监控设备

系统包括控制面板和事件查看器，通过它们可监控设备和通过设备传递的流量。

启用日志记录以获取流量统计信息

使用监控控制面板和事件查看器，可以监控各种流量统计信息。但是，必须启用日志记录才能告诉系统要收集哪些统计信息。日志记录生成各种类型的事件，有助于深入了解通过系统的连接。

以下主题详细介绍事件及其提供的信息，并特别强调连接日志记录。

事件类型

系统可以生成以下类型的事件。只有生成这些事件，才能在监控控制面板中查看相关统计信息。

连接事件

您可以在用户生成通过系统传递的流量时生成连接事件。启用访问规则连接日志记录以生成这些事件。还可启用安全智能策略和 SSL 解密规则日志记录，以生成连接事件。

连接事件包括有关连接的各种信息，包括源和目标 IP 地址及端口、使用的 URL 和应用，以及传输的字节数或数据包数。另外，还包括执行的操作（例如，允许或阻止连接）和应用于连接的策略的信息。

入侵事件

系统检查网络上传输的数据包是否存在可能影响主机及其数据的可用性、完整性和机密性的恶意活动。如果系统识别出潜在的入侵，会生成入侵事件；入侵事件是有关攻击源和攻击目标的日期、时间、攻击程序类型以及情境信息的记录。无论调用访问控制规则的日志记录配置如何，系统均会生成设为阻止或提醒的入侵规则的入侵事件。

文件事件

文件事件表示系统基于文件策略在网络流量中检测到或者被阻止的文件。只有在应用文件策略的访问规则中启用文件日志记录，才能生成这些事件。

无论调用访问控制规则采用何种日志记录配置，在系统生成文件事件时，都会记录相关连接的终止。

恶意软件事件

作为整体访问控制配置的一部分，系统可在网络流量内检测恶意软件。恶意软件防护可以生成恶意软件事件，其中包含生成事件的处置，有关检测该恶意软件的方式、位置和时间的情境数据。只有在应用文件策略的访问规则中启用文件日志记录，才能生成这些事件。

文件的处置可能发生变化，例如，从安全变为恶意软件或从恶意软件变为安全。如果 恶意软件防护 向 Cisco Secure Malware Analytics 云 查询文件，且云决定在查询一周内更改处置，系统即会生成追溯性恶意软件事件。

安全智能事件

安全智能事件是由安全智能策略为该策略阻止或监控的每个连接生成的一种连接事件。所有安全智能事件都有一个由系统填充的“安全智能类别”字段。

对于各事件，都有一个相应的“常规”连接事件。由于评估安全智能策略后才会评估许多其他安全策略（包括访问控制），所以当安全智能阻止连接时，所生成事件不含系统从后续评估中收集的信息（如用户身份）。

可配置的连接日志记录

您应该根据您组织的安全和合规性需求记录连接。如果您的目标是限制所生成事件的数量和提高性能，则只能启用对分析至关重要的连接的日志记录。然而，如果出于分析目的，您想要广泛了解网络流量，则可启用其他连接的日志记录。

由于系统可能会因为多种原因记录连接，因此禁用某一处的日志记录不能确保匹配连接不会被记录。

可在以下位置配置连接日志记录。

- 访问控制规则和默认操作 - 连接结束时的日志记录可提供有关连接的大多数信息。另外，您还可以记录连接开始信息，但这些事件的信息不完整。连接日志记录默认处于禁用状态，因此必须针对所要跟踪的流量的每个规则（和默认操作）启用该日志记录。
- 安全智能策略 - 可启用日志记录，为已阻止的各连接生成安全智能连接事件。当系统由于安全智能过滤而记录连接事件时，它也会记录匹配的安全智能事件（这是一种您可以单独查看和分析的特殊类型连接事件）。
- SSL 解密规则和默认操作 - 可在连接结束时配置日志记录。对于受阻连接，系统会立即结束会话并生成事件。对于受监控连接以及您将其传递到访问控制规则的连接，系统会在会话结束时生成事件。

自动连接日志记录

系统自动保存以下连接结束事件，而不管其他日志记录配置如何。

- 除非通过访问控制策略的默认操作来处理连接，否则系统会自动记录与入侵事件关联的连接。您必须在默认操作上启用日志记录以获取匹配流量的入侵事件。
- 系统会自动记录与文件和恶意软件事件关联的连接。这仅适用于连接操作：您可以选择禁止生成文件和恶意软件事件。

