



访问控制规则

以下主题介绍如何配置访问控制规则：

- [访问控制规则简介，第 1 页](#)
- [访问控制规则的要求和必备条件，第 9 页](#)
- [访问控制规则的准则与限制，第 9 页](#)
- [管理访问控制规则，第 10 页](#)
- [访问控制规则的示例，第 25 页](#)

访问控制规则简介

在访问控制策略中，访问控制规则提供在多台受管设备之间处理网络流量的精细方法。

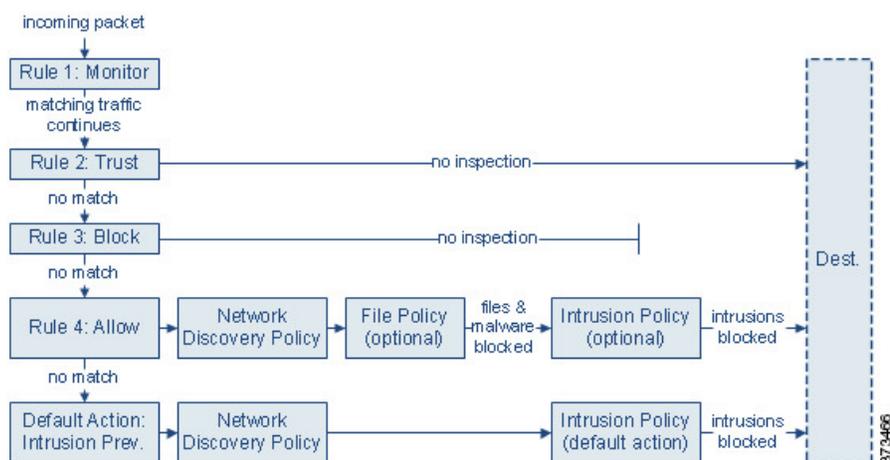


注释 安全情报过滤、解密、用户标识以及某些解码和预处理发生在访问控制规则评估网络流量之前。

系统按您指定的顺序将流量与访问控制规则相匹配。在大多数情况下，系统根据所有规则条件匹配流量的第一个访问控制规则处理网络流量。

每个规则也有操作，确定是否监控、信任、阻止或允许匹配的流量。当您允许流量时，可以指定在流量到达您的资产或退出您的网络之前，系统首先利用入侵或文件策略对其进行检查以阻止任何漏洞攻击、恶意软件或禁止的文件。

以下场景汇总了内联入侵防御部署中访问控制规则评估流量的方式。



在这种情况下，流量评估如下：

- 首先，由规则 **1：监控 (Rule 1: Monitor)** 评估流量。“监控” (Monitor) 规则跟踪和记录网络流量。系统继续根据其他规则匹配流量，以确定允许其通过，还是拒绝。（但是，请参阅[访问控制规则监控操作](#)，第 6 页中的重要例外情况和警告。）
- 规则 **2：Trust** 继续评估流量。系统允许匹配的流量传至目标，而无需进一步检查，但此类流量仍会受到身份要求和速率限制的制约。不匹配的流量继续根据下一规则进行评估。
- 第三，由规则 **3：阻止 (Rule 3: Block)** 评估流量。匹配的流量被阻止，无需进一步检测。不匹配的流量继续根据最终规则进行评估。
- 规则 **4：允许 (Rule 4: Allow)** 是最终规则。对于此规则，允许匹配的流量；但检测和阻止流量内禁止的文件、恶意软件、入侵和漏洞。系统允许其余未阻止的非恶意流量传至目标，但此类流量仍受到身份要求和速率限制的制约。您可以配置只执行文件检查、入侵检查或两类检查都不执行的“允许” (Allow) 规则。
- **Default Action** 处理不匹配任何规则的所有流量。在此场景下，默认操作在允许非恶意流量通过之前执行入侵防御。在不同的部署中，您可能有默认操作可以信任或阻止所有流量，而无需进一步检测。（您不能对默认操作处理的流量执行文件或恶意软件检测。）

无论是使用访问控制规则还是默认操作，您允许的流量都自动可用于根据网络发现策略检查主机、应用和用户数据。尽管可以增强或禁用发现功能，但不能明确启用该功能。但是，允许流量不会自动确保收集发现数据。系统仅对涉及 IP 地址的连接执行发现功能，根据网络发现策略明确监控这些 IP 地址；此外，对于加密会话，应用发现受到限制。

请注意，当解密配置允许已加密流量通过或者您不配置解密时，访问控制规则处理已加密流量。但是，某些访问控制规则条件需要未加密流量，因此，已加密流量可能匹配的规则更少。此外，默认情况下，系统禁用已加密负载的入侵和文件检查。当已加密连接与已配置入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。

访问控制规则管理

访问控制策略编辑器的规则表格让您添加、编辑、分类、搜索、过滤、移动、启用、禁用、删除或以其他方式管理当前策略中的访问控制规则。

正确创建和排序访问控制规则是一项复杂的任务，但重要的是构建有效部署。如果不认真规划您的策略，这些规则会抢占其他规则，需要额外的许可证或包含无效配置。为帮助确保系统按预期处理流量，访问控制策略接口具有规则的强大警告和错误反馈系统。

使用搜索栏来过滤访问控制策略规则列表。在新用户界面中，您可以取消选择**仅显示匹配规则 (Show Only Matching Rules)** 选项以查看所有规则。匹配的规则会被突出显示。

对于每个访问控制规则，策略编辑器显示其名称、条件概述、规则操作以及传达规则检测选项或状态的图标。在新用户界面中，操作和图标位于左侧而不是右侧，并且许多图标不会显示以便让视图更简洁（显示入侵、文件和日志记录，时间范围显示为钟面而不是如下所示的图标）。这些图标代表：

- 时间范围选项 (🕒)
- 入侵策略 (🛡️)
- 文件策略 (📁)
- 安全搜索 (🔍)
- YouTube EDU (📺)
- 日志记录 (📄)
- 注释 (💬)
- 警告 (⚠️)
- 错误 (❌)

已禁用的规则在规则名称后面呈灰色显示并带有相应的标记“(已禁用)”(disabled)。

要创建或编辑规则，请使用访问控制规则编辑器。规则编辑器会因您使用的用户界面而异。

旧版用户界面 - 您可以：

- 在编辑器的上部配置基本属性，如规则的名称、状态、位置和操作。
- 使用编辑器下部左侧的选项卡添加条件。
- 使用下部右侧的选项卡配置检测和日志记录选项，还可以向规则添加注释。为了方便，无论您在查看哪个选项卡，编辑器都列出规则的检测和日志记录选项。

