

How to – Configure Barracuda NextGen Firewall X logs to EventTracker

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

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:

10.0.10.70

Hostname or IP address of receiver.

Protocol/Port:

UDP

514

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