访问控制规则

以下主题介绍如何配置访问控制规则。

关于访问控制规则

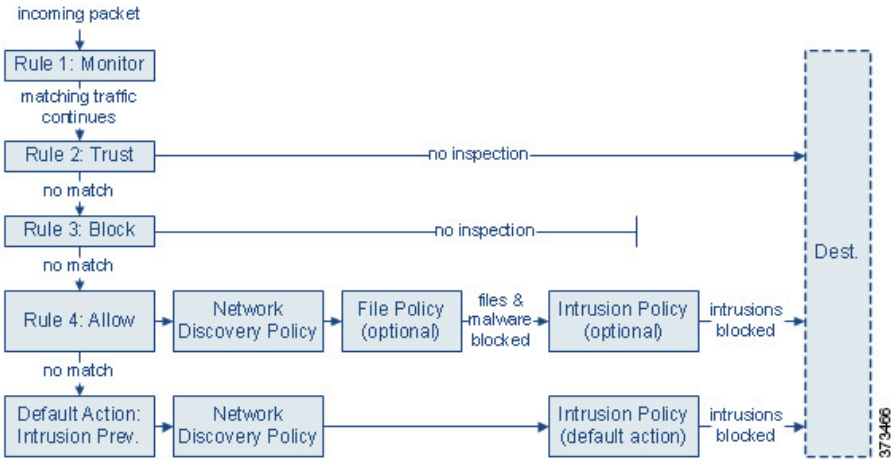
在访问控制策略中，访问控制规则提供在多台托管设备之间处理网络流量的精细方法。

注释 安全智能过滤、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。



在这种情况中，流量评估如下：

- **规则 1：监控** 首先评估流量。“监控”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：信任** 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。
- **规则 3：阻止** 第三步，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**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。
- **默认操作**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可以添加、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。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。这些图标代表：

- 时间范围选项（  ）
- 入侵策略（  ）
- 文件策略（  ）
- 日志记录（  ）
- 警告（  ）
- 错误（  ）
- 规则冲突 （  ）

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，请参阅创建和编辑访问控制规则，第 22 页。

提示 右键点击菜单提供很多规则管理选项的快捷方式，包括编辑、删除、移动、启用和禁用。

相关主题

访问控制规则组成部分，第 3 页
访问控制规则的最佳实践，第 16 页

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

您可以指定规则生效的日期和时间。

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。您可以按应用和协议记录会话，然后将这些日志转发到事件管理解决方案以进行进一步分析。

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，第 16 页
访问控制规则管理，第 3 页
创建和编辑访问控制规则，第 22 页
访问控制规则操作，第 6 页
访问控制规则条件，第 24 页
使用文件和入侵策略的深度检测，第 8 页
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准则，才可优化性能，同时满足您的需求。有关具体提示，请参阅规则排序的最佳实践，第 17 页。

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。

访问控制规则信任操作

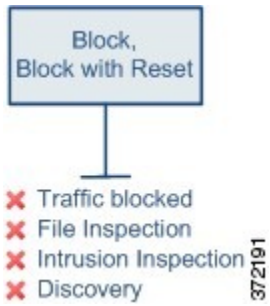
信任 (Trust) 操作允许流量通过，无需深度检查或网络发现。受信任的流量仍会受到身份要求和速率限制的制约。

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)**。
- 对于已禁用日志记录选项的信任规则，系统仍会生成流量结束事件。但是，在活动页面上看不到这些活动。
- 由于访问控制规则是在其他策略（如解密）之后进行评估的，因此信任一个连接并不一定意味着它可以快速通过而无需进行检查。例如，如果一个连接既符合需要解密的解密规则，又符合信任访问控制规则，那么在信任规则允许之前，就会对该连接进行必要的解密和检查。信任意味着不会进行额外的检查，如入侵检查。如果您打算允许连接不接受检查，则可以使用预过滤器策略来快速通过连接，或者确保没有其他策略对连接应用检查服务。

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。

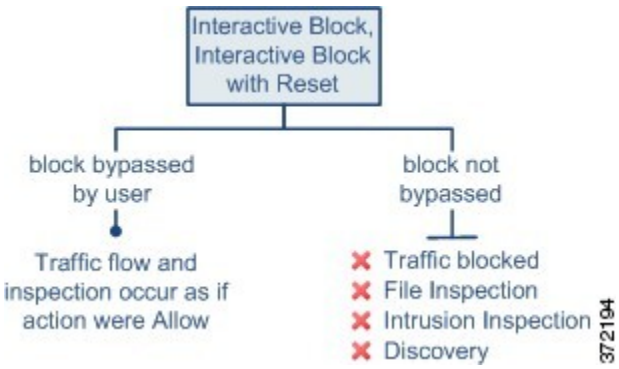
有关详细信息，请参阅配置 HTTP 响应页面。

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，请参阅配置 HTTP 响应页面。

相关主题

基于规则的解密 规则阻止操作

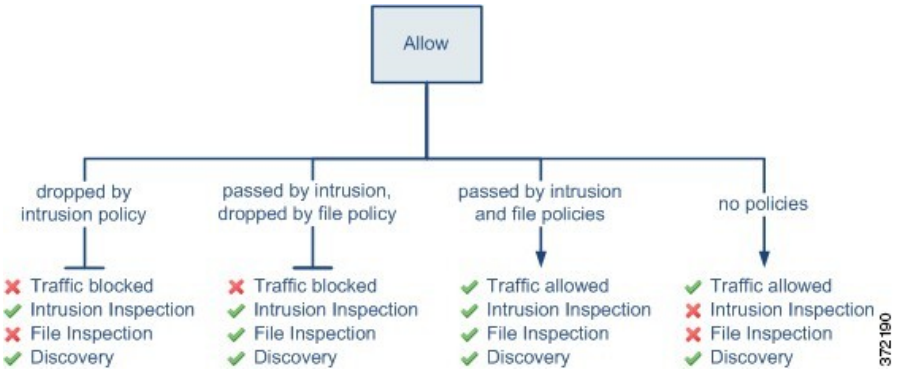
访问控制规则允许操作

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。

使用文件和入侵策略的深度检测

深度检测会将入侵策略和文件策略用作为允许流量到达其目标之前的最后一道防线。

- 入侵策略监管系统的入侵防御功能。

  有关详细信息，请参阅关于入侵防御。

- 文件策略监管系统的文件控制和恶意软件防护 功能。

  有关详细信息，请参阅网络恶意软件防护的文件策略。

访问控制发生在深度检查之前；访问控制规则和访问控制默认操作确定哪些流量由入侵和文件策略检测。

通过将入侵策略或文件策略与访问控制规则相关联，您是在告诉系统：在其传递符合访问控制规则条件的流量之前，您首先想要使用入侵策略和/或文件策略检测流量。

在访问控制策略中，您可以将一个入侵策略与每条“允许”(Allow) 和“交互式阻止”(Interactive Block) 规则以及默认操作相关联。每个唯一的入侵策略和变量集**对均**视为一个策略。

