配置部署

以下主题介绍如何在 Cisco Secure Firewall Management Center上管理各种策略：

策略管理的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 网络管理员
- 安全审批人

策略部署

⚠

注意 如果隧道也被配置为用于管理流量，请勿通过直接在 威胁防御 上终止的 VPN 隧道来推送 管理中心 部署。推动 管理中心 部署可能会停用隧道并断开 管理中心 和 威胁防御 的连接。

从这种情况下恢复设备可能会造成很大的中断，需要执行灾难恢复过程。此过程通过将管理器从 管理中心 更改为本地并从头配置设备，将 威胁防御 配置重置为出厂默认值。有关详细信息，请参阅通过 VPN 隧道部署 管理中心 策略配置，第 2 页。

在配置部署后，无论何时对该配置进行更改，您都必须向受影响设备部署更改。您可以在消息中心查看部署状态。

部署会更新以下组件：

- 设备和接口配置
- 与设备相关的策略：NAT、VPN、QoS、平台设置
- 访问控制策略以及相关策略：DNS、文件、身份、入侵、网络分析、预过滤器、SSL
- 网络发现策略
- 入侵规则更新
- 与其中任一元素相关联的配置和对象

您可以将系统配置为自动部署，方法如下：安排一个部署任务，或者将系统设置为在导入入侵规则更新时进行部署。如果允许入侵规则更新修改系统提供的基本策略以进行入侵和网络分析，则自动部署策略的方法尤其有用。入侵规则更新还可修改访问控制策略中高级预处理和性能选项的默认值。

在多域部署中，可以为您的用户帐户所属的任何域部署更改。

- 切换到祖先域，以便将更改同时部署到所有子域。
- 切换到分叶域，以便仅将更改部署到该域。

部署配置更改的最佳实践

以下是部署配置更改的指导原则。

通过 VPN 隧道部署 管理中心 策略配置

只有针对未终止隧道的设备进行部署时，才能通过 VPN 隧道部署 管理中心 策略配置。管理中心 到 威胁防御 管理流量应为其自身的安全传输 SF 隧道，无需通过 S2S VPN 隧道进行任何连接。

对于基于策略的 VPN 隧道，请选择两侧的受保护网络以排除 管理中心 到 威胁防御 的管理流量。对于基于路由的 VPN 隧道，配置路由以排除 VTI 接口的 管理中心 到 威胁防御 管理流量。

当您通过 VPN 隧道推送 管理中心 部署且管理流量也通过隧道时，如果出现任何 VPN 错误配置，则会停用隧道并导致 管理中心 和 威胁防御 断开连接。

要重新实例化隧道配置，您可以：

- 从 威胁防御 和 管理中心 中删除传感器（导致其所有配置丢失），然后再次将传感器添加到 管理中心。

  或

- 联系思科 TAC：

注释 重新实例化隧道配置需要彻底检查系统。

内联部署和被动部署

请勿将内联配置应用于被动部署的设备，反之亦然。

部署时间和内存限制

部署所需的时间取决于多个因素，包括（但不限于）：

- 发送至设备的配置。例如，如果阻止的安全情报条目数显示增加，部署时间可能要长一些。
- 设备型号和内存。内存较低的设备，部署时间可能要长一些。

请勿超过设备的能力。如果超过目标设备所支持的规则或策略最大数量，系统会显示警告。最大值取决于许多因素 - 不仅包括设备内存及处理器的数量，还与策略和规则复杂性有关。有关优化策略和规则的信息，请参阅访问控制规则的最佳实践。

部署期间的流量和检测中断

在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，部署某些配置会重新启动 Snort 进程，这会中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。请参阅Snort 重启流量行为，第 18 页和部署或激活时重启 Snort 进程的配置，第 20 页。

对于 威胁防御 设备，如果部署中断了流量或检测，“部署”(Deploy) 对话框中的**检测中断 (Inspect Interruption)** 列会显示警告。您可以继续，也可以取消或延迟部署；有关详细信息，请参阅威胁防御 设备的重启警告，第 4 页。

注意 我们强烈建议在维护窗口或在中断的影响最低时部署。

自动启用应用检测器

如果执行的是应用控制，但是禁用所需的检测器，则系统会在策略部署时自动启用系统提供的适当检测器。如果不存在检测器，则系统会为该应用启用最新修改的用户定义检测器。

网络发现策略更改带来的资产重新发现

将更改部署到网络发现策略时，系统会删除并重新发现受监控网络中主机的网络映射中的 MAC 地址、TTL 和跳数信息。此外，受影响的受管设备还会放弃任何尚未发送到 管理中心的发现数据。

相关主题

Snort® 重新启动场景，第 17 页

威胁防御 设备的重启警告

部署过程中，“部署”页中的 **检查中断** 列会指定部署的配置是否在 威胁防御 设备上重启 Snort 进程。当名为 *Snort* 进程的流量检测引擎重启时，检测会中断，直到该进程恢复为止。流量将会中断还是在中断期间允许未经检测而通过，取决于设备对流量的处理方式。请注意，您可以继续进行部署，取消部署并修改配置，也可以将部署推迟到部署对网络的影响最低时执行。

当**检查中断**列显示**是**并展开设备配置列表时，系统会以**检查中断**（）指示任何将重启 Snort 进程的特定配置类型。将鼠标指针悬停在图标上时，会显示一条消息，通知您部署配置可能会中断流量。

下表总结了“部署”页面中显示的检测中断警告。

表 *1:* 检测中断指示器

类型	检测中断	说明
威胁防御	**检查中断**（）是	至少有一个配置（如果已部署）会中断设备上的检测并可能会中断流量，具体取决于设备对流量的处理方式。展开设备配置列表可以了解详细信息。
	--	部署的配置不会中断设备上的流量。
	未确定	系统无法确定部署的配置是否可能会中断设备上的流量。 进行软件升级后，有些情况下是在呼叫支持期间，首次部署之前会显示“不确定”状态。
	错误（）	系统因内部错误而无法确定状态。 取消操作，然后再次点击**部署 (Deploy)**，以便系统可以重新确定**检测中断 (Inspect Interruption)** 状态。如果问题仍然存在，请与支持人员联系。
sensor	--	被识别为 传感器 的设备不是 威胁防御 设备；系统无法确定部署的配置是否会中断此设备上的流量。

