连接和安全相关的连接事件

以下主题介绍如何使用连接事件和安全事件表。

关于连接事件

系统可以生成其受管设备检测到的连接的日志。这些日志称为连接事件。连接事件包括 安全相关连接事件 （被基于信誉的安全情报功能被阻止的连接。）

连接事件通常包括由以下项检测到的事务：

- 访问控制策略
- 解密策略
- 预过滤器策略（由预过滤器或隧道规则捕获）
- DNS 阻止列表
- URL 阻止列表
- 网络（IP 地址）阻止列表

规则和策略中的设置可供您精细控制记录的连接、记录连接的时间以及存储数据的位置。

有关详细信息，请参阅连接日志记录。

相关主题

关于安全智能

连接与安全相关连接事件

安全相关连接事件 是一个当会话被阻止或被基于信誉的安全情报功能监控时生成的连接事件。

但是，对于每个 安全相关连接事件，都有相同的连接事件。您可以单独查看和分析 安全相关连接事件 。系统还会单独地存储和删除 安全相关连接事件 。

请注意，在进行更多资源密集型评估之前，系统会强制实施安全智能。当连接被安全智能阻止时，生成的事件不包含系统从后续评估（例如用户身份）收集的信息。

注释 在本指南中，除非另行说明，否则有关连接事件的也与 安全相关连接事件有关。

NetFlow 连接

要补充受管设备收集到的连接数据，可以使用 NetFlow 导出器广播的记录来生成连接事件。这在 NetFlow 导出器监控的网络不同于受管设备监控的网络时尤为有用。

系统会将 NetFlow 记录记录为 Cisco Secure Firewall Management Center数据库中的单向连接结束事件。这些连接的可用信息与访问控制策略检测到的连接略有不同；请参阅NetFlow 和受管设备数据之间的差异。

相关主题

NetFlow 数据

连接摘要（图形的汇聚数据）

系统会将在五分钟间隔内收集到的数据汇聚为连接摘要，供系统用于生成连接图形和流量量变曲线。或者，您可以基于连接摘要数据创建自定义工作流程，并以与基于单个连接事件的工作流程相同的方式来使用此类工作流程。

请注意，尽管相应的连接结束事件可以汇总到连接摘要数据中，但 安全相关连接事件无任何特定的连接摘要。

多个连接必须满足以下条件才能汇总到连接摘要：

- 代表连接结束
- 具有相同的源 IP 地址和目标 IP 地址，并在响应方（目标）主机上使用相同的端口
- 使用相同的协议（TCP 或 UDP）
- 使用相同的应用协议
- 由同一受管设备或由同一 NetFlow 导出器检测

每份连接摘要都包括总流量统计信息，以及摘要中连接的数量。由于NetFlow导出器生成单向连接，因此对于基于 NetFlow 数据的每个连接而言，摘要的连接计数按 2 递增。

请注意，连接摘要中并未包含与摘要中汇总的连接相关联的所有信息。例如，在汇总连接以形成连接摘要时没有使用客户端信息，因此摘要中不包含客户端信息。

长期运行连接

如果汇总连接数据的受控会话跨越两个或多个 5 分钟时间间隔，那么该连接可视为长期运行连接。当计算连接摘要中的连接数时，系统仅累加启动长期运行连接的 5 分钟间隔内的连接数。

此外，当计算由长期运行连接中的发起方和响应方传输的数据包和字节数时，系统并不会报告每 5 分钟间隔中实际传输的数据包和字节数。相反，系统会假定一个固定传输比率，并基于传输的数据包和字节总数、连接长度及每 5 分钟间隔内发生的连接部分计算预估数字。

源于外部响应方的组合连接摘要

要减少存储连接数据所需的空间并加快连接图的绘制，系统将在下列情况下合并连接摘要：

- 连接中涉及的其中一台主机并不在监控网络中
- 除外部主机的 IP 地址以外，摘要中的连接还满足摘要汇聚条件

当在“分析”>“连接”子菜单页面中查看连接摘要并使用连接图时，系统将显示`external`，而非未监控主机的 IP 地址。

由于执行汇总的缘故，如果您尝试从涉及外部响应方的连接摘要或连接图深入了解连接数据的表视图（即，访问单个连接的数据），该表视图将不包含任何信息。

连接和 安全相关连接 事件字段

注释 您不能使用连接/安全相关的连接事件“搜索”页面搜索与连接关联的事件。

访问控制策略（系统日志：ACPolicy）

监控连接的访问控制策略。

访问控制规则 (系统日志：AccessControlRuleName)

处理连接的访问控制规则或默认操作，以及最多 8 条该连接匹配的监控规则。

如果连接匹配一个监控规则，则 Cisco Secure Firewall Management Center会显示处理连接的规则的名称，后跟监控规则名称。如果连接匹配多个监控规则，则会显示匹配的监控规则数量，例如，默认操作 + 2 个监控规则。

要显示包含与连接匹配的前 8 个监控规则的列表的弹出窗口，请点击 ***N*** **个监控规则**。

操作（系统日志：AccessControlRuleAction）

与已记录连接的配置关联的操作。

对于受安全智能监控的连接，该项操作即为由连接触发的第一个非监控访问控制规则的操作，或者为默认操作。同样，由于与监控规则匹配的流量始终由后续规则或通过默认操作进行处理，因此与因监控规则而记录的连接相关联的操作绝不会是“监控”(Monitor)。不过，您仍然可以在与监控规则匹配的连接上触发关联策略违规。

操作	说明
允许	通过访问控制明确允许的或者由于用户绕过交互式阻止而允许的连接。
阻止、阻止并重置	受阻连接，包括： • 按预过滤器策略阻止的隧道及其他连接 • 被安全情报阻止的连接。 • 按 SSL 策略阻止的加密连接。 • 漏洞按入侵策略阻止的连接。 • 文件（包括恶意软件）按文件策略阻止的连接。 对于系统阻止入侵或文件的连接，即使使用访问控制“允许”(Allow)规则调用深度检查，系统也将显示 `Block`。
快速路径	按预过滤器策略使用快速路径的非加密隧道及其他连接
交互式阻止、交互式阻止并重置	在系统最初使用“交互式阻止”(Interactive Block) 规则阻止用户的 HTTP 请求时记录的连接。如果用户点击浏览系统显示的警告页面，则为会话记录的其他连接会执行操作“允许”(Allow)。
信任	访问控制信任的连接。系统根据设备型号以不同方式记录受信任的TCP连接。
默认操作	访问控制策略的默认操作处理的连接。
（空白/空）	在传递足够的数据包以匹配规则之前，连接已关闭。 只有在访问控制以外的其他设备（例如入侵防御）导致记录连接时，才会发生这种情况。

应用协议（系统日志：ApplicationProtocol）

在 Cisco Secure Firewall Management Center Web 界面中，此值限制摘要和图形。

连接中检测到的表示主机之间通信的应用协议。

应用协议类别和标记 (Application Protocol Category and Tag)

展示了应用特征的条件条件，协助您了解应用功能。

应用风险

与连接中检测到的应用流量关联的风险：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类应用都有一个相关风险；该字段显示最高风险。

身份验证源

根据所使用的身份验证类型，包含以下值之一：

- **被动身份代理的被动身份源**
- 配置为强制网络门户的 Azure AD (SAML) 领域的 **SAML 强制网络门户**

有关详细信息，请参阅《《Cisco Secure Firewall Management Center 设备配置指南》》。

业务相关性

与连接中检测到的应用流量关联的业务相关性：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类应用都有相关业务相关性；该字段显示级别最低的业务相关性。

客户端和客户端版本（系统日志：Client、ClientVersion）

在连接中检测到的客户端应用及版本。

如果系统无法识别连接中使用的特定客户端，则该字段会显示附加到应用协议名称的术语“client”，以提供通用名称，例如，FTP client。

客户端类别和标记 (Client Category and Tag)

