



访问控制策略

以下主题介绍如何使用访问控制策略：

- [关于访问控制策略，第 1 页](#)
- [访问控制策略的要求和前提条件，第 6 页](#)
- [管理访问控制策略，第 7 页](#)
- [访问控制策略的历史记录，第 26 页](#)

关于访问控制策略

访问控制是一种分层策略，可用于指定、检查和记录网络流量。您可以使用每个连接的特征来允许、信任、阻止或监控连接。

每个托管设备都可分配给一个访问控制策略。策略的已分配（也称为目标）设备收集有关网络流量的数据可用于根据以下内容过滤和控制该流量：

- 简单、易于确定的传输层和网络层特征：源和目标、端口和协议等
- 流量的最新的上下文信息，包括诸如信誉、风险、业务相关性、使用的应用或访问的 URL 等特征
- 领域、用户、用户组或 ISE 属性
- 自定义安全组标记 (SGT)
- 加密流量的特性；也可以解密此流量以进一步分析
- 未加密或已解密的流量包含禁止的文件、检测到的恶意软件还是入侵尝试
- 时间和日期（在受支持的设备上）

每种类型的流量检查和控制都以提供最大灵活性和性能的方式进行。例如，基于信誉的阻止名单使用简单的源和目标数据，因此，可以在过程的早期阻止禁止的流量。相反，检测和阻止入侵和漏洞则是最后一道防线。

访问控制策略组件

以下是访问控制策略的主要元素。

名称和描述

每个访问控制策略必须拥有唯一的名称。说明是可选的。

沿用设置

通过策略继承，您可以创建访问控制策略的层次结构。父（或基本）策略定义和执行其后代的默认设置。

策略的继承设置允许您选择其基本策略。您还可以锁定当前策略中的设置以强制所有后代继承这些设置。后代策略可以覆盖未锁定的设置。

策略分配

每个访问控制策略可识别使用策略的设备。每台设备只能作为一个访问控制策略的目标。您还可以将策略分配给设备模板。

规则

访问控制规则提供了一种精细的网络流量处理方法。访问控制策略中的规则从1开始进行编号，包括从祖先策略继承的规则。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。

通常，系统根据第一个访问控制规则（其中所有规则的条件都与流量匹配）处理网络流量。条件可以简单也可以复杂，条件的使用通常取决于某些许可证。

默认操作

默认操作确定系统如何处理和记录不是由任何其他访问控制配置处理的流量。默认操作可以阻止或信任所有流量，而不进行进一步检查，或者检查流量以获取入侵和发现数据。

尽管访问控制策略可从祖先策略继承其默认操作，但您无法强制执行这一继承。

安全智能

安全智能是抵御恶意互联网内容的第一道防线。此功能允许您根据最新的IP地址、URL和域名信誉情报将阻止连接。要确保对重要资源的持续访问，您可以使用自定义不阻止列表条目来覆盖阻止列表条目。

HTTP 响应

在系统阻止用户的网站请求时，您可以显示系统提供的通用响应页面或自定义页面。也可以显示一个警告用户，同时允许他们继续访问初始请求站点的页面。

日志记录

通过访问控制策略日志记录的设置，您可以为当前的访问控制策略配置默认系统日志目标。除非使用所包含规则和策略中的自定义设置显式覆盖系统日志目标设置，否则这些设置适用于访问控制策略以及所有包含在内的解密、预过滤和入侵策略。

高级访问控制选项

高级访问控制策略设置通常只需要进行很小的修改或不需要修改。通常，默认设置就非常适合。可修改的高级设置包括流预处理、解密、身份和各种性能选项。

访问控制策略默认操作

新创建的访问控制策略指示其分配的设备使用其默认操作处理所有流量。

在简单的访问控制策略中，默认操作指定设备如何处理所有流量。在更复杂的策略中，默认操作处理如下流量：

- 未被预过滤策略快速转发
- 不在安全智能阻止列表中
- 未被解密策略阻止（仅限加密流量）
- 与策略中的所有规则均不匹配（“监控”规则除外，这些规则会匹配和记录流量，但不处理或检查流量）。

访问控制策略默认操作可以阻止或信任流量，而不进行进一步检查，或者检查流量以获取入侵和发现数据。



注释 您不能对默认操作处理的流量执行文件或恶意软件检查。默认操作处理的连接的日志记录最初处于禁用状态，但是您可以启用该日志记录功能。

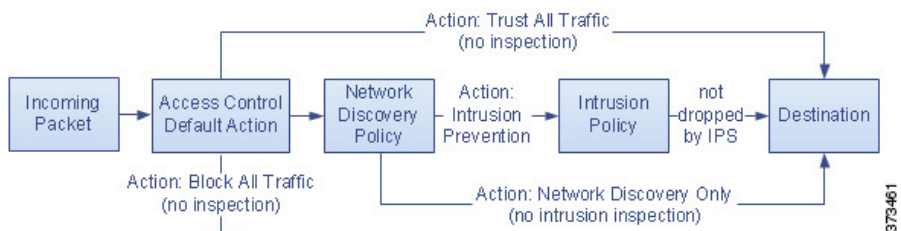
如果使用的是策略继承，则最低级别后代的默认操作会确定最终流量处理。尽管访问控制策略可从其基本策略继承其默认操作，但您无法强制执行这一继承。

下表介绍了您可以对每个默认操作处理的流量执行的检查类型。

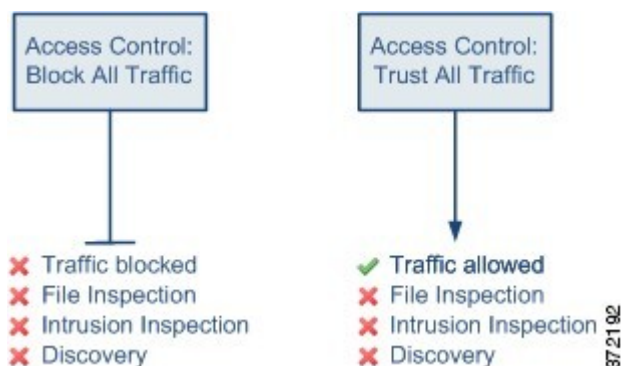
表 1: 访问控制策略默认操作

默认操作	对流量的影响	检查类型和策略
访问控制：阻止所有流量	直接阻止，不进行进一步检查。	无。
访问控制：信任所有流量	信任（允许流向其最终目标，而无需进一步检查）。	无。
入侵防御	允许，前提是其通过您指定的入侵策略检测。	入侵，使用指定的入侵策略和关联变量集。 发现，使用网络发现策略。
仅网络发现	允许。	仅发现，使用网络发现策略。
继承自基本策略	在基本策略中定义	在基本策略中定义

