工作流程

以下主题介绍如何使用工作流程：

概述：工作流程

工作流程是防火墙管理中心网络界面中可供分析师用于评估系统生成的事件的定制系列的数据页面。

防火墙管理中心提供以下类型的工作流程：

预定义工作流程

随系统交付的预设工作流程。您无法编辑或删除预定义工作流程。但是，可以复制预定义工作流程，将其用作自定义工作流程的基础。

已保存的自定义工作流程

基于随 防火墙管理中心交付的已保存自定义表的自定义工作流程。您可以编辑、删除和复制这些工作流程。

自定义工作流程

您为特定需求创建和自定义的工作流程，或者在您创建自定义表时系统自动生成的工作流程。您可以编辑、删除和复制这些工作流程。

工作流程中显示的数据通常取决于您如何许可和部署受管设备以及是否配置提供数据的功能等因素。

预定义工作流程

以下部分介绍的预定义工作流程随系统一同交付。您无法编辑或删除预定义工作流程，但是您可以复制预定义工作流程，并将其用作自定义工作流程的基础。

预定义入侵事件工作流程

下表描述 Firepower 系统随附的预定义入侵事件工作流程。

表 *1:* 预定义入侵事件工作流程

工作流程名称	说明
目标端口	由于目标端口通常绑定到应用，因此该工作流程可以帮助检测警报量异常高的应用。“目标端口”列还可以帮助识别不应存在于网络上的应用。
事件特定	此工作流程提供两个有用的功能。频繁发生的事件可能指示： • 误报 • 蠕虫 • 配置严重错误的网络 偶尔发生的事件很可能指示针对性攻击和特别关注事项。
按照优先级和分类显示事件	此工作流程按事件优先级列出事件及其类型，随之还列出一个表明每个事件已发生的次数的计数。
到目标的事件	此工作流程提供受攻击主机IP地址和攻击性质的高级视图；在适用情况下，还可查看有关攻击中涉及的国家/地区的信息。
IP 特定	此工作流程显示哪些主机IP地址生成最多警报。事件数最多的主机面向公众并接收蠕虫类型流量（指示适合进行调整的位置），或者需要进一步调查以确定警报原因。具有最低计数的主机也有必要进行调查，因为它们可能是针对性攻击的对象。低计数还可指示主机可能不属于该网络。
影响和优先级	通过此工作流程，可以快速查找影响重大的复发事件。报告的影响级别通过事件已发生的次数进行显示。使用此信息，可以识别复发最频繁的重大影响事件，此类事件可能指示网络上的大范围攻击。
影响和源	此工作流程可帮助识别正在进行攻击的源。报告的影响级别通过事件的关联源IP地址进行显示。例如，如果反复出现来自同一源IP地址的1级影响事件，则可能表示攻击者已识别易受攻击的系统并在针对它们进行攻击。
对目标的影响	可以使用此工作流程识别在易受攻击计算机上重复发生的事件，以便解决这些系统上的漏洞并停止进行的任何攻击。

工作流程名称	说明
源端口	此工作流程指示哪些服务器生成的警报最多。可以使用此信息标识需要调整的方面，并确定需要注意的服务器。
源和目标	此工作流程识别共享高级警报的主机 IP 地址。列表顶部的对可能是误报，也可能标识需要调整的方面。可以检查列表底部的对来查找针对性攻击、访问其不应访问的资源的用户或不属于该网络的主机。

预定义恶意软件工作流程

下表介绍了 防火墙管理中心中包含的预定义恶意软件工作流程。所有预定义恶意软件工作流程都使用恶意软件事件表视图。

表 *2:* 预定义恶意软件工作流程

工作流程名称	说明
恶意软件摘要	此工作流提供在网络流量中或由 Cisco Secure Endpoint 连接器检测到的恶意软件列表，按单个威胁分组。
恶意软件事件摘要 (Malware Event Summary)	此工作流程提供不同恶意软件事件类型和子类型的快速细分。
接收恶意软件的主机 (Hosts Receiving Malware)	此工作流程提供已接收恶意软件的主机 IP 地址列表，按恶意软件文件的关联性质分组。
发送恶意软件的主机 (Hosts Sending Malware)	此工作流程提供已发送恶意软件的主机 IP 地址列表，按恶意软件文件的关联性质分组。
引入恶意软件的应用 (Applications Introducing Malware)	此工作流程提供已接收文件的主机 IP 地址列表，按这些文件的关联恶意软件性质分组。

预定义文件工作流程

下表描述防火墙管理中心中包含的预定义文件事件工作流程。所有预定义文件事件工作流程都使用文件事件表视图。

表 *3:* 预定义文件工作流程

工作流程名称	说明
文件摘要	此工作流程提供不同文件事件类别和类型以及任何关联恶意软件性质的快速细分。
接收文件的主机	此工作流程提供已接收文件的主机 IP 地址列表，按这些文件的关联恶意软件性质分组。

工作流程名称	说明
发送文件的主机	此工作流程提供已发送文件的主机 IP 地址列表，按这些文件的关联恶意软件性质分组。

预定义捕获文件工作流程

下表描述 防火墙管理中心中包含的预定义捕获文件工作流程。所有预定义捕获文件工作流程都使用捕获文件表视图。

表 *4:* 预定义捕获文件工作流程

工作流程名称	说明
捕获的文件摘要	此工作流程根据类型、类别和威胁评分提供捕获文件的细分。
动态分析状态	此工作流程根据是否已提交捕获文件进行动态分析来提供此类文件的计数。

预定义连接数据工作流程

下表描述防火墙管理中心中包含的预定义连接数据工作流程。所有预定义连接数据工作流程都使用连接数据表视图。

表 *5:* 预定义连接数据工作流程

工作流程名称	说明
连接事件	此工作流程提供基本连接和检测到的应用信息的摘要视图，然后可以使用该视图向下展开至事件表视图。
按应用分类的连接	此工作流程包含从检测到的连接数来看监控网段上 10 个最活跃应用的图形。
按发起方分类的连接	此工作流程包含从连接数来看监控网段上 10 个最活跃的发起了连接事务的主机 IP 地址的图形。
按端口分类的连接	此工作流程包含从检测到的连接数来看监控网段上 10 个最活跃端口的图形。
按响应方分类的连接	此工作流程包含从连接数来看监控网段上 10 个最活跃的主机 IP 地址（主机 IP 是连接事务中的响应方）的图形。
Connections over Time	此工作流程包含某个时间跨度的监控网段上的连接总数的图形。

工作流程名称	说明
按应用分类的流量	此工作流程包含从传输的字节数来看监控网段上 10 个最活跃应用的图形。 应用计数反映与应用连接匹配的每个检测器。根据应用协议、Web 应用、客户端检测器或内部检测器是否与流量匹配，以及流量是来源于移动设备还是属于加密会话的一部分，同一应用会话可能在列表中出现多次。如果在客户端流中看到了该应用，并且不存在特定客户端检测器，则可以报告通用客户端。 例如，您可能会看到同一 YouTube 流量会话既报告为 **YouTube**（因为它与 YouTube Web 应用检测器匹配），又报告为 **YouTube 客户端**（因为内部 YouTube 检测器与客户端会话中常见的特征相匹配）。 使用连接事件中的信息和网络的网络映射确定特定应用连接的更多上下文。
按发起方分类的流量	此工作流程包含从每个地址传输的总数据量来看监控网段上 10 个最活跃主机 IP 地址的图形。
按端口分类的流量	此工作流程包含从传输的字节数来看监控网段上 10 个最活跃端口的图形。
按响应方分类的流量	此工作流程包含从每个地址接收的总字节数来看监控网段上 10 个最活跃主机 IP 地址的图形。
一段时间内的流量	此工作流程包含某个时间跨度的监控网段上传输的总数据量的图形。
按响应方分类的唯一发起方	此工作流程包含从已联系每个地址的唯一发起方数量来看监控网段上 10 个最活跃响应主机 IP 地址的图形。
按发起方分类的唯一响应方	此工作流程包含从已联系地址的唯一响应方数量来看监控网段上 10 个最活跃发起主机 IP 地址的图形。

预定义安全情报工作流程

下表描述 防火墙管理中心中包含的预定义安全情报工作流程。所有预定义安全情报工作流程均采用安全情报事件表格视图。

表 *6:* 预定义安全情报工作流程

工作流程名称	说明
安全情报事件	此工作流程提供基本安全情报和检测到的应用信息的摘要视图，然后可以使用该视图向下展开至事件表视图。
安全情报摘要 (Security Intelligence Summary)	此工作流程与“安全情报事件”(Security Intelligence Events) 工作流程相同，但是从其中仅按类别和计数列出了安全情报事件的“安全情报摘要”(Security Intelligence Summary) 页面开始。

工作流程名称	说明
具有 DNS 详细信息的安全情报 (Security Intelligence with DNS Details)	此工作流程与“安全情报事件”(Security Intelligence Events) 工作流程相同，但是从其中仅按类别和 DNS 相关特性列出安全情报事件的“具有 DNS 详细信息的安全情报”(Security Intelligence with DNS Details) 页面开始。

