Cisco Secure Firewall 集成概述指南

上次修改日期: 2025 年 2 月 27 日

简介

本指南提供将 Cisco Secure Firewall Threat Defense （以前称为 Firepower 威胁防御） 设备与以下每个工具集成以进行事件分析的说明：

- 思科 XDR
- 思科事件流
- Splunk
- IBM QRadar
- 思科安全分析和日志记录（本地部署和 SaaS）

根据事件分析工具和所需集成类型，您可以使用 Cisco Secure Firewall Management Center （以前的 Firepower 管理中心） 或 Cisco Secure Firewall 设备管理器 （以前的 Firepower 设备管理器）管理的 威胁防御 设备执行集成。本指南介绍如何集成由 管理中心 或 设备管理器（视情况而定）管理的 威胁防御 设备。

Note 截至 2024 年 7 月 31 日，思科 SecureX 已被淘汰，不再提供。购买 Cisco Secure Firewall 产品后，不再提供 Cisco SecureX 访问权限。在生命周期终止日期后，将无法为用户调配 Cisco SecureX。此外，所有现有的思科 SecureX 环境都将被禁用，所有功能将变得不可用。有关更多信息，请参阅 思科 SecureX 生命周期终止公告。

使用案例

本部分列出一般使用案例以及用于执行集成的工具。

使用案例	解决方案	支持的最低 威胁防御 版本	更多信息
您希望跨多个遥测源统一可视性并关联检测，根据最大风险确定威胁的优先级，并使安全分析师能够对需要紧急关注的事件采取快速有效的操作。	思科 XDR	6.4	与 思科 XDR集成

使用案例	解决方案	支持的最低 威胁防御 版本	更多信息
您可以从管理中心通过流传输发送主机、发现、关联、合规性白名单、入侵、用户活动、文件、恶意软件和连接数据。	思科事件流 (eStreamer)	6.0	与思科事件流转换器集成
您希望使用 Splunk 存储从 管理中心 接收的威胁和流量数据，并使用此数据发现和调查威胁。	适用于 Splunk 的 Cisco Secure Firewall（以前称为 Firepower）应用	6.0	与 Splunk 集成
您可以通过 QRadar 中的多个安全产品提供见解，从而帮助您分析并遏制对网络的威胁。	IBM QRadar 的 Cisco Firepower App for	6.0	与 IBM QRadar 集成
您想增大本地防火墙事件数据存储容量，将此数据保留更长时间，并将事件数据导出到安全网络分析设备。	Cisco Security Analytics and Logging（本地）	6.4	与思科安全分析和日志记录（本地）集成, on page 7
请将 Firewall 事件发送到 Cisco Secure Cloud Analytics（以前称为 Stealthwatch Cloud）进行存储，因为您需要比本地存储所能提供的存储更多的存储空间，并且可以选择使用 Cisco Secure Cloud Analysis 使您的 Firewall 事件数据可用于安全分析。	Cisco Security Analytics and Logging (SaaS)	6.4	与思科安全分析和日志记录（SaaS）集成, on page 9

与 思科 XDR集成

思科扩展检测和响应（思科XDR）是基于云的解决方案，通过关联多个遥测源的威胁检测来统一可视性，并使安全团队能够检测、确定优先级和响应最复杂的威胁。该解决方案通过根据风险确定事件的优先级来增强威胁检测和响应功能，并使安全分析师能够对需要紧急关注的事件采取快速有效的措施。

此集成会将支持的事件从 威胁防御 台设备发送到 思科 XDR 进行分析。

注释 思科 XDR 是单独许可的产品。除 Cisco Secure Firewall 产品所需的许可证外，还需要额外订用。有关详细信息，请参阅思科 XDR 许可证。