展示了应用特征的条件，协助您了解应用功能。

连接计数器 （仅限系统日志）

区分一个连接与另一个同时连接的计数器。此字段本身没有意义。

以下字段共同唯一标识连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

连接实例 ID （仅限系统日志）

处理连接事件的 Snort 实例。此字段本身没有意义。

以下字段共同唯一标识连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

ConnectionDuration（仅限系统日志）

此字段仅作为系统日志字段存在；不会出现在 Cisco Secure Firewall Management Center Web 界面中。（Web 界面使用“第一个数据包”列和“最后一个数据包”列来传达此信息。）

仅当在连接结束后发生日志记录时，此字段才具有值。对于 start-of-connection 系统日志消息，由于此字段在当时未知，因此不是输出。

对于 end-of-connection 系统日志消息，此字段指示第一个数据包到最后一个数据包之间经过的秒数，短连接的秒数可为零。例如，如果系统日志的时间戳为 12:34:56，ConnectionDuration 为 5，则第一个数据包出现于 12:34:51。

连接

连接摘要中的连接数。对于长期运行连接，即跨越多个连接摘要间隔的连接，只有第一个连接摘要间隔可递增。要使用**连接 (Connections)** 条件查看有意义的搜索结果，请使用具有连接摘要页面的自定义工作流程。

计数

与每行显示的信息相匹配的连接数。请注意，**计数 (Count)** 字段仅在应用了创建两个或多个相同行的约束后才显示。如果创建了自定义工作流程，但未在向下钻取页面中添加**计数 (Count)** 列，则每个连接都将单独列出，且数据包和字节并不汇总。

解密对等体

为关联连接解密数据包的 VPN 对等体的 IP 地址（对等体的 IKE 地址）。

您必须启用访问控制策略规则的日志记录设置，以便在连接开始和结束时进行记录，以查看 VPN 对等体 IP 地址。如果启用绕过已解密流量的访问控制策略 (sysopt connection permit-vpn) 选项，则无法查看已解密流量的详细信息。

检测类型（系统日志：**DetectionType**）

此字段显示客户端应用的检测来源。它可以是 **AppID** 或 **加密可视性**。

目标端口/**ICMP** 代码（系统日志：单独字段 - **DstPort**、**ICMPCode**）

在 Cisco Secure Firewall Management Center Web 界面中，这些值限制摘要和图形。

会话 响应方使用的端口或 ICMP 代码。

DestinationSecurityGroup （仅限系统日志）

此字段包含与 **DestinationSecurityGroupTag**中的数字值关联的文本值（如果可用）。如果组名不可用作文本值，则此字段包含与 DestinationSecurityGroupTag 字段相同的整数值。

DestinationSecurityGroupType （仅限系统日志）

此字段显示从中获取安全组标记的源。

值	说明
内联	目标 SGT 值来自数据包
会话目录	目标 SGT 值通过会话目录主题来自 ISE
SXP	目标 SGT 值来自 ISE 通过 SXP 主题

目标 **SGT**（系统日志： **DestinationSecurityGroupTag**）

连接中涉及的目标的数值安全组标记 (SGT) 属性。

目标 SGT 值从 **DestinationSecurityGroupType** 字段中指定的源获取。

检测类型

此字段显示客户端的检测来源。

设备

在 Cisco Secure Firewall Management Center Web 界面中，此值限制摘要和图形。

检测到连接的受管设备，或者对于从 NetFlow 数据生成的连接，是指处理数据的受管设备。

DeviceUUID （仅限系统日志）

生成事件的 防火墙 设备的唯一标识符。

以下字段共同唯一标识连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

DNS 查询（系统日志：DNSQuery）

在与名称服务器的连接中提交的用于查找域名的 DNS 查询。

当启用 DNS 过滤时，此字段还可以保存 URL 过滤匹配的域名。在这种情况下，URL 字段将为空，URL 类别和 URL 信誉字段包含与域关联的值。

有关 DNS 过滤的详细信息，请参阅 DNS 过滤：在 DNS 查找期间识别 URL 信誉和类别。

DNS 记录类型（系统日志：DNSRecordType）

用于解析连接中提交的 DNS 查询的 DNS 资源记录的类型。

DNS 响应（系统日志：DNSResponseType）

查询时在与名称服务器的连接中返回的 DNS 响应。

DNS Sinkhole 名称（系统日志：DNS_Sinkhole）

系统将连接重定向的 Sinkhole 服务器的名称。

DNS TTL（系统日志：DNS_TTL）

DNS 服务器缓存 DNS 资源记录的秒数。

域

检测到连接的受管设备的域，或者对于从 NetFlow 数据生成的连接，是指处理数据的受管设备的域。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。

加密对等体

为关联连接加密数据包的 VPN 对等体的 IP 地址（对等体的 IKE 地址）。

您必须启用访问控制策略规则的日志记录设置，以便在连接开始和结束时进行记录，以查看 VPN 对等体 IP 地址。

加密可视性指纹（系统日志： EncryptedVisibilityFingerprint）

加密可视性引擎 (EVE) 为会话检测到的 TLS 指纹。要查看安全防火墙应用检测器 (Cisco Secure Firewall Application Detectors) 页面上的其他详细信息，必须使用思科邮箱 ID 和密码登录。

加密可视性进程名称（系统日志： EncryptedVisibilityProcessName）

由加密可视性引擎（EVE）分析的 TLS 客户端呼叫数据包中的进程或客户端。

加密可视性置信度得分（系统日志： EncryptedVisibilityConfidenceScore）

加密可视性引擎检测到正确进程的置信度值范围为 0-100%。例如，如果进程名称为 Firefox，并且置信度分数为 80%，则意味着引擎 80% 的置信度表示其检测到的进程是 Firefox。

加密可视性威胁置信度（系统日志： EncryptedVisibilityThreatConfidence）

加密可视性引擎（EVE）检测到的进程包含威胁的概率级别。此字段根据威胁置信度分数中的值指示频段（非常高，高，中，低或非常低）。

加密可视性威胁置信度评分（系统日志： EncryptedVisibilityThreatConfidenceScore）

加密可视性引擎检测到的进程包含威胁的置信度值范围为 0-100%。如果威胁置信度分数非常高，例如 90%，则加密可视性进程名称字段显示“恶意软件”。

终端位置 (Endpoint Location)

使用 ISE 对用户进行身份验证的网络设备的 IP 地址，如 ISE 所识别。

终端配置文件（系统日志：Endpoint Profile）

用户的终端设备类型，如 ISE 所识别。

事件优先级 （仅限系统日志）

连接事件是否为高优先级事件。高 优先级事件是与入侵、安全智能、文件或恶意软件事件关联的连接事件。所有其他事件均为 低 优先级。

文件（系统日志：FileCount）

在与一个或多个文件事件关联的连接中检测到或阻止的文件（包括恶意软件文件）数量。

在 Cisco Secure Firewall Management Center Web 界面中， **查看文件图标** 指向文件列表。图标上的数字表示连接中检测到或阻止的文件数量（包括恶意软件文件）。

第一个数据包或最后一个数据包（系统日志：ConnectionDuration 字段）

查看了会话的第一个或最后一个数据包的日期和时间。

第一个数据包时间 （仅限系统日志）

系统遇到第一个数据包的时间。

以下字段共同唯一标识连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

HTTP 引用站点（系统日志：HTTPReferer）

HTTP 来源地址，表示在连接中检测到的 HTTP 流量的请求 URL 来源地址（例如提供到另一个 URL 的链接或从其导入链接的网站）。

HTTP 响应代码（系统日志：HTTPResponse）

发送的 HTTP 状态代码用于响应客户端通过连接的 HTTP 请求。

入口/出口接口（系统日志：IngressInterface、EgressInterface）

与连接相关的入口或出口接口。如果部署包括异步路由配置，则入口和出口接口可能属于同一内联集。

入口/出口安全区域（系统日志：IngressZone、EgressZone）

与连接相关的入口或出口安全区。

对于重新分区的封装连接，“入口”(Ingress) 字段显示您分配的隧道区域，而不是原始入口安全区域。“出口”(Engress) 字段为空。

入口虚拟路由器/出口虚拟路由器（系统日志： IngressVRF、 EgressVRF）

在使用虚拟路由的网络中，用于流量进出网络的虚拟路由器的名称。

发起方/响应方字节数（系统日志：InitiatorBytes、ResponderBytes）

会话发起方传输的总字节数或会话响应方接收的总字节数。

Initiator/Responder Continent

当检测到可路由 IP 时，与会话发起方或响应方的 IP 地址关联的大洲。

Initiator/Responder Country

当检测到可路由 IP 时，与会话发起方或响应方的 IP 地址关联的国家/地区。系统显示国家/地区的旗帜图标和国家/地区的 ISO 3166-1 alpha-3 国家/地区代码。将鼠标指针悬停在旗帜图标上可以查看该国家/地区的全名。

