访问控制概述

访问控制简介

访问控制是一项基于策略的分层功能，可用于指定、检查和记录（非快速路径）网络流量。

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。

规则简介

各种策略类型（访问控制、SSL、身份等）中的规则对网络流量实行精细控制。系统使用第一个匹配算法按您指定的顺序根据规则评估流量。

虽然这些规则可能包含在策略之间不一致的其他配置，但它们共享许多基本特征和配置机制，包括：

- 条件：规则条件指定每个规则处理的流量。您可以为每个规则配置多个条件。流量必须匹配所有条件才能与规则匹配。
- 操作：规则的操作确定系统如何处理匹配流量。请注意，即使规则没有可供选择的**操作 (Action)**列表，该规则仍然具有关联操作。例如，自定义网络分析规则使用网络分析策略作为其“操作”。 又例如，QoS 规则没有明确的操作，因为所有 QoS 规则都执行同一操作：速率限制流量。
- 位置：规则的位置确定其评估顺序。当使用策略评估流量时，系统按您指定的顺序将流量与规则匹配。通常，系统根据第一个规则（其中所有规则的条件都与流量匹配）处理流量。（用于跟踪和记录的监控规则除外。）适当的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。
- 类别：要组织某些规则类型，您可以在每个父策略中创建自定义规则类别。
- 日志记录：对于许多规则，日志记录设置会监管系统是否以及如何记录规则处理的连接。某些规则（例如身份和网络分析规则）不包括日志记录设置，因为规则既不确定连接的最终处置情况，也不是专门设计为记录连接。 又例如，QoS 规则不包括日志记录设置；只是因为其速率受限，您便无法记录连接。
- 注释：对于某些规则类型，每次保存更改时，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。

提示 许多策略编辑器中的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。

有关详细信息，请参阅讨论您感兴趣的规则的章节（例如，访问控制规则）。

相关主题

配置应用条件和过滤器
应用控制的最佳实践，第 10 页

按设备过滤规则

有些策略编辑器允许您按受影响设备过滤您的规则视图。

系统使用规则的接口限制来确定该规则是否影响设备。如果您通过接口限制规则（安全区域或接口组条件），则该规则会影响接口所在的设备。无接口限制的规则会应用于任何接口，因此也会应用于每台设备。

QoS 规则始终受接口限制。

注释 以下程序不适用于访问控制策略。要查看适用于访问控制策略中的特定设备或设备集的规则，请点击过滤器图标并选择设备。

过程

步骤 1 在策略编辑器中，点击**规则 (Rules)**，然后点击**按设备过滤 (Filter by Device)**。
系统将会显示目标设备和设备组列表。

步骤 2 选中一个或多个复选框，以仅显示应用于这些设备或组的规则。或者，选中**全部 (All)** 复选框，以重置和显示所有的规则。

提示
将指针悬停在规则标准上方可查看其值。如果标准代表具有设备特定覆盖的对象，则系统会在您仅按该设备过滤规则列表时显示覆盖值。如果标准代表具有域特定覆盖的对象，则系统会在您按该域中的设备过滤规则列表时显示覆盖值。

步骤 3 点击**确定**。

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 *1:* 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。

图标	说明	示例
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（  ）	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的规则表中。	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：

- 不受智能应用绕行信任
- 不在安全智能阻止列表中
- 未被 SSL 检查阻止（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。

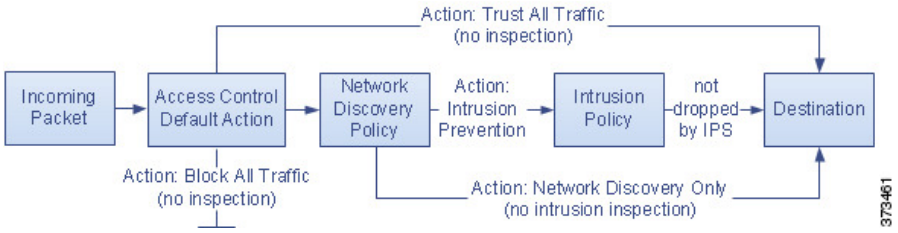
如果使用的是策略继承，则最低级别后代的默认操作会确定最终流量处理。尽管访问控制策略可从其基本策略继承其默认操作，但您无法强制执行这一继承。