集成类型

您可以使用两种集成方法将 威胁防御 设备与 思科 XDR 集成：

- 直接集成：在 管理中心 上受支持
- 系统日志集成：在 管理中心 和 设备管理器上支持

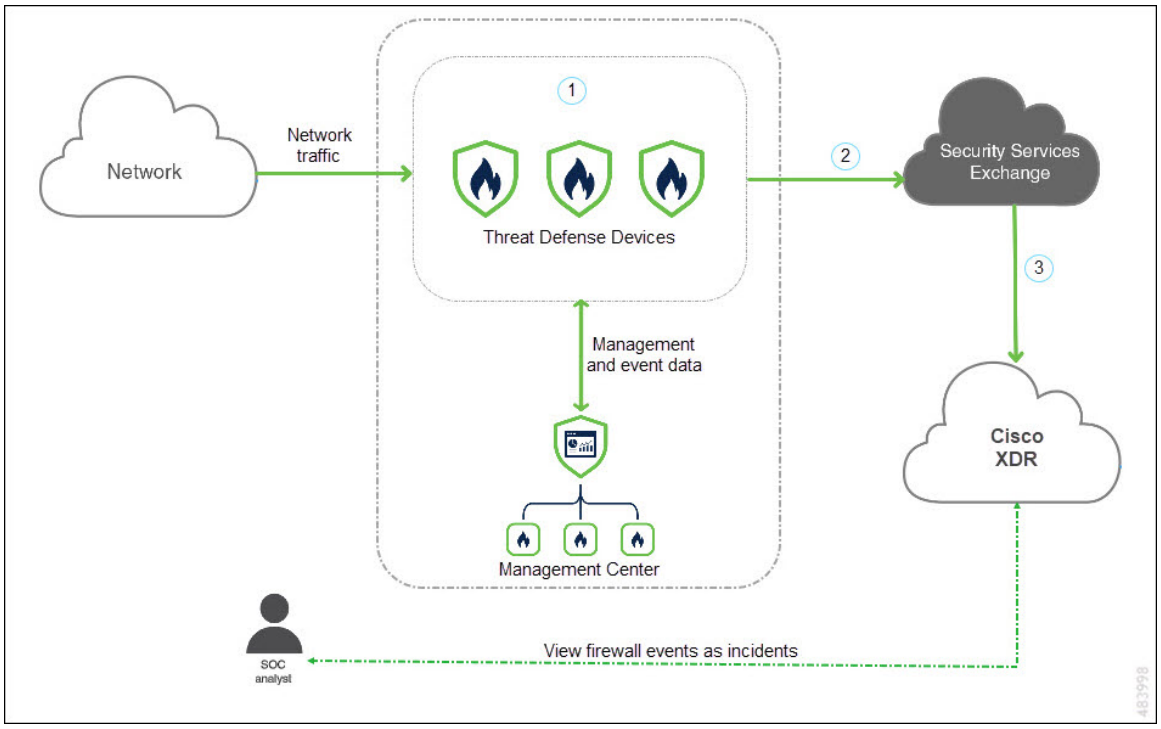
直接集成

您可以将您的受管 威胁防御 设备配置为将支持的事件直接发送到思科云中的 安全服务交换。

- 执行集成的受支持 Cisco Secure Firewall 用户角色：管理员。
- 支持的最低 威胁防御 版本：适用于北美云的 6.4 及适用于欧洲、亚太地区、日本和中国、印度和澳大利亚云的 6.5。
- 支持的最低 管理中心 版本：7.0.2 至 7.0.x 以及 7.2.0 及更高版本。

注释 如果您已使用 SecureX 订用将事件发送到思科安全云，则可以继续将事件发送到 思科 XDR。但是，如果您现在使用 安全云控制 帐户将 管理中心 注册到云租赁，则您的 安全云控制 帐户必须具有 Security Analytics and Logging 许可证才能将事件转发到 思科 XDR。

