# 流量分析

以下主题介绍如何配置流量量变曲线：



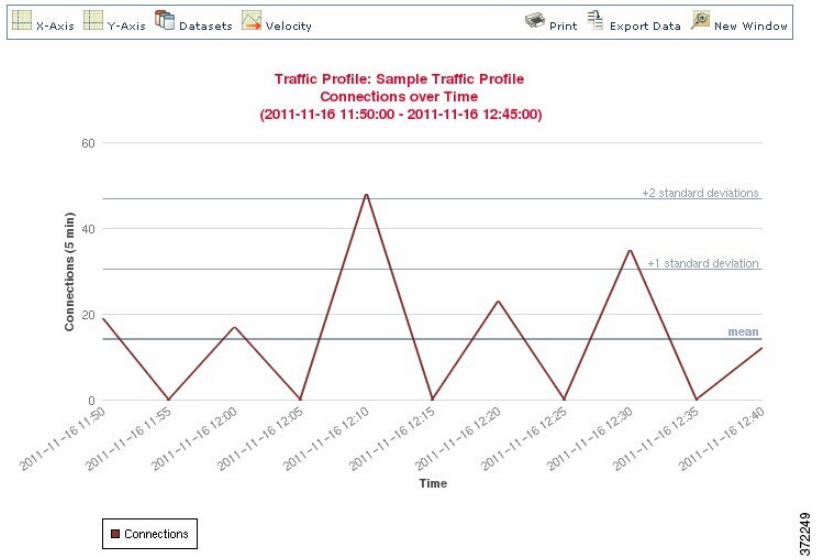
# 流量量变曲线简介

流量量变曲线是基于在分析时间窗口 (PTW) 收集的连接数据的网络流量图形。此测量可能表示正常网络流量。在学习期后，可以通过对照量变曲线评估新的流量来检测异常网络流量。

默认 PTW 是一周，但是，您可以将其更改为短至 1 小时或长至几周。默认情况下，流量量变曲线会生成系统在五分钟时间区间内生成的连接事件的统计数据。但是，可以将此采样率增加到长达 1 小时。

**提示** 思科建议 PTW 至少包含 100 个数据点。配置 PTW 和采样率，以便流量量变曲线包含足够的数据以具备统计意义。

下图显示了 PTW 为一天及采样率为五分钟的流量量变曲线。




您也可以在流量量变曲线中设置非活动周期。流量量变曲线在非活动周期内收集数据，但在计算量变曲线统计数据不使用该数据。一段时间内划分的流量量变曲线图可显示非活动周期为阴影区域。

例如，可以考虑所有工作站均在每晚午夜时备份的网络基础设施。备份大约需要30分钟，并将使网络流量达到峰值。可以为流量量变曲线配置周期性非活动周期，以与计划备份相符。

**注释** 系统使用连接结束数据创建连接图和流量量变曲线。要使用流量量变曲线，请确保将连接结束事件记录到 管理中心数据库。

### 实施流量量变曲线

当激活流量量变曲线时，系统会收集并评估所配置的学习期 (PTW) 的连接数据。在学习期后，系统评估根据流量量变曲线编写的关联规则。

例如，您可写入当通过网络的数据量（单位为数据包、KB或连接数）突然达到平均流量以上三个标准差的峰值时触发的规则，这可能表示出现攻击或其他安全策略违规。然后，您可以包括关联策略中的规则以警告您流量达到峰值或执行补救措施作为响应措施。

### 以流量量变曲线为目标

量变曲线条件和主机配置文件限定条件限制流量量变曲线。

使用量变曲线条件，可以分析所有网络流量，也可以将流量量变曲线限用于监控域、域内或跨域的子网或者单个主机。在多域部署中：

- 分叶域管理员可以分析其分叶域内的网络流量。
- 较高级别的域管理员可以在域内或跨域分析流量。

量变曲线条件还可以使用基于连接数据的条件来限制流量量变曲线。例如，可以设置量变曲线条件，以便流量量变曲线仅使用特定端口、协议或应用来分析会话。

最后，还可以使用有关被跟踪主机的信息来限制流量量变曲线。此类限制被称为主机配置条件限定条件。例如，可以仅收集具有高重要性的主机的连接数据。

注释 将流量量变曲线限于较高级别的域可汇聚并分析**每个**后代分叶域中**相同**类型的流量。系统会为每个分叶域构建单独的网络映射。在多域部署中，跨域分析流量可能会出现意外结果。

