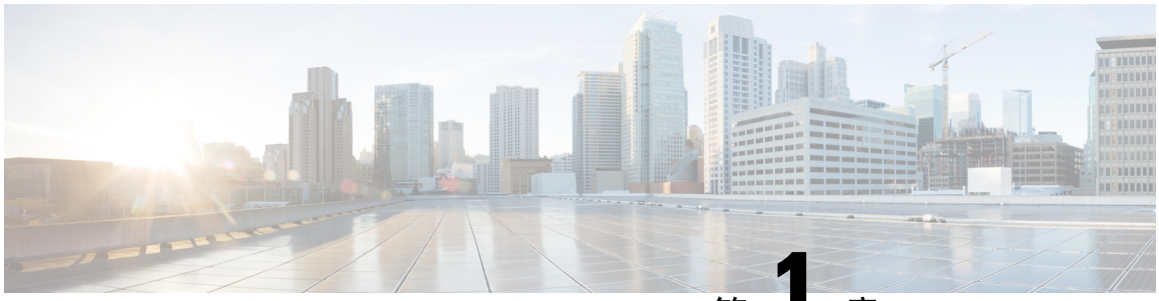
《思科安全分析和日志记录（本地部署）入门》

首次发布日期: 2021 年 5 月 26 日

上次修改日期: 2022 年 3 月 14 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2022 Cisco Systems, Inc. 保留所有权利。



第 1 章

思科安全分析和日志记录（本地部署） 入门指南：防火墙事件集成

注释 如果要将防火墙事件数据存储在思科云中而不是内部部署，请参阅思科安全分析和日志记录 (SaaS) 文档了解详细信息。

概念和架构

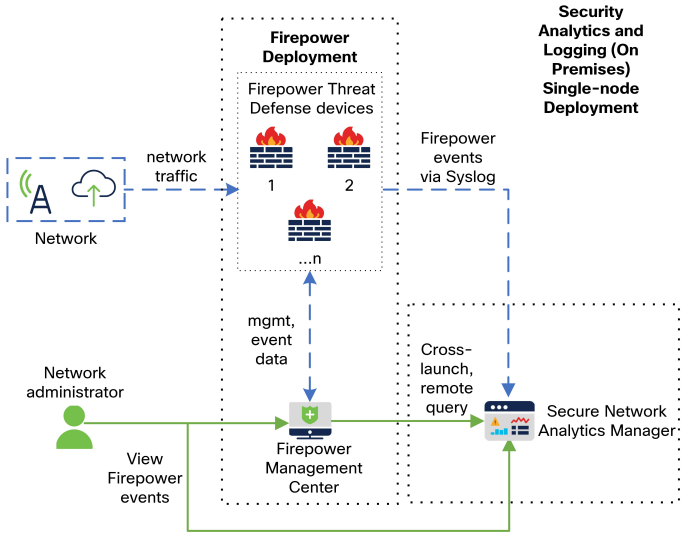
在安全分析和日志记录（本地部署）部署中，您可以使用 Secure Network Analytics 设备存储来自其他思科产品部署的数据，例如 Firepower 设备部署。在 Firepower 部署中，您可以将 Firepower 安全事件和数据平面事件从由 Firepower 管理中心管理的 Firepower Threat Defense 设备导出到管理器，以便存储这些信息。在安全分析和日志记录（本地部署）应用 v3.0.0 中，我们添加了通过系统日志将 ASA 设备中的事件导出到管理器的功能。

您的 Secure Network Analytics 部署有两个选项：

- 单节点 - 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
- 多节点 - 部署思科安全网络分析流量收集器以接收事件，部署思科安全网络分析 Data Store（包含 3 个思科安全网络分析数据节点）以存储事件，以及可从中查看和查询事件的管理器