下图显示了直接集成的工作方式。



1	威胁防御 设备会生成事件。
2	威胁防御 台设备将支持的事件发送到 安全服务交换。

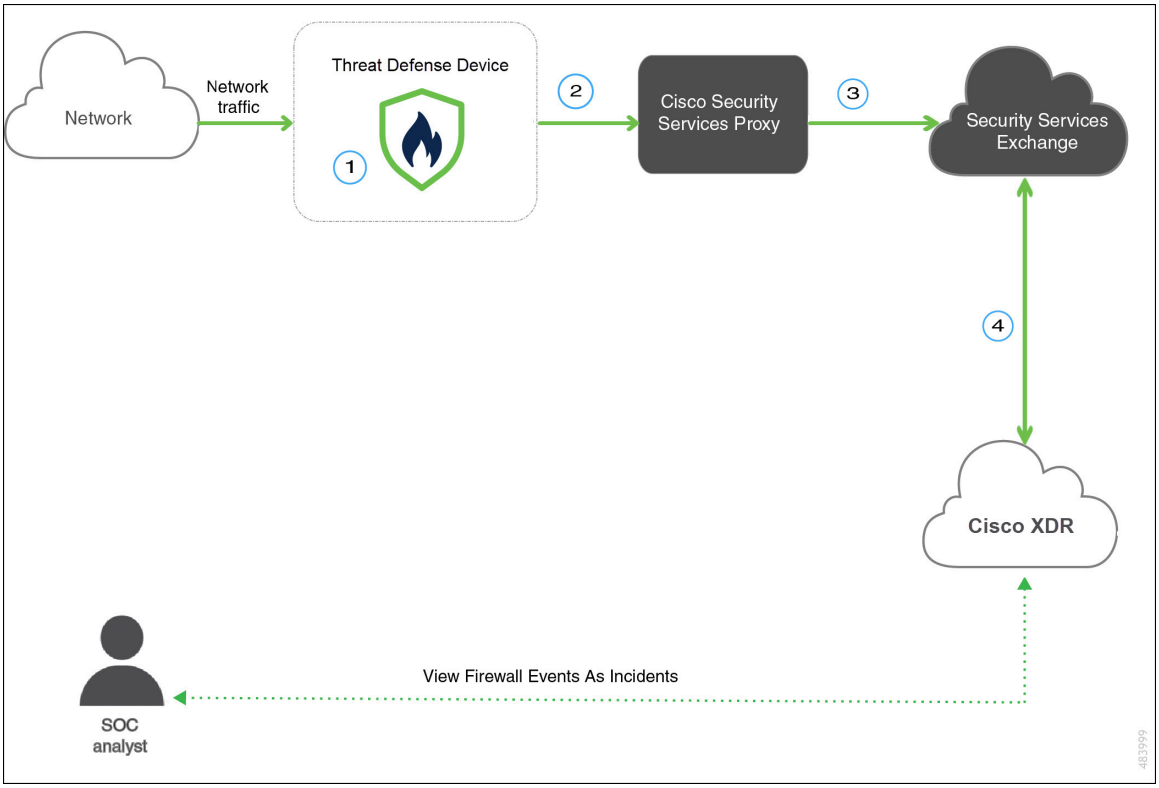
3	思科 XDR 会查询 安全服务交换 与正在调查的 IP 地址相关的目击项，并为安全分析师提供额外情景。这些事件将自动或手动升级为 思科 XDR中显示的突发事件。

系统日志集成

使用系统日志将支持的事件从 防火墙 设备发送至思科云。

- 执行集成的受支持 Cisco Secure Firewall 用户角色：管理员。
- 所有云区域支持的最低 Cisco Secure Firewall 版本：6.3。

下图显示了系统日志集成的工作方式。



1	威胁防御 设备生成事件。
2	威胁防御 设备会将支持的系统日志事件发送到思科安全服务代理 (CSSP) 服务器。
3	每隔 10 分钟，CSSP 会将收集的事件转发到 安全服务交换。
4	思科 XDR 会查询 安全服务交换 与正在调查的 IP 地址相关的目击事件，并为安全分析师提供更多背景信息。这些事件将自动或手动升级为 思科 XDR中显示的突发事件。

与思科事件流转换器集成

思科事件流（也称为 eStreamer）允许您将 Firewall 系统事件流式传输到外部客户端应用程序。

总体来看，eStreamer 服务是通过流传输将数据从 Firewall 发送到发出请求的客户端的一种机制。该服务可以通过流传输发送以下类别的数据：

- 入侵事件数据和事件额外数据
- 关联（合规性）事件数据
- 发现事件数据
- 用户事件数据
- 事件的元数据
- 主机信息
- 恶意软件事件数据

请注意，NGIPSv、Firewall 服务、threat defense virtual 和 威胁防御不支持 eStreamer。要从这些设备通过流传输发送事件，可以在这些设备向其报告的管理中心上配置 eStreamer。

创建 eStreamer 客户端并将其与 Firewall 系统集成有三个主要步骤：

1. 编写一个客户端应用程序，使用eStreamer应用程序协议与管理中心或受管设备交换消息。eStreamer SDK 包含一个标准客户端应用。
2. 配置一个管理中心或设备以将所需类型的事件发送到您的客户端应用。
3. 将您的客户端应用连接到管理中心或设备，并开始交换数据。

执行集成的受支持 防火墙 用户角色：管理员

支持的最低 Firepower 版本：6.0

有关将 Firewall 与 Cisco 事件流传输器集成的更多信息，请参阅 安全防火墙管理中心事件流媒体融合指南。

与 Splunk 集成

Cisco Secure Firewall (f.k.a. Firepower) App for Splunk 提供从 管理中心 运行 6.0 版或更高版本发送到 Splunk 的安全性和网络事件信息。您可以使用来自 管理中心的威胁和流量数据发现和调查威胁。Splunk 可存储的数据量大于 管理中心，因此您可以更好地了解网络上的活动。

此应用是适用于 Splunk 的思科 Firepower eNcore 应用的后续产品 (https://splunkbase.splunk.com/app/3663/)。如果您选择这样做，则可以并行运行这两个应用程序。

执行集成的受支持 防火墙 用户角色：管理员

支持的最低 Firepower 版本：6.0

支持的 Splunk 版本和其他兼容性信息如下： https://splunkbase.splunk.com/app/4388/.

