入侵事件

以下主题介绍如何处理入侵事件。

关于入侵事件

Firepower 系统可以帮助监控网络中可能影响主机及其数据的可用性、完整性和机密性的流量。通过将受管设备放在关键网段，可以检查流经网络的数据包是否包含恶意活动。系统通过使用多种机制查找攻击者开发的众多漏洞。

如果系统识别出潜在的入侵，会生成入侵事件（有时以传统术语称为“IPS 事件”）；入侵事件是有关攻击源和攻击目标的日期、时间、漏洞类型以及情境信息的记录。对于基于数据包的事件，还会记录触发事件的一个或多个数据包的副本。受管设备将其事件传输到Cisco Secure Firewall Management Center，在其中可以查看汇聚数据并更好地了解针对网络资产的攻击。

还可以将受管设备部署为内联式、交换式或路由式入侵系统，以便将设备配置为会丢弃或替换已知有害的数据包。

用于查看和评估入侵事件的工具

您可以使用以下工具复审入侵事件和评估其在网络环境与安全策略情境中是否重要所需的工具。

- 事件摘要页面，提供受管设备上当前活动的概览。

- 基于文本的报告和图表报告，可以针对所选的任何时间段生成此类报告；还可以自行设计报告并将其配置为按预定的时间间隔运行
- 事故处理工具，可用于收集与攻击相关的事件数据；还可以添加备注来帮助跟踪调查和响应
- 自动报警，可用于配置 SNMP、邮件和系统日志
- 可用于响应和处理特定入侵事件的自动关联策略
- 预定义和自定义工作流程，可用于向下钻取数据以识别要进一步调查的事件
- 用于管理和分析数据的外部工具。您可以使用系统日志或 eStreamer将数据发送到这些工具。有关详细信息，请参阅 使用外部工具的事件分析

此外，您还可以使用 **分析 > 高级 > 上下文交叉启动** 页面上的预定义资源等公开信息来了解有关恶意实体的详细信息。

要搜索特定消息字符串并检索生成事件的规则的文档，请参阅 https://www.snort.org/rule_docs/。

入侵事件的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

入侵事件的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 入侵管理员 (Intrusion Admin)

查看入侵事件

可以查看入侵事件来确定其是否会对网络安全构成威胁。

初始入侵事件视图因用于访问页面的工作流程而异。可以使用其中一个预定义工作流程（其中包括一个或更多向下展开页面、入侵事件表视图和一个终止数据包视图），或者也可以创建自己的工作流程。还可以查看基于自定义表的工作流程，该表可能包括入侵事件。

如果事件视图包含大量 IP 地址且已启用**解析 IP 地址 (Resolve IP Addresses)** 事件视图设置，事件视图可能显示得很慢。

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** > **入侵** > **事件**。

步骤 2 有以下选项可供选择：

- 调整时间范围 - 如更改时间窗口中所述，调整事件视图的时间范围。
- 更改工作流程 - 如果使用的是不包含入侵事件表视图的自定义工作流程，请点击工作流程标题旁边的（**切换工作流程**）**([switch workflow])** 以选择系统提供的任意工作流程。
- 限制 - 要将视图缩小至对分析非常重要的入侵事件，请参阅使用入侵事件工作流程，第 22 页。
- 删除事件 - 要从数据库删除事件，请点击**删除 (Delete)** 删除您正查看其数据包的事件，或点击**全部删除 (Delete All)** 删除您之前已选择其数据包的所有事件。
- 标记为“已审核” - 要将入侵事件标记为“已审核”，请参阅将入侵事件标记为“已审核”，第 17 页。
- 查看连接数据 - 要查看与入侵事件关联的连接数据，请参阅查看与入侵事件关联的连接数据，第 16 页。
- 查看内容 - 如入侵事件字段，第 4 页中所述，查看表中各列的内容。

相关主题

使用入侵事件数据包视图，第 25 页

关于入侵事件字段

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、漏洞类型以及情境信息的记录。对于基于数据包的事件，还会记录触发事件的一个或多个数据包的副本。

您可以在 Cisco Secure Firewall Management Center Web 界面中通过路径**分析** > **入侵** > **事件**来查看入侵事件数据，或者将某些字段中的数据作为系统日志消息发出以供外部工具使用。系统日志字段如下方列表所示；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。

搜索入侵事件时，请记住任何单独事件的可用信息视系统记录事件的方式、原因和时间而异。例如，只有加密流量上触发的入侵事件才包含 TLS/SSL 信息。

注释 在 Cisco Secure Firewall Management Center Web 界面中，入侵事件表视图内的一些字段默认被禁用。要在会话期间启用某个字段，请展开搜索限制条件，然后点击**已禁用列(Disabled Columns)**下的列名。

入侵事件字段

访问控制策略（系统日志：**ACPolicy**）

与启用了生成事件的入侵规则、预处理器规则或解码器规则的入侵策略相关联的访问控制策略。

访问控制规则 (系统日志： **AccessControlRuleName)**

调用生成事件的入侵策略的访问控制规则。`Default Action` 指示启用了规则的入侵政策未与特定访问控制规则相关联，而是配置为访问控制策略的默认操作。

如果存在以下情况，则此字段为空 （对于系统日志消息，则为省略）：

- 无关联规则/默认操作：如果入侵检测未关联访问控制规则或默认操作，例如，例如数据包已经过默认入侵策略检查的情况，系统才会决定应用哪条入侵检测规则。（此策略在访问控制策略的“高级”选项卡中指定。）
- 无关联的连接事件：如果对会话记录的连接事件已从数据库中清除，例如连接事件的周转高于入侵事件的情况。

应用协议（系统日志：**ApplicationProtocol**）

表示在触发入侵事件的流量中检测到的主机之间的通信的应用协议（如果可用）。

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

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

与在触发入侵事件的流量中检测到的应用相关联的风险：“非常高”(Very High)、“高”(High)、“中”(Medium)、“低”(Low) 或“非常低”(Very Low)。在连接中检测的各种类型的应用都有相关的风险；此字段显示当中的最高风险。

业务相关性

与在触发入侵事件的流量中检测到的应用相关联的业务关联性：“非常高”(Very High)、“高”(High)、“中”(Medium)、“低”(Low) 或“非常低”(Very Low)。连接中检测的各类应用都有相关业务；此字段显示当中最低（相关性最小）的业务相关性。

分类 (系统日志：Classification)

生成事件的规则所属的分类。

请参阅 入侵事件详细信息中的可能分类值列表。

当搜索此字段时，请为生成要查看的事件的规则输入分类编号，或者全部或部分分类名称或说明。也可以输入编号、名称或描述的以逗号分隔列表。最后，如果添加自定义分类，还可以使用其完整或部分名称或描述进行搜索。

客户端（系统日志：Client）

客户端应用（如果有），代表在触发入侵事件的流量中检测到的受监控主机上运行的软件。

客户端类别和标记 (Client Category and Tag)

展示了应用特征的标准，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。

以下字段共同唯一地标识与特定入侵件事件相关的连接事件：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。

以下字段共同唯一地标识与特定入侵件事件相关的连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

计数

与每行中所显示的信息匹配的事件数。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。此字段不可搜索。

CVE ID

此字段仅为搜索字段。

按与 MITRE 常见漏洞和披露 (CVE) 数据库 (https://cve.mitre.org/) 中漏洞相关联的标识号进行搜索。

目的地所在的大洲

入侵事件中涉及的接收主机所在的大洲。

目的地国家/地区

入侵事件中涉及的接收主机所在的国家/地区。

目标主机重要性

生成事件时的目标主机重要性（相应主机的“主机重要性”属性的值）。

请记住，当主机的重要性发生变化时，此字段不会更新。但是，新事件将具有新的重要性值。

目标 IP（系统日志：DstIP）

入侵事件中涉及的接收主机使用的 IP 地址。

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。

目标端口/ICMP 代码（系统日志：DstPort、ICMPCode）

接收流量的主机的端口号。对于 ICMP 流量，在没有端口号的情况下，此字段显示 ICMP 代码。

目标用户

与连接事件的响应方 IP 关联的用户名。此主机可能是也可能不是接收漏洞攻击的主机。此值通常仅为您的网络中的用户所知。

。

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。

设备

已部署访问控制策略的受管设备。

DeviceUUID （仅限系统日志）

生成事件的 Firepower 设备的唯一标识符。

以下字段共同唯一地标识与特定入侵件事件相关的连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

域

检测到入侵的设备的域。 仅当曾经配置 Cisco Secure Firewall Management Center以实现多租户时，此字段才存在。

出口接口（系统日志：EgressInterface）

触发事件的数据包的出口接口。对于被动接口，不填充此接口列。

出口安全区域（系统日志：EgressZone）

触发事件的数据包的出口安全区域。在被动部署中不填充此安全区域字段。

出口虚拟路由器

在使用虚拟路由的网络中，用于流量离开网络的虚拟路由器的名称。

电子邮件附件

提取自“MIME 内容性质”报头的 MIME 附件文件名。要显示附件文件名，必须启用 SMTP 预处理器的**记录 MIME 附件名称 (Log MIME Attachment Names)** 选项。支持多个附件文件名。

邮件报头

此字段仅为搜索字段。

提取自邮件报头的数据。

要将邮件报头与 SMTP 流量的入侵事件相关联，必须启用 SMTP 预处理器 **Log Headers** 选项。

邮件收件人 (Email Recipient)

提取自 SMTP RCPT TO 命令的邮件收件人的地址。要显示此字段的值，必须启用 SMTP 预处理器的**记录收件人地址 (Log To Addresses)** 选项。支持多个收件人地址。

邮件发件人 (Email Sender)

提取自 SMTP MAIL FROM 命令的邮件发件人的地址。要显示此字段的值，必须启用 SMTP 预处理器的**记录发件人地址 (Log From Addresses)** 选项。支持多个发件人地址。

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。

以下字段共同唯一地标识与特定入侵件事件相关的连接事件：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。