注释 默认情况下，系统禁用对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。

要将入侵策略和文件策略与访问控制规则相关联，请参阅：

- 访问控制规则：入侵策略选择
- 配置访问控制规则以执行恶意软件保护

文件和入侵检查顺序

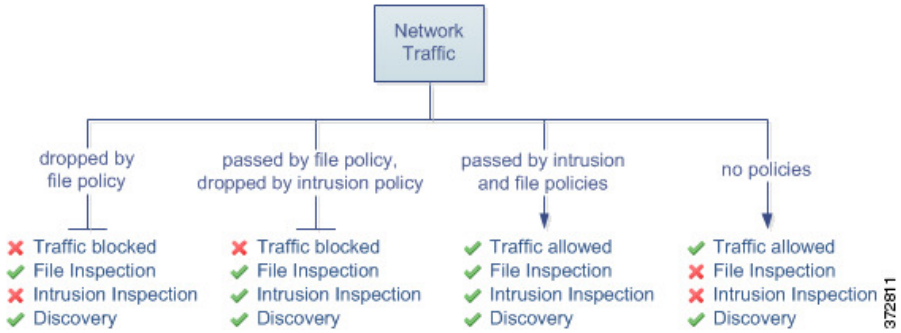
在您的访问控制策略中，您可以将多个 Allow 和 Interactive Block 规则与不同的入侵和文件策略相关联，以使检查配置文件匹配各种流量类型。

您不必在同一规则中同时执行文件和入侵检测。对于符合“允许”(Allow)或“交互式阻止”(Interactive Block) 规则的连接：

- 没有文件策略，数据流取决于入侵策略
- 没有入侵策略，数据流取决于文件策略
- 若以上两者都没有，仅由网络发现检查允许的流量

提示 系统不会对受信任的流量执行任何种类的检测。虽然没有使用入侵或文件策略配置“允许”(Allow) 规则可以放行流量，就像“信任”(Trust) 规则那样，但“允许”(Allow) 规则让您可以对匹配的流量执行发现。

下图说明对符合“允许”(Allow) 或用户绕过的“交互式阻止”(Interactive Block) 访问控制规则的条件的流量执行的检查类型。为简单起见，该图显示入侵策略和/或文件策略与单个访问控制规则关联的情况的流量。



对由访问控制规则处理的任何单个连接，文件检测均发生在入侵检测之前。也就是说，系统不检测文件策略所阻止的文件是否存在入侵。在文件检测中，基于类型的简单阻止优先于恶意软件检测和阻止。

例如，请考虑按照访问控制规则中所定义通常要允许特定网络流量的情况。但是，作为预防措施，您希望阻止下载可执行文件，检测恶意软件的已下载的 PDF 并阻止找到的所有实例，然后对流量执行入侵检测。

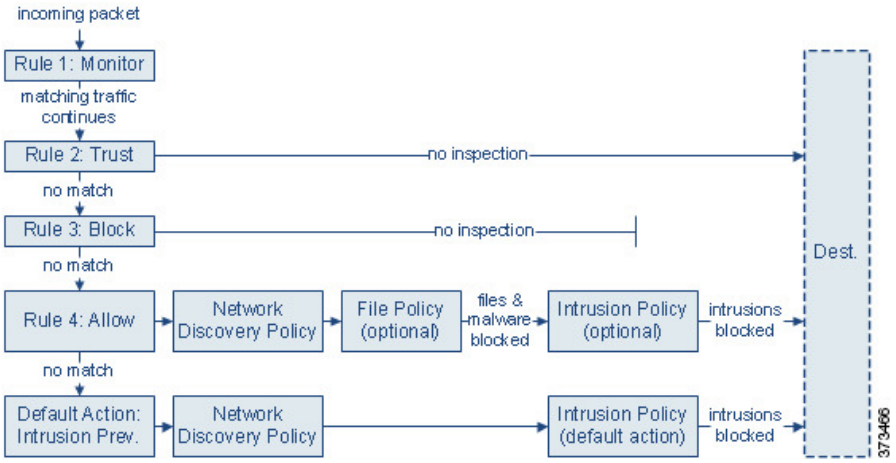
您可以使用与自己想要暂时允许通过的流量的特征相匹配的规则创建访问控制策略，然后将其与入侵策略和文件策略相关联。文件策略阻止所有可执行文件的下载，也可检测和阻止包含恶意软件的 PDF：

- 首先，系统根据文件策略中指定的简单类型匹配阻止所有可执行文件的下载。由于会立即遭到阻止，因此这些文件既无法执行恶意软件检查也无法执行入侵检查。
- 接着，系统对下载到网络主机的 PDF 执行恶意软件云查找。具有恶意软件处置情况的任何 PDF 均被阻止，且不接受入侵检查。
- 最后，系统使用与访问控制规则关联的入侵策略检测任何剩余流量，包括文件策略未阻止的文件。

注释 在会话中的文件被检测并阻止之前，该会话的数据包可能会接受入侵检查。

使用入侵和文件策略的访问控制流量处理

下图显示一个内联入侵防御和恶意软件防护 部署中的流量，它受包含四种不同类型访问控制规则和默认操作的访问控制策略监管。



在上面的情景中，策略中的前三条访问控制规则 — Monitor、Trust 和 Block — 无法检查匹配的流量。Monitor 规则跟踪和记录但不检查网络流量，因此，系统继续将流量与其他规则进行匹配以确定是允许还是拒绝该流量。（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。）Trust 和 Block 规则处理匹配流量，无需任何何类型的进一步检查，不匹配的流量继续进入下一条访问控制规则。

策略中的第四个也是最后一条规则（Allow 规则）按照以下顺序调用各种其他策略以检查和处理匹配的流量：

- **发现：网络发现策略** - 首先，网络发现策略检查流量是否存在发现数据。发现是被动分析，并不影响流量的流动。尽管不显式启用发现，但您可以增强或禁用它。但是，允许流量不会自动确保收集发现数据。系统仅对涉及网络发现策略显式监控的 IP 地址的连接进行发现。
- **恶意软件防护 和文件控制：文件策略** - 通过发现功能检查流量后，系统可以检查其是否包含禁止文件和恶意软件。恶意软件防护 将检测并选择性地阻止多种文件中的恶意软件，包括 PDF、Microsoft Office 文档等。如果贵组织不仅要阻止传输恶意软件文件，还要阻止特定类型的所有文件（无论文件是否包含恶意软件），则 *file control* 可供您监控网络流量中特定文件类型的传输，然后阻止或允许文件。
- **入侵防御：入侵策略** - 在文件检查之后，系统可以检查流量中是否存在入侵和漏洞。入侵策略根据模式检查已解码数据包中是否存在攻击，并且可以阻止或修改恶意流量。入侵策略与变量集配对，这使您能够使用指定值准确反映网络环境。
- **目标** - 通过上述所有检查的流量将传递到其目标。

“交互式阻止”(Interactive Block) 规则（未显示在图中）具有与“允许”(Allow) 规则相同的检查选项。因此，您可以在用户通过点击警告页面绕过已阻止网页时检测流量是否存在恶意内容。

在策略中不符合任何访问控制规则的流量，如果有监控以外的操作，则由默认操作来处理。在这种情况下，默认操作是入侵防御操作，只要流量由您指定的入侵策略进行传递，它就允许流量到达其最终目的地。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。请注意，系统可能检测默认操作允许的流量是否存在发现数据和入侵，而不是检测其是否存在受禁文件或恶意软件。您**无法**将文件策略与访问控制默认操作相关联。

注释 有时，当访问控制策略分析某条连接时，系统必须处理该连接中的头几个数据包，**从而让其通过**，然后才能确定哪个访问控制规则（如有）将处理流量。然而，为了让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指定一个入侵策略，以便检查这些数据包并生成入侵事件。

访问控制规则的要求和先决条件

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。

访问控制规则的准则与限制

- 当前页面一次最多可显示 1000 条规则。因此，如果您有大量规则，例如单个类别中有 3000 条规则，像选择类别中的所有规则并删除它们这样的操作不会删除所有规则。您可能需要再次选择/删除规则，以删除您要删除的所有规则。

