报告

以下主题介绍如何在 Firepower 系统中使用报告：

报告的要求和前提条件

型号支持

任何。

支持的域

任意

用户角色

- 管理员
- 维护用户 （仅风险报告）
- 安全分析师

报告简介

Firepower 系统提供两种类型的报告：

- 风险报告， 第 2 页 — 在您的网络上发现的风险的高级摘要。

- 标准报告，第 3 页 — 关于您的 Firepower 系统的所有方面的详细可自定义报告。

风险报告

风险报告是对组织中发现的风险的可移植、高级别、易于解释的摘要。您可以使用这些报告与无权访问您的系统以及可能不是网络安全专家的人员共享有关风险区域的信息以及处理这些风险的建议。这些报告旨在促进对网络安全投资领域的讨论。

风险报告模板

- **高级恶意软件风险报告**
- **攻击风险报告**。以下是此报告中的字段：
  - **攻击总数**-IPS 事件总数。
  - **相关攻击**-影响标志等于 1 的 IPS 事件的数量。
  - **目标主机**-IPS 事件中影响标志等于 1 的唯一目标 IP 地址的数量。
  - **无关攻击**-影响标志不等于 1 的 IPS 事件的百分比。
  - **需要注意的事件**-影响标志为 1 的 IPS 事件的百分比。
  - **连接到 CnC 服务器的主机**-IOC 类别为 “已连接 CnC”的唯一主机的总数。
- **网络风险报告**

生成、查看和打印风险报告

标准报告模板不适用于风险报告。

报告与当前域相关。

每个风险报告生成为 HTML 文件。

要安排风险报告生成，请参阅自动执行报告生成。

开始之前

- 确保将您的系统配置为检测要总结的风险。
- 如果要通过邮件传送报告且尚未配置中继主机，则可以立即执行此操作。有关信息，请参阅配置邮件中继主机和通知地址。

过程

步骤 1 选择**概述** > **报告**。

步骤 2 点击 **报告模板 (Report Templates)**。

步骤 3 点击所需报告的 **生成报告** 。

步骤 4 输入信息。

- 在“输入参数”(Input Parameters) 部分中输入的信息将显示在报告的标题页面上。您可以将这些字段留空。

步骤 5 点击**生成 (Generate)**。

步骤 6 点击**确定**。

下一步做什么

- 要查看、下载、移动或删除风险报告，请参阅关于使用生成的报告 ， 第 24 页。
- 可以从大多数受支持的浏览器将任何风险报告打印为 PDF。要获得最佳效果，请在浏览器的打印或打印预览设置中启用背景色、图像以及页眉和页脚（可选）。支持的页面大小为 A4 和美国信纸大小。

标准报告

系统提供一个灵活的报告系统，能够利用 防火墙管理中心上显示的事件视图或控制面板快速而轻松地生成多部分报告。还可以从头设计自定义报告。

报告是一种采用 PDF、HTML 或 CSV 格式的文档文件，其包含要传达的内容。报告模板指定报告及其各部分的数据搜索和格式。系统内有一个功能强大的报告设计器，用于自动执行报告模板的设计。可以复制 Web 界面中显示的任何活动视图表或控制面板图形的内容。

可以根据需要的数量创建报告模板。每个报告模板均可定义报告中的各个部分，并指定创建报告内容的数据库搜索，以及演示文稿格式（表、图表，详细视图等等）和时间范围。模板还指定文档属性，例如封面和目录以及文档页面是否有页眉和页脚（仅适用于 PDF 格式的报告）。可以将报告模板导出到单个的配置包文件中，然后再导入，以便在其他 防火墙管理中心上重复使用。

在模板中可以加入输入参数，以扩展其实用性。使用输入参数，可以对相同报告进行定制化变动。当使用输入参数生成报告时，生成过程会提示输入每个输入参数的值。键入的值对报告内容的限制是一次性的。例如，在生成入侵事件报告的搜索“目标 IP”字段可以放入一个输入参数；在报告生成时，可以在系统提示输入目标 IP 地址时指定部门的网段。生成的报告随后只包含该特定部门的相关信息。

关于设计报告

报告模板

使用报告模板定义报告每部分数据的内容和格式，以及报告文件的文档属性（封面、目录以及页眉和页脚）。在生成报告之后，模板仍可重复使用，直到将其删除为止。

报告包含一个或多个信息部分。为每个部分分别选择格式（文本、表或图表）。针对某部分所选的格式可能会限制其可包含的数据。例如，使用饼图格式，无法显示某些表中基于时间的信息。可以随时更改部分的数据条件或格式，以获得最佳演示效果。

可以在预定义的事件视图基础上完成报告的初始设计，也可以通过从任何定义的控制面板、工作流程或摘要导入内容开始设计。还可以从空的模板开始添加部分并逐一定义其属性。

注释 在多域部署中，可以查看但无法编辑属于祖先域的报告模板。要从这些模板生成报告，必须将它们复制到当前的域。

报告模板字段

下表列出可以用来构建报告模板组成部分的字段。并非所有字段都会在所有类型的部分中使用；选择一个部分所采用的格式后，系统会显示相应的字段。

字段名称	部分类型	定义
格式	n/a	选择部分数据所采用的格式： **条形图**（）：比较所选变量的数量。 **折线图**（）：显示所选变量随时间推移的趋势/更改。仅适用于基于时间的表。 **饼图**（）：将每个所选变量显示为总体的百分比。数量为零的变量不在图表中显示。极少的数量归到标记为 **Other** 的类别。 **表视图**（）：显示每个记录的属性值。不适用于摘要或统计数据。 **详细信息视图**（）：显示与特定事件相关联的复杂对象数据，例如数据包（用于入侵事件）和主机配置文件（用于主机事件）。此格式仅适用于涉及此类对象的事件类型。如果请求的数量很大，输出可能会降低性能。
表	全部	选择从其提取部分数据的表。
预设	全部	预定义的搜索。在定义新的搜索时，请选择合适的预设初始化搜索条件。
Search 或 Filter	全部	对于大多数表，可使用预定义的或保存的 **Search** 限制报告。您还可以通过点击 **编辑** () 来创建新搜索。 对于“应用统计信息”(Application Statistics) 表，使用用户定义的应用**过滤器**限制报告。