发起方/响应方 IP（系统日志：SrcIP、DstIP）

在 Cisco Secure Firewall Management Center Web 界面中，这些值限制摘要和图形。

会话发起方或响应方的 IP 地址（如果启用 DNS 解析，则还包括主机名）。

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 ，第 20 页。

在 Cisco Secure Firewall Management Center Web 界面中，主机图标标识导致连接被阻止的 IP 地址。

对于被预过滤器策略阻止或使用快速路径的明文、传递隧道，启动器和响应器 IP 地址不表示隧道终端（隧道任一端的网络设备的路由接口）。

发起方/响应方数据包数 (系统日志： InitiatorPackets、ResponderPackets)

会话发起方传输的总数据包数或会话响应方接收的总数据包数。

发起方用户（系统日志：User）

在 Cisco Secure Firewall Management Center Web 界面中，此值限制摘要和图形。

登录到会话发起方的用户。如果使用**无身份验证**填充此字段，则用户流量：

- 匹配没有关联身份策略的访问控制策略
- 与身份策略中的任何规则都不匹配

如果适用，用户名前面会附加 <区域>\。

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 ，第 20 页。

入侵事件（系统日志：IPSCount）

与连接相关的入侵事件数量（如有）。

在 Cisco Secure Firewall Management Center Web 界面中， **查看入侵事件图标** 指向事件列表。

IOC

事件是否针对连接中涉及的主机触发了危害表现 (IOC)。

MITRE ATT&CK

用于在事件期间的任何给定时间查看ATT&CK框架中的攻击进度的进度图。支持在新窗格中详细介绍 MITRE 策略、技术和进度图的扩展视图。

- 点击进度图可查看事件的 MITRE ATT&CK 详细信息。MITRE ATT&CK 窗口显示策略、技术、子技术以及指向 MITRE 页面的链接。
- 在显示详细信息的窗口中，点击**详细信息 (Details)** 以查看该技术的一般说明。

NAT 源/目标 IP （系统日志： NAT_InitiatorIP，NAT_ResponderIP）

会话发起方或响应方的 NAT 转换 IP 地址。

NAT 源/目标端口（系统日志： NAT_InitiatorPort，NAT_ResponderPort）

会话发起方或响应方的 NAT 转换端口。

NetBIOS 域（系统日志：NetBIOSDomain）

会话中使用的 NetBIOS 域。

NetFlow SNMP Input/Output

对于从NetFlow数据生成的连接，是指连接流量进入或退出NetFlow导出器时接口的接口索引。

NetFlow 源/目标自治系统 (NetFlow Source/Destination Autonomous System)

对于从 NetFlow 数据生成的连接，是指连接中的流量源或目标的边界网关协议自治系统编号。

NetFlow 源/目标前缀 (NetFlow Source/Destination Prefix)

对于从 NetFlow 数据生成的连接，是指与源或目标前缀掩码用 AND 连接的源或目标 IP 地址。

NetFlow 源/目标 TOS (NetFlow Source/Destination TOS)

对于从 NetFlow 数据生成的连接，是指连接流量进入或退出 NetFlow 导出器时服务类型 (TOS) 字节的设置。

网络分析策略（系统日志：NAPPolicy）

与事件生成相关的网络分析策略 (NAP)（如果有）。

原始客户端国家/地区 (Original Client Country)

原始客户端IP地址所属的国家/地区。为获取该值，系统从X-Forwarded-For (XFF)、True-Client-IP或自定义的HTTP报头提取原始客户端IP地址，然后使用地理位置数据库 (GeoDB) 将其映射到国家/地区。要填充此字段，必须启用根据原始客户端处理代理流量的访问控制规则。

原始客户端 IP（系统日志：originalClientSrcIP）

来自 X-Forwarded-For (XFF)、True-Client-IP 或自定义的 HTTP 报头的原始客户端 IP 地址。要填充此字段，必须启用根据原始客户端处理代理流量的访问控制规则。

其他扩充

与支持展开视图的事件关联的非 MITRE 信息。

预过滤器策略（系统日志：Prefilter Policy）

处理连接的预过滤器策略。

协议（系统日志：Protocol）

在 Cisco Secure Firewall Management Center Web 界面中：

- 此值限制摘要和图形。
- 此字段仅用作搜索字段。

连接中使用的传输协议。要搜索特定协议，请使用 http://www.iana.org/assignments/protocol-numbers 中所列的名称或编号协议。

QoS 应用的接口 (QoS-Applied Interface)

对于速率受限的连接，是指应用了速率限制的接口的名称。

QoS 丢弃的发起方/响应方字节数 (QoS-Dropped Initiator/Responder Bytes)

由于速率限制而从会话发起方或会话响应方丢弃的字节数。

QoS 丢弃的发起方/响应方数据包数 (QoS-Dropped Initiator/Responder Packets)

由于速率限制而从会话发起方或会话响应方丢弃的数据包的数量。

QoS 策略的比较

对连接进行了速率限制的 QoS 策略。

QoS 规则 (QoS Rule)

对连接进行了速率限制的 QoS 规则。

QUIC 会话 ID

64 位内部会话标识符，用于在防火墙内唯一标识 QUIC 连接。

QUIC 流 ID

62 位数据流标识符，用于在 QUIC 连接中唯一标识数据流。

原因（系统日志：AccessControlRuleReason）

在许多情况下记录连接的一个或多个原因。有关完整列表，请参阅 连接事件原因，第 20 页。

原因为“IP 阻止”(IP Block)、“DNS 阻止”(DNS Block) 和“URL 阻止”(URL Block) 的连接在每个唯一发起方-响应方对中的阈值都为 15 秒。系统在阻止其中一个连接后，无论端口或协议如何，在接下来的 15 秒内都不会为这两个主机之间的其他受阻连接生成连接事件。

引用的主机（系统日志：ReferencedHost）

如果连接中的协议是 HTTP 或 HTTPS，则此字段显示各协议使用的主机名。

SecIntMatchingIP（仅限系统日志）

哪些 IP 地址匹配。

可能的值：**None**、**Destination** 或 **Source**。

安全情景（系统日志：Context）

对于在多情景模式下由 ASA FirePOWER 处理的连接，是指识别流量通过的虚拟防火墙组的元数据。

安全情报类别（系统日志： URLSICategory、 DNSSICategory 、IPReputationSICategory）

代表或包含连接中被受阻的URL、域名或IP地址的对象的名称。安全智能类别可以是网络对象或组、阻止列表、自定义安全智能列表或源、与观察关联的 TID 类别或者智能源中一个类别的名称。

在 Cisco Secure Firewall Management Center Web 界面中，DNS、网络（IP 地址）和 URL 安全智能连接事件会合并为单个类别字段。在系统日志消息中，这些事件具有特定的类型。

与安全相关的连接事件包括安全情报事件和其他连接事件，例如触发入侵或恶意软件事件的连接事件。**安全情报摘要** 工作流程按类别和计数显示所有安全情报事件。没有安全情报类别的事件将分组并仅显示计数。