预定义主机工作流程

下表描述可与主机数据配合使用的预定义工作流程。

表 *7:* 预定义主机工作流程

工作流程名称	说明
主机数	此工作流程包含主机表视图，后跟主机视图。通过基于“主机”(Hosts) 表的工作流程视图可轻松查看与主机关联的所有 IP 地址上的数据。
操作系统摘要 (Operating System Summary)	可以使用此工作流程分析网络上正在使用中的操作系统。

预定义危害表现工作流程

下表描述可与 IOC（危害表现）数据配合使用的预定义工作流程。

表 *8:* 预定义危害表现工作流程

工作流程名称	说明
主机危害表现	此工作流程以按计数和类别分组的 IOC 数据的摘要视图开头，提供按事件类型进一步细分摘要数据的详细视图。 通过**分析 (Analysis) > 主机 (Hosts)** 菜单访问此工作流程。
按主机划分的危害表现 (Indications of Compromise by Host)	可以使用此工作流程衡量网络上哪些主机最可能受损（基于 IOC 数据）。 通过**分析 (Analysis) > 主机 (Hosts)** 菜单访问此工作流程。
用户危害表现	此工作流程以按计数和类别分组的 IOC 数据的摘要视图开头，提供按事件类型进一步细分摘要数据的详细视图。 通过**分析 (Analysis) > 用户 (Users)** 菜单访问此工作流程。
按用户划分的危害表现	使用此工作流程衡量网络上哪些用户最可能受到潜在危害的影响（基于 IOC 数据）。 通过**分析 (Analysis) > 用户 (Users)** 菜单访问此工作流程。

预定义应用工作流程

下表描述可与应用数据配合使用的预定义工作流程。

表 *9:* 预定义应用工作流程

工作流程名称	说明
应用业务相关性	可以使用此工作流程分析网络上正在运行的各估算业务关联性级别的应用，从而能够监控网络资源的相应使用。
应用类别 (Application Category)	可以使用此工作流程分析网络上正在运行的各类别的应用（如邮件、搜索引擎或社交网络），从而能够监控网络资源的相应使用。
Application Risk	可以使用此工作流程分析网络上正在运行的各估算安全风险级别的应用，从而能够估算用户活动的潜在风险并采取相应措施。
应用摘要 (Application Summary)	可以使用此工作流程获取有关网络上的应用和关联主机的详细信息，从而能够仔细检查主机应用活动。
应用	可以使用此工作流程分析网络上正在运行的应用，从而能够大致了解网络的使用方式。

预定义应用详细信息工作流程

下表描述可与应用详情和客户端数据配合使用的预定义工作流程。

表 *10:* 预定义应用详细信息工作流程

工作流程名称	说明
应用详情	可以使用此工作流程更详细地分析网络上的客户端应用。然后，工作流程提供客户端应用表视图，后跟主机视图。
客户端	此工作流程包含客户端应用表视图，后跟主机视图。

预定义服务器工作流程

下表描述可与服务器数据配合使用的预定义工作流程。

表 *11:* 预定义服务器工作流程

工作流程名称	说明
按计数划分的网络应用 (Network Applications by Count)	可以使用此工作流程分析网络上最频繁使用的应用。

工作流程名称	说明
按命中数划分的网络应用”(Network Applications by Hit)	可以使用此工作流程分析网络上最活跃的应用。
服务器详细信息	可以使用此工作流程详细分析检测到的服务器应用协议的供应商和版本。
服务器	此工作流程包含应用表视图，后跟主机视图。

预定义主机属性工作流程

下表描述可与主机属性数据配合使用的预定义工作流程。

表 *12:* 预定义主机属性工作流程

工作流程名称	说明
属性	可以使用此工作流程监控网络上主机的 IP 地址和主机状态。

预定义发现事件工作流程

下表介绍可用于查看发现和身份数据的预定义工作流程。

表 *13:* 预定义发现事件工作流程

工作流程名称	说明
发现事件 (Discovery Events)	此工作流程以表视图形式提供发现事件的详细列表，后跟主机视图。

预定义用户工作流程

下表介绍可用于查看用户发现和用户身份数据的预定义工作流程。

表 *14:* 预定义用户工作流程

工作流程名称	说明
活动会话	此工作流程提供用户身份源收集的活动会话列表。
用户	此工作流程提供用户身份源收集的用户信息列表。

预定义漏洞工作流程

下表描述防火墙管理中心中包含的预定义漏洞工作流程。

表 *15*: 预定义漏洞工作流程

工作流程名称	说明
漏洞	可以使用此工作流程审查数据库中的漏洞，包括仅含应用于网络上检测到的主机的活动漏洞的表视图。工作流程提供漏洞详情视图，该视图包含符合限制条件的每个漏洞的详细说明。

预定义第三方漏洞工作流程

下表描述防火墙管理中心中包含的预定义第三方漏洞工作流程。

表 *16*: 预定义第三方漏洞工作流程

工作流程名称	说明
按 IP 地址分组的漏洞 (Vulnerabilities by IP Address)	可以使用此工作流程快速了解监控网络上每个主机 IP 地址检测到的第三方漏洞数量。
Vulnerabilities by Source	可以使用此工作流程快速了解每个第三方漏洞源（如 QualysGuard 扫描程序）检测到的第三方漏洞数量。

预定义关联和 允许 列表工作流程

各类型的相关性数据、 allow 名单事件、 allow 名单违例和修复状态事件具有对应的预定义工作流程。

表 *17*: 预定义关联工作流程

工作流程名称	说明
相关事件	此工作流程包含关联事件表视图。
允许 列出事件	此工作流程包含 allow 名单事件表视图。
主机违规计数 (Host Violation Count)	此工作流程提供列出了违反至少一个 allow 名单的所有主机 IP 地址的一系列页面。
允许 名单违规事件	此工作流程包含列出了所有违例的 allow 名单违例表视图，其中最新检测到的违例位于列表顶部。该表中的每一行都包含一个检测到的违规事件。
状态	此工作流程包含修复状态表视图，其中包括所违反策略的名称以及应用的修复的名称和状态。

预定义系统工作流程

Firepower 系统随附一些其他工作流程，包括系统事件（例如审核事件和运行状况事件），以及列出了规则更新导入和活动扫描的结果的工作流程。

表 *18:* 其他预定义工作流程

工作流程名称	说明
审核日志 (Audit Log)	此工作流程包含列出了审核事件的审核日志表视图。
运行状况事件	此工作流程显示运行状况监控策略所触发的事件。
规则更新导入日志 (Rule Update Import Log)	此工作流程包含一个表视图，其中列出了有关成功和失败规则更新导入的信息。
扫描结果 (Scan Results)	此工作流程包含列出了已完成的各项扫描的表视图。

自定义表工作流程

可以使用自定义表功能创建使用来自两种或多种类型事件的数据的表。这一点非常有用，例如可以创建将入侵事件数据与发现数据关联的表和工作流程，从而能够简单地搜索影响关键系统的事件。

创建自定义表时，系统会自动创建可用于查看与表关联的事件的工作流程。工作流程中的功能根据所使用的表类型而异。例如，基于入侵事件表的自定义表工作流程始终以数据包视图结尾。但是，基于发现事件的自定义表工作流程以主机视图结尾。

与基于预定义事件表的工作流程不同，基于自定义表的工作流程没有指向其他类型工作流程的链接。

使用工作流程

过程

步骤 1 选择适当的菜单路径和选项，如工作流程选择，第 12 页表中所述。

步骤 2 在当前工作流程中导航：

- 要查看已选事件数据类型中的所有可用列，请使用表视图页面；请参阅使用表视图页面，第 18 页。
- 要查看已选事件数据类型中的一部分可用列，请使用向下钻取页面；请参阅使用向下钻取页面，第 18 页。
- 要显示工作流程下一页中的相应行，请点击 **向下箭头**（ ）。

- 要在多页工作流程的页面之间移动，请使用每页底部的工具；请参阅工作流程页面遍历工具，第 15 页。
- 要查看不同类型的事件的工作流程中应用的相同限制，请点击**跳转至 (Jump to)** 并从下拉列表中选择事件视图。

步骤 3 修改当前工作流程的显示：

- 选中页面上一行或多行的复选框以指示要影响的行，然后点击该页面底部的按钮之一（例如，**查看**），以对所有选中行执行该操作。
- 选中行顶部的复选框以选择该页面上的所有行，然后点击该页面底部的按钮之一（例如， **查看**），以对页面上的所有行执行该操作。
- 通过在要隐藏的列标题中点击 **关闭** (✕) 来限制显示的列。在显示的弹出窗口中，点击 **应用**。

  提示
  要隐藏或显示其他列，请选中或清除相应的复选框，然后点击**应用 (Apply)**。要将禁用列添加回视图中，请点击展开箭头展开搜索限制条件，然后点击 Disabled Columns 下的列名称。

- 通过所选字段的选定值限制数据视图。有关信息，请参阅事件视图限制，第 32 页和复合事件视图限制，第 33 页。
- 更改事件视图上的时间限制。位于页面右上角的日期范围为工作流程中要包含的事件设置时间范围；有关详细信息，请参阅事件时间限制，第 26 页。

