Integration Guide

Integrate AWS WAF with Netsurion Open XDR

Publication Date

December 12, 2023

Abstract

This guide provides instructions to configure and integrate AWS WAF with Netsurion Open XDR to receive the logs from AWS WAF.

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 Netsurion Open XDR version 9.3 or later and AWS WAF.

Audience

This guide is for the administrators responsible for configuring and monitoring AWS WAF in Netsurion Open XDR.

Table of Contents

1 Overview

AWS Web Application Firewall (WAF) facilitates monitoring web requests forwarded to the Amazon CloudFront distributions or other resources like the Elastic Load Balancer or the API Gateway. It allows or blocks requests based on specific conditions, such as the IP addresses in the form of allowlists or blocklists, regular expressions, and more.

Netsurion Open XDR manages the logs retrieved from AWS WAF. The alerts, reports, dashboards, and saved searches in Netsurion Open XDR are enhanced by capturing the important and critical activities in AWS WAF.

2 Prerequisites

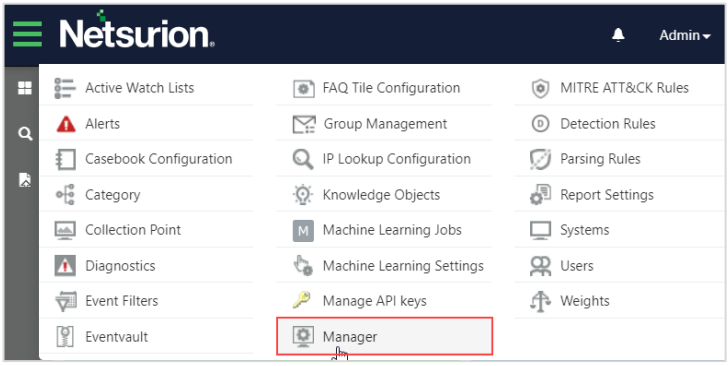
- Configure AWS WAF to forward logs to Netsurion Open XDR.

> **Note**
>
> Refer the How-To guide to configure AWS WAF to forward logs to Netsurion Open XDR.

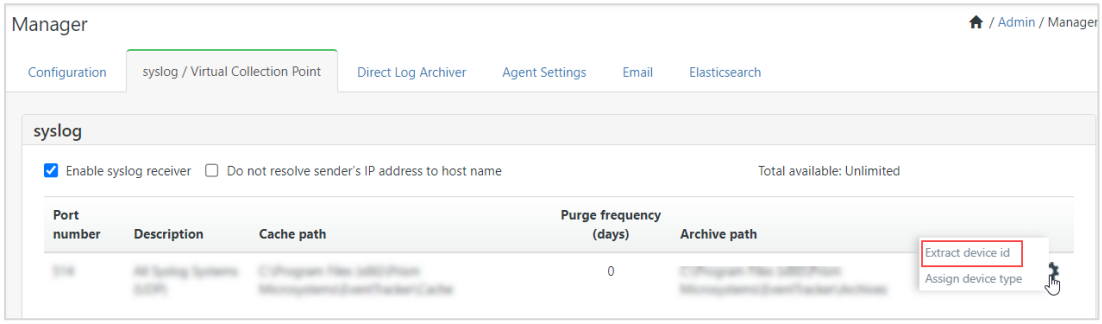
3 System Extraction

Perform the following steps for System extraction.

1. In the Netsurion Open XDR interface, hover over the **Admin** menu and click **Manager.**



2. In the **Manager** interface, go to **syslog/ Virtual Collection Point** > **syslog,** hover over the **Gear** icon located adjacent to it, and then click **Extract device id** to extract the system name.