连接日志记录的提示

在考虑日志记录配置和评估相关统计信息时，请记住以下提示：

- 当您通过访问控制规则允许流量时，可以使用关联的入侵或文件策略（或同时使用这两种策略），在流量到达其最终目标前进一步检测流量并阻止入侵、禁止文件和恶意软件。不过请注意，对于加密负载，文件和入侵检测已默认禁用。如果入侵或文件策略需要阻止连接，系统将立即记录连接结束事件，而不考虑连接日志设置。允许日志记录的连接提供有关网络流量的大多数统计信息。
- 受信任连接是由信任访问控制规则或访问控制策略中的默认操作所处理的连接。但是，不会检测受信任连接中是否存在发现数据、入侵、禁止文件和恶意软件。因此，受信任连接的连接事件包含的信息有限。
- 对于阻止流量的访问控制规则和访问控制策略默认操作，系统将记录连接开始事件。匹配流量会被拒绝，无需进一步检测。
- 在拒绝服务 (DoS) 攻击期间记录被阻止的 TCP 连接会影响系统性能并因多个相似事件使数据库不堪重负。在对“阻止”规则启用日志记录之前，请考虑该规则是否监控面向互联网的接口或其他易受 DoS 攻击的接口上的流量。
- 如果在配置远程访问 VPN 连接配置文件时选择**为已解密的流量 (sysopt permit-vpn) 绕过访问控制策略**选项，或以其他方式启用 **sysopt connection permit-vpn** 命令，则所有的站点间或远程访问 VPN 流量将绕过检测和访问控制策略。因此，您将不会收到有关此流量的任何连接事件，且此流量也不会反映在任何统计控制面板中。

将事件发送至外部系统日志服务器

除了通过 设备管理器（其事件存储容量有限）查看事件外，还可以选择配置规则和策略以将事件发送至外部系统日志服务器。然后，可使用所选系统日志服务器平台的功能和附加存储查看和分析事件数据。

要将事件发送至外部系统日志服务器，请编辑启用连接日志记录的各规则、默认操作或策略，并在日志设置中选择系统日志服务器对象。要将入侵事件发送到系统日志服务器，请在入侵策略设置中配置服务器。要将文件/恶意软件事件发送到系统日志服务器，请在**设备** > **系统设置** > **日志记录设置**中配置服务器。

有关更多信息，请参阅各规则和策略类型的帮助，另请参阅配置系统日志服务器。

使用思科基于云的服务（如 SecureX 威胁响应）评估事件

除了使用事件查看器和自身的系统日志服务器，还可以向思科基于云的服务器发送连接事件、高优先级入侵、文件和恶意软件事件。Cisco 基于云的服务，例如 SecureX 威胁响应 （前称 Cisco 威胁响应）可以从该云服务器提取事件，然后可以使用这些服务来评估这些事件。

这些基于云的服务独立于 威胁防御 和 设备管理器。如果选择使用要求将这些事件发送至 Cisco 云的服务，则必须在 **设备 (Device)** > **系统设置 (System Settings)** > **云服务 (Cloud Services)** 页面上启用该连接。请参阅将事件发送至思科云。

在美国地区通过 https://visibility.amp.cisco.com/，在欧盟地区通过https://visibility.eu.amp.cisco.com 可以连接至 SecureX 威胁响应 。您可以在 YouTube 上观看视频 (http://cs.co/CTRvideos)，了解此应用的使用方法和优点。有关 SecureX 威胁响应 与 威胁防御结合使用的更多信息，请参阅 https://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html处提供的 *Cisco Secure Firewall Threat Defense* 和 *SecureX* 威胁响应集成指南。

监控流量和系统控制面板

系统包括多个控制面板，它们可用来分析通过设备传递的流量和安全策略的结果。使用这些信息可评估您的配置的总体效率，识别和解决网络问题。

高可用性组中设备的控制面板仅显示该设备的统计信息。统计信息不会在设备之间同步。

注释 流量相关的控制面板中使用的数据基于访问控制规则进行收集，该规则实现连接或文件日志记录以及允许日志记录的其他安全策略。控制面板不会反映匹配未启用日志记录的规则的流量。请确保配置规则以记录对您重要的信息。另外，只有配置了身份规则来收集用户身份，才能获得用户信息。最后，只有拥有入侵、文件、恶意软件和URL类别功能的许可证，并配置了使用这些功能的规则，才能获得这些功能的相关信息。