  注释
  如果按时间限制事件视图，则该事件视图中可能会显示在设备的所配置时间窗口（无论是全局还是特定于事件）外部生成的事件。即使为设备配置了滑动时间窗，也可能发生这种情况。

- 要按列对数据进行排序，请点击该列的名称。要反向排序，请再次点击该列的名称。方向指示数据按哪一列排序，以及排序是 **升序** 或 **降序**。
- 点击工作流程页面链接，以使用任何活动限制显示该页面。工作流程页面链接显示在预定义工作流程表视图和向下展开页面左上角，位于事件上方和工作流程名称下方。

步骤 4 查看当前工作流程中的其他数据：

- 要在新窗口中查看文件的轨迹映射，请点击文件名和 SHA-256 散列值列中的网络文件轨迹。该图标因文件状态而异；请参阅文件轨迹图标，第 15 页。
- 要显示与 IP 地址相关的主机配置文件的弹出窗口，请点击任何 IP 地址列中的主机配置文件。该图标因文件状态而异；请参阅主机配置文件图标，第 16 页。
- 要查看与文件相关的最高威胁评分的动态分析摘要报告，请点击任何威胁评分列中的威胁评分。该图标因文件的最高威胁评分而异；请参阅威胁评分图标，第 16 页。
- 要查看用户配置文件信息，点击 **用户** 或者，对于与危害迹象有关的用户，在任何用户身份栏中点击 **红色用户** 。如果某个用户不存在于数据库中（即该用户是 Cisco Secure Endpoint 连接器用户），则该用户图标会呈灰色显示。

- 要查看第三方漏洞的漏洞详细信息，请点击任何第三方漏洞 ID 列中的 **漏洞** 。
- 查看汇聚的数据点时，将指针悬停在标志上方可查看国家/地区名称。
- 查看个别数据点时，可以点击标志以进一步查看地理定位，第 20 页中所述的地理位置详细信息。

步骤 5 导航到不同的工作流程：

要使用不同的工作流程查看同一事件类型，请点击工作流程标题旁边的（**切换工作流程**）**([switch workflow])**，然后选择要使用的工作流程。请注意，**不能**将不同的工作流程用于扫描结果。

按用户角色划分的工作流程访问

对工作流程的访问由用户角色确定。有关详细信息，请参阅下表。

用户角色	可访问的工作流程
管理员	可以访问任何工作流程，并且是仅有的可访问审核日志、扫描结果和规则更新导入日志的用户。
维护用户	可以访问运行状况事件。
“安全分析师”(Security Analyst) 和“安全分析师 [只读]”(Security Analyst [Read Only])	可以访问入侵、恶意软件、文件、连接、发现、漏洞、相关性和运行状况工作流程。

工作流程选择

系统提供下表中所列数据类型的预定义工作流程。

表 *19:* 使用工作流程的功能

功能	菜单路径	选项
连接事件	分析 (Analysis) > 连接 (Connections)	事件
安全智能事件	分析 (Analysis) > 连接 (Connections)	安全智能事件
相关事件	分析 (Analysis) > 关联 (Correlation)	相关事件 允许 列出事件 允许 名单违规事件 状态
恶意软件事件	分析 (Analysis) > 文件 (Files)	恶意软件事件

功能	菜单路径	选项
文件事件	分析 (Analysis) > 文件 (Files)	文件事件
捕获的文件	分析 (Analysis) > 文件 (Files)	捕获的文件
主机事件	分析 (Analysis) > 主机 (Hosts)	网络映射 (Network Map) 主机数 危害表现 应用 应用详细信息 服务器 主机属性 发现事件
入侵事件	分析 (Analysis) > 入侵 (Intrusions)	事件 已审核事件 (Reviewed Events)
用户事件	分析 > 用户	活动会话 用户活动 用户 危害表现
漏洞事件	分析 (Analysis) > 主机 (Hosts)	漏洞 第三方漏洞 (Third-Party Vulnerabilities)
扫描结果	策略 (Policies) > 操作 (Actions) > 扫描程序 (Scanners)	—
运行状况事件	系统> 运行状况 > 事件	—
审核事件	系统 (System) > 监控 (Monitoring)	审核
规则更新导入日志 (Rule Update Import Log)	系统 > 内容更新	规则更新

查看上表中描述的任何种类的数据时，事件显示在该数据的默认工作流程的第一页上。您可通过配置事件视图设置来指定不同的默认工作流程。请注意，工作流程访问取决于用户角色。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

相关主题

配置事件视图设置

工作流程页面

虽然各类型的工作流程中的数据不同，但是所有工作流程都共享公共的功能集。工作流程可以包含若干类型的页面。可以在工作流程页面上执行的操作取决于页面类型。

通过工作流程中的向下钻取页面和表视图页面，您可以快速缩小数据视图的范围，从而能够专注于对分析至关重要的事件。表视图页面和向下钻取页面都支持许多可用于限制要查看的事件集或浏览工作流程的功能。当查看工作流程中的向下钻取页面或表视图中的数据时，可以基于任何可用列对数据进行升序或降序排序。如果数据库包含的事件数超过单个工作流程页面上可显示的事件数，则可点击页面底部的链接以显示更多事件。点击其中一个链接时，时间窗口自动暂停，以便不会重复显示相同事件；当您准备就绪时，可以取消暂停时间窗口。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

表视图

表视图对应于工作流程所基于的数据库中的每个字段包含一列（如果默认情况下启用了该页面）。

为获得最佳性能，请仅显示所需的列。显示的列越多，显示数据所需的资源就越多。

请注意，禁用表视图中的列时，如果禁用该列会创建两个或多个相同的行，则系统将向事件视图中添加“计数”列，如果超过 6 列则显示（排除“计数”列）。

点击表视图页面中的某个值时，即受该值限制。

创建自定义工作流程时，通过点击**添加表视图**向其中添加表视图。

向下钻取页面

通常，向下钻取页面是在移至表视图页面之前用于将调查范围缩小到若干事件的中间页面。向下钻取页面包含数据库中可用的列的子集。

例如，发现事件的向下钻取页面可能仅包含“IP 地址”、“MAC 地址”和“时间”列。另一方面，入侵事件的向下钻取页面可能包含“优先级”、“影响标志”、“内联结果”和“消息”列。

通过向下钻取页面，可以缩小所查看的事件范围并在工作流程中前进。例如，如果点击向下钻取页面中的某个值，即受该值限制并会移至工作流程中的下一页，从而更密切关注与所选值匹配的事件。点击向下钻取页面中的值并不会禁用该值所在的列，即使前进到的页面是表视图也如此。请注意，预定义工作流程的向下钻取页面始终具有 Count 列。创建自定义工作流程时，通过点击 **Add Page** 向其中添加向下钻取页面。

图形

基于连接数据的工作流程可以包含图页面，也称为连接图。

例如，连接图可能会显示列出了随时间推移系统检测到的连接数的曲线图。通常，连接图是类似于向下钻取页面的中间页面，用于缩小调查范围。

最终页面

工作流程的最终页面取决于工作流程所基于的事件的类型。

- 主机视图是基于应用、应用详细信息、发现事件、主机、危害表现 (IOC)、服务器、allow 名单违规事件、主机属性或第三方漏洞的工作流程的最终页面。通过从此页面查看主机配置文件，可以轻松查看与具有多个地址的主机关联的所有 IP 地址上的数据。
- 用户详细信息视图是基于用户、用户活动和用户危害表现的工作流程的最终页面。
- 漏洞详细视图是基于思科漏洞的工作流程的最终页面。
- 数据包视图是基于入侵事件的工作流程的最终页面。

基于其他类型的事件（例如，审核日志事件和恶意软件事件）的工作流程没有最终页面。

在工作流程的最终页面上，可以展开详细信息部分以查看有关该工作流程期间所关注的集合中各对象的特定信息。尽管 Web 界面没有在工作流程的最终页面上列出限制，但是先前设置的限制会保留并应用到数据集。

工作流程页面导航工具

工作流程页面提供视觉提示，以方便在各页面之间导航并选择要在事件分析过程中显示的信息。

工作流程页面遍历工具

如果工作流程包含多个页面的数据，则每个页面的底部会显示工作流程中的页数，以及下表中所列的可用于在页面间导航的工具：

表 *20:* 工作流程页面遍历工具

页面遍历工具	操作
页码 （要查看其他页面，请输入希望查看的页码，然后按 Enter 键。）	查看其他页面
>	查看下一页
<	查看上一页
>|	跳至最后一页
|<	跳至第一页

文件轨迹图标

当工作流程页面提供机会在新窗口中查看文件的轨迹映射时，将会显示网络轨迹图标。此图标根据文件状态而异。

表 *21:* 文件轨迹图标

文件轨迹图标	文件状态
正常	正常
恶意软件	恶意软件
自定义检测	自定义检测
未知	未知
不可用	不可用

主机配置文件图标

当工作流程页面为您提供机会在弹出式窗口中查看与某个 IP 地址关联的主机配置文件时，将会显示主机配置文件图标。如果主机配置文件图标呈灰色显示，则无法查看主机配置文件，因为该主机不能位于网络映射中（例如，0.0.0.0）。根据主机的状态，此图标看起来会有所不同。