有关会为各类设备重启 Snort 进程的所有配置的信息，请参阅部署或激活时重启 Snort 进程的配置，第 20 页。

部署状态

在“部署”页上，**状态**列提供每个设备的部署状态。如果正在进行部署，则会显示部署进度的实时状态，否则会显示以下状态之一：

- 待处理 - 表示设备中有要部署的更改。
- 警告或错误 - 表示部署前检查已发现部署的警告或错误之处，而且您没有继续部署。如果出现任何警告，可以继续进行部署，但如果有任何错误，则不能继续。

注释 “状态”列仅提供“部署”页上单个用户会话的警告或错误状态。如果您离开或刷新该页面，状态将变为“待处理”。

- 失败 - 表示先前的部署失败。点击状态以查看详细信息。
- 排队中 - 表示部署已启动，而系统尚未开始部署过程。
- 已完成 - 表示部署已成功完成。

部署估计

选择设备、策略或配置后，“部署”(Deployment)页上将提供**估计 (Estimate)**链接。点击**估计 (Estimate)**链接可获取部署持续时间的估计值。持续时间是一个粗略估计值（精确度约为 70%），在少数情况下，部署所花费的实际时间可能有所不同。请参阅少数 威胁防御 设备部署的持续时间估计值。如果部署不超过 20 个 威胁防御 设备，该估计值是可靠的。

当估计值不可用时，表示数据不可用，因为所选设备上的第一次成功部署还未完成。此情况可能在管理中心 版本升级或全新安装后出现。

注释 当批量更改策略（在批量策略迁移的情况下）和选择性部署时，估计值不正确且不可靠，因为估计值基于启发式技术。

部署说明

部署说明是用户可以在部署过程中添加的自定义说明，而这些说明是可选的。

您可以在**部署历史记录 (Deployment History)** 页面中查看部署说明。在 Firepower 管理中心菜单栏中，点击**部署 (Deploy)**，然后选择**部署历史记录 (Deployment History)** 以查看每个作业的**部署说明 (Deployment Notes)** 列。

使用**部署历史记录 (Deployment History)** 页面上的“搜索”(Search) 选项按作业名称、设备名称、用户名、状态、部署说明或“收藏”等关键词进行搜索。

部署预览

预览提供要在设备上部署的所有策略和对象更改的快照。策略更改包括新策略、现有策略的更改以及已删除的策略。对象更改包括策略中使用的已添加和修改的对象。未使用的对象更改不会显示，因为它们没有部署在设备上。

在“部署”页上，“预览”列为列出的每个设备提供一个**预览**（ ）图标。点击预览图标后， 管理中心 会显示列出所有策略和对象更改的 UI 页。预览页上的左侧窗格以树状结构组织列出设备中更改的所有不同策略类型。

预览页面上提供的**过滤器**图标( )提供了在用户级别和策略级别过滤策略的选项。点击**过滤器**图标( )。选择策略或用户名，或同时选择两者，然后点击**应用 (Apply)**，将显示的列表限制为仅选定的项目。要查看所有待处理部署，请确保点击**过滤器 (Filter)** 图标并选择**重置 (Reset)**。

左侧窗格中列出策略中的所有添加、更改或删除项，或者在左侧窗格中选择的对象。右侧窗格中的两个列提供上次部署的配置设置（在 **“部署版本”** 列中）与应该部署的更改（在 **“待处理版本”** 列中）。上次部署的配置设置源自管理中心中上次保存的部署的快照，而不是来自设备。设置的背景颜色根据页面右上角的图例分类显示。

修改者列列出了修改或添加了配置设置的用户。在策略级别， 管理中心 显示所有修改过策略的用户，而在规则级别， 管理中心 只显示最后修改规则的用户。

支持对安全情报、地理定位、Sinkhole 和文件列表对象的更改进行部署预览。有关 管理中心支持的这些和其他可重用对象的说明，请参阅 对象管理。

您可以点击**下载为 PDF (Download as PDF)** 按钮下载更改日志的副本。

注释

- 要预览部署更改，您需要能从REST API访问 管理中心。要启用REST API访问，请执行 《Cisco Secure Firewall Management Center 管理指南》中 启用 *REST API* 访问 中的步骤。
- 预览不会显示跨策略的规则重新排序。

  对于DNS策略，重新排序的规则作为规则添加和删除项显示在预览列表中。例如，将规则从规则顺序中的位置 1 移动到位置 3 显示为好像该规则已从位置 1 中删除，并作为新规则添加到位置 3 中。同样，删除规则时，其下的规则会列为已编辑的规则，因为它们的位置已更改。更改按它们在策略中出现的最终顺序显示。
- 首次添加接口或平台设置策略时，预览中显示所有默认值（即使未有变更）以及其他配置的设置。同样，在高可用性对配置或中断后的首次预览中也会显示设置的高可用性相关策略和默认值（即使未有变更）。
- 某些对象不支持预览。
- 仅当对象与任何设备或接口关联时，预览中才会显示添加的对象和属性的更改。删除的对象不显示。
- 以下策略不支持预览：
  - 高可用性
  - 网络发现
  - 网络分析
  - 设备设置
- 规则级别的用户信息不可用于入侵策略。
- 管理中心 将用户名显示为 **system** 以执行以下操作：
  - 回滚
  - 升级
  - 威胁防御 备份和恢复
  - SRU 更新
  - LSP 更新
  - VDB 更新
- 如果您在 **系统**（⚙）> **配置** > **信息** 中更改 管理中心 名称，则部署预览不会指定此更改，但它需要部署。
- 要查看自动回滚导致的更改，请参阅编辑部署设置。

对部署的过滤支持

“部署”(Deployment) 页面上的**过滤器**图标（）会提供一个选项，用于过滤待部署的设备列表。过滤器图标提供了根据所选设备和用户名过滤列表的选项。您可以使用过滤器和搜索选项来缩小到所需列表的范围。

点击过滤器图标（）。选择设备或用户名，或同时选择两者，然后点击**应用 (Apply)**，将显示的列表限制为仅选定的项目。要查看所有待处理部署，请确保点击过滤器图标（）并选择**重置 (Reset)**。