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。

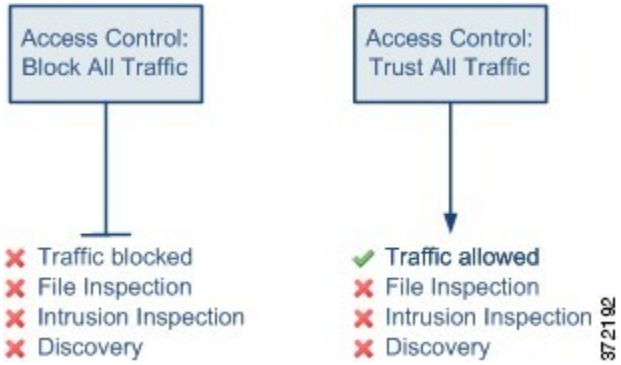
表 2: 访问控制策略默认操作

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	不进一步检查直接阻止	none
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）	none
入侵防御	允许，前提是其通过指定的入侵策略	入侵，使用指定的入侵策略和关联变量集，以及 发现，使用网络发现策略
仅网络发现	allow	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。

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。
- 文件策略监管系统的文件控制和恶意软件防护 功能。

  有关完整信息，请参阅网络恶意软件防护和文件策略。

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。

要将入侵策略和文件策略与访问控制规则相关联，请参阅：

- 用于执行入侵防御的访问控制规则配置
- 配置访问控制规则以执行恶意软件保护

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。

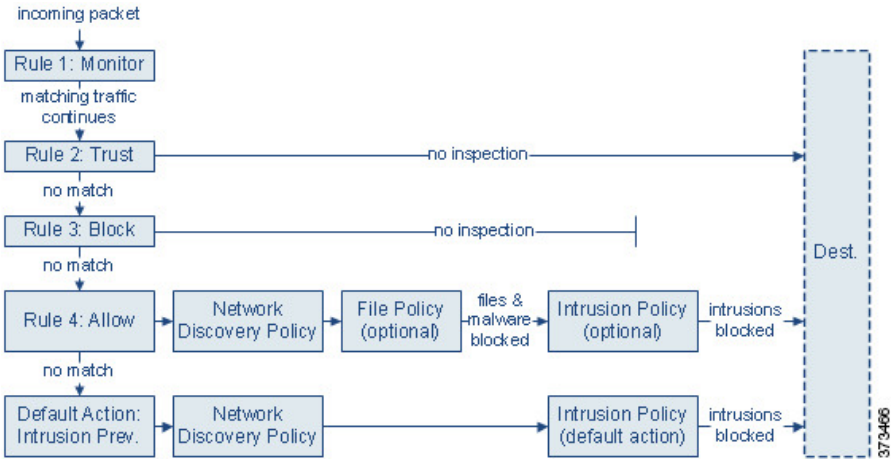
相关主题

策略如何检查流量是否存在入侵

文件策略

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。

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。

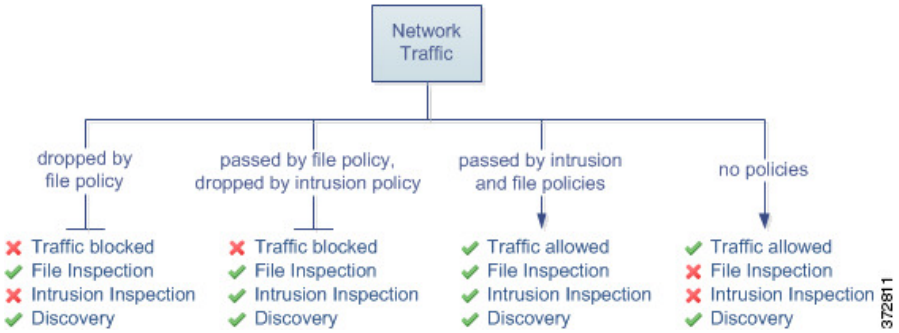
注释 可检测“入侵防御”(Intrusion Prevention) 或“仅网络发现”(Network Discovery Only) 默认操作允许的流量是否存在发现数据和入侵，但不能检测其是否存在受禁文件或恶意软件。您**无法**将文件策略与访问控制默认操作相关联。