表 *22:* 主机配置文件图标

主机配置文件图标	主机状态
	主机未被标记为可能受到危害。
	通过已触发的危害表现 (IOC) 规则，主机被标记为可能受到危害。
	列入阻止列表（仅当根据安全智能数据执行流量过滤时才会显示。）
	列入阻止列表，设置为监控（仅当根据安全智能数据执行流量过滤时才会显示。）

威胁评分图标

在工作流程页面为您提供机会查看与文件的最高威胁评分关联的动态分析摘要报告时，会显示威胁评分图标。该图标因文件的最高威胁评分而异。

表 *23:* 威胁评分图标

威胁评分图标	威胁评分级别
低	低
中等	中
高	高
很高	很高

用户图标

当工作流程页面为您提供机会在弹出窗口中查看与某个用户名关联的用户身份时，会显示用户图标。

表 *24:* 用户图标

用户图标	用户状态
用户	用户未与任何危害表现关联。
红色用户	用户与一个或多个危害表现关联。

工作流程工具栏

工作流程中的每个页面包含用于提供对相关功能的快速访问的工具栏。下表描述工具栏上的每个链接

表 *25:* 工作流程工具栏链接

功能	说明
为此页添加书签	将当前页面加入书签，以便稍后可以返回到该页面。加入书签可捕获所查看的页面上已生效的限制，以便稍后能够返回到同一数据（假设数据仍然存在）。
报告设计器	以当前受限工作流程作为选择条件打开报告设计器。
控制面板	打开与当前工作流程相关的控制面板。例如，连接事件工作流程链接到“连接摘要”控制面板。
查看书签	显示可从中进行选择的已保存书签列表。
搜索	显示可在其中对工作流程中的数据执行高级搜索的搜索页面。也可以点击向下箭头图标以选择并使用已保存的搜索。

相关主题

从事件视图创建报告模板
关于控制面板
事件搜索
书签，第 35 页
创建书签，第 36 页
查看书签，第 36 页

使用向下钻取页面

过程

步骤 1 通过选择适当的菜单路径和选项来访问工作流程，如使用工作流程的功能中所述。

步骤 2 在任何工作流程中，您有以下选择：

- 要向下展开到限制某个特定值的下一个工作流程页面，请点击某一行中的一个值。请注意，此操作仅适用于向下钻取页面。在表视图中点击一行中的一个值仅限于表视图，不能钻取到下一页面。
- 要向下展开到限制某些事件的下一个工作流程页面，请选中要在下一个工作流程页面上查看的事件旁边的复选框，然后点击**查看 (View)**。
- 要向下展开到保留当前限制的下一个工作流程页面，请点击**查看全部 (View All)**。

提示
表视图的页面名称中始终包括“Table View”。

使用表视图页面

表视图页面提供在向下钻取、主机视图、数据包视图或漏洞详细信息页面上不可用的某些功能。按如下所述使用这些功能：

过程

步骤 1 通过选择适当的菜单路径和选项来访问工作流程，如工作流程选择，第 12 页中所述。

步骤 2 从工作流程名称下方显示的工作流程路径中选择表视图。

步骤 3 如果事件数据是远程存储的，您可能会看到一个选项，用于选择显示本地数据还是远程数据。

请参阅在 Cisco Secure Firewall Management Center 和使用存储在 Cisco Secure Network Analytics 设备上的连接事件上工作，第 19 页。

步骤 4 根据需要使用下列功能在表视图中排列和导航：

- 要显示已禁用列的列表，请点击“搜索限制” **展开箭头**（>）。
- 要隐藏已禁用列的列表，请点击“搜索限制” **折叠箭头**（v）。
- 要将已禁用列重新添加到事件视图中，请点击“搜索限制” **展开箭头**（>）以展开搜索限制，然后点击禁用列下的列名。

- 要显示或隐藏（禁用）列，请点击任何列名称旁边的 **清除** ( ) 。在显示的弹出窗口中，选中或清除相应的复选框以指示要显示哪些列，然后点击**应用 (Apply)**。

在 Cisco Secure Firewall Management Center 和使用存储在 Cisco Secure Network Analytics 设备上的连接事件上工作

如果您的设备正在使用 Security Analytics and Logging（本地部署）向 Cisco Secure Network Analytics 设备发送连接事件，您可以在 防火墙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 防火墙管理中心 中的事件交叉启动，以查看 Cisco Secure Network Analytics 设备上的相关数据。

默认情况下，系统会根据您指定的时间范围自动选择适当的数据源。如果要覆盖数据源，请使用此程序。

重要事项 当您更改数据源时，您的选择会在依赖于事件数据源的所有相关分析功能（包括报告）中保持不变，直到您对其进行更改（即使在您注销后）。您的选择不适用于其他 防火墙管理中心 用户。

所选数据源仅用于低优先级连接事件。所有其他事件类型（入侵，文件和恶意软件事件；与这些事件关联的连接事件；以及安全智能事件）都会显示，无论数据源如何。

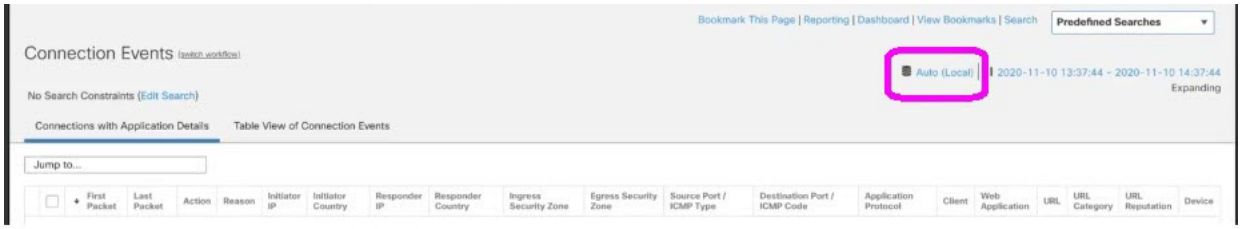
开始之前

您已使用向导向 Security Analytics and Logging（本地部署）发送连接事件。

过程

步骤 1 在 防火墙管理中心 Web 界面中，导航至显示连接事件数据的页面，例如 **分析** > **连接** > **事件**。

步骤 2 点击此处显示的数据源并选择一个选项：



注意
如果选择**本地**，则系统仅显示防火墙管理中心上的可用数据，即使本地数据在所选的整个时间范围内不可用。您不会收到此情况的通知。

步骤 3 （可选）要直接在 Cisco Secure Network Analytics 设备中查看相关数据，请右键点击（在统一事件查看器中，点击）IP 地址或域等值，然后选择交叉启动选项。

地理定位

您可以利用将 IP 地址映射到国家/大陆的地理定位数据库 (GeoDB)，根据国家和大陆查看和过滤流量。请注意，对于检测到在不同国家/地区之间移动的移动设备和其他主机，系统可能会报告大洲而不是具体的国家/地区。我们定期发布 GeoDB 更新。您必须定期更新 GeoDB 以获取准确的地理位置信息；请参阅 更新地理位置数据库 (GeoDB)。

相关主题

网络条件
地理定位
关联策略和规则简介
流量量变曲线条件
更新地理位置数据库 (GeoDB)

连接事件图形

除使用表格向下钻取页面的工作流程和事件的最终表格视图之外，系统可以用在五分钟间隔内汇聚的数据以图形方式展示某些连接数据。请注意，您只可以用图形显示用于汇聚数据的信息：源和目标 IP 地址（以及那些主机的关联用户）、目标端口、传输协议以及应用协议。

提示 您无法将安全情报事件与其关联连接事件分开单独用图形展示。有关安全情报过滤活动的图形概述，请使用控制面板和情景管理器。

有三种不同类型的连接图形：

- 饼形图，显示按各种类别分组的一个数据集中的数据。
- 条形图，显示按各种类别分组的一个或多个数据集中的数据。
- 曲线图，用标准或速度（更改速率）视图图示一个或多个数据集随着时间推移的数据。

注释 系统用曲线图显示流量量变曲线，您可以操作其他任何连接图的方式操作这些图形，但会有一些限制。要查看流量量变曲线，您必须具有管理员访问权限。

与工作流程表一样，您可以向下钻取并限制工作流程图，以重点关注您的分析。

条形图和曲线图可以显示多个数据集；也就是说，它们可以在 y 轴为每个 x 轴数据点显示几个值。例如，您可以显示独立发起方和响应方的总数。饼形图只能显示一个数据集。

