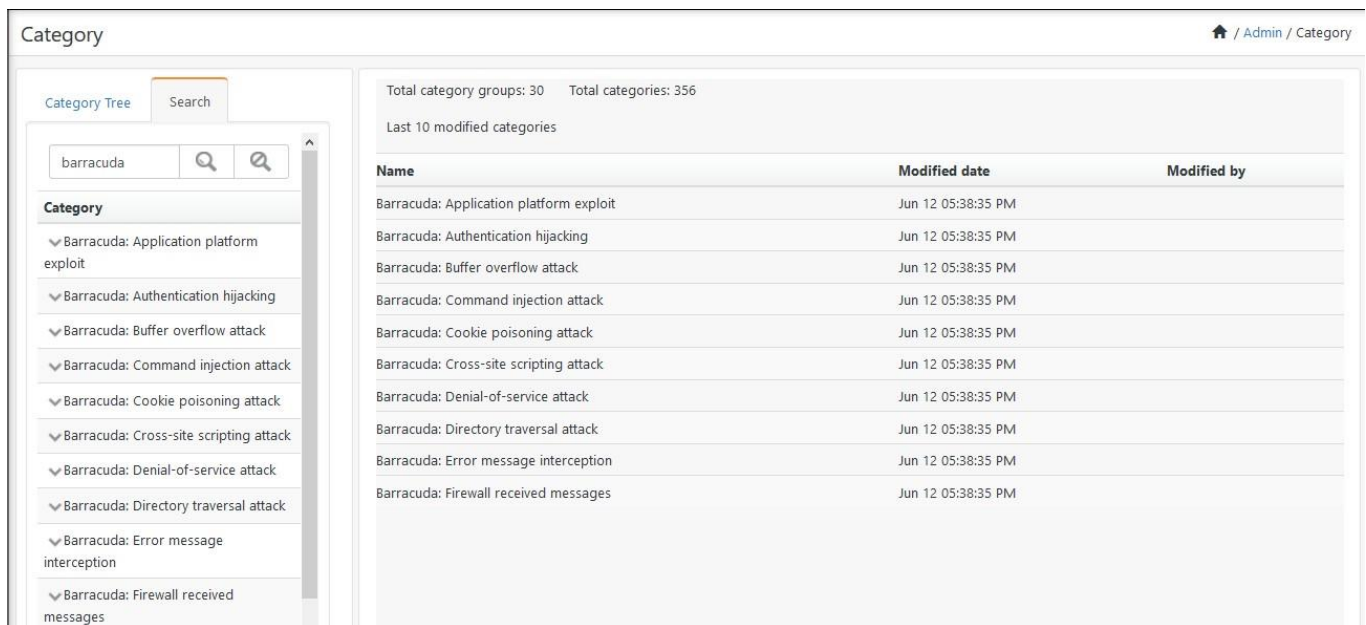


Figure 8

6.2 Alerts

1. Login to **EventTracker**.
2. Click the **Admin** menu, and then click **Alerts**.

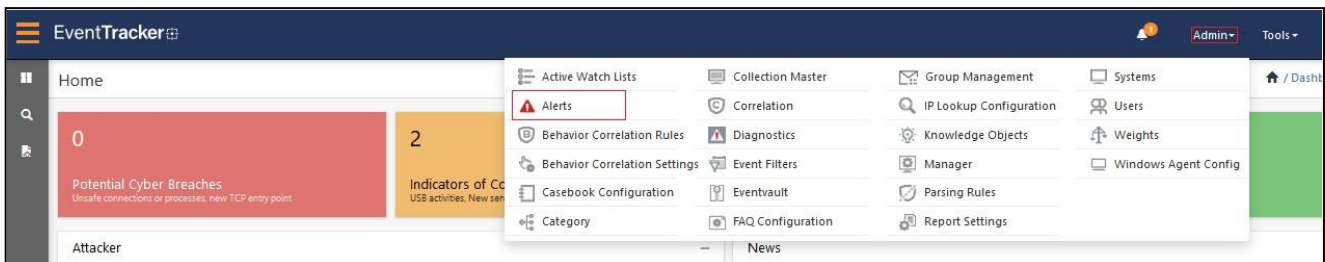


Figure 9

3. In the **Search** box, type '**Barracuda**', and then click the **search**. 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 a message box.