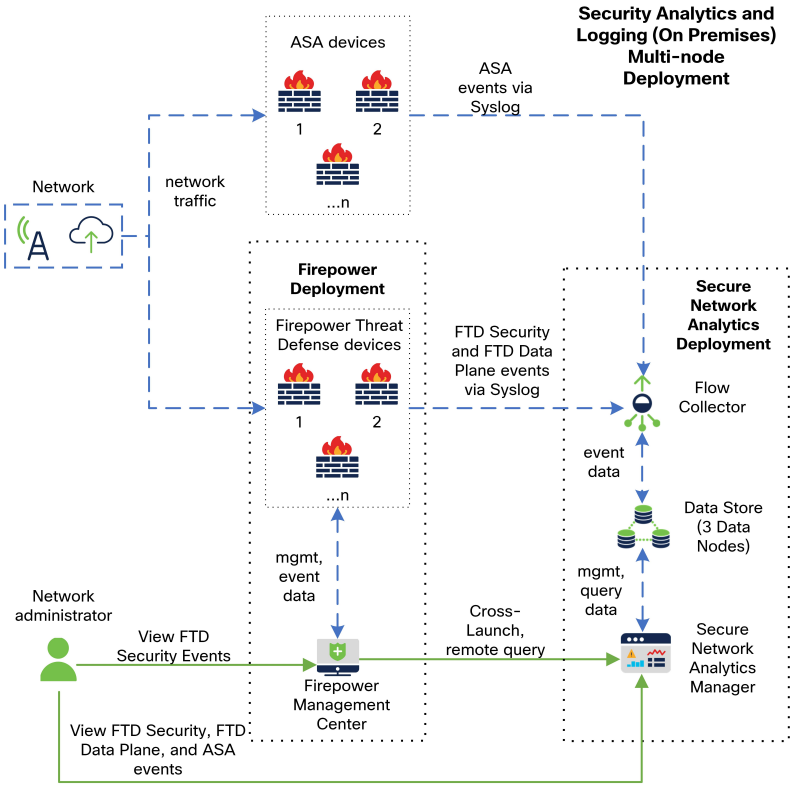
注释 我们支持在管理器上作为独立设备（单节点 ）或在管理流量收集器和 3 个数据节点（多节点）的管理器上安装应用。如果管理一个或多个流量收集器而不管理 3 个数据节点，则无法在管理器上安装该应用。有关详细信息，请参阅故障排除。

有关具有管理器的单节点 部署示例，请参阅下图：



在此部署中，Firepower Threat Defense 设备将 Firepower 事件发送到管理器，而管理器会存储这些事件。从 Firepower 管理中心 UI 中，用户可以交叉启动到管理器以查看有关存储事件的更多信息。他们还可以远程查询来自 Firepower 管理中心 的事件。

有关具有管理器、3 个数据节点和流量收集器的多节点部署示例，请参阅下图：



在该部署中，Firepower Threat Defense 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 Firepower 管理中心 UI 中，用户可以交叉启动到管理器以查看有关存储事件的更多信息。他们还可以远程查询来自 Firepower 管理中心 的事件。

参考文档

下表介绍了安全分析和日志记录（本地部署）设备兼容性、部署和使用的相关参考文档：

表 *1:*

文档	说明
Firepower 版本说明	查看 Firepower 版本说明，了解有关当前 Firepower 版本的最新信息，包括最新信息。
Secure Network Analytics 智能许可指南	查看 Secure Network Analytics 智能许可指南，了解如何注册您的 Secure Network Analytics 产品实例和许可您的 Secure Network Analytics 设备。
《Secure Network Analytics安装指南》	查看 Secure Network Analytics 安装指南，了解如何部署 Secure Network Analytics 设备以进行单节点 部署。

文档	说明
《Secure Network Analytics配置指南》	查看 Secure Network Analytics 配置指南，了解如何为Secure Network Analytics部署配置单节点 设备。
Secure Network Analytics Data Store 部署和配置指南	查看《Secure Network Analytics Data Store 部署和配置指南》，了解如何为多节点部署配置 Secure Network Analytics 设备。
Secure Network Analytics 发行说明	查看Secure Network Analytics版本说明，了解有关当前Secure Network Analytics版本的最新信息，包括最新信息。
安全分析和日志记录（本地部署）发行说明	查看安全分析和日志记录（本地部署）版本说明，了解有关当前安全分析和日志记录（本地部署）版本和安全分析和日志记录（本地部署）应用的最新信息，包括最新信息。

如果您尚未部署 Firepower 或将 Firepower 部署配置为生成预期连接、入侵、文件和恶意软件事件，请参阅以下内容：

表 *2:*

文档	说明
Firepower 兼容性指南	查看 Firepower 兼容性指南，了解 Firepower 管理中心 和 Firepower Threat Defense 设备设备型号的版本支持。
Firepower 安装和配置指南	查看 Firepower 安装和配置指南，了解如何安装和配置 Firepower 设备。
《Firepower 管理中心配置指南》	查看《Firepower 管理中心 配置指南》，了解由您的 Firepower 管理中心 管理的 Firepower Threat Defense 设备的 Firepower 设备许可和配置，访问控制策略，入侵策略和文件策略。