- 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 Firewall Threat Defense，您可以通过使用 Firewall Threat Defense **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。

- 要将完全限定域名 (FQDN) 网络对象用作源或目标条件，您还必须在平台设置策略上配置适用于数据接口的 DNS。系统不使用管理 DNS 服务器设置查找访问控制规则中使用的 FQDN 对象。

  请注意，通过 FQDN 控制访问是尽力而为机制。考虑以下几点：

  - 尽可能使用安全智能或 URL 过滤，而不是 FQDN 规则。
  - 由于 DNS 回复可能具有欺骗性，因此只能使用完全受信任的 DNS 服务器。
  - 有些 FQDN，特别是非常受欢迎的服务器，可能有成百上千个 IP 地址，而且这些地址经常都会变化。由于系统使用的是缓存的 DNS 查询结果，用户可能会获得尚未在缓存中的地址，因此他们的连接将与 FQDN 规则不匹配。使用 FQDN 网络对象的规则只对解析为 100 个以内地址的名称有效。

    建议您不要为解析为超过 100 个地址的 FQDN 创建网络对象规则，因为连接中的地址是设备 DNS 缓存中已解析和可用地址的可能性很低。对于这些情况，请使用基于 URL 的规则，而不是 FQDN 网络对象规则。
  - 对于受欢迎的 FQDN，不同的 DNS 服务器可以返回一组不同的 IP 地址。因此，如果您的用户使用的 DNS 服务器与您所配置的不同，基于 FQDN 的访问控制规则可能不适用于客户端对于该站点使用的所有 IP 地址，而您的规则也不会实现预期结果。
  - 一些 FQDN DNS 条目的生存时间 (TTL) 值非常小。这会导致查询表频繁地进行重新编译，从而可能会影响总体系统性能。
  - 如果超过 8 个 FQDN 解析为同一 IP 地址，则系统无法将流量可靠地匹配到这些 FQDN 的规则。每个 IP 地址最多可以处理 8 个 FQDN。

- 每个访问控制规则的每个匹配条件的最大对象数为 200。例如，单个访问控制规则中最多可以包含 200 个网络对象。

应用控制的最佳实践

以下主题讨论我们推荐的使用访问控制规则控制应用的最佳实践。

应用控制的建议

请牢记以下应用控制的准则与限制：

确保启用自适应分析

如果未启用（默认状态）自适应分析，访问控制规则将无法执行应用控制。

自动启用应用检测器

如果没有为要检测的应用启用检测器，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，则系统会为该应用启用最新修改的用户定义检测器。

配置策略以检查在识别应用之前必须通过的数据包

在以下两种情况发生之前，系统无法执行应用控制：

- 客户端与服务器之间建立受监控连接
- 系统识别会话中的应用

此识别应在 3 到 5 个数据包内发生，或者在 SSL 握手中的服务器证书交换（如果流量已加密）后发生。如果将访问控制规则配置为使用“应用默认端口”，则无需允许初始数据包通过即可实施应用规则。

如果早期流量与所有其他条件匹配，但应用识别未完成，系统会允许传递数据包，并允许建立连接（或允许 SSL 握手完成）。在系统完成其识别后，系统会将相应的操作应用于剩余会话流量。

要确保系统检查这些初始数据包，请在访问控制策略高级设置的**确定访问控制规则之前使用的入侵策略**选项中选择入侵策略。

了解识别应用的限制

服务器必须遵守应用的协议要求，这样系统才能识别该应用。例如，如果您有一台服务器在预期 ACK 时发送保持连接数据包而不是 ACK，则可能无法识别该应用，并且连接将不会匹配基于应用的规则。相反，它将由另一个匹配的规则或默认操作进行处理。这可能意味着您想要允许的连接会被拒绝。如果遇到此问题，并且无法修复服务器以遵循协议标准，则需要编写基于非应用的规则来覆盖该服务器的流量，例如，匹配 IP 地址和端口号。

为 URL 和应用过滤创建单独的规则

尽可能为 URL 和应用过滤创建单独的规则，因为组合应用和 URL 标准可能会导致非预期的结果，特别是对于加密的流量。

包括应用和 URL 标准的规则应位于仅应用或仅 URL 规则前，除非应用+URL 规则作为更一般仅应用或仅 URL 规则的例外。

将 URL 规则置于应用规则和其他规则之前

为了实现最有效的 URL 匹配，请将包括 URL 条件的规则放在其他规则前面，如果 URL 规则是组织规则，并且其他规则同时满足以下两个条件，则尤其应该如此：

- 它们包括应用条件。
- 将对要检查的流量进行加密。

处理无负载的应用流量数据包

在执行访问控制时，对于在用于识别出应用的连接中没有负载的数据包，系统会应用默认策略操作。

处理关联应用流量

要处理由 Web 服务器所推荐的流量（如广告流量），请匹配被推荐应用（而非推荐应用）。

控制使用多个协议的应用流量（Skype、Zoho）

某些应用使用多个协议。要控制其流量，请确保访问控制策略能够涵盖所有相关选项。这些应用通常在每个可控制的环节中都包含应用名称。另请参阅特定于应用的说明和限制，第 16 页。

控制规避应用流量

请参阅特定于应用的说明和限制，第 16 页。

在应用匹配和端口匹配之间进行选择

在传统防火墙中，可以基于 OSI 第 3 层（协议）和第 4 层（传输层）（如 IP 或 TCP/80）匹配流量。然后，根据该规则的操作，允许或阻止给定端口（或整个协议）上的所有流量。

应用条件则对应 OSI 第 7 层。不同的应用可以使用同一个 TCP/UDP 端口。通过使用应用条件，您可以有选择地允许或阻止同一端口上的不同应用，而无需允许或阻止该端口上的所有应用。

在规则中使用基于端口的条件还是基于应用的条件，都会影响规则的性能。由于可以快速识别数据包中的 TCP/UDP 端口，系统可以在第一个数据包上匹配到正确的规则。使用应用层条件时，可能需要 3-5 个数据包才能识别特定应用（如果未同时指定端口）。

请考虑以下建议。

- 如果要对指定的接口和网络，以相同方式处理给定 TCP/UDP 端口上的所有流量，请使用基于端口的匹配。例如，要以相同方式处理所有 SSH 流量，请在“端口”选项卡上选择 SSH 端口 (TCP/22)。
- 如果要严格匹配与其他应用使用相同端口的特定应用，请在“应用”选项卡上选择该应用。这就是处理所有使用 TCP/80 或 443 端口的 Web 应用的方式，以便可以选择性地阻止或允许某些 Web 应用，而不影响所有 Web 应用。
- 如果要按用户组控制应用的使用，请在“用户”选项卡上选择用户组，然后在“应用”选项卡上选择应用。例如，您可以阻止承包商用户组成员使用游戏类应用。

  如果规则应适用于某一协议/端口的所有连接，也可以按用户组允许或阻止该协议/端口。
- 对于从不太安全的网络（如互联网）通往安全性较高的网络（如受保护的内部网络）的规则，请尽可能使用“端口”选项卡。例如，您可以允许或阻止从互联网到内部网络的 ICMP 流量。
- 避免在单个规则中同时指定“端口”选项卡和“应用”选项卡的参数。相反，选择某个应用时，应将“端口”选项卡留空，并在“应用”选项卡上将端口指定为**应用默认**端口。这样可将规则确定为正确的端口（每个应用），并加快将正确的应用与规则进行匹配的速度。