发电机

生成事件的组件。

另请参阅有关以下入侵事件字段的信息：GID、消息和 Snort ID。

GID（仅限系统日志）

生成器 ID；生成事件的组件 ID。

另请参阅有关以下入侵事件字段的信息：生成器、消息和 Snort ID。

HTTP 主机名 (HTTP Hostname)

提取自 HTTP 请求主机报头的主机名（如果有）。请注意，请求数据包并非总是包含主机名。

要将主机名与 HTTP 客户端流量的入侵事件相关联，必须启用 HTTP 检查预处理器 **Log Hostname** 选项。

在表视图中，此列显示提取的主机名的前50个字符。将光标悬停在缩写主机名的显示部分上可显示完整名称（最多包含 256 个字节）。还可以在数据包视图中显示完整主机名（最多包含 256 个字节）。

HTTP 响应代码（系统日志：HTTPResponse）

在对客户端的 HTTP 请求的响应中通过触发事件的连接发送的 HTTP 状态代码。

HTTP URI

与触发入侵事件的 HTTP 请求数据包相关的原始 URI（如果有）。请注意，请求数据包并非总是包含 URI。

要将 URI 与 HTTP 客户端流量的入侵事件相关联，必须启用 HTTP 检查预处理器 **Log URI** 选项。

要查看与 HTTP 响应触发的入侵事件相关的 HTTP URI，应配置 **Perform Stream Reassembly on Both Ports** 选项中的 HTTP 服务器端口；但请注意，这样会增加流量重组的资源需求。

此列显示提取的 URI 的前五十个字符。将光标悬停在缩写 URI 的显示部分上可显示完整 URI（最多包含 2048 个字节）。还可以在数据包视图中显示完整 URI（最多包含 2048 个字节）。

影响

此字段中的影响级别指示入侵数据、网络发现数据和漏洞信息之间的相关性。

当搜索此字段时，请勿指定影响图标颜色或部分字符串。例如，请勿使用 **blue**、**level 1** 或 **0**。不区分大小写的有效值为：

- 影响 0，影响级别 0
- 影响 1，影响级别 1
- 影响 2，影响级别 2
- 影响 3，影响级别 3
- 影响 4，影响级别 4

对于从 NetFlow 数据添加到网络映射的主机，没有任何操作系统信息可用，因此，系统无法为涉及这些主机的入侵事件分配“易受攻击”（影响级别 1：红色）影响级别。在此情况下，请使用主机输入功能手动设置主机的操作系统身份。

入口接口（系统日志：IngressInterface）

触发事件的数据包的入口接口。对于被动接口，仅填充此接口列。

入口安全区域（系统日志：IngressZone）

触发事件的数据包的入口安全区域或隧道区域。在被动部署中仅填充此安全区域字段。

入口虚拟路由器

在使用虚拟路由的网络中，用于流量进入网络的虚拟路由器的名称。

内联结果（系统日志：InlineResult）

在工作流程和表视图中，此字段显示以下其中一项：

表 *1:* 工作流程和表视图中的内联结果字段内容

此图标	表明
	系统已丢弃触发规则的数据包。
	如果已启用入侵策略选项 **内联时丢弃** （在内联部署中），或在系统进行修建时“丢弃并生成”规则生成了该事件，那么 IPS 应该已丢弃该数据包。
	IPS 可能已将数据包传输或传送到目的地，但包含此数据包的连接现在已被阻止。
无图标（空）	触发的规则未设置为“丢弃并生成事件”

下表列出了内联结果的可能原因 - 已丢弃和部分丢弃。

内联结果	原因	详细原因
会丢弃	被动或分流模式下的接口	您已将接口配置为内联分流或被动模式。
	“检测”检测模式下的入侵策略	您已将入侵策略中的检测模式设置为检测。
	连接超时	由于 TCP/IP 连接超时，Snort 检测引擎已暂停检测。
部分丢弃	已关闭连接 (0x01)	在创建新流时，如果分配的流数超过允许的流数，Snort 检测引擎会删除最近最少使用的流。
	已关闭连接 (0x02)	当重新加载 Snort 检测引擎导致内存调整时，引擎会删除最近最少使用的数据流。
	连接已关闭 (0x04)	当 Snort 检测引擎正常关闭时，引擎会清除所有活动数据流。

无论入侵策略的规则状态或内联丢弃行为如何（包括当内联接口处于分流模式的情况），系统在被动部署中都不会丢弃数据包。

当搜索此字段时，请输入以下任一项：

- **已丢弃** 用于指定在内联部署中是否丢弃数据包。
- **会丢弃** 用于指定当入侵策略设置为在内联部署中丢弃数据包时是否已丢弃数据包。
- **部分丢弃** 用于指定数据包是否已传输或传送到目的地，但包含此数据包的连接现在已被阻止。

入侵策略 （系统日志： **IntrusionPolicy**）

启用了生成事件的入侵规则、预处理器规则或解码器规则的入侵策略。可以选择入侵策略作为访问控制策略的默认操作，也可以将入侵策略与访问控制规则相关联。

IOC（系统日志：**NumIOC**）

触发入侵事件的流量是否也触发了危害表现 (IOC)。

当搜索此字段时，请指定 **`triggered`** 或 **`n/a`**。

消息（系统日志：**Message**）

事件的说明文本。对于基于规则的入侵事件，事件消息提取自规则。对于基于解码器和预处理器的事件，事件消息采用硬编码。

生成器和 Snort ID（GID 和 SID）与 SID 版本（修订版本）以冒号分隔的数字格式括于括号中（GID:SID:版本）附于其后。例如，**`(1:36330:2)`**。

MITRE ATT&CK

您可以点击以显示战术和技术的完整列表的模式计数。

MPLS 标签（系统日志：**MPLS_Label**）

与触发入侵事件的数据包相关联的多协议标签交换标签。

网络分析策略（系统日志：**NAPPolicy**）

与事件生成相关联的网络分析策略（如果有）。

此字段显示提取的 URI 的前五十个字符。将光标悬停在缩写 URI 的显示部分上可显示完整 URI（最多包含 2048 个字节）。还可以在数据包视图中显示完整 URI（最多包含 2048 个字节）。

原始客户端 **IP**

提取自 X-Forwarded-For (XFF)、True-Client-IP 或自定义的 HTTP 报头的原始客户端 IP 地址。

要显示此字段的值，必须在网络分析策略中启用 HTTP 预处理器的**提取原始客户端 IP 地址 (Extract Original Client IP Address)** 选项。或者，在网络分析策略的同一区域，还可以指定最多六个自定义客户端 IP 报头，并设置系统选择“原始客户端 IP 事件”(Original Client IP event) 字段值的优先顺序。

优先级（系统日志：**Priority**）

事件优先级由Talos 情报小组 确定。优先级对应于 `priority` 关键字的值或 `classtype` 关键字的值。对于其他入侵事件，优先级由解码器或预处理器决定。有效值为“高”(high)、“中”(medium) 和“低”(low)。

协议（系统日志：**Protocol**）

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

连接中使用的传输协议的名称或编号，如 http://www.iana.org/assignments/protocol-numbers 中所列。这是与源端口和目标端口/ICMP 列相关的协议。

审核者 (Reviewed By)

审核事件的用户的名称。当搜索此字段时，可以输入 **unreviewed** 以搜索尚未审核的事件。

修订版本（仅限系统日志）

用于生成事件的签名的版本。

另请参阅有关以下入侵事件字段的信息：生成器、GID、消息、SID 和 Snort ID。

规则组

非 MITRE 规则组的计数，您可以点击该计数以调出模式，其中显示规则组的完整列表。

安全情景（系统日志：Context）

识别流量通过的虚拟防火墙组的元数据。系统仅对多情景模式下的 ASA FirePOWER 填充此字段。

SID（仅限系统日志）

生成事件的规则的签名 ID（亦称 Snort ID）。

另请参阅有关以下入侵事件字段的信息：生成器、GID、消息、修订版本和 Snort ID。

Snort ID

此字段仅为搜索字段。

（对于系统日志字段，请参阅 SID。）

在执行搜索时：指定生成事件的规则的 Snort ID (SID)，或者指定规则的生成器 ID (GID) 和 SID 组合，其中 GID 和 SID 使用冒号 (:) 隔开，格式为 GID:SID。可指定下表中的任何值：

表 *2: Snort ID* 搜索值

值	示例
单个 SID	10000
SID 范围	10000-11000
大于某个 SID	>10000
大于或等于某个 SID	>=10000
小于某个 SID	<10000
小于或等于某个 SID	<=10000
以逗号分隔的 SID 值列表	10000,11000,12000

值	示例
单个 GID:SID 组合	1:10000
以逗号分隔的 GID:SID 组合列表	1:10000,1:11000,1:12000
以逗号分隔的 SID 和 GID:SID 组合列表	10000,1:11000,12000

您查看的事件的SID在“消息”(Message)列中列出。有关详细信息，请参阅此部分中有关“消息”字段的说明。

源大洲

入侵事件中涉及的发送主机所在的大洲。

源国家/地区

入侵事件中涉及的发送主机所在的国家/地区。

源主机重要性

生成事件时的源主机重要性（相应主机的“主机重要性”属性的值）。

请记住，当主机的重要性发生变化时，此字段不会更新。但是，新事件将具有新的重要性值。

源 IP（系统日志：SrcIP）

入侵事件中涉及的发送主机使用的 IP 地址。

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。

源端口/ICMP 类型（系统日志：SrcPort、ICMPType）

发送主机上的端口号。对于 ICMP 流量，在没有端口号的情况下，此字段显示 ICMP 类型。

源用户（系统日志：User）

与发起连接的主机（可能是也可能不是漏洞攻击的源主机）的IP地址相关联的用户名。此用户值通常只有您的网络上的用户知道。

如果适用，用户名前面会附加 <区域>\。

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。

系统应用于已加密流量的操作：

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。

字段值显示在搜索工作流程页面上的 **SSL 状态 (SSL Status)** 字段中。

SSL 证书信息

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 失败原因 (SSL Failure Reason)