有关智能智能源中的类别详细信息，请参阅安全智能类别。

源设备

在 Cisco Secure Firewall Management Center Web 界面中，此值限制摘要和图形。

广播用于为连接生成的数据的 NetFlow 导出器的 IP 地址。如果受管设备检测到连接，则此字段显示 `Firepower`。

源端口/ICMP 类型（系统日志：SrcPort、ICMPType）

在 Cisco Secure Firewall Management Center Web 界面中，这些值限制摘要和图形。

会话发起方使用的端口或 ICMP 类型。

SourceSecurityGroup （仅限系统日志）

此字段包含与 **SourceSecurityGroupTag** 中的数字值关联的文本值（如果可用）。如果组名不可用作文本值，则此字段包含与 SourceSecurityGroupTag 字段相同的整数值。可以从内联设备（未指定源 SGT 名称）或从 ISE（指定源）获取标签。

SourceSecurityGroupType （仅限系统日志）

此字段显示从中获取安全组标记的源。

值	说明
内联	源 SGT 值来自数据包
会话目录	源 SGT 值通过会话目录主题来自 ISE
SXP	源 SGT 值来自 ISE 通过 SXP 主题

源 SGT（系统日志： SourceSecurityGroupTag）

连接中涉及的数据包的安全组标记 (SGT) 的数值呈现的属性。SGT 指定受信任网络中的流量源的权限。安全组访问（思科 TrustSec 和思科 ISE 的功能）在数据包进入网络时应用该属性。

SSL 实际操作（系统日志：SSLActualAction）

在 Cisco Secure Firewall Management Center Web 界面中，此字段仅为搜索字段。

系统显示搜索工作流程页面上的 **SSL 状态** 字段中的字段值。

系统应用于 SSL 策略中的加密流量的操作。

操作	说明
阻止/阻止并重置	表示阻止的加密连接。
解密（重新签名）	表示使用重新签名的服务器证书解密的传出连接。
解密（替换密钥）	表示使用具有替代公钥的自签名服务器证书解密的传出连接。
解密（已知密钥）	表示使用已知私钥解密的传入连接。
默认操作	表示连接采用默认操作处理。
不解密	表示系统未解密的连接。

SSL 证书信息（系统日志：SSLCertificate）

在 Cisco Secure Firewall Management Center Web 界面中，此字段仅为搜索字段。

用于加密流量的公钥证书上存储的信息，包括：

- 使用者/颁发者公用名称
- 使用者/颁发者组织
- 使用者/颁发者单位
- 无效时间
- 序列号
- 证书指纹
- 公钥指纹

SSL 证书信息（系统日志：SSLServerCertStatus）

仅在配置了证书状态规则条件时，此字段才适用。如果加密流量与 SSL 规则匹配，则此字段显示以下一个或多个服务器证书状态值：

- 自签名
- 有效
- 无效签名
- 无效颁发者
- 已到期
- 未知
- 无效
- 已撤销

如果无法解密的流量与 SSL 规则相匹配，则此字段显示未检查 (Not Checked)。

SSL 密码套件（系统日志：SSSLCipherSuite）

表示用于加密连接的密码套件的宏值。有关密码套件值的指定，请参阅https://www.iana.org/assignments/tls-parameters/tls-parameters.xhtml。

应用于连接的 SSL 加密

此字段在 Cisco Secure Firewall 管理中心 Web 界面中仅用作搜索字段。

在 **SSL** 搜索字段中输入 **yes** 或 **no** 以查看 TLS/SSL 加密或非加密连接。

SSL 预期操作（系统日志：SSLExpectedAction）

在 Cisco Secure Firewall Management Center Web 界面中，此字段仅为搜索字段。

在 SSL 规则生效的情况下，系统预期会应用于加密流量的操作。

输入为 SSL **实际操作**列出的任何值。

SSL 失败原因（系统日志：SSLFlowStatus）

系统无法解密已加密流量的原因：

- 未知
- 不匹配
- 成功
- 未缓存的会话
- 未知加密套件
- 不受支持的加密套件
- 不支持的 SSL 版本
- 使用了 SSL 压缩
- 会话在被动模式下无法解密

- 握手错误
- 解密错误
- 挂起的服务器名称类别查找
- 挂起的公用名类别查找
- 内部错误 (Internal Error)
- 不完全握手
- 网络参数不可用
- 服务器证书处理无效
- 服务器证书指纹不可用
- 无法缓存使用者 DN
- 无法缓存颁发者 DN
- 未知的 SSL 版本
- 外部证书列表不可用
- 外部证书指纹不可用
- 内部证书列表无效
- 内部证书列表不可用
- 内部证书不可用
- 内部证书指纹不可用
- 服务器证书验证不可用
- 服务器证书验证失败
- 无效操作

字段值显示在搜索工作流程页面上的 **SSL 状态**字段中。

SSL 流错误

当在 TLS/SSL 会话期间发生错误时，为错误名称和十六进制代码，如果未发生错误，则为 `Success`。

SSL 流标志

已加密连接的前十大调试级别标记。在工作流程页面上，要查看所有标记，请点击省略号 (**...**)。

如果您的受管设备过载，则将显示消息OVER_SUBSCRIBED。有关详细信息，请参阅对 TLS/SSL 超订用进行故障排除。

SSL 流消息

下面的关键字表示加密流量与在 TLS/SSL 握手期间客户端和服务器之间交换的指定消息类型相关联。有关详细信息，请参阅http://tools.ietf.org/html/rfc5246。

- HELLO_REQUEST
- CLIENT_ALERT
- SERVER_ALERT
- CLIENT_HELLO
- SERVER_HELLO
- SERVER_CERTIFICATE
- SERVER_KEY_EXCHANGE
- CERTIFICATE_REQUEST
- SERVER_HELLO_DONE
- CLIENT_CERTIFICATE
- CLIENT_KEY_EXCHANGE
- CERTIFICATE_VERIFY
- CLIENT_CHANGE_CIPHER_SPEC
- CLIENT_FINISHED
- SERVER_CHANGE_CIPHER_SPEC
- SERVER_FINISHED
- NEW_SESSION_TICKET
- HANDSHAKE_OTHER
- APP_DATA_FROM_CLIENT
- APP_DATA_FROM_SERVER
- 服务器_名称_不匹配

  在会话中看到的服务器证书具有不对应于指定域名的公用名或 SAN 值。
- 证书_缓存_HIT

  在缓存中找到与目标域名匹配的证书。
- 证书_缓存_MISS

  在缓存中未找到与目标域名匹配的证书。

如果应用使用 TLS/SSL 心跳扩展，则将显示消息 HEARTBEAT。有关详细信息，请参阅关于 TLS 心跳。

SSL 策略（系统日志：SSLPolicy）

处理连接的 SSL 策略。

如果在访问控制策略高级设置中启用了 TLS 服务器身份发现，并且没有与访问控制策略关联的 SSL 策略，则此字段 不 对所有 SSL 事件保留任何内容。

SSL 规则（系统日志：SSLRuleName）

处理连接的 SSL 规则或默认操作，以及与连接匹配的第一个监控规则。如果连接匹配某个监控规则，则该字段会显示处理连接的规则的名称，后跟监控规则名称。

SSLServerName（仅限系统日志）

此字段仅作为系统日志字段存在；不会出现在 Cisco Secure Firewall Management Center Web 界面中。

客户端用于建立加密连接的服务器主机名。

SSL 会话 ID（系统日志：SSLSessionID）

在 TLS/SSL 握手期间，在客户端与服务器之间协商的十六进制会话 ID。

SSL 状态

与记录加密连接的 **SSL 实际操作**（SSL 规则、默认操作或无法解密的流量操作）关联的操作。**锁定图标** 指向 SSL 证书详细信息。如果证书不可用（例如，对于因 TLS/SSL 握手错误而受阻的连接），锁定图标会显示为灰色。