- 如果混合使用了基于端口和基于应用的规则，请将基于端口的规则在规则列表中靠前排列，以便首先将连接与这些规则进行匹配。识别协议和端口比识别应用更快。

特定于应用的说明和限制

- Office 365 管理门户 - 如果访问策略在连接开始和结束时均启用了日志记录，第一个数据包将被检测为 Office 365，而连接结束时将被检测为 Office 365 管理门户。这应当不会影响拦截。
- Skype - 要控制 Skype 流量，请从**应用过滤器**列表中选择 **Skype** 标记（而不是选择个别应用）。这确保系统可以相同方式检测和控制所有 Skype 流量。
- 为了完全检测 GoToMeeting，您的规则必须包含以下所有应用：
  - GoToMeeting
  - Citrix Online
  - Citrix GoToMeeting 平台
  - LogMeIn
  - STUN
- Zoho - 要控制 Zoho 邮箱，请从“可用应用”列表中同时选择 **Zoho** 和 **Zoho 邮箱**。
- 对于规避类应用（如 Bittorrent、Tor、Psiphon 和 Ultrasurf），默认仅检测置信度最高的场景。如果需要对此流量（例如阻止或实施 QoS）采取措施，则可能需要配置效率更高、更为积极的检测。若要如此，请联系 TAC 审查您的配置，因为这些更改可能会导致误报。
- 如果您允许微信，则无法选择性地阻止微信媒体。
- 如果允许 RDP 应用但不允许文件传输，请确保 RDP 规则同时包含 TCP 和 UDP 端口 3389。RDP 文件传输会使用 UDP。

访问控制规则的最佳实践

正确配置和排序访问控制规则对于保护网络至关重要。以下主题总结了可最大限度提高规则性能和有效性的最佳实践。

注释 当部署配置更改时，系统会将所有规则共同进行评估，并创建分配的设备用于评估网络流量的扩展条件集。如果这些条件超过设备的资源（物理内存、处理器等），则您无法部署到该设备。

访问控制最佳实践

查看以下要求和一般最佳实践：

- 使用预过滤器策略为不需要的流量提供早期阻止，并为未受益于访问控制检查的流量提供快速路径。有关详细信息，请参阅快速路径预过滤器的最佳实践。
- 虽然无需为部署提供许可也可配置系统，但许多功能要求您在部署之前，先启用适当的许可证。
- 访问控制规则在设备上部署为访问控制列表 (ACL)。为了最大限度地减少每个访问控制规则创建的访问控制条目数量，并提高整体性能，请为每台设备启用对象组搜索。对象组搜索是设备设置，而不是访问控制策略设置，因此您必须编辑每台设备以确保已启用该功能。有关详细信息，请参阅配置对象组搜索。
- 在部署访问控制策略时，其规则不会应用于现有连接。现有连接上的流量不受部署的新策略的限制。此外，仅对匹配策略的连接的第一个数据包增加策略命中计数。因此，从命中计数中忽略了可能与策略匹配的现有连接上的流量。要有效应用策略规则，请清除现有连接会话，然后部署策略。
- 尽可能将多个网络对象合并为一个对象组。当您选择多个对象（分别用于源或目标）时，系统会自动创建对象组（在部署期间）。选择现有组可以避免对象组重复，并减少存在大量重复对象时对 CPU 使用率的潜在影响。
- 为让系统影响流量，必须使用路由接口、交换接口或透明接口或者内联接口对向托管设备部署相关配置。

  有时，系统会阻止您将内联配置部署到被动部署的设备，包括分流模式下的内联设备。

  在其他情况下，策略可成功部署，但尝试使用被动部署的设备阻止或修改流量可能会出现意外结果。例如，由于受阻连接在被动部署中未被阻止，因此系统可为每个受阻连接报告多个连接开始事件。
- 某些功能（包括URL过滤、应用检测和速率限制）必须允许一些数据包通过，以便系统能够识别流量。
- 某些功能仅在特定设备型号上可用。警告图标和确认对话框会指出不支持的功能。
- 如果您要使用 syslog 或在外部存储事件，请避免在对象名称（例如策略和规则名称）中使用特殊字符。对象名称不应包含特殊字符（例如逗号），接收名称的应用可能将其用作分隔符。
- 访问控制规则的最佳实践，第 16 页和子主题中详细介绍了创建、排序和实施访问控制规则的最佳实践。

规则排序的最佳实践

一般准则：

- 一般，将必须应用于所有流量的最优先规则靠近策略的顶部放置。
- 特定规则应在一般规则之前，特别当特定规则是一般规则的例外时。

  否则，流量将首先匹配一般规则，而不会命中适用的特定规则。
- 仅基于第 3/4 层条件丢弃流量的规则（如 IP 地址、安全区和端口号）应尽早出现。基于这些条件的规则不需要通过检测来识别匹配的连接。

- 尽可能将特定丢弃规则置于策略顶部附近。这确保了对非预期流量尽可能做出最早的决定。
- URL 过滤、基于应用和基于地理位置的规则以及其他需要检查的规则应位于仅根据第 3/4 层条件（例如 IP 地址、安全区域和端口号）丢弃流量的规则之后，但在规则之前指定文件和入侵策略。
- 为了实现最有效的 URL 匹配，请将包括 URL 条件的规则放在其他规则前面，如果 URL 规则是组织规则，并且其他规则同时满足以下两个条件，则尤其应该如此：
  - 它们包括应用条件。
  - 将对要检查的流量进行加密。
- 将 URL 过滤规则置于应用规则之上，并在应用规则之后加上微应用规则和通用工业协议 (CIP) 子分类应用过滤规则。
- 通常，包含应用条件的规则应位于访问控制列表的较下方，例如，与基于 IP 地址的规则相比，这些规则的匹配耗时更长。有关详细信息，请参阅在应用匹配和端口匹配之间进行选择，第 15 页和应用控制的建议，第 13 页。
- 指定文件策略和入侵策略的规则应位于规则顺序的底部。这些规则需要资源密集型深度检查，并且出于性能原因，您应首先使用强度较低的方法消除尽可能多的威胁，以便最大限度地减少需要深度检查的潜在威胁的数量。
- 始终应根据您的组织的需求对规则进行排序。

以下各节说明了上述准则的例外情况和补充内容。

应用程序规则顺序

通常，包含应用条件的规则应位于访问控制列表的较下方，例如，与基于 IP 地址的规则相比，这些规则的匹配耗时更长。

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。

有关详细信息，请参阅在应用匹配和端口匹配之间进行选择，第 15 页和应用控制的建议，第 13 页。

规则抢占

当一条规则由于评估中排序靠前的规则首先匹配流量而永远无法匹配流量时，会出现规则抢占问题。规则的条件控制其是否会抢占其他规则。在以下示例中，第二条规则无法阻止管理员流量，因为第一条规则会允许该流量：

访问控制规则 1：允许管理员用户
访问控制规则 2：阻止管理员用户

任何类型的规则条件均可以取代后续规则。第一条规则中的VLAN范围包含第二条规则中的VLAN，因此第一条规则抢占了第二条规则。要阻止 VLAN 27，您必须将该规则移到允许 VLAN 22-33 的规则上方。

访问控制规则 1：允许源网络 VLAN 22-33
访问控制规则 2：阻止源网络 VLAN 27

在以下示例中，规则 1 匹配所有 VLAN，因为没有配置 VLAN，因此规则 1 会取代尝试匹配 VLAN 2 的规则 2：

访问控制规则 1：允许源网络 10.4.0.0/16
访问控制规则 2：允许源网络 10.4.0.0/16，VLAN 2

规则还会抢占所有已配置条件均相同的相同后续规则：

访问控制规则 1：允许源网络 10.10.10.0/24 到 URL www.netflix.com
访问控制规则 2：允许源网络 10.10.10.0/24 到 URL www.netflix.com