此字段仅为搜索字段。

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)
- 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 (SSL Status)** 字段中。

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。

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 (SSL Actual Action)**（无法解密的流量操作）以及 **SSL 失败原因 (SSL Failure Reason)**。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)`。

点击 **锁图标** 可查看证书详细信息。

当搜索该字段时，请输入一个或多个 **SSL 实际操作 (SSL Actual Action)** 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。

时间

事件的日期和时间。此字段不可搜索。

VLAN ID（系统日志：VLAN_ID）

与触发入侵事件的数据包相关的最内部的 VLAN ID。

Web 应用（系统日志：WebApplication）

Web 应用，代表在触发入侵事件流量中检测到的 HTTP 流量的内容或请求的 URL。

如果系统检测到 HTTP 应用协议，但无法检测特定 Web 应用，则系统会另行提供通用 Web 浏览名称。

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

展示了应用特征的标准，以帮助您了解应用功能。

相关主题

事件搜索

入侵事件影响级别

为了帮助评估事件对网络的影响，Cisco Secure Firewall Management Center在入侵事件的表视图中显示影响级别。对于每一个事件，系统都会添加影响级别图标，其颜色表示入侵数据、网络发现数据和漏洞信息之间的相关性。

注释 对于从 NetFlow 数据添加到网络映射的主机，没有任何操作系统信息可用，因此，系统无法为涉及这些主机的入侵事件分配“易受攻击”（影响级别 1：红色）影响级别。在此情况下，请使用主机输入功能手动设置主机的操作系统身份。

下表介绍了影响级别的可能值。

表 *3:* 影响级别

影响级别 (Impact Level)	漏洞	颜色	说明
未知 （0）	未知	灰色	源主机和目标主机都不在由网络发现监控的网络上。
易受攻击 （1）	较弱	红色	可以为以下任意一项： • 源主机或目标主机在网络映射中，并且漏洞已映射到主机 • 源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。
可能易受攻击 （2）	可能易受攻击	橙色	源主机或目标主机在网络映射中，并且下列情况之一属实： • 对于面向端口的流量，端口正在运行服务器应用协议 • 对于非面向端口的流量，主机使用此协议
当前不易受攻击 （3）	当前不易受攻击	黄色	源主机或目标主机在网络映射中，并且下列情况之一属实： • 对于面向端口的流量（例如 TCP 或 UDP），端口不处于打开状态 • 对于非面向端口的流量（例如 ICMP），主机不使用此协议
未知目标 （4）	未知目标	蓝色	源主机或目标主机在受监控网络上，但网络映射中没有该主机的条目。

查看与入侵事件关联的连接数据

系统可以记录在其中检测到入侵事件的连接。虽然会对与访问控制规则关联的入侵策略自动执行这种记录，但必须手动启用连接记录才能查看与默认操作关联的连接数据。

在事件的表视图之间导航时，查看相关数据最有用。

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** > **入侵** > **事件**。

步骤 2 使用表中的复选框选择入侵事件，然后从**跳转至**下拉列表中选择**连接**。

提示 可以使用类似方法查看与特定连接相关的入侵事件。有关详细信息，请参阅工作流程间导航。

相关主题

允许连接的日志记录
使用入侵事件工作流程，第 22 页
使用连接和 安全情报 事件表

将入侵事件标记为“已审核”

如果确信入侵事件不是恶意的，可以将其标记为“已审核”。

如果检查了某个入侵事件并确信其不对网络安全构成威胁（例如，因为您知道网络中的所有主机均不易受检测到的漏洞攻击），那么可以将事件标记为“已审核”。已审核事件存储在数据库中并包括在事件摘要统计信息中，但不再显示在默认入侵事件页面中。您的姓名会作为审核者显示。

在多域部署中，如果将事件标记为“已审核”，则系统会在可以查看该事件的所有域中将其标记为“已审核”。

如果执行备份然后删除已审核的入侵事件，恢复备份会恢复已删除的入侵事件，但不能恢复其“已审核”状态。应在**入侵事件 (Intrusion Events)** 下，而不是在**已审核事件 (Reviewed Events)** 下查看这些恢复的入侵事件。

过程

在显示入侵事件的页面上，您有两个选择：

- 要标记事件列表中的一个或多个入侵事件，请选择事件旁边的复选框并点击**审核 (Review)**。
- 要标记事件列表中的所有入侵事件，请点击 **Review All**。

相关主题

使用入侵事件工作流程，第 22 页

查看之前已审核的入侵事件

在多域部署中，如果将事件标记为“已审核”，则系统会在可以查看该事件的所有域中将其标记为“已审核”。

过程

步骤 1 选择**分析** > **入侵** > **已审核事件**。

步骤 2 有以下选项可供选择：

- 调整时间范围，如更改时间窗口中所述。
- 如果使用的是不包含入侵事件表视图的自定义工作流程，请点击工作流程标题旁边的（**切换工作流程**）**([switch workflow])** 以选择系统提供的任意预定义工作流程。
- 要了解有关显示的事件的详细信息，请参阅入侵事件字段，第 4 页。

相关主题

使用入侵事件工作流程，第 22 页

将已审核的入侵事件标记为“未审核”

可以将已审核的事件返回到默认入侵事件视图，方法是将该事件标记为“未审核”。

在多域部署中，如果将事件标记为“已审核”，则系统会在可以查看该事件的所有域中将其标记为“已审核”。

过程

在显示已审核事件的页面上，您有两个选择：

- 要删除已审核事件列表中的单个入侵事件，请选中特定事件旁边的复选框并点击**取消审核 (Unreview)**。
- 要从已审核事件列表移除所有入侵事件，请点击 **Unreview All**。

预处理器事件

预处理器提供两项功能：对数据包执行指定操作（例如解码和规范化 HTTP 流量）；一旦数据包触发某个预处理器选项且相关预处理器规则处于启用状态，就会通过生成事件来报告指定预处理器选项的执行情况。例如，您可以用 HTTP 检查生成器 (GID) 119 和 Snort ID (SID) 2 来启用 `Double Encoding` HIIP 检查选项及相关的预处理器规则，以在预处理器遇到 IIS 双编码流量时生成事件。

生成事件来报告预处理器的执行情况有助于检测异常协议漏洞攻击。例如，攻击者可以制造重叠的 IP 片段来对主机进行 DoS 攻击。IP 分片重组预处理器可以检测此类攻击并为之生成入侵事件。

预处理器事件与规则事件的不同之处在于，数据包显示不包含对事件的详细规则说明。相反，数据包显示的是事件消息、GID、SID、数据包报头数据和数据包负载。这让您可以分析数据包的报头信息，确定数据包的报头选项是否正在使用以及它们是否会令系统出现漏洞，并检查数据包负载。预处理器分析每个数据包后，规则引擎对其执行适当的规则（如果预处理器能够整理数据包并将其作为有效会话的一部分），进一步分析潜在内容级别的威胁并提供相关报告。

预处理器生成器 ID

每个预处理器都有自己的生成器 ID（即 GID），用以指明数据包触发的是哪个预处理器。某些预处理器还具有相关 SID，这是用于对潜在攻击进行分类的 ID 编号。这有助于通过对事件类型进行分类来更有效地分析事件，就像规则的 Snort ID (SID) 可以提供数据包触发规则的情景一样。可以在入侵策略“规则”页面的“预处理器”筛选组中按预处理器列出预处理器规则；还可以在“类别”筛选组的预处理器和数据包解码器子组中列出预处理器规则。

注释 由标准文本规则生成的事件的生成器 ID 为 1（全局域或旧式 GID）或 1000-2000（子代域）。对于共享对象规则，事件的生成器 ID 为 3。对于二者，事件的 SID 指明触发的是哪条具体规则。

下表介绍了生成每个 GID 的事件的类型。

表 *4:* 生成器 *ID*

ID	组件	说明
1	标准文本规则	该事件是在数据包触发标准文本规则（全局域或旧式 GID）时生成的。
2	标记的数据包	事件由标记生成器生成（标记生成器会根据带标记会话生成数据包）。使用 `tag` 规则选项时会出现这种情况。
3	共享对象规则	在数据包共享对象规则时生成事件。
102	HTTP 解码器	解码器引擎解码数据包中的 HTTP 数据。
105	Back Orifice 检测器	Back Orifice 检测器识别与数据包关联的 Back Orifice 攻击。
106	RPC 解码器	RPC 解码器解码数据包。
116	数据包解码器	事件由数据包解码器生成。
119、120	HTTP 检查预处理器	事件由 HTTP 检查预处理器生成。GID 120 规则与服务器特定 HTTP 流量相关。
122	端口扫描检测器	事件由端口扫描流量检测器生成。

ID	组件	说明
123	IP 分片重组器	分片的IP数据报不能正确重组时生成事件。
124	SMTP 解码器	SMTP 预处理器检测到针对 SMTP 谓词的漏洞时生成事件。
125	FTP 解码器	FTP/Telnet 解码器检测到 FTP 流量中有漏洞时生成事件。
126	Telnet 解码器	FTP/Telnet 解码器检测到 Telnet 流量中有漏洞时生成事件。
128	SSH 预处理器	SSH 预处理器检测到SSH流量中的漏洞时生成事件。
129	流预处理器	在数据流预处理器对数据流进行预处理期间生成事件。
131	DNS 预处理器	事件由 DNS 预处理器生成。
133	DCE/RPC 预处理器	事件由 DCE/RPC 预处理器生成。
134	规则延迟 数据包延迟	规则延迟暂停 (134:1) 或重新启用 (134:2) 一组入侵规则时，或者由于超出数据包延迟阈值而使系统停止检查数据包 (134:3) 时，生成事件。
135	基于速率的攻击检测器	基于速率的攻击检测器识别到网络上的主机存在过多连接时生成事件。
137	SSL 预处理器	事件由 TLS/SSL 预处理器生成。
138、139	敏感数据预处理器	事件由敏感数据预处理器生成。
140	SIP 预处理器	事件由 SIP 预处理器生成。
141	IMAP 预处理器	事件由 IMAP 预处理器生成。
142	POP 预处理器	事件由 POP 预处理器生成。
143	GTP 预处理器	事件由 GTP 预处理器生成。
144 个	Modbus 预处理器	事件由 Modbus SCADA 预处理器生成。
145	DNP3 预处理器	事件由 DNP3 SCADA 预处理器生成。
148	CIP 预处理器	事件由 CIP SCADA 预处理器生成。

