统一事件

统一事件

统一事件是 Firewall Management Center 的一项防火墙事件监控功能，它可以：

- 提供各种防火墙事件类型的单一屏幕视图，包括连接事件、入侵事件、文件事件、恶意软件事件和安全相关连接事件。
- 在表中将相关事件堆叠在一起，以提供有关安全事件的更多背景信息。
- 关联相关事件，以便您可以更好地了解和排查网络问题，而无需在多个事件查看器之间切换。

统一事件表中的**实时视图**选项可让您实时查看防火墙事件并监控网络活动。例如，如果您是防火墙管理员，在进行策略更改后查看实时事件更新有助于确保更改在您的网络上正确实施。

统一事件表可高度自定义。您可以创建和应用自定义过滤器，以微调事件查看器上显示的信息。您可以保存经常使用的特定需求的自定义过滤器，并快速加载这些已保存的过滤器。可以通过添加、删除、固定列或重新排序列来自定义事件表。

使用统一事件的要求

在 Firewall Management Center 中使用**统一事件**之前，请确保满足以下要求。

- 您必须具有**管理员**、**安全分析师**或**安全分析师（只读）**权限才能访问**统一事件**功能。
- 您必须在设备上配置必要的策略并启用日志记录设置，以生成安全事件并在**统一事件**页面上显示它们。

使用统一事件

在单个表中查看和处理各种防火墙事件，而无需在多个事件查看器之间切换。

使用此视图：

- 在统一视图中查找不同类型事件之间的关系。
- 实时查看策略更改的影响。

Before you begin

您必须具有 管理员 或 安全分析师 权限才能执行此任务。

过程

步骤 1 选择**事件和日志** > **分析** > **统一事件**。

步骤 2 选择时间范围（固定或滑动）。

有关详细信息，请参阅在统一事件中设置时间范围，第 5 页。

步骤 3 如果要在 Cisco Secure Network Analytics 设备上远程存储事件，并且有充分的理由更改数据源，请选择数据源。

请查看 在 Cisco Secure Network Analytics 设备上存储的连接事件中的 Cisco Secure Firewall Management Center 工作中的重要信息。

步骤 4 您可以过滤统一事件表最初显示的大量防火墙事件，以了解网络中事件的更精细情景。

有关详细信息，请参阅统一事件中的过滤器，第 7 页。

步骤 5 选择更多选项：

要执行此操作...	请
自定义列	• 添加或删除列： 点击列选择器 ( ) 并选择列。某些字段中的值取决于事件类型。每个字段旁边显示的以下图标表示事件类型对应关系： • 连接事件 ( ) • 安全相关的连接事件 （ ） • 入侵事件 ( ) • 文件事件 ( ) • 恶意软件事件 ( ) • 事件 ( ) 故障排除 点击列集过滤选项旁边的事件图标，可根据所选事件类型过滤事件字段列表。 **注释** 包含许多列可能会降低性能。您可以通过展开事件行查看事件详细信息来查看隐藏列的数据。 • 对列重新排序： 拖放列标题。 • 将列固定（冻结）到表的左侧或右侧，使它们不会滚动： • 将列拖至表格的左侧或右侧，或将列标题拖放到固定区域。 • 要取消固定列，请将该列拖出固定区域。 • 调整列大小。 • 将列恢复为默认设置。 • 保存列集以便以后快速重新加载自定义视图。有关更多信息，请参阅保存列集 ， 第 9 页主题。 数据始终按时间排序，最新事件排在最前面。

要执行此操作...	请
按事件类型快速筛选	事件类型过滤器按钮位于左上方，可让您快速应用事件类型过滤器。每个事件类型按钮都会显示所选时间范围内可用事件的数量。点击事件类型按钮可包含或排除该事件类型。 **图 *1:* 事件类型过滤按钮**  **注释** “**故障排除**” 选项卡下显示 **故障排除事件** ( ) 按钮。要查看故障排除事件，必须在威胁防御设备平台设置策略中启用记录所有故障排除系统日志。有关详细信息，请参阅在 Cisco Secure Firewall Management Center 查看故障排除系统日志。
识别相关事件	点击一行可突出显示与此事件相关的其他事件。 如果需要，过滤事件以显示足够小的事件集。 **注释** 连接的发起方不一定与恶意软件文件的发送方相同。通过使用**源或目标 IP** 过滤器过滤统一事件表，搜索与连接事件关联的文件或恶意软件事件。
查看事件详情	点击行左端的 > （拓展）图标。事件详细信息不包括没有要显示的数据的字段。 **提示** 或者，双击事件行可查看 **事件详细信息** 窗格。当 **事件详细信息** 窗格打开时，点击表中的任何事件行以加载该事件的详细信息。
使用 Packet Tracer 对事件进行故障排除	1. 点击要运行数据包跟踪的行旁边的省略号图标 (⋮)。 2. 选择 **打开 Packet Tracer**，根据事件的源和目标寻址以及协议特征，在 Packet Tracer 工具中为数据包建模。跟踪模拟数据包并使用跟踪结果对安全事件进行故障排除。有关如何使用数据包跟踪器工具的详细信息，请参阅 运行数据包跟踪。
实时查看事件	点击 **上线**。有关详细信息，请参阅在统一事件中启用实时事件监控，第 6 页。 如果事件流过快，请输入过滤条件。
交叉启动到外部资源	点击表格单元格中的省略号(⋮)，查看可用于该单元格值的选项（如果有）。 有关详细信息，请参阅使用基于 Web 的资源的事件调查。