选择性策略部署

注意 如果隧道也被配置为用于管理流量，请勿通过直接在 威胁防御 上终止的 VPN 隧道来推送 管理中心 部署。推动 管理中心 部署可能会停用隧道并断开 管理中心 和 威胁防御 的连接。

从这种情况下恢复设备可能会造成很大的中断，需要执行灾难恢复过程。此过程通过将管理器从 管理中心 更改为本地并从头配置设备，将 威胁防御 配置重置为出厂默认值。有关详细信息，请参阅通过 VPN 隧道部署 管理中心 策略配置 ， 第 2 页。

管理中心 允许您在设备上应该部署的所有更改的列表内选择特定的策略，并只部署所选的策略。选择性部署仅可用于以下策略：

- 访问控制策略
- 入侵策略
- 恶意软件和文件策略
- DNS 策略
- 身份策略
- SSL 策略
- QoS 策略
- 预过滤策略
- 网络发现
- NAT 策略
- 路由策略
- VPN 策略

在部署页面上，点击**展开箭头**（）查看设备特定的配置更改后，才会显示**策略选择**（）图标。策略选择图标可让您选择要部署的个别策略或配置，而保留其余的更改不予部署。您也可以使用此

选项查看特定策略或配置之间相互依赖的更改。管理中心 动态检测策略之间的依赖关系（例如，访问控制策略和入侵策略之间），以及共享对象和策略之间的依赖关系。相互依赖的更改以彩色标记表示，以指定一组相互依赖的部署更改。选择一个部署更改时，相互依赖的更改将自动选中。

注释

- 部署共享对象的更改后，受影响的策略也应随其一起部署。在部署过程中选择共享对象时，受影响的策略会自动选中。
- 计划部署和使用 REST API 的部署不支持选择性部署。在这些情况下，您只能选择完全部署所有更改。
- 部署前对警告和错误的检查不仅在所选策略上执行，还在所有过期的策略上执行。因此，警告或错误列表也显示取消选择的策略。
- 同样，“部署”页上**检查中断**列的指示会考虑所有过时的策略，而不仅是选定的策略。有关**检查中断**列的信息，请参阅威胁防御 设备的重启警告 ，第 4 页。

选择性部署策略有特定的限制。按照下表中的内容，了解何时可以使用选择性策略部署。

表 *2:* 选择性部署的限制

类型	说明	情景
完整部署	对于特定部署场景，完整部署是必要的， 管理中心 在这类场景下不支持选择性部署。如果在这类场景下遇到错误，可选择要部署在设备上的所有更改以继续。	需要完整部署的场景包括： • 升级 威胁防御 或 管理中心后的第一次部署。 • 恢复 威胁防御 后的第一次部署。 • 修改 威胁防御 接口设置后的第一次部署。 • 修改虚拟路由器设置后的第一次部署。 • 威胁防御 设备移动到新域（从全局域到子域或从子域到全局域）时。
关联策略部署	管理中心 识别相互关联和依赖的策略。选择一个相互关联的策略时，其余相互关联的策略将自动选中。	自动选择关联策略的场景： • 新对象与现有策略关联时。 • 修改现有策略的对象时。 自动选择多个策略的场景： • 当新对象与现有策略关联并且同一对象已与其他策略关联时，所有关联的策略将自动选中。 • 修改共享对象时，所有关联的策略将自动选中。

类型	说明	情景
相互依赖的策略更改（使用彩色标记显示）	管理中心动态检测策略之间以及共享对象与策略之间的依赖关系。对象或策略的相互依赖关系使用彩色标记显示。	自动选择以彩色显示的互相依赖策略或对象的场景： • 所有过期策略都有相互依赖的更改时。 例如，当访问控制策略、入侵策略和NAT策略过期时。由于访问控制策略和 NAT 策略共享一个对象，因此系统将同时选择所有策略进行部署。 • 所有过期策略共享一个对象，而该对象被修改时。
访问策略组规范	当您点击**显示或隐藏策略**（  ）时，访问策略组的策略将同时在预览窗口中的**访问策略组 (Access Policy Group)** 下列出。	访问策略组策略的场景和预期行为如下： • 如果访问控制策略过期，则在选择访问控制策略进行部署时，将选择该组下的所有其他过期策略，但文件策略和入侵策略除外。 但是，如果访问控制策略已过期，则无论是否选择访问控制策略，都可以单独选择或取消选择入侵和文件策略，除非有任何相关更改。例如，如果为访问控制规则分配了新的入侵策略，则表明存在相关更改，则选择访问控制策略和入侵策略中的任何一个时，都会自动选择访问控制策略和入侵策略。 • 如果没有过期的访问控制策略，可以选择此组中的其他过期策略单独部署。

部署配置更改

注意 如果隧道也被配置为用于管理流量，请勿通过直接在 威胁防御 上终止的 VPN 隧道来推送 管理中心 部署。推动 管理中心 部署可能会停用隧道并断开 管理中心 和 威胁防御 的连接。

从这种情况下恢复设备可能会造成很大的中断，需要执行灾难恢复过程。此过程通过将管理器从 管理中心 更改为本地并从头配置设备，将 威胁防御 配置重置为出厂默认值。有关详细信息，请参阅通过 VPN 隧道部署 管理中心 策略配置，第 2 页。

更改配置后，将其部署到受影响的设备。我们强烈建议在维护窗口或在任何流量和检测中断的影响最低时部署。

注意 在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，部署某些配置会重新启动Snort进程，这会中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。请参阅Snort 重启流量行为，第 18 页和部署或激活时重启 Snort 进程的配置，第 20 页。

开始之前

- 查看部署配置更改的最佳实践，第 2 页中所述的准则。
- 确保所有受管设备都使用安全区域对象的相同修订版。如果已编辑安全区域对象：在编辑要同步的全部设备上接口的区域设置前，请勿将配置更改部署到任何设备。您必须同时部署到所有受管设备。。

注释 如果在部署期间系统读取传感器配置，则策略部署过程将失败。从传感器 CLI 执行 `show running-config` 等命令会干扰部署，从而导致部署失败。

