TECHNICAL
DOCUMENTATION

Fortinet Integration Guide

This guide describes how to set up and configure the Illumio and Fortinet integration.

Overview

Onboarding and Integration

Reference

Table of Contents

About the Illumio and Fortinet Integration

The Illumio - Fortinet integration enables organizations to ingest flow logs from both on-prem and cloud-based Fortinet FortiGate firewalls directly into Illumio Insights. By centralizing Fortinet telemetry within the Illumio platform, you gain unified visibility across your hybrid network, a baseline for your traffic behavior, and the capability to rapidly identify security gaps, misconfigurations, and early indicators of potential breaches.

This integration currently supports two integration methods:

NOTE
You must enable syslog monitoring for both methods of sending Fortinet logs.

- Ingest Syslogs directly from Fortinet (Recommended).

  FortiGate devices natively support syslog forwarding. Fortinet firewalls send their traffic logs directly to the Illumio Syslog Service over mTLS. After the logs reach the Syslog Service, the Illumio platform automatically processes, normalizes, and ingests the data into Illumio Insights.

  To enable this method, you must configure FortiGate and FortiManager to:

  - Enable traffic-log generation for all required firewalls.
  - Configure syslog forwarding using mTCP with TLS.
  - Point the log stream to your Illumio Syslog endpoint.
- Route Fortinet logs from Cribl to Azure Event Hub.

  For environments that are already using Cribl Stream as a centralized logging pipeline, Illumio supports routing Fortinet logs directly from Cribl directly to the Illumio-hosted Azure Event Hub. This option is ideal for when you prefer to decouple log collection from their firewalls, already have Cribl deployed, or need advanced routing, filtering, or transformation capabilities before logs reach Illumio.

  Note the following about using the Cribl method:

  - This method is supported for select customers only. Contact Illumio Support for approval.
  - You must configure Cribl with the Azure Event Hub connection string and namespace provided to you.

Prerequisites for the Illumio and Fortinet Integration

To onboard Fortinet, take the following actions to make sure that logs are properly formatted, aggregated, enriched, and securely transmitted:

□ You must have a Fortinet account with admin credentials to log into FortiGate or FortiManager to configure the syslog server.

□ All Fortinet clients must allow logs to be forwarded from the firewall or log server. You must ensure that the necessary network connectivity exists to successfully integrate with the Illumio Syslog Service. To generate and export Common Event Format (CEF) logs from Fortinet to a syslog server, you must configure a log-forwarding profile and a syslog server profile.

Performing all of these tasks makes sure that the Fortinet logs flow into the Illumio Platform in a secure and structured manner so that you can view the log data and create enforcement policies.

Preinstallation Tasks

Before you onboard the Log Exporter, do the following:

- Create a certificate signing request using your organization's private key.

Onboarding the Fortinet Connector with the Log Exporter

1. Within Illumio Console, navigate to **Connectors** and click the **Add Fortinet** tile.
2. On the **Fortinet Connector** page, in the Fortinet tile, click **+ Add Log Exporter**.
3. In the **Add Log Exporter** pane, under **Upload Certificate Signing Request**, either drag and drop your CSR or click **Choose File** and upload it. See
4. Click **Download** to download the signed certificate and Illumio root certificate.
5. Enter the target name in the **Target Name** field and click **Save**.

   > **NOTE**
   > The other field values in the **Add Log Exporter** pane are prepopulated.

   The **Log Exporter Added** status message displays and the Log Exporter appears as Active in the **Log Exporter** table.

Importing Certificates

Import the Illumio signed certificate and the Illumio root certificate that you downloaded from Illumio into FortiManager. See the following Fortinet documentation:

- CA Certificates
- Local Certificates

Add a Remote Syslog Server and Enable FortiManager to Send Local Logs to the Syslog Server

In FortiManager, navigate to System Settings > Advanced > Syslog Server and add a remote syslog server with the following values:

- **Name:** Enter a valid name
- **FQDN/IP:** Syslog.illum.io
- **Syslog Server Port:** 6514
- **Reliable Connection:** Yes
- **Secure Connection:** Yes
- **Local Certificate CN:** Use the certificate that you imported
- **Peer Certificate CN:** Use the certificate that you imported

Next, use FortiManager to configure each FortiGate instance to include the following values, using the following Fortinet instructions: Device DB CLI Configurations

- **format:** cef
- **ssl-min-proto-versio**n: TLSv1-2
- **custom-log-field:** TenantId = Obtain this value from the Log Exporter

Enable Cribl to Send Fortinet Firewall Logs to Azure Event Hub

Use the following procedures to allow Cribl Stream to send Fortinet firewall logs to the Illumio-hosted Azure Event Hub.

> **NOTE**
> For Cribl, use the current Fortinet log format instead of Common Event Format (CEF).

1. In Cribl Stream, add a Data Destination with the following values to the Azure Event Hub that you use for Illumio Insights:
   a. **Output ID:** Enter a unique name to identify the Azure Event Hubs definition.
   b. **Brokers:** arch-eventhub.servicebus.windows.net:9093
   c. **Event Hub Name:** rsyslog-logs
   d. **TLS:** Enabled
   e. **Authentication:** Enabled
   f. **SASL Mechanism:** PLAIN
   g. **Username:** $ConnectionString
   h. **Password:** Will be provided in a separate email. It is the full Event Hub connection string (usually starts with Endpoint=sb.//...;SharedAccessKeyName=...;SharedAccessKey=...).
2. Add a Data Route with the following values to the Data Destination that you created:
   a. **Route Name:** Enter a unique name for the route.
   b. **Pipeline:** Select a value.
   c. **Destination:** Select the Destination Name (Output ID) that you created in Step 1.a.

Adding the API Connector

1. Within Illumio Console, navigate to the **Connectors** page and click the **Fortinet** tile.
2. Click **Add API Connector**.
3. In the **Add API Connector** pane, enter the following values:
   a. Enter your user ID in the **Fortinet User ID** field.
   b. Enter your password in the **Fortinet Password** field.
   c. Enter the API URL in the **Fortinet API URL** field. This will be the URL plus the token.

   > **NOTE**
   > To test your connection, click **Test Connection**.

4. Click **Save**.
   The values that you entered display in the **API Connector** pane.

Reference: CEF Fields Required by Illumio Insights

Firewall traffic logs that are sent to Illumio Insights must be in CEF format.

Field Name	Description	Required
deviceVendor	The vendor of the device that is generating the log	Yes
deviceExternalId	The external identifier for the device	Yes
cs1Label	Custom string 1 label (tenant identification)	Yes
act	The action taken by the device or application	Yes
src	Source IP address of the connection	Yes
dst	Destination IP address of the connection	Yes
proto	Protocol number used	Yes
spt	Source port number	Yes
dpt	Destination port number	Yes
out	Bytes sent from source to destination	Yes
in	Bytes received at destination	Yes
conn_direction	Direction of the connection	Yes
outzone	Network security zone of the destination	Yes
inzone	Network security zone of the source	Yes
rule_uid	Primary key for rule metadata lookup	Yes
cs2Label	Rule Name indicator Use cs2Label and cs2 for Rule Name	Yes
cs2	Rule Name Use cs2 for Rule Name	Yes
cs3Label	Policy Name indicator Use c3Label and cs3 for Policy Name	Yes
cs3	Actual Policy Name Use cs3 for Policy Name	Yes

For more information about the fields available for Check Point, Fortinet, or Palo Alto Networks, see the documentation:

- Check Point: Check Point
- Fortinet: Fortinet
- Palo Alto Networks: Common Event Format (CEF) Configuration Guides