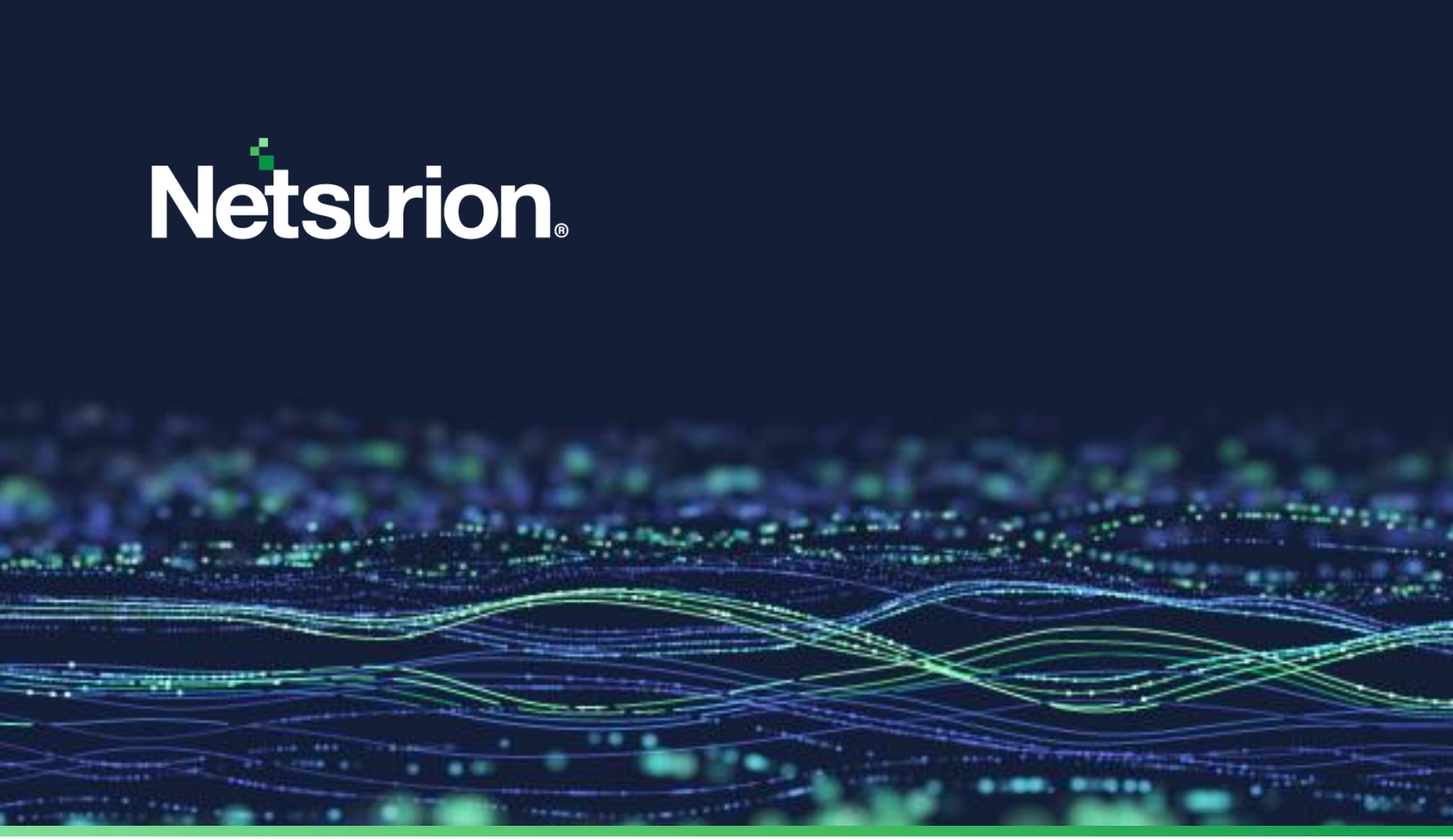


How-To Guide

Integrate Azure Firewall with Netsurion Open XDR

Publication Date

October 10, 2023

Abstract

This guide provides instructions to configure and integrate Azure Firewall with Netsurion Open XDR to retrieve its logs via Azure event hub and forward them to Netsurion Open XDR.

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 Azure Firewall and Netsurion Open XDR 9.3 or later.