过程

步骤 1 在主菜单中点击**监控 (Monitoring)**，打开“控制面板”(Dashboards) 页面。

您可以选择预定义的时间范围（例如前一小时或上周），也可以使用特定开始和结束时间自定义时间范围，以便控制控制面板图形和表格中所示的数据。

流量相关的控制面板包括以下显示类型：

- 前 5 个条形图 - 这些图形显示在**网络概况**控制面板中，以及点击控制面板表中的项目时看到的各项目的摘要控制面板中。您可以在**事务**数或**数据使用量**（收发的总字节数）之间切换信息。另外，还可以切换显示屏以显示所有事务、允许的事务或拒绝的事务。点击**查看更多**链接可查看与该图相关的表格。

- 表格 - 表格显示特定类型的项目（例如，应用或 URL 类别）及该项目的事务总数、允许的事务、阻止的事务、数据使用量和收发的字节数。您可以在原始**值**和**百分比**之间切换数字，并显示前 10、100 或 1000 个条目。如果项目是链接，点击该链接可查看摘要控制面板及更多详细信息。

步骤 2 点击目录中的**控制面板**链接，可查看以下数据的控制面板：

- **网络概况** - 显示有关网络流量的摘要信息，包括匹配的访问规则（策略）、发起流量的用户、连接中使用的应用、匹配的入侵威胁（签名）、所访问 URL 的 URL 类别和连接最常访问的目标。
- **用户** - 显示网络的热门用户。只有配置身份策略，才能查看用户信息。如果没有用户身份，则包含源 IP 地址。您可能会看到以下特殊实体：
  - **身份验证失败** - 系统提示用户进行身份验证，但用户未在允许的最大尝试次数内输入有效的用户名/密码对。身份验证失败本身不会阻止用户访问网络，但您可以写入访问规则来限制这些用户访问网络。
  - **访客** - “访客”用户与“身份验证失败”用户类似，只是您的身份规则配置为将这些用户称为“访客”。系统提示“访客”用户进行身份验证，但他们在最大尝试次数内未成功通过身份验证。
  - **无需身份验证** - 系统不提示用户进行身份验证，因为该类用户的连接与指定不进行身份验证的身份规则匹配。
  - **未知** - 没有用户的 IP 地址映射，也没有身份验证失败的记录。通常，这意味着尚无来自该地址的 HTTP 流量。
- **应用** - 显示网络中使用的热门应用，例如 Facebook。只有检测连接，才能获得这些信息。只有连接匹配“允许”规则或使用区域、地址和端口之外条件的“阻止”规则时，才会对它们进行检测。因此，在触发需要检测的任何规则之前，如果该连接受信任或被阻止，则无法获得应用信息。
- **Web 应用** - 显示网络中使用的热门 Web 应用，例如 Google。收集 Web 应用信息的条件与“应用”控制面板的条件相同。
- **URL 类别** - 基于所访问网站的分类，显示网络中使用的热门网站类别，例如博彩或教育机构。要获得这些信息，必须至少设置一条以URL类别为流量匹配条件的访问控制规则。对于匹配该规则的流量，或必须检测以确定是否匹配该规则的流量，可以获得此方面的相关信息。而对于匹配第一个 Web 类别访问控制规则之前规则的连接，则不会看到它们的类别（或信誉）信息。
- **访问和 SI 规则** - 显示热门访问规则和安全智能规则（与网络流量匹配的对应项目）。
- **区域** - 显示用于进出设备的流量的热门安全区对。
- **目的** - 显示网络流量排名靠前的目的。
- **攻击者** - 显示排名靠前的攻击者，即触发入侵事件的连接源。只有在访问规则中配置入侵策略，才能查看这些信息。

