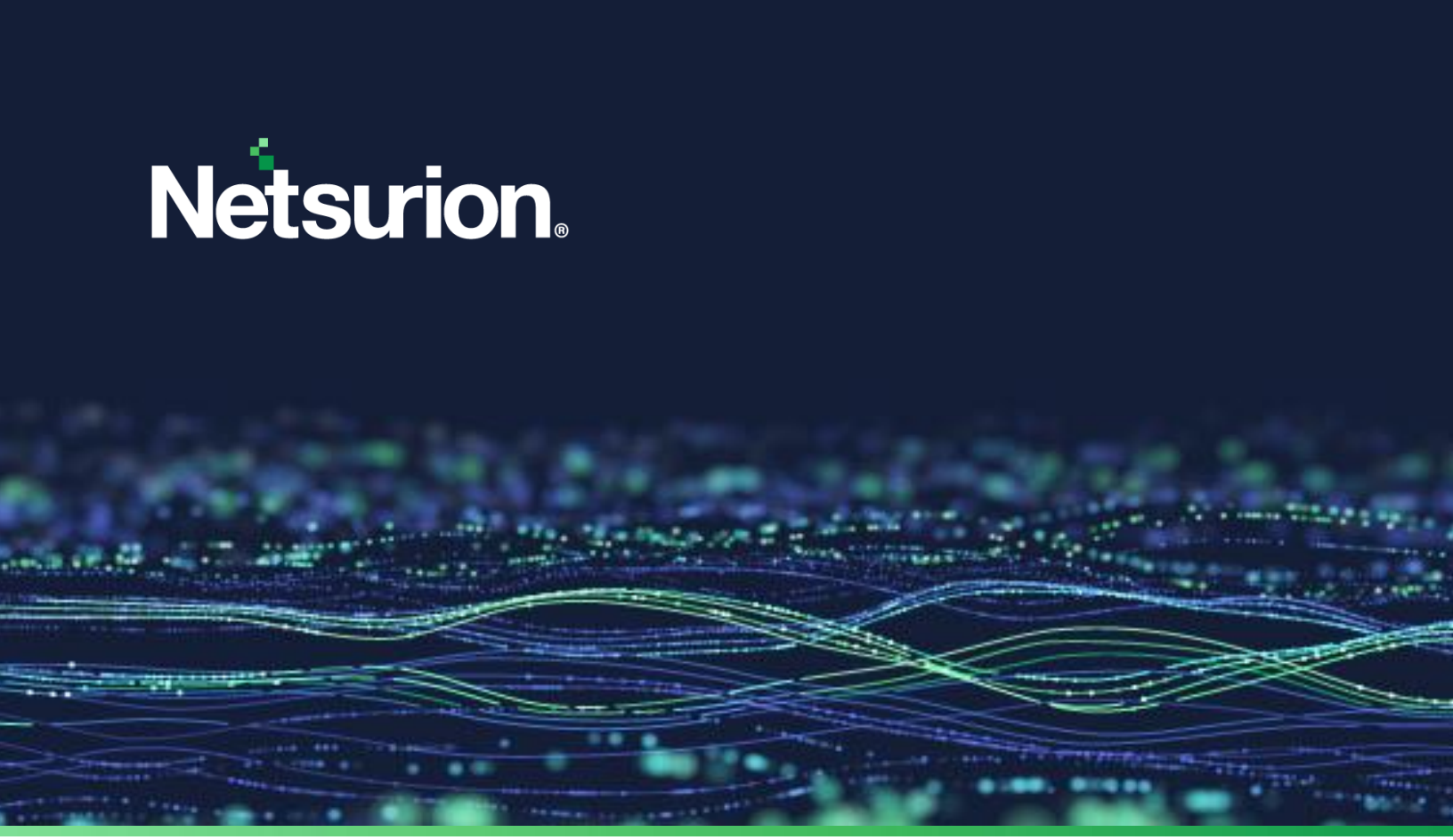

Integration Guide

Integrate Barracuda Email Security Gateway with the Netsurion Open XDR platform

Publication Date

March 13, 2023

Abstract

This guide provides instructions to configure and integrate the Barracuda Email Security Gateway with the Netsurion Open XDR platform to retrieve its event logs via syslog and forward them to the Netsurion Open XDR platform.

Note:

The screen/ figure references are only for illustration purpose and may not match the installed product UI.

Scope

The configuration details in this guide are consistent with Barracuda Email Security Gateway and the Netsurion Open XDR platform version 9.3 or later.

Audience

This guide is for the administrators responsible for configuring and monitoring Barracuda Email Security Gateway in the Netsurion Open XDR platform.

Product Terminology

The following terms are used throughout this guide:

- The term “Netsurion’s Open XDR platform” or “the Netsurion Open XDR platform” or “the Open XDR platform” refers to EventTracker.
- The term “Data Source Integrations” refers to Knowledge packs.