过程

步骤 1 在 管理中心 菜单栏中，点击**部署 (Deploy)**，然后选择**部署 (Deployment)**。

GUI 页面列出了具有待处理状态的过期配置的设备。

- **修改者**列列出了修改策略或对象的用户。展开设备列表时，您可以参照每个策略列表查看修改了策略的用户。

  注释 没有为已删除的策略和对象提供用户名。

- **检查中断**列指示在部署过程中是否可能导致设备中的流量检查中断。

  请参阅 威胁防御 设备的重启警告，第 4 页 中的信息，可帮助您识别在部署到 威胁防御 设备时会中断流量检查并可能中断流量的配置。

  如果设备的此列中这一条为空白，则表明在部署过程中该设备上不会出现流量检查中断。

- **上次修改时间**列指定上次更改配置的时间。
- **预览**列允许您预览下一次要部署的更改。有关详细信息，请参阅部署预览，第 6 页。
- **状态**列提供每个部署的状态。有关详细信息，请参阅部署状态，第 5 页。

步骤 2 识别并选择要部署配置更改的设备。

- 搜索 - 在搜索框中搜索设备名称、类型、域、组或状态。
- 展开 - 点击 **展开箭头** （ › ） 以查看要部署的设备特定的配置更改。

选中设备复选框后，该设备下列出的设备的所有更改都会推送到部署中。但是，您可以使用 **策略选择**（）选择部署个别策略或配置，而保留其余的更改不予部署。有关详细信息，请参阅选择性策略部署，第 8 页。

（可选）使用 **显示或隐藏策略**（）可选择性地查看或隐藏关联的未修改策略。

注释

- 当**检查中断 (Inspect Interruption)** 列中的状态指示（是）部署会中断 威胁防御设备上的检查并可能中断流量时，展开的列表将用 **检查中断**（）指示导致中断的特定配置。
- 当接口组、安全区或对象发生更改时，受影响的设备在 管理中心中显示为过期。为确保这些更改生效，包含这些接口组、安全区或对象的策略也需要随这些更改一起部署。受影响的策略在 管理中心的“预览”页上显示为过期。

步骤 3 （可选）点击**估计 (Estimate)** 以获取粗略估计的部署持续时间。

有关详细信息，请参阅部署估计，第 5 页。

步骤 4 点击 **部署**。

步骤 5 如果系统在要部署的更改中发现错误或警告，则会在**验证消息**窗口中显示它们。要查看完整详细信息，请点击警告或错误前的箭头图标。

有以下选项可供选择：

- 部署 - 继续部署而无需解决警告情况。如果系统识别错误，则无法继续。
- 关闭 - 退出而不部署。解决错误和警告情况，并尝试重新部署该配置。

下一步做什么

- （可选）监控部署状态；请参阅《Cisco Secure Firewall Management Center 管理指南》中的 查看部署消息 。
- 如果部署失败，请参阅部署配置更改的最佳实践，第 2 页。
- 在部署过程中，如果由于任何原因导致部署失败，则可能会影响流量。不过，这取决于某些条件。如果部署中存在特定的配置更改，则部署失败可能导致流量中断。请参阅下表，了解在部署失败时可能导致流量中断的配置更改。

配置更改	存在？	流量受影响？
访问控制策略中的**威胁防护服务**更改	是	是
VRF	是	是
接口	是	是
QoS	是	是

注释 仅当 管理中心 和 威胁防御 版本为 6.2.3 或更高版本时，部署期间中断流量的配置更改才是有效的。

相关主题

Snort® 重新启动场景，第 17 页

将现有配置重新部署到设备

可以将现有（未改变）的配置强制部署到单台受管设备。我们强烈建议在维护窗口或在任何流量和检测中断的影响最低时部署。

注意 在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，部署某些配置会重新启动 Snort 进程，这会中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。请参阅Snort 重启流量行为，第 18 页和部署或激活时重启 Snort 进程的配置，第 20 页。

开始之前

查看部署配置更改的最佳实践，第 2 页中所述的准则。

过程

步骤 1 选择**设备** > **设备管理**。

步骤 2 点击要强制部署的设备旁边的 **编辑**（ ）。

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 3 点击 **设备**。

步骤 4 点击 **常规** 部分标题旁边的 **编辑**（ ）。

步骤 5 请点击 **强制部署** （ ）。

注释 强制部署比常规部署需要更多时间，因为它涉及要在 FTD 上部署的策略规则的完整生成。

步骤 6 点击 **部署**。

系统会识别出您正在部署的配置中的所有错误或警告。您可以点击**继续**继续，而不解决警告状况。但是，如果系统识别到错误，则无法继续。

下一步做什么

- （可选）监控部署状态；请参阅《Cisco Secure Firewall Management Center 管理指南》中的 查看部署消息 。
- 如果部署失败，请参阅部署配置更改的最佳实践 ， 第 2 页。

相关主题

Snort® 重新启动场景 ， 第 17 页

查看部署历史记录

过程

步骤 1 在 Cisco Secure Firewall Management Center 菜单栏中，点击**部署 (Deploy)**，然后选择**部署历史 (Deployment History)**。

所有先前部署和回滚作业的列表按时间倒序显示。

步骤 2 点击所需部署作业旁边的 **展开箭头** （ ），以便查看作业中包含的设备及其部署状态。

步骤 3 （可选）点击 **脚本详细信息** （ ） 以查看发送到设备的命令以及收到的响应。

该脚本包含以下各节：

- **Snort 应用 (Snort Apply)** - 如果 Snort 相关的策略中有任何故障或响应，则此部分中会显示消息。通常，该部分为空。
- **CLI 应用 (CLI Apply)** - 此部分涵盖使用发送到设备的命令配置的功能。
- **Infrastructure Messages** - 此部分显示不同部署模块的状态。

在 **CLI 应用 (CLI Apply)** 部分中，部署脚本包括发送到设备的命令以及从该设备返回的任何响应。这些响应可以是信息性消息或错误消息。对于失败的部署，请查找指示命令错误的消息。如果您正在使用 FlexConfig 策略配置自定义的功能，则检查这些错误特别有用。这些错误可帮助您纠正尝试配置这些命令的 FlexConfig 对象中的脚本。