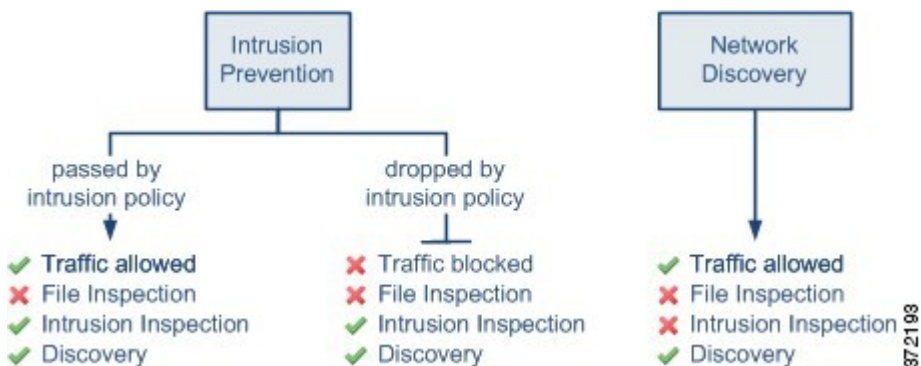
下图对该表进行了展示。



下图展示了阻止所有流量 (Block All Traffic) 和信任所有流量 (Trust All Traffic) 默认操作。



下图展示了入侵防御 (Intrusion Prevention) 和仅网络发现 (Network Discovery Only) 默认操作。



提示 **Network Discovery Only** 的目的是在仅发现部署中提高性能。如果您仅对入侵检测和防御感兴趣，则不同的配置可以禁用发现。

访问控制策略继承

您可以嵌套访问控制策略。在这种情况下，每个策略都会继承祖先（或基本）策略的规则和设置。您可以执行此继承，或允许较低级别的策略覆盖其祖先。

访问控制使用基于分层策略的实施。正如创建域层次结构一样，您也可以创建访问控制策略的相应层次结构。后代或子访问控制策略继承其直接父策略或基本策略的规则和设置。该基础策略可能有其子级的父级策略，它从父级策略沿用规则和设置等。

访问控制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。这种实施执行来自祖先策略的强制规则，但也允许当前策略写入规则以抢先于来自祖先策略的默认规则。

您可以锁定以下设置，以便在所有后代策略中执行它们。后代策略可以覆盖未锁定的设置。

- 安全智能 — 根据 IP 地址、URL 和域名的最新信誉情报而被允许或阻止的连接。
- HTTP 响应页面 — 在阻止用户的网站请求时显示自定义或系统提供的响应页面。
- 高级设置 — 指定关联的子策略、网络分析设置、性能设置和其他常规选项。

如果使用的是策略继承，则最低级别后代的默认操作会确定最终流量处理。尽管访问控制策略可从祖先策略继承其默认操作，但您无法强制执行这一继承。

策略继承和多租户

访问控制的基于分层策略的实施完善了多租户策略。

在典型的多域部署中，访问控制策略的层次结构与域结构相对应，您将最低级别的访问控制策略应用于托管设备。这种实施支持在较高的域级别选择性地执行访问控制，而低层域管理员可以定制特定部署的具体设置。（要限制后代域中的管理员，您必须使用角色而不能只靠策略继承和实施。）

例如，作为组织的全局域管理员，您可以在全局级别创建访问控制策略。然后，您可以要求所有设备（按功能分为子域）使用该全局级策略作为基本策略。

当子域管理员登录 Secure Firewall Management Center 配置访问控制时，他们可以按原样部署此全局级策略。或者，他们也可以在该全局级策略的界限之内创建和部署后代访问控制策略。



注释

虽然这种最有用的访问控制继承和执行的实施方法可以完善多租户策略，但您也可以在单个域中创建访问控制策略的层次结构。您还可以在任意级别分配和部署访问控制策略。

规则和其他策略警告

策略和规则编辑器使用图标来标记可能会对流量分析和流动有不利影响的配置。根据问题，系统可能会在您部署时向您发出警告或完全阻止您进行部署。



提示

将您的鼠标指针悬停在图标之上，即可读取警告、错误或信息文本。

表 2: 策略错误图标

图标	说明	示例
错误 (✖)	如果规则或配置具有错误，则更正错误之前无法部署，即使禁用任何受影响规则也如此。	在分配没有 URL 过滤许可证的设备之前，执行基于类别和信誉的 URL 过滤的规则有效。此时，规则旁边会出现错误图标，您必须编辑或删除规则、取消分配设备或启用许可证才能部署。
警告 (⚠)	可以部署显示规则或其他警告的策略。然而，标记有警告的不当配置将不起作用。 如果您禁用包含警告的规则，则警告图标将消失。如果在没有纠正潜在问题的情况下启用规则，警告图标将会再次显示。	已占用的规则或由于配置不当而无法与流量相匹配的规则不起作用。这包括使用空对象组的条件、与应用不匹配的应用过滤器、已排除的LDAP用户、无效端口等等。 但是，如果警告图标标记许可错误或型号不匹配，则在更正问题之前无法进行部署。
信息 (i)	信息图标传达有关可能影响流量流动的配置的有用信息。这些问题不会阻止您进行部署。	系统可能会跳过根据某些规则来匹配连接的前几个数据包，直至系统识别该连接中的应用或网络流量为止。这样，就可建立连接，以便识别应用和 HTTP 请求。
规则冲突 (⚡)	在启用规则冲突分析时，此图标会显示在具有冲突的规则规则表中。	冲突包括冗余规则、冗余对象和影子规则。冗余和影子规则不匹配流量，因为以前的规则已与条件相匹配。冗余对象会使规则变得不必要地复杂。

访问控制策略的要求和前提条件

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
- 您可以定义自定义用户角色，以区分访问控制策略和规则中的入侵配置以及访问控制策略和规则的其余部分。使用这些权限，您可以分离网络管理团队和入侵管理团队的职责。包含“修改

访问控制策略”权限的现有预定义用户角色支持所有子权限；如果要应用精细权限，则需要创建自己的自定义角色。精细化权限包括：

- **策略 > 安全策略 > 访问控制** 并选择 **访问控制策略 > 修改访问控制策略 > 修改威胁配置** 允许在规则中选择入侵策略、变量集和文件策略，配置网络分析和入侵策略的高级选项，配置安全智能策略访问控制策略，以及策略默认操作中的入侵操作。如果用户只有此选项，则不能修改策略或规则的其他部分。
- **修改剩余访问控制策略配置** 控制编辑策略所有其他方面的能力。

管理访问控制策略

您可以编辑系统提供的访问控制策略，并创建自定义访问控制策略。

过程

步骤 1 选择策略 > 安全策略 > 访问控制。

在页面顶部，有一些相关功能的便捷链接：对象管理、入侵策略、网络分析策略、DNS 策略和策略导入/导出。

步骤 2 管理访问控制策略：

- **分析策略** — 选择一个或多个策略然后点击 **分析策略** 评估冗余或影子规则等异常的访问控制策略，并采取措施修复已发现的异常。分析作业会发送到云，需要一些时间才能完成。请参阅 [使用策略分析器和优化器识别和修复异常](#)，第 20 页。

“异常”列显示分析结果。点击 **% 可优化** 以查看异常，或点击 **重新分析** 以再次运行分析。

“上次分析”列显示策略分析器和优化器上次运行的时间。

完成分析和优化后，您可以通过从 **更多** (⋮) 菜单中选择以下选项来下载报告：**下载上次策略分析、补救历史记录**。

注释

要使用策略分析功能，您必须使用云交付的防火墙管理中心或连接到 Security Cloud Control (Security Cloud Control)。如果您的设置不符合要求，当您点击包含 **集成** 按钮的按钮时，系统会打开一个说明性对话框，可帮助您入门。策略分析器和优化器仅在云中运行。

- **创建** — 点击 **创建策略**；请参阅 [创建基本访问控制策略](#)，第 8 页。
- **列** - 点击规则列表上方的 **显示/隐藏列 (Show/Hide Columns)** 图标，选择要在表中显示的信息。点击 **全部显示/全部隐藏 (Show All/Hide All)** 以快速添加或删除所有列出的列（名称和操作除外）。点击 **默认 (Default)** 以撤消所有自定义设置。
- **继承** — 垂直线表示策略之间的继承关系。
- **编辑** - 点击 **编辑** (✎)；请参阅 [编辑访问控制策略](#)，第 9 页