通过改变 x 轴、y 轴或者 x 轴和 y 轴，可以在连接图上显示不同的数据和数据集。在饼形图上改变 x 轴可以改变自变量，改变 y 轴可以改变因变量。

相关主题

连接摘要（图形的汇聚数据）

使用连接事件图形

在 防火墙管理中心上，可以查看连接事件图形并根据要查找的信息操纵这些图形。

访问连接图时看到的页面因所用的工作流程而有所不同。可以使用预定义的工作流程，最终会产生连接事件表视图。还可创建自定义工作流程，仅显示匹配特定需求的信息。

在多域部署中，可以查看当前域和任何后代域的数据。不能从更高级别的域或同级域查看数据。

过程

步骤 1 选择**分析** > **连接** > **事件**。

注释
如果显示的是连接事件表而非图形，或者要查看不同图形，请按工作流程标题点击（**切换工作流程**）**([switch workflow])**，然后选择包括图形的预定义工作流程或选择自定义工作流程。请注意，所有预定义连接事件工作流程（包括连接图）最终都会产生连接的表视图。

步骤 2 您有以下选择：

- 时间范围 - 要调整时间范围（如果是空图形会非常有用），请参阅更改时间窗口，第 29 页。
- 字段名称 - 要详细了解可以用图形表示的数据，请参阅连接和 安全相关连接 事件字段。
- 主机配置文件 - 要查看某个 IP 地址的主机配置文件，请在按发起方或响应方显示连接数据的图形上，点击条形图的某一条或饼形图的某一块，然后选择**查看主机配置文件 (View Host Profile)**。
- 用户配置文件 - 要查看用户配置文件信息，请在按发起方用户显示连接数据的图形上，点击条形图的某一条或饼形图的某一块，然后选择**查看用户配置文件 (View User Profile)**。
- 其他信息 - 要了解有关绘图数据的详细信息，请将光标移动至曲线图的某一点上、条形图的某一条上或饼形图的某一块上。
- 限制 - 要按任意 x 轴（自变量）条件限制连接图形而不前进到工作流程中的下一页，请点击曲线图的某一点、条形图的某一条或饼形图的某一块，然后选择**查看依据...** 选项，允许或拒绝 VPN 核心模块和其他可选模块的软件更新。
- 数据选择 - 要更改图形中显示的数据，请点击 **X 轴 (X-Axis)** 或 **Y 轴 (Y-Axis)**，然后选择要用图形表示的新数据。请注意，将 x 轴更改为**时间 (Time)** 或反之，还会更改图形类型；改变 y 轴会影响显示的数据集。
- 数据集 - 要更改图形的数据集，请点击**数据集 (Datasets)**，然后选择新的数据集。

- 分离 - 要分离连接图形以便在不影响默认时间范围的情况下执行进一步分析，请点击**分离 (Detach)**。

  提示
  在分离图中点击**新建窗口 (New Window)** 可创建副本。然后，您可以在每个分离图上进行不同分析。请注意，流量剖面图是分离图形。

- 向下展开 - 要向下展开到工作流程中的下一页，请点击曲线图上的某一点、条形图上的某一条或饼形图上的某一块，然后选择**向下展开 (Drill-down)**。点击曲线图上的某个点可将下一个页面的时间范围更改为以所点击点为中心的10分钟时间区间。点击条形图上的某一条或饼形图上的某一块，可基于该条或该块表示的标准限制下一个页面。
- 导出 - 要将图形的连接数据导出为 CSV（逗号分隔值）文件，请点击**导出数据 (Export Data)**。然后，点击**下载 CSV 文件 (Download CSV File)**，并保存文件。
- 图形类型：曲线图 - 要在标准曲线图与速度（变化率）曲线图之间切换，请点击**速度 (Velocity)**，然后选择**标准 (Standard)** 或**速度 (Velocity)**。
- 图表类型：条形图和饼形图 - 要在条形图与饼形图之间切换，请点击**切换为条形图 (Switch to Bar)** 或**切换为饼形图 (Switch to Pie)**。因为不能在饼形图上显示多个数据集，如果将具有多个数据集的条形图切换到饼形图，该饼形图只显示一个自动选择的数据集。当选择要显示的数据集时，防火墙管理中心会首选显示总统计信息，而不是发起方和响应方的统计信息；在显示发起方统计信息和响应方统计信息时，会首选显示发起方统计数据。
- “在页面之间导航”(Navigate Between Pages) - 要在当前工作流程中的页面之间导航，保留当前限制，请点击工作流程页面左上角相应的页面链接。
- “在事件视图之间导航”(Navigate Between Event Views) - 要导航至其他事件视图以查看关联事件，请点击**跳转至 (Jump to)** 并从下拉列表中选择事件视图。
- “重定中心”(Recenter) - 要围绕某个时间点重定曲线图的中心而不更改时间范围的长度，请点击该点，然后选择**重定中心 (Recenter)**。
- “缩放”(Zoom) - 要围绕某个时间点重定曲线图的中心，同时进行放大或缩小，请点击该点，选择**缩放 (Zoom)**，然后选择新的时间区间。

注释
除非使用分离图，否则限制、重定中心和缩放会改变 防火墙管理中心的默认时间范围。

示例

示例：限制连接图形

思考一个长时间区间连接的图形。如果在按端口图形上应用时间点限制，系统会显示一个条形图，列出基于检测到的连接事件数目、同时受以所点击点为中心的 10 分钟时间区间限制的 10 个最活跃的端口。

如果通过点击条形图中的一条并选择**按发起方 IP 查看 (View by Initiator IP)** 进一步限制该图形，系统将显示一个新的条形图。该条形图不仅受到与之前相同的 10 分钟时间区间的限制，还受到所点击条柱表示的端口的限制。

示例：更改饼形图上的 X 轴和 Y 轴

考虑一个图形化显示各端口数据量的饼形图。在这种情形下，x 轴是**响应方端口 (Responder Port)**，y 轴是 **KBytes**。该饼图表示在一定时间区间内由监控网络发送的总数据量。该饼图的楔块表示在每端口上检测到的数据百分比。

- 如果将该饼图 x 轴变更为**应用协议 (Application Protocol)**，该饼图仍然表示已传输的总数据量，但该饼图的楔块表示为每个已检测到应用协议传输的数据百分比。
- 如果将该图形的 y 轴改为**数据包数 (Packets)**，该饼形图表示在一定时间区间内监控网络传输的数据包总数，而形饼图的楔块表示每个端口上检测到的数据包在数据包总数中所占的百分比。

相关主题

使用工作流程 ，第 10 页
配置事件视图设置

连接图形数据选项

通过改变 x 轴、y 轴或者 x 轴和 y 轴，可以在连接图上显示不同的数据。在饼形图上改变 x 轴可以改变自变量，改变 y 轴可以改变因变量。

表 *26: X* 轴选项

X 轴选项	图表类型	绘制此数据的方式
应用协议	条形图或饼形图	通过 10 个最活跃的应用协议
设备	条形图或饼形图	通过 10 个最活跃的受管设备
发起方 IP	条形图或饼形图	通过 10 个最活跃的发起方主机 IP 地址
发起方用户	条形图或饼形图	通过 10 个最活跃的发起方用户
响应方 IP	条形图或饼形图	通过 10 个最活跃的响应方主机 IP 地址
响应方端口 (Responder Port)	条形图或饼形图	通过 10 个最活跃的响应方端口

X 轴选项	图表类型	绘制此数据的方式
源设备	条形图或饼形图	通过 10 个最活跃的 NetFlow 数据导出器，以及 Cisco Secure Firewall 系统托管设备检测到的所有连接的名为 `Firepower` 的源设备。
时间	折线图	在一段时间内 在**时间 (Time)** 中更改 y 轴的结束和起始时间也会更改图形类型，并可能更改数据集。

表 *27: Y* 轴选项

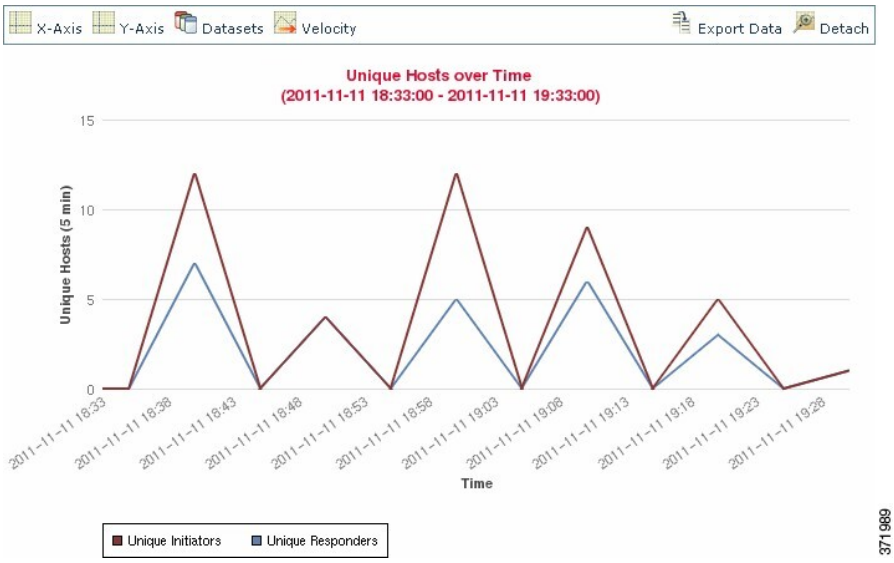
Y 轴选项	使用 X 轴标准绘制此数据
字节	传输的字节数
连接	连接数量
KBytes	传输的千字节数
KBytes Per Second	每秒的千字节数
数据包	传输的数据包数量
独立主机	检测到的独立主机数量
独立应用协议	独立应用协议数量
唯一用户	独立用户数量

