Firepower Integrations Overview Guide

First Published: 2021-12-01

Firepower Integrations Overview Guide

This guide provides instructions to integrate Firepower Threat Defence (FTD) devices with each of the following tools for event analysis:

- Cisco SecureX
- Cisco SecureX threat response
- Cisco Event Streamer
- Splunk
- IBM QRadar
- Cisco Security Analytics and Logging (On Premises and SaaS)

Based on the event analysis tool and the type of integration that is required, you can use either FMC or FDM-managed FTD devices to perform the integration. This guide includes instructions to integrate FTD devices that are managed by either the Firepower Management Center (FMC) or Firepower Device Management (FDM), as applicable.

Use Cases

This section lists generic use cases along with the tools that are used to perform the integration.

Use Case	Solution	Minimum supported Firepower release	More Information
You want to unify visibility, enable automation, and strengthen your security across network, endpoints, cloud, and applications--all without replacing your current security infrastructure or layering on new technology.	Cisco SecureX	6.3	Integrate with Cisco SecureX

Use Case	Solution	Minimum supported Firepower release	More Information
You want to combine investigation and response capabilities into one efficient workbench, speed up cyber investigations significantly, and take corrective action immediately.	Cisco SecureX threat response	6.3	Integrate with Cisco SecureX threat response
You want to stream host, discovery, correlation, compliance white list, intrusion, user activity, file, malware, and connection data from a Management Center.	Cisco Event Streamer (eStreamer)	6.0	Integrate with Cisco Event Streamer
You want to use Splunk to store threat and traffic data received from the FMC and use this data to discover and investigate threats.	Cisco Secure Firewall (formerly known as Firepower) App for Splunk	6.0	Integrate with Splunk
You want to analyze and contain threats to your network by providing insight from multiple security products in QRadar.	Cisco Firepower App for IBM QRadar	6.0	Integrate with IBM QRadar
You want to increase your on premises Firewall event data storage capacity, retain this data for a longer period of time, and export your event data to a Secure Network Analytics appliance.	Cisco Security Analytics and Logging (On Premises)	6.4	Integrate with Cisco Security Analytics and Logging (On Premises), on page 11

Use Case	Solution	Minimum supported Firepower release	More Information
You want to send Firepower events to the Cisco Secure Cloud Analytics (formerly known as Stealthwatch Cloud) for storage as you need more storage than what an on premises storage can provide, and optionally make your Firepower event data available for security analytics using Cisco Secure Cloud Analytics.	Cisco Security Analytics and Logging (SaaS)	6.4	Integrate with Cisco Security Analytics and Logging (SaaS), on page 13

Integrate with Cisco SecureX

SecureX is a simplified platform experience, connecting Cisco's integrated security portfolio with your existing infrastructure. It helps you unify visibility, enable automation, and strengthen security across your network, endpoints, cloud, and applications. SecureX is included with your Cisco security product purchase, and you can view data from all of your FTD devices in SecureX.

This integration sends supported events from Firepower devices to Cisco SecureX for analysis.

Type of Integrations

You can integrate FTD devices with SecureX using two different methods of integration:

- Direct integration – supported on FMC
- Syslog integration – supported on FMC and FDM