- 删除 - 点击 **删除** (🗑️)。您必须先删除任何设备分配，然后才能删除策略。
要一次删除多个策略，请选中策略的复选框，然后选择表上方的 **删除策略**。
- 复制-从 **更多** (⋮) 菜单中选择 **克隆**。系统在副本保留设备分配。
- 报告 -从 **更多** (⋮) 菜单中选择**生成报告**。。报告将作为后台进程生成。转到消息/通知中心并查看任务列表。报告完成后，您可以从通知中下载。
- 查看审核日志 — 从 **更多** (⋮) 点击**查看审核日志**。
- 锁定或解锁策略 - 请参阅[锁定访问控制策略](#)，第 11 页。

创建基本访问控制策略

创建新的访问控制策略时，它包含默认操作和设置。创建策略后，您会立即进入编辑会话，以便您可以调整策略以满足您的要求。

过程

步骤 1 选择策略 > 安全策略 > 访问控制。

步骤 2 点击创建策略。

步骤 3 在名称 (Name) 和说明 (Description) (可选) 中输入唯一名称和说明。

步骤 4 或者，选择基本策略。

如果已在您的域上执行访问控制策略，则此步骤不为可选步骤。必须选择已执行的策略或其后代之一作为基本策略。

如果您选择基本策略，则基本策略定义默认操作，您无法在此对话框中选择新的操作。日志记录连接由基础策略的默认操作处理。

步骤 5 不选择基本策略时，请指定初始默认操作：

- **Block all traffic** 通过 **Access Control: Block All Traffic** 默认操作创建策略。
- **入侵防御 (Intrusion Prevention)** 可以通过**入侵防御：平衡安全性和连接 (Intrusion Prevention: Balanced Security and Connectivity)** 默认操作创建策略，与默认入侵变量集相关联。
- **Network Discovery** 使用默认操作 **Network Discovery Only** 创建策略。

当您选择默认操作时，默认操作处理的连接的日志记录最初处于禁用状态。您可以稍后在编辑策略时启用它。

提示

如果要在默认情况下信任所有流量，或如果已选择基本策略但不想继承默认操作，则可以稍后更改默认操作。

步骤 6 或者，选择要分配给策略的设备。要减少显示的设备，请输入搜索字符串。该列表包括设备和设备模板。

如果要立即部署此策略，则必须执行此步骤。

步骤 7 点击保存。

新策略将打开以供编辑。您可以向其添加规则，并根据需要进行其他更改。请参阅[编辑访问控制策略，第 9 页](#)。

编辑访问控制策略

编辑访问控制策略时，应将其锁定，以确保您的更改不会被同时编辑的其他人覆盖。

您只能编辑在当前域中创建的访问控制策略。此外，不能编辑由祖先访问控制策略锁定的设置。

为保护会话隐私，当策略编辑器 30 分钟无任何活动后，系统将显示警告。60 分钟后，系统将放弃更改。



注释 当编辑某个策略但未将其锁定时，横幅消息可能会指示其他用户当前正在编辑该策略。当其中一个用户保存更改时，系统会提示您合并或放弃更改。您应该立即决定该怎么做。有关详细信息，请参阅[并发编辑和合并更改，第 12 页](#)。

过程

步骤 1 选择策略 > 安全策略 > 访问控制。

步骤 2 点击要编辑的访问控制策略旁边的 **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 3 编辑访问控制策略。

提示

您可以通过选中左列中的复选框，然后从搜索框旁边的**选择批量规则操作**下拉列表中选择要执行的操作，一次对多个规则进行操作。批量编辑可用于启用和禁用、复制、移动、删除和编辑规则，或查看命中计数或相关事件。您还可以删除所选规则中的对象重叠。

您可以更改以下设置或执行以下操作：

- 名称和说明 - 点击名称旁边的**编辑** (✎)，进行更改，然后点击**保存**。
- 默认操作和设置 - 从**默认操作**下拉列表中选择一个值，然后点击**齿轮** (⚙)，对设置进行更改并点击**确定**。有关详细信息，请参阅[设置访问控制默认操作，第 14 页](#)。

- 关联的策略 - 要编辑或更改数据包流中的策略，请点击策略名称下方数据包流表示中的策略类型。您可以选择 **预处理规则**、**解密**、**安全智能**和 **身份** 策略。必要时，点击**访问控制 (Access Control)** 以返回访问控制规则。
- 策略分配 - 要标识此策略的目标受管设备，或在子域中实施此策略，请点击**已分配: x 设备**链接。您可以将策略分配给设备或设备模板。
- 规则 - 要使用入侵和文件策略来管理访问控制规则，以及检查和阻止恶意流量，请点击**添加规则 (Add Rule)**，或右击现有规则并选择**编辑 (Edit)** 或其他响应操作。操作也可从每个规则的 **更多 (i)** 按钮获取。请参阅[创建和编辑访问控制规则](#)。
- 布局 - 使用规则列表上方的**网格/表视图 (Grid/Table View)** 图标更改布局。网格视图以易于查看的布局提供彩色编码的对象。表视图提供摘要列表，以便您可以同时查看更多规则。您可以在不影响规则的情况下自由切换视图。
- 列（仅限表视图） - 点击规则列表上方的**显示/隐藏列**图标，选择要在表中显示的信息。点击**显示/隐藏空列**以快速删除所有没有信息的列，即您不在任何规则中使用这些条件。点击**恢复为默认值 (Revert to Default)** 以撤消所有自定义设置。
- 分析规则逻辑 - 您可以从**分析**菜单中选择以下选项来检查规则的逻辑：
 - **管理规则命中计数** - 要查看每个规则的匹配连接数统计信息。请参阅[查看规则命中计数，第 21 页](#)。
 - **启用/禁用规则冲突**-选择是否要查看有关规则是否相互干扰的信息。然后，您可以使用以下命令查看结果。请参阅[分析规则冲突和警告，第 23 页](#)
 - **显示警告和错误** - 查看是否存在需要解决配置问题的规则。
 - **显示策略警告** - 查看策略是否存在配置问题。
 - **显示规则冲突**-查看是否有冗余或影子规则。这些冲突可能会阻止某些规则被连接匹配，这意味着您需要修复匹配条件、移动规则或直接删除规则。
- 其他设置 - 要更改策略的其他设置，请从数据包流末尾的**更多**下拉箭头中选择以下选项之一。
 - **加密可视性引擎** - 是否启用和配置加密可视性引擎。请参阅[配置 EVE](#)。
 - **高级设置** - 要设置预处理、解密、身份、性能及其他高级选项。请参阅[为访问控制策略配置高级设置](#)。
 - **HTTP 响应 (HTTP Responses)** - 要指定当系统阻止网站请求时用户在浏览器中看到的内容。请参阅[选择 HTTP 响应页面](#)。
 - **继承设置 (Inheritance Settings)** - 更改此策略的基本访问控制策略，并在其后代策略中实施此策略的设置。请参阅[选择基本访问控制策略，第 15 页](#)和[锁定后代访问控制策略中的设置，第 16 页](#)。
 - **日志记录 (Logging)** - 设置策略的默认日志记录选项。

步骤 4 点击保存。

锁定访问控制策略

您可以锁定访问控制策略，以防止其他管理员对其进行编辑。锁定策略可确保在您保存更改之前，如果其他管理员编辑策略并保存更改，您的更改不会失效。如果您不锁定策略，但另一个用户同时编辑该策略并必须先保存更改，则您可能必须合并更改。有关详细信息，请参阅[并发编辑和合并更改](#)，第 12 页。

该锁用于访问控制策略本身。锁定不适用于策略中所使用的对象。例如，另一个用户可以编辑锁定访问控制策略中所使用的网络对象。在明确解锁策略之前，您的锁定将保持不变，因此您可以稍后注销并返回到您的编辑。

