# 访问控制的高级设置

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。



## 高级设置的要求与前提条件

### 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。

# 为访问控制策略配置高级设置

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 中的更新入侵规则所述。

**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。

### 开始之前

**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。对于要使用父策略设置的每个设置组，选择**从（基本策略）继承**。如果您可以为该策略配置独特设置，则必须取消选择“从基本策略继承”才能进行编辑。
- 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。在这种情况下，已配置继承，因此这些设置处于锁定状态。设置为只读。

## 过程

**步骤 1** 选择**策略** > **安全策略** > **访问控制**。

**步骤 2** 创建或编辑访问控制策略。

**步骤 3** 从数据包流末尾的 **更多** 下拉箭头中选择 **高级设置** 。

**步骤 4** 对于每个设置组，点击**编辑** ( )并根据需要配置相关设置。

对于每个功能组，系统会打开一个单独的对话框，可在其中进行更改。点击**确定**以保存所有更改。

- **常规设置** - 这些设置广泛适用于该策略，包括 URL 过滤选项。有关详细信息，请参阅常规设置，第 4 页。
- **身份策略设置** - 选择用于实施用户身份发现的策略。只有实施身份策略，才能获取连接事件中的用户或用户组信息，或者才能基于用户或组编写访问控制规则。有关详细信息，请参阅关于身份策略。
- **解密策略设置** - 选择解密连接时要使用的策略。您必须解密流量才能对加密连接应用检测。
- **TLS 服务器身份识别** - 是否允许防火墙提取证书详细信息（例如通用名称 (CN)、组织或使用者备用名称 (SAN)），即使 TLS 1.3 加密通常会隐藏这些信息。这可以提高策略准确性，而无需解密规则；原始客户端连接保持加密状态。有关详细信息，请参阅TLS 服务器身份发现，第 5 页。

- **预过滤策略设置** - 选择用于静态分流大流、实施早期连接阻断或重新划分纯文本隧道流量区域的策略。
- **网络分析和入侵策略** - 高级网络分析和入侵策略设置允许您：
  - 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。
- **威胁防御服务策略** - 可以使用该服务策略将服务应用到特定流量类别。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。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信息。
- **威胁检测** - 配置端口扫描检测器，以检测和阻止所有类型流量中的端口扫描活动，保护网络免受潜在攻击。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** - 大象流是大型、长时间且高速的流量，可能会给 Snort 核心带来压力。有两种操作可应用于大象流，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%）。

  有关详细信息，请参阅配置大象流检测。
- **智能应用绕行设置** —（请使用**大象流设置**，而非此选项。）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。

  IAB 设置适用于 Snort2 设备或 7.2.0 版本之前的 Snort3 设备。有关详细信息，请参阅智能应用绕行，第 7 页。
- **传输层/网络层预处理器设置** - 高级传输层和网络层预处理器设置全局应用于所有部署了访问控制策略的网络、区域和 VLAN。有关详细信息，请参阅传输/网络层预处理器设置，第 12 页。
- **检测增强设置** - 检测增强设置确定自适应配置文件是否用于访问控制策略中的应用检测和入侵规则。通常，系统使用网络分析策略中的静态设置预处理和分析流量。通过自适应配置文件，系统可以使用由网络发现检测或从第三方导入的主机信息适应处理行为。有关详细信息，请参阅检测增强设置，第 13 页。
- **性能设置** — 关于系统分析流量以检测入侵尝试时如何提高系统性能的信息。这些设置非常高级，大多数用户应保持默认设置。请参阅性能设置，第 14 页。
- **基于延迟的性能设置**—基于延迟的性能的特定设置。这些设置非常高级，大多数用户应保持默认设置。请参阅基于延迟的性能设置，第 16 页。

- **影子流量** - 影子流量控制面板可增强源自未经批准的隐私技术的流量的可视性。此类流量专门用于规避高级防火墙的传统网络监控和分析。连接事件和统一事件中还添加了影子流量类型属性。如果您不需要查看可能包含未经批准的内容的流量，则可以禁用此选项。有关详细信息，请参阅 *Cisco Secure Firewall Management Center* 管理指南 中的影子流量构件
- **高级日志记录** - 启用此功能，以便使用应用数据丰富连接日志，并将生成的日志转发到系统日志目标。应用日志记录利用现有的深度数据包检查功能提取应用数据，使您能够加强网络监控并更深入地了解网络流量。此功能适用于 Snort 3 Firewall Threat Defense 设备。