新版用户界面 - 您可以：

- 配置规则名称并选择其在编辑器上部的位置。

- 通过选择编辑器上方或下方的行可以切换到编辑其他规则。
- 使用左侧列表来选择规则操作，并应用入侵策略和变量集、文件策略和时间范围以及顶部的日志记录选项。
- 使用规则名称旁边的选项来选择规则操作，并应用入侵策略和变量集、文件策略和时间范围以及顶部的日志记录选项。
- 使用源 (**Sources**) 和目标和应用 (**Destinations and Applications**) 列来添加匹配条件。
- 在编辑器的底部为规则添加评论。

相关主题

[访问控制规则组成部分](#)，第 4 页

[访问控制规则的最佳实践](#)

访问控制规则组成部分

除唯一名称之外，每个访问控制规则都具有以下基本组件：

状态

默认情况下，规则处于启用状态。如果禁用某规则，系统将不使用该规则并停止为该规则生成警告和错误。

位

系统已对访问控制策略中的规则进行编号，从 1 开始。如果正在使用策略继承，则规则 1 是最外层策略的第一条规则。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。除 Monitor 规则之外，流量匹配的第一个规则是处理该流量的规则。

规则也可属于某个部分和某个类别，其仅有利于组织且不影响规则位置。规则位置跨越部分和类别。

部分和类别

为帮助您组织访问控制规则，每个访问控制策略都有两个系统提供的规则部分：“强制性” (Mandatory) 规则部分和“默认” (Default) 规则部分。要进一步组织访问控制规则，您可以在“强制性” (Mandatory) 和“默认” (Default) 部分中创建自定义规则类别。

如果正在使用策略继承，则当前策略的规则嵌套在其父策略的“强制性” (Mandatory) 规则部分与“默认” (Default) 规则部分之间。

条件

条件指定规则处理的特定流量。条件可以简单也可以复杂；条件的使用通常取决于许可证。

流量必须满足规则中指定的所有条件。例如，如果应用条件指定了 HTTP 而不是 HTTPS，则 URL 类别和信誉条件将不适用于 HTTPS 流量。

适用时间

您可以指定规则适用的日期和时间。

操作

规则操作确定系统如何处理匹配的流量。您可以监控、信任、阻止或允许（执行或无需执行进一步检测）匹配的流量。系统不会对受信任、被阻止或加密的流量进行深度检查。

检查

深度检查选项管理系统如何检查和阻止您意外允许的恶意流量。通过规则允许流量时，可以指定系统先使用入侵或文件策略检测流量以在漏洞、恶意软件或禁止的文件到达您的资产或退出网络之前予以阻止。

日志记录

规则的日志记录设置管理系统保存其处理流量的记录。您可以对匹配规则的流量保存记录。一般来说，您可以在连接开始和/或结束时记录会话。您可以将连接记录到数据库，以及系统日志 (syslog) 或 SNMP 陷阱服务器。

备注

每次保存对访问控制规则所做的更改时，都可以添加注释。

相关主题

[访问控制规则的最佳实践](#)

[访问控制规则管理](#)，第 3 页

[创建和编辑访问控制规则](#)，第 10 页

[访问控制规则操作](#)，第 6 页

[访问控制规则条件](#)，第 12 页

[使用文件和入侵策略的深度检测](#)

[访问控制规则注释](#)

访问控制规则顺序

系统已对访问控制策略中的规则进行编号，从 1 开始。系统会用升序的规则号码以从上到下的顺序将流量匹配到访问控制规则中。

在大多数情况下，系统根据所有规则条件匹配流量的第一个访问控制规则处理网络流量。除监控规则，在流量匹配规则后系统不会根据其他优先级较低的规则继续评估流量。

为帮助您组织访问控制规则，每个访问控制策略都有两个系统提供的规则部分：“强制性” (Mandatory) 规则部分和“默认” (Default) 规则部分。要进一步组织，您可以在“强制性” (Mandatory) 和“默认” (Default) 部分中创建自定义规则类别。在创建类别后，无法将其移动，不过可以将其删除、对其重命名，并将规则移入、移出该类别以及在其内部或周围移动。系统跨部分和类别分配规则编号。

如果使用策略继承，则当前策略的规则嵌套在其父策略的“强制性”(Mandatory)规则部分与“默认”(Default)规则部分之间。规则1是最外层策略（不是当前策略）中的第一条规则，系统跨策略、部分和类别分配规则编号。

允许修改访问控制策略的任何预定义用户角色还允许您在规则类别内部和之间移动和修改访问控制规则。但是，可以创建自定义角色来限制用户移动和修改规则。允许修改访问控制策略的任意用户可以

可以将规则添加到自定义类别，以及无限制的修改其中的规则。



注意 未能正确设置访问控制规则可能会导致意外结果，包括允许应阻止的流量。通常，应用控制规则应在访问控制列表中较低，因为与基于 IP 地址的规则相比，匹配这些规则所需的时间更长。

使用特定条件（例如网络和 IP 地址）的访问控制规则应在使用一般条件（例如应用）的规则之前排序。如果您熟悉开放系统互联（OSI）模型，请在概念上使用类似的编号。包含第1层、第2层和第3层（物理、数据链路和网络）条件的规则应首先在访问控制规则中排序。稍后应在访问控制规则中对第5层、第6层和第7层的条件（会话，表示和应用）进行排序。有关OSI模型的详细信息，请参阅此 [维基百科文章](#)。



提示 适当的访问控制规则顺序可减少处理网络流量所需的资源并防止规则抢占。尽管您创建的规则对于每个组织和部署来说都是唯一的，但是排序规则时需要遵循几个基本原则，才可优化性能，同时满足您的需求。

相关主题

[订购规则的最佳实践](#)

访问控制规则操作

每个访问控制规则都具有用于确定系统如何处理和记录匹配流量的操作：您可以监控、信任、阻止或允许（执行或无需执行进一步检查）匹配流量。

访问控制策略的默认操作会处理不符合任何非 Monitor 访问控制规则条件的流量。

访问控制规则监控操作

监控 (Monitor) 操作不能允许或拒绝流量。相反，它的主要目的是强制连接日志记录，而不会考虑最终如何处理匹配的流量。

如果连接与监控规则匹配，则该连接匹配的下一个非监控规则应确定流量处理和任何进一步检查。如果没有其他匹配的规则，系统应使用默认操作。

但存在一个例外。如果监控规则包含第7层条件（例如应用条件），则系统将允许早期数据包通过并建立连接（或完成 SSL 握手）。即使连接应被后续规则阻止，也会发生这种情况；这是因为这些早期数据包不会根据后续规则接受评估。为了使这些数据包不会未经检查就到达目的地，您可以在访问控制策略的高级设置中为此目的指定入侵策略；请参阅[在识别流量之前检查通过的数据包](#)。在系统完成其第7层识别后，它就会将相应的操作应用于剩余会话流量。



