思科安全分析和日志记录

关于安全分析和日志记录

安全分析和日志记录 (SAL) 是一项集中日志管理和高级威胁检测服务，可提供可扩展的思科防火墙日志记录及相关分析。集中日志记录有助于提供可视性，帮助解决网络访问问题（包括中断），同时启用设备和整体网络运行状况监控。分析可提供针对高级威胁的检测。

SAL 服务可通过以下两种方法使用：

- 安全分析和日志记录 (SaaS) - 一种托管软件即服务 (SaaS)，使用 Cisco Secure Cloud Analytics（以前称为 Stealthwatch 云）存储事件并提供安全分析数据。此服务会将安全分析和日志记录云数据存储连接到防火墙云管理器 思科防御协调器 (CDO)。

  在本文档中，此方法也被称为 SAL (SaaS)。

- 安全分析和日志记录（本地部署） - 在 Secure Network Analytics（以前称为 Stealthwatch）设备上运行的服务，用于在客户自己的场所存储事件日志。此服务将 安全分析和日志记录（本地部署） 数据连接到本地管理器，Cisco Secure Firewall Management Center。

  在本文档中，此方法也被称为 SAL（本地）。

有关 安全分析和日志记录 的详细信息，请参阅 https://www.cisco.com/c/en/us/products/security/security-analytics-logging/index.html。

SAL 远程事件存储和监控选项的比较

SAL 集成显示了在 管理中心 和 CDO 外部的存储事件数据的类似选项：

	SAL（本地）	SAL (SaaS)
为什么选择此解决方案？	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。	您希望发送防火墙事件进行存储，并使用 Cisco Secure Cloud Analytics 选择性地让防火墙事件数据可用于安全分析。
许可	购买、许可并设置防火墙后的存储系统。 有关详细信息，请参阅SAL（本地） 的许可 ，第 3 页	购买许可证和数据存储计划，并将数据发送到思科云。 有关详细信息，请参阅SAL (SaaS) 的许可 ，第 8 页
支持的事件类型	• 连接 • 文件和恶意软件 • 入侵 • LINA • 安全情报	• 连接 • 文件和恶意软件 • 入侵 • 安全情报
支持的事件发送方法	支持系统日志和直接集成。	支持系统日志和直接集成。
事件查看	• 查看 Cisco Secure Network Analytics 管理器上的事件。 • 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智能事件	在 CDO 中查看事件，或者 Cisco Secure Network Analytics 管理器，具体取决于您的许可证。从管理中心 事件查看器交叉启动。

关于SAL（本地）

您可以配置 SAL（本地） 以存储防火墙事件数据，从而在更长的保留期内增加存储量。通过部署安全网络分析设备并将其与防火墙部署集成，您可以将事件数据导出到安全网络分析设备。

这会为您提供以下功能：

- 在 Cisco Secure Network Analytics 设备上存储事件。
- 指定此远程数据源以便在管理中心查看这些事件。
- 使用事件查看器从安全网络分析管理器（以前称为 Stealthwatch 管理控制台）Web 应用 UI 中查看事件数据。
- 从管理中心 UI 交叉启动到事件查看器，以便查看有关交叉启动信息的其他情景。

SAL（本地） 的许可

您必须获取日志记录和故障排除智能许可证才能使用 SAL（本地）。您可以根据预期的数据量获取许可证，同时每天将系统日志数据从防火墙部署发送到您的 Secure Network Analytics 设备。

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

有关可用 SAL（本地） 许可选项的信息，请参阅《思科安全分析和日志记录订购指南》。

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

管理 CDO 托管 威胁防御 设备的 SAL（本地）

从 Cisco Secure Firewall Threat Defense（以前称为 Firepower 威胁防御）版本 7.2 开始，您可以选择将由 CDO 托管的 威胁防御 设备生成的完全限定事件发送到 管理中心。管理中心 会接收并显示这些事件的数据分析。接收和显示事件数据的 管理中心 也称为仅分析管理中心。。