注释 为托管功能发送的命令与从 FlexConfig 策略生成的命令之间没有显著差异。

例如，以下序列显示管理中心发送了命令来为 GigabitEthernet0/0 配置外部逻辑名。设备的响应是自动将安全级别设置为 0。威胁防御 不会将安全级别用于任何操作。

```
========== CLI APPLY ==========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

步骤 4 （可选）点击**预览** （ ）以查看设备上部署的策略和对象更改与之前部署的版本。

修改者列列出了修改策略或对象的用户。在策略级别，管理中心 会显示已修改策略的所有用户名。在规则级别，管理中心 会显示最后修改规则的用户。

此外，要比较任意两个版本并查看更改日志，请在下拉框中选择所需的版本，然后点击**显示 (Show)** 按钮。点击**下载为 PDF (Download as PDF)** 按钮以下载更改日志的副本。

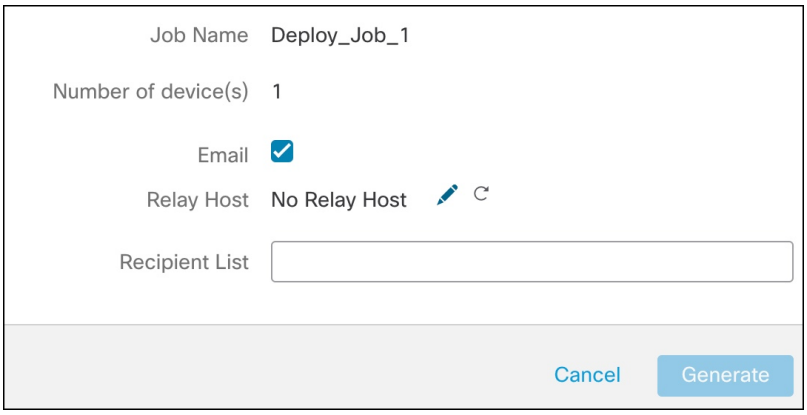
注释 认证登记、HA 操作和失败的部署不支持部署历史记录预览。

步骤 5 （可选）针对每个部署作业，点击 **更多**（⋮） 图标并执行其他操作：

- “书签”(Bookmark) - 为部署作业添加书签。
- “编辑部署说明”(Edit Deployment Notes) - 编辑为部署作业添加的自定义部署说明。
- “生成报告”(Generate Report) - 生成可用于审核的部署报告。此报告包括具有预览和脚本信息的作业属性，并且报告可以作为 PDF 文件下载。

1. 点击**生成报告 (Generate Report)** 以再次生成报告。

   图 *1:*生成报告



2. 在**生成报告 (Generate Report)** 弹出窗口中，选中**邮件 (Email)** 复选框。
3. 如果配置了邮件中继主机，也可以通过邮件发送报告。如果未配置邮件中继主机，请使用**编辑**（✎） 图标来配置或修改邮件中继主机。有关更多信息，请参阅《Cisco Secure Firewall Management Center 管理指南》中的配置邮件中继主机和通知地址。
4. 在**收件人列表 (Recipient List)** 中，您可以输入多个邮件地址并以分号分隔。
5. 点击**生成 (Generate)** 以生成报告，然后此报告将通过邮件发送给收件人。
6. 在“通知任务”(Notifications task) 选项卡中，您可以跟踪进度。完成报告生成后，点击通知任务选项卡中的链接以下载 PDF 报告。

查看部署历史记录预览

如果您看到有关自动回滚部署的横幅，请参阅编辑部署设置以了解详细信息。

过程

步骤 1 在 Cisco Secure Firewall Management Center 菜单栏中，点击**部署 (Deploy)**，然后选择**部署历史 (Deployment History)**。

所有先前部署和回滚作业的列表按时间倒序显示。

步骤 2 点击所需部署作业旁边的 **展开箭头** （ ），以便查看作业中包含的设备及其部署状态。

步骤 3 （可选）点击**预览** （ ）以查看设备上部署的策略和对象更改与之前部署的版本。

1. 要比较任意两个版本并查看更改日志，请在下拉框中选择所需的版本，然后点击**显示 (Show)** 按钮。下拉框会显示部署作业名称和部署结束时间。

   注释　　下拉框还会显示失败的部署。

2. 修改者列列出了修改策略或对象的用户。
   1. 在策略级别，FMC 会显示已修改策略的所有用户名。
   2. 在规则级别，FMC 会显示最后修改规则的用户。
3. 您还可以点击“下载为 PDF”(Download as PDF) 按钮下载更改日志的副本。

修改者列列出了修改策略或对象的用户。在策略级别，FMC 会显示已修改策略的所有用户名。在规则级别，FMC 会显示最后修改规则的用户。

此外，要比较任意两个版本并查看更改日志，请在下拉框中选择所需的版本，然后点击**显示 (Show)** 按钮。点击**下载为 PDF (Download as PDF)** 按钮以下载更改日志的副本。

注释　　认证登记、HA 操作和失败的部署不支持部署历史记录预览。

注释
- 部署历史预览仅支持在 FMC 7.0 版本中完成的所有部署。7.0 之前的部署不支持预览。
- 注册设备后，创建的作业历史记录不支持预览。
- 在部署历史记录中，将捕获最近 10 次成功部署、最近 5 次失败部署以及最近 5 次回滚部署。

不支持预览的 HA 场景

以下 HA 场景不支持预览：

- 如果设备处于单机模式并已建立链，则会触发自动部署。对于该特定作业，不支持预览。将鼠标悬停在 **预览** （） 上时会显示一条消息，指明这是 HA 引导程序部署，并且不支持预览。
- **配置组** - 考虑设备最初为独立设备的流程。随后进行了三个部署。在第四个部署中，设备是 HA 引导程序部署。在这些之后，用户会部署设备 5、6 和 7。部署 7 是 HA 中断部署，而用户会部署设备 8、9 和 10。

  在此流程中，不支持 3 和 5 之间的预览，因为 4 是 HA 部署。同样，也不支持 8 和 3 之间的预览。仅支持从 3 到 1、7、6、5、4 和 10、9 和 8 的预览。
- 如果设备已损坏（HA 已损坏），则新设备会被视为新设备。

Snort® 重新启动场景

当受管设备上的流量检测引擎（称为 *Snort* 进程）重启时，检测会中断，直到该进程继续运行。 流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 18 页。 此外，无论 Snort 进程是否重新启动，部署时的资源需求都可能导致少量数据包未经检测即被丢弃。

下表中的任何场景都将导致 Snort 进程重新启动。

表 *3: Snort* 重新启动场景

重新启动场景	更多信息
部署需要 Snort 进程重新启动的特定配置。	部署或激活时重启 Snort 进程的配置，第 20 页