策略被锁定时，其他管理员对该策略具有只读访问权限。但是，其他管理员可以将已锁定的策略分配给托管设备。

开始之前

有权修改访问控制策略的任何用户角色都有权锁定该策略，并且还可以解锁被其他用户锁定的策略。

但是，解锁被其他管理员锁定的策略的能力受以下权限控制：**策略 > 安全策略 > 访问控制** 选择访问控制 (**Access Control**) 访问控制策略 (**Access Control Policy**) > 修改访问控制策略 (**Modify Access Control Policy**) > 覆盖访问控制策略锁定 (**Override Access Control Policy Lock**)。

如果您使用的是自定义角色，则您的组织可能会通过不分配此权限来限制您的解锁能力。如果没有此权限，则只有锁定策略的管理员才能解锁策略。

过程

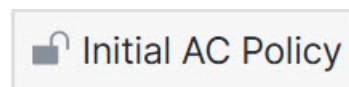
步骤 1 选择策略 > 安全策略 > 访问控制。

步骤 2 点击要锁定或解锁的访问控制策略旁边的 **编辑** (🔧)。

在访问控制策略列表中：

- 策略名称旁的锁图标表示该策略已锁定。将鼠标悬停在该图标上即可查看哪个用户锁定了策略。
- 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。否则，它已被其他用户锁定。

步骤 3 点击策略名称旁边的锁定图标可锁定或解锁策略。



如果策略从父策略继承了设置，则在点击锁定图标时必须选择以下选项之一。

- 锁定/解锁此策略 - 锁定或解锁仅适用于此策略。

- **锁定/解锁层次结构中的所有策略** - 锁定或解锁此策略和所有父策略。如果父策略已被其他管理员锁定，您将看到一条消息，并且无法锁定该父策略。解锁策略时，如果您具有“覆盖访问控制策略锁定”权限，则会解锁所有父策略，即使它们已被其他用户锁定。

并发编辑和合并更改

当允许多个用户编辑访问控制策略时，您有两种选择：

- 让用户在编辑策略时锁定策略。这可确保一次只能有一个用户进行更改。使用锁定，您永远不必担心更改丢失或冲突。但是，它会限制您快速响应意外事件的能力，尤其是在用户不在办公室时锁定策略的情况下。有关锁定策略的详细信息，请参阅 [锁定访问控制策略，第 11 页](#)。
- 允许用户同时编辑策略。如果多个用户在给定时间进行了未保存的编辑，则第一个保存策略的用户会得到其已保存的所有更改。其他用户会立即收到保存通知，然后必须合并其更改。本主题的其余部分介绍此方法。



注释 如果您使用变更管理（在故障单范围内进行编辑），故障单会锁定策略，无法进行并发编辑。

开始之前

要限制必须执行的合并量，请及早并经常保存策略。

过程

步骤 1 确定其他用户是否也在编辑策略。

编辑访问控制策略时，请查找页面顶部是否显示以下消息横幅：

User name is currently editing this policy.

此消息表明指定用户（可能有多个）当前已打开策略进行编辑。

步骤 2 留意其他用户已保存更改的通知并采取措施。

以下横幅消息表示另一用户已保存更改，您需要立即采取措施：

User name modified this policy and saved changes. **Merge Discard.**

点击以下任一链接：

- **合并**- 打开一个合并窗口，您可以在其中决定保留或放弃哪些更改，并识别无法合并的更改。采用此选项时，请参阅下一步。

- **放弃**-立即放弃所有更改并重新开始。如果选择此选项，页面会刷新，以显示其他用户的最新更改。

步骤 3 合并更改。

当您点击 **合并** 选项时，系统将打开一个合并窗口，其中汇总了观察到的您的编辑与上次用户保存的编辑之间的差异总数。不包括其他用户的未保存编辑。观察结果包括直接冲突和信息性通知。

注释

您必须在关闭窗口之前完成所有合并决定。点击 **合并** 选项后，不能等到以后再进行合并。

a) 评估每个冲突并为每个冲突制定决策。

在评估更改列表时，请考虑以下事项：

- 最初，系统会显示所有观察结果，但您可以选择/取消选择“冲突”和“信息”的过滤选项，以限制显示的信息。当用户编辑相同的规则或设置时，会产生冲突。信息项目用于对不同规则或设置进行编辑。
- 如果不存在冲突，您的缓存将立即使用上次保存的更改进行更新，然后您可以继续。例如，如果您正在编辑规则 1，而另一个用户已保存对规则 2 的更改，则不可能存在任何冲突。
- 对于每个冲突（规则名称除外），窗口会显示其他用户保存的元素版本（**防火墙管理中心上的版本**）和您的更改（**修改后的版本**）。系统对新增的（例如，以前未定义的选项）、编辑的或删除的策略元素用更改进行颜色编码。您必须选择“**放弃更改**”或“**接受我的更改**”并覆盖其他用户的更改。放弃更改时，系统会使用其他用户的保存更改来刷新规则，并删除您的更改。
- 规则冲突是在规则级别考虑的，而不是规则中的每个元素考虑的。例如，如果您编辑目标网络，且保存的更改适用于源网络，则您的更改或其他用户的更改将保留，而不会同时保留。
- 如果冲突涉及规则名称，系统会尝试在名称中添加下划线和数字来创建唯一名称，例如 Rule_1。您也可以在提供的编辑框中输入新名称，然后点击 **保存**。如果点击 **丢弃 (Discard)**，将使用生成的规则名称。
- 您无法跳过任何冲突。对于每个冲突，您必须决定是放弃还是保留更改。
- 如果保存更改的用户删除了您编辑的规则，则规则将被删除，并且您无法选择保留该规则。
- 如果保存更改的用户更新了规则，而您的更改是为了删除该规则，则保留该规则：您无法合并删除。
- 对于以下选项，如果您的更改与已保存的更改冲突，您的更改会被丢弃，并且不会合并更改：
 - 其他策略分配：预过滤策略、安全智能策略、身份策略、解密策略
 - 更改高级设置、策略日志记录、EVE、HTTP 响应页面。
 - 策略默认操作。
 - 沿用设置。

b) 点击关闭 (Close)。

步骤 4 合并完成后，您可以立即保存策略或继续编辑策略。保存策略可能会降低未来合并的影响。

设置访问控制默认操作

访问控制策略的默认操作会应用于以下任意连接：

- 未被预过滤策略快速转发
- 不在安全智能阻止列表中
- 未被解密策略阻止（仅限加密流量）
- 与策略中的所有规则均不匹配（“监控”规则除外，这些规则会匹配和记录流量，但不处理或检查流量）。

过程

步骤 1 编辑要更改其继承设置的访问控制策略；请参阅[编辑访问控制策略，第 9 页](#)。

步骤 2 选择规则列表底部的默认操作。

有关这些选项的详细信息，请参阅[访问控制策略默认操作，第 3 页](#)。

步骤 3 点击齿轮 (⚙️) 以配置默认操作设置。

你可以配置以下选项。完成后点击**确定**。

- **日志记录选项** - 是否记录连接。您可以在**连接开始时记录**、**在连接结束时记录**，或**两者都选**。如果您选择阻止作为默认操作，则只能在连接开始时进行记录。
- **将连接事件发送至** - 如果选择一个日志记录选项，请选择是否将事件发送至以下任意组合：
 - **防火墙管理中心** - 将事件发送到管理器。
 - **系统日志服务器** - 将事件发送到为策略配置的默认系统日志服务器。您可以配置覆盖以指定不同的严重性级别或系统日志服务器目标。