如果已启用设备以使用 SAL（本地） 向 Cisco Secure Network Analytics 管理器 发送连接事件，您可以在管理中心的事件查看器和情景管理器中查看和使用这些远程存储的事件，并在生成报告时包括这些事件。通过部署 Secure Network Analytics 设备并将其与防火墙部署集成，您可以将事件数据导出到安全网络分析设备。这让您能够在管理中心 UI 中查看和管理事件。您还可以从管理中心 UI 交叉启动到 Cisco Secure Network Analytics 管理器，以便查看和管理事件数据。

管理中心可以接收和显示以下 CDO 托管 威胁防御 设备的事件分析：

- 已载入 CDO 的新设备或现有 威胁防御 设备

  有关将 威胁防御 设备载入 CDO 的信息，请参阅将设备载入 云交付的防火墙管理中心的前提条件。

  工作流程如下：

  1. 将 威胁防御 设备载入 CDO。

     使用将设备载入 云交付的防火墙管理中心的前提条件中所述的载入方法来载入 威胁防御 设备。载入过程包括分配策略和选择适当的许可证。

2. 在相应的管理中心注册此 威胁防御设备。

   要使管理中心显示由 CDO 管理的 威胁防御 设备生成的事件，必须在管理中心注册该 威胁防御 设备。要在 管理中心 中注册此设备，请使用 **configure manager add** {*hostname* | *IPv4_address* | *IPv6_address*}*reg_key*[*nat_id*] CLI 启用要注册的设备，然后使用 **CDO 托管设备 (CDO Managed Device)** 复选框将设备添加到 管理中心。

注释 注册密钥和 NAT ID 必须与在将设备载入 CDO 时使用的密钥和 NAT ID 不同。

   有关详细信息，请参阅《Firepower 管理中心设备配置指南》中的将设备添加到管理中心和使用 *CLI* 完成威胁防御初始配置。

3. 在管理中心查看事件或交叉启动到已配置的 Cisco Secure Network Analytics 管理器。

   在管理中心事件查看器中查看和处理事件。如果 Secure Network Analytics 设备已部署并与防火墙部署集成，则可以将事件数据导出到 Secure Network Analytics 设备。这使您可以从管理中心 UI 交叉启动到 Cisco Secure Network Analytics 管理器，以便查看和管理事件数据。

   有关详细信息，请参阅事件和清单以及使用外部工具的事件分析。

- 管理中心的现有 威胁防御 设备。

  您可以使用更改威胁防御管理器功能将 威胁防御 设备的管理从管理中心更改为 CDO。更改威胁防御管理器功能使您能够将 威胁防御 设备管理从管理中心更改为 CDO。在更改管理器时，您可以选择将这些威胁防御设备生成的事件数据保留在管理中心。如果您选择将事件数据保留在管理中心，则仅在分析模式下才会在管理中心上保留 威胁防御 设备的副本。

  有关详细信息，请参阅将 Cisco Secure Firewall Threat Defense 迁移到云。

  工作流程如下：

  1. 将管理中心载入 CDO

     要将现有的 威胁防御 设备从管理中心载入 CDO，您必须将相应的管理中心载入 CDO。

     有关详细信息，请参阅载入 FMC。

  2. 完成变更威胁防御管理流程

     在更改威胁防御管理过程中更改设备管理器时，您可以选择将这些 威胁防御 设备生成的事件数据保留在管理中心。

     有关详细信息，请参阅将 Cisco Secure Firewall Threat Defense 迁移到云。

  3. 在管理中心查看事件或交叉启动到已配置的 Secure Network Analytics 设备。

     在管理中心事件查看器中查看和处理事件。如果 Secure Network Analytics 设备已部署并与防火墙部署集成，则可以将事件数据导出到 Secure Network Analytics 设备。这使您可以从管理中心 UI 交叉启动到 Cisco Secure Network Analytics 管理器，以便查看和管理事件数据。