- **目标** - 显示入侵事件排名靠前的目标，即攻击的受害者。只有在访问规则中配置入侵策略，才能查看这些信息。
- **威胁** - 显示已触发的排名靠前的入侵规则。只有在访问规则中配置入侵策略，才能查看这些信息。
- **文件日志** - 显示网络流量中发现的排名靠前的文件类型。只有在访问规则中配置文件策略，才能查看这些信息。
- **恶意软件** - 显示热门恶意软件操作和处置组合。您可以详细了解相关文件类型的信息。只有在访问规则中配置文件策略，才能查看这些信息。
  - 可能的操作包括：恶意软件云查找、阻止、存档阻止（加密）、检测、自定义检测、云查找超时、恶意软件阻止、存档阻止（已超出深度）、自定义检测阻止、TID 阻止、存档阻止（检测失败）。
  - 可能的处置包括：恶意软件、未知、安全、自定义检测、不可用。
- **SSL 解密** - 显示通过设备的加密与纯文本流量的细分以及根据 SSL 解密规则解密加密流量方法的细分。
- **系统** - 显示整个系统视图，包括接口及其状态（将鼠标悬停在接口上，查看其 IP 地址）、总平均系统吞吐量（一小时内的时间以 5 分钟存储桶为单位，一小时以上的时间以一小时存储桶为单位）、有关系统事件以及 CPU、内存和磁盘的使用情况的摘要信息。您可以将吞吐量图形限制为显示特定接口（而非所有接口）的吞吐量。

  注释 “系统”控制面板所示的信息为整个系统的相关信息。如果登录到设备 CLI，您可以使用各种命令来查看更多详细信息。例如，**show cpu** 和 **show memory** 命令包括用于显示其他详细信息的参数，而这些控制面板显示来自 **show cpu system** 和 **show memory system** 命令的数据。

步骤 3 另外，您还可以点击目录中的这些链接：

- **事件** - 查看发生的事件。只有在各个访问规则中启用连接日志记录，才能查看与这些规则相关的连接事件。此外，在安全智能策略和 SSL 解密规则中启用日志记录，以查看安全智能事件和其他连接事件数据。这些事件可以帮助您解决用户的连接问题。
- **会话**- 查看和管理 设备管理器 用户会话。有关详细信息，请参阅管理 设备管理器 用户会话。

使用命令行监控更多统计信息

设备管理器 控制面板提供与通过设备的流量和一般系统使用情况相关的各种统计信息。但是，您可以使用 CLI 控制面板或登录设备 CLI 获取控制面板未涵盖方面的其他信息（请参阅登录命令行界面 (CLI)）。

CLI 包含各种 **show** 命令，可用来提供这些统计信息。您还可以使用 CLI 进行常规故障排除，包括 **ping** 和 **traceroute** 等命令。大多数 **show** 命令都与 **clear** 命令结合使用，用于将统计信息重置为 0。（无法从 CLI 控制台清除统计信息。）

您可以在思科 Firepower 威胁防御命令参考(http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html) 中查找有关这些命令的文档。

例如，您会发现以下较常用的命令。

- **show nat** 显示您的 NAT 规则的命中计数。
- **show xlate** 显示处于活动状态的实际 NAT 转换。
- **show conn** 提供当前通过设备的连接的相关信息。
- **show dhcpd** 提供您在接口上配置的 DHCP 服务器的相关信息。
- **show interface** 提供每个接口的使用统计信息。

查看事件

您可以查看启用日志记录的安全策略中生成的事件。另外，也可为触发的入侵策略和文件策略生成事件。

事件查看器表格可实时显示生成的事件。有新事件生成时，旧事件将退出表格。

开始之前

除了连接匹配相关策略外，是否会生成特定类型的事件还取决于以下事件：

- 连接事件 - 访问规则必须启用连接日志记录。此外还可以在安全智能策略和 SSL 解密规则中启用连接日志记录。
- 入侵事件 - 访问规则必须应用入侵策略。
- 文件和恶意软件事件 - 访问规则必须执行文件策略并启用文件日志记录。
- 安全智能事件 - 必须启用和配置安全智能策略，并启用日志记录。