（Splunk 或 SIEM 系统日志服务器集成）如果您已将 防火墙管理中心 配置为 Splunk 配置中的连接事件源，请选择 **将连接事件发送至** 选项下的 **防火墙管理中心**。如果您已将 Firewall Threat Defense 配置为连接事件源，请选择至少一个系统日志目标。有关 Splunk 或任何 SIEM 系统日志配置程序，请参阅 [Cisco Secure Firewall Management Center 管理指南](#)。

- **SNMP 陷阱** - 如果启用日志记录，则可以将 SNMP 陷阱发送到 SNMP 服务器。选择 SNMP 配置，或点击 + 配置新的配置。
- **默认操作变量集** - 如果选择了其中一种入侵防御默认操作，请选择应与所选入侵策略一起使用的变量集。

步骤 4 点击保存。

管理访问控制策略继承

继承与使用其他策略作为访问控制策略的基本策略相关。这允许您使用一个策略来定义可应用于多个策略的一些基准特征。要了解继承的工作原理，请参阅[访问控制策略继承，第 4 页](#)。

过程

步骤 1 编辑要更改其继承设置的访问控制策略；请参阅[编辑访问控制策略，第 9 页](#)。

步骤 2 管理策略继承：

- 更改基本策略 - 要更改基本访问控制策略，请从数据包流行末尾的**更多** 下拉箭头中选择**继承设置**，然后如[选择基本访问控制策略，第 15 页](#)中所述继续操作。
- 锁定后代策略中的设置 - 要在此策略的所有后代策略中执行其设置，请从数据包流行末尾的**更多** 下拉箭头中选择**继承设置**，然后如[锁定后代访问控制策略中的设置，第 16 页](#)中所述继续操作。
- 从基本策略继承设置 - 要从基本访问控制策略继承设置，请按照[继承基本策略的访问控制策略设置，第 16 页](#)中的指示进行操作。
- 要求在域中提供 - 要在子域中执行此策略，请点击**已分配：x 台设备**链接，然后如[在域中要求访问控制策略，第 17 页](#)中所述继续操作。

选择基本访问控制策略

可以使用一个访问控制策略作为另一个访问控制策略的基础（父级）。默认情况下，子策略从其基本策略继承其设置，但是可以更改未锁定的设置。

当更改当前访问控制策略的基本策略时，系统会使用新基本策略中的任何已锁定的设置来更新当前策略。

过程

步骤 1 在访问控制策略编辑器中，从数据包流行末尾的 **更多** 下拉箭头中选择 **继承设置**。

步骤 2 从**选择基本策略 (Select Base Policy)** 下拉列表中选择策略。

选择无以删除继承。

步骤 3 点击确定。

步骤 4 点击**保存** 保存访问控制策略。

下一步做什么

- 部署配置更改；请参阅 [部署配置更改](#)。

锁定后代访问控制策略中的设置

锁定访问控制策略中的设置，以便在所有后代策略中执行该设置。后代策略可以覆盖未锁定的设置。

当您锁定设置时，系统会保存后代策略中已经做出的覆盖，以便在您再次解锁设置时可以恢复这些覆盖设置。

过程

步骤 1 在访问控制策略编辑器中，从数据包流行末尾的 **更多** 下拉箭头中选择 **继承设置**。

步骤 2 在“子策略继承设置”(Child Policy Inheritance Settings) 区域中，选中要锁定的设置。

如果控件呈灰色显示，则表明设置从祖先策略继承，或者您没有修改配置的权限。

步骤 3 点击**确定** 保存设置。

步骤 4 点击**保存** 保存访问控制策略。

下一步做什么

- 部署配置更改；请参阅 [部署配置更改](#)。

继承基本策略的访问控制策略设置

新的子策略继承其基本策略的许多设置。如果这些设置在基本策略中未锁定，您可以覆盖这些设置。

如果稍后重新继承基本策略的设置，系统会显示基本策略的设置且控件呈灰色。不过，系统会保存所做的覆盖，如果您再次禁用继承，则会恢复覆盖设置。

过程

步骤 1 在访问控制策略编辑器中，点击**安全智能**，或者从数据包流行末尾的**更多**下拉箭头中选择 **HTTP 响应、日志记录、加密可视性引擎或高级设置**。

步骤 2 选中要继承的每个设置所对应的**继承自（基本策略）**复选框。

如果控件呈灰色显示，则表明设置从祖先策略继承，或者您没有修改配置的权限。

步骤 3 点击**保存**。

下一步做什么

- 部署配置更改：请参阅 [部署配置更改](#)。

在域中要求访问控制策略

您可以要求域中的每个设备都使用相同的基本访问控制策略或其后代策略之一。此程序仅适用于多域部署。

过程

步骤 1 在访问控制策略编辑器中，点击**已分配：x 台设备**链接。

步骤 2 点击 **在域中需要**。

步骤 3 构建域列表：

- 添加 - 选择要实施当前访问控制策略的域，然后点击**添加 (Add)** 或拖放到所选域列表中。
- 删除 - 点击枝叶域旁边的 **删除** ()，或者右键点击祖先域并选择 **删除所选项**。
- 搜索 - 在搜索字段中键入搜索字符串。点击 **清除** () 以清除搜索。

步骤 4 点击**确定** 以保存域实施设置。

步骤 5 点击**保存** 保存访问控制策略。

下一步做什么

- 部署配置更改：请参阅 [部署配置更改](#)。

将设备分配给访问控制策略

访问控制策略指定使用策略的设备。每个设备只能分配给一个访问控制策略。您还可以将策略分配给设备模板。模板包含在可用设备和选定设备列表中。

过程

步骤 1 在访问控制策略编辑器中，点击**已分配：x 台设备**链接。

步骤 2 制定目标联系人列表：

- 添加 - 选择一个或多个**可用设备 (Available Devices)**，然后点击**添加到策略 (Add to Policy)** 或拖放到**所选设备 (Selected Devices)** 列表。
- 删除 - 点击单个设备旁边的**删除** ()，或选择多个设备，点击右键，然后选择**删除选择**。
- 搜索 - 在搜索字段中键入搜索字符串。点击 **清除** () 以清除搜索。

在**受影响的设备**下，系统会列出其分配的访问控制策略是当前策略子项的设备。对当前策略进行的任何更改都将影响这些设备。

步骤 3 点击**确定** 以保存目标设备设置。

步骤 4 点击**保存** 保存访问控制策略。

下一步做什么

- 部署配置更改；请参阅 [部署配置更改](#)。

访问控制策略的日志记录设置

要配置访问控制策略的日志记录设置，请从数据包流行末尾的 **更多** 下拉箭头中选择 **日志记录**。

您可以为访问控制策略配置默认系统日志目标和系统日志警报。除非使用所包含规则和策略中的自定义设置显式覆盖系统日志目标设置，否则这些设置适用于访问控制策略以及所有包含在内的解密、预过滤和入侵策略。

默认操作处理的连接的日志记录最初处于禁用状态。

只有在页面顶部选择通常用于发送系统日志消息的选项后，IPS 和文件和恶意软件设置才会生效。

默认系统日志设置

选择 **Syslog Server** 选项以便为策略配置默认系统日志服务器。然后，选择目标，如有需要，还需选择警报级别。您可以选择：

- **目标 > 特定系统日志警报对象** - 如果选择此选项，事件将根据 [Cisco Secure Firewall Management Center 管理指南](#) 中创建系统日志警报响应的说明配置的所选系统日志警报进行发送。您可以从列表中选择系统日志警报，或通过指定名称、记录主机、端口、设施和严重性来添加警报。有关详细信息，请参阅 [Cisco Secure Firewall Management Center 管理指南](#) 中的入侵系统日志警报的设施和严重性。

