关联策略

以下主题介绍如何配置关联策略和规则。

- 关联策略和规则简介， 第 1 页
- 合规的要求和必备条件， 第 2 页
- 配置关联策略， 第 3 页
- 配置关联规则， 第 5 页
- 配置关联响应组， 第 35 页

关联策略和规则简介

您可以通过关联功能，使用关联策略实时应对网络威胁。

当网络活动触发某个活动的关联策略中的 关联规则 或 合规 *allow* 名单 时，会导致关联 策略违规 的发生。

关联规则

当活动的关联策略中的关联规则触发时，系统会生成关联事件。关联规则可在以下情况下触发：

- 系统生成特定类型的事件（连接、入侵、恶意软件、发现、用户活动等）。
- 网络流量偏离其正常的量变曲线。

可以通过下列方式限制关联规则：

- 添加主机配置文件限定条件以使用涉及触发事件的主机的主机配置文件中的信息限制该规则。
- 向关联规则中添加连接跟踪器，以便在满足规则的初始条件后，系统开始跟踪某些连接。然后，只有在跟踪的连接满足其他标准时，才可生成关联事件。
- 向关联规则中添加用户资格，以跟踪某些用户或用户群。例如，您可以限制关联规则，以便只有特定用户的流量或来自特定部门的流量才会触发该关联规则。
- 添加暂停周期。当关联规则触发后，暂停周期会导致该规则在指定时间间隔内不会再次触发。暂停周期过后，该规则可再次触发并开始新的暂停周期。

- 添加非活动周期在非活动周期，关联规则不会触发。

虽然您可以配置关联规则而不对您的部署授予许可，但使用未经许可组件的规则不会触发。

合规 允许 名单

合规 allow 名单指定允许在网络中的主机上运行的操作系统、应用（Web 和客户端）及协议。当主机违反用于活动关联策略使用的 an allow 名单时，系统生成 an *allow* 名单事件。

关联响应

对关联策略违规的响应包括简单的警报以及各种补救（例如扫描主机）。您可以将每个关联规则或allow名单与单个响应或一组响应相关联。

如果网络流量触发多个规则或allow名单，系统将发起与每个规则和allow名单相关的所有响应。

关联和多租户

在多域部署中，可以在任意域级别创建关联策略，只要使用的是该级别可用的规则、 allow 名单和响应。高层域管理员可以在域中或跨域执行关联：

- 按域限制关联规则将匹配该域的后代所报告的事件。
- 高层域管理员可以跨域创建评估主机的合规 allow 名单。您可以在同一个 allow 名单中以不同域中的不同子网作为目标。

注释 系统会为每个分叶域构建单独的网络映射。使用文字配置（例如 IP 地址、VLAN 标记和用户名）限制跨域关联规则可能会出现意外结果。

相关主题

合规 允许 名单简介
Cisco Secure Firewall Management Center 警报响应
补救简介

合规的要求和必备条件

型号支持

Any

支持的域

任意

用户角色

- 管理员

配置关联策略

使用关联规则、合规 allow 名单、警报响应和补救来构建关联策略。

在多域部署中，可以在任何域级别使用该级别可用的任何构成配置来创建关联策略。

可为每个关联策略以及该策略中使用的每条规则和 allow 名单分配优先级。规则和 allow 名单优先级会覆盖关联策略优先级。如果网络流量违反关联策略，则产生的关联事件会显示策略优先级值，除非违反的规则或 allow 名单有自己的优先级。

过程

步骤 1 选择**策略** > **关联**。

步骤 2 点击**创建策略**。

步骤 3 输入**策略名称 (Policy Name)** 和**策略说明 (Policy Desription)**。

步骤 4 从**默认优先级 (Default Priority)** 下拉列表中选择策略的优先级。选择**无 (None)** 以便仅使用规则的优先级。

步骤 5 点击**添加规则 (Add Rules)**，选择要在策略中使用的规则和 allow 名单，然后点击**添加 (Add)**。

步骤 6 从每个规则或 allow 名单的**优先级 (Priority)** 列表中选择优先级：

- 优先级值介于 1 到 5 之间。
- **无**
- **默认 (Default)**，以使用策略的默认优先级

步骤 7 将响应添加到规则和 allow 名单中，如 将响应添加到规则和允许名单 ， 第 3 页中所述。

步骤 8 单击**保存**。

下一步做什么

- 通过点击滑块来激活策略。

将响应添加到规则和允许名单

您可以将每个关联规则或allow名单与单个响应或一组响应相关联。如果网络流量触发多个规则或allow名单，系统将发起与每个规则和allow名单相关的所有响应。请注意，Nmap 补救在用作对流量量变曲线更改的响应时不会启动。

在多域部署中，可以使用在当前域或祖先域中创建的或响应。

过程

步骤 1 在关联策略编辑器中要添加响应的规则或allow名单旁边，点击**响应** （  ）。

步骤 2 在“未分配的响应”(Unassigned Responses) 下，选择在规则或allow名单触发时要启动的响应，然后点击向上箭头 (^)。

步骤 3 点击**更新**。

相关主题

Cisco Secure Firewall Management Center 警报响应

补救简介

管理关联策略

对活动关联策略进行的更改会立即生效。

激活关联策略时，系统会立即开始处理事件并触发响应。请注意，系统不会在初次、激活后的评估中为不合规主机生成 allow 名单事件。

在多域部署中，系统会显示在当前域中创建的关联策略，您可以对其进行编辑。系统还会显示来自祖先域中的选定关联策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的关联策略，请切换至该域。

注释 如果配置暴露有关不相关域的信息（包括名称、受管设备等），则系统不会显示祖先域的配置。

过程

步骤 1 选择**策略** > **关联**。

步骤 2 管理关联策略：

- 激活或停用 - 点击滑块。 如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。
- 创建 - 点击**创建策略 (Create Policy)**；请参阅配置关联策略， 第 3 页。
- 编辑 - 点击 **编辑**（）；请参阅 配置关联策略， 第 3 页。 如果显示**视图**（  ），则表明配置属于祖先域，或者您没有修改配置的权限。
- 删除 - 点击 **删除**（）。 如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

配置关联规则

简单的关联规则仅要求发生特定类型的事件。您不需要提供更具体的条件。例如，基于流量量变曲线变更的关联规则不需要条件。您也可以使用多个条件和添加的限制来创建复杂的关联规则。

当创建关联规则触发条件、主机配置文件限定条件、用户资格或连接跟踪器时，语法发生变化但结构保持不变。

注释 在多域部署中，按祖先域限制关联规则将匹配该域的后代所报告的事件。

开始之前

- 确认您的部署正在收集您要用来触发关联事件的信息类型。例如，任意单个连接或连接摘要事件的可用信息取决于几个因素，包括检测方法、日志记录方法和事件类型。 系统可以将主机从导出的NetFlow记录中添加到网络映射中，但是这些主机的可用信息是有限的；请参阅NetFlow和受管设备数据之间的差异。

过程

步骤 1 选择 **策略** > **关联**，然后点击 **规则管理**。

步骤 2 点击 **Create Rule**。

步骤 3 输入**规则名称 (Rule Name)** 和**规则说明 (Rule Description)**。

步骤 4 或者，也可为规则选择**规则组 (Rule Group)**。

步骤 5 选择基础事件类型，并为关联规则指定其他触发条件（后者为可选项）。您可以选择以下基础事件类型：

- **发生入侵事件 (an intrusion event occurs)** - 请参阅入侵事件触发条件的语法， 第 6 页。
- **发生恶意软件事件 (a malware event occurs)** - 请参阅恶意软件事件触发条件的语法， 第 8 页。
- **发生发现事件 (a discovery event occurs)** - 请参阅发现事件触发条件的语法， 第 10 页。
- **检测到用户活动 (user activity is detected)** - 请参阅用户活动事件触发条件的语法， 第 13 页。
- **发生主机输入事件 (a host input event occurs)** - 请参阅主机输入事件触发条件的语法， 第 13 页。
- **发生连接事件 (a connection event occurs)** - 请参阅连接事件触发条件的语法， 第 15 页。
- **流量量变曲线更改 (a traffic profile changes)** - 请参阅流量量变曲线更改的语法， 第 18 页。

步骤 6 或者，也可以通过添加以下任一项或全部条件来进一步限制关联规则：

- 主机配置文件限定条件 - 点击**添加主机配置文件限定条件 (Add Host Profile Qualification)**；请参阅关联主机配置文件限定条件的语法， 第 20 页。
- 连接跟踪器 - 点击**添加连接跟踪器 (Add Connection Tracker)**；请参阅连接跟踪器， 第 23 页。
- 用户资格 - 点击**添加用户资格 (Add User Qualification)**；请参阅用户资格的语法， 第 22 页。