### 相关主题

关联策略和规则简介

# 流量量变曲线条件

您可以创建简单的流量量变曲线条件和主机配置文件限定条件，也可以通过结合和嵌套条件创建较复杂的结构。

条件有三部分：类别、运算符和值。

- 可以使用的类别取决于是构建流量量变曲线条件还是主机配置文件限定条件。
- 可以使用的运算符取决于选择的类别。
- 可用于指定条件值的语法取决于类别和运算符。有时侯，必须在文本字段键入值。有时候，可以从下拉列表中选择一个或多个值。

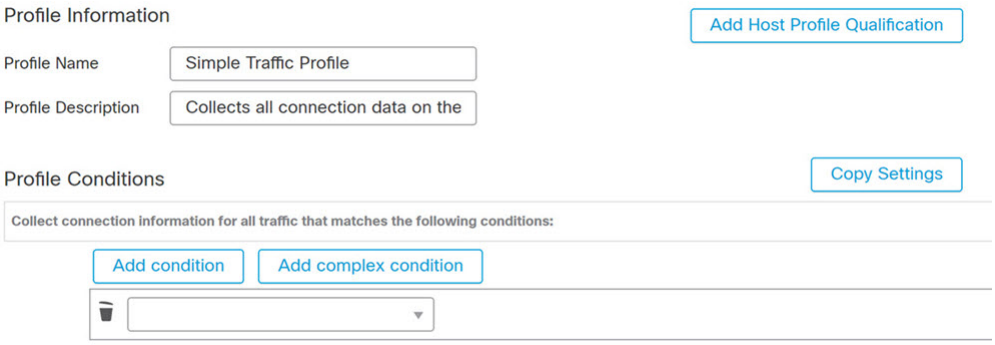
对于主机配置文件限定条件，还必须指定是否使用有关发起或响应主机的信息数据限制流量量变曲线。

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。

### 受限制的流量量变曲线

如果要创建为整个监控网段收集数据的流量量变曲线，可以创建一个非常简单的不带条件的流量量变曲线，如下图所示。



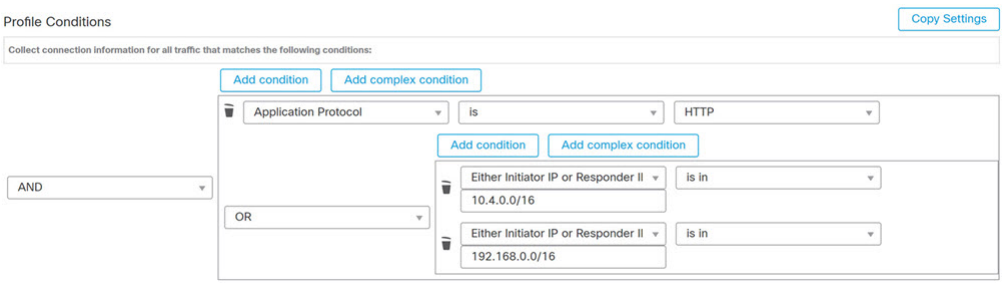

### 简单流量量变曲线

如果要仅为子网限制流量量变曲线和收集数据，可以添加单个条件，如下图所示。


### 复杂流量量变曲线

以下流量量变曲线包含以 **AND** 连接的两个条件。这意味着流量量变曲线仅会在两种条件均为真时收集连接数据。在本示例中，它会收集所有 IP 地址在特定子网中的主机的 HTTP 连接。


相反，在任意一个子网中收集HTTP活动连接数据的以下流量量变曲线有三个条件，最后一个构成复杂条件。




从逻辑上讲，上述流量量变曲线应如下进行评估：

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

| 关键字 | 为陈述以下情况的条件..... |
|---|---|
| A | 应用协议名称是 HTTP |
| B | IP 地址为 10.4.0.0/16 |
| C | IP 地址为 192.168.0.0/16 |