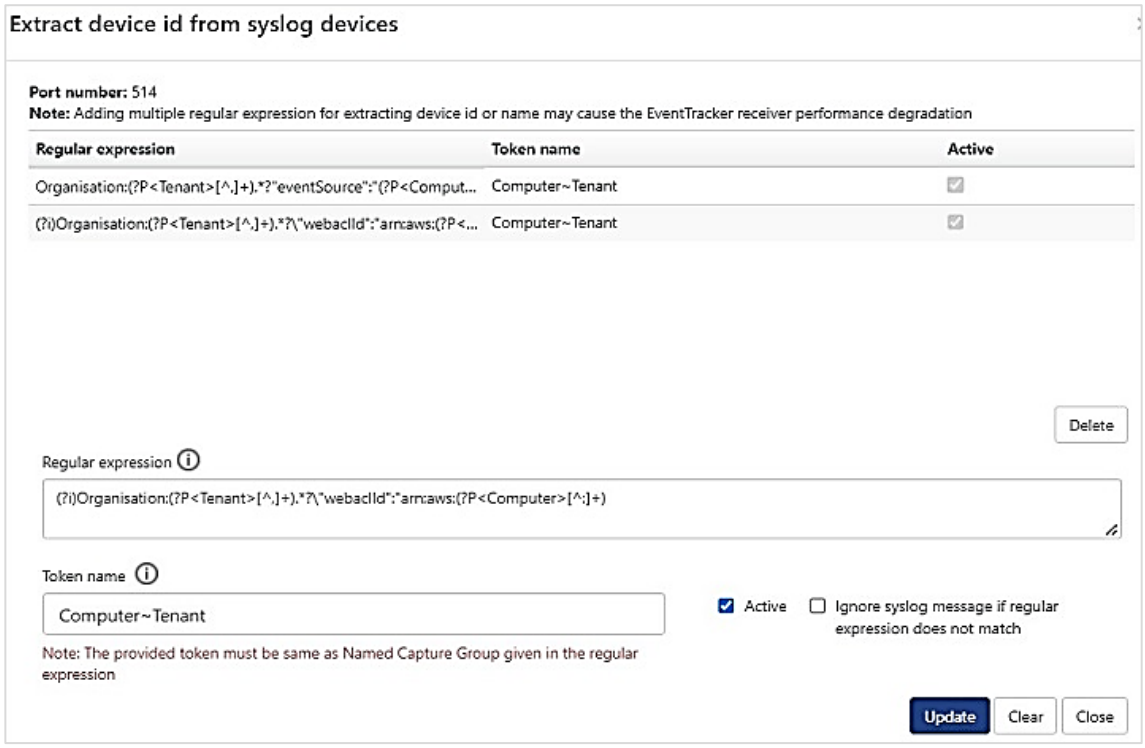
3. In the **Extract device id** interface, **Add** the following regex details for CloudTrail logs and AWS WAF logs and click **Update** to save the extraction logic details.

   Regular expression: Organisation:(?P<Tenant>[^,]+).*?"eventSource":"(?P<Computer>[^"]+)

   Token Name: Computer~Tenant

   Regular expression: (?i)Organisation:(?P<Tenant>[^,]+).*?\"webaclId":"arn:aws:(?P<Computer>[^:]+)

   Token Name: Computer~Tenant



4 Data Source Integration (DSI) in Netsurion Open XDR

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

The Data Source Integrations package contains the following DSI assets for **AWS WAF.**

- Alerts_AWS WAF.isalt
- Categories_AWS WAF.iscaf
- Dashboards_AWS WAF.etwd
- KO_AWS WAF.etko
- Reports_AWS WAF.etcrx

Note

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

The following are the key assets available in this Data Source Integration.

4.1 Alerts

Name	Description
AWS WAF: Potential SSL downgrade detected	Generated whenever an obsolete or vulnerable version of SSL/TLS makes the API calls.
AWS WAF: Rule manipulation detected	Generated whenever a WebACL configuration is deleted or maliciously modified.
AWS WAF: Configuration override detected	Generated whenever an exception(s) or update(s) is made to WebACLs related to WAF detections.

4.2 Reports

Name	Description
AWS WAF - Activity overview	Provides details of all console activities in the AWS WAF service.
AWS WAF - Traffic details	Provides details of malicious attacks detected by the AWS WAF service.

4.3 Dashboards

Name	Description
AWS WAF - Configuration modification detected	Displays information about modifications in AWS WAF configurations.
AWS WAF - Blocked traffic by country	Displays information about all the blocked requests in the country.
AWS WAF - Blocked traffic by geolocation	Displays information about all the blocked requests in the geolocation.
AWS WAF - Blocked traffic by userAgent	Displays information about the blocked requests from the user.
AWS WAF - Critical activities detected	Displays information about any deletion and disassociate action performed in the AWS WAF configuration.
AWS WAF - Blocked traffic by malicious IP	Displays information about the blocked requests from User\IP.
AWS WAF - Threat breakdown by hosts	Displays information about the host that was affected in AWS WAF.

AWS WAF - Traffic trend	Displays information about the allowed and blocked requests in AWS WAF.
AWS WAF - Http request type	Displays information about the HTTP request that hits the browser.

About Netsurion

Netsurion® delivers an adaptive managed security solution that integrates our Open XDR platform with your existing security investments and technology stack, easily scaling to fit your business needs. Netsurion's 24x7 SOC 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 & Response (MXDR). 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

Use the form to submit your technical support tickets. Or reach us directly at 1 (877) 333-1433

Managed XDR Enterprise Customers	SOC@Netsurion.com
Managed XDR Enterprise MSPs	SOC-MSP@Netsurion.com
Managed XDR Essentials	Essentials@Netsurion.com
Software-Only Customers	Software-Support@Netsurion.com

https://www.netsurion.com/support