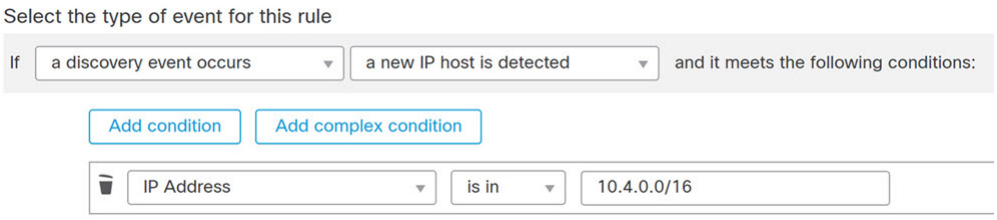
- 暂停周期 - 在“规则选项”(Rule Options) 下，使用**暂停 (Snooze)** 文本字段和下拉列表指定在关联规则触发后系统要再次触发该规则应等待的时间间隔。
- 非活动周期 - 在“规则选项”(Rule Options) 下，点击**添加非活动周期 (Add Inactive Period)**。使用文本字段和下拉列表，指定您希望系统停止根据关联规则评估网络流量的时间和频率。

提示 要移除暂停周期，请将时间间隔指定为 **0**（秒、分钟或小时）。

步骤 7 点击**保存规则 (Save Rule)**。

简单的关联规则示例

如果在特定子网中检测到新的主机，则会触发以下简单的关联规则。请注意，当类别为 IP 地址时，选择 **is in** 或 **is not in** 作为运算符使您可以指定 IP 地址是还是不是在 IP 地址块中，如特殊表示法（例如 CIDR）所述。



下一步做什么

- 使用关联策略中的规则，如配置关联策略，第 3 页中所述。

相关主题

管理关联规则，第 34 页
关联规则构建机制，第 31 页
暂停和非活动周期，第 31 页
NetFlow 和受管设备数据之间的差异

入侵事件触发条件的语法

下表介绍将入侵事件选定为基础事件时如何构建关联规则条件。

表 *1:* 入侵事件的语法

如果您指定.....	选择运算符，然后.....
访问控制策略	选择使用生成入侵事件的入侵策略的一个或多个访问控制策略。
访问控制规则名称	输入使用生成入侵事件的入侵策略的访问控制规则的全部或部分名称。
应用协议	选择一个或多个与入侵事件关联的应用协议。

如果您指定.....	选择运算符，然后.....
应用协议类别	选择一个或多个应用协议类别。
分类	选择一个或多个分类。
客户端	选择一个或多个与入侵事件关联的客户端。
客户端类别	选择一个或多个客户端类别。
目标国家/地区或源国家/地区	选择一个或多个与入侵事件中的源或目标 IP 地址关联的国家/地区。
目标 IP、源 IP、源 IP 和目标 IP，或者源 IP 或目标 IP	输入单个 IP 地址或地址块。
目标端口/ICMP 代码或源端口/ICMP 类型	输入源流量的端口号或 ICMP 类型或目标流量的端口号或 ICMP 代码。
设备	选择一个或多个可能生成事件的设备。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。
出口接口或入口接口	选择一个或多个接口。
出口安全区域或入口安全区域	选择一个或多个安全区域或隧道区域。
生成器 ID	选择一个或多个预处理器。
影响标志	选择分配给入侵事件的影响级别。 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。
内联结果	选择系统**已丢弃 (dropped)** 还是**应该已丢弃 (would have dropped)** 违反入侵策略的数据包。 在内联、交换或路由部署中，系统可以丢弃数据包。但是在被动部署中，包括当内联集处于分路模式下时，不管入侵规则状态或入侵策略的丢弃行为如何，系统都无法丢弃数据包。
入侵策略	选择一个或多个生成入侵事件的入侵策略。
IOC 标记	选择危害表现标记是不是因为入侵事件而设置。
优先级	选择规则优先级。 对于基于规则的入侵事件，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。
协议	输入 http://www.iana.org/assignments/protocol-numbers 中所列的传输协议的名称或编号。

如果您指定.....	选择运算符，然后.....
规则消息	输入全部或部分规则消息。
规则 SID	输入由逗号分隔的单个 Snort ID (SID) 或多个 SID。 如果将 **is in** 或 **is not in** 选定为运算符，则无法使用具有多项选择的弹出窗口。必须输入由逗号分隔的 SID 列表。
规则类型	指定规则是否本地规则。 本地规则包括自定义的标准文本入侵规则、经您修改的标准文本规则，以及您在保存包含已修改报头信息时创建的共享对象规则的任何新实例。
SSL 实际操作	选择指示系统如何处理加密连接的 SSL 规则操作。
SSL 证书指纹	输入用来加密流量的证书的指纹或选择与指纹相关的使用者公用名。
SSL 证书使用者公用名 (CN)	输入用于加密会话的证书的全部或部分使用者公用名。
SSL 证书使用者国家/地区 (C)	选择一个或多个用于加密会话的证书使用者国家/地区代码。
SSL 证书使用者组织 (O)	输入用于加密会话的证书的全部或部分使用者组织名称。
SSL 证书使用者组织单位 (OU)	输入用于加密会话的证书的全部或部分使用者组织单位名称。
SSL 流状态	基于系统尝试解密流量的结果选择一种或多种状态。
用户名	输入登录入侵事件中的源主机的用户的用户名。
VLAN ID	输入与触发入侵事件的数据包关联的最内部的 VLAN ID
Web 应用程序	选择与入侵事件关联的一个或多个 Web 应用。
Web 应用类别	选择一种或多种 Web 应用类别。

相关主题

入侵事件字段

Firepower 系统 IP 地址约定

恶意软件事件触发条件的语法

要使关联规则基于恶意软件事件，首先得指定要使用的恶意软件事件类型。您的选择决定您可以使用的一组触发条件。您可以选择：

- **通过基于终端的恶意软件检测**（由面向终端的 AMP 检测）
- **通过基于网络的恶意软件检测**（由面向网络的 AMP 检测）
- **通过基于网络的追溯性恶意软件检测**（由面向网络的 AMP 进行追溯性检测）

下表介绍将恶意软件事件选定为基础事件时如何构建关联规则条件。

表 2: 恶意软件事件的语法

如果您指定.....	选择运算符，然后.....
应用协议	选择一个或多个与恶意软件事件相关的应用协议。
应用协议类别	选择一个或多个应用协议类别。
客户端	选择一个或多个与恶意软件事件相关的客户端。
客户端类别	选择一个或多个客户端类别。
目标国家/地区或源国家/地区	选择一个或多个与恶意软件事件中的源或目标 IP 地址相关的国家/地区。
“目标 IP”、“主机 IP”或“源 IP”	输入单个 IP 地址或地址块。
目标端口/ICMP 代码	输入目标流量的端口号或 ICMP 代码。
处理结果	选择**恶意软件 (Malware)** 或 **自定义检测 (Custom Detection)** 或选择两者。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。
事件类型	选择一个或多个与由面向终端的 AMP 检测的恶意软件事件关联的事件类型。
文件名	输入文件的名称。
文件类型	选择文件类型。
文件类型类别	选择一个或多个文件类型类别。
IOC Tag	选择危害表现标记**是 (is**） 还是**不是 (is not)** 因为恶意软件事件而设置。
SHA-256	输入或粘贴文件的 SHA-256 散列值。
SSL 实际操作	选择指示系统如何处理加密连接的 SSL 规则操作。
SSL 证书指纹	输入用来加密流量的证书的指纹或选择与指纹相关的使用者公用名。
SSL 证书使用者公用名 (CN)	输入用于加密会话的证书的全部或部分使用者公用名。
SSL 证书使用者国家/地区 (C)	选择一个或多个用于加密会话的证书使用者国家/地区代码。
SSL 证书使用者组织 (O)	输入用于加密会话的证书的全部或部分使用者组织名称。

如果您指定.....	选择运算符，然后.....
SSL 证书使用者组织单位 (OU)	输入用于加密会话的证书的全部或部分使用者组织单位名称。
SSL 流状态	基于系统尝试解密流量的结果选择一种或多种状态。
源端口/ICMP 类型	输入源流量的端口号或 ICMP 类型。
Web 应用程序	选择一个或多个与恶意软件事件相关的 Web 应用。
Web 应用类别	选择一种或多种 Web 应用类别。

相关主题

文件和恶意软件事件字段

Firepower 系统 IP 地址约定

发现事件触发条件的语法

要使关联规则基于发现事件，首先得指定要使用的发现事件类型。您的选择决定您可以使用的一组触发条件。下表列出可以选择的发现事件类型。

在跃点变更上或由于达到主机限制而使系统丢弃新的主机时，不能触发关联规则。然而，当任何类型的发现事件发生时，可选择 **there is any type of event** 来触发该规则。

表 *3:* 关联规则触发条件对比发现事件类型

选择的选项	要使用的发现事件类型
a client has changed	客户端更新
a client timed out	客户端超时
a host IP address is reused	DHCP：IP 地址已重新分配
a host is deleted because the host limit was reached	已删除主机:已达主机限制
a host is identified as a network device	主机类型已更改为网络设备
a host timed out	主机超时
a host’s IP address has changed	DHCP：IP 地址已更改
a NETBIOS name change is detected	NETBIOS 名称更改
a new client is detected	新客户端
a new IP host is detected	新主机
a new MAC address is detected	为主机检测的其他 MAC