修改立即重新启动 Snort 进程的配置。	会立即重新启动 Snort 进程的更改，第 21 页
流量激活当前部署的自动应用程序旁路 (AAB) 配置。	配置自动应用旁路

相关主题

访问控制策略高级设置

部署或激活时重启 Snort 进程的配置，第 20 页

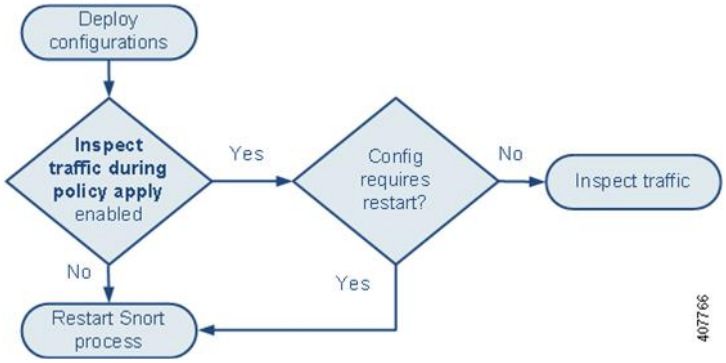
在策略应用期间检测流量

在策略应用期间检查流量是一项高级访问控制策略常规设置，支持受管设备在部署配置更改时检查流量；该设置在部署的配置需要重启 Snort 进程时不适用。可以按如下方式配置此选项：

- 已启用 - 在部署过程中会检查流量，除非某些配置要求重启 Snort 进程。

  当部署的配置不需要 Snort 重启时，系统最初使用当前部署的访问控制策略检查流量，并在部署期间切换到您正在部署的访问控制策略。
- 已禁用 - 部署期间不会检查流量。Snort 进程在您部署时总是会重启。

下图展示了当启用或禁用**在策略应用期间检查流量 (Inspect traffic during policy apply)** 时，Snort 如何重启。



注意 在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，部署某些配置会重新启动 Snort 进程，这会中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。请参阅Snort 重启流量行为，第 18 页和部署或激活时重启 Snort 进程的配置，第 20 页。

Snort® 重启流量行为

下表说明在 Snort 进程重新启动时不同设备处理流量的方式。

表 4: 威胁防御 和 *Threat Defense Virtual* 重新启动流量影响

接口配置	重启流量行为
内联：**Snort 故障时自动打开：关闭：**禁用	被丢弃
内联：**Snort 故障时自动打开：关闭：**启用	不检查直接通过 在系统识别 Snort 已关闭之前，某些数据包可能会在缓冲区中延迟几秒钟。此延迟可能因负载分布而异。但是，缓冲的数据包最终会通过。

接口配置	重启流量行为
路由式、透明（包括 EtherChannel、冗余、子接口）：**preserve-connection**启用（**configure snort preserve-connection enable**；默认） 有关详细信息，请参阅Cisco Secure Firewall Threat Defense 命令参考。	现有 TCP/UDP 流：只要在 Snort 关闭时至少有一个数据包到达，无需检查即可通过 新 TCP/UDP 数据流和所有非 TCP/UDP 数据流：丢弃 请注意，即使启用 **preserve-connection**，以下流量也会丢弃： • 纯文本、与**Analyze**规则操作或**Analyze all tunnel traffic** 默认策略操作匹配的贯通式隧道流量 • 与访问控制规则不匹配，并由默认操作处理的连接。 • 解密的 TLS/SSL 流量 • 安全搜索流量 • 强制网络门户流量
路由式、透明（包括 EtherChannel、冗余、子接口）：**preserve-connection**禁用 (**configure snort preserve-connection disable**)	被丢弃
内联：分流模式	立即传出数据包，副本绕过 Snort
被动	不中断，不检查

注释 除了当 Snort 进程在重启时关闭这一情况下的流量处理外，在 Snort 进程繁忙时，流量也可不检查直接通过或丢弃，具体取决于 Snort 故障时自动打开**繁忙**选项（请参阅配置内联集）的配置。设备只支持“故障保护”选项或“Snort 故障时自动打开”选项，不同时支持这两个选项。

注释 如果 Snort 进程在部署期间正忙但未关闭，则在 CPU 总负载超过 60% 的情况下，路由式、交换式或透明接口上可能会丢弃某些数据包。

警告 在 Snort 规则更新过程中，请勿重新启动系统。

当 snort 无法足够快速地处理数据包时，会出现 Snort-busy 丢弃。Lina 不知道 Snort 是否由于处理延迟而繁忙，是否卡住或由于呼叫阻塞。当传输队列已满时，发生 snort-busy 丢弃。根据传输队列利用率，Lina 将尝试在队列服务正常时进行访问。

部署或激活时重启 Snort 进程的配置

如下所述，部署以下任何配置（AAB 除外）都会重启 Snort 进程。部署 AAB 不会导致重启，但过多的数据包延迟会激活当前部署的 AAB 配置，从而导致 Snort 进程的部分重启。

访问控制策略高级设置

- 禁用**应用策略期间检查流量**时部署。
- 添加或删除 SSL 策略。

文件策略

首先或最后部署以下任一配置；请注意，尽管以其他方式部署这些文件策略配置不会导致重启，但部署非文件策略配置则可能会导致重启。

- 执行下列操作之一：
  - 当部署的访问控制策略包括至少一个文件策略时，启用或禁用**检查存档**。
  - 当已启用**检查存档**时，添加第一个文件策略规则或删除最后一个文件策略规则（请注意，需要至少一个规则才能使**检查存档**生效）。
- 在 **Detect Files** 或 **Block Files** 规则中启用或禁用 **Store files**。
- 添加第一个将**恶意软件云查找**或**阻止恶意软件**规则操作与分析选项（**Spero 分析**或 **MSEXE**、**动态分析**或**本地恶意软件分析**）或存储文件选项（**恶意软件**、**未知**、**正常**或**自定义**）组合到一起的活动文件规则，或删除最后一个符合上述条件的活动文件规则。

请注意，仅在您的配置满足以下条件时，将这些文件策略配置部署到安全区或隧道区域的访问控制规则才会导致重启：

- 您的访问控制规则中的源或目标安全区必须匹配与目标设备上的接口相关的安全区。
- 除非您的访问控制规则中的目标区域为任何，否则规则中的源隧道区域必须与分配给预过滤器策略中隧道规则的隧道区域相匹配。

身份策略

