Netsurion | EventTracker®

How to – Configure Barracuda NextGen Firewall X logs to EventTracker

EventTracker v9.0 and Above

Publication Date: November 25, 2019

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.

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.**

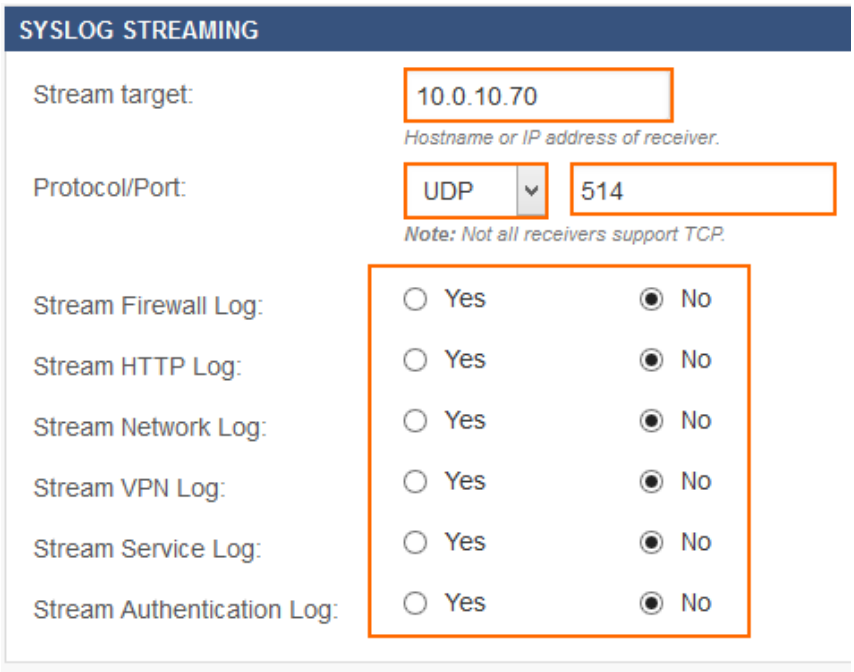
SYSLOG STREAMING
Stream target:
10.0.10.70
Hostname or IP address of receiver.
Protocol/Port:
UDP
514
Note: Not all receivers support TCP.
Stream Firewall Log:
Stream HTTP Log:
Stream Network Log:
Stream VPN Log:
Stream Service Log:
Stream Authentication Log:
Yes
No

Figure 1