     有关详细信息，请参阅事件和清单以及使用外部工具的事件分析。

配置 SAL（本地） 集成

您可以使用以下部署选项之一将 CDO 配置为将事件发送到安全网络分析设备：

- 仅安全网络分析管理器 - 部署独立管理器以接收和存储事件。威胁防御设备会将事件数据发送到网络分析管理器。所有事件数据都会被存储在网络分析管理器上。从管理中心用户界面中，您可以交叉启动管理器以查看有关存储事件的更多信息。
- 安全网络分析数据存储 - 部署思科安全网络分析流收集器以接收事件，部署思科安全网络分析数据存储（包含 3 个思科安全网络分析数据节点）以存储事件和管理器。威胁防御设备会将事件数据发送到流收集器，然后再将事件发送到数据存储进行存储。从管理中心用户界面中，您可以交叉启动管理器以查看有关存储事件的更多信息。

  从 威胁防御 版本 7.2 开始，您可以选择将不同的流收集器关联到不同的设备。

配置 Cisco Secure Network Analytics 管理器

配置 Cisco Secure Network Analytics 管理器 部署以便将 SAL（本地） 与 CDO 托管的 威胁防御 设备集成。

开始之前

请确保执行以下操作：

- 您有一个已调配的 CDO 租户，并具有以下 CDO 用户角色：
  - 管理
  - 超级管理员
- 您的 威胁防御 设备按预期工作，并且正在生成事件。
- 如果您当前使用系统日志将事件从支持直接发送事件的设备版本发送到 Cisco Secure Network Analytics 管理器，请禁用这些设备的系统日志（或为这些设备分配不包含系统日志配置的访问控制策略），以避免在远程卷上复制事件。
- 您有 Cisco Secure Network Analytics 管理器 的主机名或 IP 地址。

注释 您可能会在注册过程中从Cisco Secure Network Analytics管理器注销；请完成所有正在进行的工作，然后再开始使用部署向导。

过程

步骤 1 登录 CDO。

步骤 2 从 CDO 菜单中，导航至 **工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)**。

步骤 3 选择**防火墙管理中心 (Firewall Management Center)**，然后点击**配置 (Configuration)**。

步骤 4 导航至**集成 (Integration)** > **安全分析和日志记录 (Security Analytics & Logging)**。

步骤 5 在**仅 Cisco Secure Network Analytics 管理器 (Secure Network Analytics Manager Only)** 构件中，点击**开始 (Start)**。

步骤 6 输入 Cisco Secure Network Analytics 管理器 的主机名或 IP 地址和端口号，然后点击**下一步 (Next)**。

步骤 7 将更改部署到托管设备。

在将日志记录策略更改部署到已注册的威胁防御设备之前，事件数据不会被记录到SAL（本地）。

注释 如果必须更改其中任何配置，请再次运行向导。如果禁用配置或再次运行向导，则会保留除帐户凭证之外的所有设置。

您可以在管理中心的事件查看器和情景管理器中查看和使用这些远程存储的事件，并在生成报告时包括这些事件。您还可以从管理中心中的事件交叉启动，以便查看 Secure Network Analytics 设备上的相关数据。

有关详情，请参阅管理中心的在线帮助。

步骤 8 点击**确定 (OK)**。

配置 Secure Network Analytics 数据存储

配置 Secure Network Analytics 数据存储部署以便将 SAL（本地） 与 CDO 管理的 威胁防御 设备集成。

开始之前

请确保执行以下操作：

- 您有一个已调配的 CDO 租户，并具有以下 CDO 用户角色：
  - 管理
  - 超级管理员
- 您的 威胁防御 设备按预期工作，并且正在生成事件。
- 如果您当前使用系统日志将事件从支持直接发送事件的设备版本发送到安全网络分析设备，请禁用这些设备的系统日志（或为这些设备分配不包含系统日志配置的访问控制策略），以避免在远程卷上复制事件。
- 收集以下信息：
  - Cisco Secure Network Analytics 管理器 的主机名或 IP 地址。
  - 流收集器的 IP 地址。

注释 您可能会在注册过程中从Cisco Secure Network Analytics管理器注销；请完成所有正在进行的工作，然后再开始使用部署向导。

过程

步骤 1 登录 CDO。

步骤 2 从 CDO 菜单中，导航至 **工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)**。

步骤 3 选择**防火墙管理中心 (Firewall Management Center)**，然后点击**配置 (Configuration)**。

步骤 4 导航至**集成 (Integration)** > **安全分析和日志记录 (Security Analytics & Logging)**。

步骤 5 在**仅 Cisco Secure Network Analytics 数据存储 (Secure Network Analytics Data Store)** 构件中，点击**开始 (Start)**。

