访问控制策略

以下主题介绍如何使用访问控制策略：

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。

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。

安全情报

安全情报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 SSL、预过滤器和入侵策略。

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、SSL 检查、身份和各种性能选项。

系统创建的访问控制策略

根据设备的初始配置，系统提供的策略可以包括：

- “默认访问控制”(Default Access Control) - 阻止所有流量，而不进行进一步检查。
- “默认入侵防御”(Default Intrusion Prevention) - 允许所有流量，但是还会使用“平衡安全性和连接”(Balanced Security and Connectivity) 入侵策略和默认入侵变量集进行检查。
- “默认网络发现”(Default Network Discovery) - 检查时允许发现数据的所有流量，但不允许入侵或漏洞的流量。

访问控制策略的要求和必备条件

型号支持

Any

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** > **访问控制** > **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，配置安全情报策略访问控制策略，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** > **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：

- 创建 - 点击**新建策略 (New Policy)**；请参阅创建基本访问控制策略， 第 4 页。
- 继承 - 点击具有后代的策略旁边的**加号**，展开策略层次结构视图。
- 编辑 - 点击 **编辑**（ ）；请参阅编辑访问控制策略， 第 4 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。
- 复制-点击 **复制** ( )。系统在副本保留设备分配。
- 点击 **报告**（ ）。
- 锁定或解锁策略 - 请参阅锁定访问控制策略， 第 6 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** > **访问控制**。

步骤 2 点击**新建策略 (New Policy)**。

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

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，选择要部署策略的**可用设备 (Available Devices)**，然后点击**添加到策略 (Add to Policy)**（或拖放）以添加所选设备。要减少显示的设备，请在 **Search** 字段中键入搜索字符串。

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 (Save)**。

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 4 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。

注释 如果不锁定策略，请考虑以下事项：一个用户一次只能使用一个浏览器窗口编辑一个策略。如果多个用户保存同一个策略，系统会保留最后的更改。为方便起见，系统会显示有关当前正在编辑每条策略的人员（如有任何人）的信息。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。

过程

步骤 1 选择**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**选择操作 (Select Action)** 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、克隆、移动、删除和编辑规则，或查看命中计数或相关事件。

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 (Save)**。
- 默认操作 - 从**默认操作 (Default Action)** 下拉列表中选择一个值。
- 默认操作设置 - 点击 **齿轮**（ ），进行更改，然后点击**确定 (OK)**。您可以配置日志记录设置、外部系统日志服务器或 SNMP 陷阱服务器的位置，以及与入侵防御默认操作关联的变量集。
- 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**、 **安全情报**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**目标：x 设备 (Targeted: x devices)** 链接。
- 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**（ ） 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 (Show/Hide Columns)** 图标，选择要在表中显示的信息。点击**隐藏空列 (Hide Empty Columns)** 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 (Analyze)** 菜单中选择以下选项来检查规则的逻辑：
  - **命中计数**-要查看有关与每个规则匹配的连接数的统计信息。
  - **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。
  - **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。
  - **显示警告**-查看是否存在需要解决的配置问题的规则。
- 其他设置 - 要更改策略的其他设置，请从数据包流行末尾的**更多 (More)** 下拉箭头中选择以下选项之一。
  - **高级设置 (Advanced Settings)** - 要设置预处理、SSL 检查、身份、性能及其他高级选项。请参阅访问控制策略高级设置，第 11 页。
  - **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 8 页和锁定后代访问控制策略中的设置，第 9 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 (Save)**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

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。在不锁定的情况下，如果多个管理员同时编辑策略，则以保存更改的第一个用户为准，而所有其他用户的更改都会被清除。

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 (Policies)** > **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

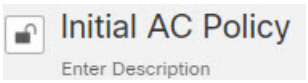
步骤 1 选择**策略** > **访问控制**。

步骤 2 点击要锁定或解锁的访问控制策略旁边的 **编辑**（ ）。

锁定状态 (Lock Status) 列会显示策略是否已被锁定，如果已锁定，则显示被谁锁定。空单元格表示策略未被锁定。

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 (Lock/Unlock This Policy)** - 锁定或解锁仅适用于此策略。
- **锁定/解锁此策略和层次结构中的父项 (Lock/Unlock This Policy and Parents in the Hierarchy)** - 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。

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。

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 4 页。

步骤 2 管理策略继承：

- 更改基本策略 (Change Base Policy) - 要更改基本访问控制策略，请从数据包流行末尾的**更多 (More)** 下拉箭头中选择**继承设置 (Inheritance Settings)**，然后如选择基本访问控制策略，第 8 页中所述继续操作。