Table of Contents

1 Overview

The Barracuda Email Security Gateway is an integrated hardware and software solution designed to protect the email server from spam, virus, spoofing, phishing, and spyware attacks. Outbound filtering and encryption options also prevent Data Leakage Prevention (DLP). The optional cloud protection layer (CPL) shields email servers from inbound malware and DoS attacks while filtering out normal spam before it ever touches the network's perimeter.

The Netsurion Open XDR platform facilitates monitoring events retrieved from Barracuda Email Security Gateway. The alerts, reports, dashboard, and saved search in the Netsurion Open XDR platform benefit in detecting any suspicious activities.

2 Prerequisites

- The Barracuda Email Security Gateway v6.0 or above must be installed and configured.
- An exception must be added to the windows firewall on the Netsurion Open XDR machine for syslog port **514**.
- The Data Source Integrator package.

> **Note**
>
> To get the Data Source Integrator package, contact your Netsurion Account Manager

3 Integrating Barracuda Email Security Gateway with the Netsurion Open XDR platform

1. Log in to the Barracuda Web Filter web interface and go to **Advanced** > **Advanced Networking**.
2. In the **Syslog Configuration** section, specify the **FQDN/ IP address (FQDN recommended)** of the Netsurion Open XDR in the Mail Syslog and Web Interface Syslog fields.
3. Enter port **514** and select **UDP** protocol.
4. Click **Add** and **Save** to confirm the syslog configuration details.

4 Data Source Integrations (DSIs) in the Netsurion Open XDR platform

After the logs are received by the Netsurion Open XDR platform, configure the Data Source Integrations in the Netsurion Open XDR platform.

The Data Source Integrations package contains the following files for the Barracuda Email Security Gateway.

- Categories_Barracuda ESG.iscat
- Alerts_Barracuda ESG.isalt
- Reports_Barracuda ESG.etcrx
- KO_Barracuda ESG.etko
- Dashboards_Barracuda ESG.etwd

Note

Refer the How To Configure DSI guide for the procedures to configure the above DSIs in the Netsurion Open XDR platform.

Data Source Integrations Details

4.1 Alerts

Name	Description
Barracuda ESG: Malicious file detected in email	This alert is generated whenever any virus is detected in the email attachment.

4.2 Reports

Name	Description
Barracuda ESG - Email Traffic details	This report provides detailed information on inbound, outbound, email scan and email statistics, including hostname, sender email address, recipient email, hostname, source IP address, the action was taken on malicious activity and subject of the email. This report makes it easier to sort through sensitive audit data to determine the scenarios (clarifying the questions of who did what, when, where, and how) to satisfy audits for various industry regulatory requirements.
Barracuda ESG - Virus detection in emails	This report provides the information about any virus detected in the email attachment, including the details of sender and recipient address.

4.3 Dashboard

Name	Description
Barracuda ESG - Action taken on inbound emails	This dashlet displays the actions taken on inbound emails with their sender and recipient address.
Barracuda ESG - Action taken on outbound emails	This dashlet displays the actions taken on outbound emails with their IP address.
Barracuda ESG - Emails blocked by geolocation	This dashlet displays the emails blocked by geolocation.
Barracuda ESG - Virus detection by sender address	This dashlet displays virus detected by sender address.
Barracuda ESG - Spam emails detail	This dashlet displays all the spam emails with their sender and recipient address.

4.4 Saved Search

Name	Description
Barracuda ESG - Email Traffic details	This saved search provides detailed information on inbound, outbound, email scan and email statistics, including hostname, sender email address, recipient email, hostname, source IP address, the action was taken on malicious activity and subject of the email. This saved search makes it easier to sort through sensitive audit data to determine the scenarios (clarifying the questions of who did what, when, where, and how) to satisfy audits for various industry regulatory requirements.
Barracuda ESG - Virus detection in the email	This saved search provides the information about any virus detected in the email attachment, also provides the details of sender and recipient address.

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's managed offering includes our 24x7 SOC that operates as your trusted cybersecurity partner, working closely with your IT team to strengthen your cybersecurity posture. Our solution delivers Managed Threat Protection so you can confidently focus on your core business.

Headquartered in Ft. Lauderdale, FL with a global team of security analysts and engineers, Netsurion is a leader in Managed Detection and Response (MDR) and a Top 25 Global MSSP. Learn more at www.netsurion.com.

Contact Us

Corporate Headquarters

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

Contact Numbers

Direct Enterprise	SOC@Netsurion.com	1 (877) 333-1433 Option 1, Option 1
MSP Enterprise	SOC-MSP@Netsurion.com	1 (877) 333-1433 Option 1, Option 2
Essentials	Essentials-Support@Netsurion.com	1 (877) 333-1433 Option 1, Option 3
Self-Serve	EventTracker-Support@Netsurion.com	1 (877) 333-1433 Option 1, Option 4

https://www.netsurion.com/eventtracker-support