字段名称	部分类型	定义
X 轴	条形图 折线图 饼图	所选图表的 X 轴的可用数据。 对于折线图，X 轴值始终是 **Time**。对于条形图和饼图，则不能选择 **Time** 为 X 轴值。
Y 轴	条形图 折线图 饼图	所选图表的 Y 轴的可用数据。
部分说明	全部	位于部分中的搜索数据前面的描述性文本。 输入文本和输入参数组合。新部分的默认设置是 `$<Time Window>` 和 `$<Constraints>`。
时间窗口	全部	部分中显示的数据的时间窗口。 如果部分搜索基于时间的表，可以选择复选框以继承报告的全局时间窗口。或者，可以为部分设置特定时间窗口。
数据源	所有 (All)	如果使用向导配置 Security Analytics and Logging（本地部署）使用的远程（外部）数据存储，则可以选择用于连接和安全智能事件的数据源。 选项如下： • **自动**：显示 FMC 上存储的数据（如果可用）。如果 FMC 上的数据在整个所选时间段内不可用，则仅显示远程存储的数据。 • **本地**：仅显示存储在 FMC 上的数据，无论选择的时间段如何。 选择此选项以包括远程卷上不可用的数据，例如从未配置为将事件发送到远程卷的设备生成的事件。 • **扩展**：仅显示存储在远程卷上的数据。
最大结果数	表格视图 详细信息视图	要包括的匹配记录最大数。 与 CSV 或 HTML 报告相比，PDF 报告可以包括更少的记录。如果数量太大，Web 界面将通过警告和错误图标加以指示。将鼠标指针悬停在图标上可查看限制。
结果	条形图 饼图	选择**顶部**或**底部**并输入构建图表所用的匹配记录数。
颜色	条形图 折线图	部分中绘制数据的颜色。

报告模板创建

报告模板是各部分的框架，每个部分通过自己的数据库查询独立构建。

您可以通过创建新模板，使用现有模板，将模板基于事件视图，或者导入控制面板或工作流程来构建新的报告模板。

如果不想复制现有报告模板，可以创建一个全新模板。创建模板的第一步是生成用于添加和格式化各部分的框架。然后，按照希望的顺序设计各个模板部分并设置报告文档的属性。

每个模板部分均包括由搜索或过滤器生成的数据集，且具有确定展现方式的格式规格（表、饼图等）。通过选择要在输出中包含的数据记录中的字段，以及要显示的时间范围和记录数量，进一步确定部分内容。

注释 使用部分预览实用程序可检查列选择和饼图颜色等输出特性。但这并不能可靠地表明配置的搜索是否正确。

从模板生成的报告具有多个覆盖所有部分和控制功能的文档属性，例如封面、页眉和页脚、页码等。

请注意，如果选择 CSV 作为文档格式，则无需设置文档属性。

如果在现有模板中找到理想模型，则可以复制模板并编辑其属性以创建新报告模板。思科还提供一组在模板列表中的**报告 (Reports)** 选项卡上可视的预定义报告模板。

从事件视图中，可以创建报告模板并将其修改为满足您的需求。可以添加更多部分、修改自动包含的部分和删除各部分。

通过导入控制面板、工作流程和统计摘要，可以快速创建新的报告。导入会为控制面板中的每个构件图形以及工作流程中的每个事件视图都创建一个部分。为重点显示最重要的信息，可以删除任何不必要的部分。

创建自定义报告模板

过程

步骤 1 选择**概述** > **报告**。

步骤 2 点击 **报告模板 (Report Templates)**。

步骤 3 点击 **Create Report Template**。

步骤 4 在**报告标题**字段中输入新模板的名称。

步骤 5 要向报告标题添加输入参数，请将光标置于应显示参数值的标题中，然后点击插入**输入参数**（+）。

步骤 6 根据需要，使用“报告部分”标题栏下的一组添加来插入部分。

步骤 7 配置部分内容，如报告模板配置，第 9 页中所述。

提示
可以点击部分窗口底部的**预览 (Preview)**，查看所选择的列布局或图形格式。

步骤 8 点击**高级 (Advanced)**，设置 PDF 和 HTML 报告的属性，如报告模板中的文档属性，第 17 页中所述。

步骤 9 点击**保存**。

如果看到一条错误，请查找每部分中结果值旁边的黄色三角形。如果看到任何此类三角形，请执行以下任一操作：

- 对于显示黄色三角形的每个字段，将鼠标指针悬停在三角形上方，并将结果数量减少到指示的数字。
- 点击**生成**，并包括 PDF 之外的输出格式。

从现有模板创建报告模板

过程

步骤 1 选择**概述** > **报告**。

步骤 2 点击 **报告模板 (Report Templates)**。

步骤 3 点击要复制的报告模板旁边的 **复制** ( ) 。

步骤 4 在**报告标题 (Report Title)** 字段中，输入名称。

步骤 5 根据需要对模板进行更改。

步骤 6 点击**保存**。

从事件视图创建报告模板

过程

步骤 1 在事件视图中填入要在报告中显示的事件：

- 使用事件搜索定义要查看的事件。
- 深入查找工作流程，直到在事件视图中获得相应的事件。

步骤 2 从事件视图页面中，点击**创建报告 (Create Report)**。

“报告部分”(Report Sections) 页面为已捕获工作流程中的每个视图显示一个部分。

步骤 3 或者，在**报告标题**字段中输入新名称并点击**保存**。

步骤 4 您可以执行以下操作：

- 添加封面、目录、开始页码或页眉和页脚文本 - 点击 **高级** 设置。
- 添加分页符 - 点击 **添加分页符**（ ），并将新分页符对象从模板底部拖动到应该开始新页面的那个部分的前面。
- 添加文本部分 - 点击 **添加文本部分**（ ），并将新文本部分从模板底部拖动到要在报告模板中显示的位置。
- 更改某个部分的标题 - 点击标题栏中该部分的标题，输入部分标题，然后点击**确定 (OK)**。