选择的选项	要使用的发现事件类型
a new MAC host is detected	新主机
a new network protocol is detected	新网络协议
a new transport protocol is detected	新传输协议
a TCP port closed	TCP 端口已关闭
a TCP port timed out	TCP 端口超时
a UDP port closed	UDP 端口已关闭
a UDP port timed out	UDP 端口超时
a VLAN tag was updated	VLAN 标记信息更新
an IOC was set	危害表现
an open TCP port is detected	新 TCP 端口
an open UDP port is detected	新 UDP 端口
the OS information for a host has changed	新操作系统
the OS or server identity for a host has a conflict	身份冲突
the OS or server identity for a host has timed out	身份超时
there is any kind of event	any event type
there is new information about a MAC address	MAC 信息更改
there is new information about a TCP server	TCP 服务器信息更新
there is new information about a UDP server	UDP 服务器信息更新

下表介绍将发现事件选定为基础事件时如何构建关联规则条件。

表 *4:* 发现事件的语法

如果您指定.....	选择运算符，然后.....
应用协议	选择一个或多个应用协议。
应用协议类别	选择一个或多个应用协议类别。
应用端口	输入应用协议端口号。
客户端	选择一个或多个客户端。

如果您指定.....	选择运算符，然后.....
客户端类别	选择一个或多个客户端类别。
客户端版本	输入客户端的版本号。
设备	选择一个或多个可能生成发现事件的设备。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。
硬件	输入移动设备的硬件型号。例如，要与所有 Apple iPhone 都匹配，请输入 **`iPhone`**。
主机类型	选择一个或多个主机类型。可以在一个主机或多种网络设备中的一种之间选择。
“IP 地址”(IP Address) 或“新建 IP 地址”(New IP Address)	输入单个 IP 地址或地址块。
Jailbroken	选择**是 (Yes)** 表示事件中的主机是破解移动设备，选择**否 (No)** 表示其不是破解移动设备。
MAC 地址	输入主机的全部或部分 MAC 地址。 例如，如果知道特定硬件制造商的设备拥有的 MAC 地址以 0A:12:34 开头，则可选择**开头为 (begins with)** 作为运算符，然后输入 **`0A:12:34`** 作为值。
MAC 类型	选择 MAC 地址是否是**按 ARP/DHCP 检测 (ARP/DHCP Detected)**。 例如，选择系统是否将 MAC 地址明确识别为属于主机（**按 ARP/DHCP 检测 [is ARP/DHCP Detected]**），或者因为，打个比方，受管设备和主机之间有路由器，因此系统是否可以看见许多具有该 MAC 地址的主机（**不是按 ARP/DHCP 检测 [is not ARP/DHCP Detected}**）。
MAC 供应商	输入触发发现事件的网络流量使用的 NIC 的 MAC 硬件供应商的全部或部分名称。
移动	选择**是 (Yes)** 表示事件中的主机是移动设备，选择**否 (No)** 表示其不是移动设备。
NETBIOS 名称	输入主机的 NetBIOS 名称。
网络协议	输入 http://www.iana.org/assignments/ethernet-numbers 中所列的网络协议编号。
操作系统名称	选择一个或多个操作系统名称。
操作系统供应商	选择一个或多个操作系统供应商。
操作系统版本	选择一个或多个操作系统版本。
“协议”(Protocol) 或“传输协议”(Transport Protocol)	输入 http://www.iana.org/assignments/protocol-numbers 中所列的传输协议的名称或编号。
来源	选择主机输入数据的源（用于操作系统和服务器标识更改与超时）。

如果您指定.....	选择运算符，然后.....
源类型	选择主机输入数据的源的类型（用于操作系统和服务器标识更改与超时）。
VLAN ID	输入涉及事件的主机的 VLAN ID。
Web 应用程序	选择 Web 应用。

相关主题

发现事件类型
发现事件字段
Firepower 系统 IP 地址约定

用户活动事件触发条件的语法

要将关联规则以用户活动为基础，请首先选择要使用的用户活动的类型。您的选择决定您可以使用的一组触发条件。您可以选择：

- **检测到的新用户身份**
- **登录到主机的用户**

下表介绍将用户活动选定为基础事件时如何构建关联规则条件。

表 5: 用户活动的语法

如果您指定.....	选择运算符，然后.....
设备	选择可能检测到用户活动的一个或多个设备。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。
IP 地址	输入单个 IP 地址或地址块。
用户名	输入用户名。

相关主题

用户活动数据字段
Firepower 系统 IP 地址约定

主机输入事件触发条件的语法

要使关联规则基于主机输入事件，首先得指定要使用的主机输入事件类型。您的选择决定您可以使用的一组触发条件。下表列出可以选择的主机输入事件类型。

当添加、删除或更改用户定义的主机属性的定义，或设置漏洞影响限定条件时，不能触发关联规则。

表 *6:* 关联规则触发条件与主机输入事件类型

选择的选项	触发该事件类型的规则...
添加客户端	添加客户端
删除客户端	删除客户端
添加主机	添加主机
添加协议	添加协议
删除协议	删除协议
添加扫描结果	添加扫描结果
设置服务器定义	设置服务器定义
添加服务器	添加端口
删除服务器	删除端口
漏洞标记为无效	漏洞设置为无效
漏洞标记为有效	漏洞标记为有效
删除地址	删除主机/网络
删除属性值	主机属性删除值
设置属性值	主机属性设置值
设置操作系统定义	设置操作系统定义
设置主机严重性	设置主机严重性

下表介绍将主机输入事件选定为基础事件时如何构建关联规则条件。

表 *7:* 主机输入事件的语法

如果您指定.....	选择运算符，然后.....
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。
IP 地址	输入单个 IP 地址或地址块。
来源	选择主机输入数据的源。
源类型	选择主机输入数据的源类型。

相关主题

主机输入事件类型
发现事件字段
Firepower 系统 IP 地址约定

连接事件触发条件的语法

要使关联规则基于连接事件，首先指定要使用的连接事件类型。请注意，可用于连接事件的信息可能会根据系统记录连接的方式、原因和时间而异。您可以选择：

- **位于连接开头或末尾**
- **位于连接开头**
- **位于连接末尾**

下表介绍将连接事件选定为基础事件时如何构建关联规则条件。

表 *8:* 连接事件的语法

如果您指定.....	选择运算符，然后.....
访问控制策略	选择记录连接的一个或多个访问控制策略。
Access Control Rule Action	选择与记录连接的访问控制规则相关的一个或多个操作。 当网络流量与任何监控规则的条件匹配时，不管随后处理连接的规则或默认操作如何，都选择**监控 (Monitor)** 以触发关联事件。
访问控制规则	输入记录连接的访问控制规则的全部或部分名称。 不管随后处理连接的规则或默认操作如何，您都可以输入其条件与连接匹配的任何监控规则的名称。
应用协议	选择一个或多个与连接相关的应用协议。
应用协议类别	选择一个或多个应用协议类别。
客户端	选择一个或多个客户端。
客户端类别	选择一个或多个客户端类别。
客户端版本	输入客户端的版本号。
连接持续时间	输入连接事件的持续时间，单位为秒。
连接类型	指定是否要根据获取连接信息的方式触发关联规则： • 为已导出 NetFlow 数据生成的连接事件选择**是 (is)** 和 **Netflow**。 • 为 Firepower 系统受管设备检测到的连接事件选择**不是 (is not)** 和 **Netflow**。

如果您指定.....	选择运算符，然后.....
目标国家/地区或源国家/地区	选择一个或多个与连接事件中的源或目标 IP 地址相关的国家/地区。
设备	选择一个或多个检测到连接或处理连接（对于已导出 NetFlow 记录的连接数据）的设备。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。 仅当曾经配置 管理中心以实现多租户时，此字段才存在。
出口接口或入口接口	选择一个或多个接口。
出口安全区域或入口安全区域	选择一个或多个安全区域或隧道区域。
“发起方字节数”(Initiator Bytes)、“响应方字节数”(Responder Bytes) 或“总字节数”(Total Bytes)	输入以下其中一项： • 发送的字节数（**发起方字节数 [Initiator Bytes]**）。 • 接收的字节数（**响应方字节数 [Responder Bytes]**）。 • 发送和接收的字节数（**总字节数 [Total Bytes]**）。
“发起方 IP”、“响应方 IP”、“发起方和响应方 IP”或“发起方 IP 或响应方 IP”	指定单个 IP 地址或地址块。
“发起方数据包数”(Initiator Packets)、“响应方数据包数”(Responder Packets) 或“数据包总数”(Total Packets)	输入以下其中一项： • 发送的数据包数量（**发起方数据包数 [Initiator Packets]**）。 • 接收的数据包数量（**响应方数据包数 [Responder Packets]**）。 • 发送和接收的数据包数量（**数据包总数 [Total Packets]**）
“发起方端口/ICMP 类型”(Initiator Port/ICMP Type) 或“响应方端口/ICMP 代码”(Responder Port/ICMP Code)	输入发起方流量的端口号或 ICMP 类型或接收方流量的端口号或 ICMP 类型。
IOC 标记	指定危害表现标记**是 (is)** 还是**不是 (is not)** 因为连接事件而设置。
NetBIOS 名称	输入连接中受监控主机的 NetBIOS 名称。
NetFlow 设备	选择要用于触发关联规则的 NetFlow 导出器的 IP 地址。如果没有将任何 NetFlow 导出器添加到网络发现策略，则 **NetFlow 设备 (NetFlow Device)** 下拉列表为空。
预过滤器策略 (Prefilter Policy)	选择一个或多个处理连接的预过滤器策略。
原因	选择一个或多个与连接事件关联的原因。