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 文件在会话中得以检测和阻止之前，来自该会话的数据包均可能接受入侵检测。

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 Cisco 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。

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

在发生以下两种情况之前，系统无法执行应用控制，包括智能应用绕行 (IAB) 和速率限制：

- 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。

注释 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。

在应用和其他规则之前应用 URL 规则

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。

加密和解密流量的应用控制

系统可识别和过滤已加密和解密的流量：

- 加密流量 - 系统可以检测使用 StartTLS（包括 SMTP、PoP、FTP、Telnet 和 IMAP）加密的应用流量。此外，系统还可以根据 TLS ClientHello 消息中的服务器名称指示或服务器证书中的使用者专有名称值来识别某些加密应用。这些应用附以 `SSL Protocol` 标记；在 SSL 规则中，可以仅选择这些应用。只有在未加密或已解密的流量中才能检测到没有此标记的应用。
- 解密流量 - 系统还会将 `decrypted traffic` 标记分配给系统只能在解密流量中检测到（在加密或未加密流量中无法检测到）的应用。

TLS 服务器身份发现和应用控制

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。

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。

有关详细信息，请参阅访问控制策略高级设置。

将应用免于进行主动授权

在身份策略中，可以将某些应用免于主动授权，允许流量继续进行访问控制。这些应用附以 `User-Agent Exclusion` 标记。在身份规则中，仅可以选择这些应用。

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。

处理推荐应用流量

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。例如：

- 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。
- 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**。

内容限制功能支持的搜索引擎

系统仅支持特定搜索引擎的安全搜索过滤。系统将 `safesearch supported` 标记从这些搜索引擎分配给应用流量。

控制规避应用流量

请参阅特定于应用的说明和限制，第 14 页。

配置应用控制的最佳实践

我们建议如下控制应用对网络的访问：

- 要允许或阻止从安全性较低的网络到安全性较高的网络的应用访问，请执行以下操作：在访问控制规则中使用 **端口** （所选目标端口）条件

  例如，允许从互联网（不太安全）到内部网络（更安全）的 ICMP 流量。

- 要允许或阻止用户组访问应用，请执行以下操作：在访问控制规则上使用 **应用** 条件

  例如，阻止承包商组成员访问 Facebook

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。

下表提供了如何设置访问控制规则的示例：

控制类型	操作 (Action)	区域、网络、VLAN 标记	用户	应用	端口	URL	SGT/ISE 属性	检测、日志记录、注释
当应用使用端口（例如 SSH）时，应用从更安全到不太安全的网络	您的选择（在本例中为 **允许** ）	使用外部接口的目标区域或网络	任意	不设置	可用的端口： **SSH** 添加至 **选定的目标端口**	任意	仅用于 ISE/ISE-PIC。	任意
当应用不使用端口（例如，ICMP）时，应用从更安全到不安全的网络	您的选择（在本例中为 **允许** ）	使用外部接口的目标区域或网络	任意	不设置	选定的目标端口 **协议：ICMP** **类型： 任何**	不设置	仅用于 ISE/ISE-PIC。	任意
用户组的应用访问	您的选择（在本例中为 **Block** ）	您的选择	选择用户组（本例中为承包商组）	选择应用的名称（本例中为 **Facebook** ）	不设置	不设置	仅用于 ISE/ISE-PIC。	您的选择

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 3: 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。
标记	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`。

特定于应用的说明和限制

- Office 365 管理员门户：

  限制：如果访问策略在开始和结束时启用了日志记录，第一个数据包将被检测为 Office 365，而连接结束则会被检测为 Office 365 门户管理员用户。这应当不会影响拦截。