- 配置报告部分 - 调整每个部分中的字段设置。

  提示
  要查看某一部分的当前列布局或图表格式，请点击该部分的 **Preview** 链接。

- 从报告中排除模板部分 - 点击该部分标题栏中的 **删除** (✕) 并确认删除。

  注释
  有些工作流程中，报告的最后部分包含显示数据包、主机配置文件或漏洞的详细视图，具体视工作流程而定。生成报告时使用这些详细视图检索大量事件，可能会影响 防火墙管理中心的性能。

步骤 5 点击**保存**。

通过导入控制面板或工作流程创建报告模板

过程

步骤 1 确定要在报告中复制的控制面板、工作流程或摘要。

步骤 2 选择**概述** > **报告**。

步骤 3 点击 **报告模板 (Report Templates)**。

步骤 4 点击 **Create Report Template**。

步骤 5 在**报告标题 (Report Title)** 字段中输入新报告模板的名称。

步骤 6 点击**保存**。

步骤 7 点击 **导入部分** （）。可以选择导入报告部分的数据源选项， 第 9 页中所述的任何数据源。

步骤 8 从下拉菜单中选择控制面板、工作流程或摘要。

步骤 9 对要添加的数据源，点击**导入**。

对于控制面板，每个构件图形都有自己的部分；对于工作流程，每个事件视图都有自己的部分。

步骤 10 根据需要更改各部分的内容。

注释
有些工作流程中，报告的最后部分包含显示数据包、主机配置文件或漏洞的详细视图，具体视工作流程而定。生成报告时使用这些详细视图检索大量事件，可能会影响 防火墙管理中心的性能。

步骤 11 点击**保存**。

导入报告部分的数据源选项

表 *1:* 导入报告部分窗口上的数据源选项

选择的选项	导入内容
导入控制面板 (Import Dashboard)	所选控制面板上的任何自定义分析构件。
导入工作流程 (Import Workflow)	任何预定义或自定义的工作流程。 选项具有以下格式： `Table - Workflow name` 例如，`Connection Events - Traffic by Port` 可导入从“连接事件”(Connection Events) 表生成的“按端口划分的流量”(Traffic by Port) 工作流程中的视图。
导入摘要部分 (Import Summary Sections)	以下任意一种通用摘要： • 入侵详细摘要 • 入侵简要摘要 • 发现详细摘要 • 发现简要摘要

报告模板配置

创建报告模板后，可以进行修改和自定义。可以通过修改各种报告部分属性调整部分的内容及其数据展示。

报告模板中的各部分通过查询数据库表生成该部分的内容。更改部分的数据格式使用相同的数据查询，但会根据格式类型的分析用途修改部分中显示的字段。例如，入侵事件的表视图在部分中填入每个事件记录的大量数据字段，而饼图部分则显示各个选定属性代表的所有匹配记录的比例，不显示单个事件的详细信息。条形图部分比较具有特定属性的匹配记录总数。折线图就单个属性总结匹配记录随时间推移的变化。折线图仅适用于基于时间的数据，不适用于有关主机、用户和第三方漏洞等信息。

报告部分中的搜索或过滤器指定部分内容所基于的数据库查询。对于大多数表，可以使用预定义或保存的搜索来限定报告，也可以即时创建新的搜索：

- 预定义的搜索作为示例用于搜索特定事件表，并可以对可能想要在报告中包含的重要网络信息提供快速访问。
- 保存的事件搜索包括您或他人已创建的全部公共事件搜索，以及所有保存的私密事件搜索。
- 只有在报告模板本身中才能实现当前报告模板的保存搜索。已保存报告模板搜索的搜索名称以字符串“Custom Search”结尾。用户在设计报告时创建这些搜索。

对于“应用统计信息”(Application Statistics) 表，使用用户定义的应用过滤器限制报告。

如果在部分中包括表数据，则可以选择要显示数据记录中的哪些字段。表中所有字段都可以包括或排除。选择实现报告用途的字段，然后进行相应的排列和排序。

可以向模板添加文本部分以提供自定义文本，例如，整个报告或各部分的简介。

在模板中，可以在任何部分的前面或后面添加分页符。此功能尤其适用于多部分报告，其具有介绍各个部分的文本页面。

报告模板的时间段定义模板的报告周期。

注释 安全分析人员仅可以编辑由其创建的报告模板。在多域配置中，无法从祖先域编辑报告模板，但是可以复制以创建后代版本。

设置报告模板部分的表和数据格式

过程

步骤 1 点击**概述 (Overview)** > **报告 (Reporting)** > **报告模板 (Report Templates)** > **创建报告模板 (Create Report Template)**。