- 当禁用 SSL 解密时（即，当访问控制策略不包含 SSL 策略时），请添加第一个或删除最后一个主动身份验证规则。

  主动身份验证规则具有**主动身份验证**规则操作或**被动身份验证**规则操作，并且**如果无法建立被动或 VPN 识别，则使用主动身份验证**已选中。

网络发现

- 使用网络发现策略，通过 HTTP、FTP 或 MDNS 协议启用或禁用基于流量的非授权用户检测。

设备管理

- MTU：在设备上的所有非管理接口中更改最高 MTU 值。
- 自动应用旁路 (AAB)：当前部署的 AAB 配置会在 Snort 进程出现故障或设备误配置导致单个数据包使用过多处理时间时激活。结果是Snort进程部分重启，以缓解极高的延迟或防止流量彻底停顿。此部分重启会导致几个数据包在不检查的情况下通过或丢弃，具体取决于设备处理流量的方式。

更新

- 系统更新：在包含新版本 Snort 二进制或数据采集库 (DAQ) 的软件更新后首次部署配置。
- VDB：对于运行 Snort 2 的受管设备，在安装包含适用于受管设备的更改的漏洞数据库 (VDB) 更新后首次部署配置需要重新启动检测引擎，并可能导致临时流量中断。这些情况下，系统会显示消息，警告您选择 管理中心 以开始安装。当 VDB 更改处于待处理状态时，部署对话框将为 威胁防御 设备提供其他警告。仅适用于 管理中心 的 VDB 更新不会导致检测引擎重启，并且您无法部署这些更新。

  对于运行 Snort 3 的受管设备，在安装漏洞数据库 (VDB) 更新后首次部署配置可能会暂时中断应用检测，但不会出现流量中断。

相关主题

部署配置更改，第 10 页
Snort® 重新启动场景，第 17 页

会立即重新启动 Snort 进程的更改

以下更改将立即重新启动 Snort 进程，而不执行部署过程。 重启对流量的影响取决于目标设备处理流量的方式。有关详细信息，请参阅Snort 重启流量行为，第 18 页。

- 采取以下任何涉及应用或应用检测器的操作：
  - 激活或者停用系统或自定义应用检测器。
  - 删除激活的自定义检测器。
  - **保存并重新激活**已激活的自定义检测器。
  - 创建用户定义的应用。

  系统会提醒您继续操作会重新启动所有受管设备上的Snort进程，并允许您取消；重启会在当前域或其任何子域中的任何受管设备上发生。
- 创建或中断 威胁防御高可用性对 - 系统会提醒您继续操作会重新启动所有受管设备上的 Snort 进程，并允许您取消。

策略比较

要查看策略更改是否符合您的组织的标准或优化系统性能，您可以检查两个策略之间的区别，或者已保存策略和正在运行策略之间的区别。

您可以比较以下策略类型：

- DNS
- 文件
- 健康状况
- 身份
- 入侵（仅限 Snort 2 策略）
- 网络分析
- SSL

比较视图以并排形式显示两个策略。突出显示两个策略之间的差异：

- 蓝色表示两个策略中此突出显示的设置存在不同，并且用红色文本注明其不同之处。
- 绿色表示突出显示的设置出现在一个策略中但未出现在另一个策略中。

比较策略

仅当您有特定策略的访问权限和任何所需的许可，并且处于配置该策略的正确域中时，才能比较策略。

过程

步骤 1 访问要比较的策略的管理页面：

- DNS - **策略** > **访问控制** > **DNS**
- 文件 - **策略** > **访问控制** > **恶意软件和文件**
- 运行状况 - **系统**（⚙） > **运行状况** > **策略**
- 身份 - **策略** > **访问控制** > **身份**
- 入侵 - **策略** > **访问控制** > **入侵**

  注释 您只能比较 Snort 2 策略。

- 网络分析 - **策略** > **访问控制**，然后点击 **网络分析策略** 或 **策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

- SSL - **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**

步骤 2 点击**比较策略 (Compare Policies)**。

步骤 3 从**对比 (Compare Against)** 下拉列表中，选择要进行的比较类型：

- 要比较两个不同的策略，请选择**其他策略 (Other Policy)**。
- 要比较同一策略的两个版本，请选择**其他版本 (Other Revision)**。
- 要将其他策略与当前有效的策略进行比较，请选择**运行配置 (Running Configuration)**。

步骤 4 根据所选的比较类型，您将具有以下选项：

- 如果要比较两个不同的策略，请从**策略 A (Policy A)** 和**策略 B (Policy B)** 下拉列表中选择要比较的策略。
- 如果要比较运行配置与其他策略，请从**策略 B (Policy B)** 下拉列表中选择第二个策略。

步骤 5 点击**确定 (OK)**。

步骤 6 查看比较结果：

- 比较查看器 - 要使用比较查看器逐个浏览策略差异，请点击标题栏上方的**上一个 (Previous)**或**下一个 (Next)**。
- 比较报告 - 要生成 PDF 报告来列出两个策略之间的差异，请点击**比较报告 (Comparison Report)**。

策略报告

对于大多数策略，可以生成两种报告。有关单个策略的报告提供该策略的当前已保存配置的详细信息，而比较报告仅列出两个策略之间的区别。您可以为运行状况策略之外的所有策略类型生成单策略报告。

注释 入侵策略报告将基本策略中的设置与策略层的设置组合在一起，不区分源自基本策略或策略层的设置。

生成当前策略报告

仅当您有特定策略的访问权限和任何所需的许可，并且处于配置该策略的正确域中时，才能生成策略报告。

过程

步骤 1 访问要为其生成报告的策略的管理页面：

- 访问控制 -**策略** > **访问控制**
- DNS - **策略** > **访问控制** > **DNS**
- 文件 - **策略** > **访问控制** > **恶意软件和文件**
