网络映射

以下主题介绍如何使用网络映射：

- 网络映射的要求和前提条件，第 1 页
- 网络映射，第 1 页
- 自定义网络拓扑，第 6 页

网络映射的要求和前提条件

型号支持

任意。

支持的域

枝叶

用户角色

- 管理员
- 发现管理员

网络映射

Firepower 系统监控通过网络传输的流量，解码流量数据，然后将该数据与既有的操作系统和指纹进行比较。系统之后会使用该数据构建网络的详细表示，称为网络映射。在多域部署中，系统为每个枝叶域都创建单个网络映射。

系统从标识用于在网络发现策略中监控的受管设备收集数据。受管设备直接从受监控流量和间接从已处理的 NetFlow 记录检测网络资产。如果多台设备检测到同一网络资产，则系统会将信息合并成资产的复合表示。

要通过被动检测扩充数据，请执行以下操作：

- 使用开源扫描工具 Nmap™ 主动扫描主机，并将扫描结果添加到网络映射。
- 使用主机输入功能从第三方应用手动添加主机数据。

网络映射显示根据检测到的主机和网络设备显示网络拓扑。

网络映射可用于：

- 获取网络的快速整体视图。
- 选择不同的视图，以适应要执行的分析。网络映射的每个视图都有相同的格式：具有可扩展的类别和子类别的分层树。点击某个类别时，该类别将展开显示其下属的子类别。
- 通过自定义拓扑功能组织并识别子网。例如，如果贵公司中的每个部门使用不同的子网，则可使用自定义拓扑功能将熟悉的标签分配到这些子网。
- 通过深入了解任何受监控主机的主机配置文件查看详细信息。
- 如果对于调查资产不再感兴趣，请将其删除。

注释 如果系统检测到与已从网络映射中删除的主机关联的活动，则其会将该主机重新添加到网络映射。同样，如果系统检测到应用发生更改（例如，如果 Apache Web 服务器升级到新版本），则会将已删除的应用重新添加到网络映射。如果系统检测到使主机易受攻击的更改，则表明在特定主机上重新激活了漏洞。

提示 如果要从网络映射永久排除主机或子网，请修改网络发现策略。如果您发现负载均衡器和 NAT 设备生成额外或不相关的事件，则可能希望从监控中将其排除。

主机网络映射

“主机”选项卡上的网络映射将显示主机计数以及主机 IP 地址和主 MAC 地址的列表。每个地址或部分地址都是一条指向下一级的链接。此网络映射视图提供系统检测到的所有唯一主机的计数，无论主机有一个 IP 地址还是多个 IP 地址。

使用主机网络映射查看网络上按分层树中子网排列的主机，以及向下钻取到特定主机的主机配置文件。

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 与受管设备数据之间的差异。

通过为网络创建自定义拓扑，可向主机网络映射中显示的子网分配有意义的标签，例如，部门名称。也可根据在自定义拓扑中指定的公司查看主机网络映射。

可从主机网络映射中删除整个网络、子网或个别主机。例如，如果知道主机不再连接到网络，则可将其删除以简化分析。如果系统此后检测到与已删除主机关联的活动，则会将该主机重新添加至网络映射。如果要从网络映射永久排除主机或子网，请修改网络发现策略。

注意 请勿从网络映射删除网络设备。系统会使用它们来确定网络拓扑。

在主机网络映射页面上，只能搜索主 MAC 地址，而主机 [MAC] 计数器仅包括主 MAC 地址。有关主 MAC 地址和辅助 MAC 地址的说明，请参阅 主机配置文件中的基本主机信息。

网络设备网络映射

“网络设备”(Network Devices) 选项卡上的网络映射显示将一个网段连接到另一个网段的网络设备（网桥、路由器、NAT 设备和负载平衡器）。该映射包含两个部分，分别列出按 IP 地址识别的设备和按 MAC 地址识别的设备。

该映射还提供系统检测到的所有唯一网络设备的计数，无论设备具有一个 IP 地址还是多个 IP 地址。

如为网络创建自定义拓扑，则网络设备网络映射中会显示分配给子网的标签。

系统用于区分网络设备的方法包括：

- 分析思科发现协议 (CDP) 消息，可识别网络设备及其类型（仅限思科设备）
- 检测生成树协议 (STP)，可将设备识别为交换机或网桥
- 检测多个使用相同 MAC 地址的主机，可识别属于路由器的 MAC 地址
- 检测客户端 TTL 值变化，或检测比典型启动时间变化更频繁的 TTL 值，可识别 NAT 设备和负载均衡器