使用此选项时，系统会使用管理接口将系统日志消息发送到服务器。确保有从管理接口到系统日志服务器的路由，否则信息将无法到达服务器。

- **目标 > 使用 FTD 平台设置** - 如果选择此选项并指定**严重性**，系统会将具有该严重性的连接或入侵事件发送到“平台设置”中配置的系统日志收集器。使用此选项，您可以通过在“平台设置”中配置系统日志配置并重新使用访问控制策略中的设置来统一系统日志配置。本部分中选择的严重性适用于所有连接和入侵事件。默认严重性为警报。

入侵设置

- **发送 IPS 事件的系统日志消息** - 将 IPS 事件作为系统日志消息发送。除非覆盖，否则将使用上面设置的默认值。
- **显示/隐藏覆盖** - 如果要使用默认系统日志目标和严重性，请将这些选项留空。否则，可以为 IPS 事件设置不同的系统日志服务器目标，并更改事件的严重性。

文件和恶意软件设置

- **发送文件和恶意软件事件的系统日志消息**-将文件和恶意软件事件作为系统日志消息发送。除非覆盖，否则将使用上面设置的默认值。
- **显示/隐藏覆盖** - 如果要使用默认系统日志目标和严重性，请将这些选项留空。否则，可以为文件和恶意软件事件设置不同的系统日志服务器目标，并更改事件的严重性。

将其他策略与访问控制相关联

将主策略与访问控制策略相关联的最简单方法是点击访问控制策略主题中显示的数据包流中的策略链接。您可以快速选择关联的策略。或者，您可以使用策略的高级设置来关联策略，如本主题中所述。这些策略包括：

- **预过滤器策略** - 使用有限网络（第 4 层）外部报头条件执行早期流量处理。
- **解密策略** - 用于监控、解密、阻止或允许使用安全套接字层 (SSL) 或传输层安全 (TLS) 加密的应用层协议流量。
- **身份策略** - 根据与流量关联的领域和确认方法执行用户身份验证。

开始之前

在将解密策略与访问控制策略关联之前，请查看[TLS 服务器身份发现](#)中有关 TLS 服务器身份发现的信息。

过程

步骤 1 在访问控制策略编辑器中，从数据包流行末尾的 **更多** 下拉箭头中选择 **高级设置**。

步骤 2 在相应的“策略设置”区域点击**编辑** (✎)。

如果显示**视图** (👁)，则表明设置继承自祖先策略，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 3 从下拉列表中选择策略。

如果选择用户创建的策略，则可以点击显示的编辑图标来编辑策略。

步骤 4 点击**确定**。

步骤 5 点击**保存** 保存访问控制策略。

下一步做什么

- 部署配置更改；请参阅 [部署配置更改](#)。

使用策略分析器和优化器识别和修复异常

您可以使用“策略分析和优化器”来评估访问控制策略中的异常情况，如冗余规则或阴影规则，并采取行动修复发现的异常情况。策略分析器和优化器托管在云中，与未与云集成的可用规则分析不同。与云集成后，非云策略分析不可用。

系统会每日定期自动执行策略分析（每24小时）。您也可以手动启动分析。最初启用该服务时，系统会开始分析所有现有访问控制策略。



注释 在优化策略之前，请创建策略的副本。如果您对优化结果不满意，可以轻松地将托管设备重新分配给副本，并将系统返回到其起始状态。

开始之前

- 您可以直接从带有 防火墙管理中心 7.2+ 的 Security Cloud Control 使用策略分析器和优化器，但只能从 7.6 开始交叉启动该功能。分配给访问控制策略的托管设备上运行的软件版本无关紧要。策略分析器和优化器仅托管在云中，因此无论您是从防火墙管理中心还是直接从 Security Cloud Control 运行分析，都没有区别。
- 要使用该功能，您必须在 **集成 > 安全云控制** 下选择 **启用策略分析和优化**。
- 如果您已启用变更管理，则策略分析器和优化器会自动为更改创建通知单，并提交通知单。审批人必须先批准通知单，然后才能部署更改。
- 如果您使用的是域，则无法点击异常列中的链接来查看报告。请登录 Security Cloud Control 并从该应用程序中使用该功能。
- 策略分析器和优化器会在已更新、禁用或合并的规则上添加规则注释。您可以稍后搜索这些注释以查找优化的规则。
- 策略分析器和优化器实施的更改在审核日志中反映为默认名称 `internaladmin` 下的 API 调用。
- 启用策略分析器和优化器后，每次添加或编辑规则时，系统都会评估更改。如果应用规则编辑更改将导致冗余或影子规则等异常，用户会收到通知。

过程

步骤 1 选择策略 > 安全策略 > 访问控制。

如果您已运行分析，“异常” (Anomaly) 列会显示策略的问题数量和策略可以优化的百分比，以及策略分析的状态，例如“错误” (Error) 或“已完成” (Completed)。上次分析显示运行分析的日期/时间。

步骤 2 选择一个或多个策略，然后点击分析策略 (Analyze Policy)。

分析在云中作为后台进程运行。分析完成后，结果将显示在“异常” (Anomaly) 列中。

说明：

- 您还可以在编辑策略时通过选择**分析 (Analyze) > 策略 (Policy)** 来开始分析。该菜单中的其他选项允许您显示命中计数和警告。
- 如果您尚未连接到云，当您点击此按钮时，系统会打开一个说明性对话框，其中包含可帮助您开始的**集成 (Integrate)** 按钮。策略分析器和优化器仅在云中运行。

步骤 3 分析完成后，点击“异常” (Anomaly) 列中的**可优化百分比 (% Optimizable)**，以在云中启动策略分析器和优化器。

完成要执行的所有操作后，点击**应用补救 (Apply Remediations)**（在云中）。系统将向您显示要执行的操作的确认。点击**继续 (Proceed)** 以实施更改。

如果初始分析以错误结束，您可以点击**重新分析 (Re-analyze)** 以重新启动该过程。

步骤 4 部署策略以完成更改。

如果您启用了变更管理，则审批者必须先批准包含补救措施的通知单，然后才能部署这些补救措施。

查看规则命中计数

命中计数表示策略规则或默认操作与连接匹配的次数。命中计数只会随匹配策略的连接的第一个数据包递增。您可以使用此信息来确定规则的有效性。只会为应用于 Firewall Threat Defense 设备的访问控制和预过滤规则提供命中计数信息。

**注释**

- 即便是重新启动和升级，计数也会仍然存在。
- 计数会按高可用性对或集群中的每台设备来维护。
- 当设备上正在进行部署或任务时，您将无法从设备获取命中计数信息。
- 您还可以使用 **show rule hits** 命令在设备 CLI 中查看规则命中计数信息。
- 如果已从“访问控制策略” (Access Control Policy) 页面访问“命中计数” (Hit Count) 页面，则无法查看或编辑预过滤器规则，反之亦然。
- 命中计数不适用于使用“监控”操作的规则。