- 锁定后代策略中的设置 (Lock Settings in Descendants) - 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 (More)** 下拉箭头中选择**继承设置 (Inheritance Settings)**，然后如锁定后代访问控制策略中的设置，第 9 页中所述继续操作。
- 要求在域中提供 (Required in Domains) - 要在子域中执行此策略，请点击**目标：x 个设备 (Targeted: x devices)** 链接，然后如在域中需要访问控制策略，第 9 页中所述继续操作。
- 继承基本策略的设置 (Inherit Settings from Base Policy) - 要继承基本访问控制策略的设置，请点击 **安全情报 (Security Intelligence)**，或从数据包流行末尾的下拉箭头中选择 **HTTP 响应 (HTTP Responses)** 或**高级设置 (Advanced Settings)**，然后如继承基本策略的访问控制策略设置，第 8 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。

步骤 3 点击**保存 (Save)**。

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 (Security Intelligence)**，或者从从数据包流行末尾的**更多 (More)** 下拉箭头中选择 **HTTP 响应 (HTTP Responses)** 或**高级设置 (Advanced Settings)**

步骤 2 选中要继承的每个设置所对应的**继承自基本策略 (Inherit from base policy)** 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 (Save)**。

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 (OK)** 保存设置。

步骤 4 点击**保存 (Save)** 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。

在域中需要访问控制策略

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 **目标： x 高级** 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 (OK)** 以保存域实施设置。

步骤 5 点击**保存 (Save)** 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。

设置访问控制策略的目标设备

访问控制策略指定使用策略的设备。每台设备只能作为一个访问控制策略的目标。

过程

步骤 1 在访问控制策略编辑器中，点击 **目标： x 高级** 链接。

步骤 2 在 **目标设备** 上，建立目标列表：

- 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 (Ok)** 以保存目标设备设置。

步骤 4 点击**保存 (Save)** 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SSL/TLS解密、预过滤器和入侵策略。

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

- **使用特定系统日志警报发送**-如果选择此选项，则会根据 《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发送事件。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。此选项适用于所有设备。

  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。

- **使用设备上部署的威胁防御平台设置策略中配置的系统日志设置**-如果选择此选项并选择严重性，则系统会将具有所选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。

  此选项仅适用于 Cisco Secure Firewall Threat Defense 6.3 及更高版本。

IPS 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。

访问控制策略高级设置

要配置访问控制策略的高级设置，请从数据包流行末尾的 **更多** 下拉箭头中选择 **高级设置** 。

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。默认设置适用于大多数的部署。请注意，规则更新可能会修改访问控制策略中的许多高级预处理和性能选项，如 《Cisco Secure Firewall Management Center 管理指南》 中 更新入侵规则 所述。

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。

⚠

注意 有关重启 Snort 进程的高级设置修改列表，请参阅部署或激活时重启 Snort 进程的配置，以暂时中断流量检查。 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。

从父策略继承设置

如果访问控制策略具有基本策略，则可以选择从基本策略继承设置。为要使用父策略设置的每个设置组选择**从基本策略继承 (Inherit from base policy)**。如果已配置继承，以便锁定这些设置，则无法为策略配置唯一设置，这些设置为只读。

如果允许您为策略配置唯一设置，则必须取消选择**从基本策略继承 (Inherit from base policy)** 以进行编辑。

常规设置

选项	说明
要在连接事件中存储的最大URL字符数	要自定义您为用户所请求的每个URL存储的字符数。有关详细信息，请参阅 《Cisco Secure Firewall Management Center 管理指南》中的 限制长 *URL* 的日志记录 。 要自定义用户绕过初始阻止后您重新阻止网站前的时长；请参阅为受阻网站设置用户绕过超时。
允许交互式阻止绕过阻止的时长（秒）	请参阅为受阻网站设置用户绕过超时。
重试 URL 缓存缺失查询	系统第一次遇到没有本地存储的类别和信誉的URL时，会在云中查找该URL并将结果添加到本地数据存储中，以便在将来更快地处理该 URL。 此设置确定系统需要在云中查找 URL 的类别和信誉时执行的操作。 默认情况下，此设置处于启用状态：系统在检查云的URL信誉和类别时会暂时延迟流量，并使用云判定来处理流量。 如果禁用此设置：当系统遇到不在其本地缓存中的URL时，系统会根据为未分类和无信誉流量配置的规则立即传递和处理流量。 在被动部署中，由于系统无法保留数据包，因此不会重试查询。
启用威胁情报导向器	禁用此选项以停止将 TID 数据发布到配置的设备。
对 DNS 流量启用信誉实施	默认情况下会启用此选项，以提高URL过滤性能和效力。有关详细信息和其他说明，请参阅 DNS 过滤：在 DNS 查找期间识别 URL 信誉和类别 和子主题。