Audience

This guide is for the administrators responsible for configuring and monitoring Azure Firewall in Netsurion Open XDR.

Table of Contents

1 Overview

Azure Firewall is a cloud-based network security service provided by Microsoft Azure. It acts as a high-level, scalable network security solution that allows to control and monitor network traffic flowing in and out of Azure Virtual Network (VNet).

Netsurion Open XDR manages logs retrieved from Azure Firewall through Azure event hub. The alerts, reports, dashboards, and saved searches in Netsurion Open XDR are enhanced by capturing important and critical activities in Azure Firewall.

2 Prerequisites

- Azure subscription with Global Administrator access.
- Azure Resource group.
- The Data Source Integration package.

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

3 Integrating Azure Firewall with Netsurion Open XDR

Integrate Azure Firewall with Netsurion open XDR by streaming the logs to the Azure Event Hub, and from Azure Event Hub to Netsurion Open XDR using the Function App.

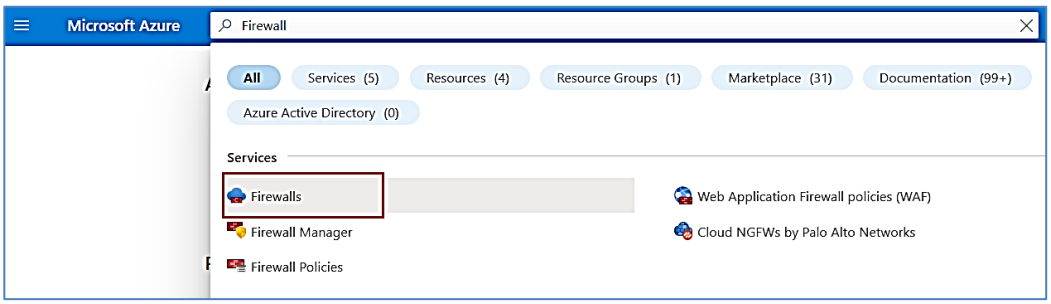
3.1 Create Event Hub and Function App

Refer to the configuration of Event Hub and Function App to forward logs to Netsurion open XDR.

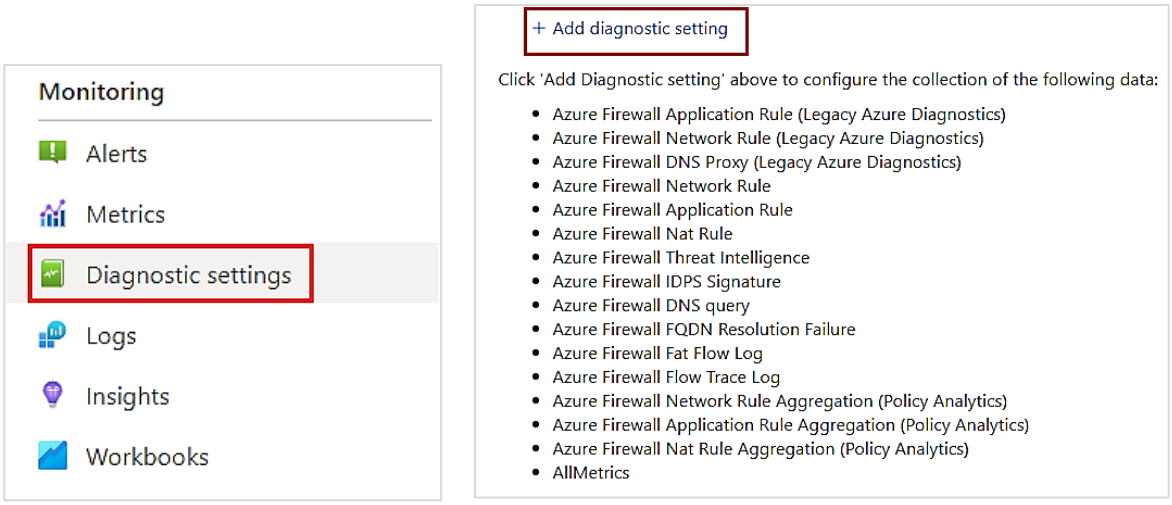
3.2 Configuring Azure Firewall to stream events to Event Hub

To configure Microsoft Azure Firewall to stream events to Event Hub, as an Administrator

1. Log in to Microsoft Azure and create an event hub namespace.
2. In the **Microsoft Azure** console, click **All** services, then search and click **Firewalls**.