开始之前

如果使用自定义用户角色，请确保角色包括以下权限：

- 查看设备，以查看命中计数。
- 修改设备，以刷新命中计数。

过程

步骤 1 在访问控制策略或预过滤器策略编辑器中，点击页面右上角的分析 > 管理规则命中计数。

步骤 2 在“命中计数”页面上，从**选择设备**下拉列表中选择设备。

如果不是第一次为此设备生成命中计数，最后一次获取的命中计数信息将出现在下拉框旁边。此外，验证**最新部署**时间，以确认最新的策略更改。

选择**全部**以查看分配给该策略的所有设备的命中计数汇总。

步骤 3 如有必要，请点击 **刷新** (🔄) 以便从所选设备获取当前命中计数数据。

在预过滤器策略中，您可能需要点击**获取当前命中计数 (Fetch Current Hit Count)**，获取初始命中计数数据。

您无法在部署到设备的过程中刷新命中计数。

步骤 4 查看和分析数据。

可以执行以下操作：

- 点击**预过滤器 (Prefilter)** 或 **访问控制 (Access Control)**，以便在这些策略的命中计数之间切换。
- 通过在**过滤器框**中输入搜索字符串来搜索特定规则。
- 通过在**过滤条件 (Filter by)** 字段中选择这些选项，将列表广泛地限制为**命中规则 (Hit Rules)** 或 **从不命中规则 (Never Hit Rules)**。在查看命中规则时，您可以通过在**最后时间 (In Last)** 字段中选择一个时间范围（例如，最近 1 天）来进一步限制列表。
- （在从访问控制策略查看时。）通过选中规则的复选框，然后点击 **清除命中计数**，清除一个或多个规则的命中计数。确认操作时，选择**清除并重新加载**以刷新命中计数数据。一次最多可以清除 500 条规则的命中计数。您无法撤消清除命中计数。

注释

点击表信头中的复选框以选择列表中的所有规则。要选择一系列规则，请选中第一个规则的复选框，然后按住 Shift 键并点击最后一个规则的复选框；中间的所有规则也会被选中。

- （在从访问控制策略查看时。）您可以对单个规则执行以下操作：
 - 通过点击 **更多** (⋮) 菜单中的 **编辑** 来编辑规则。
 - 通过点击 **更多** (⋮) 菜单中的 **删除** 来从策略中删除规则。
 - 通过点击 **更多** (⋮) 菜单中的 **启用/禁用规则** 来启用或禁用规则。
 - 通过点击 **更多** (⋮) 菜单中的 **清除命中计数** 来清除规则的命中计数（将其重置为零）。您无法撤销此操作。
- （从预过滤器策略查看时。）通过点击 **齿轮** (⚙️) 并选择要显示的列来更改显示的列。

- （从预过滤器策略查看时。）点击规则名称以对其进行编辑，或点击最后一列中的 **视图** (👁) 以查看规则详细信息。点击规则名称会在策略页面中突出显示它，您可以在该页面中对规则进行编辑。
- （从预过滤器策略查看时。）通过右键点击规则并选择 **清除命中计数 (Clear Hit Count)**，清除规则的命中计数信息（将其重置为零）。您可以使用 Ctrl+ 点击来选择多个规则。您无法撤销此操作。
- 通过点击页面左下角的 **生成 CSV (Generate CSV)** 来生成页面详细信息的逗号分隔值报告。

步骤 5 点击 **关闭** 返回策略页面。

分析规则冲突和警告



注释 仅当未与思科安全云集成时，本主题中介绍的功能才可用。当您与云集成时，功能更强大的策略分析器和优化器将取代此功能。请参阅 [使用策略分析器和优化器识别和修复异常](#)，第 20 页。

您可以查看有关规则冲突的警告和信息，以便检查访问控制策略的逻辑并确定需要更改的规则。当规则重叠时，您可能在策略中使用不必要的规则，而这些规则将永远不会与流量匹配。分析可以帮助您删除不必要的规则，或者确定应移动或修改的规则，以便实施所需的策略。

策略警告和错误会指出您应该了解并可能解决的问题，从而确保您的规则提供所需的服务。

规则冲突分析可识别以下类型的问题：

- **对象重叠** - 规则某字段中的元素是该规则同一字段中一个或多个元素的子集。例如，源字段可能包括 10.1.1.0/24 的网络对象以及主机 10.1.1.1 的另一个对象。由于 10.1.1.1 位于 10.1.1.0/24 覆盖的网络内，因此 10.1.1.1 的对象是冗余的且可被删除，从而简化规则并节省设备内存。
- **冗余规则** - 两个规则对同一类型的流量应用相同的操作，删除基础规则不会改变最终结果。例如，如果允许特定网络的 FTP 流量的规则后接允许该网络的 IP 流量的规则，并且在拒绝访问之间没有规则，则第一条规则是冗余的，您可以将其删除。
- **阴影规则** - 这与冗余规则相反。在这种情况下，一条规则将与另一条规则匹配相同的流量，因此第二条规则永远不会被应用于访问列表中稍后出现的任何流量。如果两个规则的操作相同，则您可以删除被屏蔽的规则。如果两个规则为流量制定了不同的操作，则您可能需要移动阴影规则或编辑两条规则之一，以便实施所需的策略。例如，对于给定的源或目标，基本规则可能会拒绝 IP 流量，而阴影规则可能会允许 FTP 流量。

开始之前

进行分析时：

- 仅识别给定规则的第一个冲突。在问题得到修复后，该规则可能会被识别为与表中的另一个规则存在冲突。但是，一个规则可能会有多个警告或错误。

- 规则冲突分析只会考虑源/目标安全区域、网络、VLAN和服务/端口匹配条件和操作。它不会考虑其他匹配条件，因此明显冗余的规则可能并非完全冗余。
- 无法分析 FQDN 网络对象是否存在冲突，因为无法在进行 DNS 查找之前知道 FQDN 的 IP 地址。
- 已禁用的规则会被忽略。
- 时间范围属性会被忽略。不同时间段的规则在时间范围内实际上不是冗余时，它们可能会被标记为冗余。
- 在启用该功能时，警告和错误以及规则冲突的图标会显示在规则表中。有关图标的参考，请参阅[规则和其他策略警告，第 5 页](#)。

过程

步骤 1 选择策略 > 安全策略 > 访问控制，然后编辑该策略。

步骤 2 执行以下操作之一打开规则冲突和警告对话框：

- 要查看规则冲突，请点击**分析 (Analyze)** 下拉列表，然后点击**启用规则冲突 (Enable Rule Conflicts)**。分析完成后，您会在页面顶部看到冲突摘要。然后，从同一菜单中点击**显示规则冲突**以查看具体结果。

每次进行打开策略或更改并保存策略时，都必须重新启用规则冲突检测。

- 要查看规则警告和错误，请点击**分析 > 显示警告和错误**。

对策略进行更改后，您可以通过点击分析按钮旁边的重新加载图标来刷新结果。

- 要查看策略警告，请点击**分析 > 显示策略警告**。
- 如果您已查看完规则冲突，请点击**分析 (Analyze) > 禁用规则冲突 (Disable Rule Conflicts)**。

步骤 3 在规则冲突和警告对话框中：

- 规则警告和错误会显示在与规则冲突分开的选项卡上。还有一个单独的选项卡用于显示策略警告。
- 每个选项卡都包含子选项卡，可让您检查各个类型的问题，例如冗余与阴影或警告与错误。此外，也可以搜索项目。
- 每个规则名称旁边的**更多 (⋮)** 提供编辑、禁用或删除规则的快捷方式。