如果系统无法解密已加密连接，则其会显示所采取的 **SSL 实际操作**（无法解密的流量操作）以及 **SSL 失败原因**。例如，如果系统检测到使用未知密码套件加密的流量并且未做进一步检查即允许了该流量，则此字段显示 `Do Not Decrypt (Unknown Cipher Suite)`。

如果加密连接的 SSL 握手不完整，并且系统无法解密流量，则 SSL **状态**字段显示未知（不完整握手）。

当搜索该字段时，请输入一个或多个 **SSL 实际操作**和 **SSL 失败原因 (SSL Failure Reason)** 值以查看系统处理或无法解密的已加密流量。

SSL 使用者/颁发者所在国家/地区

此字段仅在 Cisco Secure Firewall Management Center Web 界面中可用，且仅作为搜索字段。

与加密证书关联的使用者或颁发者所在国家/地区的双字符 ISO 3166-1 alpha-2 国家/地区代码。

SSL 票证 ID（系统日志：SSLTicketID）

在 TLS/SSL 握手期间发送的会话单信息的一个十六进制哈希值。

SSLURLCategory（仅限系统日志）

加密连接中受访 URL 的 URL 类别。

此字段仅作为系统日志字段存在；在 Cisco Secure Firewall Management Center Web 界面中，此字段中的值包含在“URL 类别”列中。

另请参阅 **URL**。

SSL 版本（系统日志：SSLVersion）

用来加密连接的 TLS/SSL 协议版本。

- 未知
- SSLv2.0
- SSLv3.0
- TLSv1.0
- TLSv1.1
- TLSv1.2
- TLSv1.3

TCP 标志（系统日志：TCPFlags）

对于从 NetFlow 数据生成的连接，是指在连接中检测到的 TCP 标志。

当搜索此字段时，输入逗号分隔的 TCP 标志列表以查看 至少 具有其中一个标志的所有连接。

时间

系统用来在连接摘要中汇总连接的 5 分钟时间间隔的结束时间。此字段不可搜索。

数据包总数

此字段仅用作搜索字段。

在连接中传输的数据包的总数。

流量 (KB)

此字段仅用作搜索字段。

在连接中传输的总数据量（以千字节为单位）。

隧道/预过滤器规则（系统日志：Tunnel or Prefilter Rule）

处理连接的隧道规则、预过滤器规则或预过滤器策略默认操作。

URL、URL 类别和 URL 信誉（系统日志： URL、 URL 类别 和 SSLURLCategory， URL 类别）

会话期间受控主机请求的 URL 以及该 URL 的类别和信誉（如有）。

要使事件显示 URL 类别和信誉，必须在访问控制策略中包含适用的 URL 规则，并在 **URL** 选项卡下为该规则配置 URL 类别和 URL 信誉。

如果连接在与 URL 规则匹配之前得到处理，则 URL 类别和信誉不会显示在事件中。

如果 URL 列为空且 DNS 过滤已启用，则 DNS 查询字段显示域，并且 URL 类别和 URL 信誉值适用于该域。

如果系统识别或阻止 TLS/SSL 应用，而请求的 URL 位于加密流量中，系统会基于 SSL 证书识别流量。因此，对于 TLS/SSL 应用，此字段表示包含在证书中的通用名称。

另请参阅上述 **SSLURLCategory**。

用户代理（系统日志：UserAgent）

从连接中检测到的 HTTP 流量提取的用户代理字符串应用信息。

VLAN ID（系统日志：VLAN_ID）

与触发连接的数据包关联的最内部的 VLAN ID。

VPN 操作

与连接关联的 VPN 操作。

可能的值包括：

- **加密**：VPN 对已记录连接的流量进行加密。请参阅 **加密对等体** 列，了解加密连接的 VPN 对等体的 IP 地址。
- **解密**：VPN 解密已记录连接的流量。请参阅 **加密对等体** 列，了解解密连接的 VPN 对等体的 IP 地址。
- **VPN 路由**：流量通过 VPN 隧道转换。VPN 在连接开始时执行解密，在连接结束时执行加密。请参阅 **加密对等体** 和 **解密对等体列**，了解加密和解密连接的 VPN 对等体的 IP 地址。

Web 应用（系统日志：WebApplication）

表示连接中检测到的 HTTP 流量内容或请求的 URL 的 Web 应用。

如果 Web 应用不匹配事件的 URL，该流量大概是推荐流量，例如广告流量。如果系统检测到推荐流量，则会存储该推荐应用（如有），并将该应用列为 Web 应用。

如果系统不能在 HTTP 流量中识别特定的网络应用，该字段显示网络浏览 (`Web Browsing`)。

Web 应用类别和标记 (Web Application Category and Tag)

展示了应用特征的条件，以帮助您了解应用功能。

关于连接和 安全相关连接事件 字段

在 Cisco Secure Firewall Management Center Web 界面中，您可以使用 **分析 > 连接** 子菜单下的表格和图形工作流程查看和搜索连接和 安全相关连接 事件。

注释 对于每个 安全相关连接事件，都有相同、独立存储的连接事件。所有 安全相关连接事件 都有一个由系统填充的 **安全情报类别** 字段。

任何单独事件的可用信息视系统记录连接的方式、原因和时间而异。

搜索限制

搜索页面上标有星号 (*) 的字段会限制连接图形和连接摘要。由于连接图基于连接摘要，因此，约束连接摘要的相同条件也约束连接图。如果使用无效搜索限制来搜索连接摘要，并在自定义工作流程中使用连接摘要页面查看结果，则无效限制会标记为不适用 (N/A)，并标有删除线。

系统日志字段

大多数字段会同时显示在 Cisco Secure Firewall Management Center Web 界面和系统日志消息中。没有所列的系统日志等同项的字段在系统日志消息中不可用。如前所述，一些字段仅在系统日志中提供，并且其他一些字段在系统日志消息中为分开字段，而在 Web 界面中为合并字段，反之亦然。

有关发起方/响应方，源/目标和发件人/接收方字段的说明

表 *1:* 术语比较

字段	事件类型	说明
发起方/响应方	连接	连接的发起方/响应方。 连接的发起方不一定与入侵源或恶意软件文件的发送方相同。
源/目标	入侵	攻击的源/目标。 入侵事件的源可以是连接的发起方或响应方。
发件人/收件人 （正在发送...，正在接收...）	文件，恶意软件	文件或恶意软件的发件人/收件人。 文件的发送方不一定是连接的发起方，因为可以上传或下载文件。

连接事件原因

在以下情况下，连接事件中的“原因”(Reason) 字段显示记录连接的原因：

原因	说明
内容限制	系统修改数据包以实施与安全搜索功能相关的内容限制。
DNS 阻止	系统未经检查就根据域名和安全智能数据拒绝连接。“DNS 阻止”原因与“阻止”、“找不到域”或 Sinkhole 操作匹配，具体取决于 DNS 规则操作。
DNS 监控	系统将根据域名和安全智能数据拒绝连接，但您将系统配置为监控而不是拒绝连接。