注意 最佳实践是避免将第 7 层条件放在规则优先级较高的广泛定义的监控规则上，以防止无意中允许流量进入您的网络。此外，如果本地约束的流量与第 3 层部署中的 Monitor 规则相匹配，则该流量可能绕过检查。为确保对流量进行检查，在路由流量的受管设备的高级设备设置中启用 **Inspect Local Router Traffic**。

访问控制规则信任操作

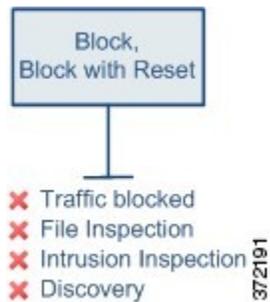
信任 (**Trust**) 操作允许流量通过，无需深度检查或网络发现。受信任的流量仍会受到身份要求和速率限制的制约。



注释 某些协议（例如 FTP 和 SIP）会使用辅助信道，而系统会通过检测过程将其打开。在某些情况下，受信任的流量可以绕过所有检查，并且无法正确打开这些辅助通道。如果遇到此问题，请将信任规则更改为允许 (**Allow**)。

访问控制规则阻止操作

Block 和 **Block with reset** 操作拒绝流量，无需任何类型的进一步检测。



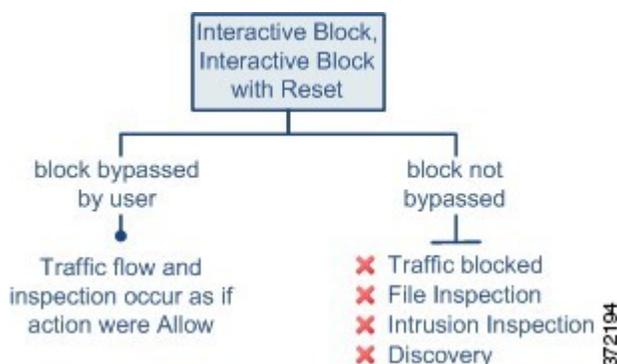
“阻止并重置”规则会重置连接，但 *HTTP* 响应页面遇到的 Web 请求除外。这是因为，如果立即重置连接，则配置为在系统阻止 Web 请求时显示的响应页面将无法显示。有关详细信息，请参阅[HTTP 响应页面和交互式阻止](#)。

相关主题

[配置 HTTP 响应页面](#)

访问控制规则交互式阻止操作

交互式阻止和交互式阻止并重置操作为 Web 用户提供继续访问其预期目的地的选项。



如果用户绕过阻止，该规则模拟“允许”规则。因此，您可以将交互式阻止规则与文件和入侵策略关联，并且匹配的流量也可用于网络发现。

如果用户未（或无法）绕过阻止，该规则模拟“阻止”规则。匹配流量会被拒绝，无需进一步检测。

请注意，如果启用交互式阻止，则无法重置所有被阻止的连接。这是因为，如果立即重置连接，响应页面将无法显示。使用**交互式阻止并重置**操作，以（通过非交互的方式）阻止并重置所有非 Web 流量，同时仍然为 Web 请求启用交互式阻止。

有关详细信息，请参阅[HTTP 响应页面和交互式阻止](#)。

相关主题

[TLS/SSL 规则 阻止操作](#)

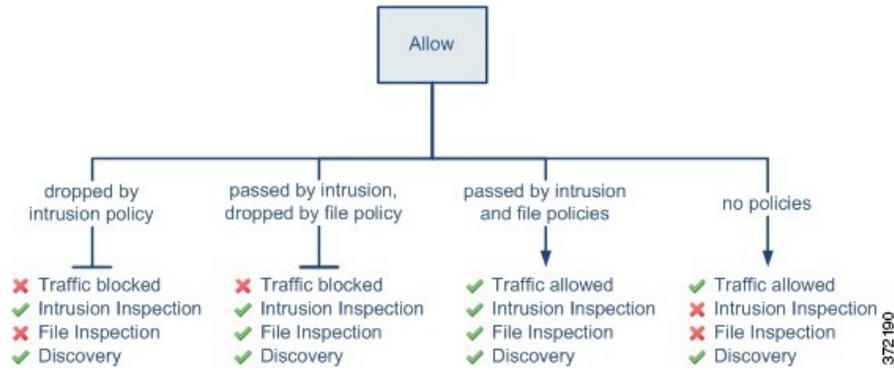
访问控制规则允许操作

允许 (Allow) 操作允许匹配的流量通过，但是仍会受到身份要求和速率限制的制约。

或者，您可以使用深度检查以在未加密或已解密流量到达目的地之前进一步对其进行检查和阻止：

- 您可以使用入侵策略，以便根据入侵检测和防御配置来分析网络流量，并根据配置丢弃恶意数据包。
- 您可使用文件策略执行文件控制。借助文件控制，可以检测和阻止用户通过特定应用协议上传（发送）或下载（接收）特定类型的文件。
- 您还可以使用文件策略执行基于网络的高级恶意软件防护 (AMP)。恶意软件防护 可检测文件中的恶意软件，并根据配置阻止检测到的恶意软件。

下图展示对满足“允许” (Allow) 规则（或用户绕过的“交互式阻止” [Interactive Block] 规则）条件的流量执行的检查类型。请注意，文件检测会在入侵检测之前发生；被阻止文件不会进行入侵相关漏洞检测。



为简单起见，该图显示入侵和文件策略均与访问控制规则相匹配（或都不匹配）的情况下的流量。但是，可以单独配置其中一个策略。如果没有文件策略，流量将由入侵策略确定；如果没有入侵策略，流量将由文件策略确定。

不管入侵或文件策略会检查还是丢弃流量，系统都可以使用网络发现功能进行检查。但是，允许流量不会自动确保发现检查。系统仅对涉及 IP 地址的连接执行发现功能，根据网络发现策略明确监控这些 IP 地址；此外，对于加密会话，应用发现受到限制。

访问控制规则的要求和必备条件

型号支持

任意

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

访问控制规则的准则与限制

- 如果编辑正在使用的访问控制规则，则更改不会在部署时应用于已建立的连接。此更新的规则用于根据未来的连接进行匹配。但是，如果系统正在主动检查连接（例如，使用入侵策略），则会 将更改的匹配或操作条件应用于现有连接。

对于威胁防御，您可以通过使用威胁防御 **clear conn** CLI 命令结束已建立的连接，确保您的更改适用于所有当前连接。请注意，你应该只在结束这些连接是可以接受的情况下才这样做，前提是连接的来源将试图重新建立连接，从而与新规则进行适当的匹配。