如果您指定.....	选择运算符，然后.....
安全情报类别	选择一个或多个与连接事件关联的安全情报类别。 要将安全情报类别用作连接结束事件的条件，请在访问控制策略中该类别设置到**监控 (Monitor)** 而非**阻止 (Block)** 中。
SSL 实际操作	指定指示系统如何处理加密连接的 SSL 规则操作。
SSL 证书指纹	输入用来加密流量的证书的指纹或选择与指纹相关的使用者公用名。
SSL 证书状态	选择一个或多个与用于加密会话的证书关联的状态。
SSL 证书使用者公用名 (CN)	输入用于加密会话的证书的全部或部分使用者公用名。
SSL 证书使用者国家/地区 (C)	选择一个或多个用于加密会话的证书使用者国家/地区代码。
SSL 证书使用者组织 (O)	输入用于加密会话的证书的全部或部分使用者组织名称。
SSL 证书使用者组织单位 (OU)	输入用于加密会话的证书的全部或部分使用者组织单位名称。
SSL 密码套件	选择一个或多个用于加密会话的加密套件。
SSL 加密会话	选择**已成功解密 (Successfully Decrypted)**。
SSL 流状态	基于系统尝试解密流量的结果选择一种或多种状态。
SSL 策略	选择一个或多个记录加密连接的 SSL 策略。
SSL 规则名称	输入记录加密连接的 SSL 规则的全部或部分名称。
SSL 服务器名称	输入客户端用来建立加密连接的服务器的全部或部分名称。
SSL URL 类别	选择一个或多个在加密连接中受访的 URL 的 URL 类别。
SSL 版本	选择一个或多个用于加密会话的 SSL 或 TLS 版本。
TCP 标志	选择为了触发关联规则，连接事件必须包含的 TCP 标志。只有 NetFlow 记录生成的连接数据包含 TCP 标志。
传输协议	输入连接使用的传输协议：**TCP** 或 **UDP**。
隧道/预过滤器规则 (Tunnel/Prefilter Rule)	输入处理连接的隧道或预过滤器规则的全部或部分名称。
URL	输入在连接中受访的全部或部分 URL。
URL 类别	选择一个或多个在连接中受访的 URL 的 URL 类别。
URL 信誉	选择一个或多个在连接中受访的 URL 的 URL 信誉值。
用户名	输入登录连接中的任一主机的用户的用户名。

如果您指定.....	选择运算符，然后.....
Web 应用程序	选择一个或多个与连接关联的 Web 应用。
Web 应用类别	选择一种或多种 Web 应用类别。

相关主题

连接和 安全相关连接 事件字段

Firepower 系统 IP 地址约定

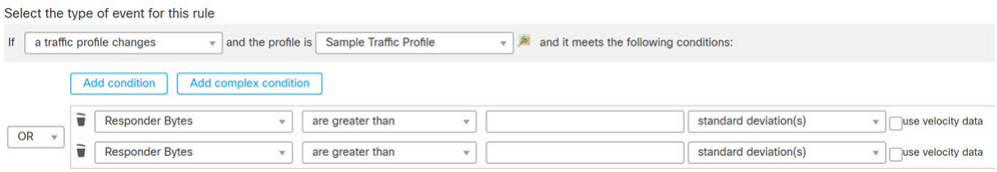
流量量变曲线更改的语法

要使关联规则基于流量量变曲线更改，首先选择要使用的流量量变曲线。当网络流量偏离以您所选量变曲线为特征的模式时，触发此规则。

可以基于原始数据或从计算数据得出的统计结果触发该规则。例如，您可以编写如果通过网络的数据量（单位：字节）突然达到高峰时触发的规则，该高峰可能是由于攻击或其他安全策略违规造成的。如果出现下列两种情况中的一种，可以指定规则触发：

- 通过网络的字节数量激增，超过一定数量的字节
- 通过网络的字节数激增，超过流量平均值上下的一定数量的标准偏差

  请注意，要创建在通过网络的字节数超出一定数量的标准偏差（高于或低于）时触发的规则，必须指定上下限，如下图所示。



  要创建在通过网络的字节数超过一定数量的高于平均值的标准偏差时触发的规则，请仅使用图中所示的第一个条件。

  要创建在通过网络的字节数超过一定数量的低于平均值的标准偏差时触发的规则，请仅使用第二个条件。

选中**使用速度数据 (use velocity data)** 复选框，以基于数据点之间的变化率触发关联规则。如果要使用上例中的速度数据，则可以指定在出现下列任何一种情况时触发规则：

- 通过网络的字节数量变化幅度非常大，高于或低于一定数量的高于平均变化率的标准偏差
- 通过网络的字节数激增，高于一定数量的字节

下表介绍在将流量量变曲线变更选定为基础事件时如何构建关联规则中的条件。

表 *9:* 流量量变曲线更改的语法

如果您指定.....	选择运算符，然后输入.....	然后选择以下之一.....
连接数	检测到的连接总数 **或** 高于或低于平均值的标准偏差的数量，检测到的连接数量必须在此范围内以触发该规则	连接 标准偏差
总字节数、发起方字节数或响应方字节数	以下任一项： • 发送的总字节数（**字节总数**） • 发送的字节数（**发起方字节数 [Initiator Bytes]**） • 接收的字节数（**响应方字节数 [Responder Bytes]**） **或** 高于或低于平均值的标准偏差的数量，上述标准之一必须在此范围内以触发该规则	字节 标准偏差
数据包总数、发起方数据包数或响应方数据包数	以下任一项： • 发送的数据包总数（**数据包总数**） • 发送的数据包数量（**发起方数据包数 [Initiator Packets]**） • 接收的数据包数量（**响应方数据包数 [Responder Packets]**） **或** 高于或低于平均值的标准偏差的数量，上述标准之一必须在此范围内以触发该规则	数据包 标准偏差
独立发起方	发起会话的独立主机的数量 **或** 高于或低于平均值的标准偏差的数量，检测到的独立发起方的数量必须为该平均值以触发该规则	发起方 标准偏差
独立响应方	响应会话的独立主机的数量 **或** 高于或低于平均值的标准偏差的数量，检测到的唯一响应方的数量必须为该平均值以触发该规则	响应方 标准偏差

关联主机配置文件限定条件的语法

要根据事件中所涉及的主机的主机配置文件来限制关联规则，请添加主机配置文件限定条件。不能将主机配置文件限定条件添加到在恶意软件事件、流量量变曲线更改或新的 IP 主机的检测上触发的关联规则。

当构建主机配置文件限定条件时，先指定要用于限制关联规则的主机。可选择的主机取决于规则的基础事件类型：

- 连接事件 - 选择**响应方主机 (Responder Host)** 或**发起方主机 (Initiator Host)**。
- 入侵事件 - 选择**目标主机 (Destination Host)** 或**源主机 (Source Host)**。
- 发现事件、主机输入事件或用户活动 - 选择**主机 (Host)**。

下表介绍如何构建关联规则的主机配置文件限定条件。

表 *10:* 主机配置文件限定条件的语法

如果您指定.....	选择运算符，然后.....
应用协议 (Application Protocol) > 应用协议 (Application Protocol)	选择应用协议。
应用协议 (Application Protocol) > 应用端口 (Application Port)	输入应用协议端口号。
应用协议 (Application Protocol) > 协议 (Protocol)	选择一个协议。
Application Protocol Category	选择类别。
客户端 > 客户端	选择客户端。
客户端 > 客户端版本	输入客户端版本。
客户端类别	选择类别。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。仅当曾经配置 管理中心以实现多租户时，此字段才存在。
硬件	输入移动设备的硬件型号。例如，要与所有 Apple iPhone 都匹配，请输入 **`iPhone`**。
主机重要性	选择主机重要性。
主机类型	选择一个或多个主机类型。您可以在一个常规主机或多种网络设备中的一种之间选择。
IOC 标记	选择一个或多个危害表现标记。
Jailbroken	选择**是 (Yes)** 表示事件中的主机是破解移动设备，选择**否 (No)** 表示其不是破解移动设备。

