自定义表格

以下主题介绍如何使用自定义表：

自定义表简介

Firepower 系统收集有关网络的信息时， 防火墙管理中心 会将这些信息存储在一系列数据库表中。当您使用工作流程查看生成的信息时，防火墙管理中心会从其中一个表提取数据。例如，“按计数统计的网络应用”工作流程的每个页面的列取自“应用”表中的字段。

如果您确定通过组合不同表中的字段会增强对网络上活动的分析，则可创建自定义表。

请注意，您可以为预定义表或自定义表创建自定义工作流程。

预定义的自定义表

自定义表包含两个或多个预定义表中的字段。Firepower 系统随附多个系统定义的自定义表，但是，您可以创建其他仅包含符合自身特定需求的信息的自定义表。

例如，Firepower 系统随附用于将入侵事件数据与主机数据相关联的系统定义的自定义表，因此，您可以搜索会影响关键系统的事件并在一个工作流程中查看搜索结果。

在多域部署中，预定义的自定义表属于全局域，不能在低层域中进行修改。

下表介绍系统随附的自定义表。

表 *1:* 系统定义的自定义表

表	说明
主机及服务器 (Hosts with Servers)	包含“主机”(Hosts) 和服务器 (Servers) 表中的字段，提供有关检测到的在网络上运行的应用的信息，以及有关运行这些应用的主机的基本操作系统信息。

可能的表组合

创建自定义表时，可以组合具有相关数据的预定义表中的字段。下表列出了可用来组合创建新自定义表的预定义表。请记住，创建的自定义表也可以组合两个以上预定义自定义表中的字段。

表 *2:* 自定义表组合

可以将这些表中的字段...	与这些表中的字段进行组合...
应用	• 相关事件 • 入侵事件 • 连接摘要数据 (Connection Summary Data) • 主机属性 (Host Attributes) • 应用详情 • 发现事件 (Discovery Events) • 主机数 • 服务器 • 允许 列出事件
相关事件	• 应用 • 主机属性 (Host Attributes) • 主机数
入侵事件	• 应用 • 主机属性 (Host Attributes) • 主机数 • 服务器

可以将这些表中的字段...	与这些表中的字段进行组合...
连接摘要数据 (Connection Summary Data)	• 应用 • 主机属性 (Host Attributes) • 主机数 • 服务器
主机危害表现	• 应用 • 应用详细信息 • 捕获的文件 • 连接摘要数据 (Connection Summary Data) • 相关事件 • 发现事件 (Discovery Events) • 主机属性 (Host Attributes) • 主机数 • 入侵事件 • 安全情报事件 • 服务器 • 允许 列出事件
主机属性 (Host Attributes)	• 应用 • 相关事件 • 入侵事件 • 连接摘要数据 (Connection Summary Data) • 应用详情 • 发现事件 (Discovery Events) • 主机数 • 服务器 • 允许 列出事件

可以将这些表中的字段...	与这些表中的字段进行组合...
应用详情	• 应用 • 主机属性 (Host Attributes) • 主机数
发现事件 (Discovery Events)	• 应用 • 主机属性 (Host Attributes) • 主机数
安全情报事件	• 应用 • 主机属性 (Host Attributes) • 主机数 • 服务器
主机数	• 应用 • 相关事件 • 入侵事件 • 连接摘要数据 (Connection Summary Data) • 主机属性 (Host Attributes) • 应用详情 • 发现事件 (Discovery Events) • 服务器 • 允许 列出事件
服务器	• 应用 • 入侵事件 • 连接摘要数据 (Connection Summary Data) • 主机属性 (Host Attributes) • 主机数

可以将这些表中的字段...	与这些表中的字段进行组合...
允许 列出事件	• 应用 • 主机属性 (Host Attributes) • 主机数

有时，一个表中的字段会映射到另一个表中的多个字段。

创建新的自定义表时，系统会自动创建显示表中所有列的默认工作流程。此外，如同预定义表一样，您可以搜索自定义表来获取要在网络分析中使用的数据。您还可以根据自定义表生成报告，就像使用预定义表时一样。

用户定义的自定义表

提示 可以从另一个防火墙管理中心导出自定义表，然后将其导入到您的防火墙管理中心，而不是创建新的自定义表。

要创建自定义表，请确定哪些预定义表含有要在自定义表中包含的字段。然后，可以选择要包含的字段，如有必要，请为所有公共字段配置字段映射。

提示 借助涉及“主机”(Hosts) 表的数据，可以查看与来自一台主机的所有 IP 地址而不是一个特定 IP 地址相关的数据。

例如，不妨考虑将“关联事件”(Correlation Events) 表和“主机”(Hosts) 表中的字段组合起来以创建自定义表。通过这样的自定义表，您可以获取有关涉及任何关联策略违例的主机的详细信息。请注意，您必须决定从“主机”(Hosts) 表显示与“关联事件”(Correlation Events) 表中的源 IP 地址还是目标 IP 地址匹配的数据。

如果查看此自定义表的事件表视图，则它会显示相关性事件（每行一个）。可以将自定义表配置为包含以下信息：

- 事件的生成日期和时间
- 违例的关联策略的名称
- 触发违例的规则的名称
- 与相关性事件中涉及的源主机（又称为发起主机）相关的 IP 地址
- 源主机的 NetBIOS 名称
- 源主机运行的操作系统和版本
- 源主机的关键性