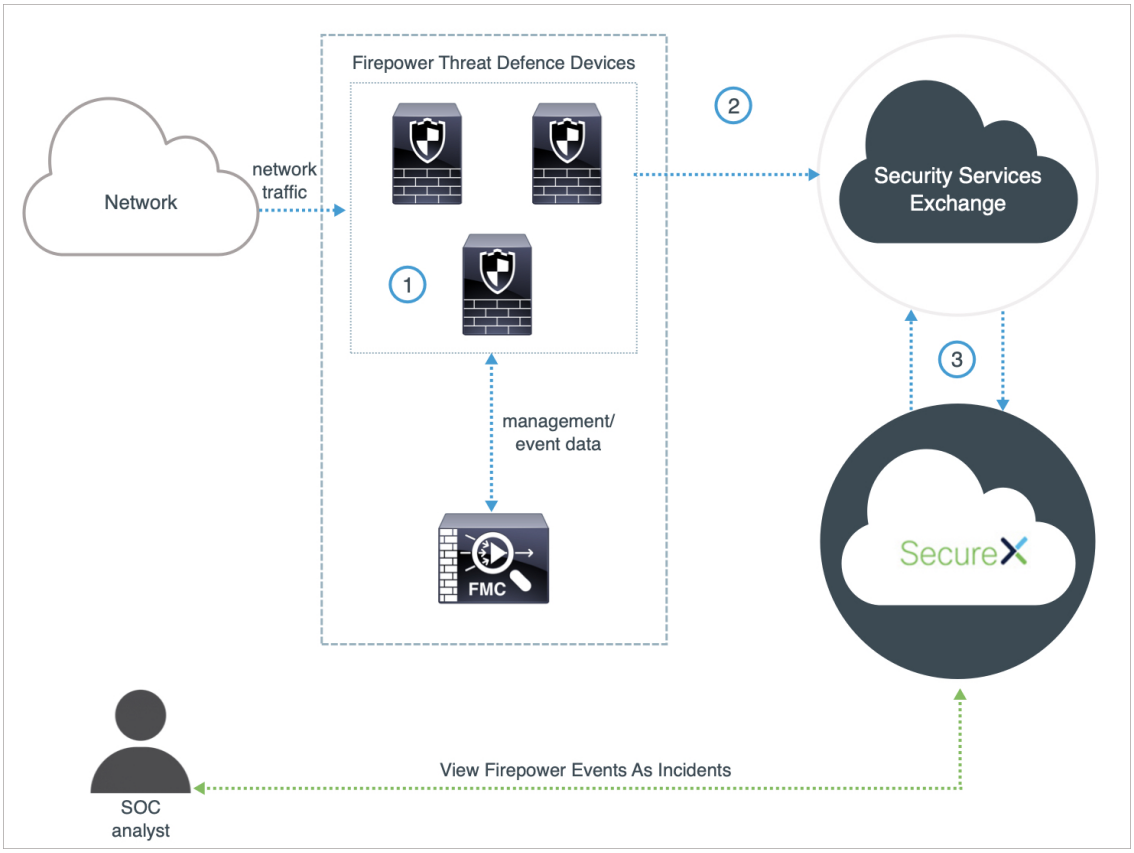
Direct Integration

You can configure your managed FTD devices to send supported events directly to the Security Services Exchange (SSE) in the Cisco cloud.

Supported Firepower user role to perform the integration: Administrator

Minimum supported Firepower release: 6.4 for the North America cloud and 6.5 for the Europe and Asia cloud

The following diagram shows how the direct integration works.



1	The FTD devices generate events.
2	The FTD devices send supported events to SSE.
3	SecureX queries SSE for sightings related to the IP address being investigated and provides the SOC analyst with the additional context. The events are automatically or manually promoted to incidents that appear in SecureX.

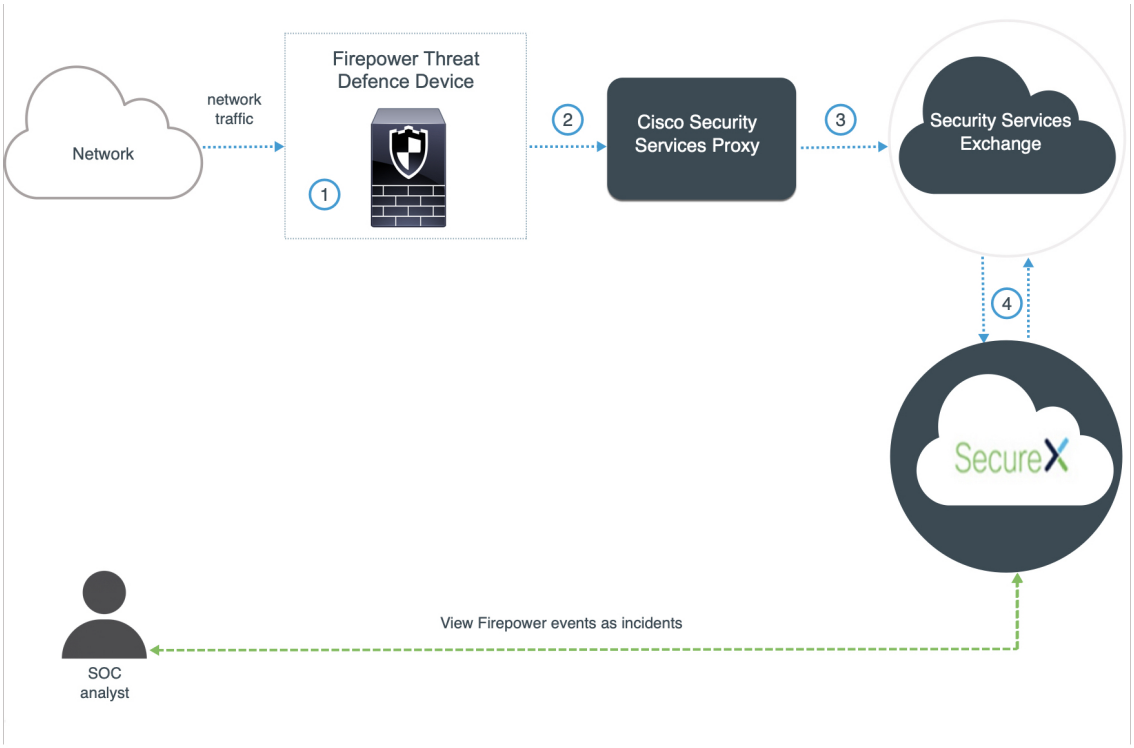
Syslog Integration

You can use syslog to send supported events to the Cisco cloud from Firepower devices.

Supported Firepower user role to perform the integration: Administrator

Minimum supported Firepower release: 6.3 for all cloud regions

The following diagram shows how the syslog integration works.



1	The FMC or FDM-managed FTD device generates events.
2	The FTD device sends the supported syslog events to the Cisco Security Services Proxy (CSSP) server.
3	Every 10 minutes, the CSSP forwards the collected events to the Security Services Exchange (SSE),
4	SecureX queries SSE for sightings related to the IP address being investigated and provides the SOC analyst with the additional context. The events are automatically or manually promoted to incidents that appear in SecureX.

Comparison of Methods for Sending Events to the Cloud

Firepower devices make events available to SecureX via the Security Services Exchange portal, either using syslog or directly.