如果网络设备使用 CDP 进行通信，则其可能有一个或多个 IP 地址。如果它使用 STP 进行通信，则可能仅有 MAC 地址。

由于系统使用其位置来确定网络拓扑，因此不能从网络映射中删除网络设备。

网络设备的主机配置文件具有“系统”(System) 部分而不是“操作系统”(Operating Systems) 部分，其中包括反映网络设备后检测到的任何移动设备的硬件平台的“硬件”(Hardware) 列。如果“系统”下列出了硬件平台值，则该系统代表在网络设备后检测到的一个或多个移动设备。请注意，移动设备可能有，也可能没有硬件平台信息，但不会检测到非移动设备系统的硬件平台信息。

移动设备网络映射

“移动设备”(Mobile Devices) 选项卡上的网络映射显示连接到网络的移动设备。此网络映射视还提供系统检测到的所有唯一移动设备的计数，无论设备有一个 IP 地址还是多个 IP 地址。

每个地址或部分地址都是一条指向下一级的链接。您也可以删除子网或 IP 地址；如果系统重新发现设备，则会将该设备重新添加到网络映射。

您还可以向下展开以查看移动设备的主机配置文件。

要识别移动设备，系统应执行以下操作：

- 分析来自移动设备的移动浏览器的 HTTP 流量中的用户代理字符串

- 监控特定移动应用的 HTTP 流量

如为网络创建自定义拓扑，则移动设备网络映射中会显示分配给子网的标签。

危害表现网络映射

“危害表现”(Indications of Compromise) 选项卡上的网络映射显示网络上按 IOC 类别组织的受损主机。受影响主机列在每个类别下方。每个地址或部分地址都是一条指向下一级的链接。

从危害表现网络映射中，可查看通过特定方式确定为已受损的每个主机的主机配置文件。也可删除（标记为已解析）任何 IOC 类别或任何特定主机，这会从相关主机中移除 IOC 标记。例如，如已确定问题得到解决且不可能复发，即可从网络映射中删除 IOC 类别。

标记从网络映射解析的主机或 IOC 类别不会将其从网络中移除。如果系统最近检测到触发该 IOC 的信息，则网络映射中会重新显示已解析的主机或 IOC 类别。

有关系统如何确定危害表现的详细信息，请参阅危害表现数据和子主题。

应用协议网络映射

“应用协议”(Application Protocols) 选项卡上的网络映射显示您的网络上运行的应用，按应用名称、供应商、版本并最终按运行每个应用的主机在分层树中排列。

系统检测到的应用可能随系统软件和 VDB 更新而变化，并且在导入任何附加探测器的情况下也会变化。每个系统或 VDB 更新的版本说明或咨询文本均包含有关任何新的和已更新的探测器的信息。有关探测器的全面最新列表，请参阅思科支持网站 (http://www.cisco.com/cisco/web/support/index.html)。

在此网络映射中，您可查看运行特定应用的每台主机的主机配置文件。

还可以删除任何应用类别、在所有主机上运行的任何应用或在特定主机上运行的任何应用。例如，如果知道应用在主机上已禁用并要确保系统不使用它进行影响级别限定，即可从网络映射中删除该应用。

从网络映射中删除应用不会将其从网络中移除。如果系统检测到应用发生变化（例如，如果 Apache 网络服务器升级到新版本），或者如果重新启动系统的发现功能，则网络映射中会重新显示已删除的应用。

视乎删除的内容，行为有所不同：

- 应用类别 - 删除应用类别会将其从网络映射中移除。驻留在该类别下的所有应用都会从包含应用的任何主机配置文件中移除。

  例如，如果删除 **http**，则会从所有主机配置文件中移除标识为 **http** 的所有应用，并且网络映射的应用视图中不再显示 **http**。

- 特定应用、供应商或版本 - 删除特定应用、供应商或版本会从网络映射中以及从包含该网络映射的任何主机配置文件中移除受影响的应用。

  例如，如果展开 **http** 类别并删除 **Apache**，则会从包含列为 Apache 的所有应用（具有 Apache 下列出的任何版本）的任何主机配置文件中移除这些应用。同样，如果删除特定版本（例如 **1.3.17**）而不是删除 **Apache**，则仅会将所选版本从受影响主机配置文件中删除。