过程

步骤 1 点击主菜单中的**监控**。

步骤 2 从目录中选择**事件**。

事件查看器将基于事件类型在选项卡中组织事件。有关详细信息，请参阅事件类型，第 1 页。

步骤 3 点击显示您要查看的事件类型的选项卡。

您可以对事件列表执行以下操作：

- 点击**暂停**以停止添加新事件，这样即可更加轻松地查找和分析事件。点击**继续**以允许显示新事件。
- 选择不同的刷新率（5 秒、10 秒、20 秒或 60 秒）以控制新事件的显示速度。
- 创建包含所需列的自定义视图。要创建自定义视图，请点击选项卡栏中的 + 按钮，或点击**添加/删除列**。无法更改预设的选项卡，所以添加或删除列将会创建新视图。有关详细信息，请参阅配置自定义视图，第 8 页。
- 要更改列的宽度，请点击列标题并将列标题分隔符拖动至所需的宽度。
- 将鼠标悬停在某个事件上方，点击**查看详细信息**可查看该事件的完整信息。有关事件中各个字段的描述，请参阅事件字段说明，第 10 页。

步骤 4 如果需要，对表格应用过滤器，以协助您基于各种事件属性找到所需的事件。

要创建新过滤器，请通过从下拉列表中选择原子元素，手动键入过滤器；也可以点击事件表格中包括要基于其过滤的值的单元格，构建一个过滤器。您可以点击同一列中的多个单元格，在这些值之间创建 OR 条件；也可以点击不同列的单元格，在列之间创建 AND 条件。如果通过点击单元格构建过滤器，还可以编辑生成的过滤器对其微调。有关创建过滤器规则的详细信息，请参阅过滤事件，第 9 页。

在构建过滤器后，执行以下任一操作：

- 要应用过滤器和更新表格以仅显示匹配过滤器的事件，请点击**过滤器**按钮。
- 要清除您应用的整个过滤器并使表返回未过滤状态，请点击**过滤器**框中的**重置过滤器**。
- 要清除过滤器中的某个原子元素，请将鼠标悬停在该元素上方，并点击该元素的 **X**。然后，点击**过滤器**按钮。

配置自定义视图

您可以创建自己的自定义视图，这样即可在查看事件时轻松地查看所需的列。另外，还可以编辑或删除自定义视图，但无法编辑或删除预定义的视图。

过程

步骤 1 依次选择**监控** > **事件**。

步骤 2 执行以下操作之一：

- 要基于现有自定义（或预定义）视图创建新视图，请点击该视图的选项卡，然后点击选项卡左侧的 + 按钮。
- 要编辑现有的自定义视图，请点击该视图的选项卡。

注释 要删除自定义视图，只需点击该视图选项卡中的 **X** 即可。删除无法撤消。

步骤 3 点击右侧事件表上方的**添加/删除列**链接，选择或取消选择列，直到选定列表中仅包含要包含在视图中的列为止。

点击列，并在可用（但未使用）列表和选定列表之间拖动它们。另外，您还可以点击和拖动选定列表中的列，以更改表格中从左至右的列顺序。有关列的描述，请参阅事件字段说明，第 10 页。

完成后，点击**确定**以保存列更改。

注释 如果在查看预定义视图时更改列选项，将会创建一个新视图。

步骤 4 如果需要，点击和拖动列分隔符可更改列宽。

过滤事件

您可以创建复杂过滤器，将事件表格限制为您当前感兴趣的事件。您可以单独或组合使用以下方法来构建过滤器：

点击列

要构建过滤器，最简单的方法就是点击事件表格中包含要基于其过滤的值的单元格。点击单元格会用为该值和字段组合正确设定的规则更新**过滤器**字段。但是，使用此方法要求现有的事件列表中包含所需的值。

不能基于所有列执行过滤。如果可基于某个单元格的内容过滤，将鼠标悬停在该单元格上方时，它将显示下划线。

选择原子元素

另外，您还可以构建过滤器，具体方法为：点击**过滤器**字段，从下拉列表中选择所需的原子元素，然后再键入匹配值。这些元素包括在事件表格中未作为列显示的事件字段。另外，还包括定义您键入的值和要显示的事件之间关系的操作符。而点击列总会生成“equals (=)”过滤器，在选择元素时，还可以对数值字段选择“大于 (>)”或“小于 (<)”。

无论采用何种方式在**过滤器**字段中添加元素，均可通过在该字段中键入信息来调整操作符或值。点击**过滤器**可将过滤器应用于表格。

事件过滤器的操作符

在事件过滤器中可以使用以下操作符：

=	等于。该事件与指定值匹配。不能使用通配符。
!=	不等于。该事件与指定值不匹配。要构建不等表达式，必须键入！（感叹号）。
>	大于。该事件包含大于指定值的值。此操作符仅可用于数值，例如端口和IP地址。
<	小于。该事件包含小于指定值的值。此操作符仅可用于数值。