Sending Directly	Sending via Syslog Using Proxy
Supports only Firepower Threat Defense(NGFW) devices running supported versions of Firepower software	Supports all devices running supported versions of Firepower software
Supports Firepower 6.4 and later	Supports Firepower 6.3 and later
Supports all event types listed in Supported Event Types	Supports only intrusion events.

Sending Directly	Sending via Syslog Using Proxy
Supports SecureX tiles that show system status information such as whether your appliances and devices are running the optimal software versions	System status features are not supported with syslog-based integrations
Firepower Threat Defense devices must be connected to the internet	Firepower devices do not need to be connected to the internet
Your Firepower deployment cannot be using a Smart Software Manager On-Prem server (formerly known as a Smart Software Satellite Server.)	Your deployment can be using a Smart Software Manager On-Prem server.
No need to set up and maintain an on-premises proxy server	Requires an on-premises virtual Cisco Security Services Proxy (CSSP) server. More information about this proxy server is available from the online help in Security Services Exchange (SSE). To access SSE, see Access Security Services Exchange.

For more information on integrating Firepower devices with SecureX, see the following guides:

- Cisco Firepower Management Center and SecureX Integration Guide.
- Cisco Firepower and SecureX Integration Guide.

Integrate with Cisco SecureX threat response

Cisco SecureX threat response (formerly Cisco Threat Response or CTR) is the platform in the Cisco cloud that helps you detect, investigate, analyze, and respond to threats using data aggregated from multiple products and sources.

This integration sends supported events from Firepower devices to Cisco SecureX threat response for analysis alongside data from your other products and other sources.

Type of Integrations

You can integrate FTD devices with Cisco SecureX threat response using two different methods of integration:

- Direct integration – supported on FMC
- Syslog integration – supported on FMC and FDM

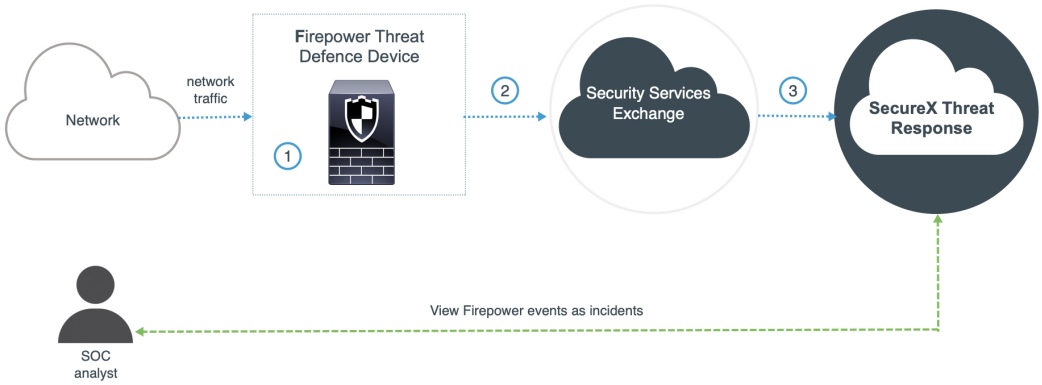
Direct Integration

You can configure your Firepower system to send supported events directly to the Cisco cloud from Firepower Threat Defense (FTD) devices.

Specifically, your Firepower devices send events to Security Services Exchange (SSE), from where they can be automatically or manually promoted to incidents that appear in Cisco SecureX threat response.

Supported Firepower user role to perform the integration: Administrator

Minimum supported Firepower release: 6.4 for the North America cloud and 6.5 for the Europe and Asia cloud



1	The FTD device generate events.
2	The FTD device sends supported events to SSE.
3	SecureX threat response queries SSE for sightings related to the IP address being investigated and provides the SOC analyst with the additional context. The events are automatically or manually promoted to incidents that appear in SecureX threat response.