如有任何条件不同，则后续规则不会被抢占：

访问控制规则 1：允许源网络 10.10.10.0/24 到 URL www.netflix.com
访问控制规则 2：允许源网络 10.10.11.0/24 到 URL www.netflix.com

规则操作和规则顺序

规则操作确定系统如何处理匹配的流量。通过将不执行也不确保进一步流量处理的规则置于会执行并确保进一步流量处理的资源密集型规则之前来提高性能。然后，系统可以转移可能已另外检查的流量。

以下示例显示在规则集中无任何规则更重要且抢占不是问题的情况下，可能如何在各种策略中对规则进行排序。

如果您的规则包括应用条件，另请参阅在应用匹配和端口匹配之间进行选择，第 15 页。

访问控制规则的最佳顺序

入侵、文件和恶意软件检测需要资源，尤其是您使用多个自定义入侵策略和变量集时情况更加如此。请将调用深度检查的访问控制规则放在最后。

1. 监控 - 记录匹配连接但不对流量采取任何其他操作的规则。（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。）
2. 信任、阻止、阻止并重置 - 处理流量而不进一步检测的规则。
3. 允许，交互式阻止（无深度检查）- 不进一步检测流量，但是允许发现的规则。
4. 允许，交互式阻止（深度检查）- 与对禁止的文件、恶意软件和漏洞执行深度检查的文件或入侵策略关联的规则。

简化和集中规则的最佳实践

简化：不要过度配置

最小化单个规则条件。在规则条件中使用尽可能少的单独元素。例如，在网络条件中，使用 IP 地址块，而不是单独的 IP 地址。

如果一个条件足以匹配您想要处理的流量，请不要使用两个条件。使用冗余条件可能会大大扩展已部署的配置，这可能会导致设备性能问题以及集群和高可用性设备重新加入中的意外设备行为。例如：

- 请谨慎使用代表多个接口的安全区域。如果指定源和目标网络作为条件，并且这些条件足以匹配您的目标流量，则无需指定安全区域。
- 例如，如果要将一组内部接口与互联网上的任何目的地进行匹配，则只需使用包含内部接口的源安全区域。不需要网络或目标接口标准。

将元素组合到对象中**不**会提高性能。例如，使用包含 50 个 IP 地址的网络对象，与逐一将这些 IP 地址纳入条件中相比，只能给您带来组织优势，而不是性能优势。

有关应用检测的建议，请参阅在应用匹配和端口匹配之间进行选择，第 15 页。

集中：更严格地限制资源密集型规则，尤其是按接口限制

尽可能使用规则条件以更严格定义资源密集型规则处理的流量。集中规则很重要的另一原因是，有着广泛条件的规则可能与许多不同类型的流量相匹配，并且可以抢占较为靠后、更为具体的规则。资源密集型规则的示例包括：

- 解密流量的TLS/SSL 规则 - 不仅解密，而且进一步分析已解密流量，也都需要资源。缩小集中范围，并尽可能阻止或选择不解密加密流量。

  某些 Firewall Threat Defense 模型在硬件中执行 TLS/SSL 加密和解密，这大大提高了性能。有关详细信息，请参阅TLS 加密加速。

- 调用深度检查的访问控制规则 - 入侵、文件和恶意软件检查需要资源，尤其是您使用多个自定义入侵策略和变量集时情况更是如此。确保只在必要时调用深度检查。
- 如果在规则中指定安全区域，该规则仅会部署到接口位于指定区域的设备上。因此，如果要将规则仅应用于分配给策略的某些设备，请确保选择适用于相应设备子集的安全区域。这可确保不会将不必要的规则部署到设备。

访问控制规则和入侵策略的最大数量

设备支持的访问控制规则或入侵策略的最大数量取决于许多因素，包括设备上的策略复杂度、物理内存以及处理器数量。

如果超出设备支持的最大值，您将无法部署访问控制策略，必须重新评估。

入侵策略的准则：

- 在访问控制策略中，您可以将一个入侵策略与每条“允许”(Allow) 和“交互式阻止”(Interactive Block) 规则以及默认操作相关联。每个唯一的入侵策略和变量集**对均**视为一个策略。
- 您可能希望整合入侵策略或变量集，从而能够将单个入侵策略/变量集对与多个访问控制规则相关联。在某些设备上，您可能会发现只能对所有入侵策略使用单个变量集，甚至对整个设备采用单个入侵策略-变量集对。

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**应用 (Apply)**。

步骤 5 点击**保存**保存策略。

下一步做什么

现在，您可以：

- 将规则拖放到类别中或从类别中拖出。
- 创建规则时，请选择其所属的类别。
- 编辑规则时，请将规则重新定位到类别中，或者将其移出类别。

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。

开始之前

如果已启用策略分析器和优化器工具，系统会在您进行编辑时进行评估。如果检测到异常，则在编辑期间会收到通知，并在您点击“**应用**”保存规则时提示您进行更改。您可以查看异常（例如冗余和阴影规则），并选择编辑或删除规则。您还可以继续按原样保存规则，以便稍后处理问题。

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** (✎)。
- 要从现有规则的副本开始，请从 **更多** (⋮) 菜单中选择以下命令之一。
  - **复制规则 (Copy Rule)**，将规则复制到剪贴板，以便可以使用 “**上方粘贴**”/“**下方粘贴**” 命令将其放置在同一策略中的任何位置。
  - **复制规则到其他策略** - 将该规则复制到另一个访问控制策略。系统将打开一个对话框，以便您选择目标策略并确定规则的放置位置。
  - **克隆规则**，以在复制规则的正下方创建副本。
- 要编辑多个规则，请使用复选框选择多个规则，然后从搜索框旁边的**选择操作/批量规则操作**列表中选择**编辑**或其他操作。
- 要执行内联编辑（更改规则条件中的对象配置），请右键点击该值并选择 **编辑**。您还可以使用右键点击菜单删除项目，将其添加到过滤器或复制文本或值。

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 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（新规则选择**插入**位置，现有规则使用规则名称旁的**重新定位**图标）；请参阅访问控制规则顺序，第 5 页。
- **操作**：选择规则**操作**；请参阅访问控制规则操作，第 6 页。
- **高级日志记录**：点击**高级日志记录**，为应用感知和协议感知事件日志选择协议。有关详细信息，请参阅关于应用 程序感知事件日志记录 *Cisco Secure Firewall Management Center* 管理指南 。

  注释
  当访问控制策略高级设置中启用了**高级日志记录**功能时，此选项可用。请参阅 启用应用感知事件日志记录，位于 *Cisco Secure Firewall Management Center* 管理指南 中。

- **日志记录**：点击**日志记录**，指定连接日志记录和 SNMP 陷阱的选项。相同的日志设置可以在默认 **操作配置 (Default Action Configuration)**配置 对话框（导航路径：编辑访问控制策略。在**“默认操作”(Default Action)** 区域中，点击 **默认日志记录和检测 (Default logging and inspection)** 图标 (**齿轮**（ ）) 。