必须先将您的 防火墙 事件数据置于 Splunk 中，然后才能使用此应用程序。要将 防火墙 数据导入 Splunk，请使用适用于 Splunk 的 Cisco Secure eStreamer 客户端附加服务（以前称为适用于 Splunk 的 Cisco eStreamer eNcore eNcore 附加服务）。可从https://splunkbase.splunk.com/app/3662/获取此技术性插件 (TA)。

此 TA 的相关文档可从以下网址获取：
https://www.cisco.com/c/en/us/support/security/defense-center/Products-programming-reference-guides-list.html。

有关 Cisco Secure Firewall (f.k.a. 的详细信息Firepower) App for Splunk，请参阅 Cisco Secure Firewall (fka 用户指南面向 Splunk 的 Firepower) App。

与 IBM QRadar 集成

Cisco Firepower App for IBM QRadar 通过 QRadar 中的多个安全产品提供见解，从而帮助您分析并遏制对网络的威胁。

QRadar 安全信息和活动管理 (SIEM) 工具提供异常检测、事件调查分析和漏洞管理功能。

在安装应用程序后，可以在 QRadar 控制台中以图形形式查看 防火墙 系统中的事件数据。

执行集成的受支持 防火墙 用户角色：管理员

支持的最低 Firepower 版本：6.0

有关面向 IBM QRadar 的 Cisco Firepower 应用的详细信息，请参阅 面向 IBM QRadar 的 Cisco Firepower 应用的集成指南。

与思科安全分析和日志记录集成

思科安全分析和日志记录 (CSAL) 通过聚合来自各种思科设备的日志并提供网络活动的直观视图，简化了决策过程。您可以自行决定扩展安全分析和日志记录，以便进行更长时间的保留和分析，甚至可以对防火墙和其他网络设备中发现的潜在威胁发出警报。

防火墙 设备可使用两种方法与 CSAL 集成 - 本地方法和安全即服务 (SaaS) 方法。

思科安全分析和日志记录远程事件存储选项的比较

本地	SaaS
您购买、许可并设置防火墙后的存储系统。	您购买许可证和数据存储计划，并将数据发送到思科云。

本地	SaaS
支持的事件类型： • 连接 • 安全情报 • 入侵 • 文件和恶意软件 • LINA	支持的事件类型： • 连接 • 安全情报 • 入侵 • 文件和恶意软件
支持系统日志和直接集成。	支持系统日志和直接集成。
• 查看 Cisco Secure Network Analytics 管理器上的所有事件。 • 从 管理中心 事件查看器交叉启动，以查看 Cisco Secure Network Analytics 管理器 上的事件。 • 在 管理中心中查看远程存储的连接和安全情报事件	在 安全云控制 中查看事件，或者 Secure Network Analytics，具体取决于您的许可证。从 管理中心 事件查看器交叉启动。

有关详细信息，请参阅 《Cisco Secure Firewall Management Center 设备配置指南》 或联机帮助中“数据存储”一章中的链接。

与思科安全分析和日志记录（本地）集成

您可以使用思科安全分析和日志记录（本地）存储防火墙事件数据，以便在更长的保留期内增加存储量。通过部署 Cisco Secure Network Analytics（前身为 Stealthwatch）设备并将其与防火墙部署集成，您可以将事件数据导出到 Secure Network Analytics 设备。

