Cisco Secure Firewall Integrations Overview Guide

First Published: 2021-12-01

Introduction

This guide provides instructions to integrate Secure Firewall Threat Defense (formerly Firepower Threat Defense) devices with each of the following tools for event analysis:

- Cisco XDR
- 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 (formerly Firepower Management Center) or Secure Firewall Device Manager (formerly Firepower Device Manager)-managed Firewall Threat Defense devices to perform the integration. This guide includes instructions to integrate Firewall Threat Defense devices that are managed by either the or Firewall Device Manager, as applicable.

Note As of July 31, 2024, Cisco SecureX will be phased out and no longer available. Cisco SecureX access is no longer provided alongside Cisco Secure Firewall product purchases. After the end-of-life date, it will not be possible to provision Cisco SecureX for users. Additionally, all existing Cisco SecureX environments will be disabled and all capabilities will become unavailable.

Use Cases

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

Use Case	Solution	Minimum Supported Firewall Threat Defense Release	More Information
You want to unify visibility and correlate detections across multiple telemetry sources, prioritize threats based on the greatest risk, and enable security analysts to take rapid and effective action on what requires urgent attention.	Cisco XDR	6.4	Integrate with Cisco XDR
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 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 8
You want to send Firewall 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 Firewall 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 10

Integrate with Cisco XDR

Cisco Extended Detection and Response (Cisco XDR) is a cloud-based solution that unifies visibility by correlating threat detections across multiple telemetry sources and enables security teams to detect, prioritize, and respond to the most sophisticated threats. The solution enhances threat detection and response capabilities by prioritizing incidents based on risk, and enables security analysts to take rapid and effective action on what requires urgent attention.

This integration sends supported events from the Firewall Threat Defense devices to Cisco XDR for analysis.

Note Cisco XDR is a separately licensed product. It requires an additional subscription beyond the licenses required for Cisco Secure Firewall products. For more information, see Cisco XDR Licenses.

Type of Integrations

You can integrate Firewall Threat Defense devices with Cisco XDR using two methods of integration:

- Direct integration: Supported on
- Syslog integration: Supported on and Firewall Device Manager