- 访问规则中的 VLAN 标记仅适用于内联集；它们不能在应用于防火墙接口的访问规则中使用。

管理访问控制规则

以下主题介绍了如何管理访问控制规则。

添加访问控制规则类别

您可以将访问控制策略的“强制性” (Mandatory) 和“默认” (Default) 规则部分划分为自定义类别。在创建类别后，无法将其移动，不过可以将其删除、对其重命名，并将规则移入、移出该类别以及在其内部或周围移动。系统跨部分和类别分配规则编号。

过程

步骤 1 在访问控制策略编辑器中，点击**添加类别 (Add Category)**。

提示 如果您的策略已经包含规则，则可以点击现有规则在该行的空白区域，先设置新类别的位置，然后才能添加。还可以右键点击现有规则并选择 **Insert new category**。

步骤 2 输入 **Name**。

步骤 3 从**插入 (Insert)** 下拉列表中，选择要添加类别的位置：

- 要在某个部分中的所有现有类别下方插入类别，请选择**插入强制性类别 (into Mandatory)** 或 **插入默认类别 (into Default)**。
- 要在现有类别上方插入类别，请选择**类别上方 (above category)**，然后选择类别。
- 要在访问控制规则上方或下方插入类别，请选择**规则上方 (above rule)** 或 **规则下方 (below rule)**，然后输入现有规则编号。

步骤 4 点击**确定 (OK)**。

步骤 5 点击**保存 (Save)** 保存策略。

创建和编辑访问控制规则

使用访问控制规则将操作应用于特定流量类。规则允许您选择性地允许所需流量并丢弃不需要的流量。

过程

步骤 1 在访问控制策略编辑器中，您有以下选择：

- 要添加新规则，请点击 **Add Rule**。
- 要编辑现有规则，请点击 **编辑** (✎) (旧版UI)。在 **新建 UI**中，右键单击或 **更多** (⋮) 菜单中提供 **编辑**。
- 要编辑多个规则，请按住 **Shift** 键并点击一系列规则，或按住 **Control** 键并点击要编辑的多个规则，然后右键单击并选择一个选项。在 **新建 UI**中，使用复选框选择多个规则，然后从搜索框旁边的 **选择操作** 列表中选择 **编辑** 或其他操作。

如果规则旁显示视图 (👁)，则表明规则属于祖先策略，或者您没有修改规则的权限。

步骤 2 如果这是新规则，请输入 **名称**。

步骤 3 (旧版 UI。) 配置规则组成部分。

如果批量编辑多个规则，则只有一部分选项可用。

- **已启用** -指定规则是否为已启用。
- **位置** - 指定规则位置；请参阅[访问控制规则顺序](#)，第 5 页。
- **操作** - 在**操作 (Action)** 中选择规则操作；请参阅[访问控制规则操作](#)，第 6 页。
- **时间范围**- (可选)。对于 **威胁防御** 设备，请选择规则适用的日期和时间。有关详细信息，请参阅[创建时间范围对象](#)。
- **条件** - 点击要添加的对应条件。有关详细信息，请参阅[访问控制规则条件](#)，第 12 页。

注释 访问规则中的 VLAN 标记仅适用于内联集；它们不能在应用于防火墙接口的访问规则中使用。

- **深度检测**- (可选)。对于允许和交互组织规则，点击 **入侵策略** (🛡) 或 **文件策略** (📁) 配置规则的 **检查** 选项。如果选项呈灰色显示，则表示没有为规则选择此类型的策略。有关详细信息，请参阅[访问控制概述](#)。
- **内容限制** - 点击 **安全搜索** (🔒) 或 **YouTube EDU** (📺) 以配置规则编辑器的 **应用** 选项卡上的内容限制设置。如果选项呈灰色显示，则表示对规则禁用内容限制。有关详细信息，请参阅[关于内容限制](#)。
- **日志记录** - 点击 **日志记录** (📄) 以指定 **日志记录** 选项。如果选项呈灰色显示，则表示对规则禁用连接日志记录。
- **注释** - 点击注释列中的数值可添加**注释 (Comments)**。编号指示规则已包含的注释数。

步骤 4 (**新建 UI**) 配置规则组成部分。

如果批量编辑多个规则，则只有一部分选项可用。

- 位置 - 指定规则位置；请参阅[访问控制规则顺序](#)，第 5 页。
- 操作 - 在操作 (**Action**) 中选择规则操作；请参阅[访问控制规则操作](#)，第 6 页。
- 深度检测-(可选)。对于允许和交互阻止规则，选择[入侵策略](#)，[变量集](#)和[文件策略](#)选项。您可以单独应用入侵和文件策略；您不需要同时配置两者。
- 时间范围-(可选)。对于威胁防御设备，请选择规则适用的日期和时间。如果不选择选项，则规则始终处于活动状态。有关详细信息，请参阅[创建时间范围对象](#)。
- 日志记录-点击[日志记录](#)可指定连接日志记录和 SNMP 陷阱的选项。
- 条件-点击[源](#)和[目标](#)列中的+以添加连接的匹配条件。有关详细信息，请参阅[访问控制规则条件](#)，第 12 页。
- 注释-打开对话框底部的注释列表，输入注释，然后点击[发布](#)添加注释。

步骤 5 点击**确定**以保存该规则。

步骤 6 点击**保存 (Save)**保存策略。

下一步做什么

如果要部署基于时间的规则，请指定策略分配到的设备的时区。请参阅[为策略应用配置设备时区](#)。
部署配置更改。

相关主题

[访问控制规则的最佳实践](#)

访问控制规则条件

规则条件定义要使用每条规则作为目标的连接的特征。精确使用条件来微调规则，以应用于仅应由规则处理的流量。以下主题介绍可使用的匹配条件。

安全/隧道区域规则条件

可以使用安全区域和隧道区域为规则选择流量。

安全区域可对网络进行分段，以通过跨多个设备将接口分组来帮助管理和分类流量。隧道区域允许您识别应作为隧道处理的隧道流量（例如 GRE），而不是将访问控制规则应用于隧道内的封装连接。

您可以使用安全区域按源接口和目标接口控制流量。如果将源区域和目标区域均添加到区域条件中，则匹配流量必须源自其中一个源区域的接口，并通过其中一个目标区域的接口流出，以匹配规则。正如安全区域中的所有接口都必须为同一类型（均为内联、被动、交换或路由），区域条件中使用的所有区域也必须为同一类型。由于被动部署的设备不会传输流量，因此不能使用具有被动接口的区域作为目标区域。

使用隧道区域时，请确保预过滤器策略中有匹配的规则，以将隧道流量与该区域相关联。然后，您可以选择隧道区域作为规则中的源区域；隧道区域不能是目的地。如果没有将隧道重新分区到隧道