# 流量配置文件的要求和必备条件

**型号支持**

Any

**支持的域**

任意

**用户角色**

- 管理员
- 发现管理员

# 管理流量量变曲线

只有对处于活动状态的完整流量量变曲线写入的规则才可触发关联策略违规。每个流量量变曲线旁边的滑块表示该配置文件是否处于活动状态并正在收集数据。进度条显示流量量变曲线学习期的状态。

在多域部署中，系统会显示在当前域中创建的流量量变曲线，您可以对其进行编辑。系统还会显示祖先域中的选定流量量变曲线，您不可以对其进行编辑。要查看和编辑在较低域中创建的流量量变曲线，请切换至该域。

**注释** 如果祖先域中的流量量变曲线的条件可透露无关域的信息（包括名称、受管设备等），则系统不会显示该配置文件。

过程

**步骤 1** 选择 **策略** > **关联**，然后点击 **流量量变曲线**。

**步骤 2** 管理流量量变曲线：

- 激活/停用 - 要激活或停用流量量变曲线，请点击滑块。停用流量量变曲线会删除其关联的数据。如果重新激活该配置文件，必须等待 PTW 时长后，对其写入的规则才会触发。
- 创建 - 要创建新的流量量变曲线，请点击**新建配置文件**，然后如配置流量量变曲线，第 6 页中所述继续操作。您也可以点击 **复制**（  ）编辑现有流量量变曲线的副本。
- 删除 - 要删除流量量变曲线，请点击 **删除**（），然后确认您的选择。
- 编辑 - 要修改现有流量量变曲线，请点击 **编辑**（  ），然后如配置流量量变曲线，第 6 页中所述继续操作。如果流量量变曲线处于活动状态，则只能更改其名称和说明。
- 图表 - 要查看图表形式的流量量变曲线，请点击 **图形**（  ）。在多域部署中，如果属于祖先域的流量量变曲线的图表可透露无关域的信息，则无法查看该图表。

# 配置流量量变曲线

将流量量变曲线限于较高级别的域可汇聚并分析**每个**后代分叶域中**相同**类型的流量。系统会为每个分叶域构建单独的网络映射。在多域部署中，跨域分析流量可能会出现意外结果。

过程

**步骤 1** 选择 **策略** > **关联**，然后点击 **流量量变曲线**。

**步骤 2** 点击 **New Profile**。

**步骤 3** 输入**配置文件名称 (Profile Name)** 和输入**配置文件说明 (Profile Description)**（可选）。

**步骤 4** 或者，限制流量量变曲线：

- “复制设置”(Copy Settings) - 要复制某个现有流量量变曲线的设置，请点击**复制设置 (Copy Settings)**，选择要使用的流量量变曲线，然后点击**加载 (Load)**。
- “配置文件条件”(Profile Conditions) - 要使用被跟踪连接的信息限制流量量变曲线，请按添加流量量变曲线条件，第 7 页中所述进行操作。
- “主机配置文件限定条件”(Host Profile Qualification) - 要使用被跟踪主机的信息限制流量量变曲线，请按将主机配置文件限定条件添加到流量量变曲线中，第 8 页中所述进行操作。
- “分析时间窗口 (PTW)”(Profiling Time Window [PTW]) - 要更改**分析时间窗口 (Profiling Time Window)**，请输入时间单位，然后选择**小时数 (hour[s])**、**天数 (day[s])** 或**周数 (week[s])**。
- “采样率”(Sampling Rate) - 选择**采样率 (Sampling Rate)**（以分钟为单位）。
- “非活动周期”(Inactive Period) - 点击**添加非活动周期 (Add Inactive Period)**，然后使用下拉列表指定希望流量量变曲线保持非活动的时间和频率。非活动流量量变曲线不会触发关联规则。流量量变曲线不包含配置文件统计信息中非活动时期的数据。