选项	说明
在策略应用期间检测流量	要在部署配置更改时检查流量（除非特定配置需要重新启动 Snort 进程），请确保**在策略应用期间检查流量 (Inspect traffic during policy apply)** 设置为其默认值（已启用）。 启用此选项后，资源需求可能会导致丢弃少量数据包而不进行检查。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。有关详细信息，请参阅Snort 重新启动场景。

关联策略

使用高级设置将子策略（解密、身份、预过滤器）与访问控制相关联；请参阅 将其他策略与访问控制相关联，第 16 页。

TLS 服务器身份发现

RFC 8446定义的最新版本的传输层安全（TLS）协议 1.3 是许多 Web 服务器提供安全通信的首选协议。由于 TLS 1.3 协议会加密服务器的证书以提高安全性，并且需要使用证书来匹配访问控制规则中的应用和 URL 过滤条件，因此 Firepower 系统提供了一种提取服务器证书而 不 解密整个数据包的方法。

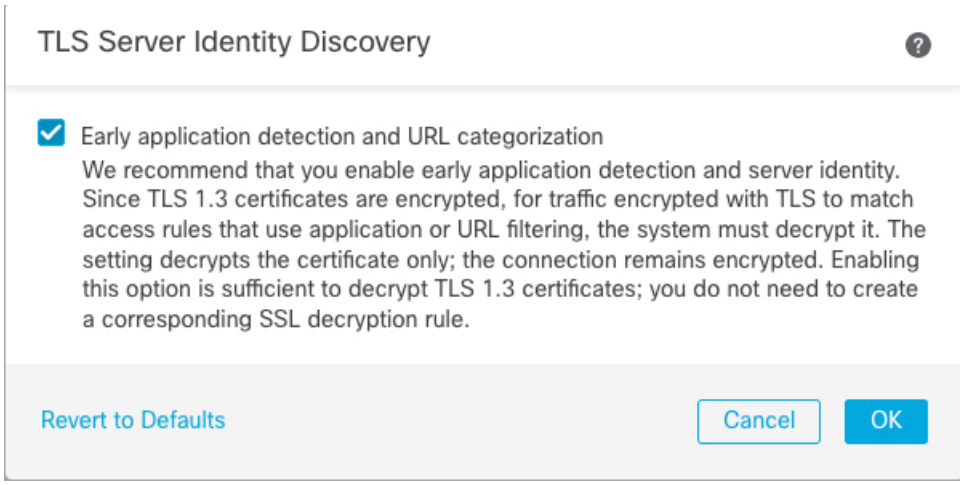
在为访问控制策略配置高级设置时，可以启用此功能，称为 *TLS* 服务器身份发现。

如果启用此选项，我们建议您同时启用解密策略的高级 TLS 自适应服务器身份探测选项。总之，这些选项可更有效地解密 TLS 1.3 流量。有关详细信息，请参阅TLS 1.3 解密最佳实践。

当新连接开始且受 TLS 服务器身份发现影响时，威胁防御 会保留原始 ClientHello 数据包，以确定其连接的服务器的身份，然后再继续。威胁防御 设备会从 威胁防御 向服务器发送专用连接。服务器的响应包括服务器证书，专用连接会被终止，并根据访问控制策略的要求评估原始连接。

TLS 服务器身份发现将证书的通用名称 (CN) 优先于服务器名称指示 (SNI)。

要启用 TLS 服务器身份发现，请点击 **高级** 选项卡，点击 **编辑**（ ） 以获取设置，然后选择**早期应用检测和 URL 类别**。



我们强烈建议您为要根据应用或URL条件匹配的任何流量启用此功能，尤其是在您想要对该流量执行深度检查时。解密策略 不需要 SSL 策略，因为在提取服务器证书的过程中不会解密流量。

注释

- 由于证书是解密的，因此 TLS 服务器身份发现会降低性能，具体取决于硬件平台。
- 内联分路模式或被动模式部署不支持 TLS 服务器身份发现。
- 任何部署到 AWS 的 Cisco Secure Firewall Threat Defense Virtual 都不支持启用 TLS 服务器身份发现。如果您有任何由 Cisco Secure Firewall Management Center管理的此类受管设备，则每次设备尝试提取服务器证书时，连接事件 **PROBE_FLOW_DROP_BYPASS_PROXY** 都会增加。
- TLS 服务器身份发现也可在 TLS 1.2 会话上运行。

网络分析和入侵策略

高级网络分析和入侵策略设置可供您：

- 指定用于检查数据包的入侵策略和相关变量集，在系统确定如何准确检查该流量之前，这些数据包必须通过。
- 更改访问控制策略的默认网络分析策略，该默认策略监管许多预处理选项。
- 使用自定义网络分析规则和网络分析策略根据特定安全区域、网络和 VLAN 定制预处理选项。