提示 可以创建类似的自定义表来显示目标主机（又称为响应主机）的以上信息。

创建自定义表

过程

步骤 1 选择**分析** > **高级** > **自定义表**。

步骤 2 点击 **Create Custom Table**。

步骤 3 在**名称 (Name)** 字段中，输入自定义表的名称。

示例：

例如，您可输入 `Correlation Events with Host Information (Src IP)`。

步骤 4 从**表 (Tables)** 下拉列表中，选择**关联事件 (Correlation Events)**。

步骤 5 在 **字段 (Fields)** 下，选择 **时间 (Time)** 并点击 **添加 (Add)** 以添加生成关联事件的日期和时间。

步骤 6 重复第 5 步以添加**策略 (Policy)** 和**规则 (Rule)** 字段。

提示
按住 Ctrl 或 Shift 键并点击可选择多个字段。也可以点击并拖动以选择多个相邻值。但是，如果要指定字段在与表关联的事件表视图中的出现顺序，请一次添加一个字段。

步骤 7 从**表 (Tables)** 下拉列表中，选择**主机 (Hosts)**。

步骤 8 向自定义表添加 **IP 地址 (IP Address)**、**NetBIOS 名称 (NetBIOS Name)**、**OS 名称 (OS Name)**、**OS 版本 (OS Version)** 和**主机重要性 (Host Criticality)** 字段。

步骤 9 在**通用字段 (Common Fields)** 下的**关联事件 (Correlation Events)** 旁边，选择**源 IP (Source IP)**。

这样，自定义表即配置为显示在第8步中选择的有关相关性事件中涉及的源主机（又称为发起主机）的主机信息。

提示
可以按照以上步骤创建显示有关相关性事件中涉及的目标主机（又称为响应主机）的主机详细信息的自定义表，但在操作过程中应选择**目标 IP (Destination IP)** 而不是**源 IP (Source IP)**。

步骤 10 点击**保存**。

修改自定义表

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

过程

步骤 1 选择**分析** > **高级** > **自定义表**。

步骤 2 点击要编辑的表旁边 **编辑** (✎) 。

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。

步骤 3 或者，点击要删除的字段旁边的 **删除** (🗑) ，从表中删除字段。

注释
如果删除报告中当前正在使用的字段，则系统将提示您确认是否要删除使用这些报告中的这些字段的部分。

步骤 4 根据需要进行其他更改。

步骤 5 点击**保存**。

删除自定义表

在多域部署中，系统会显示在当前域中创建的自定义表，您可以对其进行删除。系统还会显示在祖先域中创建的自定义表，您不可以对其进行删除。要删除较低域中的自定义表，请切换至该域。

过程

步骤 1 选择**分析** > **高级** > **自定义表**。

步骤 2 点击要删除的自定义表旁边的 **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。

根据自定义表查看工作流程

创建自定义表时，系统会自动为其创建默认工作流程。默认工作流程的第一页显示事件表视图。如果在自定义表中包含入侵事件，则工作流程的第二页是数据包视图。否则，工作流程的第二页是主机页面。您也可以根据自定义表创建自己的自定义工作流程。

提示 根据某个自定义表创建自定义工作流程后，可以将创建的自定义工作流程指定为该自定义表的默认工作流程。

您可以使用相同方法查看自定义表中根据预定义表用于事件视图的事件。

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

过程

步骤 1 选择**分析** > **高级** > **自定义表**。

步骤 2 点击与要查看的工作流程有关的自定义表旁边的 **视图** () 。

搜索自定义表

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

过程

步骤 1 选择**分析** > **高级** > **自定义表**。

步骤 2 点击要搜索的自定义表旁边的 **视图** () 。

提示
要使用不同的工作流程（包括自定义工作流程），请点击工作流程标题旁边的（**切换工作流程**）**([switch workflow])**。

步骤 3 点击 **Search**。

提示
要在数据库中搜索不同类型的事件或数据，请从表下拉列表中进行选择。

步骤 4 在相应的字段中输入搜索条件。

如果您输入多个字段的条件，搜索只返回符合所有字段指定搜索条件的记录。

提示
点击搜索字段旁边的 **对象** （+） 可将对象用作搜索条件。

步骤 5 如果您计划保存搜索，也可以选中**私有 (Private)** 复选框将搜索另存为私有，这样就只有您可以访问它。否则，请清除此复选框，将搜索保存为适用于所有用户。

提示
如想要使用搜索作为对自定义用户角色的数据限制，**必须**将其另存为私有搜索。

步骤 6 或者，您可以保存搜索，以备以后使用。您有以下选择：

- 点击 **Save**，保存搜索条件。如果选中**私有 (Private)** 复选框，则该搜索只对您的帐户显示。
- 点击 **Save As New** 可保存新搜索或通过修改之前保存的搜索为您已创建的搜索指定名称。如果选中**私有 (Private)** 复选框，则该搜索保存成功并只对您的帐户显示。

步骤 7 点击**搜索 (Search)** 开始搜索。

搜索结果显示在自定义表的默认工作流程中，通过当前时间范围（如适用）进行约束。

自定义表的历史记录

功能	防火墙管理中心最低版本	最低版本	详细信息
删除了对自定义表中连接事件的支持	6.6	任意	您无法再创建包含连接事件的自定义表。 如果您升级到版本 6.6：包含连接事件的现有表将被列为已弃用，并且不会显示任何数据，并且您无法导出或编辑这些表。现有报告、自定义工作流程和控制面板可能包括已弃用的表；您可能需要查看这些内容。 修改了屏幕：**分析 (Analysis)** > **高级 (Advanced)** > **自定义表 (Custom Tables)** 以及用于添加或编辑自定义表的页面。 受影响的平台： 防火墙管理中心

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。