步骤 6 输入流收集器的主机名或 IP 地址和端口号。

要添加更多流收集器，请点击 **+添加其他流收集器 (+Add another Flow Collector)**。

步骤 7 如果配置了多个流收集器，请将托管设备与不同的流收集器相关联：

注释 默认情况下，所有托管设备都会被分配给默认流收集器。

a) 点击**分配设备 (Assign Devices)**。
b) 选择要分配的托管设备。
c) 从重新分配设备下拉列表中选择流收集器。

如果您不希望托管设备将事件数据发送到任何流收集器，请选择该设备，然后从重新分配设备的下拉列表中选择**不记录到流收集器 (Do not log to flow collector)**。

您可以通过将鼠标悬停在预期的流收集器上并点击**设置默认值 (Set default)** 来更改默认流收集器。

d) 点击 **Apply Changes**（应用更改）。
e) 点击**下一步 (Next)**。

步骤 8 点击**下一步 (Next)**。

步骤 9 将更改部署到已注册的托管设备。

在将日志记录策略更改部署到已注册的威胁防御设备之前，事件数据不会被记录到SAL（本地）。

注释 如果必须更改其中任何配置，请再次运行向导。如果禁用配置或再次运行向导，则会保留除帐户凭证之外的所有设置。

您可以在管理中心的事件查看器和情景管理器中查看和使用这些远程存储的事件，并在生成报告时包括这些事件。您还可以从管理中心中的事件交叉启动，以便查看 Cisco Secure Network Analytics 管理器 上的相关数据。

有关详情，请参阅管理中心的在线帮助。

关于SAL (SaaS)

SAL (SaaS) 允许您从所有威胁防御设备捕获连接、入侵、文件、恶意软件和安全情报事件，并在CDO中的一个位置进行查看。事件存储在思科云中，可从CDO中的“事件日志记录”(Event Logging)页面查看，您可以在其中过滤和查看事件，以便清楚地了解在网络中触发的安全规则。

通过额外许可，在捕获这些事件后，您可以从CDO交叉启动为您调配的安全云分析门户。安全云分析是一种软件即服务 (SaaS) 解决方案，通过对事件和网络流数据执行行为分析来跟踪网络状态。通过从源（包括防火墙事件和网络流数据）收集有关网络流量的信息，它会创建有关流量的观察结果，并根据其流量模式自动识别网络实体的角色。使用此信息与其他威胁情报来源（例如 Talos）相结合，安全云分析会生成警报，警告可能存在恶意行为。除警报外，安全云分析还提供网络和主机可视性以及所收集的情景信息，为您研究警报和查找恶意行为的来源提供更好的基础。

SAL (SaaS) 的许可

SAL (SaaS) 许可证允许您使用 CDO 租户来查看防火墙日志和思科 Cisco Secure Cloud Analytics 分析实例，而无需为这些产品单独持有许可证。

有关可用 SAL (SaaS) 许可选项的详细信息，请参阅《思科安全分析和日志记录订购指南》。

配置 SAL (SaaS) 集成

要部署此集成，您必须使用系统日志或直接连接在 SAL (SaaS) 中设置事件数据存储。

- 使用系统日志将事件发送到 SAL (SaaS)，第 9 页
- 使用直接连接将事件发送到 SAL (SaaS)，第 11 页

SAL (SaaS)集成的要求

要求类型	要求
Cisco Secure Firewall Threat Defense	• CDO管理的独立威胁防御设备，版本7.2及更高版本。 • 使用系统日志发送事件：威胁防御版本 6.4 或更高版本 • 直接发送事件：威胁防御版本 7.2 • 必须部署防火墙系统并成功生成事件。