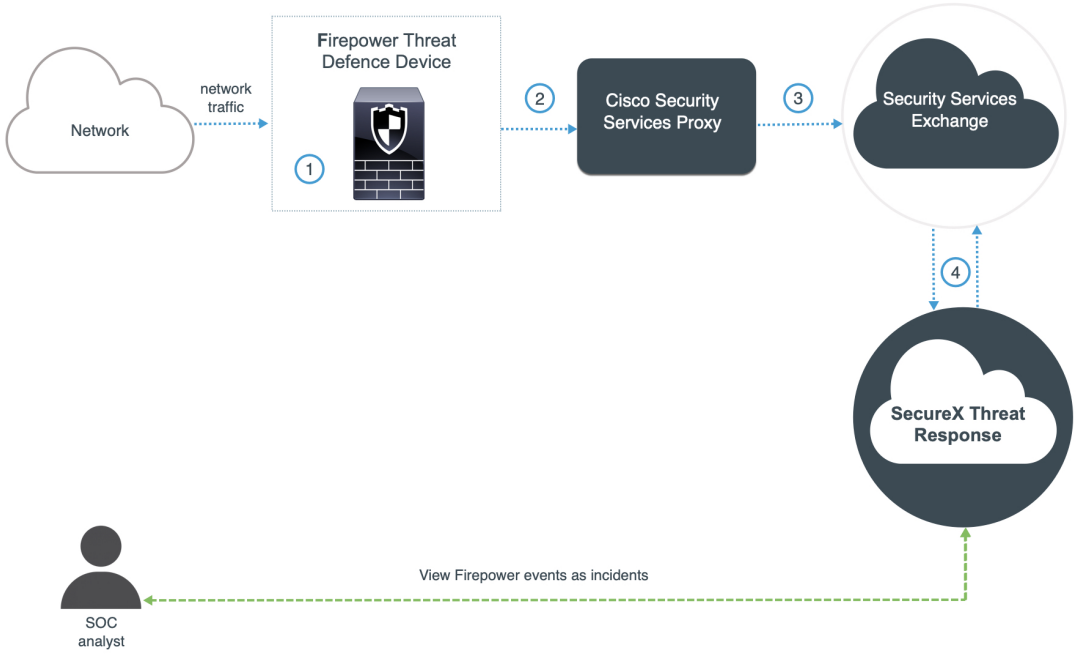
Syslog Integration

You can use syslog to send supported events to the Cisco cloud from Firepower devices. You must set up an on-premises Cisco Security Services Proxy (CSSP) server and configure your devices to send syslog messages to this proxy.

Every 10 minutes, the proxy forwards collected events to Security Services Exchange (SSE), from where they can be automatically or manually promoted to incidents that appear in Cisco SecureX threat response.

Supported Firepower user role to perform the integration: Administrator

Minimum supported Firepower release: 6.3 for all cloud regions



1	The FMC or FDM-managed FTD device generates events.
2	The FTD device sends the supported syslog events to the Cisco Security Services Proxy (CSSP) server.
3	Every 10 minutes, the CSSP forwards the collected events to the Security Services Exchange (SSE).
4	SecureX threat response queries SSE for sightings related to the IP address being investigated and provides the SOC analyst with the additional context. The events are automatically or manually promoted to incidents that appear in SecureX threat response.

Comparison of Methods for Sending Events to the Cloud

Firepower devices make events available to Cisco SecureX threat response via the Security Services Exchange portal, either using syslog or directly.

Sending Directly	Sending via Syslog Using Proxy
Supports only Firepower Threat Defense(NGFW) devices running supported versions of Firepower software	Supports all devices running supported versions of Firepower software.
Supports Firepower 6.4 and later	Supports Firepower 6.3 and later.

Sending Directly	Sending via Syslog Using Proxy
Supports all event types listed in Supported Event Types.	Supports only intrusion events.
Firepower Threat Defense devices must be connected to the internet	Firepower devices do not need to be connected to the internet.
Your Firepower deployment cannot be using a Smart Software Manager On-Prem server (formerly known as a Smart Software Satellite Server.)	Your deployment can be using a Smart Software Manager On-Prem server.
No need to set up and maintain an on-premises proxy server	Requires an on-premises virtual Cisco Security Services Proxy (CSSP) server. More information about this proxy server is available from the online help in Security Services Exchange (SSE). To access SSE, see Access Security Services Exchange.

For more information on integrating Firepower devices with Cisco SecureX threat response, see the Firepower and Cisco SecureX threat response Integration Guide.

Integrate with Cisco Event Streamer

The Cisco Event Streamer (also known as eStreamer) allows you to stream Firepower System events to external client applications.

At the highest level, the eStreamer service is a mechanism for streaming data from the Firepower System to a requesting client. The service can stream the following categories of data:

- Intrusion event data and event extra data
- Correlation (compliance) event data
- Discovery event data
- User event data
- Metadata for events
- Host information
- Malware event data

Note that eStreamer is not supported on NGIPSv, Firepower Services, Firepower Threat Defense Virtual, and Firepower Threat Defense. To stream events from these devices, you can configure eStreamer on the Management Center that the device reports to.

There are three major steps to creating and integrating an eStreamer client with a Firepower system:

1. Write a client application that exchanges messages with the Management Center or managed device using the eStreamer application protocol. The eStreamer SDK includes a reference client application.
2. Configure a Management Center or device to send the required type of events to your client application.
3. Connect your client application to the Management Center or device and begin exchanging data.

Supported Firepower user role to perform the integration: Administrator

Minimum supported Firepower release: 6.0

For more information on integrating Firepower with the Cisco Event Streamer, refer the Firepower System Event Streamer Integration Guide.

Integrate with Splunk

Cisco Secure Firewall (f.k.a. Firepower) App for Splunk presents security and network event information sent to Splunk from Firepower Management Center running version 6.0 or later. You can discover and investigate threats using threat and traffic data from the Firepower Management Center (FMC). Splunk can store far more data than FMC can, so you have greater visibility into activity on your network.

This app is a successor to the Cisco Firepower eNcore App for Splunk (https://splunkbase.splunk.com/app/3663/). You can run both apps in parallel if you choose to do so.

Supported Firepower user role to perform the integration: Administrator

Minimum supported Firepower release: 6.0

Supported Splunk versions and other compatibility information is here: https://splunkbase.splunk.com/app/4388/.

Before you can use this app, your Firepower event data must be in Splunk. To bring your Firepower data into Splunk, use the Cisco Secure eStreamer Client Add-On for Splunk (formerly known as the Cisco eStreamer eNcore Add-on for Splunk.) This technical add-on (TA) is available from https://splunkbase.splunk.com/app/3662/.

Documentation for this TA is available from https://www.cisco.com/c/en/us/support/security/defense-center/products-programming-reference-guides-list.html.

For more information on the Cisco Secure Firewall (f.k.a. Firepower) App for Splunk, see the User Guide for Cisco Secure Firewall (f.k.a. Firepower) App for Splunk.