原因	说明
大象流	连接速率大到足以被认为是大象流，这种流的大小足以影响整体系统性能。默认情况下，大象流是速率大于每 10 秒 1GB 的流。您可以使用 **系统支持大象流检测** 命令调整字节和时间阈值，以在 威胁防御 CLI 中识别大象流。有关详细信息，请参阅Cisco Secure Firewall Threat Defense 命令参考。 **注释** 仅当超过字节和时间阈值时，流才被视为大象流。 您可以创建自定义控制面板来关联象流和其他相互关联的指标，例如 Snort、系统和物理核心等 CPU 指标。有关详细信息，请参阅“测试和故障排除”章节。
已豁免大象流	如果检测到大型流，并且该流与为必须免于补救的流定义的 L4 ACL 规则匹配。
文件阻止	连接中包含系统禁止传输的文件或恶意软件文件。“文件阻止”原因始终与“阻止”操作匹配。
文件自定义检测	连接中包含自定义检测列表上系统禁止传输的文件。
文件监控	系统在连接中检测到特定类型的文件。
允许继续传输文件	文件传输最初被“阻止文件”或“阻止恶意软件”文件规则阻止。在部署允许该文件的新访问控制策略之后，将自动继续 HTTP 会话。此原因只出现在内联部署中。
阻止继续传输文件	“检测文件”或“恶意软件云查找”文件规则最初允许文件传输。在新访问控制策略阻止文件部署之后，会自动停止 HTTP 会话。此原因只出现在内联部署中。
智能应用绕行 (Intelligent App Bypass)	智能应用绕行 (IAB) 模式： • 如果操作是“信任”(Trust)，则 IAB 处于绕行模式。匹配的流量通过，无需进一步检查。 • 如果操作是“允许”(Allow)，则 IAB 处于测试模式。匹配流量可供进一步检查。
入侵阻止	Snort2 引擎-系统阻止或本可阻止在连接中检测到的漏洞（入侵策略违规）。“入侵阻止”原因与用于阻止漏洞的“阻止”操作和用于本可阻止漏洞的“允许”操作匹配。 Snort3引擎-当出现“将被丢弃”结果时，连接事件原因为空，而不是“入侵阻止”。对于“已丢弃”事件，在填充连接事件原因方面将其视为“允许”。
入侵监控	系统检测到但并未阻止连接中检测到的漏洞。当触发的入侵规则状态设置为“生成事件”时，即会发生这种情况。
IP 阻止	系统未经检查就根据 IP 地址和安全智能数据拒绝连接。“IP 阻止”原因始终与“阻止”操作匹配。

原因	说明
IP 监控	系统将根据 IP 地址和安全智能数据拒绝连接，但您将系统配置为监控而不是拒绝连接。
SSL 阻止	系统基于 TLS/SSL 检查配置阻止加密连接。“SSL 阻止”(SSL Block) 原因始终与“阻止”(Block) 操作匹配。
URL 阻止	系统未经检查就根据 URL 和安全智能数据拒绝连接。“URL 阻止”原因始终与“阻止”操作匹配。
URL 监控	系统将根据 URL 和安全智能数据拒绝连接，但您将系统配置为监控而不是拒绝连接。
用户绕行	系统最初阻止用户的 HTTP 请求，但用户点击浏览警告页面以查看网站。“用户绕行”(User Bypass) 原因始终与“允许”(Allow) 操作匹配。

填充连接事件字段的要求

可用于连接事件、 安全相关的连接事件或连接摘要的信息取决于多种因素。

设备型号和许可证

许多功能要求您启用目标设备上的特定许可功能，并且许多功能仅在部分型号上可用。

流量特征

系统仅报告在网络流量中展示（并且可检测）的信息。例如，可能没有与发起人主机相关联的用户，或者在协议不是 DNS、HTTP 或 HTTPS 的连接中未检测到引用的主机。

源/检测方法：基于流量的检测与 NetFlow

除纯 NetFlow 字段以外，NetFlow 记录中可用的信息比由基于流量的检测生成的信息更有限；请参阅NetFlow 和受管设备数据之间的差异。

评估阶段

每种类型的流量检查和控制都以提供最大灵活性和性能的方式进行。

例如，在进行更多资源密集型评估之前，系统会强制实施安全情报。当连接被安全情报阻止时，生成的事件不包含系统本该从后续评估中收集的信息（例如用户身份）。

记录方法：连接的开始或结束

当系统检测到连接时，您可以在其开始还是结束（或两者）时记录该连接取决于如何将系统配置为检测和处理该连接。

开始连接事件不具有必须通过检查会话持续时间内的流量来确定的信息（例如，连接中传输数据的总量或最终数据包的时间戳）。也不保证开始连接事件拥有关于会话中应用或URL流量的信息，且该等事件不包含有关会话加密的任何详细信息。连接开始日志记录通常是受阻连接的唯一选项。

连接事件类型：个别与摘要

连接摘要不包含与其汇聚连接相关联的所有信息。例如，在汇总连接以形成连接摘要时没有使用客户端信息，因此摘要中不包含客户端信息。

请记住，连接图基于连接摘要数据，这些数据仅使用连接结束日志。如果系统配置为仅记录连接开始数据，则连接图和连接摘要事件视图不包含任何数据。

注释 与安全相关的连接事件包括安全情报事件和其他连接事件，例如触发入侵或恶意软件事件的连接事件。**安全情报摘要 (Security Intelligence Summary)** 工作流程将没有安全情报类别的安全相关连接事件分组，并显示没有 **安全情报类别 (Security Intelligence Category)** 值的计数。

其他配置

影响连接日志记录的其他配置包括但不限制：

- 仅当在与通过 Active Directory 域控制器进行身份验证的用户关联的连接中配置 ISE 时，才填充 ISE 相关字段。连接事件不包含通过 LDAP、RADIUS 或 RSA 域控制器进行身份验证的用户的 ISE 数据。
- 仅当将 ISE 配置为身份源或添加自定义 SGT 规则条件时，才会填充“安全组标记” (SGT) 字段。
- 仅在由预过滤器策略处理的连接中，才会填充预过滤器相关字段（包括安全区域字段中的隧道区域信息）。
- 仅在由 解密策略处理的加密连接中，才会填充TLS/SSL相关字段。如果不需要解密流量，则可以使用“不解密”规则操作查看这些字段的值。
- 仅在由与文件策略关联的访问控制规则记录的连接中，才会填充文件信息字段。
- 仅在由与入侵策略关联或使用默认操作的访问控制规则记录的连接中，才会填充入侵信息字段。
- 仅在速率受限的连接中，才会填充 QoS 相关字段。
- 仅在特定情况下（例如，当用户绕过交互式阻止配置时），才会填充“原因”(Reason) 字段。
- 仅当曾经配置 Cisco Secure Firewall Management Center以实现多租户时，才存在“域”字段。
- 访问控制策略中的一项高级设置控制系统为 HTTP 会话中的受监控主机请求的每个 URL 存储在连接日志中的字符数。如果您使用此设置来禁用URL日志记录，则虽然您仍可查看类别和信誉数据（如果存在），但系统不会在连接日志中显示单个 URL。
- 要使连接事件显示 URL 类别和信誉，必须在访问控制策略中包含适用的 URL 规则，并在 **URL** 选项卡下配置具有 URL 类别和 URL 信誉的规则。如果连接在与 URL 规则匹配之前得到处理，则 URL 类别和信誉不会显示在事件中。

相关主题

NetFlow 和受管设备数据之间的差异

连接事件字段中的可用信息

本主题中的表指示系统何时可以填充连接和安全智能字段。表中的列表示以下事件类型：

- 源：直接 - 代表由系统受管设备检测和处理的连接的事件。
- 源：NetFlow - 代表由 NetFlow 导出器导出的连接的事件。
- 记录：开始 - 代表在开始时记录的连接的事件。
- 记录：结束 - 代表在结束时记录的连接的事件。

表中的“是”并不意味着系统必须填充连接事件字段，而表示它可以填充。系统仅报告在网络流量中展示（并且可检测）的信息。例如，只有由 解密策略处理的加密连接的记录，才会填充 TLS/SSL 相关字段。

连接事件字段	源：直接	源：NetFlow	记录：开始	记录：结束
访问控制策略	是	否	是	是
访问控制规则	是	否	是	是
操作	是	否	是	是
应用协议	是	是	如果有	是
应用协议类别和标记	是	否	如果有	是
应用风险	是	否	如果有	是
业务相关性	是	否	如果有	是
客户端	是	否	如果有	是
客户端类别和标记	是	否	如果有	是
客户端版本	是	否	如果有	是
连接	是	是	否	是
计数	是	是	是	是
目标端口/ICMP 类型	是	是	是	是
目标 SGT	是	否	是	是
设备	是	是	是	是
域	是	是	是	是