步骤 2 在报告模板部分，使用**表 (Table)** 下拉菜单选择要查询的表。

格式 字段显示适用于所选表的每个输出格式。

步骤 3 选择相关部分适用的输出格式。

步骤 4 要更改搜索限制，请点击 **搜索** 或 **过滤器** 字段旁边的 **编辑** (✎) 。

步骤 5 对于图形输出格式（饼图、条形图等），请使用下拉菜单调整 **X-Axis** 和 **Y-Axis** 参数。

当为 X 轴选择值时，只有相对应的值才显示在 Y 轴下拉菜单中，反之亦然。

步骤 6 对于表输出，请在输出中选择列、显示顺序和排序顺序。

步骤 7 点击**保存**。

相关主题

报告模板字段，第 4 页

为报告模板部分指定搜索或过滤器

过程

步骤 1 在报告模板部分中，从**表 (Table)** 下拉菜单中选择要查询的数据库表：

- 对于大多数表，显示**搜索 (Search)** 下拉列表。
- 对于“应用统计信息”(Application Statistics) 表，显示**过滤器 (Filter)** 下拉列表。

步骤 2 选择要用于限制报告的搜索或过滤器。

点击 **编辑** (✎)可查看搜索条件或创建新的搜索。

修改报告模板表格式部分中的字段

过程

步骤 1 对于表格式报告部分，请点击 **字段** 参数旁边的 **编辑** (✎) 图标。

步骤 2 在显示的表字段选择器对话框中，您可以执行以下操作：

- 点击列名称或列旁边的 添加＋图标可将其添加到报告。添加的列名称将填充在**选定列 (Selected Column)** 窗格中。
- 点击列旁边的 删除 ✕ 图标，从报告中删除该列。
- 根据需要，拖放**选定列 (Selected Column)** 窗格中的列以重新排列它们。
- 选择**排序方向 (Sort direction)** 并设置列的**排序优先级 (Sort priority)**，以修改数据的排序顺序。

步骤 3 点击**确定**。

向报告模板添加文本部分

文本部分可包含使用多种字体大小和样式（如粗体、斜体等）的富文本，以及输入参数和导入的图像。

提示 文本部分对于介绍报告或报告各部分非常有用。

过程

步骤 1 在报告模板编辑器中，点击 **添加文本部分**（T）。

步骤 2 将新文本部分拖放到其在报告模板的指定位置。

步骤 3 如果要将文本部分放在页面开始或末尾，请在文本部分之前或之后添加分页符。

步骤 4 如果要更改文本部分的通用名称，请点击标题栏中的部分名称并输入新名称。

步骤 5 在文本部分的正文中添加带格式的文本和图像。

可以包括在生成报告时动态更新的输入参数。

步骤 6 点击**保存**。

相关主题

输入参数，第 14 页

向报告模板添加分页符

过程

步骤 1 在报告模板编辑器中，点击 **添加分页符**（）。

分页符显示在模板的底部。

步骤 2 将分页符拖放到部分前面或后面的指定位置。

步骤 3 点击**保存**。

全局时间窗口与报告模板部分

包含基于时间的数据的报告模板（例如，入侵或发现事件）具有全局时间窗口，默认情况下，模板中基于时间的部分创建时会继承该时间窗口。更改全局时间窗口会更改配置为继承全局时间窗口的部分的本地时间窗口。您可以通过清除**继承时间窗口 (Inherit Time Window)** 复选框来禁用单个部分的时间窗口继承。然后，您可以编辑本地时间窗口。

注释 全局时间窗口继承仅适用于具有基于时间的表数据的报告部分，例如入侵事件和发现事件。对于报告网络资产（主机和设备）和相关信息（如漏洞）的部分，必须分别设置每个时间窗口。

为报告模板及其部分设置全局时间窗口

提示 报告的每个部分可以有不同的时间范围。例如，第一部分可能是一个月度摘要，而剩余部分则可深入提供周级别的详细信息。在这些情况下，单独设置部分级别的时间窗口。

过程

步骤 1 在报告模板编辑器中，点击**生成 (Generate)**。

步骤 2 要修改全局时间段，请点击 **时间窗口** （）。

步骤 3 在 **事件时间窗口**中修改时间设置。

步骤 4 点击 **Apply**。

步骤 5 点击**生成 (Generate)** 以生成报告并点击**是 (Yes)** 进行确认。

为报告模板部分设置本地时间窗口

过程

步骤 1 在模板的“报告部分”页面上，清除该部分的**继承时间窗口**复选框（若有）。

步骤 2 要更改部分的本地时间段，请点击 **时间窗口** （）。

注释
包含统计表的数据的部分只能有滑动时间窗。

步骤 3 点击“事件时间窗口”(Events Time Window) 上的**应用 (Apply)**。

步骤 4 点击**保存**。

重命名报告模板部分

过程

步骤 1 在报告模板编辑器中，点击部分页眉中的当前部分名称。

步骤 2 为该部分输入新名称。

步骤 3 点击**确定 (OK)**。

预览报告模板部分

预览功能显示表视图的字段布局和排序顺序以及图形的重要易读特征，如饼图颜色。

过程

步骤 1 在编辑报告模板部分时，可随时点击**预览 (Preview)** 预览该部分。

步骤 2 点击**确定 (OK)** 关闭预览。

报告模板部分中的搜索

生成成功报告的关键在于定义填入报告部分的搜索。Firepower 系统提供搜索编辑器，可查看报告模板中可用的搜索以及定义新的自定义搜索。

在报告模板部分搜索

过程

步骤 1 在报告模板的相关部分中，点击 **搜索** 字段旁边的 **编辑** (✎) 。

步骤 2 如果要根据预定义搜索进行自定义搜索，必须从**已保存搜索 (Saved Searches)** 下拉列表中选择预定义搜索。

此列表包含此表格的所有可用预定义搜索，包括系统范围和报告特定的预定义搜索。

步骤 3 在相应的字段中编辑搜索条件。

对于某些字段，限制可以包含与事件搜索相同的运算符（<、<>等）。如果输入多个条件，则搜索只返回与所有条件匹配的记录。

步骤 4 如果要从下拉菜单插入输入参数，而不是输入限制值，则必须点击 **输入参数**（＋）。

注释
在编辑报告搜索的限制时，系统会使用以下名称保存已编辑的搜索：*section* `custom search`，其中 *section* 是部分标题栏中的名称，后跟字符串 `custom search`。要使保存的自定义搜索具有有意义的名称，请确保更改部分名称后再保存编辑的搜索。无法重命名已保存的报告搜索。

