![Netsurion logo] **Netsurion**®
Powering Secure and Agile Networks

How-To Guide

Configuring Barracuda Web Security Gateway to Forward Logs to EventTracker

EventTracker v9.2 and later

Publication Date:

March 26, 2021

Abstract

This guide provides instructions to retrieve the **Barracuda Web Security Gateway** events. Once **EventTracker** is configured to collect and parse these logs, the dashboard and reports can be configured to monitor **Barracuda WSG**.

Scope

The configuration details in this guide are consistent with EventTracker version 9.2 or above and **Barracuda Web Security Gateway.**

Audience

Administrators who are assigned the task to monitor **Barracuda Web Security Gateway** events using EventTracker.

Table of Contents

1. Overview

The Barracuda Web Security Gateway lets organizations benefit from online applications and tools without exposure to web-borne malware and viruses, lost user productivity, and misused bandwidth.

Barracuda WSG logs can be integrated with EventTracker via syslog. Barracuda WSG can send events like user login failure, configuration changes, allowed traffic, blocked traffic, malware activities detected, and malware blocked, etc. It created detailed reports for user login failure, configuration changes, malware activities, web traffic allowed, and web traffic blocked. Its graphical representation shows the malicious URL's blocked by reason, malware detected by IP address, configuration changes by usernames, etc.

EventTracker triggers alerts in the event when a malware is detected, changes in configuration by any user, or an unsuccessful user login.

2. Prerequisites

- Barracuda Web Security Gateway version 610,710,810,910,1010.
- Barracuda Web Security Gateway firmware version 11.0.0.019.
- An exception should be added into windows firewall on EventTracker machine for syslog port 514.

3. Integrating Barracuda Web Security Gateway Events to EventTracker Server

To enable syslog reporting on your Barracuda Web Security Gateway:

- Log into the web interface as **Admin**.
- Navigate to the **Advanced >> Syslog** page.
- For both the **Web Traffic Syslog** and **Web Interface Syslog**, enter the **IP address** (192.168.1.1) of the **EventTracker** with **port 514** to which you want to direct messages.

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's cybersecurity platforms enable companies to deliver on both. Netsurion's approach of combining purpose-built technology and an ISO-certified security operations center gives customers the ultimate flexibility to adapt and grow, all while maintaining a secure environment.

Netsurion's EventTracker cyber threat protection platform provides SIEM, endpoint protection, vulnerability scanning, intrusion detection and more; all delivered as a managed or co-managed service. Netsurion's BranchSDO delivers purpose-built technology with optional levels of managed services to multi-location businesses that optimize network security, agility, resilience, and compliance for branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit netsurion.com or follow us on Twitter or LinkedIn. Netsurion is #19 among MSSP Alert's 2020 Top 250 MSSPs.

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)
EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3)
EventTracker Essentials SOC: 877-333-1433 (Option 4)
EventTracker Software Support: 877-333-1433 (Option 5)
https://www.netsurion.com/eventtracker-support