连接事件字段	源：直接	源：NetFlow	记录：开始	记录：结束
DNS 查询	是	否	是	是
DNS 记录类型	是	否	是	是
DNS 响应	是	否	是	是
DNS Sinkhole 名称	是	否	是	是
DNS TTL	是	否	是	是
出口接口	是	否	是	是
出口安全区域	是	否	是	是
终端位置	是	否	是	是
终端配置文件	是	否	是	是
文件	是	否	否	是
首个数据包	是	是	是	是
HTTP 引用站点	是	否	否	是
HTTP 响应代码	是	否	是	是
入口接口	是	否	是	是
入口安全区域	是	否	是	是
发起方字节数	是	是	不实用	是
发起方所在国家/地区	是	否	是	是
发起方 IP	是	是	是	是
发起方数据包数	是	是	不实用	是
发起方用户	是	是	是	是
入侵事件	是	否	否	是
入侵策略	是	否	是	是
IOC（危害表现）	是	否	是	是
最后数据包	是	是	否	是
NetBIOS 域	是	否	是	是
NetFlow 源/目标自治系统	否	是	否	是

连接事件字段	源：直接	源：**NetFlow**	记录：开始	记录：结束
NetFlow 源/目标前缀	否	是	否	是
NetFlow 源/目标 TOS	否	是	否	是
NetFlow SNMP 输入/输出	否	是	否	是
Network Analysis Policy	是	否	是	是
原始客户端国家/地区	是	否	是	是
原始客户端 IP	是	否	是	是
预过滤器策略	是	否	是	是
QoS 适用接口	是	否	否	是
QoS 丢弃的发起方字节数	是	否	否	是
QoS 丢弃的发起方数据包数	是	否	否	是
QoS 丢弃的响应方字节数	是	否	否	是
QoS 丢弃的响应方数据包数	是	否	否	是
QoS 策略的比较	是	否	否	是
QoS 规则	是	否	否	是
原因	是	否	是	是
引用的主机	是	否	否	是
响应方字节数	是	是	不实用	是
响应方所在国家/地区	是	否	是	是
响应方 IP	是	是	是	是
响应方数据包数	是	是	不实用	是
安全情景（仅 ASA）	是	否	是	是
安全智能类别	是	否	是	是
源设备	是	是	是	是
源端口/ICMP 类型	是	是	是	是
源 SGT	是	否	是	是
SSL 证书状态	是	否	否	是

连接事件字段	源：直接	源：NetFlow	记录：开始	记录：结束
SSL 密码套件	是	否	否	是
SSL 流错误	是	否	否	是
SSL 流量标志	是	否	否	是
SSL 流量消息	是	否	否	是
解密策略	是	否	否	是
解密规则	是	否	否	是
SSL 会话 ID	是	否	否	是
SSL 状态	是	否	否	是
SSL 版本	是	否	否	是
TCP 标志	否	是	否	是
时间	是	是	否	是
隧道/预过滤器规则	是	否	是	是
URL	是	否	如果有	是
URL 类别	是	否	如果有	是
URL 信誉	是	否	如果有	是
用户代理	是	否	否	是
VLAN ID	是	否	是	是
Web 应用程序	是	否	如果有	是
Web 应用类别和标记	是	否	如果有	是

使用连接和 安全相关连接 事件表

可以使用 Cisco Secure Firewall Management Center 查看连接或 安全相关连接事件表。然后，可根据要查找的信息操纵事件视图。

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。

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，最终会产生事件的表视图。还可创建自定义工作流程，仅显示匹配特定需求的信息。

使用连接或安全情报工作流程表时，可以执行许多常见操作。

请注意，当您在向下展开解页面上约束连接事件时，来自相同事件的数据包和字节数将累加。然而，如果您正使用自定义工作流程，且没有将**计数 (Count)** 列添加到向下钻取页面，则会单独列出事件，数据包和字节将不会累加。

请注意，如果系统生成的连接事件数超过 25，则**连接事件 (Connection Events)** 表视图会显示**众多事件中的 1 个 (1 of Many)**，而不是可用的事件页面数。

开始之前

您必须是管理员或安全分析师用户才能执行此任务。

过程

步骤 1 选择以下其中一个选项：

- **分析** > **连接** > **事件** （适用于连接事件）
- **分析 (Analysis)** > **连接 (Connections)** > **安全相关事件 (Security-Related Events)**

注释
如果系统显示连接图而不是表，请按工作流程标题点击**切换工作流程 (switch workflow)**，然后选择预定义**连接事件 (Connection Events)** 工作流程，或自定义工作流程。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 有以下选项可供选择：

- “时间范围”(Time Range) - 要调整时间范围（如果未显示事件，则非常有用），请参阅更改时间窗口。
- 数据源 - 如果使用 Security Analytics and Logging（本地部署）远程存储数据，并且您有充分的理由更改数据源，请选择数据源。有关此选项的重要信息，请参阅在 Cisco Secure Firewall Management Center 和使用存储在 Secure Network Analytics 设备上的连接事件上工作。
- “字段名称”(Field Names) - 要了解有关表中各列内容的详细信息，请参阅连接和 安全相关连接 事件字段 ， 第 3 页。

  提示
  事件表视图中的多个字段在默认情况下处于隐藏状态。要更改显示的字段，请点击任何列名称中的 禁用列  以显示字段选择器。

- 其他信息 - 要查看系统外部可用源中的数据，请右键点击事件值。您看到的选项取决于数据类型，包括公共源；其他来源取决于您配置的资源。有关信息，请参阅使用基于 Web 的资源的事件调查
- 外部情报 - 要收集有关事件的情报，请右键点击表中的事件值，然后从思科或第三方情报源中进行选择。例如，您可以从思科 Talos 获取有关可疑 IP 地址的详细信息。您看到的选项将取决于数据类型以及系统上配置的集成。有关详细信息，请参阅 使用基于 Web 的资源的事件调查。

- 主机配置文件 - 要查看 IP 地址的主机配置文件，请点击**主机配置文件 (Host Profile)**，或者对于具有活动危害表现 (IOC) 标记的主机，点击该 IP 地址旁边显示的**受损主机 (Compromised Host)**。
- 用户配置文件 - 要查看用户身份信息，请点击显示在**用户身份 (User Identity)**旁的用户图标，或对于与 IOC 相关联的用户，请点击**红色用户 (Red User)**。
- 文件和恶意软件 - 要查看在连接中检测到或阻止的文件（包括恶意软件），请点击**查看文件 (View Files)**，然后如查看连接中检测到的文件和恶意软件，第 30 页中所述继续操作。
- 入侵事件 - 要查看与某个连接关联的入侵事件，及其优先级和影响，请点击**入侵事件 (Intrusion Events)** 列中的**入侵事件 (Intrusion Events)** 列，然后如查看与连接关联的入侵事件，第 31 页中所述继续操作。

  提示
  要快速查看与一个或多个连接关联的入侵、文件或恶意软件事件，请使用表中的复选框选中连接，然后从**跳转至**下拉列表中选择合适的选项。请注意，由于它们在访问控制规则评估之前已被阻止，因此可能没有与列入安全情报阻止名单的连接关联的文件或入侵。如果已配置安全情报来监控连接（而非将其阻止），则只可以看到安全情报事件的这一信息。

- 证书 - 要查看有关用于解密连接的可用证书的详细信息，请在 **SSL 状态 (SSL Status)** 列中点击**已启用的锁定 (Enabled Lock)**。
- 限制 - 要限制显示的列，请在要隐藏的列标题中点击 **关闭** (×) 在显示的弹出窗口中，点击 **Apply**。

  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)**。要将已禁用列添加回视图中，请展开搜索限制条件，然后点击“已禁用列”(Disabled Columns) 下的列名称。

- 删除事件 - （仅限安全相关连接事件 表） 要删除当前限制视图中的部分或全部项目，请选中要删除的项目旁边的复选框，然后点击 **删除** 或点击 **全部删除**。
- 向下展开 - 请参阅使用向下钻取页面。