ID	组件	说明
149	S7Commplus 预处理器	事件由 S7Commplus SCADA 预处理器生成。
1000 - 2000	标准文本规则	在数据包触发标准文本规则（子代域）时生成事件。

入侵事件工作流程页面

如果监控的流量违反策略，当前入侵策略中启用的预处理器规则、解码器规则和入侵规则就会生成入侵事件。

Firepower 系统提供使用事件数据填充的一组预定义工作流程，可用于查看和分析入侵事件。这些工作流程中，每个都会引导您浏览一系列页面，从而帮助您确定要评估的入侵事件。

预定义的入侵事件工作流程包含三种不同类型的页面（又称为事件视图）：

- 一个或多个向下钻取页面
- 入侵事件的表视图
- 数据包视图

向下钻取页面通常在一个表中包含两列或更多列（对于某些向下钻取视图，有多个表），通过其可查看一种特定类型的信息。

“向下钻取”以查找有关一个或多个目标端口的详细信息时，将会自动选择这些事件，然后显示工作流程中的下一页。这样，向下展开表就能够帮助减少一次分析的事件数。

入侵事件的初始表视图在其各自的行中列出每个入侵事件。表中的各列列出各种信息，例如时间、源 IP 地址、源端口、目标 IP 地址、目标端口、事件优先级和事件消息，等等。

在表视图中选择事件时，可以先不选择事件并显示工作流程中的下一页，而是为事件添加限制条件。限制条件是对要分析的事件类型施加的限制。

例如，如果点击任何列中的 **关闭**（×） 并从下拉列表清除 **时间** ，可以将“时间”作为一列移除。要减少分析中事件列表的事件数，可以点击表视图任一行中某个值的链接。例如，要将分析范围缩小为从其中一个源 IP 地址（假设是潜在攻击者）生成的事件，请点击**源 IP 地址 (Source IP Address)** 列中的 IP 地址。

如果选择表中的一行或多行，然后点击**视图 (View)**，将会显示数据包视图。数据包视图提供有关触发生成事件的规则或预处理器的数据包的信息。数据包视图的每个部分都包含有关数据包中特定层的信息。您可以展开折叠的部分以了解详细信息。

注释 由于每个端口扫描事件均由多个数据包触发，因此端口扫描事件会使用特殊版本的数据包视图。

如果预定义工作流程无法满足您的特定需求，则您可以创建仅显示您感兴趣的信息的自定义工作流程。自定义入侵事件工作流程可以包含向下钻取页面和/或事件表视图；系统自动将数据包视图包含作为最后一页。根据调查事件的需要，您可以轻松地在预定义工作流程和自定义工作流程之间切换。

使用入侵事件工作流程

事件的下钻式视图和表视图共享一些常见功能，这些功能可用于缩小事件列表，以便将分析焦点集中到一组相关事件上。

为了避免在不同的工作流程页面上显示相同的入侵事件，当您点击位于页面底部的链接显示另一页事件时，事件范围会暂停；当您在后续页面上点击以执行任何其他操作时，事件范围将会继续。

提示 在操作过程中，可以随时将限制条件保存为一组搜索条件。例如，如果您发现几天内您的网络被来自某个 IP 地址的攻击者探测，您可以在调查期间保存限制条件，以供日后再次使用。但是，不能将复合限制条件保存为一组搜索条件。

过程

步骤 1 使用**分析** > **入侵** > **事件**访问入侵事件工作流程。

步骤 2 或者，限制事件视图中显示的入侵事件数，如入侵事件向下钻取页面限制，第 23 页或入侵事件表视图限制，第 24 页中所述。

步骤 3 有以下选项可供选择：

- 要了解有关显示的列的详细信息，请参阅入侵事件字段，第 4 页。
- 要查看主机的配置文件，请点击显示在主机 IP 地址旁边的 **主机配置文件** 。
- 要查看地理位置详细信息，请点击“源国家/地区”或“目标国家/地区”列中显示的旗帜。
- 要查看 Firepower 系统外部可用源中的数据，请右键单击事件值。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
- 要收集有关事件的一般情报，请右键单击表中的事件值，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。
- 要修改所显示事件的时间和日期范围，请参阅更改时间窗口。

  提示 如果入侵事件未显示在事件视图中，调整指定的时间范围可能会返回结果。建议不要指定旧的时间范围，因为旧时间范围内的事件可能已被删除。调整规则阈值配置可能生成事件。

  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段（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。

- 要在当前工作流程页面排序事件或在当前工作流程页面内导航，请参阅使用工作流程。
- 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。
- 要从事件数据库中删除事件，选中要删除的事件旁边的复选框，然后点击**删除 (Delete)** 或点击**全部删除 (Delete All)**。
- 要将事件标记为“已审核”以将其从入侵事件页面上移除，但不将其从事件数据库中移除，请参阅将入侵事件标记为“已审核”，第 17 页。
- 要下载触发每个所选事件的数据包的本地副本（libpcap 格式的数据包捕获文件），请选中由要下载的数据包触发的事件旁边的复选框，然后点击**下载数据包 (Download Packets)** 或点击**下载所有数据包 (Download All Packets)**。捕获的数据包以 libpcap 格式保存。多个常用的协议分析器均使用此格式。
- 要导航至其他事件视图以查看关联事件，请参阅工作流程间导航。
- 要暂时使用另一个工作流程，请点击**切换工作流 (switch workflow)**。
- 要为当前页面添加书签以便快速返回该页面，请点击**将此页面加入书签 (Bookmark This Page)**。
- 要查看“摘要”(Summary) 控制面板的“入侵事件”(Intrusion Events) 部分，请点击**控制面板 (Dashboards)**。
- 要导航至书签管理页面，请点击**查看书签 (View Bookmarks)**。
- 要根据当前视图中的数据生成报告，请参阅从事件视图创建报告模板。

相关主题

事件搜索
书签

入侵事件向下钻取页面限制

下表介绍如何使用向下钻取页面。

表 *5:* 限制向下钻取页面上的事件

所需的操作…	可执行的操作
向下展开到下一个工作流程页面，约束特定值	点击该值。 例如，在“目标端口”(Destination Port) 工作流程中，要将事件限制为目标端口为 80 端口的事件，请点击 **DST 端口/ICMP 代码 (DST Port/ICMP Code)** 列中的 **80/tcp**。屏幕上将会显示工作流程的下一页（“事件”[Events] 页面），其中仅包含 80/tcp 端口事件。

所需的操作…	可执行的操作
向下展开到下一个工作流程页面，约束选定事件	选择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)**。 例如，在“目标端口”(Destination Port) 工作流程中，要将事件限制为目标端口为 20/tcp 和 21/tcp 端口的事件，请选择这些端口对应行旁边的复选框，然后点击**查看 (View)**。屏幕上将会显示工作流程的下一页（“事件”[Events] 页面），其中仅包含 20/tcp 和 21/tcp 端口事件。 请注意，如果对多行施加限制，并且表具有多列（不包括“计数”[Count] 列），则会构建复合限制。复合限制可确保您限制中的事件数不会超过意欲包含的数量。例如，如果使用“事件和目标”(Event and Destination) 工作流程，在第一个向下钻取页面上选择的每一行都会创建一个复合限制条件。如果您选择的是目标 IP 地址为 10.10.10.100 的事件 1:100，同时也选择了目标 IP 地址为 192.168.10.100 的事件 1:200，则复合限制可确保您不会同时也选择事件类型为 1:100、目标 IP 地址为 192.168.10.100 的事件，或者事件类型为 1:200、目标 IP 地址为 10.10.10.100 的事件。
向下展开到下一个工作流程页面，保留当前限制	点击**查看全部 (View All)**。

入侵事件表视图限制

下表介绍如何使用表视图。

表 *6:* 限制事件表视图中的事件

所需的操作…	可执行的操作
将视图限制为仅显示具有单个属性的事件	点击该属性。 例如，要将视图限制为仅显示目标端口为 80 端口的事件，请点击 **DST 端口/ICMP 编码 (DST Port/ICMP Code)** 列中的 **80/tcp**。
从表中移除列	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**。 如果要隐藏或显示其他列，请选择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**以展开搜索限制条件，然后点击**禁用列**下的列名称。

所需的操作…	可执行的操作
查看与一个或多个事件相关的数据包	执行以下其中一种操作： • 点击要查看的数据包的事件旁边的向下 **箭头图标** 。 • 选择要查看的一个或多个数据包，然后点击页面底部的 **View**。 • 在页面底部，点击**查看全部**以查看与当前限制条件匹配的所有事件的数据包。

使用入侵事件数据包视图

数据包视图提供有关触发生成入侵事件的规则的数据包的信息。

提示 如果用于检测事件的设备的**传输数据包**选项已禁用，则 Cisco Secure Firewall Management Center 上的数据包视图不包含数据包信息。

数据包视图通过提供有关数据包触发的入侵事件的信息来指示捕获特定数据包的原因，这些信息包括事件的时间戳、消息、分类和优先级（如果事件由标准文本规则生成，则还包括生成事件的规则）。数据包视图还提供有关数据包的一般信息（例如大小）。