执行集成时支持的 防火墙 用户角色：管理员、分析师、安全分析师

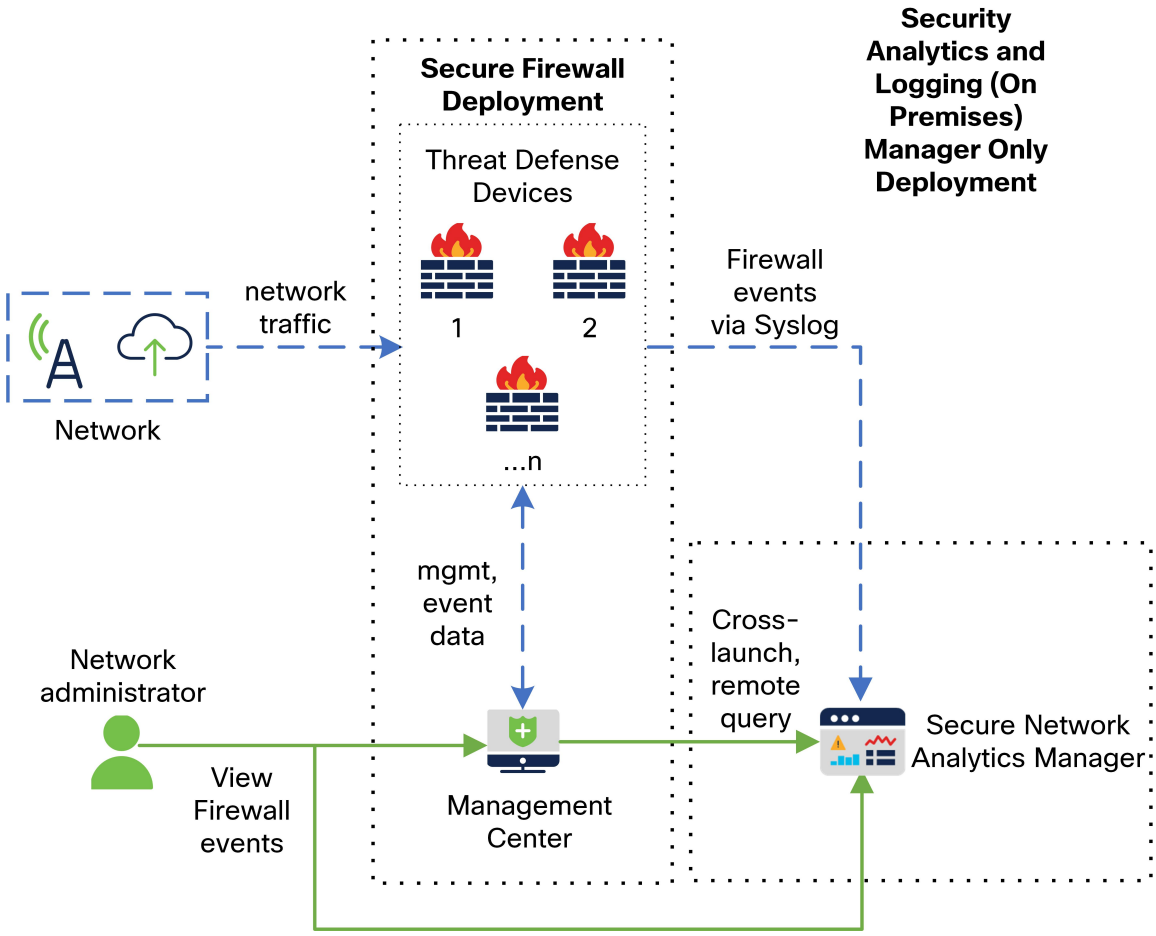
支持的最低 Cisco Secure Firewall 版本：6.4

部署类型

仅管理器部署

部署独立管理器以接收和存储事件，您可以从中查看和查询事件。

请参阅下图，了解使用管理器的仅管理器部署示例：



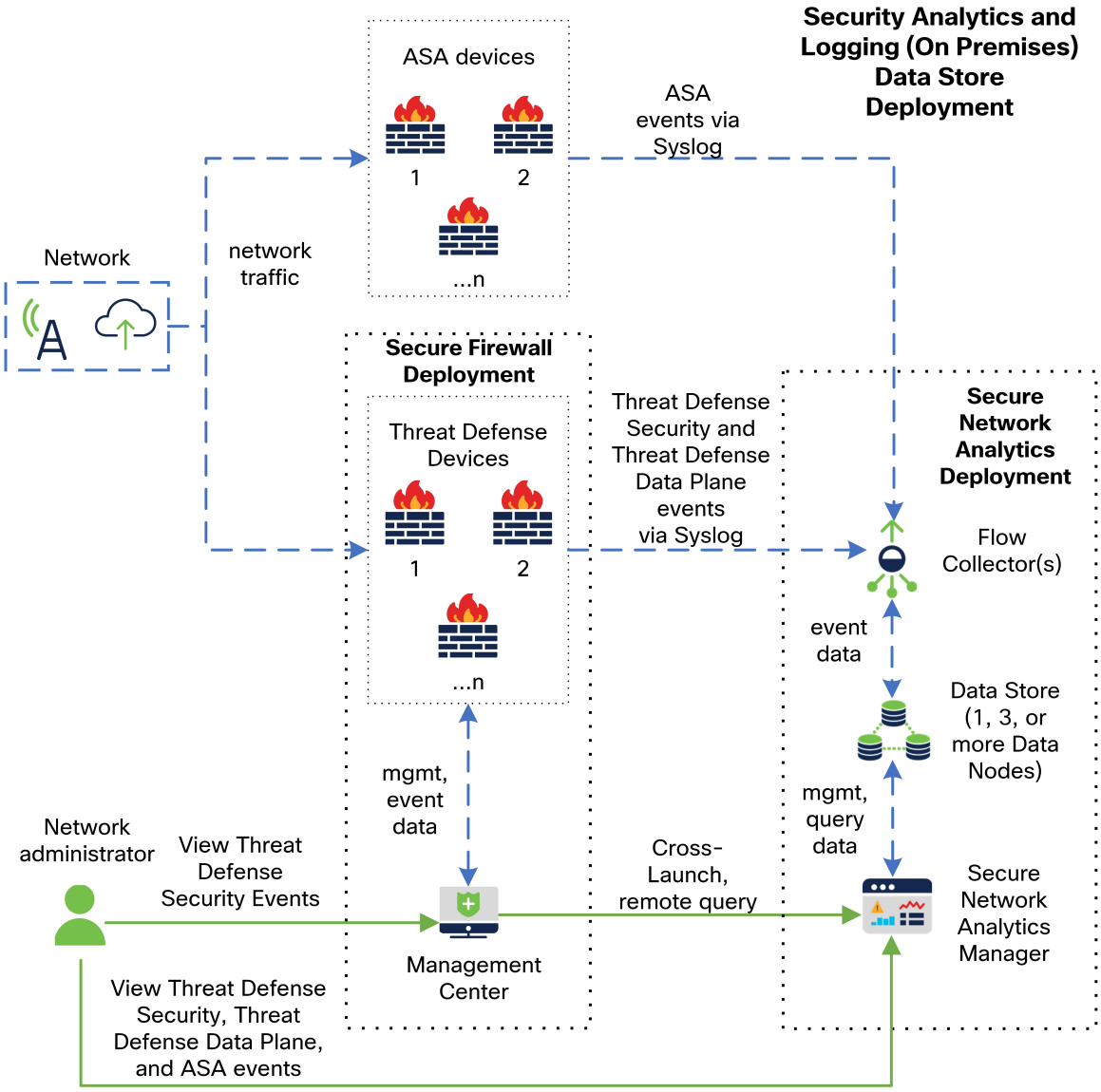
在此部署中， 威胁防御 设备将防火墙事件发送到管理器，而管理器会存储这些事件。从 管理中心 UI 中，您可以交叉启动管理器以查看有关存储事件的更多信息。此外，您可以从管理中心执行事件的远程查询。

Note Secure Network Analytics 设备版本 7.5.1 或更高版本不支持**仅管理器**部署。有关详细信息，请参阅思科安全分析和日志记录文档。

数据存储部署

部署一个 CiscoSecure Network Analytics 流量收集器来接收事件，一个 CiscoSecure Network Analytics 数据存储（包含 3 个 Cisco Secure Network Analytics 数据节点）来存储事件，以及一个可以查看和查询事件的管理器。

有关具有管理器、3 个数据节点和流量收集器的数据存储部署示例，请参阅下图：



在该部署中，威胁防御 和 ASA 设备会向流量收集器发送防火墙事件。流量收集器会将事件发送到 Data Store（3 个数据节点）进行存储。从 管理中心 UI 中，您可以交叉启动管理器以查看有关存储事件的更多信息。此外，您可以从 管理中心执行事件的远程查询。

有关将 防火墙 与SAL（本地部署）集成的详细信息，请参阅 思科安全分析与日志记录（本地部署）集成指南。

与思科安全分析和日志记录（SaaS）集成

如果需要更多空间来存储 Firewall 事件，您可以使用思科安全分析和日志记录 (SaaS) 将 Firewall 事件发送到思科安全云分析 （以前称为 Stealthwatch Cloud）进行存储，并且可以选择将您的 Firewall 事件数据可用于使用 Cisco Secure Cloud Analytics 进行安全分析。