**步骤 5** 保存流量量变曲线：

- 要保存量变曲线并立即开始收集数据，请点击 **Save & Activate**。
- 要保存量变曲线而不激活它，请点击 **Save**。

# 添加流量量变曲线条件

**过程**

**步骤 1** 在流量量变曲线编辑器中的“量变曲线条件”下，为要添加的每个条件点击**添加条件**或**添加复杂条件**。相同级别的条件会被放在一起评估。

- 如果需要所有条件都位于满足操作符控制的级别上，选择 **AND**。
- 如果需要只有一个条件位于满足操作符控制的级别上，请选择 **OR**。

**步骤 2** 为每个条件指定类别、运算符和值，如流量量变曲线条件的语法，第 8 页和流量量变曲线条件，第 3 页中所述。

如果选择 **is in** 或 **is not in** 作为运算符，则可以在单个条件中选择多个值，如在流量量变曲线条件中使用多个值，第 12 页中所述。

当类别为某个 IP 地址时，选择 **is in** 或 **is not in** 作为操作符使您可以指定 IP 地址是还是不是在某个 IP 地址范围中。

**示例**

以下流量量变曲线收集有关特定子网的信息。条件的类别是 **Initiator/Responder IP**，操作符是 **is in**，值为 `10.4.0.0/16`。


**相关主题**

Firepower 系统 IP 地址约定

# 将主机配置文件限定条件添加到流量量变曲线中

过程

**步骤 1** 在流量量变曲线编辑器上，点击**添加主机配置文件限定条件 (Add Host Profile Qualification)**。

**步骤 2** 在“主机配置文件限定条件”下，为要添加的每个条件点击**添加条件** 或**添加复杂条件**。相同级别的条件会被放在一起评估。

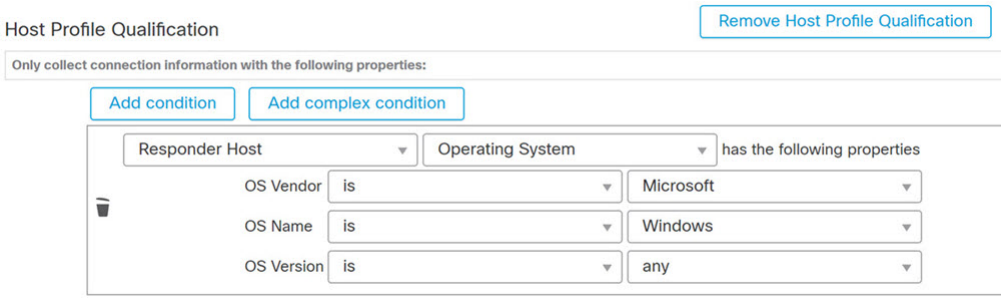
- 如果需要所有条件都位于满足操作符控制的级别上，选择 **AND**。
- 如果需要只有一个条件位于满足操作符控制的级别上，请选择 **OR**。

**步骤 3** 为每个条件指定主机类型、类别、运算符和值，如流量量变曲线中主机配置文件限定条件的语法，第 10 页和流量量变曲线条件，第 3 页中所述。

如果选择 **is in** 或 **is not in** 作为运算符，则可以在单个条件中选择多个值，如在流量量变曲线条件中使用多个值，第 12 页中所述。

示例

以下主机配置文件限定条件则限制了流量量变曲线以便其只在检测到的连接中的响应主机运行 Microsoft Windows 版本时才会收集连接数据。




# 流量量变曲线条件的语法

下表介绍了如何构建流量量变曲线条件。请记住，可用于构建流量量变曲线的连接数据取决于多个因素，包括流量特征和检测方法。

表 *1:* 流量量变曲线条件的语法

| 如果选择..... | 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。 |

| 如果选择..... | 选择运算符，然后..... |
|---|---|
| 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。 |
| 连接类型 | 选择配置文件是使用来自 Firepower 系统受管设备监控的流量还是来自已导出的 NetFlow 记录的连接数据。<br>如果您不指定连接类型，则流量量变曲线会同时包括两者。 |
| “目标国家/地区”(Destination Country)或“源国家/地区”(Source Country) | 选择一个或多个国家/地区。 |
| 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。 |
| “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 IP 地址或 IP 地址范围。<br>系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 |
| NetFlow 设备 | 选择要使用其数据创建流量量变曲线的 NetFlow 导出器。 |
| 响应器端口/ICMP 代码 | 输入端口号或 ICMP 代码。 |
| 安全情报类别 | 选择一个或多个安全情报类别。<br>要将安全情报类别用于流量量变曲线条件，该类别必须在访问控制策略中设置为**监控(Monitor)**而不是**阻止 (Block)**。 |
| SSL 加密会话 | 选择**已成功解密 (Successfully Decrypted)**。 |
| 传输协议 | 输入 **TCP** 或 **UDP** 作为传输协议。 |
| 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。 |