复杂事件过滤器的规则

在构建包含多个原子元素的复杂过滤器时，请记住以下规则：

- 相同类型的元素在该类型的所有值之间具有 OR 关系。例如，“包括发起方 IP=10.100.10.10”和“发起方 IP=10.100.10.11”与包含其中任一地址作为流量源的事件匹配。
- 不同类型的元素之间为 AND 关系。例如，“包括发起方 IP=10.100.10.10”和“目标端口/ICMP 类型=80”与仅包含此源地址 AND 目标端口的事件匹配。不显示从 10.100.10.10 传至不同目标端口的事件。
- 数值元素（包括 IPv4 和 IPv6 地址）可以指定范围。例如，您可以指定“目标端口=50-80”，以捕获此范围内端口的所有流量。使用连字符分隔开始和结束编号。并不是所有数值字段均可使用范围，例如在源元素中无法指定 IP 地址范围。
- 不能使用通配符或正则表达式。

事件字段说明

事件可包含以下信息。在查看事件详细信息时可以看到这些信息。另外，您还可以向事件查看器表格中添加列，以显示您最感兴趣的信息。

下面是可用字段的完整列表。并不是每个字段都适用于每种事件类型。请记住，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。

操作

对于连接或安全智能事件，与记录连接的访问控制规则关联的操作或默认操作：

允许

明确允许的连接。

信任

受信任的连接。信任规则在第一个数据包上检测到的 TCP 连接仅生成连接结束事件。系统将在最终会话数据包发送完毕 1 小时后生成事件。

阻止

阻止的连接。在以下条件下，**阻止**操作可与“允许”访问规则相关联：

- 某个攻击程序漏洞被入侵策略阻止的连接。
- 某个文件被文件策略阻止的连接。
- 被安全智能阻止的连接。
- 被 SSL 策略阻止的连接。

默认操作

连接按默认操作处理。

对于文件或恶意文件事件，与文件所匹配规则的规则操作相关联的文件规则操作，以及任何关联的文件规则操作选项。

允许的连接

系统是否允许事件的流量通过。

应用

在连接中检测到的应用。

应用业务相关性

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。

应用类别、应用标记

展示了应用特征的条件标准，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。

阻止类型

在与事件中的流量匹配的访问控制规则中指定的与事件中的流量匹配的阻止类型：阻止或交互式阻止。

客户端应用、客户端版本

在连接中检测到的客户端应用及版本。

客户端业务相关性

与连接中检测到的客户端流量关联的业务相关性：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类客户端都有相关的业务相关性；该字段显示级别最低（最不相关）的业务相关性。

客户端类别、客户端标记

展示了应用特征的条件标准，协助您了解应用功能。

客户端风险

与连接中检测到的客户端流量关联的风险：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类客户端都有一个相关风险；该字段显示最高风险。

连接

内部产生的流量的唯一 ID。

连接阻止类型指示器

在与事件中的流量匹配的访问控制规则中指定的与事件中的流量匹配的阻止类型：阻止或交互式阻止。

连接字节数

连接的总字节数。

连接时间

连接开始的时间。

连接时间戳

检测到连接的时间。

拒绝的连接

系统是否已拒绝事件的流量通过。

目标国家/地区和大洲

接收主机所在的国家/地区和大洲。

目标 IP

入侵、文件或恶意软件事件中的接收主机使用的 IP 地址。

目标端口/ICMP 代码；目标端口；目标 Icode

会话响应方使用的端口或 ICMP 代码。

目标安全组标记、目标安全组标记名称

与目标关联的 TrustSec 安全组标记编号和名称（如有）。

方向

文件传输的方向。

处置

文件的处置：

恶意软件

表示 Cisco Secure Malware Analytics 云 将文件归类为恶意软件，或文件威胁评分超过文件策略定义的恶意软件阈值。本地恶意软件分析也可以将文件标记为恶意软件。

干净

表示 Cisco Secure Malware Analytics 云 将文件分类为干净，或用户将文件添加到干净列表。

未知

表示系统已查询 Cisco Secure Malware Analytics 云，但文件尚未被分配处置情况；换句话说， Cisco Secure Malware Analytics 云 尚未对文件进行分类。