要执行此操作...	请
打开多个统一事件窗口	• 您可以使用多个浏览器选项卡或窗口显示统一事件表的不同视图。 • 每个新选项卡或窗口都具有最近修改的选项卡/窗口的特征。 • 要将任何打开的选项卡/窗口设置为模板，请对其进行细微更改。 • 多个选项卡中的查询按顺序处理。 • 根据视图（例如，复杂查询或传入事件速率较高时在实时视图模式的查看），如果同时打开超过 4 个选项卡，性能可能会降低。
保存搜索	将自定义搜索保存为您的收藏，并在以后快速加载。有关详细信息，请参阅在统一事件中保存搜索，第 8 页。
为查询结果添加书签或共享	将 URL 加入书签或复制粘贴到浏览器窗口中。 • 如果 URL 使用滑动时间范围，则稍后将检索不同的事件。 • 列可视性、大小和顺序以及实时流设置不会在 URL 中捕获。

在统一事件中设置时间范围

在统一事件中设置时间范围，以查看特定时间段内的防火墙事件，并控制表中显示哪些事件。

当您更改时间范围时，统一事件表会自动刷新以反映您的更改。您选择的时间范围不适用于事件查看器中的其他表。例如，您在查看连接事件时选择的时间范围不适用于统一事件表，反之亦然。

注释 如果您的时间窗口向后延伸超出了连接事件的保留期，请在 **事件和日志** > **+ 显示更多** > **连接** > **安全相关事件** 下的表中查找与安全相关的连接事件。

过程

步骤 1 选择**事件和日志** > **分析** > **统一事件**。

默认情况下，统一事件表显示过去一小时的事件。

步骤 2 点击当前时间范围。

步骤 3 选择以下其中一个选项：

- 如果要查看固定时间范围内的事件，请点击 **固定时间范围** 并选择 **开始时间** 和 **结束时间**。

要将当前时间设置为**结束时间**，请点击**现在**。

- 如果您想要一个滑动的默认时间窗口（例如过去一小时），请选择**滑动时间范围**并指定所需的时间长度。

  该表显示从特定开始时间（例如过去一小时）相对于现在生成的所有事件。刷新视图可确保窗口始终显示最近一小时的活动。

步骤 4 点击**应用 (Apply)**。

在统一事件中启用实时事件监控

配置**统一事件**以实时显示防火墙事件，无需手动刷新。

当实时视图模式处于活动状态时，安全事件在您的网络中发生时，事件日志会实时显示。这使您能够快速识别和解决安全事件。

过程

步骤 1 选择**事件和日志** > **分析** > **统一事件**。

默认情况下，**统一事件**表会显示过去一小时的历史事件。

步骤 2 点击**上线**查看新事件。

新事件显示在事件表的顶部。时间范围部分包含一个计时器，指示实时视图已处于活动状态的时间长度。

注释
使用**上线功能**时，此限制适用于 UDP 流量：

- 默认情况下，防火墙管理中心 中的**上线**功能会考虑过去 30 秒的流量数据，这比 UDP 连接被处理并包含在**统一事件**表中所需的 120 秒要短。这可能导致 UDP 事件在**统一事件** 表中显示不完整。
- 为 UDP 流量配置连接开始时的日志记录，以提高可视性。

下一步做什么

要退出实时视图模式，请点击 **实时**。

统一事件中的过滤器

统一事件表显示过去一小时内的防火墙事件。使用以下步骤过滤和缩小视图，以便对网络流量进行更精细的分析。

过滤器可帮助您快速访问关键信息。例如，如果要监控特定用户的应用访问，可以应用搜索条件来隔离相关的防火墙日志。事件查看器仅显示符合您条件的条目。

您可以使用包含和排除条件来有效地优化搜索结果。

过程

步骤 1 选择**事件和日志** > **分析** > **统一事件**。

步骤 2 输入过滤器条件：

- 手动输入过滤条件：
  1. 在搜索字段中输入过滤器条件，或从下拉列表中选择过滤器。
  2. 输入所选过滤条件的值。键入内容时，建议将显示在下拉列表中。
- 要从表格中选择过滤条件，请点击单元格中的点，然后选择一个选项，将该值包含在过滤条件中或从过滤条件中排除。