具有多个数据集的连接图形

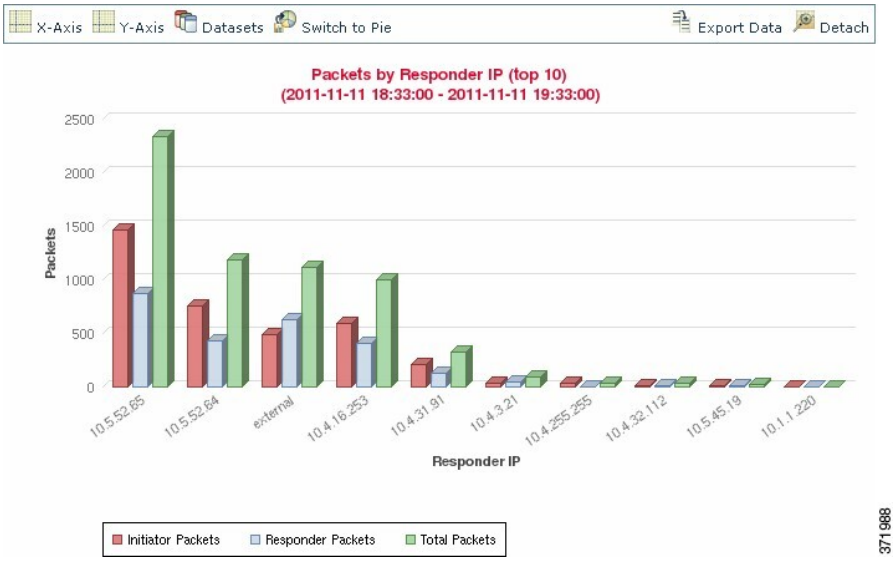
条形图和曲线图可以显示多个数据集；也就是说，它们可以在 y 轴为每个 x 轴数据点显示几个值。例如，您可以显示独立发起方和响应方的总数。

注释 饼形图上**不能**显示多个数据集。如果将具有多个数据集的条形图切换到饼形图，该饼形图只显示一个自动选择的数据集。当选择要显示的数据集时，防火墙管理中心会首选显示总统计信息，而不是发起方和响应方的统计信息；在显示发起方统计信息和响应方统计信息时，会首选显示发起方统计数据。

在曲线图上，多个数据集显示为多条线，每条线颜色不同。例如，下面的图形显示了在一个小时的时间区间内监控网络上检测到的独立发起方总数和独立响应方总数。



在条形图上，与 x 轴的各个数据点对应的多个数据集显示为一组彩色条形柱。例如，下面的条形图显示监控网络上传输的数据包总数、发起方传输的数据包总数以及响应方传输的数据包总数。



连接图形数据集选项

下表介绍了在连接图 x 轴上可以显示的数据集。

表 *28:* 数据集选项

如果 **y** 轴显示...	可以选为数据集的对象为...
连接	仅默认数量，即在受监控网络上检测到的连接数（**连接数 [Connections]**）这是流量配置文件图的唯一选项。

如果 y 轴显示...	可以选为数据集的对象为...
千字节数 (KBytes)	组合： • 监控网络上传输的总数据量（**总千字节数 [Total KBytes]**） • 监控网络上的主机 IP 地址传输的数据量（**发起方千字节数 [Initiator KBytes]**） • 监控网络上的主机IP地址收到的数据量（**响应方千字节数 [Responder KBytes]**）
每秒千字节数 (KBytes Per Second)	仅默认数量，指在监控网络上每秒传输的总数据量（**每秒总千字节数 [Total KBytes Per Second]**）
数据包	组合： • 在监控网络上传输的数据包总数（**数据包总数 [Total Packets]**） • 在监控网络上从主机 IP 地址传输的数据包总数（**发起方数据包数 [Initiator Packets]**） • 在监控网络上主机 IP 地址收到的数据包总数（**响应方数据包数 [Responder Packets]**）
独立主机数 (Unique Hosts)	组合： • 在监控网络上独立会话发起方的数量（**独立发起方数 [Unique Initiators]**） • 在监控网络上独立会话响应方的数量（**独立响应方数 [Unique Responders]**）
独立应用协议数 (Unique Application Protocols)	仅默认数量，指监控网络上的独立应用协议的数量（**独立应用协议数 [Unique Application Protocols]**）
唯一用户	仅默认数量，指登录到监控网络上会话发起方的独立用户的数量（**独立发起方用户数 [Unique Initiator Users]**）

事件时间限制

每个事件具有指示事件发生时间的时间戳。可以通过设置时间窗口（有时称为时间范围）限制某些工作流程中显示的信息。

基于可按时间限制的事件的工作流程在页面顶部具有一条时间范围线。

默认情况下，工作流程使用设置为前一小时的扩展式时间窗口。例如，如果您在上午 11:30 登录，将会看到发生在上午 10:30 和上午 11:30 之间的事件。随着时间的推进，时间窗口进行扩展。在中午 12:30，您将会看到发生在上午 10:30 和中午 12:30 之间的事件。

可以通过在事件视图设置中设置自己的默认时间窗口来更改此行为：该时间窗口管理三个属性：

- 时间窗口类型（静态、扩展式或滑动式）
- 时间窗口长度
- 时间窗口数量（多个时间窗口或单个全局时间窗口）

无论默认时间窗口设置如何，都可以在事件分析期间手动更改时间窗口，方法是点击页面顶部的时间范围，该页面会显示“日期/时间”(Date/Time) 弹出窗口。根据配置的时间窗口数量和使用的设备类型，还可以使用“日期/时间”(Date/Time) 窗口更改所查看的事件类型的默认时间窗口。

最后，您可以在查看滑动式或扩展式工作流程时暂停时间窗口。请参阅暂停时间窗口以暂时冻结数据集，第 29 页。

相关主题

配置事件视图设置
使用连接和 安全相关连接 事件表

事件的每次会话时间窗口自定义

无论默认时间窗口设置如何，都可以在事件分析期间手动更改时间窗口。

注释 手动时间窗口设置仅对当前会话有效。在注销然后重新登录时，时间窗口会重置为默认值。

根据配置的时间窗口数量，更改一个工作流程的时间窗口可能会影响设备上的其他工作流程。例如，如果具有单个全局时间窗口，则更改一个工作流程的时间窗口会更改设备上所有其他工作流程的时间窗口。另一方面，如果使用的是多个时间窗口，则更改审核日志或运行状况事件工作流程时间窗口对于任何其他时间窗口没有影响，而更改其他种类的事件的时间窗口则会影响可按时间限制的所有事件（审核事件和运行状况事件除外）。

请注意，由于并非所有工作流程都可按时间限制，因此时间窗口设置对基于主机、主机属性、应用、应用详情、漏洞、用户或 allow 名单违例的工作流程没有影响。

使用“日期/时间”窗口上的“时间窗口”选项卡可手动配置时间窗口。根据在默认时间窗口设置中配置的时间窗口数量，选项卡的标题为以下之一：

- **事件时间窗口** - 如果配置了多个时间窗口，并且是为除审核日志和运行状况事件工作流程以外的工作流程设置的时间窗口
- **运行状况监控时间窗口** - 如果配置了多个时间窗口，并且是为运行状况事件工作流程设置的时间窗口
- **审核日志时间窗口** - 如果配置了多个时间窗口，并且是为审核日志设置的时间窗口
- **全局时间窗口** - 如果配置了单个时间窗口

配置时间窗口时必须首先决定要使用的时间窗口的类型。

- 静态时间窗口显示从特定开始时间到特定结束时间生成的所有事件。

- 扩展式时间窗口显示从特定开始时间到目前生成的所有事件；随着时间的推进，时间窗口会进行扩展，并会有新事件添加到事件视图中。
- 滑动式时间窗口显示从特定开始时间（例如，一周前）到目前生成的所有事件；刷新页面时，时间窗口会“滑动”，以便仅显示您配置的时间范围（在此示例中是上周）内的事件。要在检查数据集时暂时阻止更新数据集，请参阅暂停时间窗口以暂时冻结数据集，第 29 页。