自定义检测

表示用户将文件添加到自定义检测列表。

不可用

表示系统无法查询 Cisco Secure Malware Analytics 云。您可能看到很少一部分事件为此处置；这是预期行为。

不适用

表示“检测文件”或“阻止文件”规则处理了文件，系统未查询 Cisco Secure Malware Analytics 云。

传出接口、传出安全区

连接离开设备所通过的接口和区域。

出口虚拟路由器

目标接口所属的虚拟路由器（如有）名称。

事件、事件类型

事件的类型。

事件秒数、事件微秒数

检测到事件的时间（秒或微秒）。

文件类别

文件类型的一般类别，例如：Office 文档、存档、多媒体、可执行文件、PDF 文件、编码文件、图形或系统文件。

文件事件时间戳

文件或恶意软件文件的创建时间和日期。

文件名

文件名称。

文件规则操作

检测文件的文件策略规则的相关操作以及任何相关文件规则操作选项。

文件 SHA-256

文件的 SHA-256 散列值。

文件大小 (KB)

文件大小（千字节）。如果文件在完全接收前被系统阻止，文件大小可能为空。

文件类型

文件类型，例如 HTML 或 MSEXE。

文件/恶意软件策略

与事件生成相关的文件策略。

文件日志阻止类型指示器

在与事件中的流量匹配的文件规则中指定的与事件中的流量匹配的阻止类型：阻止或交互式阻止。

防火墙策略规则、防火墙规则

处理连接的访问控制规则或默认操作。

首个数据包

查看会话的第一个数据包的日期和时间。

HTTP 来源地址

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

发送的 HTTP 状态代码用于响应客户端通过连接的 HTTP 请求。

IDS 分类

生成事件的规则所属的分类。

传入接口、传入安全区

连接进入设备所通过的接口和区域。

入口虚拟路由器

源接口所属的虚拟路由器（如有）名称。

发起方字节、发起方数据包

会话发起方发送的总字节数或数据包总数。

发起方国家/地区和大洲

发起会话的主机所在的国家/地区和大洲。只有发起方的 IP 地址可路由，方可用。

发起方 IP

在连接或安全智能事件中发起会话的主机 IP 地址（以及主机名，如果已启用 DNS 解析）。

内联结果

系统是否丢弃或本可丢弃触发入侵事件的数据包（如果在内联模式下操作）。空白表示触发的规则未被设置为“丢弃并生成事件”

入侵策略

启用了生成事件的规则的入侵策略。

IPS 阻止类型指示器

与事件中的流量匹配的入侵规则的操作。

最后一个数据包

查看会话的最后一个数据包的日期和时间。

MPLS 标记

与触发此入侵事件的数据包相关的多协议标记交换标记。

恶意软件阻止类型指示器

在与事件中的流量匹配的文件规则中指定的与事件中的流量匹配的阻止类型：阻止或交互式阻止。

消息

对于入侵事件，事件的解释性文本。对于恶意软件或文件事件而言，与恶意软件事件相关的任何其他信息。

NAT 目标 IP

对于接受网络地址转换 (NAT) 的数据包，为转换后的目标 IP 地址。

NAT 目标端口

对于接受网络地址转换 (NAT) 的数据包，为转换后的目标端口。

NAT 源 IP

对于接受网络地址转换 (NAT) 的数据包，为转换后的源 IP 地址。

NAT 源端口

对于接受网络地址转换 (NAT) 的数据包，为转换后的源端口。

NetBIOS 域

会话中使用的 NetBIOS 域。

原始客户端国家/地区和大洲

发起会话的原始客户端所在的国家/地区和大洲。只有原始客户端的 IP 地址可路由，方可用。

原始客户端 IP

发起 HTTP 连接的客户端的原始 IP 地址。此地址由 X-Forwarded-For (XFF) 或 True-Client-IP HTTP 报头字段或其对应项目派生。