此外，数据包视图有一部分是介绍数据包中的每一层（数据链路层、网络层和传输层），还有一部分介绍组成数据包的字节。如果系统已解密数据包，可以查看解密的字节。可以展开折叠的部分以显示详细信息。

注释 由于每个端口扫描事件均由多个数据包触发，因此端口扫描事件会使用特殊版本的数据包视图。

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 在入侵事件的表视图中，选择要查看的数据包，如入侵事件表视图限制，第 24 页中所述。

步骤 2 或者，如果选择多个事件，可以使用页面底部的页码来浏览数据包视图中的数据包。

步骤 3 此时，您还有以下选择：

- 调整 - 要修改数据包视图中的日期和时间范围，请参阅更改时间窗口。
- 配置 - 要配置触发事件的入侵规则，请点击“操作”(Actions) 旁边的箭头，然后如在数据包视图中配置入侵规则，第 29 页中所述继续操作。

- 删除 - 要从数据库删除事件，请点击**删除 (Delete)** 以删除您正在查看其数据包的事件，或点击**全部删除 (Delete All)** 以删除您之前已选择其数据包的所有事件。
- 下载 - 要下载触发事件的数据包的本地副本（libpcap 格式的数据包捕获文件），请点击**下载数据包** 保存您正在查看的事件的已捕获数据包副本，或点击**下载所有数据包**保存您之前已选择其数据包的所有事件的已捕获数据包副本。捕获的数据包以 libpcap 格式保存。多个常用的协议分析器均使用此格式。

  注释 不能下载端口扫描数据包，因为单个端口扫描事件基于多个数据包；但端口扫描视图提供所有可用的数据包信息。要下载，必须至少有 15% 的可用磁盘空间。

- 标记为已审核 - 要将事件标记为“已审核”以从事件视图中将其移除，但不从事件数据库中移除，请点击**审核 (Review)** 以标记您正在查看其数据包的事件，或点击**全部审核 (Review All)** 以标记您之前已选择其数据包的所有事件。有关详细信息，请参阅将入侵事件标记为“已审核”，第 17 页。
- 查看其他信息 - 要展开或折叠页面部分，请点击该部分旁边的箭头。有关详细信息，请参阅事件信息字段，第 26 页、帧信息字段，第 32 页和数据链路层信息字段，第 33 页。
- 查看网络层信息 - 请参阅查看网络层信息，第 34 页。
- 查看数据包字节信息 - 请参阅查看数据包字节信息，第 39 页。
- 查看传输层信息 - 请参阅 查看传输层信息，第 36 页

相关主题

端口扫描检测

事件信息字段

在数据包视图上，可以查看有关“事件信息”部分数据包的信息。

事件

事件消息。对于基于规则的事件，这相当于规则消息。对于其他事件，这取决于解码器或预处理器。

事件 ID 以 (GID:SID:Rev) 格式附加到消息后面。GID 是生成事件的规则引擎、解码器或预处理器的生成器 ID。SID 是规则、解码器消息或预处理器消息的标识符。Rev 是规则的修订号。

时间戳

捕获数据包的时间，采用 UTC 时区。

分类

事件分类。对于基于规则的事件，这相当于规则分类。对于其他事件，这取决于解码器或预处理器。

优先级

事件优先级。对于基于规则的事件，这相当于 `priority` 关键字的值或 `classtype` 关键字的值。对于其他事件，这取决于解码器或预处理器。

入口安全区域

触发事件的数据包的入口安全区域。在被动部署中仅填充此安全区域字段。

出口安全区域

触发事件的数据包的出口安全区域。在被动部署中未填充此字段。

域

受管设备所属的域。 仅当曾经配置 Cisco Secure Firewall Management Center以实现多租户时，此字段才存在。

设备

已部署访问控制策略的受管设备。

安全情景

识别流量通过的虚拟防火墙组的元数据。请注意，系统仅对多情景模式下的 ASA FirePOWER 填充此字段。

入口接口

触发事件的数据包的入口接口。对于被动接口，仅填充此接口列。

出口接口

对于内联部署，指触发事件的数据包的出口接口。

源/目标 IP

触发事件的数据包源自的（源）主机 IP 地址或域名，或触发事件的流量的目标主机（目的地）。

源端口/ICMP 类型 (Source Port/ICMP Type)

触发事件的数据包的源端口。对于 ICMP 流量，在没有端口号的情况下，系统将显示 ICMP 类型。

目标端口/ICMP 代码 (Destination Port/ICMP Code)

接收流量的主机的端口号。对于 ICMP 流量，在没有端口号的情况下，系统将显示 ICMP 代码。

邮件报头

提取自邮件报头的数据。请注意，邮件报头不显示在入侵事件表视图中，但可以将邮件报头数据作为搜索条件。

要将邮件报头与 SMTP 流量的入侵事件相关联，必须启用 SMTP 预处理器的**记录报头 (Log Headers)** 选项。对于基于规则的事件，提取邮件数据时会显示此行。

HTTP 主机名 (HTTP Hostname)

提取自HTTP请求主机报头的主机名（如果有）。此行显示完整的主机名（最多包含256个字节）。如果完整主机名不再是单行，则可以将其展开。

要显示主机名，必须启用 HTTP 检查预处理器 **Log Hostname** 选项。

请注意，HTTP 请求数据包并非总是包含主机名。对于基于规则的事件，当数据包包含 HTTP 主机名或 HTTP URI 时，会显示此行。

HTTP URI

与触发入侵事件的HTTP请求数据包相关的原始URI（如果有）。此行显示完整URI（最多包含2048个字节）。如果完整 URL 不再是单行，则可以将其展开。

要显示 URI，必须启用 HTTP 检查预处理器 **Log URI** 选项。

请注意，HTTP 请求数据包并非总是包含 URI。对于基于规则的事件，当数据包包含 HTTP 主机名或 HTTP URI 时，会显示此行。

要查看与HTTP响应触发的入侵事件相关的HTTP URI，应配置 **Perform Stream Reassembly on Both Ports** 选项中的 HTTP 服务器端口；但请注意，这样会增加流量重组的资源需求。

入侵策略

启用了生成入侵事件的入侵规则、预处理器规则或解码器规则的入侵策略。可以选择入侵策略作为访问控制策略的默认操作，也可以将入侵策略与访问控制规则相关联。

访问控制策略

包含入侵策略（启用了生成事件的入侵规则、预处理器规则或解码器规则）的访问控制策略。

访问控制规则

与生成事件的入侵规则关联的访问控制规则。默认操作指示启用了规则的入侵策略未与访问控制规则关联，而是配置为访问控制策略的默认操作。

规则

对于标准文本规则事件，是指生成事件的规则。

请注意，如果事件基于共享对象规则、解码器或预处理器，则规则不可用。

由于规则数据可能包含有关网络的敏感信息，管理员可以使用用户角色编辑器中的 View Local Rules 权限来设置用户查看数据包视图中的规则信息的权限。

操作

对于标准文本和自定义规则事件，展开**操作**以对触发事件的规则执行以下任何操作：

- 编辑规则
- 查看规则修订文档；仅对于标准文本规则，在“操作”下点击**查看文档**后，您可以点击文档弹出窗口中的**规则文档**以查看更具体的规则详情。

- 向规则添加注释
- 更改规则的状态
- 设置规则的阈值
- 抑制规则

请注意，如果事件基于共享对象规则、解码器或预处理器，则规则不可用。

在数据包视图中配置入侵规则

在入侵事件的数据包视图中，可以对触发事件的规则执行几项操作。请注意，如果事件基于共享对象规则、解码器或预处理器，则规则不可用。

过程

步骤 1 在入侵规则生成的入侵事件的数据包视图中，展开“事件信息”(Event Information) 部分的**操作 (Actions)**。

步骤 2 有以下选项可供选择：

- 注释 - 对于标准文本规则事件，点击**规则注释 (Rule Comment)** 可以向生成事件的规则添加文本注释。这样做可以提供有关规则以及其识别出的漏洞或策略违规的额外上下文和信息。还可以在入侵规则编辑器中添加和查看规则注释。
- 禁用 - 要禁用此规则，请点击以下选项之一：
  - **在当前 Snort 2 策略 (<policy_name>) 中禁用此规则**
  - **在所有本地创建的 Snort 2 策略中禁用此规则**

  如果此事件由标准文本规则生成，必要时可以禁用此规则。可以在能够在本地编辑的所有策略中设置此规则。或者，如果您能够在本地编辑当前策略，可以仅在当前策略（即，生成事件的策略）中设置此规则。

  请注意，仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑系统提供的默认策略。

  注释 不能从数据包视图禁用共享对象规则，也不能禁用默认策略中的规则。

- 丢弃数据包并生成事件 - 要将规则设置为丢弃触发该规则的数据包并生成事件，请点击以下选项之一：
  - **设置此规则可丢弃触发数据包并在当前 Snort 2 策略 (<policy_name>) 中生成事件**
  - **设置此规则可丢弃触发数据包并在所有本地创建的 Snort 2 内联策略中生成事件**

  如果受管设备在网络中以内联方式部署，可以在能够在本地编辑的所有策略中将触发事件的规则设置为丢弃触发该规则的数据包。或者，如果您能够在本地编辑当前策略，可以仅在当前策略（即，生成事件的策略）中设置此规则。

请注意，仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑系统提供的默认策略。请注意，仅在当前策略中启用了 **Drop when Inline** 的情况下，才会显示此选项。

- 编辑 - 对于标准文本规则事件，点击 **编辑** （以编辑 Snort 2 规则）或 **编辑 Snort 3 规则** 可修改生成事件的规则。如果事件基于共享对象规则、解码器或预处理器，则规则不可用。

  注释 如果编辑由系统提供的规则（而不是自定义的标准文本规则），则实际上会创建新的本地规则。请确保将本地规则设置为生成事件，并禁用当前入侵策略中的原始规则。但请注意，不能启用默认策略中的本地规则。