要求和最佳实践

以下列出了部署安全分析和日志记录（本地部署）以存储防火墙事件数据的要求和最佳实践。

下表简要概述了使用管理器在安全分析和日志记录（本地部署）部署中存储防火墙事件数据所需的解决方案组件：

防火墙设备

您必须部署以下防火墙设备：

解决方案组件	需要的版本	思科安全分析和日志记录（本地部署） 的许可	说明
Firepower 管理中心（硬件或虚拟）	v7.0+ 有关运行早期版本的 Firepower 管理中心，请参阅 https://cisco.com/go/sal-on-prem-docs。	无	• 每个 Firepower 管理中心可以部署一个管理器，以及（可选）一个流量收集器和一个 Data Store（3 个数据节点）
Firepower 托管设备 由 FMC 管理的 Firepower Threat Defense 设备（硬件或虚拟）	v7.0+，使用向导 Firepower Threat Defense v6.4 或更高版本，使用系统日志 NGIPS v6.4，使用系统日志	无	由一个 Firepower 管理中心 管理的多个 Firepower Threat Defense 设备可以将事件导出到同一个 Secure Network Analytics 部署
ASA 设备	v9.12+	无	• 在安全分析和日志记录（本地部署）应用 v3.0.0+ 和 Secure Network Analytics v7.4.0+ 多节点部署上支持

Secure Network Analytics 设备

您可以选择用于部署 Secure Network Analytics 的以下选项：

- 单节点 - 只部署一个管理器来注入和存储事件，以及审查和查询事件
- 多节点 - 部署流量收集器以注入事件，部署 Data Store 来存储事件，以及部署管理器来查看和查询事件

注释 不能同时部署 Secure Network Analytics 硬件和 Secure Network Analytics VE 设备。

表 *3:* 单节点

解决方案组件	需要的版本	安全分析和日志记录（本地部署） 的许可	说明
管理器	Secure Network Analytics v7.3.1+	无	• 可以部署管理器 2210 硬件设备或管理器虚拟版 (VE) 设备 • 可以从多个 Firepower Threat Defense 设备接收事件，所有均由一个 Firepower 管理中心管理 • 必须安装安全分析和日志记录（本地部署）应用以进行事件注入，以及在管理器 Web 应用中查看防火墙事件
安全分析和日志记录（本地部署）应用	安全分析和日志记录（本地部署）应用 v2.0+	日志记录和故障排除智能许可证，根据每天的 GB 数	在管理器上安装该应用并配置为启用事件注入

表 *4:* 多节点

解决方案组件	需要的版本	安全分析和日志记录（本地部署）的许可	说明
管理器	Secure Network Analytics v7.3.2+	无	• 可以部署管理器 2210 硬件设备或管理器虚拟版 (VE) 设备 • 必须安装安全分析和日志记录（本地部署）应用以进行事件注入，以及在管理器 Web 应用中查看防火墙事件

解决方案组件	需要的版本	安全分析和日志记录（本地部署）的许可	说明
流量收集器	Secure Network Analytics v7.3.2+	无	• 可以部署流量收集器 4210 硬件设备或流量收集器 VE 设备 • 可以从多个 Firepower Threat Defense 设备接收事件，所有均由一个 Firepower 管理中心管理 • 可以从多个 ASA 设备 (v7.4+) 接收 ASA 事件
Data Store（3 个 Data Node）	Secure Network Analytics v7.3.2+	无	• 可以部署 Data Store 6200（3 个数据节点）硬件或 Data Store VE（3 个数据节点 VE） • 可以存储流量收集器接收的防火墙事件
安全分析和日志记录（本地部署） 应用	安全分析和日志记录（本地部署） 应用 v2.0+	日志记录和故障排除智能许可证，根据每天的 GB 数	在管理器上安装该应用并配置为启用事件注入

除了这些组件之外，您还必须确保所有设备都可以使用 NTP 来同步时间。

如果要远程访问 Firepower 或 Secure Network Analytics 设备的控制台，您可以启用通过 SSH 访问。

Secure Network Analytics 许可

在评估模式下，安全分析和日志记录（本地部署）可以在没有许可证的情况下使用 90 天。若要在 90 天后继续使用安全分析和日志记录（本地部署），根据预期每天会从防火墙部署向 Secure Network Analytics 设备发送系统日志数据的 GB 数，您必须为智能许可获取日志记录和故障排除智能许可证。