Integrate with IBM QRadar

The Cisco Firepower App for IBM QRadar helps you analyze and contain threats to your network by providing insight from multiple security products in QRadar.

The QRadar Security Information and Event Management (SIEM) tool provides anomaly detection, incident forensics, and vulnerability management.

After you set up the app, you can view event data from your Firepower system in graphical form in the QRadar console.

Supported Firepower user role to perform the integration: Administrator

Minimum supported Firepower release: 6.0

For more information on the Cisco Firepower app for IBM QRadar, see the Integration Guide for the Cisco Firepower App for IBM QRadar.

Integrate with Cisco Security Analytics and Logging

Cisco Security Analytics and Logging (CSAL) streamlines decision making by aggregating logs from various Cisco devices and providing an intuitive view of network activity. Security Analytics and Logging can be expanded at the user's discretion, allowing for longer retention and analysis, and even alerts on potential threats found in your firewall and other networking devices.

The Firepower devices can be integrated with CSAL using two methods– On Premises and Security as a Service (SaaS).

Comparison of Cisco Security Analytics and Logging Remote Event Storage Options

On Premises	SaaS
You purchase, license, and set up the storage system behind your firewall.	You purchase licenses and a data storage plan and send your data to the Cisco cloud.
Supported event types: • Connection • Security Intelligence • Intrusion • File and Malware • LINA	Supported event types: • Connection • Security Intelligence • Intrusion • File and Malware
Supports both syslog and direct integration.	Supports both syslog and direct integration.
• View all events on the Stealthwatch Management Console. • Cross-launch from FMC event viewer to view events on the Stealthwatch Management Console. • View remotely stored connection and Security Intelligence events in FMC	View events in CDO or Stealthwatch, depending on your license. Cross-launch from FMC event viewer.

For more information, see links in the Data Storage chapter in the *Firepower Management Center Configuration Guide* or online help.

Integrate with Cisco Security Analytics and Logging (On Premises)

You can use Cisco Security Analytics and Logging (On Premises) to store your Firewall event data for increased storage at a larger retention period. By deploying Cisco Secure Network Analytics (formerly Stealthwatch) appliances, and integrating them with your Firewall deployment, you can export your event data to a Secure Network Analytics appliance.

Supported Firepower user role to perform the integration: Admin, Analyst, Security Analyst

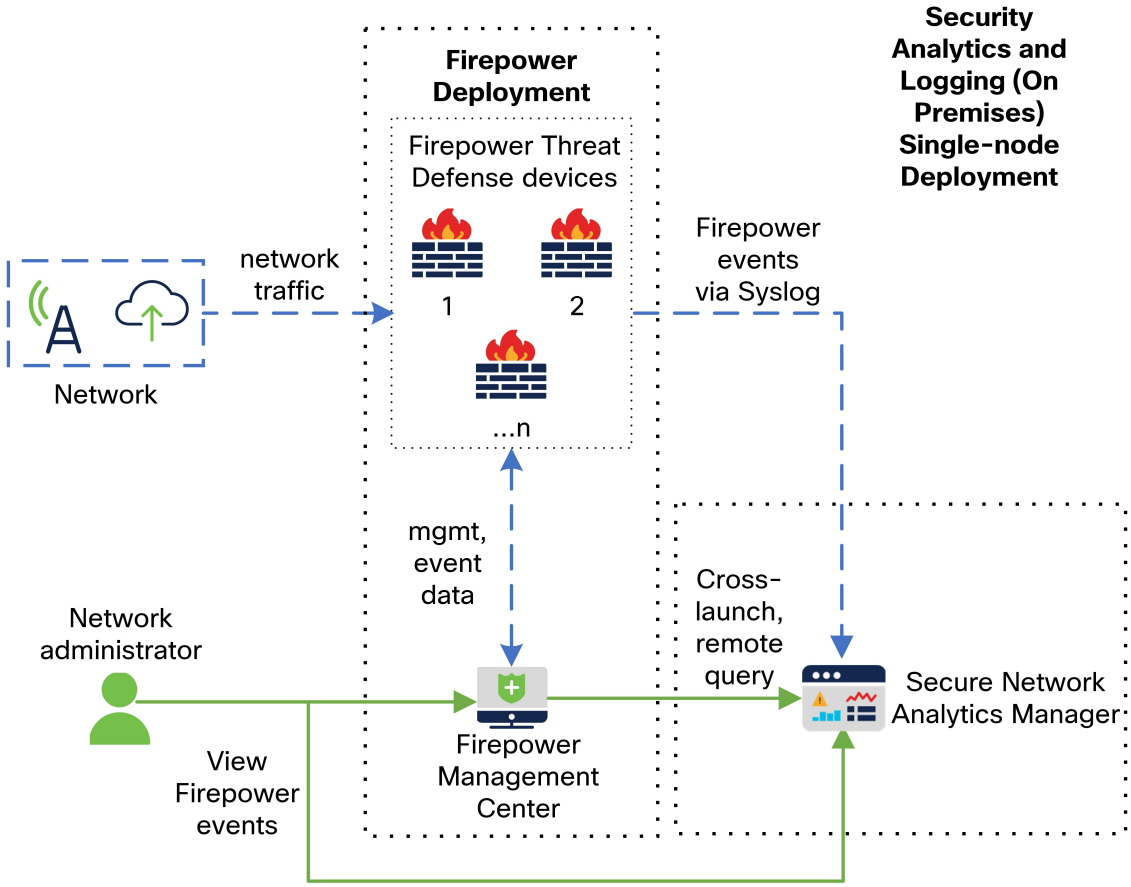
Minimum supported Firepower release: 6.4

Type of Deployments

Single-Node Deployment

Deploy a standalone Manager to receive and store events, and from which you can review and query events.