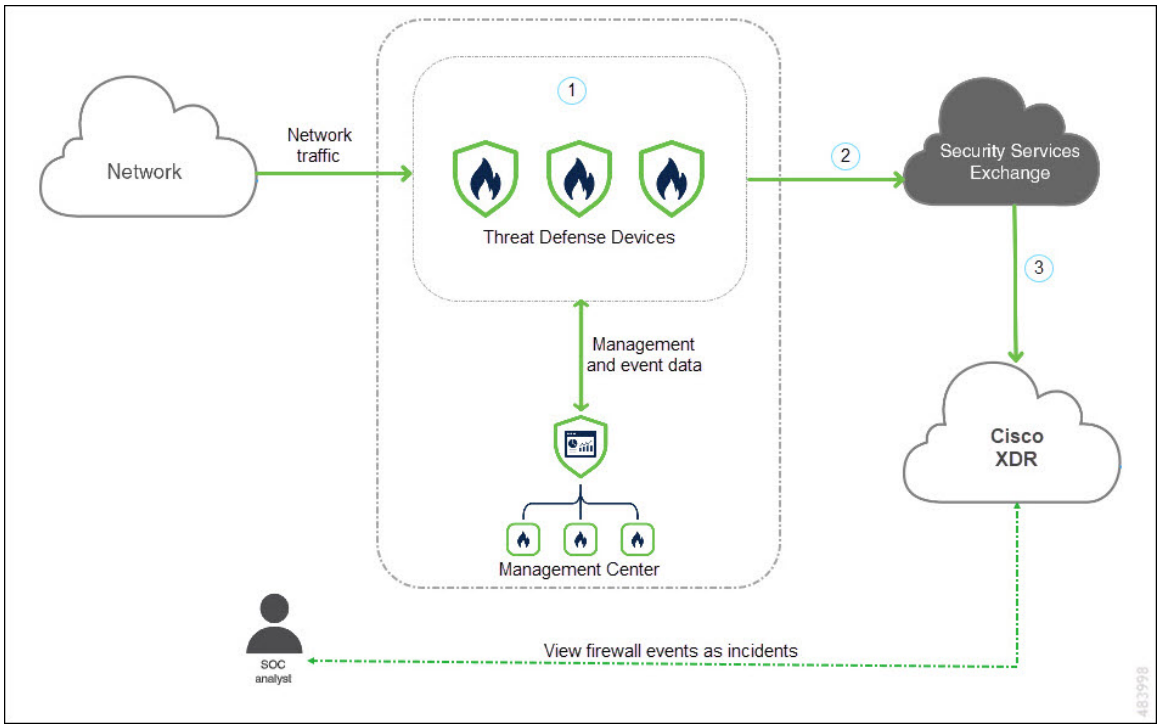
Direct Integration

You can configure your managed Firewall Threat Defense devices to send supported events directly to the Security Services Exchange in Cisco Security Cloud.

- Supported Secure Firewall user role to perform the integration: Administrator.
- Minimum supported Firewall Threat Defense version: 6.4 for the North America cloud and 6.5 for the Europe, APJC, India, and Australia clouds.
- Minimum supported version: 7.0.2 through 7.0.x, and 7.2.0 and later.

Note If you were already sending events to the Cisco Security Cloud using a SecureX subscription, you can continue to send events to Cisco XDR. However, if you now register your to the cloud tenancy using your Security Cloud Control account, your Security Cloud Control account must have a Security Analytics and Logging license to forward events to Cisco XDR.

The following diagram shows how direct integration works.



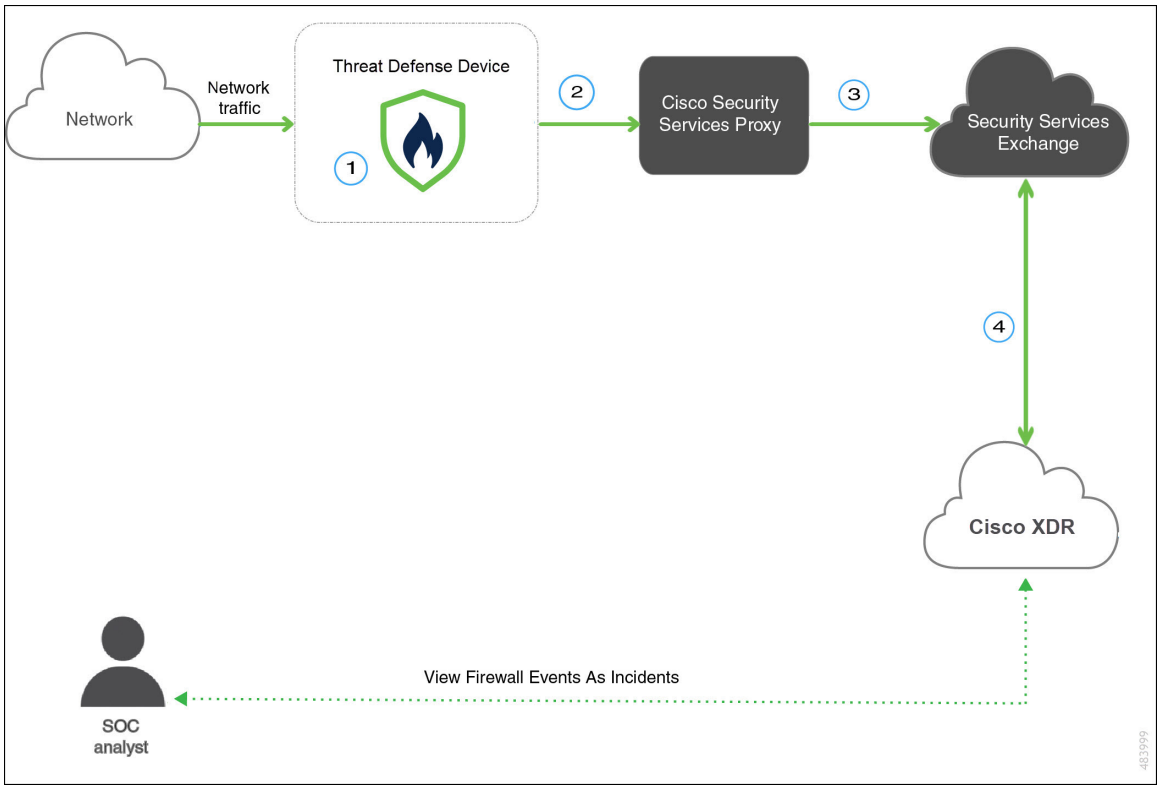
1	Firewall Threat Defense devices generate events.
2	Firewall Threat Defense devices send supported events to Security Services Exchange.
3	Cisco XDR queries Security Services Exchange for sightings related to the IP address being investigated and provides the security analyst with the additional context. The events are automatically or manually promoted as incidents that appear in Cisco XDR.