注释 出于许可证计算的目的，数据量会以最接近的整数 GB 来报告（往下舍入）。例如，如果一天会发送 4.9 GB，则报告为 4 GB。

有关许可 Secure Network Analytics 设备的详细信息，请参阅《Secure Network Analytics 智能软件许可指南》。

Secure Network Analytics 资源分配

为安全分析和日志记录（本地部署）部署时，Secure Network Analytics 提供以下注入速率：

- 硬件或虚拟版本 (VE) 单节点 部署平均每秒可以注入大约 2 万个事件 (EPS)，短时间内可迅速达到 3.5 万个 EPS
- 虚拟版 (VE) 多节点部署平均可注入大约 5 万个 EPS，短时间内可迅速达到 17.5 万个 EPS
- 硬件多节点部署平均可注入大约 10 万个 EPS，短时间内可迅速达到 35 万个 EPS

根据分配的硬盘驱动器存储，您可以将数据存储数周或数月。这些估计值受各种因素影响，包括网络负载、流量峰值和每个事件传输的信息。

注释 在较高的 EPS 注入速率下，安全分析和日志记录（本地部署）应用可能会丢弃数据。此外，如果发送所有事件类型，而不是仅发送连接、入侵、文件和恶意软件事件，则应用可能会随着您的整体EPS上升而丢弃数据。在这种情况下，查看日志文件。

单节点 VE 建议

为了获得最佳性能，请在部署管理器 VE 时分配以下资源：

Resource	信息提示
CPU	12
RAM	64 GB
硬盘驱动器存储	2 TB

根据您分配的存储空间，您可以在单节点 部署中大致按以下时间范围来存储数据：

平均 EPS	平均每日事件数	1 TB 存储的预计保留期	2 TB 存储的预计保留期	4 TB 存储的预计保留期
1,000	8650 万	250 天	500 天	1000 天
5,000	4.3 亿	50 天	100 天	200 天
10,000	8.65 亿	25 天	50 天	100 天
20,000	17.3 亿	12.5 天	25 天	50 天

当管理器达到最大存储容量时，它会首先删除最早的数据，以便为传入数据腾出空间。

注释 我们已在此估计的注入和存储期间使用这些资源配置对 管理器 VE 进行了测试。如果您没有为虚拟设备分配足够的 CPU 或 RAM，您可能会发现由于资源配置不足而导致的意外错误。如果将存储分配增加到 2 TB 以上，则可能会发现由于资源配置不足而导致的意外错误。

多节点建议

为获得最佳性能，请在部署管理器 VE、流量收集器 VE 和 Data Store VE 时分配以下资源：

表 *5:* 管理器 *VE*

Resource	信息提示
CPU	8 个 Intel Xeon，最低 2.29 GHz
RAM	64 GB
硬盘驱动器存储	480 GB

表 *6:* 流量收集器 *VE*

Resource	信息提示
CPU	8 个 Intel Xeon，最低 2.29 GHz
RAM	70 GB
硬盘驱动器存储	480 GB

表 *7:* 数据节点 *VE*（作为 *Data Store* 的一部分）

Resource	信息提示
CPU	12 个 Intel Xeon，每个数据节点至少 2.29 GHz
RAM	每个数据节点 32 GB
硬盘驱动器存储	每个数据节点 VE 5 TB，或 3 个数据节点总共 15 TB

根据您分配的存储空间，您可以在多节点部署中大致按以下时间范围来存储数据：

平均 **EPS**	平均每日事件数	虚拟	硬件
1,000	8650 万	1,500 天	3,000 天
5,000	4.3 亿	300 天	600 天
10,000	8.65 亿	150 天	300 天

平均 EPS	平均每日事件数	虚拟	硬件
20,000	17.3 亿	75 天	150 天
25,000	21.6 亿	60 天	120 天
50000	43.2 亿	30 天	60 天
75,000	64.8 亿	不支持	40 天
100,000	86.4 亿	不支持	30 天

当 Data Store 达到最大存储容量时，它会首先删除最早的数据，以便为传入数据腾出空间。

注释 我们已在此估计的注入和存储期间使用这些资源配置对这些虚拟设备进行了测试。如果您没有为虚拟设备分配足够的 CPU 或 RAM，您可能会发现由于资源配置不足而导致的意外错误。如果将存储分配增加到 5 TB 以上，则可能会发现由于资源配置不足而导致的意外错误。

通信端口

下表列出了必须为安全分析和日志记录（本地部署）部署的单节点 集成打开的通信端口。

从（客户端）	到（服务器）	端口	协议或用途
外部互联网（NTP 服务器）	FMC、FTD 设备和管理器	123/UDP	NTP 时间同步，全部同步到同一台 NTP 服务器
用户工作站	FMC 和管理器	443/TCP	使用 Web 浏览器通过 HTTPS 登录设备的 Web 界面
由 FMC 管理的 FTD 设备	管理器	8514/UDP	系统日志从 FTD 设备导出，注入到管理器
FMC	管理器	443/TCP	从 FMC 远程查询到管理器