- 特定 IP 地址 - 删除 IP 地址会将其从应用列表中移除，并从所选 IP 地址的主机配置文件中移除应用本身。

  例如，如果展开 **http**、**Apache**、**1.3.17 (Win32)**，然后删除 **172.16.1.50:80/tcp**，则会从 IP 地址 172.16.1.50 的主机配置文件中删除 Apache 1.3.17 (Win32) 应用。

漏洞网络映射

“漏洞”选项卡上的网络映射显示系统在网络中检测到的漏洞，按旧版漏洞 ID (SVID)、 CVE ID 或 Snort ID排列。

从此网络映射中，可查看特定漏洞的详细信息；还可查看受特定漏洞影响的任何主机的主机配置文件。此信息有助于评估该漏洞对特定受影响主机造成的威胁。

如果确定特定漏洞不适用于网络上的主机（例如，已应用补丁），则可停用漏洞。已停用的漏洞仍显示在网络映射中，但是其先前受影响主机的 IP 地址以灰色斜体显示。那些主机的主机配置文件将已停用的漏洞显示为无效，不过可以手动将其标记为对于个别主机有效。

如果主机上的应用或操作系统存在身份冲突，则系统会列出两种潜在身份的漏洞。解决身份冲突后，漏洞保持与当前身份关联。

默认情况下，仅当数据包包含应用的供应商和版本时，网络映射才会显示检测到的应用的漏洞。但是，可将系统配置为列出缺少供应商和版本数据的应用的漏洞，只需在 防火墙管理中心配置中为应用启用漏洞映射设置。

漏洞 ID（或漏洞 ID 的范围）旁边的数字表示两个计数：

受影响的主机

第一个数字是受漏洞影响的非唯一主机的计数。如果主机受多个漏洞影响，则会多次对其进行计数。因此，计数可能高于网络上的主机数。停用漏洞会按可能受该漏洞影响的主机数减小此计数。如果尚未面向漏洞或漏洞范围停用任何潜在受影响主机的任何漏洞，则不显示此计数。

可能受影响的主机

第二个数字是系统已确定为潜在受漏洞影响的非唯一主机的总数的计数。

停用漏洞致使其仅对指定的主机处于非活动状态。可停用已判定为易受攻击的所有主机或指定的个别易受攻击主机的漏洞。漏洞停用之后，适用的主机 IP 地址以灰色斜体显示在网络映射中。此外，这些主机的主机配置文件将已停用的漏洞显示为无效。

如果系统随后在主机上检测到未尚未停用的漏洞（例如，在网络映射中的新主机上），则系统会激活该主机的漏洞。必须明确停用最近发现的漏洞。此外，如果系统检测到主机的操作系统或应用变化，则可能重新激活关联的已停用漏洞。

主机属性网络映射

“主机属性”选项卡上的网络映射显示按用户定义的主机属性或合规 allow 名单主机属性组织的主机。您不能使用此显示中的预定义主机属性组织主机。

选择要用于组织主机的主机属性时，防火墙管理中心列出该属性在网络映射中的可能值并根据其分配值将主机分组。例如，如果选择按allow名单主机属性组织主机，则系统会在类别“合规”、“不合规”和“未评估”中显示这些主机。

还可查看为其分配了特定主机属性值的任何主机的主机配置文件。

相关主题

主机配置文件中的主机属性

查看网络映射

您必须是 管理员 或 安全分析师 用户才能查看网络映射。

过程

步骤 1 选择**事件和日志** > **主机** > **网络映射**。

步骤 2 点击要查看的网络映射。

步骤 3 根据情况继续操作：

- 选择域 - 在多域部署中，从**域 (Domain)** 下拉列表中选择分叶域。
- 过滤主机 - 如果要按 IP 或 MAC 地址过滤，请在搜索字段中输入地址。要清除搜索，请点击 **清除** ()。
- 向下展开 - 如果要调查类别或主机配置文件，请向下展开映射中的类别或子网。如果已定义自定义拓扑，请点击 **主机** 中的 （**拓扑**） 以查看它，然后在要切换回默认视图时点击 （**主机**） 。
- 删除 - 点击相应元素旁边的 **删除** () 以执行下列操作：
  - 从**主机 (Hosts)**、**网络设备 (Network Devices)**、**移动设备 (Mobile Devices)** 或**应用协议 (Application Protocols)** 选项卡上的映射中删除元素。
  - 标记**危害表现 (Indications of Compromise)** 上解析的 IOC 类别、受损主机或受损主机组。
  - 停用**漏洞 (Vulnerabilities)** 上所有主机或单个主机的漏洞。
- 指定漏洞类 - 在 **漏洞**上，从 **类型** 下拉列表中选择要查看的漏洞的类。
- 指定组织属性 - 在**主机属性 (Host Attributes)** 上，从**属性 (Attribute)** 下拉列表中选择属性。