如果您指定.....	选择运算符，然后.....
MAC 地址 > MAC 地址	输入主机的全部或部分 MAC 地址。
MAC 地址 > MAC 类型	选择 MAC 类型是否为“按 ARP/DHCP 检测”(ARP/DHCP detected)： • 系统是否明确地将 MAC 地址识别为属于主机（**按 ARP/DHCP 检测 [ARP/DHCP Detected]**） • 打个比方，因为设备和主机之间有路由器，所以系统看到许多主机具有该 MAC 地址（**不按 ARP/DHCP 检测 [is not ARP/DHCP Detected]**） • MAC 类型不相关（**为任意 [is any]**）
MAC 供应商	输入主机使用的硬件的全部或部分 MAC 供应商。
移动	选择**是 (Yes)** 表示事件中的主机是移动设备，选择**否 (No)** 表示其不是移动设备。
NetBIOS 名称	输入主机的 NetBIOS 名称。
网络协议	输入 http://www.iana.org/assignments/ethernet-numbers 中所列的网络协议编号。
操作系统 > 操作系统供应商	选择一个或多个操作系统供应商名称。
操作系统 > 操作系统名称	选择一个或多个操作系统名称。
操作系统 > 操作系统版本	选择一个或多个操作系统版本。
传输协议	输入 http://www.iana.org/assignments/protocol-numbers 中所列的传输协议的名称或编号。
VLAN ID	输入主机的 VLAN ID 号。
Web 应用程序	选择 Web 应用。
Web 应用类别	选择类别。
任何可用的主机属性，包括默认合规性 allow 名单主机属性	根据主机属性类型输入或选择适合的值。

使用隐含或通用客户端来构建主机配置文件限定条件

如果系统报告检测到的客户端使用的应用协议名称后跟 `client`（例如，`HTTPS client`），则该客户端是隐含或通用客户端。在这些情况下，系统未检测到特定客户端，但根据服务器响应流量推断客户端的存在。

要使用隐含或通用客户端创建主机配置文件限定条件，应限制使用在响应方主机上而不是客户端上运行的应用协议。

使用事件数据来构建主机配置文件限定条件

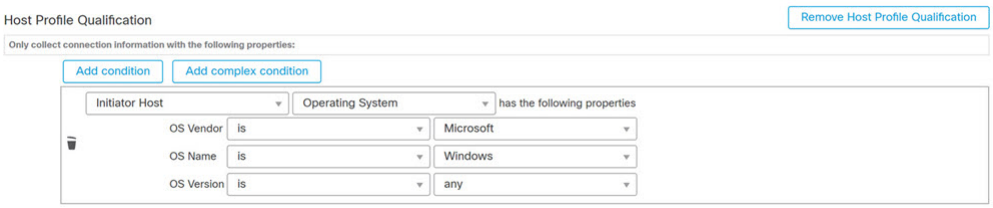
在构建主机配置文件限定条件时，通常可以使用关联规则的基础事件中的数据。

例如，当系统检测到受监控主机之一使用了特定浏览器时，假设触发关联规则。进一步假设，当检测此使用时，如果浏览器版本不是最新版本，则您要生成事件。

您可将主机配置文件限定条件添加到此关联规则，以便只有在**客户端 (Client)** 是**事件客户端 (Event Client)**，但**客户端版本 (Client Version)** 不是最新版本的情况下才会触发规则。

主机配置文件限定条件示例

下列主机配置文件限定条件会限制关联规则，以便该规则仅在涉及作为其基础的发现事件的主机运行一个 Microsoft Windows 版本时才触发。



相关主题

主机数据字段

用户资格的语法

如果您使用连接事件、入侵事件、发现事件或主机输入事件触发关联规则，则您可以基于涉及事件的用户的标识限制该规则。此限制称为用户资格。例如，您可以限制关联规则，以便仅当源用户或目标用户源自销售部门时才会触发关联规则。

不能将用户资格添加到在流量量变曲线发生更改或检测到用户活动时触发的关联规则中。此外，系统还通过在身份领域中建立的管理中心-服务器连接获取用户详细信息。该信息不能提供给数据库中的所有用户。

当构建用户资格时，先指定要用于限制关联规则的身份。可选择的身份取决于规则的基础事件类型：

- 连接事件 - 选择**发起方身份**或**响应方身份**。
- 入侵事件 - 选择**目标身份**或**源身份**。
- 发现事件 - 选择**主机身份 (Identity on Host)**。
- 主机输入事件 - 选择**主机身份 (Identity on Host)**。

下表介绍如何构建关联规则的用户资格。

表 *11:* 用户资格的语法

如果您指定.....	选择运算符，然后.....
身份验证协议	选择用于检测用户的身份验证协议（或用户类型协议）。
部门	输入部门。
域	选择一个或多个域。在多域部署中，受祖先域限制的数据与该域的后代所报告的数据相匹配。仅当曾经配置 管理中心以实现多租户时，此字段才存在。
电子邮件	输入邮箱地址。
名字	输入名字。
姓氏	输入姓氏。
电话	输入电话号码。
用户名	输入用户名。

相关主题

用户数据字段

连接跟踪器

连接跟踪器限制关联规则，以便在满足规则的初始标准后（包括主机配置文件和用户资格），系统开始跟踪某些连接。如果跟踪的连接满足在指定的时间段内收集到的其他条件，则系统会为规则生成关联事件。

提示 通常，连接跟踪器监控非常具体的流量，而且当被触发时，仅运行指定的一段时间。将连接跟踪器与流量量变曲线进行对比，发现后者一般监控的网络流量范围比较广并且持续运行。

连接跟踪器可以通过两种方法生成事件。

满足条件时，立即触发的连接跟踪器

可以配置连接跟踪器，以便在网络流量满足跟踪器的条件时，立即触发关联规则。如果出现这种情况，即使还没有超过超时周期，系统也为该连接跟踪器实例停止跟踪连接。如果此前触发关联规则的相同类型的策略违规再次发生，则系统可创建新的连接跟踪器。

但是，如果在网络流量满足连接跟踪器中的条件之前时间到期，则系统不会生成关联事件，并且还会停止跟踪该规则实例的连接。

例如，只有在特定类型的连接发生的次数超过一定时间周期内的具体次数时，连接跟踪器才可以通过生成关联事件作为一种事件阈值。或者，只有在初始连接之后，系统检测到过多数据传输时，才可以生成关联事件。

在超时期结束时触发的连接跟踪器

可以配置连接跟踪器，以便连接跟踪器可依靠在整个超时周期内搜集到的数据，因此在超时期结束前，您不能触发该连接跟踪器。

例如，如果将连接跟踪器配置为在特定时间段内检测到的字节数少于特定的传输字节数时触发，则系统在那段时间终止前处于等待状态，然后再在网络流量满足该条件时生成事件。

添加连接跟踪器

开始之前

- 根据连接、入侵、发现、用户身份或主机输入事件创建关联策略。不能将连接跟踪器添加到基于恶意软件事件或流量量变曲线更改的规则。

过程

步骤 1 在关联策略编辑器中，点击**添加连接跟踪器 (Add Connection Tracker)**。

步骤 2 指定要跟踪的连接；请参阅连接跟踪器的语法，第 24 页。

步骤 3 根据跟踪的连接，指定要生成关联事件的时间；请参阅连接跟踪器事件的语法，第 27 页。

步骤 4 指定在此期间必须满足跟踪器的条件的时间间隔（单位：秒、分或小时）。

连接跟踪器的语法

下表介绍如何构建指定要跟踪的连接种类的连接跟踪器条件。

表 *12:* 连接跟踪器的语法

如果您指定.....	选择运算符，然后.....
访问控制策略	选择一个或多个处理要跟踪的连接的访问控制策略。
访问控制规则操作	选择一个或多个与记录要跟踪的连接的访问控制规则关联的访问控制规则操作。 不管随后处理连接的规则或默认操作如何，请选择**监控 (Monitor)** 以跟踪与任何监控规则的条件匹配的连接。
访问控制规则名称	输入记录要跟踪的连接的访问控制规则的全部或部分名称。 要跟踪匹配监控规则的连接，请输入监控规则的名称。不管随后处理连接的规则或默认操作如何，系统都对连接进行跟踪。
应用协议	选择一个或多个应用协议。
应用协议类别	选择一个或多个应用协议类别。
客户端	选择一个或多个客户端。

如果您指定.....	选择运算符，然后.....
客户端类别	选择一个或多个客户端类别。
客户端版本	输入客户端的版本。
连接持续时间	输入连接持续时间，以秒为单位。
连接类型	指定是否要根据获取连接信息的方式触发关联规则： • 为已导出 NetFlow 记录生成的连接事件选择**是 (is)** 和 **Netflow**。 • 为 Firepower 系统受管设备检测到的连接事件选择**不是 (is not)** 和 **Netflow**。
目标国家/地区或源国家/地区	选择一个或多个国家/地区。
设备	选择一个或多个要跟踪其已检测连接的设备。如果要跟踪 NetFlow 连接，请选择处理来自已导出 NetFlow 记录的连接数据的设备。
入口接口或出口接口	选择一个或多个接口。
“入口安全区域”(Ingress Security Zone) 或“出口安全区域”(Egress Security Zone)	选择一个或多个安全区域或隧道区域。
“发起方 IP”(Initiator IP)、“响应方 IP”(Responder IP)、或“发起方/响应方 IP”(Initiator/Responder IP)	输入单个 IP 地址或地址块。
“发起方字节数”(Initiator Bytes)、“响应方字节数”(Responder Bytes) 或“总字节数”(Total Bytes)	输入以下其中一项： • 发送的字节数（**发起方字节数 [Initiator Bytes]**） • 接收的字节数（**响应方字节数 [Responder Bytes]**） • 发送和接收的字节数（**总字节数 [Total Bytes]**）
“发起方数据包数”(Initiator Packets)、“响应方数据包数”(Responder Packets) 或“数据包总数”(Total Packets)	输入以下其中一项： • 发送的数据包数量（**发起方数据包数 [Initiator Packets]**） • 接收的数据包数量（**响应方数据包数 [Responder Packets]**） • 发送和接收的数据包数量（**数据包总数 [Total Packets]**）
“发起方端口/ICMP 类型”(Initiator Port/ICMP Type) 或“响应方端口/ICMP 代码”(Responder Port/ICMP Code)	输入发起方流量的端口号或 ICMP 类型或接收方流量的端口号或 ICMP 类型。