要求类型	要求
区域云	• 确定要向其发送事件的区域云。 • 无法在不同的区域云之间查看或移动事件。 • 如果您使用直接连接将事件发送到云以与 SecureX 或思科 SecureX 威胁响应集成，则必须使用相同的区域 CDO 云来进行此集成。 • 如果直接发送事件，则在 CDO 中指定的区域云必须与 CDO 租户的区域相匹配。
数据计划	• 您必须购买一个数据计划，以反映思科云每天从威胁防御设备接收的事件数量。这称为“每日注入速率”。 • 使用日志记录量估算器工具来估算您的数据存储要求。
帐户	当您购买此集成的许可证时，系统会为您提供一个 CDO 租户账户来支持集成。

使用系统日志将事件发送到 SAL (SaaS)

此程序记录从CDO管理的设备发送安全事件（连接、安全情报、入侵、文件和恶意软件事件）的系统日志消息的最佳实践配置。

开始之前

- 配置策略以生成安全事件，并验证您希望看到的事件显示在“分析”菜单下的适用表中。
- 收集系统日志服务器 IP 地址，端口和协议（UDP 或 TCP）

  从 CDO 浏览器窗口右上角的用户菜单中选择**安全连接器 (Secure Connectors)**，以查看所需的信息。
- 确保您的设备可以访问系统日志服务器。

过程

步骤 1 登录 CDO。

步骤 2 从 CDO 菜单中，导航至 **工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)**。

步骤 3 选择**防火墙管理中心 (Firewall Management Center)**，然后点击**配置 (Configuration)**。

步骤 4 为威胁防御设备配置系统日志设置：

a) 导航至**设备 (Devices)** > **平台设置 (Platform Settings)** 并编辑与您的威胁防御设备关联的平台设置策略。

b) 在左侧导航窗格中，点击**系统日志 (Syslog)** 并配置系统日志设置，如下所示：

点击	要执行以下操作
日志记录设置	启用日志记录，制定 FTP 服务器设置，以及闪存用法。
日志记录目标	启用对特定目标的日志记录，并指定对邮件严重性级别、事件类或自定义事件列表的过滤。
邮件设置	指定用作以邮件形式发送的系统日志消息的源地址的邮件地址。
事件列表	定义包括事件类、严重性级别和事件 ID 的自定义事件列表。
速率限制	指定发送到所有配置的目标的邮件数量，并定义要为其分配速率限制的邮件严重性级别。
系统日志设置	指定日志记录设施，启用时间戳包含，并启用其他设置以将服务器设置为一个系统日志目标。
系统日志服务器	为指定为日志记录目标的系统日志服务器指定 IP 地址、使用的协议、格式和安全区域。

c) 点击**保存 (Save)**。

步骤 5 配置访问控制策略的常规日志记录设置（包括文件和恶意软件日志记录）：

a) 导航至 **策略 (Policies)** > **访问控制 (Access Control)** 以编辑与威胁防御设备关联的访问控制策略。

b) 点击**日志记录 (Logging)** 选项卡并配置访问控制策略的常规日志记录设置（包括文件和恶意软件日志记录），如下所示：

点击	要执行以下操作
使用特定系统日志警报发送	从现有的预定义警报列表中选择一个系统日志警报，或者通过指定名称、日志主机、端口、设施和严重程度来添加一个警报。
使用在设备上部署的 FTD 平台设置策略中配置的系统日志设置	通过在“平台设置”中配置系统日志配置并重新使用访问控制策略中的设置来统一系统日志配置。所选的严重性适用于所有连接和入侵事件。默认严重性为警报。
发送 IPS 事件的系统日志消息	将事件作为系统日志消息发送。除非覆盖，否则将使用上面设置的默认值。
发送文件和恶意软件事件的系统日志消息	将文件和恶意软件事件作为系统日志消息发送。除非覆盖，否则将使用上面设置的默认值。

c) 点击**保存**。

步骤 6 为访问控制策略启用安全情报事件日志记录：

a) 在同一访问控制策略中，点击 **安全情报** 选项卡。

b) 在以下每个位置，点击**日志记录 (Logging)** 图标并启用连接的开始和结束和系统日志服务器：

- 在**DNS 策略 (DNS Policy)** 旁边。
- 在**阻止列表 (Block List)** 框中，对于**网络 (Networks)** 和 **URLs**。