See the following diagram for an example of a Single-node deployment with a Manager:

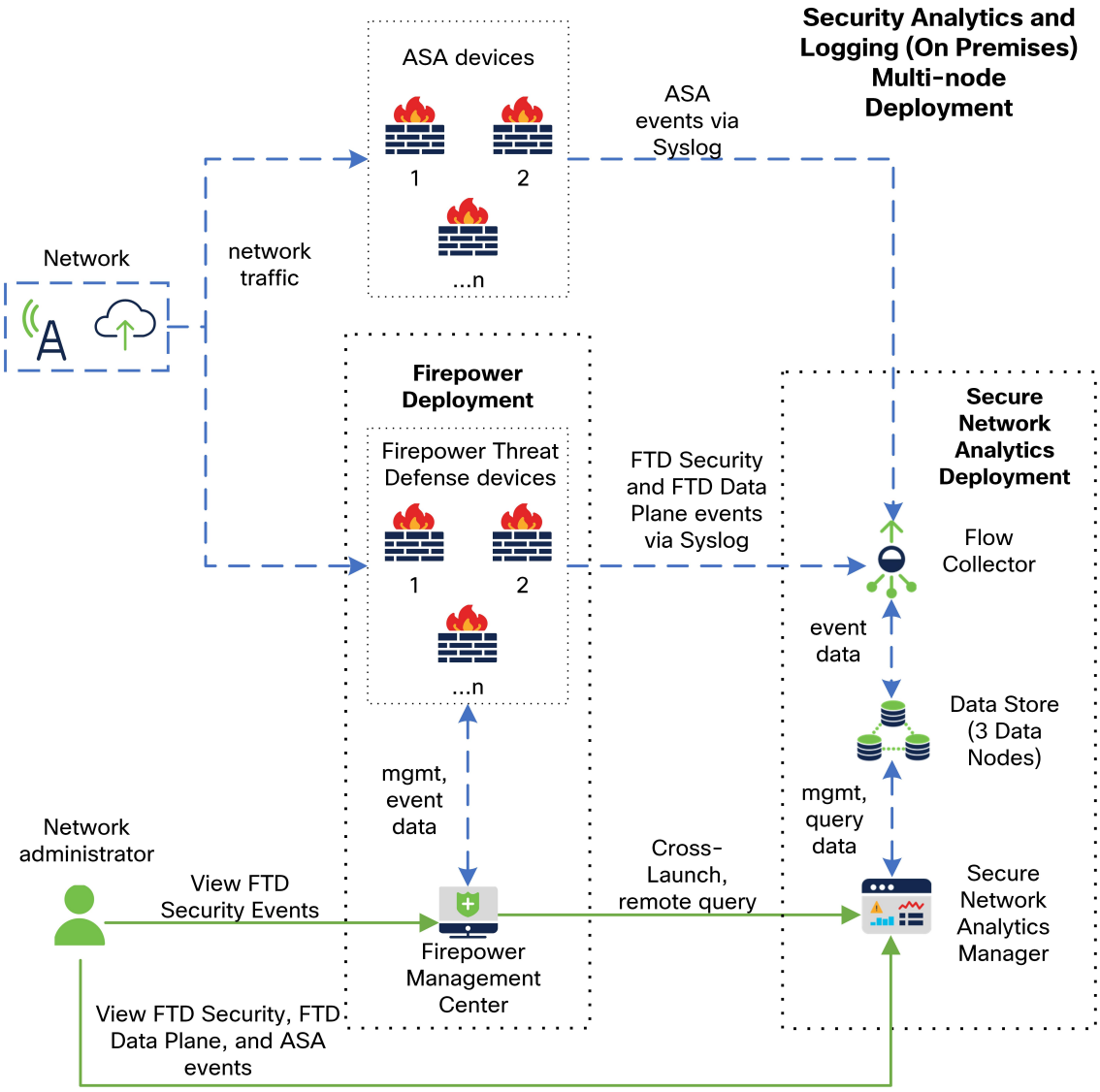


In this deployment, the Firepower Threat Defense devices send Firepower events to the Manager, and the Manager stores these events. From the Firepower Management Center UI, users can cross-launch to the Manager to view more information about the stored events. They can also query remotely the events from the Firepower Management Center.

Multi-Node Deployment

Deploy a Cisco Secure Network Analytics Flow Collector to receive events, a Cisco Secure Network Analytics Data Store (containing 3 Cisco Secure Network Analytics Data Nodes) to store events, and a Manager from which you can review and query events.

See the following diagram for an example of a Multi-node deployment with a Manager, 3 Data Nodes, and a Flow Collector:



In this deployment, the Firepower Threat Defense and ASA devices send Firewall events to the Flow Collector. The Flow Collector sends the events to the Data Store (3 Data Nodes) for storage. From the Firepower Management Center UI, users can cross-launch to the Manager to view more information about the stored events. They can also query remotely the events from the Firepower Management Center.