根据选择的类型，“日期/时间”窗口会更改以提供不同的配置选项。

注释 Firepower 系统根据在时区首选项中指定的时间使用 24 小时制时钟。

时间窗口设置

下表说明可在 Time Window 选项卡上配置的各种设置。

表 *29:* 时间窗口设置

设置	时间段类型	说明
时间段类型下拉列表	n/a	选择要使用的时间段类型：静态、扩展式或滑动式。 请注意，如果按时间限制事件视图，则在设备配置的时间窗口外生成的事件（无论是全局还是特定事件）可能显示在事件视图中。即使为设备配置了滑动时间窗口，也可能发生这种情况。
“开始时间”(Start Time) 日历	静态和扩展式	指定时间段的开始日期和时间。所有时间段的最大时间范围都是从 1970 年 1 年 1 日午夜 (UTC) 到 2038 年 1 月 19 日凌晨 3:14:07 (UTC)。 可以使用“预设”(Presets) 选项而不是使用日历，如下所述。
“结束时间”(End Time) 日历	静态	指定时间段的结束日期和时间。所有时间段的最大时间范围都是从 1970 年 1 年 1 日午夜 (UTC) 到 2038 年 1 月 19 日凌晨 3:14:07 (UTC)。 请注意，如果使用的是扩展式时间段，则“结束时间”(End Time) 日历会灰显并指定结束时间为“现在”(Now)。 可以使用“预设”(Presets) 选项而不是使用日历，如下所述。
显示“最后”(Last) 字段和下拉列表	滑动式	配置滑动式时间段的长度。
预设：最后 (Presets: Last)	all	根据设备的本地时间，点击列表中的其中一个时间范围以更改时间段。例如，点击 **1 周 (1 week)** 会将时间段更改为反映上周。点击预设会将日历更改为反映选择的预设。

设置	时间段类型	说明
预设：当前 (Presets: Current)	静态和扩展式	根据设备的本地时间和日期，点击列表中的其中一个时间范围以更改时间段。点击预设会将日历更改为反映选择的预设。 请注意： • 当日在午夜开始 • 当周在星期天午夜开始 • 当月在月份第一日午夜开始
预设：同步 (Presets: Synchronize with)	所有（如果使用的是全局时间段则不适用）	点击其中一项： • **事件时间段 (Events Time Window)** 将当前时间段与事件时间段同步 • **运行状况监控时间段 (Health Monitoring Time Window)** 将当前时间段与运行状况监控时间段同步 • **审核日志时间段 (Audit Log Time Window)** 将当前时间段与审核日志时间段同步

更改时间窗口

过程

步骤 1 在按时间限制的工作流程中，点击 **时间范围**（ ） 以转至“日期/时间”(Date/Time) 窗口。

步骤 2 在**事件时间窗口 (Events Time Window)** 上，设置时间窗口，如时间窗口设置，第 28 页中所述。

提示
点击**重置 (Reset)** 以将时间窗口重新更改为默认设置。

步骤 3 点击**应用 (Apply)**。

暂停时间窗口以暂时冻结数据集

如果您正在使用滑动式或扩展式时间窗口，您可以暂停时间窗口来检查工作流程提供的数据快照。这样会有所帮助，因为未暂停的工作流程在更新时，可能会移除要检查的事件，或者添加无关的事件。

当您点击页面底部的链接以显示另一事件页面时，时间窗口会自动暂停；您可以在准备好时取消暂停时间窗口。

完成分析后，可以取消暂停时间窗口。取消暂停时间窗口将根据您的喜好对其进行更新，并且还更新事件视图以反映已取消暂停的时间窗口。

暂停事件时间窗口对控制面板没有影响，而暂停控制面板对暂停事件时间窗口也没有任何影响。

过程

在受时间限制的工作流程上，选择所需的时间范围控件：

- 要暂停时间窗口，请点击时间范围控件 **暂停** ( )。
- 要取消暂停时间窗口，请点击时间范围控件 **播放** ( )。

事件的默认时间窗口

在事件分析期间，可以使用“日期/时间”窗口上的“首选项”选项卡更改所查看的事件类型的默认时间窗口，而不必使用事件视图设置。

请记住，以此方式更改默认时间窗口仅会更改所查看的事件类型的默认时间窗口。例如，如果配置了多个时间窗口，则更改“首选项”(Preferences) 选项卡上的默认时间窗口会更改事件、运行状况监控或审核日志窗口的设置，换句话说，以第一个选项卡指示的时间窗口为准。如果配置了单个时间窗口，则更改“首选项”(Preferences) 选项卡上的默认时间窗口会更改所有事件类型的默认时间窗口。

相关主题

默认时间窗口

事件类型的默认时间窗口选项

下表说明可在 Preferences 选项卡上配置的各种设置。

表 *30:* 时间窗口首选项

偏好	说明
刷新间隔	设置事件视图的刷新间隔（以分钟为单位）。输入零会禁用刷新选项。
时间窗口数	指定要使用的时间窗口数量： • 选择**多个 (Multiple)** 以根据可按时间限制的事件为审核日志、运行状况事件和工作流程配置单独的默认时间窗口。 • 选择**单个 (Single)** 以使用适用于所有事件的全局时间窗口。
默认时间窗口：显示最后时间 - 滑动式	此设置允许配置指定长度的滑动式默认时间窗口。 设备显示在某个特定开始时间（例如，1 小时前）和当前时间期间生成的所有事件。更改事件视图时，时间窗口会“滑动”，以便始终显示最后一小时的事件。

偏好	说明
默认时间窗口：显示最后时间 - 静态/扩展式	此设置允许配置指定长度的静态或扩展式默认时间窗口。 对于**静态**时间窗口（启用**使用结束时间 [Use End Time]** 复选框），设备显示从特定开始时间（例如，1 小时前）到首次查看事件时生成的所有事件。更改事件视图时，时间窗口保持固定，以便仅显示静态时间窗口期间发生的事件。 对于**扩展式**时间窗口（禁用**使用结束时间 [Use End Time]** 复选框），设备显示从特定开始时间（例如，1 小时前）到目前生成的所有事件。更改事件视图时，时间窗口会扩展到当前时间。
默认时间窗口：当日 - 静态/扩展式	此设置允许配置当日的静态或扩展式默认时间窗口。当日从午夜开始，基于当前会话的时区设置。 对于**静态**时间窗口（启用**使用结束时间 [Use End Time]** 复选框），设备显示从午夜到首次查看事件时生成的所有事件。更改事件视图时，时间窗口保持固定，以便仅显示静态时间窗口期间发生的事件。 对于**扩展式**时间窗口（禁用**使用结束时间 [Use End Time]** 复选框），设备显示从午夜到目前生成的所有事件。更改事件视图时，时间窗口会扩展到当前时间。请注意，如果在您注销之前，分析持续 24 小时以上，则此时间窗口可以超过 24 小时。
默认时间窗口：当周 - 静态/扩展式	此设置允许配置当周的静态或扩展式默认时间窗口。当周从上一周日的午夜开始，基于当前会话的时区设置。 对于**静态**时间窗口（启用**使用结束时间 [Use End Time]** 复选框），设备显示从午夜到首次查看事件时生成的所有事件。更改事件视图时，时间窗口保持固定，以便仅显示静态时间窗口期间发生的事件。 对于**扩展式**时间窗口（禁用**使用结束时间 [Use End Time]** 复选框），设备显示从星期天午夜到目前生成的所有事件。更改事件视图时，时间窗口会扩展到当前时间。请注意，如果在您注销之前，分析持续 1 周以上，则此时间窗口可以超过 1 周。

更改事件类型的默认时间窗口

过程

步骤 1 在按时间限制的工作流程中，点击 **时间范围**（ ） 以转至“日期/时间”窗口。

步骤 2 点击 **首选项** 选项卡并更改您的首选项，如 事件类型的默认时间窗口选项，第 30 页表中所述。

步骤 3 点击**保存首选项**。

步骤 4 此时您有两种选择：

- 要将新的默认时间窗口设置应用于所使用的事件视图，请点击**应用**以关闭“日期/时间”窗口并刷新事件视图。

- 要继续分析而不应用默认时间窗口设置，请关闭“日期/时间”窗口而不点击**应用**。

事件视图限制

工作流程页面上显示的信息由实施的限制来确定。例如，最初打开事件工作流程时，信息限制为前一小时生成的事件。

要前进到工作流程中的下一页并通过特定值限制所查看的数据，请选择页面上具有这些值的行，然后点击**查看 (View)**。要前进到工作流程中的下一页并保留当前限制和传递所有事件，请选择**查看全部 (View All)**。

注释 如果选择含有多个非计数值的行并点击**查看 (View)**，则会创建复合限制。

限制工作流程中的数据有第三种方法。要将页面限制为含有选定值的行，并且还将选定值添加到页面顶部的限制列表中，请点击页面上某一行中的值。例如，如果查看的是已记录连接的列表，并要使用访问控制将该列表仅限于允许的连接，请点击**操作 (Action)** 列中的**允许 (Allow)**。又例如，如果查看的是入侵事件，并要将列表仅限于目标端口为 80 的事件，请点击**目标端口/ICMP 代码 (Destination Port/ICMP Code)** 列中的 **80 (http)/tcp**。

提示 根据监控规则条件来限制连接事件的程序略有不同，可能需要采取一些额外步骤。此外，不能按关联文件或入侵信息来限制连接事件。

还可以使用搜索来限制工作流程中的信息。要根据一列中的多个值进行限制时，请使用此功能。例如，如果要查看与两个 IP 地址相关的事件，请点击**编辑搜索 (Edit Search)**，然后修改“搜索”(Search) 页面上相应的 IP 地址字段以将两个地址均包含在内，然后点击**搜索 (Search)**。

在搜索页面上输入的搜索条件会列为页面顶部的限制，并且产生的事件相应地受限制。在 防火墙管理中心中，除非当前限制是复合限制，否则导航到其他工作流程时也会应用这些限制。