c) 点击**保存**。

步骤 7 为访问控制策略中的每个规则启用系统日志记录：

a) 在同一访问控制策略中，点击 **规则** 选项卡。

b) 点击要编辑的规则。

c) 点击规则中的**日志记录 (Logging)** 选项卡。

d) 在连接开始和结束时启用。

e) 如果要记录文件事件，请选择 **日志文件**。

f) 启用 **系统日志服务器**。

g) 验证规则是“**在访问控制日志记录中使用默认系统日志配置**”。

h) 点击**保存 (Save)**。

i) 对策略中的每个规则重复上述步骤。

下一步做什么

如果完成更改，请将更改部署到托管设备。

使用直接连接将事件发送到 SAL (SaaS)

配置 云交付的防火墙管理中心 以便直接向 SAL (SaaS) 发送事件。

开始之前

- 将设备载入云交付的防火墙管理中心，将许可证分配给这些设备，然后将这些设备配置为直接将事件发送到 SAL (SaaS)。
- 通过编辑规则并选择**在连接开始时记录 (Log at Beginning of Connection)** 和**在连接结束时记录 (Log at End of Connection)** 选项来启用基于每个规则的连接日志记录。

过程

步骤 1 登录 CDO。

步骤 2 从 CDO 菜单中，导航至 **工具和服务 (Tools & Services)** > **防火墙管理中心 (Firewall Management Center)**。

步骤 3 选择 **Firewall 管理中心 (Firewall Management Center)**，然后在右侧的“设置”(Settings) 窗格中，选择**思科云事件 (Cisco Cloud Events)**。

步骤 4 在**配置思科云事件 (Configure Cisco Cloud Events)** 构件中，执行以下操作：

1. 点击**将事件发送到云 (Send Events to the Cisco Cloud)** 滑块以启用整个配置。
2. 选中**将入侵事件发送到云 (Send Intrusion Events to the cloud)** 复选框以将入侵事件发送到云。
3. 选中**将文件和恶意软件事件发送到云 (Send File and Malware Events to the cloud)** 复选框，将文件和恶意软件事件发送到云。
4. 选择一个选项以便将连接事件发送到云：
   - 点击**无 (None)** 单选按钮可不将连接事件发送到云。
   - 点击**安全事件 (Security Events)** 单选按钮，仅将安全情报事件发送到云。
   - 点击**全部 (All)** 单选按钮，将所有连接事件发送到云。
5. 点击**保存 (Save)**。

查看和处理 CDO 中的事件

过程

步骤 1 登录 CDO。

步骤 2 从 CDO 菜单中，选择 **分析 (Analytics)** > **事件日志记录 (Event Logging)**。

步骤 3 使用**历史 (Historical)** 选项卡查看所有历史事件数据。默认情况下，查看器会显示此选项卡。

步骤 4 要查看实时事件，请点击**实时 (Live)** 选项卡。

有关可以在此页面上执行的操作的详细信息，请参阅 CDO 在线帮助。

查看和处理思科安全云分析中的事件

开始之前

为确保事件无缝传输，在使用事件查看器之前，请在 Stealthwatch 云门户中执行以下操作：

- 验证 Cisco Secure Cloud Analytics 是否与正确的 CDO 租户集成。

  要查看 CDO 租户，请点击**设置 (Settings)** > **传感器 (Sensors)**。
- 将要监控的子网添加到 Cisco Secure Cloud Analytics。

要添加子网，请点击**设置 (Settings)** > **子网 (Subnets)**。

过程

步骤 1 登录 CDO。

步骤 2 从 CDO 菜单中，选择 **分析 (Analytics)** > **安全云分析 (Secure Cloud Analytics)**。

Cisco Secure Cloud Analytics 门户将在新的浏览器选项卡中打开。

步骤 3 点击**调查 (Investigate)** > **事件查看器 (Event Viewer)**。

有关详细信息，请参阅 Cisco Secure Cloud Analytics 联机帮助。

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。