相关主题

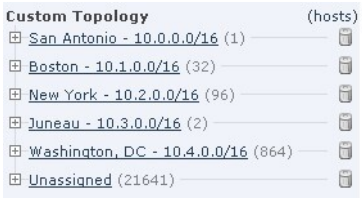
自定义网络拓扑 ，第 6 页
主机配置文件

自定义网络拓扑

使用自定义拓扑功能帮助排列和识别主机及网络设备网络映射中的子网。

例如，如果贵公司中的每个部门使用不同的子网，则可使用自定义拓扑功能标示这些子网。

也可根据在自定义拓扑中指定的公司查看主机网络映射。



您可以使用以下任何或所有策略指定自定义拓扑的网络：

- 您可以从网络发现策略导入网络，以添加您将系统配置为要监控的网络。
- 您可以手动向拓扑中添加网络。

“自定义拓扑”(Custom Topology) 页面列出自定义拓扑及其状态。如果策略名称旁边的灯泡图标亮起，表明拓扑处于活动状态并影响网络映射。如果该图标呈灰色显示，则表明拓扑处于不活动状态。

相关主题

主机网络映射，第 2 页
网络设备网络映射，第 3 页

创建自定义拓扑

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击工具栏中的**自定义拓扑 (Custom Topology)**。

步骤 3 点击 **Create Topology**。

步骤 4 输入 **Name**。

步骤 5 输入**说明 (Description)**（可选）。

步骤 6 向拓扑添加网络。可使用以下任何或所有策略：

- 从网络发现策略导入网络，如从网络发现策略导入网络，第 8 页中所述。
- 手动添加网络，如手动向自定义拓扑添加网络，第 8 页中所述。

步骤 7 点击**保存**。

下一步做什么

- 激活拓扑，如激活和停用自定义拓扑，第 9 页中所述。

从网络发现策略导入网络

过程

步骤 1 访问要将网络导入到的自定义拓扑：

- 创建自定义拓扑；请参阅创建自定义拓扑，第 7 页。
- 编辑现有自定义拓扑；请参阅编辑自定义拓扑，第 9 页。

步骤 2 点击**导入策略网络 (Import Policy Networks)**。

步骤 3 点击**加载 (Load)**。系统显示网络发现策略的拓扑信息。

步骤 4 优化拓扑：

- 通过点击网络旁边的 **编辑** ()，键入名称并点击 **重命名**来对拓扑中的网络进行重命名。
- 通过点击 **删除** ()，然后点击 **确定** 以确认来从拓扑中删除网络。

步骤 5 点击**保存**。

下一步做什么

- 激活拓扑，如激活和停用自定义拓扑，第 9 页中所述。

手动向自定义拓扑添加网络

过程

步骤 1 访问您要添加网络的自定义拓扑：

- 创建自定义拓扑；请参阅创建自定义拓扑，第 7 页。
- 编辑现有自定义拓扑；请参阅编辑自定义拓扑，第 9 页。

步骤 2 点击 **Add Network**。

步骤 3 如果要将网络的自定义标签添加到主机和网络设备网络映射中，请键入**名称 (Name)**。

步骤 4 输入用于表示待添加网络的 **IP 地址**和**网络掩码** (IPv4)。

步骤 5 点击**添加 (Add)**。

步骤 6 点击**保存**。

下一步做什么

- 激活拓扑，如激活和停用自定义拓扑，第 9 页中所述。

相关主题

IP 地址约定

激活和停用自定义拓扑

注释 只有一个自定义拓扑可以随时处于活动状态。如已创建多个拓扑，则激活一个拓扑会自动停用当前活动的拓扑。

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 选择**自定义拓扑 (Custom Topology)**。

步骤 3 点击拓扑旁边的滑块以激活或停用该拓扑。

编辑自定义拓扑

对活动拓扑进行的更改会立即生效。

过程

步骤 1 选择**策略** > **+ 显示更多** > **内容关联** > **网络发现**。

在多域部署中，如果您不在枝叶域中，则系统会提示您切换。

步骤 2 点击**自定义拓扑 (Custom Topology)**。

步骤 3 点击要编辑的拓扑旁边的 **编辑** (✎) 。

步骤 4 编辑拓扑，如创建自定义拓扑 ， 第 7 页中所述。

步骤 5 点击**保存**。

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。

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。

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。

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。