此集成专门用于 管理中心 管理的 威胁防御 设备。未运行 防火墙 软件的设备、由 设备管理器管理的设备或由 管理中心管理的非威胁防御 设备不支持此集成。

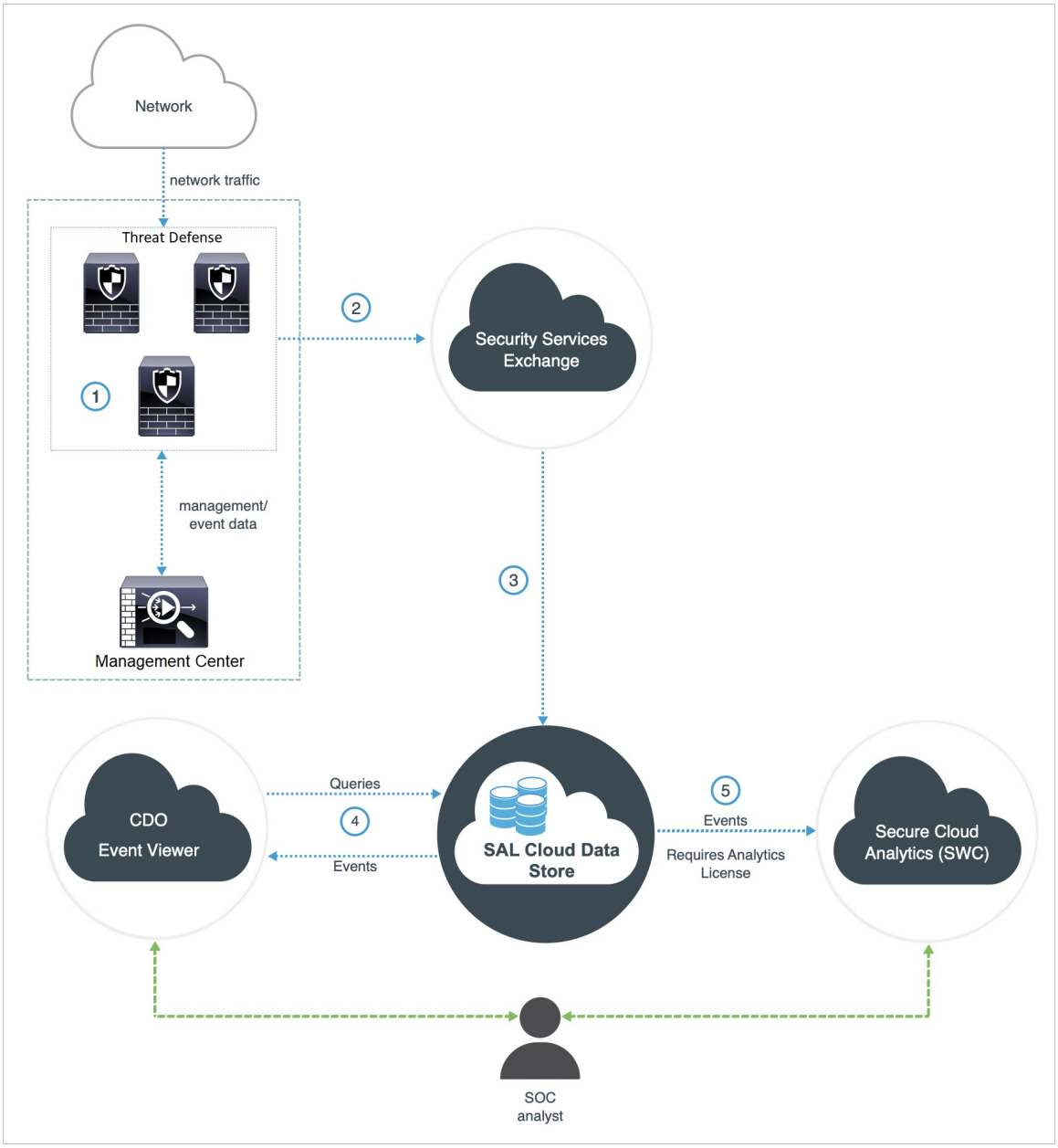
集成类型

直接集成

执行集成的受支持的 防火墙 用户角色：管理员、访问管理员、网络管理员、安全审批人

支持的最低 Firepower 版本：6.4

下图显示了直接集成的工作方式。



1	威胁防御 设备会生成事件。
2	威胁防御 设备将支持的事件发送到 安全服务交换，这是一种安全的中间云服务，用于处理思科云安全产品中使用的云到云和场所到云的标识、身份验证和数据存储。
3	安全服务交换 将事件转发到 Cisco Security Analytics and Logging (SAL) 云数据存储。