步骤 4 完成后点击“关闭”。

搜索规则

您可以使用搜索功能来帮助自己查找规则，尤其是在有大量的规则时。

过程

步骤 1 编辑访问控制策略时，通过点击**搜索 (Search)** 框构建搜索字符串。

- 对于简单的文本字符串搜索，请键入字符串。搜索将返回在任何列中包含该字符串的规则。不能将字符串搜索与标记搜索结合使用，例如将字符串搜索与源网络搜索结合使用。
- 要搜索特定的列，请开始键入列的名称，直到系统提示您输入全称，例如“源网络”，或选择可搜索字段的列表名称。在选择搜索标记后，即可输入该标记的搜索字符串。例如，**源网络 10.1.1.1**。
- 在源/目标列中搜索 IP 地址时（但不是作为简单的文本搜索），可以使用**搜索内部子网和范围**选项来控制是完全匹配 IP 地址（未选中）还是匹配包含搜索地址的任何子网或范围（选中）。例如，选中该选项后，搜索 10.1.1.1 将包含 10.1.1.0/24 的规则。
- 在端口字段中搜索仅会返回完全匹配项。
- 输入多个值时，请用逗号分隔这些值。
- 第一次搜索后，点击搜索框会提示您最近的搜索和标记。您可以通过选择快速重复搜索，或通过选择以前的搜索或标记并在其基础上来构建类似的搜索。
- 构建具有多个标记的搜索字符串时，请不要在标记之间包含空格。
- 在选择标记时，系统会提示您输入这些列中显示的值。选择您要搜索的值。
- 您可以根据一些常见功能快速进行筛选，方法是点击搜索框左侧的过滤器图标，然后选择显示具有以下任意组合的规则：允许、阻止、监视、入侵策略、时间范围、冲突、警告、错误、禁用规则、过期规则、包含定义重叠的对象的规则。。
- 要查看适用于特定设备或一组设备的规则，请点击过滤器图标并选择设备。如果规则使用包含设备上至少一个接口的安全区域，或者它们不包含安全区域，则这些规则适用于设备。

步骤 2 将光标置于搜索框中搜索字符串的末尾，然后按 **Enter** 键。

满足搜索字符串的规则会被突出显示，而不匹配的规则会被隐藏。您可以取消选择**仅显示匹配规则 (Show Only Matching Rules)** 以查看整个表，以及该表中突出显示的规则。这让您能够查看周围的规则。

“仅显示匹配规则” (Show Only Matching Rules) 复选框旁边是与匹配搜索字符串的数量相比的策略中规则总数的摘要。

步骤 3 要关闭搜索并返回到未过滤和未突出显示的表，请点击搜索框右侧的 **X**。您还可以将光标放在搜索字符串的末尾，然后按 **Esc** 键。

访问控制策略的历史记录

表 3:

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
多个用户同时编辑访问控制策略。	10.0.0	任意	在以前的版本中，如果两个或多个用户同时编辑访问控制策略，第一个保存的用户将保留其更改，所有其他用户将立即丢失其所有编辑内容。现在，这些用户能够有选择地合并其更改，并且与第一个用户保存的更改不冲突的更改将自动被接受。这改进了用户之间的协作，并减少了在编辑期间锁定策略的需求。
对象组搜索性能增强。	7.6.0	7.6.0	对象组搜索现在速度更快，使用的 CPU 资源更少。 新的 CLI 命令： clear asp table network-object 、 show asp table network-object 、 debug acl ogs 修改的 CLI 注释（增强的输出）： packet-tracer 、 show access-list 、 show object-group
用于访问控制的策略分析器和优化器。	从管理中心：7.6.0 从 Security Cloud Control：7.2.0	任意	策略分析器和优化器评估冗余或影子规则等异常的访问控制策略，并采取修复措施修复已发现的异常。 您可以直接从版本 7.6 以上的防火墙管理中心启动访问控制策略分析与优化器；这需要思科安全云。对于版本 7.2-7.4 的防火墙管理中心，请使用 Security Cloud Control。 新增/修改的屏幕： - 要启用：集成 (Integration) > 思科安全云 (Cisco Security Cloud) > 启用策略分析器和优化器 (Enable Policy Analyzer & Optimizer) - 要分析策略：策略 (Policies) > 访问控制 (Access Control)，选择策略，点击分析策略 (Analyze Policies)。
用于修改访问控制策略和规则的精细权限。	7.4.0	任意	您可以定义自定义用户角色，以区分访问控制策略和规则中的入侵配置以及访问控制策略和规则的其余部分。使用这些权限，您可以分离网络管理团队和入侵管理团队的职责。 定义用户角色时，可以选择 策略 > 访问控制 > 访问控制策略 > 修改访问控制策略 > 修改威胁配置 选项，以允许在规则中选择入侵策略、变量集和文件策略，以及配置网络分析的高级选项和入侵策略、访问控制策略的安全智能策略配置以及策略默认操作中的入侵操作。您可以使用 修改其余访问控制策略配置 来控制编辑策略的所有其他方面的能力。包含“修改访问控制策略”权限的现有预定义用户角色继续支持所有子权限；如果要应用精细权限，则需要创建自己的自定义角色。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
新的访问控制策略用户界面和规则冲突分析。	7.3.0	任意	7.2 中引入的访问控制策略用户界面现在为默认界面。您还可以启用规则冲突分析，以便帮助识别冗余规则和对象，以及识别由于策略中的先前规则而无法匹配的影子规则。
访问控制策略锁定。	7.2.0	任意	您可以锁定访问控制策略，以防止其他管理员对其进行编辑。锁定策略可确保在您保存更改之前，如果其他管理员编辑策略并保存更改，您的更改不会失效。任何有权修改访问控制策略的用户都有权锁定它。 我们在策略名称旁边添加了一个图标，用于在编辑策略时锁定或解锁策略。此外，还有一个允许用户解锁其他管理员锁定的策略的新权限：覆盖访问控制策略锁定。默认情况下，管理员、访问管理员和网络管理员角色启用此权限。
规则命中计数在重新启动后保持不变。	7.2.0	任意	重新启动托管设备不会再将访问控制规则命中计数重置为零。仅当您主动清除计数器时，才会重置命中计数。此外，高可用性对或集群中的每台设备单独维护计数。您可以使用 show rule hits 命令查看 HA 对或集群中的累计计数器，或查看每个节点的计数。 修改了以下设备 CLI 命令：show rule hits。
访问控制策略的可用性改进。	7.2.0	任意	有一个可用于访问控制策略的新用户界面。您可以继续使用旧版用户界面，也可以试用新的用户界面。新界面同时具有规则列表的表和网格视图、显示或隐藏列的功能、增强的搜索、无限滚动、与访问控制策略相关联的更清晰的数据包流视图，以及简化的用于创建规则的添加/编辑对话框。编辑访问控制策略时，可以在新旧用户界面之间自由切换。
DNS 过滤	7.0.0 6.7.0（实验性）	任意	如果启用并配置了 URL 过滤，则默认情况下会为每个新的访问控制策略启用一个新的选项，以用于增强类别和信誉过滤效率。 有关信息，请参阅 DNS 过滤：在 DNS 查找期间识别 URL 信誉和类别和子主题。 访问控制策略的“高级” (Advanced) 选项卡在“常规设置” (General Settings) 下有一个新选项：对 DNS 流量启用信誉实施 (Enable reputation enforcement on DNS traffic)。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
TLS 服务器身份发现	6.7.0	任意	在客户端连接到支持 TLS 1.3 的服务器时，启用访问控制策略以评估 URL 和应用条件。通过 TLS 服务器身份发现，无需解密流量即可对这些条件进行评估。 启用此功能可能会影响设备性能，但具体取决于型号。 访问控制策略的“高级”(Advanced)选项卡页面具有新选项： - 警告会显示在“高级”(Advanced)选项卡上；向右移动滑块可启用 TLS 服务器身份发现。 “高级”(Advanced)选项卡页面上的新选项：TLS 服务器身份发现 (TLS Server Identity Discovery)。
新的安全智能类别	-	任意	以下类别是在 6.6 版本时引入的，但并非特定于 6.6： - banking_fraud - high_risk - ioc - link_sharing - 广告的 - newly_seen - 间谍软件

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。