区域的预过滤器规则，则隧道的访问控制规则将永远不会应用于任何连接。您可以将目标安全区域指定为通过特定接口离开设备的目标隧道。

安全区域注意事项

在决定安全区域标准时，请考虑以下事项：

- 尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。
- 访问控制规则会在设备配置中生成 ACL 条目 (ACE)，以便尽可能提供早期处理和丢弃。如果在规则中指定安全区域，则会为区域中的每个接口创建 ACE，这会大大增加 ACL 的大小。从访问控制规则生成的过大 ACL 可能会影响系统性能。
- 在多域部署中，在祖先域中创建的区域可以包含位于不同域中的设备上的接口。在后代域中配置区域条件时，您的配置仅适用于可以看到的接口。

网络规则条件

网络规则条件是定义流量的网络地址或位置的网络对象或地理位置。

- 要匹配来自某个 IP 地址或地理位置的流量，请将条件添加到源列表。
- 要将流量匹配到某个 IP 地址或地理位置，请将条件添加到目标列表。
- 如果同时向一条规则添加源网络条件和目标网络条件，匹配流量必须源自其中一个指定 IP 地址并流向其中一个目标 IP 地址。

添加此条件时，可从以下选项卡中进行选择：

- **网络** - 为您要控制的流量选择定义源或目标 IP 地址的网络对象或组。您可以使用通过完全限定域名 (FQDN) 定义地址的对象；通过 DNS 查询确定地址。
- **地理位置** - 选择要基于流量的源或目的国家/地区或大洲控制流量的地理位置。选择大洲将会选择该大洲内的所有国家/地区。除了直接在规则中选择地理位置外，也可以选择您创建的地理位置对象来定义位置。使用地理位置，可以便捷地限制对特定国家/地区的访问，而不需要知道此位置所用的全部潜在 IP 地址。



注释 为了确保使用最新的地理位置数据来过滤流量，思科强烈建议您定期更新地理位置数据库 (GeoDB)。

网络条件中的原始客户端（过滤代理流量）

对于某些规则，可以根据始发客户端处理代理流量。使用源网络条件指定代理服务器，然后添加原始客户端限制以指定原始客户端 IP 地址。系统将使用数据包的 X-Forwarded-For (XFF)、真实客户端 IP 或自定义的 HTTP 标头报头字段来确定原始客户端 IP。

如果代理的 IP 地址与规则的源网络限制匹配，并且原始客户端的 IP 地址与规则的原始客户端限制匹配，则流量与规则匹配。例如，要允许来自特定原始客户端地址的流量，但仅允许其中使用特定代理的流量，请创建三条访问控制规则：

访问控制规则 1：阻止来自特定 IP 地址 (209.165.201.1) 的代理流量

源网络：209.165.201.1
原始客户端网络：无/任意
Action: Block

访问控制规则 2：允许来自同一 IP 地址的代理流量，但只允许其代理服务器为您所选的代理服务器 (209.165.200.225 或 209.165.200.238) 的流量

源网络：209.165.200.225 和 209.165.200.238
原始客户端网络：209.165.201.1
Action: Allow

访问控制规则 3：阻止来自同一 IP 地址但使用任何其他代理服务器的代理流量。

源网络：任意
原始客户端网络：209.165.201.1
Action: Block

VLAN 标记规则条件



注释 访问规则中的 VLAN 标记仅适用于内联集。带 VLAN 标记的访问规则与防火墙接口上的流量不匹配。

VLAN 规则条件可控制 VLAN 标记的流量，包括 Q-in-Q（堆栈 VLAN）流量。系统使用最内层的 VLAN 标记过滤 VLAN 流量，但不包括预过滤器策略，因为它在其规则中使用最外层的 VLAN 标记。

请注意以下 Q-in-Q 支持：

- Firepower 4100/9300 上的威胁防御 -不支持 Q-in-Q（仅支持一个 VLAN 标记）。
- 所有其他型号上的威胁防御：
 - 内联集和被动接口-支持 Q-in-Q，最多2个 VLAN 标记。
 - 防火墙接口-不支持 Q-in-Q（仅支持一个 VLAN 标记）。

可以使用预定义对象构建 VLAN 条件，或手动输入从 1 到 4094 之间的任意 VLAN 标记。使用连字符可指定 VLAN 标记范围。

最多可以指定 50 个 VLAN 条件。

在集群中，如果遇到 VLAN 匹配问题，请编辑访问控制策略高级选项“传输/网络预处理器设置” (Transport/Network Preprocessor Settings)，然后选择跟踪连接时忽略 VLAN 信头 (**Ignore the VLAN header when tracking connections**) 选项。



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 VLAN 标记限制此配置可产生意外结果。通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

用户规则条件

用户规则条件会根据发起连接的用户或用户所属的组来匹配流量。例如，您可以配置阻止规则以禁止财务组中的任何人访问网络资源。

（仅适用于访问控制规则）您必须首先将身份策略与访问控制策略相关联，如[将其他策略与访问控制相关联](#)中所述。

除了为已配置的领域配置用户和组之外，您还可以为以下特殊身份的用户设置策略：

- 身份验证失败：强制网络门户身份验证失败的用户。
- 访客：在强制网络门户中被配置为访客用户的用户。
- 无需身份验证：匹配**无需身份验证 (No Authentication Required)** 规则操作的用户。
- 未知：无法识别的用户；例如，配置的领域未下载的用户。

应用规则条件

系统分析 IP 流量时，可以识别网络上的常用应用并将其分类。这种基于发现的应用感知是应用控制的基础 - 能够控制应用流量。

借助系统提供的应用过滤器，您可以根据应用的基本特征（类型、风险、业务关联性、类别和标记）组织应用，从而执行应用控制。您可以系统提供的过滤器的组合或以应用的自定义组合为基础，创建可重复使用的用户定义过滤器。

对于策略中的每个应用程序规则条件，必须启用至少一个检测器。如果没有为应用启用检测器，则系统会为该应用自动启用所有系统提供的检测器；如果不存在检测器，则系统为该应用启用最新修改的用户定义的检测器。有关应用检测器的详细信息，请参阅[应用检测器基础知识](#)。

您可以使用应用过滤器和单独指定的应用来确保完整覆盖。但是，在订购访问控制规则之前，请了解以下说明。

应用过滤器的优势

应用过滤器可帮助您快速配置应用控制。例如，您可以轻松地使用系统提供的过滤器创建一条访问控制规则，用于识别并阻止所有业务关联性较低的高风险应用。如果用户尝试使用其中一个应用，则系统会阻止会话。

使用应用过滤器可简化策略创建和管理。此方法可保证系统按预期控制应用流量。由于思科经常通过系统和漏洞数据库 (VDB) 更新和添加应用检测器，因此您可确保系统使用最新的检测器监控应用流量。您还可以创建自己的检测器并将特征分配给其检测到的应用，自动将应用添加到现有过滤器。