Syslog Integration

Use syslog to send supported events to the Cisco cloud from Firewall devices.

- Supported Secure Firewall user role to perform the integration: Administrator.
- Minimum supported Secure Firewall release: 6.3 for all cloud regions.

The following diagram shows how syslog integration works.



1	Firewall Threat Defense device generates events.
2	Firewall Threat Defense 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.
4	Cisco XDR queries Security Services Exchange for sightings related to the IP address being investigated and provides the security analyst with additional context. The events are automatically or manually promoted as incidents that appear in Cisco XDR.

Integrate with Cisco Event Streamer

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

At the highest level, the eStreamer service is a mechanism for streaming data from the Firewall 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, Firewall Services, Firewall Threat Defense Virtual, and Firewall 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 Firewall 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 Firewall user role to perform the integration: Administrator

Minimum supported Firepower release: 6.0

For more information on integrating Firewall with the Cisco Event Streamer, refer the Secure Firewall Management Center 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 running version 6.0 or later. You can discover and investigate threats using threat and traffic data from the . Splunk can store far more data than 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 Firewall 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 Firewall event data must be in Splunk. To bring your Firewall 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 Firewall system in graphical form in the QRadar console.

Supported Firewall 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 Firewall 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.

On Premises	SaaS
• View all events on the Secure Network Analytics Manager. • Cross-launch from event viewer to view events on the Secure Network Analytics Manager. • View remotely stored connection and Security Intelligence events in	View events in Security Cloud Control or Secure Network Analytics, depending on your license. Cross-launch from event viewer.

For more information, see links in the Data Storage chapter in the *Cisco Secure Firewall Management Center Device 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 Firewall user role to perform the integration: Admin, Analyst, Security Analyst