  提示
  要使用匹配已记录连接的多个监控规则之一向下展开，请点击一个 *N* **监控规则**值。在出现的弹出窗口中，点击要用于限制连接事件的监控规则。

- “导航此页面”(Navigate This Page) - 请参阅工作流程页面遍历工具。
- “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。
- “排序”(Sort) - 要对工作流程中的数据排序，请点击列标题。再次点击列标题以反转排列顺序。

相关主题

概述：工作流程
配置事件视图设置

查看连接中检测到的文件和恶意软件

如果将一个文件策略与一个或多个访问控制规则相关联，系统可以在匹配的流量中检测文件（包括恶意软件）。使用“分析”>“连接”菜单选项可查看与这些规则记录的连接关联的文件事件（如有）。 Cisco Secure Firewall Management Center 不显示文件列表，而是在**文件 (Files)** 列中显示视图文件 ()。“查看文件”上的数字表示连接中检测到或阻止的文件数量（包括恶意软件文件）。

并非所有文件和恶意软件事件都与连接有关。具体包括：

- 面向终端的AMP检测到的恶意软件事件（“基于终端的恶意软件事件”）与连接不相关。这些事件是从面向终端的 AMP 导入。
- 许多启用 IMAP 的邮件客户端使用单个 IMAP 会话，仅当用户退出应用时才结束。尽管长期运行的连接是由系统进行记录，但是在会话结束之前，会话中下载的文件不会与连接关联。

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。

开始之前

您必须是管理员或安全分析师用户才能执行此任务。

过程

步骤 1 转到**分析 > 连接**并选择相关选项。

步骤 2 使用连接事件表时，点击**查看文件 (View Files)**。
系统会显示弹出窗口，其中显示连接中检测到的文件列表及其类型和恶意软件处置情况（如适用）。

步骤 3 有以下选项可供选择：

- 查看 - 要查看文件事件表视图，请点击**文件的查看 (Malware File’s View)**。
- 查看 - 要查看恶意软件事件表视图的详细信息，请点击**恶意软件的查看 (Malware File’s View)**。
- 跟踪 - 要跟踪通过您的网络传输的文件，请点击**文件的轨迹 (File’s Trajectory)**。
- 查看 - 要查看连接的所有检测到的文件或面向网络的 AMP 检测到的恶意软件事件（“基于网络的恶意软件事件”），请点击**查看文件事件**或**查看恶意软件事件**。

相关主题

概述：工作流程
配置事件视图设置

查看与连接关联的入侵事件

如果您将入侵策略与访问控制规则或默认操作相关联，系统可以检测匹配流量中的漏洞。使用“分析”>“连接”菜单选项可查看与已记录连接相关联的入侵事件（如有），及其优先级和影响。

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。

开始之前

您必须是管理员或安全分析师用户才能执行此任务。

过程

步骤 1 转到**分析 > 连接**并选择相关选项。

步骤 2 使用连接事件表时，点击**入侵事件 (Intrusion Events)** 列中的**入侵事件 (Intrusion Events)** 。

步骤 3 在显示的弹出窗口中，您有以下选择：

- 点击 **所列事件的视图 (Listed Event’s View)** 以查看数据包视图中的详细信息。
- 点击**查看入侵事件 (View Intrusion Events)**，查看与连接关联的所有入侵事件的详细信息。

相关主题

概述：工作流程
配置事件视图设置

已加密连接的证书详细信息

可以使用“分析”>“连接”菜单下的选项来显示用于加密系统处理的连接的公钥证书（如有）。该证书包含以下信息。

表 *2:* 已加密连接的证书详细信息

属性	说明
使用者/颁发者公用名 (Subject/Issuer Common Name)	证书使用者或证书颁发者的主机名和域名。
使用者/颁发者组织 (Subject/Issuer Organization)	证书使用者或证书颁发者的组织。
使用者/颁发者组织单位 (Subject/Issuer Organization Unit)	证书使用者或证书颁发者的组织单位。
无效时间	证书有效日期。
序列号	由发行 CA 分配的序列号。

属性	说明
证书指纹	用于验证证书的 SHA 散列值。
公钥指纹	用于对证书内所含公钥进行身份验证的 SHA 哈希值。

相关主题

概述：工作流程

配置事件视图设置

查看连接摘要页面

“连接摘要”(Connection Summary) 页面仅对于满足以下条件的用户才可视：具有受连接事件搜索限制的自定义角色，已被授予对“连接摘要”(Connection Summary) 页面的基于菜单的显式访问权限。此页面提供按不同条件组织的受监控网络上的活动的图形。例如，“随时间推移的连接”(Connections over Time) 图形显示在选择的间隔内受监控网络上的连接总数。

如同连接图，您几乎可以在连接摘要图上执行完全一样的操作。然而，由于“连接摘要”(Connection Summary) 页面上的图形基于汇总数据，因此，您无法检查图形依赖的单个连接事件。换句话说，您无法从连接摘要图展开到连接数据表视图。

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**概述** > **摘要** > **连接摘要**。

步骤 2 从**选择设备 (Select Device)** 列表中，选择要查看其摘要的设备，或者选择**所有 (All)** 以查看所有设备的摘要。

步骤 3 要操纵和分析连接图，请如使用连接事件图形中所述继续操作。

提示
要将连接图分离，以便可以执行进一步分析而不影响默认时间范围，请点击**查看 (View)**。

相关主题

启用用户角色升级

连接和安全智能事件历史记录

功能	管理中心最低版本	威胁防御最低版本	详情
新建连接事件原因 - 象流。	7.1	任意	请参阅连接事件原因，第 20 页。
NAT 转换后的 IP 地址和端口	7.1	任意	连接和安全智能事件表中添加了四个新字段： • NAT 源 IP • NAT 目标 IP • NAT 源端口 • NAT 目标端口
能够在处理远程存储的某些事件时选择数据源	7.0	任意	请参阅工作流程历史记录。
DNS 过滤	7.0 6.7（测试版功能）	任意	启用 DNS 过滤时： • DNS 查询字段可能包含与 DNS 过滤匹配项关联的域。 • 如果 URL 字段为空，但 DNS 查询、URL 类别和 URL 信誉有值，则事件由 DNS 过滤功能生成，类别和信誉适用于 DNS 查询中指定的域。 • 另请参阅《Cisco Secure Firewall Management Center 设备配置指南》中的 *DNS* 过滤和事件。
删除对连接事件的自定义表的支持	6.6	任意	您无法再为连接事件创建自定义表。如果升级，则连接事件的任何预先存在的自定义表仍然可用，但始终不返回结果。 其他类型的自定义表没有变化。 新增/修改的屏幕： **分析 > 高级 > 自定义表**上的“表”选项 平台： 管理中心
删除和删除所有连接事件的功能	6.6	任意	删除和全部删除按钮已从连接事件表页面中删除。 要清除所有连接事件，请参阅 数据清除和存储。 新增/修改的屏幕： **分析 > 连接 > 事件** 平台： 管理中心

功能	管理中心最低版本	威胁防御最低版本	详情
VRF 和 SGT 的新字段	6.6	任意	• 入口虚拟路由器（系统日志：IngressVRF） • 出口虚拟路由器（系统日志：EgressVRF） • DestinationSecurityGroupType （仅限系统日志） • SourceSecurityGroupType （仅限系统日志）
新增和更改的安全组标记字段	6.5	任意	管理中心 Web 界面中的字段更改： • 更改的字段：安全组标记现在是源 SGT • 新字段：目标 SGT 对系统日志字段的更改： • 更改的字段： SecurityGroup 现在是 SourceSecurityGroupTag • 新字段： • SourceSecurityGroup • DestinationSecurityGroup • DestinationSecurityGroupTag 支持的平台： 管理中心、托管设备
新系统日志字段：事件优先级	6.5	任意	当连接事件与入侵、文件、恶意软件或安全智能事件相关联时，该字段将它们标识为高优先级。
系统日志中连接事件的唯一标识符	6.4.0.4	任意	以下系统日志字段共同唯一标识连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

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。