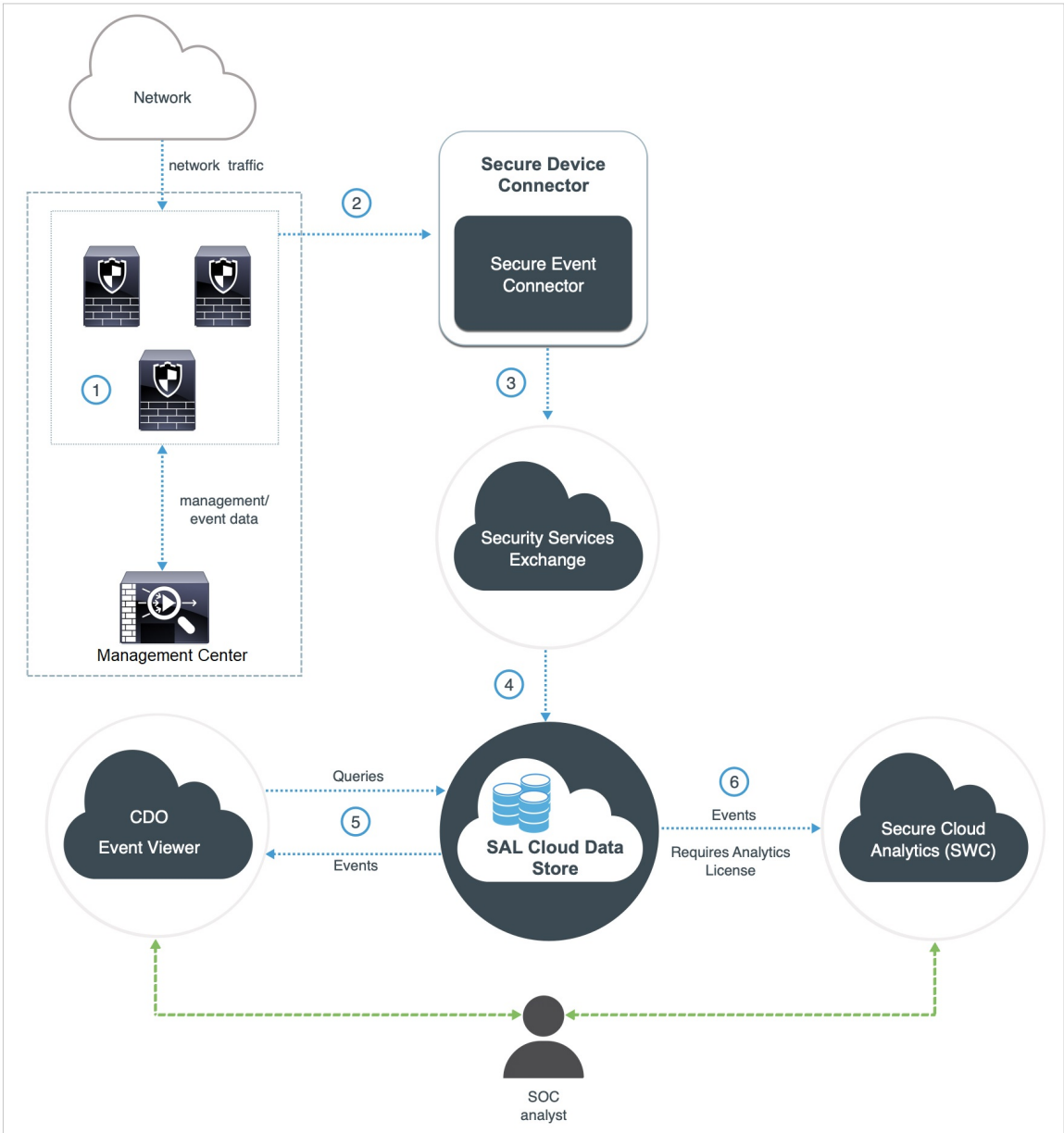
4	安全云控制 事件查看器查询 SAL 云数据存储中的事件，并为 SOC 分析师提供其他背景信息。
5	（仅具有分析许可证）Cisco Secure Cloud Analytics（以前称为 SWC）从 SAL 云数据存储库接收事件，并为SOC分析师提供对产品分析功能的访问权限。

系统日志集成

执行集成的受支持的 防火墙 用户角色：管理员、访问管理员、网络管理员、安全审批人

支持的最低 Firepower 版本：7.0

下图显示了系统日志集成的工作方式。



1	威胁防御 设备会生成事件。
2	威胁防御 设备将支持的事件作为系统日志消息发送到安装在网络中虚拟机上的 安全事件连接器 (SEC)。
3	SEC 将事件转发到 安全服务交换，这是一种安全的中间云服务，用于处理思科云安全产品中使用的云到云和场所到云的标识、身份验证和数据存储。

4	安全服务交换 将事件转发到 Cisco Security Analytics and Logging (SAL) 云数据存储。
5	安全云控制 事件查看器查询 SAL 云数据存储中的事件，并为 SOC 分析师提供其他背景信息。
6	（仅具有分析许可证）Cisco Secure Cloud Analytics（以前称为 SWC）从 SAL 云数据存储库接收事件，并为SOC分析师提供对产品分析功能的访问权限。

有关将 防火墙 与 CSAL (SaaS) 集成的详细信息，请参阅 思科 Cisco Secure Firewall Management Center 和思科安全分析与日志记录 (SaaS) 集成指南。

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. 保留所有权利。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。