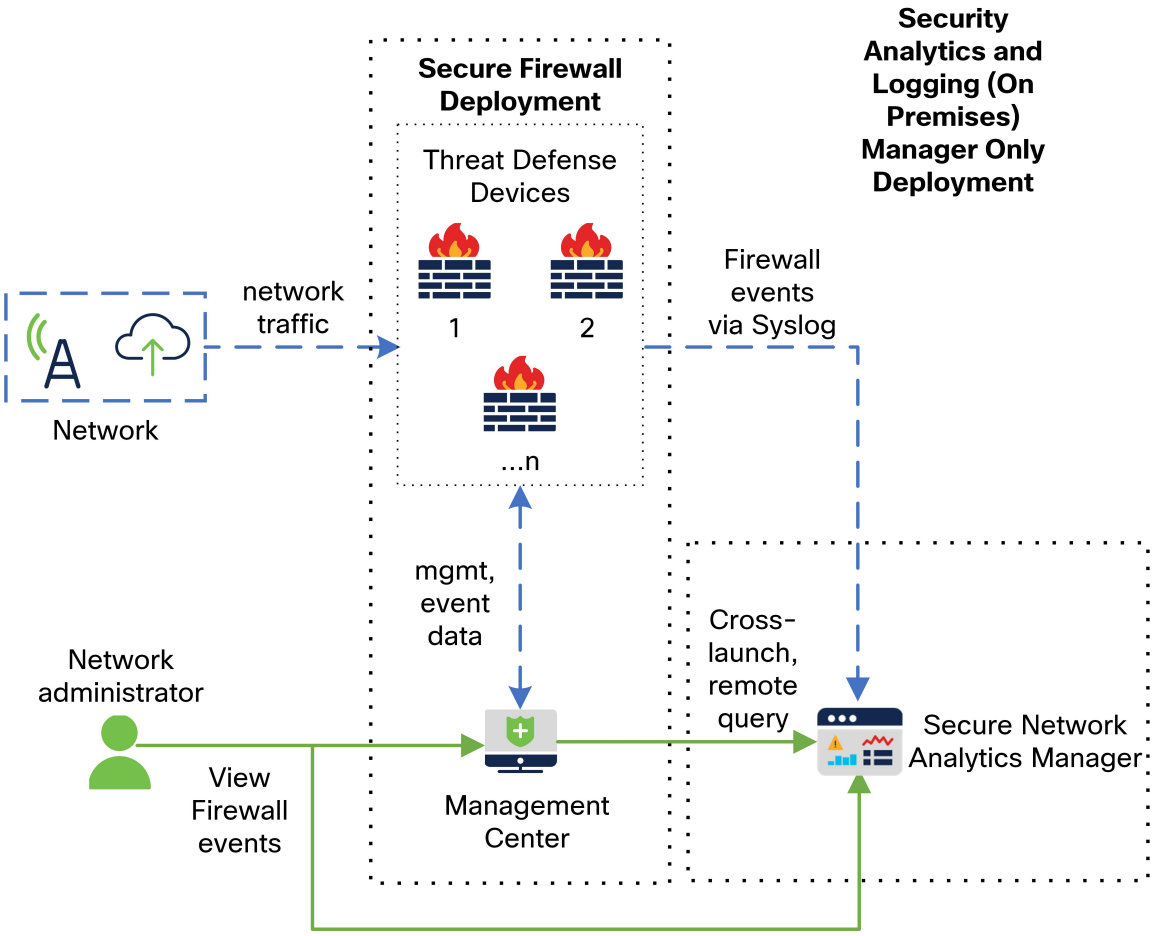
Minimum supported Secure Firewall release: 6.4

Type of Deployments

Manager Only 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 manager only deployment with a manager:



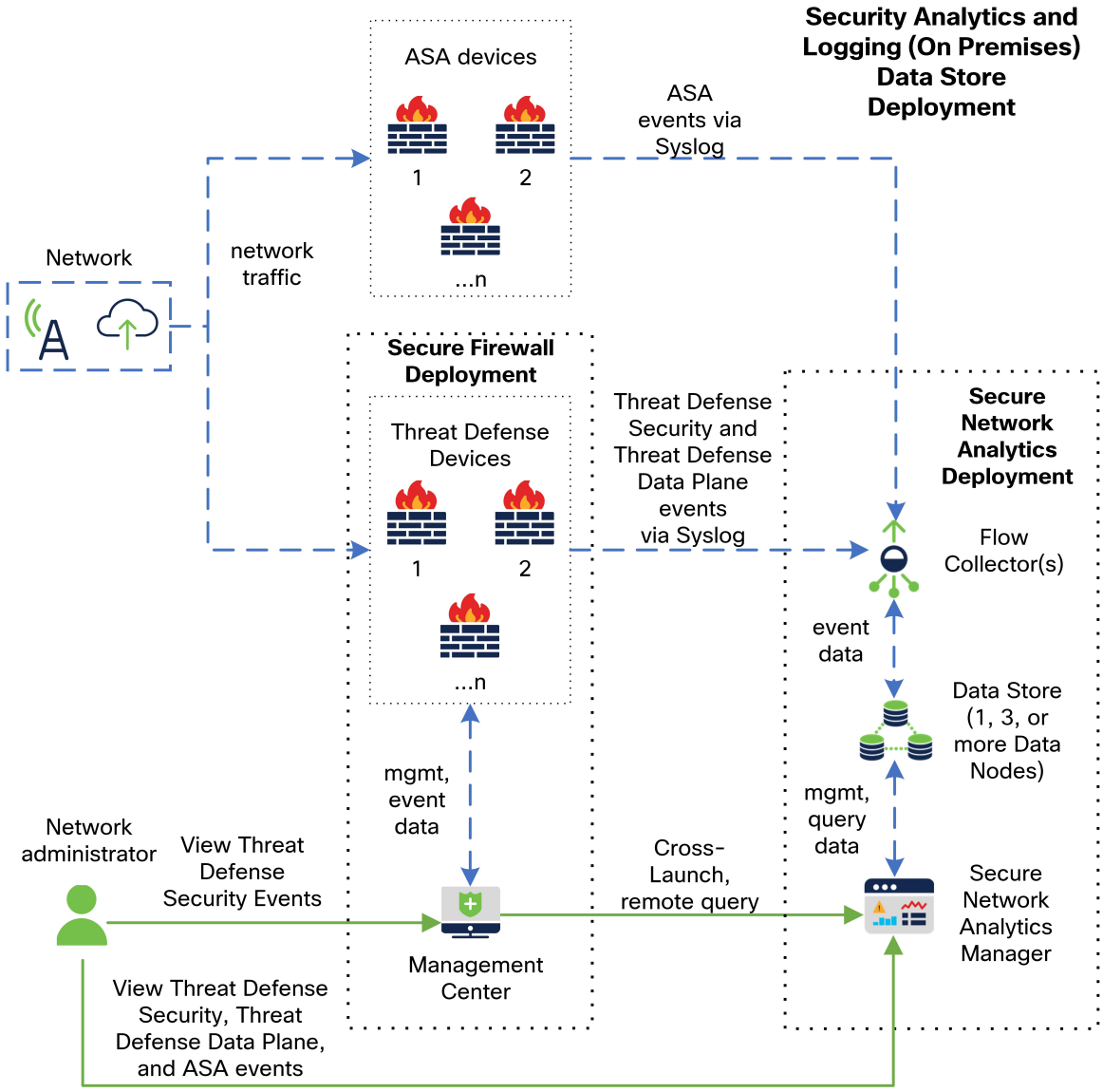
In this deployment, the Firewall Threat Defense devices send firewall events to the manager, which then stores these events. From the UI, you can cross-launch to the manager to view more information about the stored events. Additionally, you can perform remote queries of the events from the .

Note **Manager Only** deployment is not supported on Secure Network Analytics appliance version 7.5.1 or later. For more information, see Cisco Security Analytics and Logging documentation.

Data Store 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 data store deployment with a manager, 3 data nodes, and a flow collector:



In this deployment, the Firewall Threat Defense and ASA devices send firewall events to the flow collector. The flow collector then sends the events to the data store (3 data nodes) for storage. From the UI, you can cross-launch to the manager to view more information about the stored events. Additionally, you can perform remote queries of the events from the .

For more information about integrating Firewall with SAL (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 Firewall events, you can send Firewall 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 Firewall event data available for security analytics using Cisco Secure Cloud Analytics.

This integration is specifically for Firewall Threat Defense devices managed by . This integration is not supported on devices that are not running Firewall software, devices managed by Firewall Device Manager, or non-Firewall Threat Defense devices managed by .