应用特征

系统使用下表中所述的条件来展示其检测到的每个应用的特征。这些特征用作应用过滤器。

表 1:应用特征

| 特征 | 说明 (Description) | 示例 |
|-------|--------------------------------------------------------------------|-------------------------------------------------------------------|
| 类型 | 应用协议代表主机之间的通信。 客户端代表在主机上运行的软件。 Web 应用代表 HTTP 流量的内容或所请求的 URL。 | HTTP 和 SSH 是应用协议。 网络浏览器和邮件客户端是客户端。 MPEG 视频和 Facebook 是网络应用。 |
| 风险 | 应用于可能违反您的组织安全策略的用途的可能性。 | 点对点应用的风险通常很高。 |
| 业务相关性 | 应用于您的组织的业务运营（相对于娱乐目的）的情景中的可能性。 | 游戏应用的业务相关性通常很低。 |
| 类别 | 说明应用的最基本功能的应用通用分类。每个应用至少属于一个类别。 | Facebook 属于社交网络类别。 |
| 标签 | 有关应用的附加信息。应用可以包括任何数量的标记，也可以没有标记。 | 视频流网络应用通常标记为 high bandwidth 和 displays ads。 |

相关主题

[配置应用控制的最佳实践](#)

配置应用条件和过滤器

要构建应用条件或过滤器，请从可用应用列表中选择要控制其流量的应用。或者，可以按照建议使用过滤器限制可用应用。在相同条件下可以使用过滤器和单独指定的应用。

开始之前

- 必须按照 [配置自适应配置文件](#) 中的说明来启用（其默认状态）自适应分析，以便访问控制规则可以执行应用控制。
- 如果要实施内容限制，请遵循 [使用访问控制规则执行内容限制](#) 中的程序而不是本程序。
- 对于经典设备型号，您必须拥有控制许可证才能配置这些条件。

过程

步骤 1 调用规则或配置编辑器：

- 访问控制（旧版 UI）、解密、QoS 规则条件 - 在规则编辑器中，点击 **应用 (Applications)**。在新的访问控制 UI 中，点击“目标和应用” (Destinations and Applications) 列中的 +，然后点击“应用” (App) 选项卡。
- 身份规则条件 - 在规则编辑器中，点击 **领域和设置 (Realm & Settings)** 并启用主动身份验证；请参阅 [创建身份规则](#)。
- 应用过滤器 - 在对象管理器的“应用过滤器” (Application Filters) 页面上，添加或编辑应用过滤器。在 **名称 (Name)** 中为过滤器提供唯一名称。

- 智能应用绕行 (IAB)- 在访问控制策略编辑器中，点击高级 (Advanced) 选项卡，编辑 IAB 设置，然后点击可绕行的应用和过滤器 (Bypassable Applications and Filters)。

步骤 2 从可用应用 (Available Applications) 列表查找并选择要添加的应用。

要限制可用应用 (Available Applications) 中显示的应用，请选择一个或多个应用过滤器 (Application Filters) 或搜索单个应用。

提示 点击应用旁边的 信息 (i) 以显示摘要信息和互联网搜索链接。解锁 标记系统只能在已解密流量中识别的应用。

选择过滤器 (单一或组合) 时，“可用应用” (Available Applications) 列表会更新为仅显示符合条件的应用。您可以选择系统提供的组合形式的过滤器，但不能选择用户定义的过滤器。

- 针对同一特征选择多个过滤器 (风险、业务关联性等) - 应用流量必须仅匹配其中一个过滤器。例如，如果选择中风险和高风险过滤器，则“可用应用” (Available Applications) 列表会显示所有中风险和高风险应用。
- 针对不同应用特征选择过滤器 - 应用流量必须与两个过滤器类型匹配。例如，如果您选择高风险和低业务关联性过滤器，则“可用应用” (Available Applications) 列表仅显示满足这两个条件的应用。

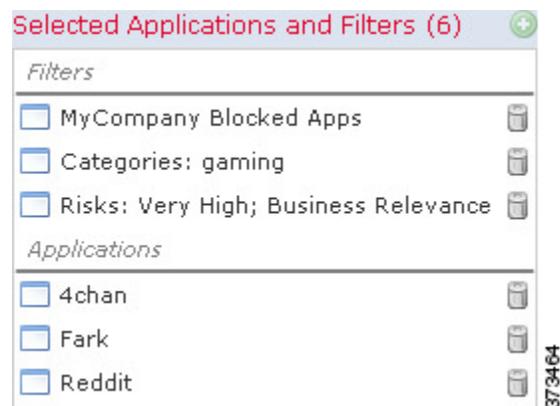
步骤 3 点击添加到规则 (Add to Rule)，或进行拖放操作。在新的访问控制 UI 中，点击 添加应用 (Add Application)。

提示 在添加更多过滤器和应用之前，点击清除过滤器 (Clear Filters) 以清除当前选择。

步骤 4 保存或继续编辑规则或配置。

示例：访问控制规则中的应用条件

下图显示用于阻止以下内容的访问控制规则的应用条件：MyCompany 的用户定义应用过滤器、具有高风险和低业务关联性的所有应用、游戏应用以及一些单独选定的应用。



下一步做什么

- 部署配置更改。

端口、协议和 ICMP 代码规则条件

端口条件根据源和目标端口匹配流量。根据规则类型，“端口”可以表示以下任何一项：

- TCP 和 UDP - 可以根据端口控制 TCP 和 UDP 流量。系统使用括号内的协议号，以及可选的关联端口或端口范围来表示此配置。例如：TCP(6)/22。
- ICMP - 可以根据 ICMP 和 ICMPv6 (IPv6-ICMP) 流量的互联网层协议及可选类型和代码控制该流量。例如：ICMP(1):3:3。
- 协议-您可以借助于未使用端口的其他协议控制流量。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

基于端口的规则的最佳实践

指定端口是目标应用的传统方式。但是，可以将应用配置为使用唯一端口绕过访问控制块。因此，尽可能使用应用过滤条件而不是端口条件来确定流量目标。请注意，应用过滤在预过滤器规则中不可用。

应用过滤也建议用于动态打开单独通道的应用（如 FTP），以实现控制和数据流。使用基于端口的访问控制规则可能会阻止此类应用正确执行，并可能导致阻止所需的连接。

使用源端口和目标端口限制

如果同时添加源端口和目标端口限制，则只能添加共享单一传输协议（TCP 或 UDP）的端口。例如，如果添加经由 TCP 的 DNS 作为源端口，则可以添加 Yahoo Messenger Voice Chat (TCP) 而不是 Yahoo Messenger Voice Chat (UDP) 作为目标端口。