  有关详细信息，请参阅*Cisco Secure Firewall Management Center* 管理指南 中的连接日志记录最佳实践。

  注释
  您可以集成 Splunk 或任何 SIEM 系统日志服务器，以直接从 防火墙管理中心 或其托管设备接收连接事件。如果您在 Splunk 配置中已将防火墙管理中心配置为连接事件源，请在**将连接事件发送至**下选择 **防火墙管理中心**。如果您已将Firewall Threat Defense配置为连接事件源，请选择至少一个目标地址。有关 Splunk 配置程序，请参阅 *Cisco Secure Firewall Management Center* 管理指南。

- **时间范围**：（可选。）对于 Firewall Threat Defense 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。
- **启用规则**：规则是否处于活动状态。禁用的规则不会应用于连接。您可以禁用规则以暂时将其关闭（例如，在故障排除期间）。
- **安全保护**（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。
- 条件：选择要添加到源或目标的对象，然后点击**添加到源**或**添加到目标**以添加匹配的连接条件。您可以点击选项卡将可用对象列表限制为“网络”、“安全区域”、“应用”等。但是，无论您在哪个选项卡上，源和目标列始终显示所有选定的对象。有关详细信息，请参阅访问控制规则条件，第 24 页。
- **注释**：打开对话框底部的注释列表，输入您的注释，然后点击**添加注释/发布**以添加注释。

步骤 4 点击**添加 (Add)** 或**应用 (Apply)** 保存规则。点击**应用并添加新规则 (Apply and Add New Rule)** 让对话框保持打开，以便创建新规则。

步骤 5 点击**保存** 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。请参阅时区。

部署配置更改；请参阅 部署配置更改。

相关主题

访问控制规则的最佳实践 ，第 16 页

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：

- 尽可能将匹配条件减少，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。

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。

  尽可能将多个网络对象合并为一个对象组。当您选择多个对象（分别用于源或目标）时，系统会自动创建对象组（在部署期间）。选择现有组可以避免对象组重复，并减少存在大量重复对象时对 CPU 使用率的潜在影响。

  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。然而，访问控制策略中的以下部分不支持 FQDN 对象：原始客户端网络、SGT/ISE 属性、网络分析和入侵策略、安全智能、威胁检测、大象流设置。

- **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Firewall Threat Defense -不支持 Q-in-Q （仅支持一个 VLAN 标记）。
- 所有其他型号上的Firewall Threat Defense ：
  - 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。

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。

用户规则条件

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。

您只能为 Microsoft Active Directory 领域中的用户配置用户规则条件。

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。

（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。

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	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`。

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

- 必须在访问控制策略的高级设置中启用自适应分析（其默认状态），访问控制规则才能执行应用程序控制。

过程

步骤 1 在访问策略规则编辑器中，点击**应用程序**。

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**( ) 以显示摘要信息和互联网搜索链接。**锁**图标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**添加应用 (Add Application)** 或**添加到规则 (Add to Rule)**，或进行拖放操作。

提示
在添加更多过滤器和应用之前，点击**清除过滤器/选择**以清除当前选择。

步骤 4 如果在“端口”选项卡上未指定目标端口，请为应用选择**端口**。

端口规格适用于列表中的所有应用；不适用于任何过滤器。无法为每个应用指定不同的“端口”选项。如果您已在“端口”选项卡上指定了目标端口，则该选择会反映在应用列表中，且无法进行以下选择。

如果尚未为规则指定目标端口，请选择以下选项之一：

- **应用默认** - 系统仅在评估流量以匹配应用时查看默认端口。点击信息按钮 (i)，查看每个应用的默认端口。

编辑规则时，如果规则已包含源端口，且您添加了具有不兼容端口的应用并选择“应用默认端口”，系统会发出警告。如果选择使用应用默认端口，不兼容的源端口会被删除。

- **任意** - 系统不根据连接中使用的端口来限制应用标识。如果“端口”选项卡上指定了源端口，则可能需要选择此选项才能保存规则。

无论选择哪个选项，如果后续在“端口”选项卡上配置了任何目标值，则“端口”选项卡上指定的端口会覆盖此处的选择，并将应用端口更改为“任意”。如果要将规则限制为非应用默认端口的一个、多个或一个范围的端口，请使用“端口”选项卡。

此选项不适用于自定义检测器。

注释
如果访问控制策略分配给运行 7.x 版本的设备，且规则中包含具有不同默认端口的应用，则规则的处理方式会有所不同。当您选择仅将规则应用于默认端口时，对于 7.7 系统，该规则会拆分为单独的规则，每个应用对应一条规则。对于运行 7.3-7.6 版本的系统，规则仍为单条规则，但“端口”页面会更新为每个默认端口。如果您管理的设备运行较低版本的软件，且希望使用默认端口匹配，建议将每条规则中的应用列表限制为具有相同默认端口的应用。

步骤 5 保存或继续编辑规则或配置。

下一步做什么

- 部署配置更改；请参阅 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。

尽可能将匹配条件减少，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 标记。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 Firewall Threat Defense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。
- 解密 规则 - SSL 规则仅支持 TCP 端口条件。
- IMCP 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，请参阅关于使用类别和信誉进行 URL 过滤。

动态属性规则条件

动态属性包括：

- （源或目标。）动态对象（例如来自 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 Secure Firewall Management Center 以便将它们用于访问控制规则中。

  有关dynamic attributes connector的详细信息，请参阅《关于 dynamic attributes connector》。

- （仅源。）安全组标记 (SGT) 对象，包含手动定义或通过 ISE 定义的标记。有关更多信息，请参阅《源和目标安全组标记 (SGT) 匹配》和《安全组标记》。
- （仅源。）位置 IP 对象 由Cisco ISE定义
- （仅源。）设备类型对象，由（也称为终端配置文件）Cisco ISE定义。

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。例如，如果同时选择安全组标记和列出 IP 地址的动态对象，如果带有 标记的流量源自（或发往）其中一个 IP 地址，则该规则匹配。

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 Firewall Threat Defense 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**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

从一项访问控制策略复制访问控制规则

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。

过程

步骤 1 执行以下操作之一：

- 要复制单个规则，右键点击规则并选择**将规则复制到不同策略**。
- 要复制多个规则，选中它们的复选框，然后从**选择批量操作**菜单中选择**将规则复制到不同策略**。

步骤 2 从**访问策略 (Access Policy)** 下拉列表中选择目标访问控制策略。

步骤 3 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。您可以将它们放在“强制”或“默认”部分的顶部或 底部。

步骤 4 点击**复制 (Copy)**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

将访问控制规则移至预过滤策略

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策略 时，无法移动访问控制规则中的第 7 层 (L7) 参数（例如应用程序或 URL 过滤）。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

访问控制规则中的操作	预过滤器规则中的操作
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 阻止并重置 交互式阻止 交互式阻止并重置	• 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	• 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 执行以下操作之一：

- 要移动单个规则，请右键点击该规则并选择**将规则移至预过滤策略**。
- 要移动多个规则，请选中其复选框，然后从**选择批量操作**菜单中选择**将规则移至预过滤策略**。

步骤 2 从**放置规则**下拉列表中，选择要放置移动规则的位置（**位于底部**或**位于顶部**）：

步骤 3 点击 **移动**。

下一步做什么

- 部署配置更改；请参阅 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。

开始之前

查看访问控制规则的最佳实践，第 16 页中的规则顺序准则。

过程

步骤 1 执行以下操作之一：

- 新规则 - 将鼠标悬停在现有规则之间的行上，然后点击**添加规则**即可插入新规则。在“添加规则”对话框的**插入**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)**。
- 查看规则表时的现有规则 - 点击规则并将其拖动到新位置。此操作是最终的，系统不会提示您进行确认。
- 查看规则表时的现有规则 - 右键点击单个规则，然后选择**重新定位规则 (Reposition Rule)**。要将多个规则作为一个组移动，请选中其复选框，然后从**选择批量操作 (Select Bulk Action)** 菜单中选择**重新定位规则 (Reposition Rules)**。系统会提示您选择规则的目标位置。
- 编辑规则时的现有规则 - 点击规则名称旁边的**重新定位规则 (Reposition Rule)** 图标。