步骤 5 点击 **OK**。

输入参数

在报告模板中可以使用输入参数，使报告可以在生成时自动更新。 **输入参数**（＋） 指示可处理它们的字段。有两种输入参数：

- 预定义的输入参数由内部系统功能或配置信息解析。例如，在生成报告时，系统用当前日期和时间替换 `$<Time>` 参数。
- 用户定义的输入参数提供部分搜索限制。使用输入参数限制搜索，会指示系统在生成时从请求报告的人员那里收集值。这样，可以在生成时动态地定制报告显示特定数据子集，而无需更改模板。例如，可以为报告部分搜索的**目标 IP (Destination IP)** 字段提供输入参数。然后，当生成报告时，可以输入特定部门的 IP 网段，以仅获得该部门的数据。

  还可以定义字符串类型输入参数，在报告的以下特定区域中添加动态文本，例如，邮件（主题或正文）、报告文件名和文本部分。可以为不同部门个性化设置报告，具有自定义的报告文件名、邮件地址和邮件消息，使同一模板适用一切。

预定义输入参数

表 *2:* 预定义输入参数

插入此参数.....	.....在模板中包括此信息：
`$<Logo>`	所选的上传徽标

插入此参数.....	.....在模板中包括此信息：
$<Report Title>	报告标题
$<Time>	运行报告的日期和时间，精细度为一秒
$<Month>	当前月份
$<Year>	当前年份
$<System Name>	防火墙管理中心的名称
$<Model Number>	防火墙管理中心的型号
$<Time Window>	当前应用于报告部分的时间窗口
$<Constraints>	当前应用于报告部分的搜索限制

表 *3:* 预定义输入参数的使用

参数	报告模板封面	报告模板报告标题	报告模板部分说明	报告模板文本部分	生成报告文件名	生成报告邮件主题、正文
$<Logo>	是	否	否	否	否	否
$<Report Title>	是	否	是	是	是	是
$<Time>	是	是	是	是	是	是
$<Month>	是	是	是	是	是	是
$<Year>	是	是	是	是	是	是
$<System Name>	是	是	是	是	是	是
$<Model Number>	是	是	是	是	是	是
$<Time Window>	否	否	是	否	否	否
$<Constraints>	否	否	是	否	否	否

用户定义的输入参数

使用输入参数可扩展搜索的实用性。输入参数指示系统在生成时从请求报告的人员那里收集值。这样，可以在生成时动态地限制报告显示特定数据子集，而无需更改搜索。例如，可以为深度提供部门级安全事件的报告部分的**目标 IP (Destination IP)** 字段提供输入参数。当生成报告时，可以输入特定部门的 IP 网段，以仅获得该部门的数据。

输入参数的类型确定可以使用其的搜索字段。只能在相应的字段中使用指定类型。例如，定义为字符串类型的用户参数可插入文本字段，但不可插入接受 IP 地址的字段。

定义的每个输入参数均具有名称和类型。

表 4: 用户定义的输入参数类型

将此参数类型.....	用于包含此数据的字段.....
网络/IP (Network/IP)	CIDR 格式的任何 IP 地址或网段
应用	应用协议、客户端应用或 Web 应用的名称
事件消息 (Event Message)	任何事件视图消息
设备	防火墙管理中心 或受管设备
用户名	用户身份，比如发起方用户和响应方用户
编号 (Number)（VLAN ID、Snort ID、Vuln ID）	任何 VLAN ID、Snort ID 或漏洞 ID
字符串	文本字段（如应用或操作系统版本、注释或说明）

创建用户定义的输入参数

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。
步骤 2 点击 **添加输入参数**（＋）。
步骤 3 输入参数**名称 (Name)**。
步骤 4 从**类型 (Type)** 下拉列表中选择值。
步骤 5 点击**确定 (OK)** 添加参数。
步骤 6 点击**确定 (OK)** 返回到编辑器。

编辑用户定义的输入参数

报告模板的**输入参数 (Input Parameters)** 部分列出模板的所有可用用户定义参数。

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。
步骤 2 点击要修改的参数旁边的 **编辑** (✎) 。
步骤 3 在**名称 (Name)** 中输入新名称。
步骤 4 使用**类型 (Type)** 下拉列表来更改参数类型。

步骤 5 点击 **OK**，保存更改。

步骤 6 如果要删除输入参数，请点击输入参数旁边的 **删除** (🗑) 并确认。

步骤 7 点击**确定 (OK)** 返回到报告模板编辑器。

使用用户定义的输入参数限制搜索

定义的输入参数仅适用于与其参数类型匹配的搜索字段。例如，**网络/IP (Network/IP)** 类型的参数仅适用于接受 CIDR 格式的 IP 地址或网段的字段。