如果仅添加源端口或仅添加目标端口，则可以添加使用不同传输协议的端口。例如，在单一访问控制规则中，可以将经由 TCP 的 DNS 和经由 UDP 的 DNS 二者添加为目标端口条件。

将非 TCP 流量与端口条件相匹配

您可以匹配非基于端口的协议。默认情况下，如果不指定端口条件，则匹配 IP 流量。虽然可以将端口条件配置为与非 TCP 流量相匹配，但有一些限制：

- 访问控制规则 - 对于典型设备，可以通过使用 GRE (47) 协议作为目标端口条件将 GRE 封装的流量与访问控制规则相匹配。对于 GRE 限制的规则，只能添加基于网络的条件：区域、IP 地址、端口和 VLAN 标签。此外，系统使用外部报头将访问控制策略中的所有流量与 GRE 限制的规则相匹配。对于威胁防御设备，请使用预过滤器策略中的隧道规则来控制 GRE 封装的流量。
- SSL 规则 - SSL 规则仅支持 TCP 端口条件。

- **ICMP 回应** - 类型设置为 0 的目标 ICMP 端口或类型设置为 129 的目标 ICMPv6 端口仅与主动回应回复相匹配。为应答 ICMP 回应请求而发送的 ICMP 回应回复被忽略。为使某个规则匹配任何 ICMP 回应，请使用 ICMP 类型 8 或 ICMPv6 类型 128。

URL 规则条件

使用 URL 条件控制网络上的用户可以访问的网站。

有关完整信息，请参阅[URL 过滤](#)。

动态属性规则条件

动态属性包括以下内容：

- **动态对象**（例如来自 Cisco Secure Dynamic Attributes Connector）

dynamic attributes connector 让您能够从云提供商收集数据（例如网络和 IP 地址）并将其发送到 Firepower 管理中心，以便将其用于访问控制规则中。。

有关 dynamic attributes connector 的详细信息，请参阅本指南后面的信息。

- **SGT 对象**
- **位置 IP 对象**
- **设备类型对象**
- **终端配置文件对象**

动态属性可用作访问控制规则中的源条件和目标条件。使用以下准则：

- 不同类型的对象通过 AND 连接在一起
- 将相似类型的对象一起进行 ORd 运算

例如，如果选择源目标条件 SGT 1、SGT 2 和设备类型 1；如果在 SGT 1 或 SGT 2 上检测到设备类型 1，则规则匹配。

动态对象

动态对象是可以使用 IP 或使用 Cisco Secure Dynamic Attributes Connector 来创建的对象，作为一种集成，它允许在管理中心访问控制规则中使用来自云网络产品的对象。

有关 dynamic attributes connector 的详细信息，请参阅本指南后面的信息。

动态对象和网络对象之间的差异如下：

- 使用 dynamic attributes connector 创建的动态对象会在创建后立即被推送到管理中心，并且还会定期更新。
- **API 创建的动态对象：**
 - 是 IP 地址，有或没有或无类域间路由(CIDR)，可以在访问控制规则中使用，与网络对象很相似。

- 不支持完全限定域名或地址范围。
- 必须使用 API 进行更新。

相关主题

[添加或编辑动态对象](#)

时间和日期规则条件

您可以指定连续时间范围或周期性时间段。

例如，规则只能在工作日工作时间或每个周末或节假关闭期间应用。

基于时间的规则基于处理流量的设备的本地时间应用。

基于时间的规则仅在 FTD 设备上受支持。如果将具有基于时间的规则的策略分配给不同类型的设备，则在该设备上会忽略与该规则关联的时间限制。在这种情况下，您将看到警告。

启用和禁用访问控制规则

创建访问控制规则时，默认情况下启用规则。如果您禁用某规则，系统将不用该规则来评估网络流量并停止为该规则生成警告和错误。在查看访问控制策略中的规则列表时，禁用的规则会呈灰色显示，不过，您仍然可以修改它们。

您还可以使用规则编辑器启用或禁用访问控制规则。

过程

步骤 1 在访问控制策略编辑器中，右键点击规则并选择规则状态。

如果规则旁显示视图 ()，则表明规则属于祖先策略，或者您没有修改规则的权限。

步骤 2 点击保存 (Save)。

下一步做什么

- 部署配置更改。

相关主题

[访问控制规则组成部分](#)，第 4 页

将访问控制规则从一个访问控制策略复制到另一个

您可以将访问控制规则从一个访问控制策略复制到另一个访问控制策略。您可以将规则复制到访问控制策略的默认 (Default) 部分或强制 (Mandatory) 部分。

已复制规则的所有设置（注释除外）都将保留在粘贴的版本中。但是，复制的规则中会添加一条新注释，其中提及了源访问控制策略。

过程

步骤 1 在访问控制策略编辑器中，选择要复制的规则。

（旧版 UI。） 要选择多条规则，请使用 Ctrl + 点击。

（新用户界面。） 要选择多个规则，请选中每个规则的复选框。

步骤 2 右键点击所选规则，然后选择复制到 (Copy to) > 其他策略 (Another policy)（旧版 UI (Legacy UI)）或复制到其他策略 (Copy to Different Policy)（新用户界面 (New UI)）。

步骤 3 从访问策略 (Access Policy) 下拉列表中选择目标访问控制策略。

步骤 4 从放置规则 (Place Rules) 下拉列表中，选择要放置所复制规则的位置。

- 要将其定位为默认 (Default) 部分中的最后一组规则，请选择底部（在“默认”部分中）(At the bottom [within the Default section])。
- 要将其定位为必填 (Mandatory) 部分中的第一组规则，请选择顶部（在“必填”部分中）(At the top [within the Mandatory section])。

步骤 5 点击复制 (Copy)。

下一步做什么

- 部署配置更改。

将访问控制规则移至预过滤器策略

您可以将访问控制规则从访问控制策略移至关联的非默认预过滤器策略。

您必须先将用户定义的预过滤器策略应用于访问控制策略。无法将访问控制规则移至默认的预过滤器策略，因为默认预过滤器策略不能包含规则。

开始之前

请在继续之前注意以下条件：

- 在将访问控制规则移至预过滤器策略时，无法移动访问控制规则中的第 7 层 (L7) 参数。L7 参数会在操作期间被丢弃。
- 在移动规则后，访问控制规则配置中的注释会丢失。但是，移动的规则中会添加一条新注释，其中提及了源访问控制策略。
- 您不能移动将监控 (Monitor) 设置为操作 (Action) 参数的访问控制规则。

- 移动时，访问控制规则中的操作 (Action) 参数将更改为预过滤器规则中的适当操作。要了解访问控制规则中的每个操作，请参阅下表：

| 访问控制规则中的操作 | 预过滤器规则中的操作 |
|------------|------------|
| 允许 | 分析 |
| 阻止 | 阻止 |
| 阻止并重置 | 阻止 |
| 交互式阻止 | 阻止 |
| 交互式阻止并重置 | 阻止 |
| 信任 | 快速路径 |