For more information on integrating Firepower with CSAL (On Premises), see the Cisco Security Analytics and Logging (On Premises): Firewall Event Integration Guide.

Integrate with Cisco Security Analytics and Logging (SaaS)

If you require additional space to store Firepower events, you can send Firepower events to the Cisco Secure Cloud Analytics (formerly known as Stealthwatch Cloud) for storage using Cisco Security Analytics and Logging (SaaS), and optionally make your Firepower event data available for security analytics using Cisco Secure Cloud Analytics.

This integration is specifically for Firepower Threat Defense (FTD) devices managed by Firepower Management Center (FMC). This integration is not supported on devices that are not running Firepower software, devices managed by Firepower Device Manager (FDM), or non-FTD devices managed by FMC.

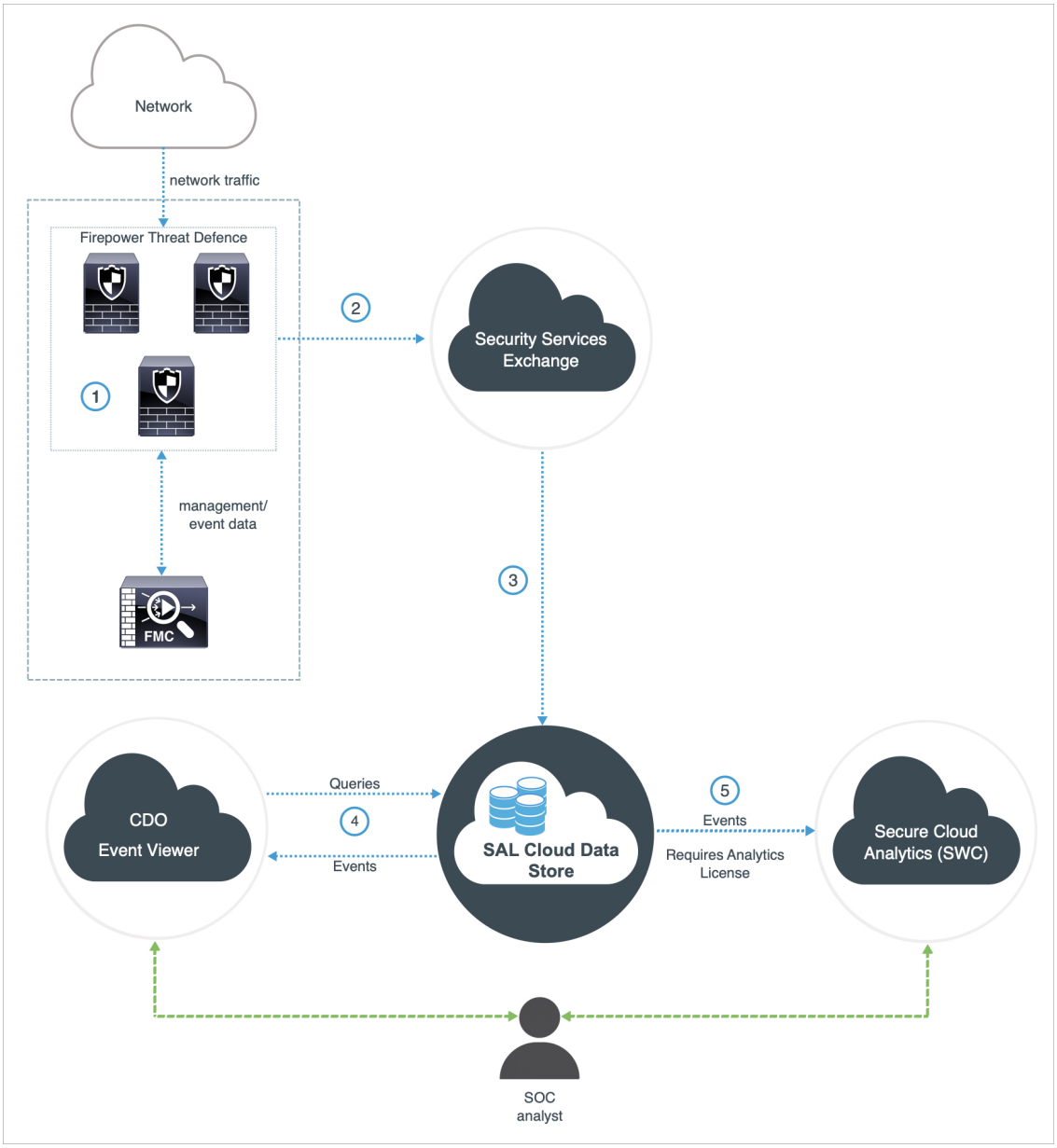
Type of Integrations

Direct Integration

Supported Firepower user role to perform the integration: Admin, Access Admin, Network Admin, Security Approver

Minimum supported Firepower release: 6.4

The following diagram shows how the direct integration works.



1	The FTD devices generate events.
2	The FTD devices send supported events to Security Services Exchange (SSE), a secure intermediary cloud service that handles cloud-to-cloud and premises-to-cloud identification, authentication, and data storage for use in Cisco cloud security products.
3	The SSE forwards the events to the Cisco Security Analytics and Logging (SAL) Cloud Data Store.