过程

步骤 1 在报告模板编辑器中，点击该部分中 **搜索** 字段旁边 **编辑** (✎) 。

可接受输入参数的字段标有 **输入参数**（＋）。

步骤 2 点击字段旁边的 **输入参数**（＋），然后从下拉菜单中选择输入参数。

用户定义的输入参数标有 (🖼)。

步骤 3 点击**确定 (OK)**。

报告模板中的文档属性

在生成报告之前，可以设置影响报告外观的文档属性。这些属性包括可选封面和目录。对一些属性是否支持取决于所选的报告格式：PDF、HTML 或 CSV。

表 *5:* 文档属性支持

属性	是否支持 **PDF**?	是否支持 **HTML**?	是否支持 **CSV**?
封面页	是，具有可选徽标和自定义外观	是，具有可选徽标和自定义外观	否
目录	是	是	否
页眉和页脚	是，在任意字段中均具有可选文本或徽标	否	否
自定义开始页码	是	否	否
不显示首页页码的选项	是	否	否

编辑报告模板中的文档属性

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。

步骤 2 有以下选项可供选择：

- 添加封面 - 要添加封面，请选中**包含封面 (Include Cover Page)** 复选框。
- 自定义封面 - 要编辑封面设计，请参阅自定义封面，第 18 页。
- 添加目录 - 要添加目录，请选中**包含目录 (Include Table of Contents)** 复选框。
- 管理徽标 - 要管理与模板关联的徽标图像，请参阅管理报告模板徽标，第 18 页。
- 配置页眉和页脚 - 要指定此模板的页眉和页脚的元素，请使用**页眉 (Header)** 和**页脚 (Footer)** 字段中的下拉列表。
- 设置首页码 - 要指定报告首页的页码，请输入**页码开始 (Page Number Start)** 值。
- 显示首页码 - 要显示报告首页的页码，请选中**对首页编号？(Number First Page?)** 复选框。如果选择此选项，则封面未编号。

步骤 3 点击**确定 (OK)**，保存更改。

自定义封面

可以自定义报告模板的封面。封面可包含使用多种字体大小和样式（如粗体、斜体等）的富文本，以及输入参数和导入的图像。

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。

步骤 2 点击 **覆盖页面设计**旁边的 **编辑** (✎) 。

步骤 3 在富文本编辑器中编辑封面设计。

步骤 4 点击**确定 (OK)**。

管理报告模板徽标

可以在 防火墙管理中心上存储多个徽标，并将其与其他报告模板关联。在设计模板时设置徽标关联。如果导出模板，导出包会包含徽标。

将徽标上传到 防火墙管理中心时，该徽标可用于：

- 防火墙管理中心上的所有报告模板，或
- 在多域部署中，当前域中的所有报告模板

徽标图像可为 GIF、JPG 或 PNG 格式。

可以将报告中的徽标更改为上传到 防火墙管理中心的任何 JPG 图像。例如，如果重复使用模板，可以将另一个公司的徽标与报告关联。

可以删除任何已上传的徽标。删除徽标会将其从使用它的所有模板中都删除。删除操作无法撤消。请注意，不能删除预定义思科徽标。

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。

当前与模板相关联的徽标显示在 **General Settings** 中的 **Logo** 下。

步骤 2 点击徽标旁边的 **编辑** (✎) 。

步骤 3 有以下选项可供选择：

- 添加 - 添加新徽标，如添加新徽标 ， 第 19 页中所述。
- 更改 - 更改报告模板的徽标，如更改报告模板的徽标 ， 第 19 页中所述。
- 删除 - 删除徽标，如删除徽标 ， 第 20 页中所述。

添加新徽标

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。

步骤 2 点击 **徽标** 字段旁边的 **编辑** (✎) 。

步骤 3 点击 **Upload Logo**。

步骤 4 点击 **浏览**，浏览至文件的位置，然后点击 **打开**。

步骤 5 点击**上传**。

步骤 6 如果要将新徽标与当前模板关联，请选择当前模板，然后点击**确定 (OK)**。

更改报告模板的徽标

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。

步骤 2 点击 **徽标** 字段旁边的 **编辑** (✎) 。

步骤 3 从“选择徽标”(Select Logo) 对话框中，选择要与报告模板关联的徽标。

步骤 4 点击**确定 (OK)**。

删除徽标

过程

步骤 1 在报告模板编辑器中，点击**高级 (Advanced)**。

步骤 2 点击 **徽标** 字段旁边的 **编辑** (✎) 。

步骤 3 从“选择徽标”(Select Logo) 对话框中，选择要删除的徽标。

步骤 4 点击 **Delete Logo**。

步骤 5 点击**确定 (OK)**。

管理报告模板

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

您必须是管理员用户才能执行此任务。

过程

步骤 1 选择**概述** > **报告**。

步骤 2 点击 **报告模板 (Report Templates)**。

步骤 3 有以下选项可供选择：

- 删除 - 在要删除的模板旁边，点击 **删除** (🗑) 并确认。

  不能删除系统提供的报告模板。安全分析人员仅可删除由其创建的报告模板。在多域部署中，仅可以删除属于当前域的报告模板。

- 编辑 - 要编辑报告模板，请参阅编辑报告模板 ， 第 20 页。
- 导出 - 要导出报告模板，请参阅导出报告模板 ， 第 21 页。

  提示
  也可以使用标准配置导出过程导出报告模板；请参阅导出配置。

- 导入 - 要导入报告模板，请参阅导入配置。

编辑报告模板

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

过程

步骤 1 选择**概述** > **报告**。

步骤 2 点击 **报告模板 (Report Templates)**。

步骤 3 点击要编辑的模板的 **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 4 有以下选项可供选择：