如果您指定.....	选择运算符，然后.....
IOC 标记	选择危害表现标记是**已设置 (is)** 还是**未设置 (is not)**。
NETBIOS 名称	输入连接中受监控主机的 NetBIOS 名称。
NetFlow 设备	选择要跟踪的 NetFlow 导出器的 IP 地址。如果没有将任何 NetFlow 导出器添加到网络发现策略，则“NetFlow 设备”(NetFlow Device) 下拉列表为空。
预过滤器策略 (Prefilter Policy)	选择一个或多个处理要跟踪的连接的预过滤器策略。
原因	选择一个或多个与要跟踪的连接关联的原因。
安全情报类别	选择一个或多个与要跟踪的连接关联的安全情报类别。
TCP 标志	选择为了跟踪连接在连接中必须包含的 TCP 标志。只有导出的 NetFlow 记录生成的连接包含 TCP 标志数据。
传输协议	选择连接使用的传输协议。
URL	输入要跟踪的连接中受访的全部或部分 URL。
URL 类别	选择要跟踪的连接中受访的 URL 的一个或多个 URL 类别。
URL 信誉	选择要跟踪的连接中受访的 URL 的一个或多个 URL 信誉值。
用户名	输入登录要跟踪的连接中的任一主机的用户的用户名。
Web 应用程序	选择一个或多个 Web 应用。
Web 应用类别	选择一个或多个 Web 应用类别。

使用事件数据构建连接跟踪器

在构建连接跟踪器时，通常可以使用关联规则的基础事件中的数据。

例如，假设系统检测到新客户端时会触发关联规则。将连接跟踪器添加到此类型的关联规则时，系统会自动向跟踪器填充指向基础事件的限制：

- **发起方/响应方 IP (Initiator/Responder IP)** 设置为**事件 IP 地址 (Event IP Address)**。
- **客户端 (Client)** 设置为**事件客户端 (Event Client)**。

提示 要跟踪特定 IP 地址或 IP 地址块的连接，请点击**切换至手动输入 (switch to manual entry)** 以手动指定 IP。点击 **switch to event fields** 返回以使用事件中的 IP 地址。

相关主题

连接和 安全相关连接 事件字段

Firepower 系统 IP 地址约定

连接跟踪器事件的语法

下表介绍如何构建指定何时基于正在跟踪的连接生成关联事件的连接跟踪器条件。

表 *13:* 连接跟踪器事件的语法

如果您指定.....	选择运算符，然后输入.....
连接数	检测到的连接总数
SSL 加密会话数	检测到的 SSL 或 TLS 加密会话的总数
总字节数、发起方字节数或响应方字节数	以下任一项： • 发送的总字节数（**字节总数**） • 发送的字节数（**发起方字节数 [Initiator Bytes]**） • 接收的字节数（**响应方字节数 [Responder Bytes]**）
数据包总数、发起方数据包数或响应方数据包数	以下任一项： • 发送的数据包总数（**数据包总数**） • 发送的数据包数量（**发起方数据包数 [Initiator Packets]**） • 接收的数据包数量（**响应方数据包数 [Responder Packets]**）
独立发起方或 独立响应方	以下任一项： • 检测到的发起会话的独立主机的数量 (**Unique Initiators**) • 响应检测到的连接的独立主机的数量 (**Unique Responders**)

外部主机连接过多的配置示例

考虑这样一个场景：您将敏感文件存档到网络 10.1.0.0/16 上，而且该网络外的主机通常不向网络内的主机发起连接。网络外的主机偶尔会发起连接，但您已确定如果在两分钟内发起四次或更多次的连接，则说明有令人担心的问题。

下图所示规则规定当 10.1.0.0/16 网络外的主机向网络内的主机发起连接时，系统将开始跟踪符合该标准的连接。然后，如果系统在两分钟内检测到匹配该签名的四次连接（包括原始连接），系统会生成关联事件。

Rule Information

Add User Qua

Rule Name: Archive Connections - Outside

Rule Description: Trigger on 4 ouside connections tc

Rule Group: Ungrouped

Select the type of event for this rule

If a connection event occurs | at either the beginning or the en | and it meets the following conditions:

Add condition | Add complex condition

OR	Initiator IP	is not in	10.1.0.0/16	
	Responder IP	is in	10.1.0.0/16	

Connection Tracker

... start tracking connections that meet the following conditions:

Add condition | Add complex condition

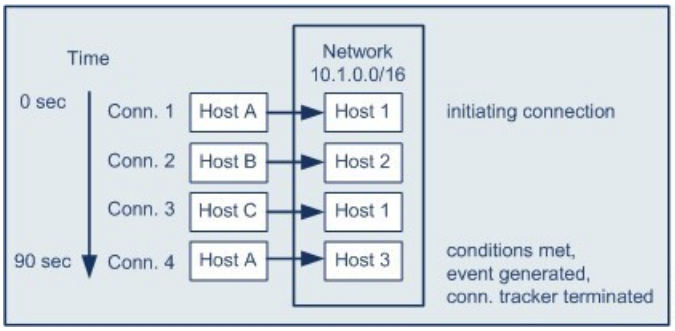
AND	Initiator IP	is not in	10.1.0.0/16	
	Responder IP	is in	10.1.0.0/16	

... and generate an event if:

Add condition | Add complex condition

total	Number of Connections	are greater than or equal to	4

下图显示网络流量如何触发上述关联规则。



在本示例中，系统检测到满足关联规则基本条件的连接，即系统检测到从 10.1.0.0/16 网络外的主机到该网络内主机的连接。这样创建连接跟踪器。

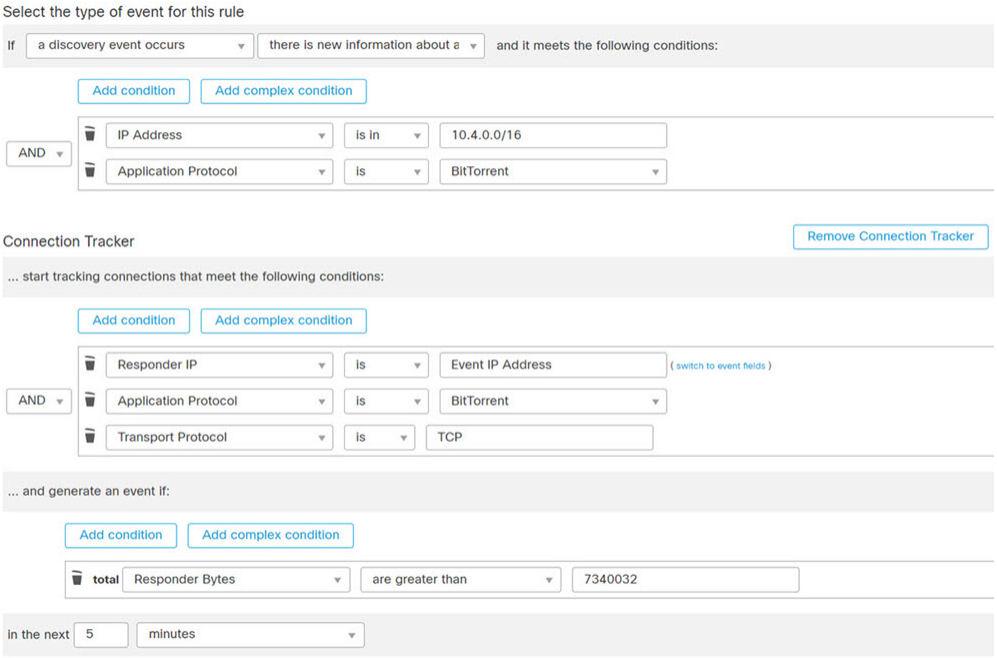
处理连接跟踪器的阶段如下：

- 首先，当系统检测到从网络外的主机 A 向网络内的主机 1 进行的连接时，系统开始跟踪连接。
- 系统又检测到符合连接跟踪器特征的两次连接：Host B 至 Host 2 和 Host C 至 Host 1。
- 当在两分钟的时间限制内 Host A 连接到 Host 3 时，系统检测到第四次符合特征的连接。满足规则条件。
- 最后，系统生成关联事件，且系统停止跟踪连接。