在搜索时，必须特别注意搜索限制是否适用于所搜索的表。例如，客户端数据在连接摘要中不可用。如果根据连接中检测到的客户端搜索连接事件，然后在连接摘要事件视图中查看结果，则 防火墙管理中心会显示连接数据，如同其完全未受限制一样。无效限制会标示为不适用 (N/A)，并带有删除线标记。

限制事件

过程

步骤 1 通过选择适当的菜单路径和选项来访问工作流程，如工作流程选择，第 12 页中所述。

步骤 2 在任何工作流程中，您有以下选择：

- 要将视图限于与单个值相匹配的事件，请点击页面上行中的所需值。
- 要将视图限于与多个值相匹配的事件，请选中具有这些值的事件的对应复选框，然后点击**视图 (View)**。

  注释
  如果行包含多个非计数值，则会添加复合限制。

- 要删除限制，请点击“搜索限制” **展开箭头**（>），然后点击展开的“搜索限制”(Search Constraints) 列表中的限制名称。
- 要使用“搜索”(Search) 页面编辑限制，请点击**编辑搜索 (Edit Search)**。
- 要将限制另存为已保存的搜索，请点击**保存搜索 (Save Search)** 并指定查询名称。

  注释
  不能保存包含复合限制的查询。

- 要对其他事件视图使用相同限制，请点击**跳至 (Jump to)** 并选择事件视图。

  注释
  当切换到其他工作流程时，不会保留复合限制。

- 要切换限制的显示，请点击“搜索限制”**展开箭头**（>）或“搜索限制” **折叠箭头**（v）。这在限制列表较大并占据大部分屏幕时有用。

复合事件视图限制

复合限制基于特定事件的所有非计数值。选择含有多个非计数值的行时，需要设置复合限制，该限制仅检索与该页面上的该行中所有非计数值都匹配的事件。例如，如果选择源 IP 地址为 `10.10.31.17` 且目标 IP 地址为 `10.10.31.15` 的行以及源 IP 地址为 `172.10.10.17` 且目标 IP 地址为 `172.10.10.15` 的行，则会检索下列所有内容：

- 源 IP 地址为 10.10.31.17 且目标 IP 地址为 10.10.31.15 的事件

  或

- 源 IP 地址为 172.10.31.17 且目标 IP 地址为 172.10.31.15 的事件

将复合限制与简单限制组合时，简单限制分布在各复合限制集合中。例如，如果在以上所列的复合限制中为协议值 `tcp` 添加了一条简单限制，则会检索下列所有内容：

- 源 IP 地址为 10.10.31.17 且目标 IP 地址为 10.10.31.15 且协议为 tcp 的事件

  或

- 源 IP 地址为 172.10.31.17 且目标 IP 地址为 172.10.31.15 且协议为 tcp 的事件

不能对复合限制执行搜索或保存搜索操作。您也不能在使用事件视图链接或点击（**切换工作流程**）以切换到其他工作流程时保留复合限制。如果将应用了复合限制的事件视图加入书签，则不使用书签保存限制。

使用复合事件视图限制

过程

步骤 1 通过选择适当的菜单路径和选项来访问工作流程，如工作流程选择，第 12 页中所述。

步骤 2 要管理复合限制，您有以下选择：

- 要创建复合限制，请选择一个或多个具有多个非计数值的行，然后点击**查看 (View)**。
- 要清除复合限制，请点击“搜索限制” **展开箭头**（>） 并点击 **复合限制**。

工作流程间导航

您可以使用工作流程页面上的**跳至...(Jump to...)** 下拉列表中的链接导航到其他工作流程。选择下拉列表以查看并选择其他工作流程。

选择新工作流程时，所选行共享的属性和所设置的限制用于新工作流程中（如果其适用）。如果配置的限制或事件属性没有映射到新工作流程中的字段，则表明其已丢弃。此外，从一个工作流程切换到另一个工作流程时未保留复合限制。而且，捕获的文件工作流程中的限制仅传输到文件和恶意软件事件工作流程。

注释 查看某个时间范围的事件计数时，事件的总数可能无法反映为其提供了更详细数据的事件的数量。因为系统有时会删掉较旧的事件详细信息以管理磁盘空间使用情况，所以会发生这种情况。要将事件详细信息删除的情况降到最少，您可以微调事件日志记录，以只记录对部署最重要的事件。

请注意，除非已暂停时间段或已配置静态时间段，否则在更改工作流程时时间段会更改。

此功能可增强您调查可疑活动的能力。例如，如果查看的是连接数据并发现内部主机在向外部站点传送异常大量的数据，则可以选择响应方 IP 地址和端口作为限制，然后跳至**应用 (Applications)** 工作流程。应用工作流程将使用响应方 IP 地址和端口作为 IP 地址和端口限制，并显示有关应用的其他信息，如应用的种类。也可以点击页面顶部的**主机 (Hosts)** 以查看远程主机的主机配置文件。

在找到有关应用的详细信息后，可以选择**关联事件**以返回到连接数据工作流程，从限制中删除响应方 IP，向限制中添加发起方 IP，然后选择**应用详细信息**以了解发起主机上的用户在将数据传输到远程主机时使用了哪个客户端。请注意，端口限制未转移到“应用详细信息”(Application Details) 页面。保持本地主机作为限制时，也可以使用其他导航按钮查找其他信息。

- 要发现本地主机是否已违反任何策略，请保持 IP 地址作为限制并从**跳至 (Jump to)** 下拉列表中选择**关联事件 (Correlation Events)**。

- 要了解是否对主机触发了指示危害的入侵规则，请从**跳至 (Jump to)** 下拉列表中选择**入侵事件 (Intrusion Events)**。
- 要查看本地主机的主机配置文件并确定主机是否易受可能已被利用的任何漏洞的攻击，请从**跳至 (Jump to)** 下拉列表中选择**主机 (Hosts)**。

使用统一事件查看器操作

统一事件为您提供多种类型（连接、入侵、文件、恶意软件和一些安全相关的连接事件）的单一屏幕视图。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。通过“统一事件”表中的**实时视图**选项，您可以实时查看防火墙事件并监控网络上的活动。

使用统一事件查看器执行以下操作：

- 查找不同类型事件之间的关系
- 实时查看策略更改的影响

过程

步骤 1 选择**分析** > **统一事件**。

步骤 2 选择时间范围（固定或滑动）以查看特定时间段的防火墙事件。默认情况下，统一事件查看器表显示前一小时的事件。您可以过滤该表以获取更精细的安全事件上下文，自定义表列，或启用实时视图并实时查看事件更新。

有关统一事件的详细信息，请参阅 统一事件。

书签

如果要在事件分析中快速返回到特定位置和时间，请创建书签。书签保留以下有关信息：

- 使用的工作流程
- 查看的工作流程部分
- 工作流程中的页码
- 任何搜索限制
- 任何已禁用列
- 使用的时间范围

创建的书签可供具有书签访问权限的所有用户帐户使用。这意味着，如果发现需要深入分析的事件集，则可以轻松创建书签并将调查移交给具有相应特权的其他用户。

注释 如果删除书签中显示的事件（直接由用户删除或通过自动数据库清除），则书签不再显示原始事件集。

创建书签

在多域部署中，只能查看在当前域中创建的书签。

过程

步骤 1 在事件分析期间，显示了有关事件的情况下，点击 **Bookmark This Page**。

步骤 2 在**书签名称 (Bookmark Name)** 字段中，输入名称。

步骤 3 点击**保存书签**。

查看书签

在多域部署中，只能查看在当前域中创建的书签。

过程

从任何事件视图中，您有两个选项：

- 将指针悬停在**查看书签 (View Bookmarks)** 上方，然后点击下拉菜单中的所需书签。
- 点击 **查看书签**，然后在“查看书签”页面上，点击所需的书签名称或其旁边的 **视图** ( ) 。

  注释
  如果删除书签中最初显示的事件（直接由用户删除或通过自动数据库清除），则书签不再显示原始事件集。

工作流程的历史记录

*表 **31**:*

功能	防火墙管理中心最低版本	最低版本	详细信息
已弃用：入侵事件和事件剪贴板。	7.1	任意	入侵事件和事件剪贴板已弃用。 弃用的屏幕： • **分析** > **入侵** > **剪贴板** • **分析** > **入侵** > **事故**
统一事件查看器。	7.0	任意	在单个表中查看和处理多种事件类型：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**
处理远程存储的事件。	7.0	任意	您可以使用 FMC 处理存储在 Cisco Secure Network Analytics 设备上的连接事件。系统会自动使用最合适的数据源，您也可以明确选择数据源。仅当您已完成 Security Analytics and Logging（本地部署） 向导时，才会显示此选项。 新增/修改的屏幕：显示连接事件的页面，例如事件查看器、控制面板、上下文资源管理器和报告。
在某些情况下提高了工作流程表的加载速度。	6.6	任意	工作流程页面上的表现在仅在不超过六列时显示相同行的计数列。这可以最大限度地减少所需的计算量，从而提高表加载速度。 新增/修改的屏幕：事件查看器。

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。