有关详细信息，请参阅网络分析和入侵策略的高级访问控制设置。

威胁防御服务策略

可以使用威胁防御设备策略将服务应用到特定流量类。例如，可以使用服务策略创建特定于某项TCP应用而非应用于所有TCP应用的超时配置。此策略仅适用于 威胁防御设备，对于其他任何设备类型将被忽略。在访问控制规则之后应用服务策略规则。有关详细信息，请参阅服务策略。

文件和恶意软件设置

调整文件和恶意软件检测性能和存储提供有关文件控制和 恶意软件防护的性能选项的信息。

端口威胁检测

Portscan 检测器是一种威胁检测机制，旨在帮助您检测和阻止所有类型流量中的端口扫描活动，以保护网络免受最终攻击。可以在允许和拒绝的流量中高效检测 Portscan 流量。有关详细信息，请参阅威胁检测。

大象流设置

象流是大型，持续时间长且快速的流，可能会导致 Snort 核心受到威胁。有两种操作可应用于象流，以减少系统压力、CPU 占用、丢包等。这些操作包括：

- 绕过任何或所有应用-此操作绕过来自 Snort 检测的流。
- Throttle-此操作对象流应用动态速率限制策略（降低 10%）。

有关更多信息，请参阅《Cisco Secure Firewall Management Center Snort 3 配置指南》中的“象流检测”一章。

智能应用绕行设置

智能应用绕行 (IAB) 是一种专业级配置，指定如果流量超出检查性能和流量阈值的组合，则应用绕行或测试是否要绕行。有关详细信息，请参阅智能应用旁路。

传输/网络层预处理器设置

高级传输和网络预处理器设置全局应用于会部署访问控制策略的所有网络、区域和 VLAN。可以在访问控制策略中而非网络分析策略中配置这些高级设置。有关详细信息，请参阅高级传输/网络预处理器设置。

检测增强功能设置

您可以使用高级检测增强功能设置配置自适应配置文件，以便：

- 使用访问控制规则中的文件策略和应用。
- 使用入侵规则中的服务元数据。
- 在被动部署中，根据您的网络主机操作系统改善数据包分片和 TCP 流的重组。

有关详细信息，请参阅自适应配置文件。

性能设置和基于延迟的性能设置

关于入侵防御性能调整提供了在您系统分析流量是否存在入侵尝试时如何提高系统性能的信息。

有关特定于基于延迟的性能设置的信息，请参阅数据包和入侵规则延迟阈值配置。

加密可视性引擎

有关此功能的详细信息，请参阅《Cisco Secure Firewall Management Center Snort 3 配置指南》中的“加密可视性引擎”一章。

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。

注意 仅*Snort 2*。添加或删除 SSL 政策在部署配置更改时重新启动 Snort 进程，从而暂时中断流量检测。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。有关详细信息，请参阅Snort 重启流量行为。

- 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 SSL 策略与访问控制策略关联之前，请查看 访问控制策略高级设置，第 11 页中有关 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来编辑策略。

步骤 4 点击**确定 (OK)**。

步骤 5 点击**保存 (Save)** 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。

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。只会为应用于威胁防御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**分析命中计数 (Analyze Hit Counts)**。

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。

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。）通过右键单击规则并选择**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

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，您可能会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：

- 对象交叉 - 规则字段中的元素是规则的相同字段中的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，而删除基本规则并不会改变最终结果。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 - 它与冗余规则相反。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。

过程

步骤 1 选择**策略 (Policy)** > **访问控制 (Access Control)**，然后编辑访问控制策略。

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 (Analyze)** > **显示警告 (Show Warnings)**。

  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：

- 警告和错误会显示在规则冲突的单独选项卡上。
- 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 完成后单击“**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。

当您在源或目标网络中搜索 IP 地址时（但不是作为简单的文本搜索），系统会返回与该地址匹配的规则。这不仅包括精确匹配，还包括子网匹配。例如，搜索 10.1.1.1 将包括 10.1.1.0/24 的规则。

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签搜索结合使用，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。在选择搜索标签后，即可输入该标签的搜索字符串。例如，**源网络 10.1.1.1**。
- 第一次搜索后，点击搜索框会提示您最近的搜索和标签。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。
- 构建具有多个标签的搜索字符串时，请不要在标签之间包含空格。
- 在选择标签时，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，方法是单击搜索框左侧的筛选器图标，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。

- 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

功能	最低 管理中心	最低 威胁防御	详情
用于修改访问控制策略和规则的精细权限。	7.4	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情报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。
新的访问控制策略用户界面和规则冲突分析。	7.3	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	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。

功能	最低 管理中心	最低 威胁防御	详情
规则命中计数在重新启动后保持不变。	7.2	任意	重新启动受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	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 6.7（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)**。
TLS 服务器身份发现	6.7	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)**。

功能	最低 管理中心	最低 威胁防御	详情
新的安全情报类别	-	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。