**相关主题**

填充连接事件字段的要求

Firepower 系统 IP 地址约定

# 流量量变曲线中主机配置文件限定条件的语法

当构建主机配置文件限定条件时，必须首先选择要用于限制流量量变曲线的主机。您可以选择**响应方主机 (Responder Host)** 或**发起方主机 (Initiator Host)**。在选择主机角色之后，请继续构建主机配置文件限定条件。

虽然可以使用 NetFlow 记录将主机添加到网络映射中，但是有关这些主机的可用信息有限。例如，这些主机没有可用的操作系统数据，除非您使用主机输入功能提供这些数据。此外，如果流量量变曲线使用已导出的 NetFlow 记录中的连接数据，请记住，NetFlow 记录不包含有关连接中的哪台主机是发起方和哪台主机是响应方的信息。当系统处理 NetFlow 记录时，它会根据各主机正在使用的端口以及此类端口是否为公认端口来使用一种算法确定该信息。

要匹配隐含或一般客户端，请根据响应客户端的服务器所用的应用协议创建主机配置文件限定条件。当作为连接发起方或源的主机上的客户端列表包含**客户端**遵循的应用协议名称时，该客户端可能实际上就是一种隐含客户端。换句话说，系统会根据使用该客户端的应用协议的服务器响应流量，而非检测到的客户端流量来报告该客户端。

例如，如果系统将 **HTTPS 客户端**作为主机上的一个客户端进行报告，请为**响应方主机**创建主机配置限定条件，其中**应用协议 (Application Protocol)** 被设置为 **HTTPS**，因为 HTTPS 客户端会根据响应方或目标主机发送的 HTTPS 服务器响应流量被报告为一种一般客户端。

**表 *2:* 主机配置文件限定条件的语法**

| 如果选择..... | 选择运算符，然后..... |
|---|---|
| 应用协议 (Application Protocol) > 应用协议 (Application Protocol) | 选择一个或多个应用协议。 |
| 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) | 选择协议。 |
| 应用协议类别 | 选择一个或多个应用协议类别。 |
| 客户端 > 客户端 | 选择一个或多个客户端。 |
| 客户端 > 客户端版本 | 输入客户端版本。 |
| 客户端类别 | 选择一个或多个客户端类别。 |
| 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。 |
| 硬件 | 输入移动设备硬件型号。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。 |

| 如果选择..... | 选择运算符，然后..... |
|---|---|
| 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 IOC 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。 |
| 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 类型是否是**按 ARP/DHCP 检测 (ARP/DHCP Detected)**，即，<br>• 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]**）<br>• 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]**）<br>• 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。<br>系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 VLAN 标记限制此配置可产生意外结果。 |
| 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。 |

| 如果选择..... | 选择运算符，然后..... |
| --- | --- |
| 任何可用的主机属性，包括默认合规性 allow 名单主机属性 | 指定适当的值，这取决于您选择的主机属性类型：<br>• 如果主机属性类型为 Integer，请在针对该属性确定的范围中输入一个整数值。<br>• 如果主机属性类型为“文本”(Text)，请输入文本值。<br>• 如果主机属性类型为“列表”(List)，请选择有效的列表字符串。<br>• 如果主机属性类型是 URL，请输入 URL 值。 |

# 在流量量变曲线条件中使用多个值

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

例如，如果想要将主机配置文件限定条件添加到需要主机运行 UNIX 的流量量变曲线，而非构建使用 OR 操作符连接的多个条件，请使用以下步骤。

**过程**

**步骤 1** 在构建流量量变曲线或主机配置文件限定条件时，选择 **is in** 或 **is not in** 作为运算符。
下拉列表会更改至文本字段。

**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。

**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)**。

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。