- 生成事件 - 点击 **设置此规则以在所有本地创建的 Snort 2 策略中生成事件** 可将规则设置为生成事件。

  如果此事件由标准文本规则生成，则可以将规则设置为在可本地编辑的所有策略中生成事件。

  请注意，仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑系统提供的默认策略。

  注释 不能将共享对象规则设置为从数据包视图生成事件，也不能禁用默认策略中的规则。

- 设置抑制选项 - 展开**设置抑制选项 (Set Suppression Options)**，然后如在数据包视图中设置抑制选项 ，第 31 页中所述继续操作。

  可以使用此选项以在能够在本地编辑的所有策略中抑制触发此事件的规则。或者，如果能够在本地编辑当前策略，可以仅在当前策略（即，生成事件的策略）中抑制此规则。

  请注意，仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑思科提供的默认策略。

- 设置阈值选项 - 展开**设置抑制选项 (Set Thresholding Options)**，然后如在数据包视图中设置阈值选项 ，第 30 页中所述继续操作。

  可以使用此选项在能够在本地编辑的所有策略中为触发此事件的规则创建阈值。或者，如果能够在本地编辑当前策略，可以仅为当前策略（即，生成事件的策略）创建阈值。

  请注意，仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑系统提供的默认入侵策略。

- 查看文档 - 点击**查看文档**可了解有关生成事件的规则的详细信息。或者，然后点击**规则文档**来查看更具体的规则详细信息。

在数据包视图中设置阈值选项

通过在入侵事件的数据包视图中设置阈值选项，可以控制每个规则随时间推移生成的事件数。可以在能够在本地编辑的所有策略中设置阈值选项；或者，如果能够在本地编辑策略，可以仅在当前策略（即，导致事件生成的策略）中设置阈值选项。

过程

步骤 1 在入侵规则生成的入侵事件的数据包视图中，展开“事件信息”(Event Information) 部分的**操作 (Actions)**。

步骤 2 展开**设置阈值选项 (Set Thresholding Options)**，并在两个选项中选择一个：

- **在当前 Snort 2 策略 (<policy_name>)**
- **在所有本地创建的 Snort 2 策略中**

步骤 3 选择要设置的阈值的类型：

- 点击**限制 (limit)** 以将通知限制为每个时间段内仅为指定数目的事件实例提供通知。
- 点击**阈值 (threshold)** 为每个时间段内每发生指定数目的事件实例提供通知。
- 点击**两者 (both)** 则在每个时间段内事件实例数达到指定数量后提供一次通知。

步骤 4 点击相应的阈值，以指明是要按**源 (Source)** 或**目标 (Destination)** IP 地址跟踪事件实例。

步骤 5 在**计数 (Count)** 字段中，输入要用作阈值的事件实例数。

步骤 6 在**秒 (Seconds)** 字段中，输入一个 1 和 86400 之间的数字来指定跟踪事件实例的时间段。

步骤 7 如果要覆盖现有入侵策略中的规则的所有当前阈值，请选中**覆盖此规则的任何现有设置 (Override any existing settings for this rule)** 复选框。

步骤 8 点击 **Save Thresholding**。

在数据包视图中设置抑制选项

可以使用抑制选项抑制全部入侵事件，或者基于源或目标 IP 地址抑制入侵事件。可在能够在本地编辑的所有策略中设置抑制选项。或者，如果能够在本地编辑当前策略，可以仅在当前策略（即，生成事件的策略）中设置抑制选项。

过程

步骤 1 在入侵规则生成的入侵事件的数据包视图中，展开“事件信息”(Event Information) 部分的**操作 (Actions)**。

步骤 2 展开**设置抑制选项 (Set Suppression Options)**，并在两个可能的选项中选择一个：

- **在当前 Snort 2 策略 (<policy_name>)**
- **在所有本地创建的 Snort 2 策略中**

注释 仅在能够编辑当前策略的情况下，当前策略选项才会显示；例如，可以编辑自定义策略，但是，不能编辑思科提供的默认策略。

步骤 3 选择以下其中一个**跟踪方式 (Track By)** 选项：

- 点击**源 (Source)** 可抑制由指定源 IP 地址发出的数据包生成的事件。
- 点击**目标 (Destination)** 可抑制由发往指定目标 IP 地址的数据包生成的事件。
- 点击**规则 (Rule)** 可完全抑制触发此事件的规则的事件。

步骤 4 在 **IP address or CIDR block** 字段中，输入要指定为源或目标 IP 地址的 IP 地址或 CIDR 块/前缀长度。

步骤 5 点击 **Save Suppression**。

相关主题

Firepower 系统 IP 地址约定

帧信息字段

在数据包视图中，点击**帧 (Frame)** 旁边的箭头可查看捕获的帧的信息。数据包视图可以显示单个帧或多个帧。每个帧提供有关单个网络数据包的信息。您会看到多个帧，例如，对于已标记的数据包或重组的 TCP 数据流中的数据包。

帧 n (Frame n)

捕获的帧，其中，*n* 为 1（对于单帧数据包）或递增帧编号（对于多帧数据包）。帧中捕获的字节数将附加到帧编号后面。

到达时间 (Arrival Time)

捕获帧的日期和时间。

与捕获上一个帧的时间间隔 (Time delta from previous captured frame)

对于多帧数据包，表示自捕获上一个帧以来经过的时间。

与显示上一个帧的时间间隔 (Time delta from previous displayed frame)

对于多帧数据包，表示自显示上一个帧以来经过的时间。

自引用或第一个帧以来经过的时间 (Time since reference or first frame)

对于多帧数据包，表示自捕获第一个帧以来经过的时间。

帧编号 (Frame Number)

递增的帧编号。

帧长度 (Frame Length)

帧的长度，以字节为单位。

捕获长度 (Capture Length)

捕获的帧的长度，以字节为单位。

帧标记 (Frame is marked)

帧是否被标记（true 或 false）。

帧中的协议 (Protocols in frame)

帧中包括的协议。

相关主题

tag 关键字
TCP 数据流重组

数据链路层信息字段

在数据包视图中，点击数据链路层协议（例如，**以太网 II [Ethernet II]**）旁边的箭头可查看有关数据包的数据链路层信息，这些信息包括源主机和目标主机的 48 位介质访问控制 (MAC) 地址。它还可能根据硬件协议，显示有关数据包的其他信息。

注释 请注意，本示例介绍以太网链路层信息，也可能出现其他协议。

数据包视图反映数据链路层使用的协议。以下列表说明在数据包视图中可能会看到的以太网 II 或 IEEE 802.3 以太网数据包的信息。

目标

目标主机的 MAC 地址。

注释 以太网还可以使用组播地址和广播地址作为目标地址。

来源

源主机的 MAC 地址。

类型

对于以太网 II 数据包，代表在以太网帧中封装的数据包的类型，例如 IPv6 或 ARP 数据报。请注意，此项目仅对以太网 II 数据包显示。

长度

对于 IEEE 802.3 以太网数据包，代表数据包的总长度（以字节为单位，不包括校验和）。请注意，此项目仅对 IEEE 802.3 以太网数据包显示。

查看网络层信息

过程

在数据包视图中，点击网络层协议（例如，**互联网协议**）旁边的箭头可查看有关与数据包相关的网络层的更多详细信息。

注释 请注意，本示例介绍的是 IP 数据包；也可能出现其他协议。

IPv4 网络层信息字段

以下列表介绍在 IPv4 数据包中可能显示的协议特定信息。

版本

互联网协议的版本号。

报头长度 (Header Length)

报头（包括任何 IP 选项）中的字节数。不带选项的 IP 报头的长度为 20 字节。

差分服务字段 (Differentiated Services Field)

差分服务的值，用以指明发送主机如何支持显式堵塞通知 (ECN)：

- `0x0` - 不支持具有 ECN 功能的传输 (ECT)
- `0x1` 和 `0x2` - 支持 ECT
- `0x3` - 堵塞情况 (CE)

总长度 (Total Length)

IP 数据包的长度（以字节为单位，不包括 IP 报头在内）。

标识

唯一标识源主机发送的 IP 数据报的值。此值用于跟踪同一数据报的数据分片。

标志 (Flags)

控制 IP 分片的值，其中：

“最后一个分片”(Last Fragment) 标志的值指明是否有更多与数据报相关的分片。

- `0` - 没有更多与数据报相关的分片
- `1` - 有更多与数据报相关的分片

“不分片”(Don’t Fragment) 标志的值控制数据报是否可以分片：

- 0 - 数据报可以分片
- 1 - 数据报不可分片

分片偏移量 (Fragment Offset)

自数据报开始以来分片偏移量的值。

生存时间 (ttl) (Time to Live [ttl])

数据包在过期之前可以在路由器之间跳转的剩余跳数。

协议

封装在 IP 数据报中的传输协议；例如，ICMP、IGMP、TCP 或 UDP。

报头校验和 (Header Checksum)

指明 IP 校验和是否有效。如果校验和无效，表示数据报在传输期间可能已损坏或可能正被用于躲避入侵。

源/目标 (Source/Destination)

源（或目标）主机的 IP 地址或域名。

请注意，要显示域名，必须启用 IP 地址解析。

点击地址或域名查看上下文菜单，然后选择 **Whois** 可在主机上执行 whois 搜索，选择 **查看主机配置文件** 可查看主机信息，或选择可将地址添加到全局黑名单或白名单。