- 运行状况 - **系统**（⚙） > **运行状况** > **策略**
- 身份 - **策略** > **访问控制** > **身份**
- 入侵 - **策略** > **访问控制** > **入侵**
- NAT-**设备** > **NAT**
- 网络分析 - **策略** > **访问控制**，然后点击 **网络分析策略** 或 **策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**

  注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

- SSL - **策略 (Policies)** > **访问控制 (Access Control)** > **SSL**

步骤 2 点击要生成报告的策略旁边的**报告**（）。

过时策略

Firepower 系统使用红色状态文本标记过期策略，表明其需要策略更新的目标设备的数量。要清除此状态，必须将策略重新部署到设备。

要求策略重新部署的配置更改包括：

- 修改访问控制策略：对访问控制规则、默认操作、策略目标、安全情报过滤、高级选项（包括预处理）等等的任何更改。
- 修改访问控制策略调用的任何策略：SSL 策略、网络分析策略、入侵策略、文件策略、身份策略或 DNS 策略。
- 更改访问控制策略或其调用的策略中所使用的任何可重用对象或配置：
  - 网络、端口、VLAN 标记、URL 和地理位置对象。
  - 安全情报列表和源
  - 应用过滤器或检测器
  - 入侵策略变量集
  - 文件列表
  - 与解密相关的对象和安全区域

- 更新系统软件、入侵规则或漏洞数据库 (VDB)。

请记住，可以从 Web 界面中的多个位置更改其中某些配置。例如，可以使用对象管理器（**对象** > **对象管理**）修改安全区域，但是修改设备配置（**设备** > **设备管理**）中的接口类型还可更改区域并要求策略重新部署。

请注意，以下更新**不**要求策略重新部署：

- 使用上下文菜单自动对安全情报源进行更新和对安全情报全局阻止或不阻止列表进行添加
- 对 URL 过滤数据的自动更新
- 计划的地理位置数据库 (GeoDB) 更新

有限部署的性能注意事项

通过主机、应用和用户发现数据，系统可以创建完整、最新的网路配置文件。系统还可用作入侵检测和防御系统 (IPS)，分析网络流量是否存在入侵和漏洞利用，或者丢弃攻击性数据包。

将发现和 IPS 组合可提供网络活动情景并允许您利用许多功能，包括：

- 影响标志和危害指示，可以告诉您哪些主机易受特定漏洞、攻击或某种恶意软件的攻击
- 自适应配置文件 和思科 建议，允许您根据目标主机以不同方式检查流量
- 关联，允许您根据受影响主机以不同方式响应入侵（和其他事件）

但是，如果您的组织对仅执行 IPS 或仅执行发现感兴趣，则有一些配置可以优化系统的性能：

不带入侵防御的发现

通过发现功能，可以监控网络流量并确定网络上主机（包括网络设备）的数量和类型，以及这些主机上的操作系统、活动应用和开放式端口。您还可以配置受管设备以监控网络上的用户活动。可以使用发现数据执行流量量变分析，评估网络合规性和对策略违规作出响应。

在基本部署中（仅包含发现和简单、基于网络的访问控制），可以通过在配置设备的访问控制策略时遵循一些重要准则来提高该设备的性能。

注释 必须使用访问控制策略，即使其只是允许所有流量也如此。网络发现策略**只**能检查访问控制策略允许通过的流量。

首先，确保访问控制策略不要求复杂的处理并仅使用简单、基于网络的条件处理网络流量。必须实施以下**所有**准则；错误配置其中任何一个选项都会消除性能优势：

- 请**勿**使用安全情报功能。从策略的安全情报配置中移除任何已填充的全局阻止或不阻止列表。
- 请**勿**包含具有 Monitor 或 Interactive Block 操作的访问控制规则。仅使用 Allow、Trust 和 Block 规则。请记住，可以通过发现检查允许的流量，但无法检查受信任和受阻止的流量。

- 请**勿**包含具有应用、用户、URL，ISE 属性或基于地理位置的网络条件的访问控制规则。仅使用简单的基于网络的条件：区域、IP 地址、VLAN 标记和端口。
- 请**勿**包含执行文件、恶意软件或入侵检查的访问控制规则。换句话说，请勿将文件策略或入侵策略与任何访问控制规则相关联。
- 在访问控制策略的“高级”(Advanced) 设置中，确保**确定访问控制规则前使用的入侵策略 (Intrusion Policy used before Access Control rule is determined)** 被设为**没有活动规则 (No Rules Active)**。
- 选择 **Network Discovery Only** 作为策略的默认操作。请**勿**为执行入侵检查的策略选择默认操作。

与访问控制策略相结合，可以配置并部署网络发现策略，它指定系统为发现数据检查的网段、端口和区域，以及是否在网段、端口和区域上发现了主机、应用和用户。

相关主题

在识别流量之前检查通过的数据包

不带发现的入侵防御

在不需要的情况下禁用发现（例如，在仅限 IPS 的部署中）可以提高性能。要禁用发现，必须实施所有这些更改：

- 从网络发现策略中删除所有规则。
- 仅使用简单的、基于网络的条件执行访问控制：区域、IP 地址、VLAN 标记和端口。

  不执行任何类型的安全情报、应用、用户、URL 或地理位置控制。虽然可以禁止系统存储发现数据，但系统仍须收集和检查该数据才能实施这些功能。
- 通过从访问控制策略的安全情报配置中删除所有阻止和不阻止列表（包括默认全局名单）来禁用基于网络和 URL 的安全情报。
- 通过删除或禁用关联的 DNS 策略中的所有规则（包括 DNS 的默认全局不阻止列表和 DNS 规则的全局阻止列表）来禁用基于 DNS 的安全情报。

部署后，目标设备上会停止进行新发现。系统会根据超时偏好设置逐渐删除网络映射中的信息。或者，可以立即清除所有发现数据。

配置部署的历史记录

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。