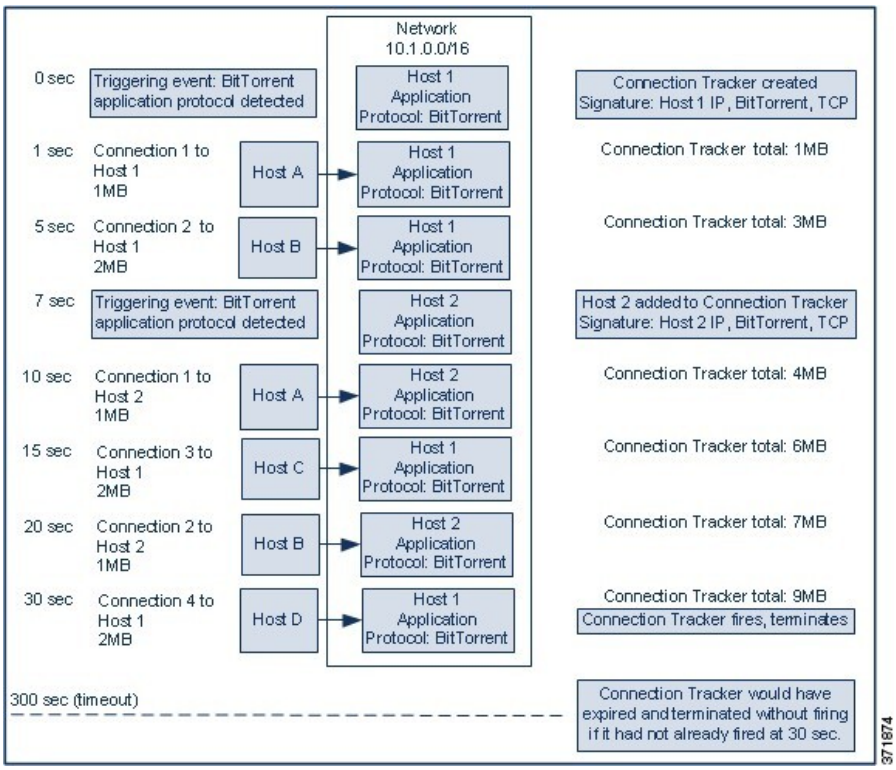
BitTorrent 数据传输过多的配置示例

考虑这样一个场景：您希望在初始连接受监控网络的任何主机后，如果系统检测到 BitTorrent 数据传输量过多，则生成一个关联事件。

下图显示当系统检测到受监控网络上的 BitTorrent 应用协议时触发的关联规则。该规则具有限制规则的连接跟踪器，以便仅当受监控网络（在本例中为 10.1.0.0/16）上的主机在出现初始策略违规后的五分钟内通过 BitTorrent 传输的总数据超过 7 MB（7340032 字节）时触发该规则。



下图显示网络流量如何触发上述关联规则。



在本示例中，系统在两个不同的主机上检测到 BitTorrent TCP 应用协议：Host 1 和 Host 2。这两台主机通过 BitTorrent 将数据传输到其他四台主机：Host A、Host B、Host C 和 Host D。

处理该连接跟踪器的阶段如下：

- 首先，当系统检测到 Host 1 上的 BitTorrent 应用协议时，系统开始跟踪 0 秒标记处的连接。请注意，如果系统在接下来的 5 分钟（到 300 秒标记）内未检测到 7 MB 的 BitTorrent TCP 传输数据，则连接跟踪器将过期。
- 5 秒钟时，Host 1 已经传输符合特征的 3 MB 数据：
  - 在 1 秒标记处时，从 Host 1 传输至 Host A 的 1 MB 的数据量 （1MB 符合连接跟踪器条件的 BitTorrent 总流量）
  - 在 5 秒标记处时，从 Host 1 传输至 Host B 的 2MB 的数据量（总共 3MB）
- 在 7 秒种时，系统在 Host 2 上检测到 BitTorrent 应用协议，同时也开始跟踪该主机的 BitTorrent 连接。
- 在 20 秒种时，系统已经检测到从 Host 1 和 Host 2 传输的符合特征的其他数据：
  - 在 10 秒标记处时，从 Host 2 传输至 Host A 的 1MB 的数据量（总共 4MB）
  - 在 15 秒标记处时，从 Host 1 传输至 Host C 的 2 MB 的数据量（总共 6 MB）
  - 在 20 秒标记处时，从 Host 2 传输至 Host B 的 1MB 的数据量（总共 7MB）

- 尽管 Host 1 和 Host 2 目前已经传输 7 MB 的 BitTorrent 综合数据，但因为传输字节总数必须**超过** 7 MB，所以规则不会触发（**响应方字节数超过 7340032 [Responder Bytes are greater than 7340032]**）。此时，如果系统在跟踪器超时期间余下的 280 秒内没有检测到其他 BitTorrent 数据传输，则跟踪器过期且系统不会生成关联事件。
- 但是，在 30 秒钟时，系统检测到其他 BitTorrent 传输，且满足规则条件：
  - 在 30 秒标记处时，2 MB 数据从 Host 1 传输至 Host D（总共 9 MB）
- 最后，系统会生成关联事件。此外，尽管 5 分钟的周期尚未过期，但是在该连接跟踪器示例中，系统也停止跟踪连接。如果此时系统检测到使用 BitTorrent TCP 应用协议的新连接，则系统会创建新的连接跟踪器。请注意，在 Host 1 向 Host D 传输总计 2 MB 的数据后，系统生成关联事件，因为其在会话终止后才会计算连接数据。

暂停和非活动周期

您可以在关联规则中配置暂停周期。当关联规则触发时，即使在指定间隔期间违反该规则，暂停周期也会指示系统在该间隔内停止触发该规则。在暂停周期过后，规则可以再次触发（并开始进入新的暂停周期）。

例如，您网络上的某个主机可能不应产生流量。每当系统检测到涉及该主机的连接时都会触发一个的简单关联规则，致使可能在短时间内创建多个关联事件，具体取决于发往和来自该主机的网络流量。要限制披露策略违规的关联事件数量，可以添加暂停周期，以便仅为系统检测到的涉及该主机的第一个连接（在指定的时间周期内）生成关联事件。

此外，还可以在关联规则中设置非活动周期。在非活动周期，关联规则将不会触发。您可以将非活动周期设置为每日、每周或每月循环。例如，您每天可能会对内部网络执行夜间 Nmap 扫描，以查找主机操作系统的变化情况。在这种情况下，可以对扫描时间和期间影响到的关联规则设置一个每天非活动周期，以便那些规则不会被错误地触发。

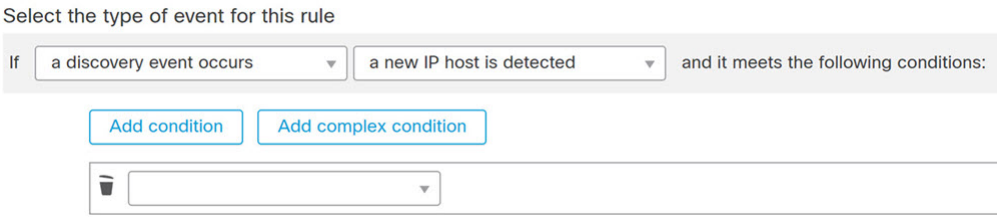
关联规则构建机制

您可通过指定触发条件来构建关联规则。您可以在条件中使用的语法会根据您正在创建的元素而变化，但是机制相同。

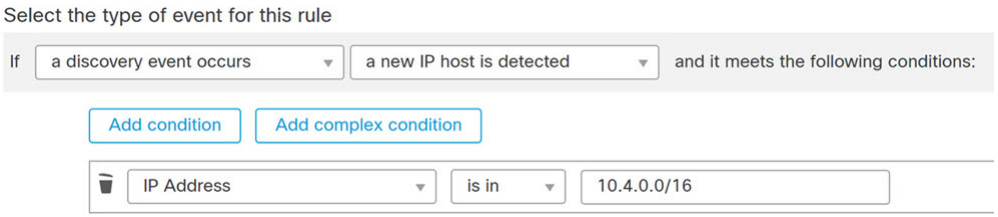
大多数条件有三部分：类别、运算符和值。

- 可选择的类别取决于您是在构建关联规则触发器、主机配置文件限定条件、连接跟踪器还是用户资格。在关联规则触发器中，类别的划分进一步取决于规则的基础事件类型。某些条件可能包含多个类别，每个类别都可能有自己的运算符和值。
- 条件的可用运算符取决于类别。
- 可用于指定条件值的语法取决于类别和运算符。有时侯，您可以在文本字段键入值。有时候，您可以从下拉列表中选择一个值（或多个值）。