步骤 2 编辑或重新定位规则时，选择要移动或插入规则的位置，然后点击**移动**、**确认**或**重新定位**（具体取决于您在执行的操作）。

- 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**，然后选择规则。

步骤 3 如果正在编辑规则，请保存该规则。

步骤 4 点击**保存** 保存策略。

下一步做什么

- 部署配置更改；请参阅 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 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 3 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对分配到这些区域，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。

如何控制应用的使用

Web 已成为企业交付应用（无论是基于浏览器的应用平台，还是使用 Web 协议传入和传出企业网络的富媒体应用）普遍使用的平台。

Firewall Threat Defense通过检查连接确定使用的应用。这样即可写入针对应用的访问控制规则，而不只是针对特定的 TCP/UDP 端口。因此，即使使用相同的端口，也可以选择性地阻止或允许基于 Web 的应用。

虽然可以选择要允许或阻止的特定应用，但也可以基于类型、类别、标记、风险或业务相关性写入规则。例如，您可以创建一条访问控制规则，用于识别并阻止所有业务相关性较低的高风险应用。如果用户尝试使用这些应用中的任何一个，系统会阻止会话。

思科会通过系统和漏洞数据库 (VDB) 更新频繁更改并添加其他应用检测器。因此，阻止高风险应用的规则可自动应用到新应用中，而无需您手动更新规则。

在此使用案例中，我们将阻止属于**匿名程序/代理**类别的任何应用。

过程

步骤 1 选择**策略** > **安全策略** > **访问控制**，然后编辑访问控制策略。

步骤 2 点击**添加规则**并配置应用控制规则。

a) 为该规则指定一个有意义的名称，例如 Block_Anonymizers。

b) 对于**操作 (Action)**，选择**阻止 (Block)**。

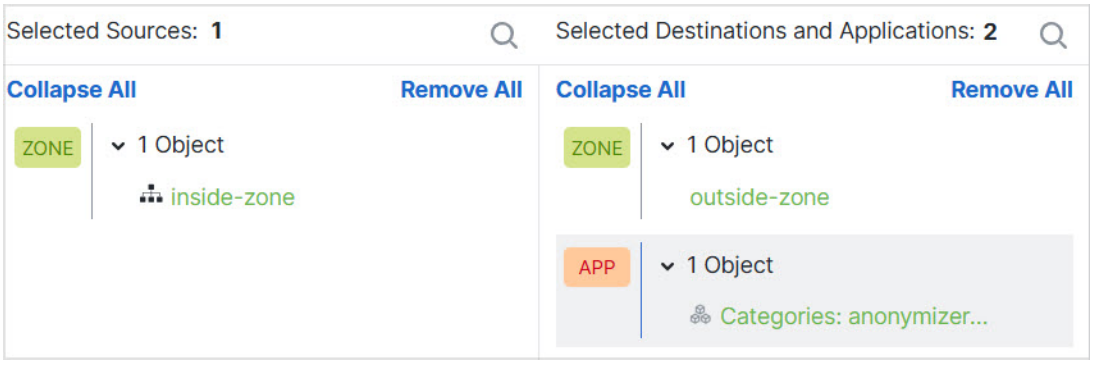
c) 假设您已配置区域，并希望将此规则应用于从内部到外部的流量，请选择**区域 (Zones)** 选项卡，然后选择内部区域作为源区域，选择外部区域作为目标区域。

d) 点击**应用 (Applications)** 选项卡，选择要匹配的应用，然后点击**添加应用 (Add Application)**。

在选择条件（例如类别和风险级别）时，条件右侧的列表会更新，从而准确显示哪些应用与条件匹配。您要编写的规则将应用到这些应用中。

仔细查看此列表。例如，您可能会希望阻止风险极高的所有应用。但是，截至本文撰写之时，TFPT 被归为风险极高类别。而大多数组织不想阻止该应用。请花些时间测试各种过滤条件，以查看哪些应用符合您的选择。请注意，这些列表可能随着每次 VDB 更新而变化。

在本例中，从“类别”(Categories) 列表中选择匿名程序/代理，并将其添加到“目标和应用”(Destinations and Applications)。匹配条件现在应如下图所示。



注释

对于**端口**，保留默认值应用默认值。这样可确保系统仅查看用于所选应用的默认端口，而不是所有端口。

e) 点击规则操作旁边的**日志记录 (Logging)**，并在连接开始时启用日志记录。如果您使用系统日志服务器，则可以选择一个。

您必须启用日志记录选项卡才能获取与此规则阻止的任何连接相关的信息。

步骤 3 移动规则，使其位于任何仅使用协议和端口条件的规则后面，但不允许应由应用规则阻止的流量。

匹配应用需要进行 Snort 检查。由于仅使用协议和端口的规则不需要 Snort 检查，因此可以将这些简单规则尽可能地分组到访问控制策略的顶部，从而提高系统性能。

步骤 4 部署更改。

您可以使用应用规则命中计数和分析控制面板来查看此规则的执行情况，以及用户尝试这些应用的频率。

如何阻止威胁

通过将入侵策略添加到访问控制规则中，可以实施下一代入侵防御系统 (IPS) 过滤。入侵策略可分析网络流量，根据已知威胁比较流量内容。如果某个连接与您正在监控的威胁匹配，系统将丢弃该连接，从而阻止攻击。

处理所有其他流量后，才会检验网络流量中是否存在入侵。通过将入侵策略与访问控制规则相关联，您是在告诉系统：在其传递符合访问控制规则条件的流量之前，您首先想要使用入侵策略检测流量。

您只能对**允许**流量的规则配置入侵策略。对于设置为**信任**或**阻止**流量的规则，系统不会执行检测。此外，如果不想使用简单阻止，您可以将入侵策略配置为默认操作。

除了检查允许的流量是否存在潜在入侵之外，您还可以使用安全智能策略来预先阻止所有传送至或来自已知不良 IP 地址，或传送至已知不良 URL 的流量。

此示例添加了一个允许内部 192.168.1.0/24 网络进入外部的入侵策略，并且假设您已经具有阻止规则来选择性地消除不需要的连接，同时还添加了一个安全智能策略来执行预先阻止。

开始之前

您必须将 IPS 许可证应用于使用此规则的任何托管设备。

此示例假定您已经为内部和外部接口创建了安全区域，并且为内部网络创建了网络对象。

过程

步骤 1 创建应用入侵策略的访问控制规则。

a) 在编辑访问控制策略师，点击**添加规则**。

b) 为规则指定一个有意义的名称（例如 Inside_Outside），并确保规则操作为**允许 (Allow)**。

c) 对于**入侵策略 (Intrusion Policy)**，选择“平衡安全和连接”(Balanced Security and Connectivity)。您可以接受默认变量集，也可以选择自己的变量集（如果要对其进行自定义）。

对于大多数网络，合适的策略是**平衡安全和连接**策略。它提供良好的入侵防御，而不会过度激进，有可能会丢弃可能不想被丢弃的流量。如果您确定要丢弃很多流量，可以选择**连接优先于安全**以放宽策略。