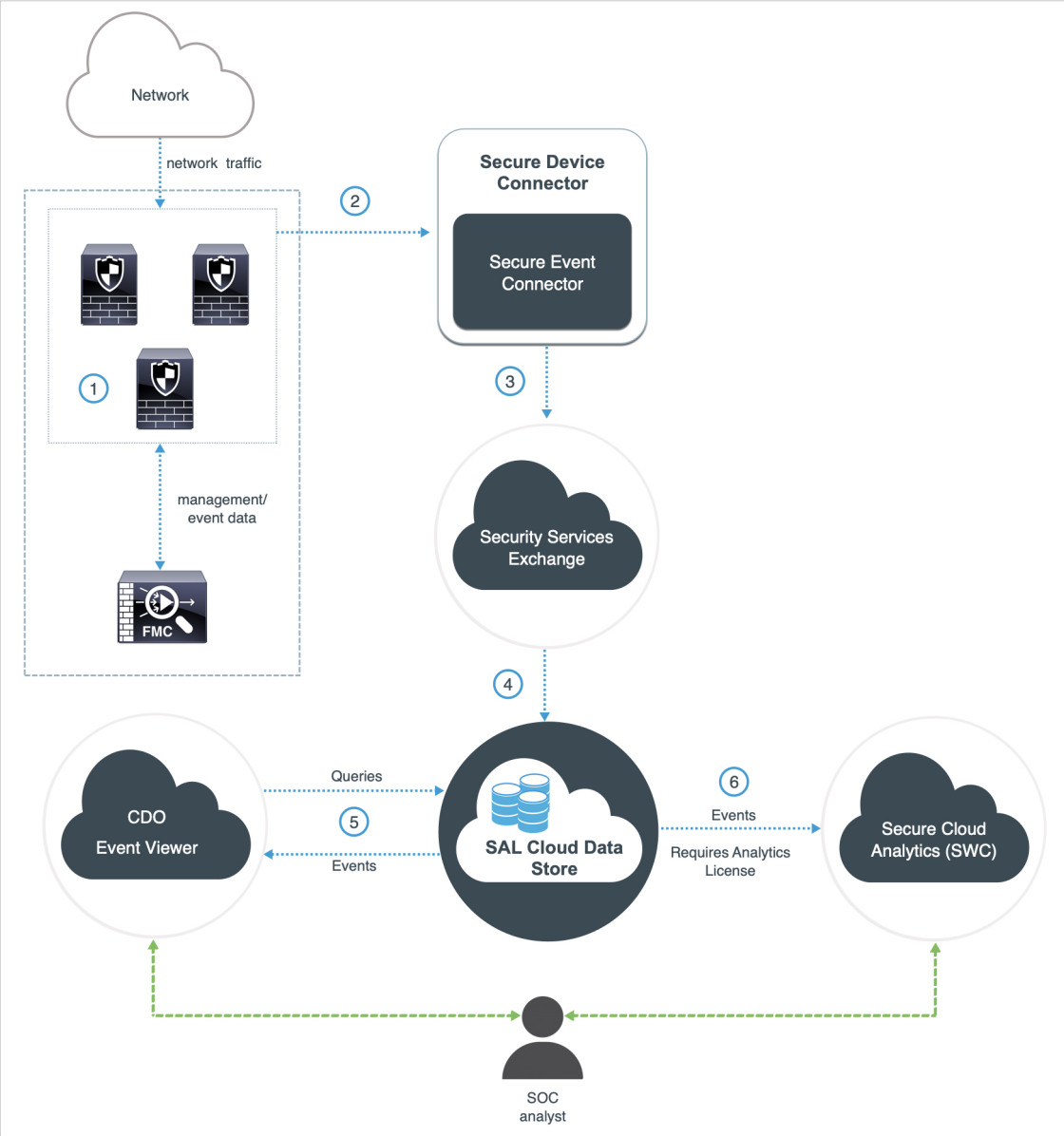
4	The CDO Event Viewer queries SAL Cloud Data Store for events and provides the SOC analyst with additional context.
5	(Only with Analytics License) Cisco Secure Cloud Analytics (formerly SWC) receives the events from the SAL Cloud Data Store and provides the SOC analyst access to the analytics features of the product.

Syslog Integration

Supported Firepower user role to perform the integration: Admin, Access Admin, Network Admin, Security Approver

Minimum supported Firepower release: 7.0

The following diagram shows how the syslog integration works.



1	The FTD devices generate events.
2	The FTD devices send supported events as syslog messages to a Secure Event Connector (SEC) installed on a virtual machine on your network.
3	The SEC forwards the events to Security Services Exchange (SSE), a secure intermediary cloud service that handles cloud-to-cloud and premises-to-cloud identification, authentication, and data storage for use in Cisco cloud security products.

4	The SSE forwards the events to the Cisco Security Analytics and Logging (SAL) Cloud Data Store.
5	The CDO Event Viewer queries SAL Cloud Data Store for events and provides the SOC analyst with additional context.
6	(Only with Analytics License) Cisco Secure Cloud Analytics (formerly SWC) receives the events from the SAL Cloud Data Store and provides the SOC analyst access to the analytics features of the product.

For more information on integrating Firepower with CSAL (SaaS), see the Firepower Management Center and Cisco Security Analytics and Logging (SaaS) Integration Guide.