3. Then, select the appropriate Firewall from the available lists to monitor.
4. From the left panel, go to **Monitoring** > **Diagnostics settings** and click **Add diagnostics setting.**



Note

The log categories for **Azure Firewall Threat Intelligence** and **Azure Firewall IDPS Signature** are available only for Azure Firewall with **Premium SKU**.

5. In the **Diagnostic setting** interface, specify the following details.
   - Provide the **Diagnostics settings name**, such as **Netsurion_Azurefirewall**.
   - From the left of the interface, in the **Logs** section, select the following logs.
     - Azure Firewall Network Rule
     - Azure Firewall Application Rule
     - Azure Firewall Threat Intelligence
     - Azure Firewall IDPS Signature
     - Azure Firewall DNS query
     - Azure Firewall FQDN Resolution Failure
   - From the right of the interface, in the **Destination details** section, select **stream to an Event Hub** and then choose the following.
     - **Subscription:** Select the desired Azure subscription.
     - **Event Hub namespace:** Select the Event Hub namespace.
     - **Event Hub name:** Select Event Hub created under Event Hub namespace.
     - **Event Hub policy name:** Select the Event Hub policy.
6. After providing all the details, click **Save**.

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 files for Azure Firewall.

- Categories_Azure Firewall.iscat
- Alerts_ Azure Firewall.isalt
- Reports_ Azure Firewall.etcrx
- KO_ Azure Firewall.etko
- Dashboards_ Azure Firewall.etwd

IMPORTANT

Enable the following specified Alerts, Dashboard, Reports, and Saved Searches only if the Azure Firewall is configured with Premium SKU.

Alerts	Azure Firewall: IDPS event detected Azure Firewall: Suspicious event detected
Dashboard	Azure Firewall - IDPS detected by source IP address
Reports	Azure Firewall - Threat intelligence events Azure Firewall - IDPS events
Saved Searches	Azure Firewall - Threat intelligence events Azure Firewall - IDPS events

Note

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

4.1 Alerts

Name	Description
Azure Firewall: IDPS event detected	Generated when an event, such as IDPS events which high and medium severity is detected by Azure Firewall.
Azure Firewall: Suspicious event detected	Generated when an event, such as threat intelligence event is detected by Azure Firewall.

4.2 Reports

Name	Description
Azure Firewall - DNS proxy events	Provides details about all the DNS proxy events log data monitored by Azure Firewall. This includes information such as, source IP address, port number, action, error message, response codes, query details.
Azure Firewall - Internal FQDN failure events	Provides details about the internal firewall FQDN resolution request failure events monitored by Azure Firewall. This includes information such as, server IP address, port number, failure reason.
Azure Firewall - Threat intelligence events	Provides details about threat intelligence events monitored by Azure Firewall. This includes information such as source IP address, destination IP address, port number, threat description, FQDN, action.
Azure Firewall - Traffic events	Provides details about network and application events monitored by Azure Firewall. This includes information such as, action, source IP address, destination IP address, port number, target URL, FQDN.
Azure Firewall - IDPS events	Provides details about all the data plane packets that were matched with one or more IDPS signatures monitored by Azure Firewall. This includes information such as, source IP address, port number, severity, IDPS signature id, signature description, action, source system.

4.3 Dashboards

Name	Description
Azure Firewall - DNS query by response codes	Displays all the failed DNS query by response codes.
Azure Firewall - Action by source IP address	Displays all the source IP address of the blocked and allowed events.
Azure Firewall - IDPS detected by source IP address	Displays all the IDPS events detected based on source IP address.

4.4 Saved Searches

Name	Description
Azure Firewall - DNS proxy events	Provides details about all the DNS proxy events log data monitored by Azure Firewall.
Azure Firewall - Internal FQDN failure events	Provides details about the internal firewall FQDN resolution request failure events monitored by Azure Firewall.
Azure Firewall - Threat intelligence events	Provides details about threat intelligence events monitored by Azure Firewall.
Azure Firewall - Traffic events	Provides details about network and application events monitored by Azure Firewall.
Azure Firewall - IDPS events	Provides details about all the data plane packets that were matched with one or more IDPS signatures monitored by Azure Firewall.

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