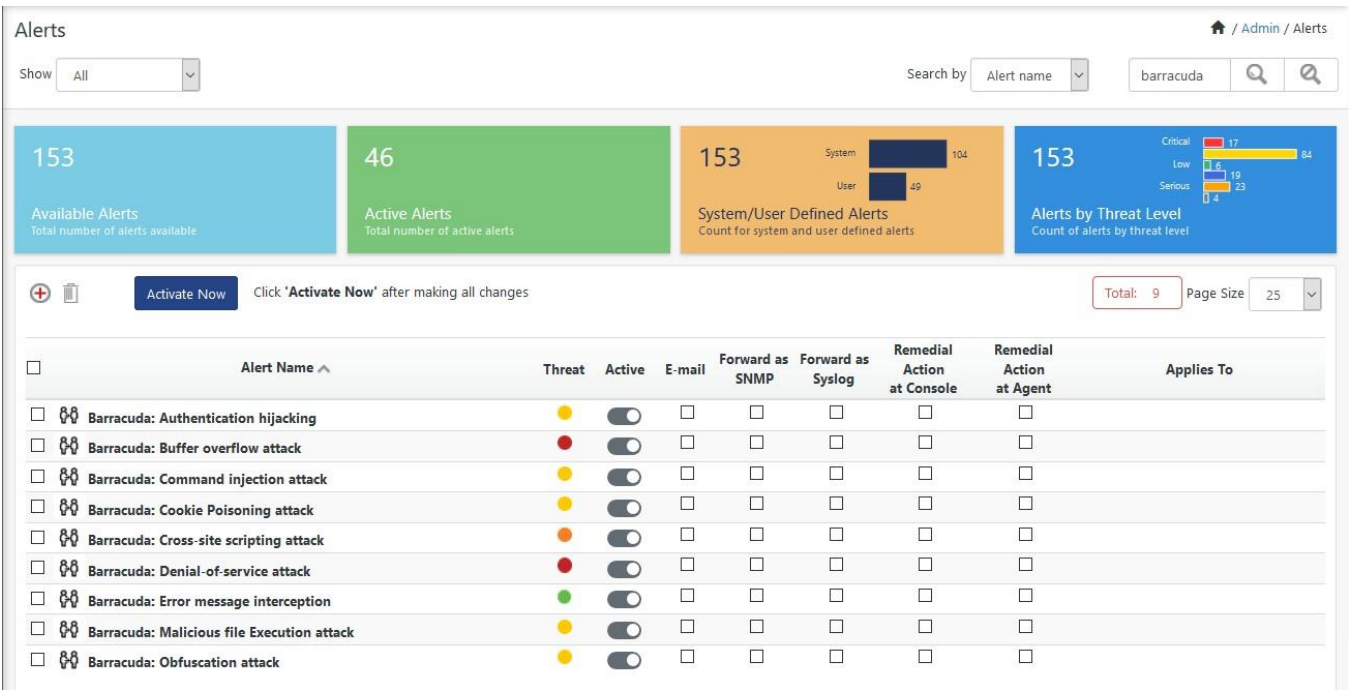


Figure 10

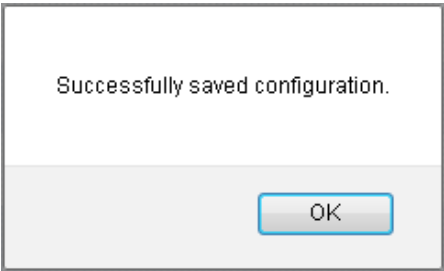


Figure 11

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

NOTE: Specify appropriate **systems** in the **alert configuration** for better performance.