如果您需要积极关注安全性，请尝试**安全优先于连接**策略。**最大检测**策略更加重视网络基础设施的安全性，有可能对操作造成更大的影响。

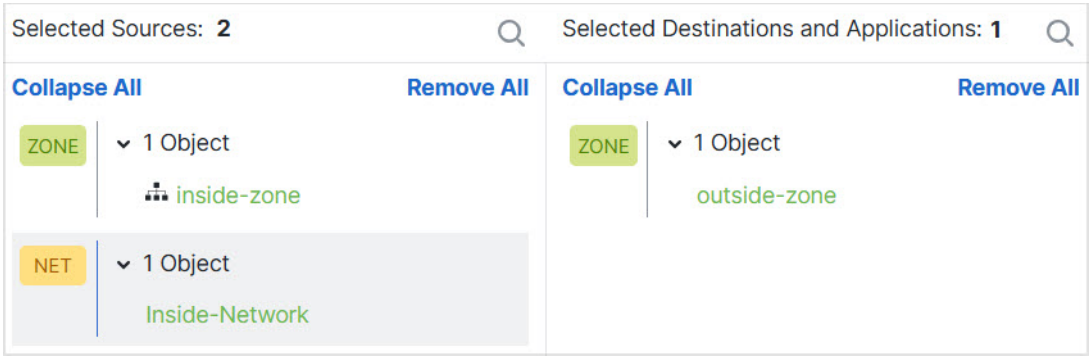
如果您要创建自己的自定义策略，则可以改为选择该策略。

对变量集的讨论不在本示例的范围之内。有关变量集和自定义策略的详细信息，请阅读入侵策略章节。

d) 选择**区域 (Zones)** 选项卡，将内部安全区域添加到源条件，将外部区域添加到目标条件。

e) 选择**网络 (Networks)** 选项卡，并将定义内部网络的网络对象添加到源条件。

匹配条件应如下所示：



f) 点击**日志记录 (Logging)** 并根据需要在连接开始或结束时启用日志记录。

g) 点击**应用**保存规则，然后点击**保存**保存更新后的策略。

h) 将规则移至访问控制策略中的适当位置。

步骤 2 配置安全智能策略预先丢弃主机和站点已知不良的连接。

通过使用安全智能阻止连接属于已知威胁的主机或站点，为系统节省执行深度数据包检测，以识别每个连接中的威胁所需的时间。安全智能可提早阻止不必要的流量，为系统留出更多的时间来处理您真正关心的流量。

a) 在编辑访问控制策略时，点击数据包路径中的**安全智能 (Security Intelligence)** 链接。

该链接包括两个策略：顶部的 DNS 策略以及底部的安全智能（网络和 URL）。在本例中，我们将配置网络和 URL 列表。默认情况下，这些列表已包含全局阻止列表和不阻止列表，但在向其添加项目之前，这些列表都默认为空。

b) 选择**网络**并选择**任意**安全区域，在网络列表中向下滚动，直到您到达全局源和第一个安全智能类别（可能是攻击者）。点击“攻击者”(Attackers)，然后滚动到类别的末尾（可能是 Tor_exit_node），然后按住 Shift 键并点击以选择所有类别。点击**添加到阻止列表 (Add To Block List)**。

c) 选择 **URL** 选项卡和**任何**安全区域，然后使用 Shift +点击来选择相同类别的 URL 版本。点击**添加到阻止列表 (Add To Block List)**。

d) 点击**保存**保存策略。

e) 如有必要，您可以将网络和 URL 对象添加到阻止或不阻止列表。

不阻止列表不是真正的“允许”列表。它们是例外列表。如果例外列表中的地址或 URL 也出现在阻止列表中，系统允许该地址或 URL 的连接传递到访问控制策略。

通过这种方式，您可以阻止源，但如果您后期发现所需的地址或站点被阻止，可以使用例外列表来覆盖阻止，而不需要彻底删除源。

注意，这些连接随后由访问控制和入侵策略（如果已配置）评估。因此，如果任何连接包含威胁，这些连接将在入侵检查过程中被识别和阻止。

使用事件和控制面板来判断哪些流量实际上被策略丢弃，以及您是否需要在**不阻止**列表中添加地址或 URL。

步骤 3 部署更改。

访问控制规则的历史记录

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
基于应用的访问控制规则的默认端口规范。	10.0	10.0	向访问控制规则添加应用时，可以指定规则限于应用的默认端口。这与在“端口”选项卡上手动指定端口不同。也可以指定应用在任何端口上被识别，这是此增强功能之前系统的行为。 如果指定默认端口并且还在“端口”选项卡上进行指定，则“端口”选项卡会覆盖应用默认端口。您可以使用端口选项卡将规则限制为一个、多个或一系列端口。 升级后，现有的基于应用的规则继续应用于任何端口。如果要将这些规则限制为默认端口，必须编辑规则，清除“端口”选项卡上的所有规范，在“应用”选项卡上选择“应用默认端口”，然后保存规则。编辑所有要更改的规则后部署更改。 向访问控制规则添加应用时，添加了选择“应用默认”或“任何”端口的功能，只要“端口”选项卡上未配置任何内容。此选项不适用于任何类型的应用过滤器，也不适用于除访问控制规则之外的任何其他策略或对象。

功能	防火墙管理中心最低版本	Firewall Threat Defense最低版本	详细信息
每个访问控制规则的每个匹配条件的最大对象数为 200。	7.3	任意	以前，单个访问控制规则中的每个匹配条件最多可以有 50 个对象。例如，单个访问控制规则中最多可以包含 50 个网络对象。现在，单个规则中的每个匹配条件的限制为 200 个对象。 我们更新了访问控制策略，以便允许添加对象限制。
搜索访问控制规则注释	6.7	任意	**搜索规则 (Search Rules)** 栏现在提供搜索注释的选项。 新增/修改的页面：访问控制规则页面、**搜索规则**文本输入字段。 支持的平台： 防火墙管理中心
在访问控制策略和预过滤器策略之间复制或移动规则。	6.7	任意	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。您还可以将访问控制规则从访问控制策略移至关联的预过滤器策略。 新增/修改的页面：访问控制策略页面；所选规则的右键点击菜单提供了用于复制和移动的其他选项。 支持的平台： 防火墙管理中心
批量编辑访问控制规则中的某些设置	6.6	任意	在策略中的规则列表中，按住 Shift 点击或按住 Control 点击可以选择多个规则，然后右键点击并选择一个选项。批量操作示例：您可以启用或禁用规则，选择规则操作，以及编辑大多数检测和日志记录设置。 新增/修改的页面：访问控制规则页面。 支持的平台： 防火墙管理中心
增强了对已配置规则的搜索	6.6	任意	增强了对已配置规则的搜索。 新增/修改的页面：访问控制规则页面。 支持的平台： 防火墙管理中心
规则应用的时间范围	6.6	任意	可以为要应用的规则指定绝对时间或循环时间或时间范围。规则会根据处理流量的设备的时区来应用。 新增/经修改的页面： • 访问控制“添加规则”(Add Rule) 页面上的新选项。 • **设备** > **平台设置** > **威胁防御**页面上的一个相关新选项，用于为托管设备指定时区。 支持的平台：仅限 Firewall Threat Defense 设备

功能	防火墙管理中心最低版本	**Firewall Threat Defense**最低版本	详细信息
从访问控制规则页面查看对象详细信息	pre-6.6	任意	要在规则列表中或从规则配置对话框中查看有关对象的信息，请右键点击该对象。 新/修改的页面：**策略** > **访问控制** > **访问控制**，以及**添加规则**页面。 支持的平台： 防火墙管理中心

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。