IPv6 网络层信息字段

以下列表介绍在 IPv6 数据包中可能显示的协议特定信息。

流量类别

IPv6 报头中的试验性 8 位字段，用于识别 IPv6 数据包类别或优先级，类似于 IPv4 提供的差分服务功能。未使用时，此字段设为零。

流标签

可选的 20 位 IPv6 十六进制值（从 1 到 FFFFF），用于识别特殊流（例如，非默认服务质量或实时服务）。未使用时，此字段设为零。

负载长度

表示 IPv6 负载中八位组数的 16 位字段，负载由 IPv6 报头后面的所有数据包组成，包括任何扩展报头。

下一报头

表示紧随 IPv6 报头之后的报头类型的 8 位字段，使用与 IPv4 协议字段相同的值。

跳数限制

一个 8 位十进制整数，其中用于转发数据包的每个节点每次减 1。如果递减的值达到零，则丢弃数据包。

来源

源主机的 128 位 IPv6 地址。

目标

目标主机的 128 位 IPv6 地址。

查看传输层信息

过程

步骤 1 在数据包视图中，点击传输层协议（例如，**TCP**、**UDP** 或 **ICMP**）旁边的箭头。

步骤 2 或者，点击**数据 (Data)**（如果显示）可在紧接其上方的数据包视图的“数据包信息”(Packet Information) 部分中查看协议负载的前二十四个字节。

步骤 3 查看 TCP、UDP 和 ICMP 协议的传输层内容，如TCP 数据包视图字段，第 36 页、UDP 数据包视图字段，第 37 页或ICMP 数据包视图字段，第 38 页中所述。

注释 请注意，这些示例讨论 TCP、UDP 和 ICMP 数据包；也可能出现其他协议。

TCP 数据包视图字段

本节介绍 TCP 数据包的特定于协议的信息。

源端口

用于识别发起应用协议的编号。

目标端口

用于识别接收应用协议的编号。

序列号

当前 TCP 分段中第一个字节的值，包含在 TCP 数据流中的初始序列号中。

下一个序列号

在响应数据包中，要发送的下一个数据包的序列号。

确认号

TCP 确认，包含在之前接受的数据的序列号中。

报头长度 (Header Length)

报头中的字节数。

标志

六位，表示 TCP 分段的传输状态：

- `U` - 紧急指针有效
- `A` - 确认号有效
- `P` - 接收方应推送数据
- `R` - 重置连接
- `S` - 同步序列号以开始新连接
- `F` - 发送方完成发送数据

窗口大小

接收主机将接受的未确认数据数量（以字节为单位）。

校验和

指明 TCP 校验和是否有效。如果校验和无效，表示数据报在传输期间可能已损坏或可能正被用于躲避入侵。

紧急指针

TCP 分段中发送紧急数据的位置（如果存在）。与 `U` 标记一起使用。

选项

TCP 选项的值（如果有）。

UDP 数据包视图字段

本节介绍 UDP 数据包的特定于协议的信息。

源端口

用于识别发起应用协议的编号。

目标端口

用于识别接收应用协议的编号。

长度

UDP 报头和数据的总长度。

校验和

指明 UDP 校验和是否有效。如果校验和无效，表示数据报在传输期间可能已损坏。

ICMP 数据包视图字段

本节介绍 ICMP 数据包的协议特定信息。

类型

ICMP 消息的类型：

- 0 - 回应应答
- 3 - 目的地不可达
- 4 - 源抑制
- 5 - 重定向
- 8 - 回应请求
- 9 - 路由器通告
- 10 - 路由器请求
- 11 - 超时
- 12 - 参数问题
- 13 - 时间戳请求
- 14 - 时间戳应答
- 15 - 信息请求（过时）
- 16 - 信息应答（过时）
- 17 - 地址掩码请求
- 18 - 地址掩码应答

代码

ICMP 消息类型随附的代码。ICMP 消息类型 3、5、11 和 12 都有一个相应的代码，如 RFC 792 中所述。

校验和 (Checksum)

指明 ICMP 校验和是否有效。如果校验和无效，表示数据报在传输期间可能已损坏。

查看数据包字节信息

过程

在数据包视图中，点击**数据包字节数 (Packet Bytes)** 旁边的箭头可查看构成数据包的字节的十六进制和 ASCII 版本。如果系统已解密流量，可以查看解密的数据包字节。

内部来源的入侵事件

来自内部源的入侵事件表示网络上的主机受到攻击。如果源 IP 地址在您的网络上，则表明您应该调查此主机。

查看入侵事件统计信息

Intrusion Event Statistics 页面提供设备当前状态和网络生成的所有入侵事件的简要摘要。

页面上显示的每个 IP 地址、端口、协议和事件消息等均为链接。点击任意链接可查看相关的事件信息。例如，如果前 10 大目标端口之一是 `80 (http)/tcp`，点击该链接会显示默认入侵事件工作流程的第一个页面，并列出以该端口为目标的事件。请注意，只会显示当前时间范围内的事件（以及生成事件的受管设备）。此外，标记为“已审核”的入侵事件会继续显示在统计信息中。例如，如果当前时间范围是过去一小时，但第一个事件是在五小时前生成的，当点击 **First Event** 链接时，打开的事件页面将不会显示事件，直至时间范围被更改。

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** > **入侵事件统计信息**。

步骤 2 从页面顶部的两个选择框选择要查看其统计信息的区域和设备，或者选择**所有安全区域 (All Security Zones)** 和**所有设备 (All Devices)** 以查看收集入侵事件的所有设备的统计信息。

步骤 3 点击 **Get Statistics**。

提示 要查看自定义时间范围内的数据，请点击页面右上角区域的链接并按照更改时间窗口中的指示操作。

主机统计信息

“入侵事件统计信息”(Intrusion Event Statistics) 页面的“主机统计信息”(Host Statistics) 部分提供有关设备本身的信息。在 Cisco Secure Firewall Management Center上，此部分还提供有关所有受管设备的信息。

这些信息包括以下内容：

时间

设备的当前时间。

正常运行时间

设备本身重新启动以来的天数、小时数和分钟数。在Cisco Secure Firewall Management Center上，Uptime 还显示每个受管设备上一次重新启动的时间、已登录用户数和平均负载。

磁盘使用情况

正使用的磁盘空间的百分比。

内存使用率

正使用的系统内存的百分比。

平均负载 (Load Average)

过去 1 分钟、5 分钟和 15 分钟内 CPU 队列的平均进程数。

事件概述

“入侵事件统计信息”(Intrusion Event Statistics) 页面的“事件概述”(Event Overview) 部分提供入侵事件数据库中信息的概述。

这些统计信息包括以下内容：

事件

入侵事件数据库中的事件数。

时间范围内的事件 (Events in Time Range)

当前选定的时间范围以及数据库中属于该时间范围的事件数量和所占百分比。

第一个事件 (First Event)

事件数据库中第一个事件的事件消息。

上一事件

事件数据库中最后一个事件的事件消息。

注释 如果在 Cisco Secure Firewall Management Center上查看入侵事件数据时选择受管设备，将会转而显示该设备的“事件概述”部分。

事件统计信息

“入侵事件统计信息”页面的“事件统计信息”部分提供有关入侵事件数据库中信息的更具体信息。

这些信息包括以下方面的详细信息：

- 前 10 大事件类型
- 前 10 大源 IP 地址
- 前 10 大目标 IP 地址
- 前 10 大目标端口
- 具有最大数量事件的协议、入口安全区域、出口安全区域和设备

注释 在多域部署中，系统会为每个枝叶域构建单独的网络映射。因此，枝叶域可以包含这样一个 IP 地址，该地址在它的网络内是唯一的，但与另一枝叶域中的 IP 地址完全相同。在祖先域中查看事件统计信息时，系统可以展示该重复 IP 地址的多个实例。初看上去，似乎是重复条目。但是，如果向下展开到每个 IP 地址的主机配置数据，则系统会显示它们属于不同的枝叶域。

查看入侵事件性能图表

在入侵事件性能页面上，可生成用于说明 Cisco Secure Firewall Management Center或受管设备的入侵事件在特定时间段内的性能统计信息的图表。可以生成图表来反映每秒入侵事件数、每秒兆位数、每个数据包的平均字节数、Snort 未检查的数据包百分比以及因 TCP 规范化而被阻止的数据包数量。这些图表可以显示过去一小时、前一天、上一周或上个月的运行统计信息。

注释 新数据将进行累计，统计信息图表每五分钟更新一次。因此，如果快速重新加载图表，直到下一次五分钟更新间隔之前数据可能不会更改。每个图表显示所选时间段（上个月、上周、前一天或前一小时）内所示时间间隔（每天、每小时或每五分钟）的平均 值。如果平均值小于 1，则以十进制形式显示值。

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** > **入侵事件性能**。

步骤 2 从**选择设备 (Select Device)** 列表中，选择要查看其数据的设备。

步骤 3 从**选择图表 (Select Graph[s])** 列表中，选择要创建的图表类型，如入侵事件性能统计信息图表类型，第 42 页中所述。

步骤 4 从**选择时间范围 (Select Time Range)** 列表中，选择要用于图表的时间范围。

步骤 5 点击 **Graph**。

步骤 6 要保存图表，请右键点击它并按照浏览器的指示保存图像。

入侵事件性能统计信息图表类型

下表列出了可用的图表类型。请注意，如果图表类型填充的数据受网络分析策略 **Inline Mode** 设置影响，则图表类型显示会有所不同。如果禁用**内联模式**，Web 界面上标有星号 (*) 的图表类型（在下方列中列出 `yes`）会使用有关流量的数据进行填充；如果启用**内联模式**，则系统会修改或丢弃数据。

表 *7:* 入侵事件性能图表类型

要为以下项生成数据：	您必须.....	代表含义.....	是否受“内联模式”**(Inline Mode)** 影响？
平均字节/数据包	n/a	每个数据包中包含的平均字节数。	否
在 TCP 流量/数据包中规范化的 ECN 标志	启用 **Explicit Congestion Notification** 并选择 **Packet**	无论是否协商，以数据包为单位，已为其清除 ECN 标记的数据包的数量。	是
在 TCP 流量/会话中规范化的 ECN 标记	启用 **Explicit Congestion Notification** 并选择 **Stream**	未协商使用 ECN 使用时，以数据流为单位，ECN 标记被清除的次数。	是
事件/秒	n/a	设备上每秒生成的事件数。	否
ICMPv4 回应规范化	启用 **Normalize ICMPv4**	回显（请求）或回显回复消息中 8 位 Code 字段被清除的 ICMPv4 数据包的数量。	是
ICMPv6 回应规范化	启用 **Normalize ICMPv6**	回显（请求）或回显回复消息中 8 位 Code 字段被清除的 ICMPv6 数据包的数量。	是
IPv4 DF 标记规范化	启用 **Normalize IPv4** 和 **Normalize Don’t Fragment Bit**	IPv4 Flags 报头字段的一位 Don’t Fragment 子字段被清除的 IPv4 数据包的数量。	是
IPv4 选项规范化	启用**规范化 IPv4 (Normalize IPv4)**	选项八位字节被设置为 1（“无操作”[No Operation]）的 IPv4 数据包的数量。	是