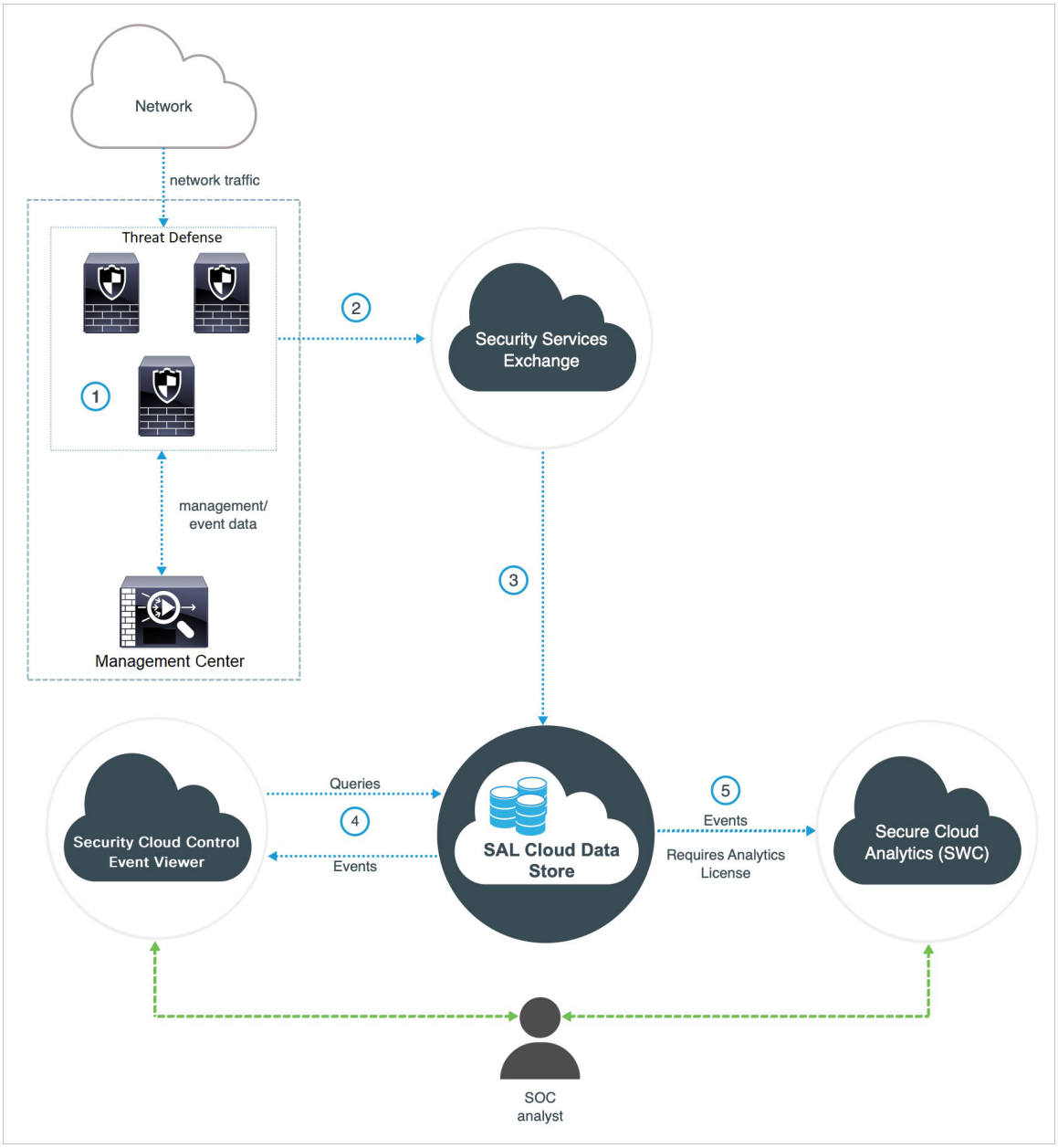
Type of Integrations

Direct Integration

Supported Firewall 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 Firewall Threat Defense devices generate events.
2	The Firewall Threat Defense devices send supported events to Security Services Exchange, 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.