  提示
  - 使用 **Ctrl+点击** (Windows) 或 **Command-点击** (Mac) 键快速添加包含过滤条件。
  - 使用 **Alt+点击** (Windows) 或 **Option 点击** (Mac) 键快速添加排除过滤条件。
- 请细化您的过滤条件。有关通配符和搜索行为的信息，请参阅事件搜索。
- 在值字段中，在值前面添加运算符（例如 <、>、!）。例如，在 **操作** 字段中输入 **!Allow** 可查找操作不是“允许”的所有事件。

步骤 3 执行搜索。

提示
您可以使用 **Ctrl+Enter** (Windows) 或 **Command-Enter** (Mac) 键盘命令启动搜索。

当显示的列都具有相同的值时，统一事件表中的事件不会聚合。与过滤条件匹配的每个事件都单独列出。

统一事件表根据您的条件显示过滤结果，从而仅显示与您的包含和排除过滤器匹配的事件，以便进行更有针对性的分析。

下一步做什么

要保存自定义过滤器，请参阅 在统一事件中保存搜索，第 8 页 主题。

在统一事件中保存搜索

将自定义搜索保存为收藏夹，以便稍后快速加载，从而高效地进行防火墙事件分析。

请注意，此选项不适用于 “**故障排除**” 表。

过程

步骤 1 选择**事件和日志** > **分析** > **统一事件**。

步骤 2 点击**事件 (Events)** 选项卡。

步骤 3 按照统一事件中的过滤器，第 7 页主题中的说明输入搜索条件。

步骤 4 点击搜索文本框中的 **收藏搜索**（☆） 图标。

步骤 5 执行以下操作之一：

- 要保存新搜索，请指定搜索名称，然后点击 **另存为**。
- 要覆盖已保存的搜索，请在已保存的搜索旁点击**编辑**，然后点击**覆盖**。

下一步做什么

要加载已保存的搜索，请参阅在统一事件中加载搜索，第 8 页。

在统一事件中加载搜索

如果您之前在**统一事件**中保存了搜索条件，则可以快速加载这些条件并关注特定防火墙事件，而无需再次输入条件。

Before you begin

确保您已保存首选搜索条件。有关保存搜索条件的信息，请参阅在统一事件中保存搜索，第 8 页。

过程

步骤 1 选择**事件和日志** > **分析** > **统一事件**。

步骤 2 点击搜索文本框中的 **收藏搜索**（☆） 图标。

步骤 3 点击要加载的已保存搜索。

保存列集

将自定义列集另存为收藏夹以供稍后加载，或在自定义表之间快速切换。

此选项允许您创建个性化表布局，以更有效地查看防火墙事件。请注意，此选项不适用于“**故障排除**”表。

过程

步骤 1 选择**事件和日志** > **分析** > **统一事件**。

步骤 2 点击列选择器图标 ( )，然后选择要保存的列集。

步骤 3 点击 **收藏列集** (☆ 图标。

步骤 4 执行以下操作之一：

- 要保存新列集，请指定列集名称，然后点击 **另存为**。
- 要覆盖收藏夹列集，请在要覆盖的列集上点击 **编辑** ( )，然后点击**覆盖 (Overwrite)**。

系统将保存自定义列集，稍后可以加载该集，以便快速访问您喜欢的表布局。

下一步做什么

要加载已保存的列集，请参阅 加载已保存的列集，第 9 页 主题。

加载已保存的列集

通过加载此前在**统一事件**页面保存的列集，应用偏好表格布局并简化防火墙事件分析。

Before you begin

确保您已经保存过列集。有关保存列集的详细信息，请参阅保存列集，第 9 页。

过程

步骤 1 选择**事件和日志** > **分析** > **统一事件**。

步骤 2 点击列选择器图标 ( )。

步骤 3 点击 **收藏列集** (☆。

步骤 4 点击要加载的列集。

在统一事件中查看来自威胁防御设备的故障排除系统日志

将威胁防御设备配置为将所有故障排除系统日志记录到防火墙管理中心，并将其视为**统一事件**表中的**故障排除事件**。使用此选项可实时查看设备系统日志。您可以在同一张表格中筛选和分析它们以及其他事件类型，以便对 Firewall Threat Defense 设备进行故障排除。