- 添加分页符；请参阅向报告模板添加分页符 ， 第 12 页。
- 添加文本部分；请参阅向报告模板添加文本部分 ， 第 11 页。
- 配置部分内容，如报告模板配置 ， 第 9 页中所述。
- 创建输入参数；请参阅创建用户定义的输入参数 ， 第 16 页。
- 编辑输入参数；请参阅编辑用户定义的输入参数 ， 第 16 页。
- 编辑文档属性；请参阅编辑报告模板中的文档属性 ， 第 18 页。
- 搜索模板部分；请参阅在报告模板部分搜索 ， 第 14 页。
- 通过点击**高级 (Advanced)** 来设置文档属性，如报告模板中的文档属性 ， 第 17 页中所述。
- 设置全局时间窗口；请参阅为报告模板及其部分设置全局时间窗口 ， 第 12 页。
- 设置本地时间窗口；请参阅为报告模板部分设置本地时间窗口 ， 第 13 页。
- 设置搜索字段；请参阅修改报告模板表格式部分中的字段 ， 第 11 页。
- 设置表和数据格式；请参阅设置报告模板部分的表和数据格式 ， 第 10 页。
- 指定搜索和过滤器；请参阅为报告模板部分指定搜索或过滤器 ， 第 10 页。

导出报告模板

您必须是管理员用户才能执行此任务。

过程

步骤 1 选择**概述** > **报告**。

步骤 2 选择 **报告模板**。

步骤 3 点击要导出的模板的 **导出** 图标。

关于生成报告

生成报告

创建并自定义报告模板后，便可生成报告了。在生成过程中，可以选择报告格式（HTML、PDF 或 CSV）。还可以调整报告的全局时间段，它对所有部分应用一致的时间范围，但您排除的时间范围除外。

PDF 报告：

- 不支持使用 Unicode (UTF-8) 字符的文件名。
- 包含特殊 Unicode 文件名（例如，文件或恶意活动中显示的那些文件名）的任何报告部分将以转换形式显示这些文件名。
- 在每个报告部分配置的结果数必须接受某些限制。要查看这些限制，请将鼠标指针移至报告模板中显示的任意黄色三角形上。

如果报告模板的搜索规格中包括用户输入参数，生成过程会提示输入值，将报告的这次运行定制为数据的一个子集。

如已配置 DNS 服务器且启用 IP 地址解析，则当解析成功时，报告包含主机名。

在多域部署中，如果在祖先域中生成报告，该报告可包括来自所有后代域的结果。要为特定叶域生成报告，请切换至该域。

过程

步骤 1 选择**概述** > **报告**。

步骤 2 点击 **报告模板 (Report Templates)**。

步骤 3 点击要用于生成报告的模板旁边的 **报告** ( ) 。

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。

提示
要从祖先模板生成报告，请将该模板复制到当前域。

步骤 4 或者，也可以配置报告名称：

- 输入新的**文件名 (File Name)**。如果不输入新名称，系统将使用报告模板中指定的名称。
- 使用 **输入参数**（＋） 向文件名添加一个或多个输入参数。

步骤 5 通过点击，选择报告的输出格式：HTML、PDF 或 CSV。

如果 PDF 选项显示为灰色，说明在一个或多个报告部分中配置的结果数量可能太高。有关特定限制，请查找报告模板中的黄色三角形并将鼠标指针悬停在所查找的任意黄色三角形上。

步骤 6 如果要更改全局时间段，请点击 **时间窗口** （ ）。

注释

只有当单个报告部分配置为继承全局设置时，设置全局时间段才会影响单个报告的内容。

步骤 7 为**输入参数 (Input Parameters)** 部分中显示的任何字段输入值。

提示
通过在字段中键入 * 通配符，可以忽略用户参数。这会消除对搜索的用户参数限制。

注释
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地址或VLAN标记限制报告结果可能会出现意外结果。

步骤 8 如果在 防火墙管理中心配置中启用了邮件中继主机，点击**邮件**可在报告生成时自动通过邮件传送报告。

步骤 9 点击**生成**，并在显示提示时进行确认。

点击**生成**会保存报告模板的“生成”设置。

如果点击**关闭 (Close)**，则只会在会话持续期间保存您所做的选择。

步骤 10 有以下选项可供选择：

- 点击报告链接以在新窗口中显示该报告。
- 点击**确定 (OK)** 返回到报告模板编辑器。

报告生成选项

可以配置报告生成选项来执行以下操作：

- 安排生成未来报告，可以是一次报告也可以是循环报告。请参阅自动执行报告生成。可以在每日、每周和每月等全程时间范围上自定义计划。
- 使用调度程序分发邮件报告。必须在计划任务**之前**配置报告模板和邮件中继主机。
- 当生成报告时，将报告作为邮件附件自动发送到收件人列表。必须具有适当配置的邮件中继主机，才能通过邮件传送报告。
- 将新生成的报告文件保存到所配置的远程存储位置。要使用远程存储，必须先配置远程存储位置。

注释 如果在远程存储后又切换回本地存储，则远程存储中的报告不在“报告”(Reports)选项卡列表上显示。同样地，如果从一个远程存储位置切换到另一个远程存储位置，则前一个位置中的报告不在列表中显示。

在生成时通过邮件分发报告

过程

步骤 1 选择**概述** > **报告**。

步骤 2 点击 **报告模板 (Report Templates)**。

步骤 3 点击要用于生成报告的模板旁边的 **报告** ( ) 。

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。

提示
要从祖先模板生成报告，请将该模板复制到当前域。

步骤 4 展开窗口的**邮件 (Email)** 部分。

步骤 5 在**邮件选项 (Email Options)** 字段中，选择**发送邮件 (Send Email)**。

步骤 6 在**收件人列表 (Recipient List)**、**CC** 和 **BCC** 字段中，输入逗号分隔列表形式的收件人电子邮件地址。

步骤 7 在**主题 (Subject)**字段中，输入邮件主题。

提示
可以在**主题 (Subject)** 和邮件正文中提供输入参数，以动态生成邮件中的信息，例如时间戳或防火墙管理中心名称。

步骤 8 根据需要在邮件正文中输入附函。

步骤 9 点击**确定 (OK)** 并确认。

相关主题
配置邮件中继主机和通知地址

安排未来报告

请参阅自动执行报告生成。

关于使用生成的报告

在“报告”(Reports) 选项卡页面上访问和使用之前生成的报告。

查看报告

“报告”列出所有以前生成的报告，提供报告名称、生成日期和时间、生成用户以及报告是在本地还是远程存储的信息。状态栏指示报告是已生成，处于生成队列中（例如，对于计划任务）还是无法生成（例如，由于磁盘空间不足）。