例如，如果要在每次检测到新主机时都生成关联事件，则可以创建无条件的简单规则。



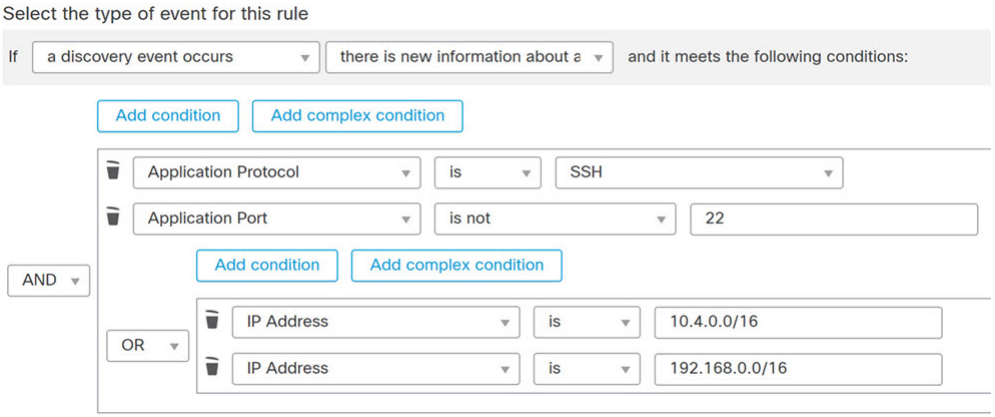
如果要在仅当 10.4.x.x 网络中检测到该新的主机时进一步限制规则并生成事件，则可以添加一个条件。



当构建的结构不止一个条件时，必须使用 **AND** 或 **OR** 运算符将这些条件结合起来。相同级别的条件会被放在一起评估：

- **AND** 运算符要求必须满足其控制的级别上的所有条件。
- **OR** 运算符要求必须满足其控制的级别上的至少一个条件。

检测 10.4.x.x 网络和 192.168.x.x 网络上的非标准端口的 SSH 活动的以下规则具有四个条件，底部的两个的条件较复杂。



从逻辑上讲，该规则被评估如下：

```
(A and B and (C or D))
```

表 *14:* 规则评估

关键字	为陈述以下情况的条件.....
A	应用协议为 SSH

关键字	为陈述以下情况的条件.....
B	应用端口不是 22
选	IP 地址为 10.0.0.0/8
D	IP 地址为 196.168.0.0/16

注意 评估触发常见事件的复杂关联规则可降低系统的性能。例如，系统必须根据每个已记录的连接评估的多条件规则可能会导致资源超载。

关联规则中的添加和连接条件

过程

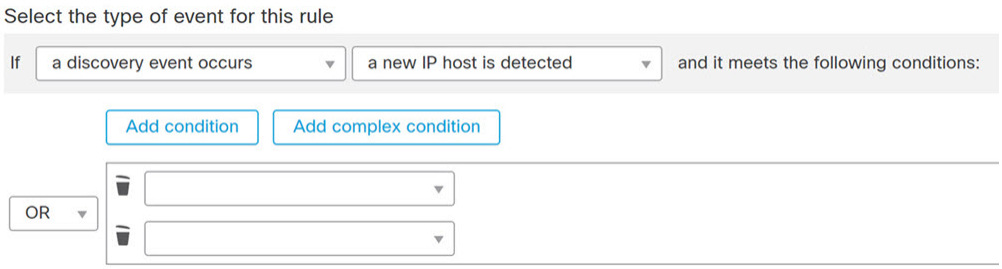
步骤 1 在关联规则编辑器中，添加简单或复杂条件：

- 简单 - 点击**添加条件 (Add condition)**。
- 复杂 - 点击**添加复杂条件 (Add complex condition)**。

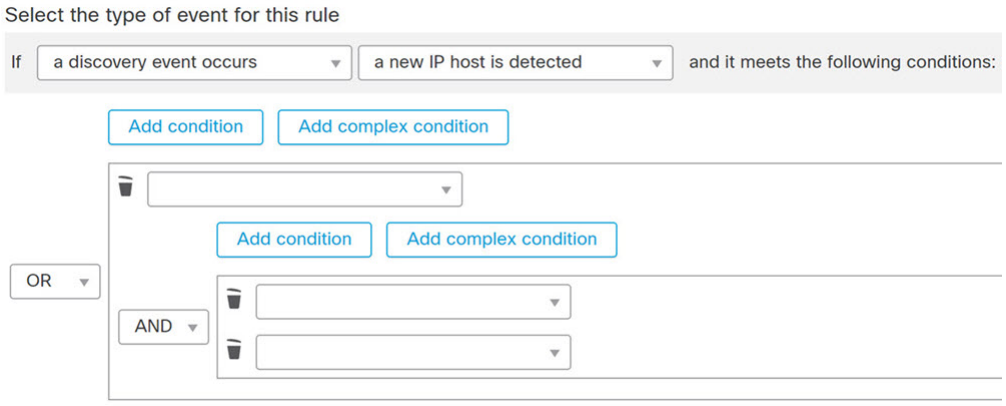
步骤 2 通过从条件左侧的下拉列表中选择 **AND** 或 **OR** 运算符来连接条件。

示例：简单和复杂条件

下图显示具有使用 **OR** 运算符结合的两个简单条件的关联规则。



下图显示具有使用**OR**运算符结合的一个简单条件和一个复杂条件的关联规则。复杂条件包括使用 **AND** 运算符结合的两个简单条件。



在关联规则条件中使用多个值

在构建关联条件且条件语法允许您从下拉列表中选择值时，通常可以从列表中选择多个值。

过程

步骤 1 在关联条件编辑器中，构建条件，选择 **is in** 或 **is not in** 作为运算符。

步骤 2 点击文本字段或**编辑 (Edit)** 链接的任意位置。

步骤 3 在**可用 (Available)** 下，选择多个值。也可以点击并拖动以选择多个相邻值。

步骤 4 点击右箭头 (>) 将选定条目移动到**选定项 (Selected)** 中。

步骤 5 点击**确定 (OK)**。

管理关联规则

在多域部署中，系统会显示在当前域中创建的关联规则和组，您可以对这些关联规则和组进行编辑。它还显示祖先域中的所选关联规则和组，您无法对这些关联规则和组进行编辑。要查看和编辑在较低域中创建的关联规则和组，请切换至该域。

注释 如果配置暴露有关不相关域的信息（包括名称、受管设备等），则系统不会显示祖先域的配置。

对活动关联策略中的规则进行的更改会立即生效。

开始之前

- 如果要删除规则，请从所有关联策略中将其删除，如管理关联策略，第 4 页中所述。

过程

步骤 1 选择 **策略** > **关联**，然后点击 **规则管理**。

步骤 2 管理规则：

- 创建 - 点击**创建规则 (Create Rule)**；请参阅配置关联规则，第 5 页。
- 创建组 - 点击**创建组 (Create Group)**，输入组的名称，然后点击**保存 (Save)**。要向组中添加规则，请编辑该规则。
- 编辑 - 点击 **编辑**（）；请参阅配置关联规则，第 5 页。 如果显示**视图**（），则表明配置属于祖先域，或者您没有修改配置的权限。
- 删除规则或规则组 - 点击 **删除**（）。删除规则组会对规则取消分组。 如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

配置关联响应组

您可以创建警报和补救的关联响应组，然后将该组激活并分配到活动关联策略中的关联规则。当网络流量与关联规则相匹配时，系统会启动所有分组的响应。

在活动关联策略中使用时，对活动组或其任何分组响应的更改会立即生效。

过程

步骤 1 选择**策略** > **关联**，然后点击**组**。

步骤 2 点击 **Create Group**。

步骤 3 输入 **Name**。

步骤 4 如果在创建后激活组，请选中**活动 (Active)** 复选框。

已停用的组不会启动响应。

步骤 5 选择对组的**可用响应 (Available Responses)**，然后点击向右箭头 (>) 以将其移至**组中的响应 (Responses in Group)**。要向另一边移动响应，请使用向左箭头 (<)。

步骤 6 点击**保存 (Save)**。

下一步做什么

- 如果在创建后未激活组并要立即将其激活，请点击滑块。

相关主题

Cisco Secure Firewall Management Center 警报响应
补救简介

管理关联响应组

如果关联策略中没有使用响应组，可以删除该组。删除响应组将取消对响应的分组。您也可以在不删除响应组的情况下，暂时停用响应组。这样可以在系统中保留响应组，但在违反策略时不会启动响应组。

在多域部署中，系统会显示在当前域中创建的组，您可以对其进行编辑。系统还会显示在祖先域中创建的组，您不可以对其进行编辑。要查看和编辑在较低域中创建的组，请切换至该域。

对活动的、正在使用的相应组进行的更改会立即生效。

过程

步骤 1 选择**策略** > **关联**，然后点击**组**。

步骤 2 管理响应组：

- 激活或停用 - 点击滑块。 如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。
- 创建 - 点击**创建组 (Create Group)**；请参阅配置关联响应组， 第 35 页。
- 编辑 - 点击 **编辑**（ ）；请参阅 配置关联响应组， 第 35 页。 如果显示**视图**（ ），则表明配置属于祖先域，或者您没有修改配置的权限。
- 删除 - 点击 **删除**（ ）。 如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

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。