有关详细信息，请参阅在 Cisco Secure Firewall Management Center 查看故障排除系统日志。

Before you begin

确保通过在设备的平台设置中配置**日志记录到 Cisco Secure Firewall Management Center**选项，使托管 Firewall Threat Defense 设备能够将所有日志发送到防火墙管理中心。有关详细信息，请参阅 *Cisco Secure Firewall Management Center* 设备配置指南中的启用日志记录和配置基本设置。

过程

步骤 1 选择**事件和日志** > **分析** > **统一事件**。

步骤 2 点击**故障排除 (Troubleshooting)** 选项卡。

步骤 3 在故障排除事件表中，您可以执行以下操作：

- 查看和分析故障排除事件以及相应的连接事件，以获取更多故障排除信息。
- 点击**上线 (Go Live)** 以实时查看故障排除事件。这有助于将设备日志与最近的设备配置更改相关联。

统一事件列详细信息

统一事件页面上某些字段中的值取决于事件类型。有关默认字段的按事件类型划分的值，请参阅此表。

要查看所有事件字段及其对应关系，请使用列选择器 (▥) 图标。

统一事件字段	连接或安全相关连接事件字段	入侵事件字段	文件事件字段	恶意软件事件字段
时间	首个数据包	时间	时间	时间
活动类型	--	--	--	--
操作	操作	内联结果	操作	操作

统一事件字段	连接或安全相关连接事件字段	入侵事件字段	文件事件字段	恶意软件事件字段
原因	原因	原因	（不适用）	（不适用）
源 IP	发起方 IP	源 IP	发送 IP	发送 IP
目标 IP	响应方 IP	目标 IP	接收 IP	接收 IP
源端口/ICMP 类型	源端口	源端口	发送端口	发送端口
目标地端口/ICMP 代码	目的端口	目的端口	接收端口	接收端口
Web 应用程序	Web 应用程序	Web 应用程序	Web 应用程序	Web 应用程序
规则	访问控制规则	访问控制规则	（不适用）	（不适用）
策略	访问控制策略	入侵策略	文件策略	文件策略
设备	设备	设备	设备	设备

有关事件字段的详细信息，请参阅：

- 连接和 安全相关连接 事件字段
- 入侵事件字段
- 文件和恶意软件事件字段

另请参阅：有关发起方/响应方，源/目标和发件人/接收方字段的说明。

注释 即使在连接开始时未启用日志记录，系统也会将此值作为统一事件表中的**时间**字段使用。要检查连接开始和结束时是否记录了连接事件，请展开事件行以查看详细信息。如果连接的两端均已记录，您会看到**最后一个数据包**字段。

统一事件的历史记录

此表按时间顺序提供统一事件功能更新和改进的历史记录，使您能够在不同防火墙管理中心版本中跟踪功能的可用性和要求。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
查看“统一事件”(Unified Events) 表中的诊断系统日志消息。	7.6.0	任意	现在，您可以在**统一事件 (Unified Events)** 页面中以名为**故障排除事件 (Troubleshoot Events)** 的新事件类型查看设备系统日志。通过统一事件表，您可以实时查看故障排除事件，并将其与同一事件表中的其他事件类型关联起来，从而提供更深入的见解，帮助您排除威胁防御设备配置的故障。 新增/修改的屏幕：**分析 (Analysis)** > **统一事件 (Unified Events)** > **故障排除 (Troubleshooting)**。
在统一事件表中快速应用事件类型过滤器。	7.6.0	任意	引入了事件类型筛选器按钮，可快速将**事件类型 (Event Type)** 筛选器应用于统一事件表。此外，每个按钮都会显示与所选时间段相对应的事件计数。 新增/修改的屏幕：**分析** > **统一事件**。
用于统一事件的数据包跟踪器	7.4.1 7.2.6	任意	现在，您可以从**统一事件 (Unified Events)** 页面打开数据包跟踪器，以对安全事件进行故障排除。 点击要运行数据包跟踪的事件旁边的 **省略号**(⋮) 图标，然后点击**在数据包跟踪器中打开**链接。 版本限制：不支持版本 7.3.x 或 7.4.0。
统一事件改进	7.4	任意	改进了保存收藏列集和搜索功能。
保存常用搜索	7.3	任意	将列集和搜索保存为收藏项，稍后快速启动它们。
统一事件表	7.0	任意	查看和处理具有多种事件类型的单个表：连接（包括安全智能）、入侵、文件和恶意软件。 新增/修改的屏幕：**分析** > **统一事件**下的新页面。 支持的平台： 防火墙管理中心

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。

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。

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。

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。