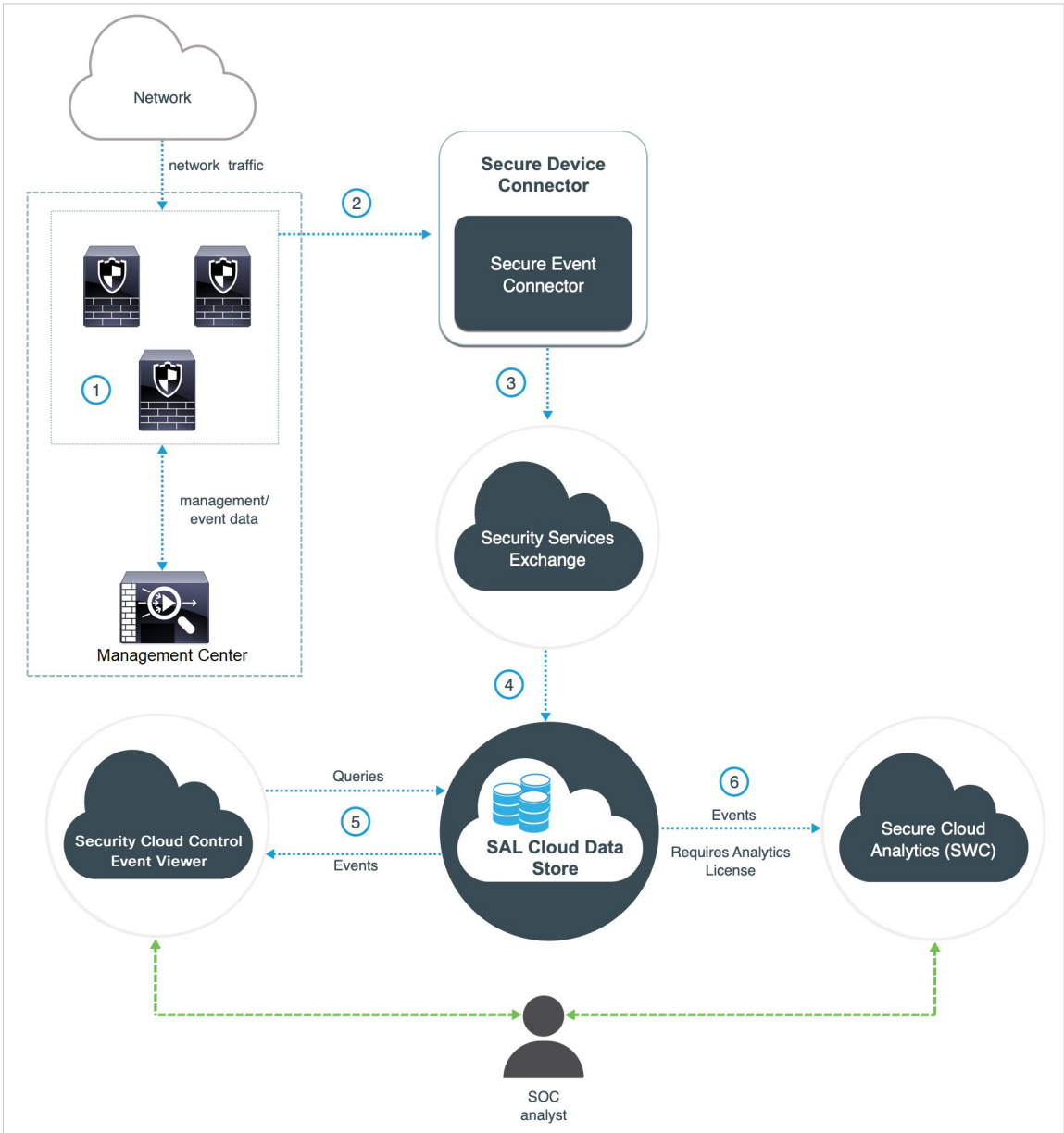
3	Security Services Exchange forwards the events to the Cisco Security Analytics and Logging (SAL) Cloud Data Store.
4	The Security Cloud Control Event Viewer queries SAL Cloud Data Store for events and provides the SOC analyst with additional context.
5	(Only with Analytics License) Cisco Secure Cloud 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 Firewall 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 Firewall Threat Defense devices generate events.
2	The Firewall Threat Defense 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, 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	Security Services Exchange forwards the events to the Cisco Security Analytics and Logging (SAL) Cloud Data Store.
5	The Security Cloud Control 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 Firewall with CSAL (SaaS), see the Cisco and Cisco Security Analytics and Logging (SaaS) Integration Guide.

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. All rights reserved.