策略、策略版本

访问控制策略及其版本，包括与事件相关的访问（防火墙）规则。

优先级

由 思科 Talos 情报小组 (Talos) 确定的事件优先级：高、中或低。

协议

连接中使用的传输协议。

原因

各种情况下的连接记录原因如下表所述。否则该字段为空。

原因 (Reason)	说明
DNS 阻止	系统未经检查就根据域名和安全情报数据拒绝连接。“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情报数据拒绝连接，但您将系统配置为监控而不是拒绝连接。
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 **system support elephant-flow-detection** 命令调整字节和时间阈值，以在设备 CLI 中识别大象流。
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。
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。
入侵阻止	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。
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 地址和安全情报数据拒绝连接。“IP 阻止”原因始终与“阻止”操作匹配。
SSL 阻止	系统基于 SSL 检查配置阻止加密连接。“SSL 阻止”原因始终与“阻止”操作匹配。
URL 阻止	系统未经检查就根据 URL 和安全情报数据拒绝连接。“URL 阻止”原因始终与“阻止”操作匹配。

接收时间

事件生成的日期和时间。

引用的主机

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

响应方字节、响应方数据包

会话响应方发送的总字节数或数据包总数。

响应方国家/地区和大洲

响应会话的主机所在的国家/地区和大洲。只有响应方的 IP 地址可路由，方可用。

响应方 IP

连接或安全智能事件中的会话响应者主机 IP 地址（以及主机名，如果已启用 DNS 解析）。

SI 类别 ID（安全智能类别）

包含被阻止项的对象的名称，例如网络或 URL 对象名称，或智能源类别名称。

签名

文件/恶意软件事件的签名 ID。

源国家/地区和大洲

发送主机所在的国家/地区和大洲。只有源 IP 地址可路由，方可用。

源 IP

入侵、文件或恶意软件事件中的发送主机使用的 IP 地址。

源端口/ICMP 类型；源端口；源端口 Itype

会话发起方使用的端口或 ICMP 类型。

源安全组标记、源安全组标记名称

与源关联的 TrustSec 安全组标记编号和名称（如有）。

SSL 实际操作

系统应用于连接的实际操作。此操作可能与预期操作不同。例如，连接可能与应用解密的规则匹配，但出于某些原因不能被解密。

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。

操作	说明
不解密	表示系统未解密的连接。

SSL 证书指纹

用于验证证书的 SHA 散列值。

SSL 证书状态

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”。

SSL 加密套件

连接中使用的加密套件。

SSL 预期操作

连接匹配的 SSL 规则中指定的操作。

SSL 流标志

已加密连接的前十大调试级别标记。

SSL 流信息

在 SSL 握手期间客户端与服务器之间交换的 SSL/TLS 消息，例如 HELLO_REQUEST 和 CLIENT_HELLO。有关 TLS 连接中交换的消息的详细信息，请参阅 http://tools.ietf.org/html/rfc5246。

SSL 策略

应用于连接的 SSL 解密策略的名称。

SSL 规则

应用于连接的 SSL 解密规则的名称。

SSL 会话 ID

在 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 通知单 ID

在 SSL 握手期间发送的会话单信息的一个十六进制散列值。

SSL URL 类别

SSL 解密处理过程中确定的目标 Web 服务器的 URL 类别。

SSL 版本

连接中使用的 SSL/TLS 版本。

TCP 标志

在连接中检测到的 TCP 标记。

数据包总数

在连接中传输的数据包总数，即**发起方数据包** + **响应方数据包**。

URL、**URL 类别**、**URL 信誉**、**URL 信誉评分**

会话期间受控主机请求的 URL 以及 URL 类别、信誉和信誉评分（如有）。

对于 DNS 查找请求过滤，类别和信誉用于 DNS 查询字段中显示的 FQDN。URL 字段将为空，因为正在为 DNS 请求而不是 Web 请求执行类别/信誉查找。

如果系统识别或阻止 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 SSL 应用，URL 表示包含在证书中的通用名称。

用户

与发起方 IP 地址关联的用户。

VLAN

与触发事件的数据包相关的最内部的 VLAN ID。

Web 应用业务相关性

与连接中检测到的 Web 应用流量相关的业务相关性：“非常高”、“高”、“中”、“低”或“非常低”。连接中检测的各类网络应用都有相关的业务相关性；该字段显示级别最低（最不相关）的业务相关性。

Web 应用类别、**Web 应用标记**

展示了 Web 应用特征的条件标准，协助您了解 Web 应用功能。

Web 应用风险

与连接中检测到的 Web 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 Web 应用都有一个相关风险；该字段显示最高风险。

Web 应用

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。

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。