下表列出了必须为安全分析和日志记录（本地部署）部署的多节点集成打开的通信端口。此外，有关必须为 Secure Network Analytics 部署打开的端口，请参阅《Data Store 硬件部署和配置指南》或《Data Store 虚拟版部署和配置指南》。

从（客户端）	到（服务器）	端口	协议或用途
外部互联网（NTP 服务器）	FMC、FTD 设备、管理器、流量收集器和 Data Store	123/UDP	NTP 时间同步，全部同步到同一台 NTP 服务器

从（客户端）	到（服务器）	端口	协议或用途
用户工作站	FMC 和管理器	443/TCP	使用 Web 浏览器通过 HTTPS 登录设备的 Web 界面
由 FMC 管理的 FTD 设备	流量收集器	8514/UDP	系统日志从 FTD 设备导出，注入到流量收集器
ASA 设备	流量收集器	8514/UDP	系统日志从 ASA 设备导出，注入到流量收集器
FMC	管理器	443/TCP	从 FMC 远程查询到管理器

配置概述

下面介绍了配置部署以存储事件数据的高级步骤。

在开始部署之前，请查看这些任务：

组件和任务	步骤
部署单节点	您有以下选择： • 将管理器 2210 部署到您的网络并执行初始配置，包括分配 eth0 管理接口 IP 地址和其他信息。有关详细信息，请参阅《x2xx 系列硬件安装指南》和《Secure Network Analytics 系统配置指南》。 • 下载管理器 VE ISO，并将管理器 VE 部署到虚拟机监控程序。执行初始配置，并分配 eth0 管理接口 IP 地址和其他信息。有关更多信息，请参阅《Secure Network Analytics 虚拟版安装指南》。
部署多节点	您有以下选择： • 将硬件管理器、流量收集器和 3 个数据节点部署到您的网络。对每个设备执行初始配置，然后初始化 Data Store。有关详细信息，请参阅《x2xx 系列硬件（带 Data Store）设备安装指南》。 • 下载管理器 VE ISO、流量收集器 VE ISO 和数据节点 ISO。将 1 个管理器 VE、1 个流量收集器 VE 和 3 个数据节点 VE 部署到虚拟机监控程序。对每个设备执行初始配置，然后初始化 Data Store。有关详细信息，请参阅《虚拟版（带 Data Store）设备安装指南》。

组件和任务	步骤
在管理器上下载并安装安全分析和日志记录（本地部署）应用，并配置 Secure Network Analytics 部署以接收和存储防火墙事件。	• 在管理器上，转到“集中管理”(Central Management)中的“应用管理器”(App Manager) 并下载应用。将其配置为从 Firepower 设备接收事件。 • 有关使用该应用的详细信息，请参阅安全分析和日志记录（本地部署）版本说明和应用帮助。
配置 Firepower 管理中心以便将事件发送到安全分析和日志记录（本地部署）	您有以下选择： • 配置 Firepower 管理中心以便将事件发送到 Secure Network Analytics 设备。 • 使用配置数据平面事件日志来配置数据平面事件日志记录。 • 在上使用在 Firepower 管理中心 上停止存储低优先级连接事件 来减少 Firepower 管理中心 上的日志记录负载。
配置 ASA 设备以便将事件发送到安全分析和日志记录（本地部署）	• 配置 ASA 设备以便将事件发送到 Secure Network Analytics 设备。请参阅 ASA 设备配置。 • 安全分析和日志记录（本地部署）应用 v3.0.0+ 和 Secure Network Analytics v7.4.0+ 多节点部署支持 ASA 事件。
查看后续步骤	查看后续步骤： • 有关详细信息，请查看 Firepower 在线帮助。请参阅通过 Secure Network Analytics 设备上存储的连接事件在 Firepower 管理中心操作。 • 有关如何使用 Secure Network Analytics 的详细信息，请查看管理器 Web 应用在线帮助。

后续步骤

在将防火墙设备配置为将事件数据作为安全分析和日志记录（本地部署）的一部分发送到 Secure Network Analytics 设备后，您可以执行以下步骤：

- 查看 FMC 在线帮助。
- 查看 管理器 Web 应用在线帮助，了解关于 Secure Network Analytics 的更多信息。