- 同样，根据访问控制规则中配置的操作，在移动规则后，日志记录配置会被设置为适当的设置，如下表中所述。

| 访问控制规则中的操作 | 在预过滤器规则中启用日志记录配置 |
|------------|---------------------------------------------------------------------------------------------------------------------|
| 允许 | 未选中任何复选框。 |
| 阻止 | <ul style="list-style-type: none"> • 在连接开始时记录 • 事件查看器 • 系统日志服务器 • SNMP 陷阱 |
| 阻止并重置 | <ul style="list-style-type: none"> • 在连接开始时记录 • 事件查看器 • 系统日志服务器 • SNMP 陷阱 |
| 交互式阻止 | <ul style="list-style-type: none"> • 在连接开始时记录 • 事件查看器 • 系统日志服务器 • SNMP 陷阱 |

| 访问控制规则中的操作 | 在预过滤器规则中启用日志记录配置 |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| 交互式阻止并重置 | <ul style="list-style-type: none"> • 在连接开始时记录 • 事件查看器 • 系统日志服务器 • SNMP 陷阱 |
| 信任 | <ul style="list-style-type: none"> • 在连接开始时记录 • 在连接结束时记录 • 事件查看器 • 系统日志服务器 • SNMP 陷阱 |

- 从源策略移动规则时，如果其他用户修改了这些规则，您将看到一条消息。您可以在刷新页面后继续该过程。

过程

步骤 1 在访问控制策略编辑器中，选择要移动的规则。

（旧版 UI。）要选择多条规则，请使用 Ctrl+单击。

（新用户界面。）要选择多个规则，请选中每个规则的复选框。

步骤 2 右键点击所选规则，然后选择**移动到其他策略 (Move to another policy)**（旧版 UI）或**移动到预过滤器策略 (Move to Prefilter Policy)**（新版 UI）。

步骤 3 从**放置规则 (Place Rules)** 下拉列表中，选择要放置移动规则的位置：

- 要定位为最后一组规则，请选择在**底部 (At the bottom)**。
- 要定位为第一组规则，请选择在**顶部 (At the top)**。

步骤 4 点击 **移动**。

下一步做什么

- 部署配置更改。

定位访问控制规则

您可以移动访问控制策略中的现有规则，或在所需位置插入新的规则。将某条规则添加或移动到某个类别时，系统会将其置于该类别的末尾。

以下程序介绍如何在编辑规则时移动规则。您还可以执行以下操作：

- （旧版 UI。）通过右键点击规则并选择**插入规则 (Insert Rule)**，在特定位置插入新规则。系统将打开“添加规则”(Add Rule)对话框，其中包含“插入”(Insert)菜单和指定的所选规则编号。您可以在规则下方或上方插入规则，并在必要时对规则编号进行更改。
- （旧版 UI。）通过右键点击现有规则，选择**剪切 (Cut)**或**复制到同一策略 (Copy to Same Policy)**，然后右键点击新位置并选择**粘贴到上方 (Paste Above)**或**粘贴到下方 (Paste Below)**。复制时，请确保删除旧位置的规则，以避免存在重复的规则。
- （新 UI。）将鼠标悬停在现有规则之间的行上，然后点击**添加规则 (Add Rule)**即可插入新规则。在“添加规则”(Add Rule)对话框的**插入 (Insert)**框中选择位置；您可以选择其他规则来调整位置。您还可以从右键点击菜单中选择**在上面添加规则 (Add Rule Above)**或在**下面添加规则 (Add Rule below)**。
- （新用户界面。）通过右键点击规则，选择**复制 (Copy)**，然后右键点击新位置并选择**粘贴到上方 (Paste Above)**或**粘贴到下方 (Paste Below)**。请确保删除旧位置的规则，以免出现重复的规则。

开始之前

查看[访问控制规则的最佳实践](#)中的规则顺序指南。

过程

步骤 1 在访问控制规则编辑器中，您有以下选择：

- 如果添加的是新规则，请使用**插入 (Insert)**下拉列表。
- （旧版 UI。）如果编辑的是现有规则，请点击**移动 (Move)**。
- （新用户界面。）如果要编辑现有规则，请点击规则名称旁边的**移动规则 (Move Rule)**图标。

步骤 2 选择要移动或插入规则的位置：

- 选择插入强制性类别 (**into Mandatory**) 或插入默认类别 (**into Default**)。
- 选择插入强制性类别 (**into Mandatory**)，然后选择类别。
- 选择规则上方或规则下方，然后键入相应的规则编号。在**新 UI (New UI)**，您只用选择规则，而不是键入规则编号。

步骤 3 保存规则。

步骤 4 点击**保存 (Save)**保存策略。

下一步做什么

- 部署配置更改。

将注释添加到访问控制规则

创建或编辑访问控制规则时，可以添加注释。例如，您可为其他用户汇总整体配置，或者当您变更规则和更改的原因时进行记录。您可以显示规则的所有注释列表，以及添加每条注释的用户以及添加注释的日期。

保存规则时，自上次保存所做的所有注释都将变为只读。

要搜索访问控制规则注释，请使用规则列表页面上的“搜索规则”(Search Rules) 栏。

过程

步骤 1 在访问控制规则编辑器中，点击**注释 (Comments)**。

步骤 2 (旧版 UI。) 点击**新建注释 (New Comment)**，输入注释，然后点击**确定 (OK)**。您可以在保存规则之前编辑或删除此注释。

步骤 3 (新 UI。) 输入注释，然后点击**添加备注 (Add Comment)**。您可以在保存规则之前编辑或删除此注释。

步骤 4 保存规则。

访问控制规则的示例

以下主题提供了访问控制规则的示例。

如何使用安全区域来控制访问

假设在某个部署中，您希望主机对互联网具有不受限制的访问权限，但是仍然通过检测传入流量是否存在入侵和恶意软件来保护这些主机。

首先，创建两个安全区域：内部和外部。然后，将一个或多个设备上的接口分配到这些区域，每个对中的一个接口位于内部区域，另一个接口位于外部区域。在内侧连接至网络的主机代表您的受保护资产。



注释 您不需要将所有内部（或外部）接口分组至单个区域。选择对您的部署和安全策略有意义的分组。

然后，配置访问控制规则，其中目标区域条件设置为“内部”(Internal)。此简单规则与从内部区域中的任何接口传出设备的流量相匹配。要检查匹配流量中是否存在入侵和恶意软件，请选择规则操作**允许 (Allow)**，然后将该规则与入侵和文件策略相关联。

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。