要为以下项生成数据：	您必须.....	代表含义.....	是否受“内联模式”(Inline Mode) 影响？
IPv4 保留标记规范化	启用 **Normalize IPv4** 和 **Normalize Reserved Bit**	IPv4 Flags 报头字段的一位 Reserved 子字段被清除的 IPv4 数据包的数量。	是
IPv4 调整大小规范化	启用 **Normalize IPv4**	已按照 IP 报头中指定数据报长度截断多余长度负载的 IPv4 数据包的数量。	是
IPv4 TOS 规范化	启用 **Normalize IPv4** 和 **Normalize TOS Bit**	单字节 Differentiated Services (DS) 字段（之前叫做 Type of Service (TOS) 字段）被清除的 IPv4 数据包的数量。	是
IPv4 TTL 规范化	启用**规范化 IPv4 (Normalize IPv4)**、**最大 TTL (Maximum TTL)** 和**重置 TTL (Reset TTL)**	IPv4 生存时间规范化的数量。	是
IPv6 选项规范化	启用 **Normalize IPv6**	Hop-by-Hop Options 或 Destination Options 扩展报头中 Option Type 字段设置为 00（跳过并继续处理）的 IPv6 数据包的数量。	是
IPv6 TTL 规范化	启用**规范化 IPv6 (Normalize IPv6)**、**最小 TTL (Minimum TTL)** 和**重置 TTL (Reset TTL)**	IPv6 跳数限制 (TTL) 规范化的数量。	是
兆位/秒	n/a	每秒通过设备的流量兆位数。	否
调整大小以适应 MSS 的数据包规范化	启用**调整数据以适应 MSS (Trim Data to MSS)**	负载长于“TCP 数据”(TCP Data) 字段，因而被调整至“最大分片大小”(Maximum Segment Size) 的数据包的数量。	是
调整大小以适应 TCP 窗口的数据包规范化	启用**调整数据以适应窗口 (Trim Data to Window)**	“TCP 数据”(TCP Data) 字段被调整以适应接收主机的 TCP 窗口的数据包的数量。	是

要为以下项生成数据：	您必须.....	代表含义.....	是否受“内联模式”**(Inline Mode)** 影响？
丢包率	n/a	所有选定设备上未经检查的数据包的平均百分比。例如，如果选择两个设备，那么平均百分比 50% 可能表示一个设备的丢包率为 90%，另一个的丢包率为 10%。也可能表示这两个设备的丢包率均为 50%。当选择一个设备时，此图表仅表示总丢包率。	否
数据条带化的 RST 数据包规范化	启用 **RST 时删除数据 (Remove Data on RST)**	数据被从 TCP 重置 (RST) 数据包移除的数据包的数量。	是
数据条带化的 SYN 数据包规范化	启用 **SYN 时删除数据 (Remove Data on SYN)**	当 TCP 操作系统不是 Mac OS 时数据被从 SYN 数据包移除的数据包的数量。	是
TCP 报头填充规范化	启用**规范化/清除选项填充字节 (Normalize/Clear Option Padding Bytes)**	选项填充字节设置为 0 的 TCP 数据包的数量。	是
无选项 TCP 规范化	启用**允许这些 TCP 选项 (Allow These TCP Options)** 并设置为 `any` 之外的任意选项	“时间戳”(Time Stamp) 选项条带化的数据包的数量。	是
TCP NS 标记规范化	启用**显式堵塞通知**并选择**数据包**	“ECN 随机数总和 (NS)”(ECN Nonce Sum [NS]) 选项规范化的数量。	是
TCP 选项规范化	启用**允许这些 TCP 选项 (Allow These TCP Options)** 并设置为 `any` 之外的任意选项	选项字段设置为“无操作（TCP 选项 1）”(No Operation [TCP Option 1]) 的选项的数量（MSS、“窗口比例”[Window Scale]、“时间戳”[Time Stamp] 以及明确允许的选项除外）。	是
TCP 数据包阻止条件规范化	启用**规范化 TCP 负载 (Normalize TCP Payload)**（分片重组必须失败）	因为 TCP 分段无法正确重组而被丢弃的数据包的数量。	是
TCP 保留标记规范化	启用**规范化/清除保留位 (Normalize/Clear Reserved Bits)**	“保留”(Reserved) 位被清除的 TCP 数据包的数量。	是

要为以下项生成数据：	您必须.....	代表含义.....	是否受“内联模式”**(Inline Mode)** 影响？
TCP 分段重组规范化	启用**规范化 TCP 负载 (Normalize TCP Payload)**（分片重组必须成功）	“TCP 数据”(TCP Data) 字段已规范化以确保重传数据一致性的数据包数量（无法正确重组的所有分段都被丢弃）。	是
TCP SYN 选项规范化	启用**允许这些 TCP 选项 (Allow These TCP Options)** 并设置为 `any` 之外的任意选项	由于未设置 SYN 控制位，“最大分片大小”(Maximum Segment Size) 或“窗口比例”(Window Scale) 选项被设置为“无操作（TCP 选项 1）”(No Operation [TCP Option 1]) 的选项的数量。	是
TCP 时间戳 ECR 规范化	启用**允许这些 TCP 选项 (Allow These TCP Options)** 并设置为 `any` 之外的任意选项	“时间戳回应答复 (TSecr)”(Time Stamp Echo Reply [TSecr]) 选项字段由于未设置确认 (ACK) 控制位而被清除的数据包的数量。	是
TCP 紧急指针规范化	启用 **Normalize Urgent Pointer**	双字节 TCP 报头 Urgent Pointer 字段大于负载长度，因而被设置成负载长度的数据包的数量。	是
被阻止的地址块总数	配置**内联模式 (Inline Mode)** 或**内联时丢弃 (Drop when Inline)**	丢弃的数据包总数，包括规则、解码器和预处理器丢弃。	否
总计注入的数据包	配置**内联模式 (Inline Mode)**	在重新传输前调整大小的数据包的数量。	否
总 TCP 过滤的数据包	配置“TCP 数据流预处理”(TCP Stream Preprocessing)	由于 TCP 端口过滤而被数据流跳过的数据包的数量。	否
总 UDP 过滤的数据包	配置“UDP 数据流预处理”(UDP Stream Preprocessing)	由于 UDP 端口过滤而被数据流跳过的数据包的数量。	否
紧急标记清除规范化	启用**如果未设置紧急指针则清除 URG (Clear URG if Urgent Pointer is Not Set)**	因为未设置紧急指针，TCP 报头 URG 控制位被清除的数据包的数量。	是

要为以下项生成数据：	您必须.....	代表含义.....	是否受“内联模式”**(Inline Mode)** 影响？
紧急指针和紧急标记清除规范化	启用**空负载时清除紧急指针/URG (Clear Urgent Pointer/URG on Empty Payload)**	TCP 报头“紧急指针”(Urgent Pointer) 字段和 URG 控制位由于没有负载而被清除的数据包的数量。	是
紧急指针清除规范化	启用 **Clear Urgent Pointer if URG=0**	16 位 TCP 报头 Urgent Pointer 字段由于未设置紧急 (URG) 控制位而被清除的数据包的数量。	是

相关主题

内联规范化预处理器
内联部署中预处理器流量的修改
内联部署中的丢弃行为

查看入侵事件图表

Firepower 系统提供显示入侵事件随时间推移变化趋势的图表。可为一个或所有受管设备生成时间变化范围为过去一小时至上个月的入侵事件图表。

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** > **入侵事件图表**。

步骤 2 在**选择设备 (Select Device)** 下，选择**全部 (all)** 以包括所有设备，或选择要包括在图表中的特定设备。

步骤 3 在**选择图表 (Select Graph[s])** 下，选择要生成的图表类型：

- 前 10 个目标端口
- 前 10 个源 IP 地址
- 前 10 个事件消息

步骤 4 在**选择时间范围 (Select Time Range)** 下，选择图表的时间范围：

- 过去一小时
- 最近一天
- 上周
- 上个月

步骤 5 点击 **Graph**。

入侵事件历史记录

特性	版本	详细信息
IPS 事件数据存储库替换	7.1	• 入侵事件、入侵事件剪贴板和默认自定义表（使用入侵事件列 - **具有源重要性的入侵事件** 和 **具有目标重要性的入侵事件**）已弃用。 您无法再使用 **复制** 和 **全部复制** 按钮将事件添加到剪贴板。 弃用的页面： • **分析 > 入侵 > 事故** • **分析 > 入侵 > 事故** • 主入侵事件表中添加了两个新字段 - **源主机重要性** 和 **目标主机重要性**。 支持的平台： Cisco Secure Firewall Management Center
系统日志中连接事件的唯一标识符	6.4.0.4	以下系统日志字段共同唯一标识连接事件并在入侵事件的系统日志中显示：DeviceUUID，第一个数据包时间，连接实例 ID 和连接计数器。
系统日志中现包括 IntrusionPolicy 字段	6.4	入侵事件系统日志现在指定触发事件的入侵策略。
新入侵事件搜索字段：CVE ID	6.4	您现在可以按 MITRE 的常见漏洞和风险标识号进行搜索 修改的屏幕： **分析 > 入侵 > 事件 > 编辑搜索** 支持的平台：所有。

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。