- Skype：

  请参阅 应用控制的建议，第 10 页

- GoToMeeting

  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：

请参阅 应用控制的建议，第 10 页

- 诸如 Bittorrent、Tor、Psiphon 和 Ultrasurf 的规避应用：

  对于规避应用，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。

- 微信：

  如果您允许微信，则无法选择性地阻止微信媒体。

- RDP（远程桌面协议）：

  如果允许 RDP 应用不允许进行文件传输，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

对规则正确进行配置和排序对于构建有效的部署至关重要。以下主题概述了规则性能准则。

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。

访问控制的一般最佳实践

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。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、速率限制和智能应用旁路）必须允许某些数据包通过，以便系统识别流量。
- 您不能对访问控制策略的默认操作处理的流量执行文件或恶意软件检查。
- 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。
- 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。
- 访问控制规则的最佳实践，第 15 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。

订购规则的最佳实践

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。
- 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。
- 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。

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 SSL 规则中的 VLAN 范围包含第二条规则中的 VLAN，因此第一条规则将抢占第二条规则：

规则 1：不解密 VLAN 22-33
SSL 规则 2：阻止 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：

QoS 规则1：速率限制 VLAN 1 URL www.netflix.com
QoS 规则2：速率限制 VLAN 1 URL www.netflix.com

如有任何条件不同，则后续规则不会被抢占：

QoS 规则1：速率限制 VLAN 1 URL www.netflix.com
QoS 规则2：速率限制 VLAN 2 URL www.netflix.com

示例：对 SSL 规则进行排序以避免抢占

请考虑以下场景，其中受信任 CA（好 CA ）错误地将 CA 证书颁发给恶意实体（坏 CA），但是尚未撤销该证书。您希望使用 SSL 策略来阻止使用由不受信任 CA 颁发的证书加密的流量，但是以其他方式允许受信任 CA 的信任链中的流量。在上传 CA 证书和所有中间 CA 证书后，请配置包含如下排序规则的 SSL 策略：

SSL 规则 1：阻止颁发者 CN=www.badca.com
SSL 规则 2：不解密颁发者 CN=www.goodca.com

如果恢复规则，会首先与受良好 CA 信任的所有流量相匹配，包括受不良 CA 信任的流量。由于流量不曾与后续不良 CA 规则相匹配，因此可能会允许而非阻止恶意流量。

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，另请参阅配置应用控制的最佳实践，第 12 页。

最佳顺序：解密 规则

不仅解密需要资源，进一步分析已解密的流量也同样需要资源。请将用于解密流量的规则放在最后。

注释 某些托管的设备支持对硬件中的 TLS/SSL 流量进行加密和解密，这大大提高了性能。有关详细信息，请参阅TLS 加密加速。

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。
2. 阻止、阻止并重置 - 阻止流量而不进一步检测的规则
3. 不解密 - 不解密加密流量，从而将加密会话传递到访问控制规则的规则。这些会话的负载不执行深度检查。
4. 解密 - 已知密钥 - 使用已知私钥解密传入流量的规则。
5. 解密 - 重新签名 - 通过对服务器证书重新签名来解密传出流量的规则。

最佳顺序：访问控制规则

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。请注意，受信任的流量会受到身份策略实施的身份验证要求和速率限制的制约。
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。请注意，允许的流量会受到身份策略实施的身份验证要求和速率限制的制约。
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。

应用规则顺序

如果将包含应用条件的规则移至规则列表中较低的顺序，则更有可能与流量匹配。

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。

有关详细信息和示例，请参阅配置应用控制的最佳实践，第 12 页和应用控制的建议，第 10 页。

URL 规则顺序

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。

如果为规则配置例外，请将例外置于另一条规则之上。

简化和集中规则的最佳实践

简化：不过度配置

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，请参阅配置应用控制的最佳实践，第 12 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 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。

为获得最大性能优势，请按接口限制规则。如果规则排除了某个设备的所有接口，则该规则不影响该设备的性能。

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。

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。