请注意，具有管理员访问权限的用户可以查看所有报告；其他用户只能查看自己所生成的报告。

在多域部署中，只能查看在当前域中生成的报告。

“报告”页面显示所有本地存储的报告。如果当前配置了远程存储，该页面也显示远程存储的报告。远程存储的报告的**位置 (Location)** 列数据为 `Remote`。

注释 如果在远程存储后又切换回本地存储，则远程存储中的报告不在“报告”(Reports) 选项卡列表上显示。同样地，如果从一个远程存储位置切换到另一个远程存储位置，则前一个位置中的报告不在列表中显示。

过程

步骤 1 选择**概述** > **报告**。

步骤 2 点击 **报告**。

步骤 3 点击要查看的报告。

下载报告

可以将任何报告文件下载到本地计算机。由此，可以通过邮件发送报告，或者通过其他可用的手段以电子方式分发。

在多域部署中，只能下载在当前域中生成的报告。

过程

步骤 1 选择**概述** > **报告**。

步骤 2 点击 **报告**。

步骤 3 选中要下载的报告旁边的复选框，然后点击**下载 (Download)**。

提示
点击页面左上方的复选框以下载页面上的所有报告。如果有多个报告页面，则系统会再显示一个复选框，可以点击该复选框以下载所有页面上的所有报告。

步骤 4 根据浏览器提示下载报告。如果选择多个报告，则以单个 `.zip` 文件形式对其进行下载。

远程存储报告

当前配置的报告存储位置显示在“概述”(Overview) > “报告”(Reporting) > “报告”(Reports) 页面的底部，提供本地、NFS 和 SMB 存储的磁盘使用率。如果使用 SSH 访问远程存储，则不提供磁盘使用量的数据。

注释 如果在远程存储后又切换回本地存储，则远程存储中的报告不在“报告”(Reports) 选项卡列表上显示。同样地，如果从一个远程存储位置切换到另一个远程存储位置，则前一个位置中的报告不在列表中显示。

开始之前

- 配置远程存储位置，如 远程存储设备中所述。

过程

步骤 1 选择**概述** > **报告**。

步骤 2 选择 **报告**。

步骤 3 选中页面底部的**启用报告的远程存储 (Enable Remote Storage of Reports)** 复选框。

下一步做什么

- 将报告从本地存储移至远程存储；请参阅将报告移至远程存储器，第 26 页。

相关主题

远程存储设备

将报告移至远程存储器，第 26 页

将报告移至远程存储器

可以按批量处理模式或单个地将本地存储的报告转移到远程存储位置。

注释 如果在远程存储后又切换回本地存储，则远程存储中的报告不在“报告”(Reports) 选项卡列表上显示。同样地，如果从一个远程存储位置切换到另一个远程存储位置，则前一个位置中的报告不在列表中显示。

开始之前

- 配置远程存储位置，如 远程存储设备中所述。

过程

步骤 1 选择概述 > 报告。

步骤 2 选择 报告。

步骤 3 选中要移动的报告旁边的复选框，然后点击移动 (Move)。

提示
选中页面左上方的复选框以移动页面上的所有报告。如果报告有多页，则会再显示一个复选框，可以选中该复选框来移动所有页面上的全部报告。

步骤 4 确认要转移报告。

删除报告

可以随时删除报告文件。此步骤会完全删除文件，并且无法恢复。尽管仍然有生成了报告的报告模板，但如果时间段已扩展或滑动，就可能难以重新生成特定报告文件。如果模板使用输入参数，重新生成可能也很困难。

在多域部署中，只能删除在当前域中生成的报告。

过程

步骤 1 选择概述 > 报告。

步骤 2 点击 报告。

步骤 3 有以下选项可供选择：

- 删除所选项 - 选中要删除的报告旁边的复选框，然后点击删除 (Delete)。
- 删除所有 - 选中页面左上方的复选框以删除页面上的所有报告。如果报告有多页，则会再显示一个复选框，可以选中该复选框来删除所有页面上的全部报告。

步骤 4 确认删除。

报告的历史记录

功能	防火墙管理中心最低版本	最低版本	详细信息
报告模板创建的可用性改进	7.6.0	任意	改进了用户界面，用于设置报告的表格式部分中显示的搜索字段。此新用户界面包括用于添加和删除报告字段的按钮、用于重新排列字段的拖放功能以及简化的排序选项。 新增/修改的屏幕：**概述 (Overview)** > **报告 (Reporting)** > **报告模板 (Report Templates)** > **创建报告模板 (Create Report Template)**，点击**添加表视图 (Add Table View)** 图标，然后点击**字段 (Fields)** 旁边的编辑图标。
在报告模板中选择连接事件的数据源	7.0	任意	如果使用向导配置远程数据存储时使用 Security Analytics and Logging（本地部署），则可以选择在报告中包含存储在该卷上的数据。 修改的页面：报告模板
漏洞报告的更改	6.7	任意	报告输出已根据 Bugtraq 数据的可用性进行了调整。

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。