  有关应用日志记录的详细信息，请参阅 。*Cisco Secure Firewall Management Center* 管理指南中的应用程序感知事件日志

  **注释**
  如果在访问控制规则中没有配置过滤器的情况下使用应用程序日志记录，则可能会导致网络中的性能下降。使用访问控制规则过滤特定流量类型，以减少记录的流量。

**步骤 5** 点击**保存** 以保存对访问控制策略的更改。

- 要返回规则列表，请点击数据包流程中的**访问控制**。
- 您必须部署配置，才能将更改应用到受管设备。

# 常规设置

以下是可为访问控制策略配置的常规高级设置

- **连接事件中存储的最大 URL 字符数** - 设置用户在连接结束事件中请求的每个 URL 的最大字符长度。禁用或限制存储的URL字符数可能会提升系统性能。默认值为1024。范围为0到4096。

  将长度设置为 0 可禁用 URL 日志记录。存储零字符（禁用 URL 日志记录）不会影响 URL 过滤。尽管系统不会记录流量，但会根据请求的 URL 过滤流量。

- **允许交互式阻止绕过限制（秒）** - 设置用户绕过URL过滤限制后允许浏览的时间。超时到期后，用户必须再次绕过阻止。默认值为 600 秒（10 分钟）。范围为 0 到 31536000（8760 小时）。

  将此值设置为 0 表示交互式阻止响应显示一次，并且用户绕行永远不会过期。

- **重试URL缓存未命中查询** - 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。

  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。

  此设置默认启用。系统在云中检查URL的信誉和类别时会暂时延迟流量，并根据云判定结果处理流量。

  如果禁用此设置，当系统遇到不在其本地缓存中的URL时，会根据为未分类和无信誉流量配置的规则立即放行并处理该流量。

  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** - 是否使用威胁情报导向器。禁用此选项以停止将 TID 数据发布到配置的设备。默认设置为启用。有关详细信息，请参阅如何设置威胁智能导向器。
- **启用 DNS 流量信誉实施** - 当浏览器查找域名以获取 IP 地址时，是否让系统在 URL 事务初期评估域类别和信誉。启用此选项可提高URL过滤的性能和效力。默认设置为启用。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。
- **策略应用期间检查流量** - 部署配置更改时是否检查流量（除非特定配置要求重新启动 Snort 进程）。默认设置为启用。

  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直接通过而不进一步检查而，取决于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。

# 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。

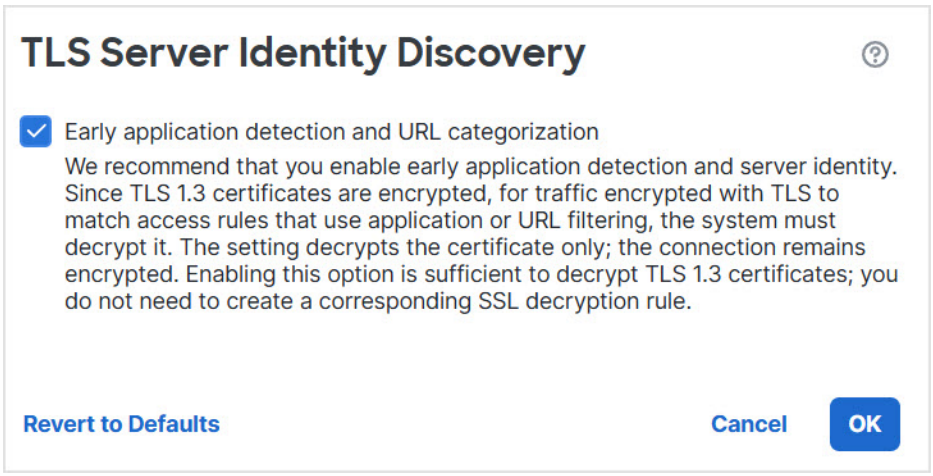
在为访问控制策略配置高级设置时，可以启用此功能，称为 *TLS* 服务器身份发现。某些功能不受支持，例如 STARTTLS 流量、HTTP CONNECT 方法，以及在已有其他设备正在解密流量的网络中。

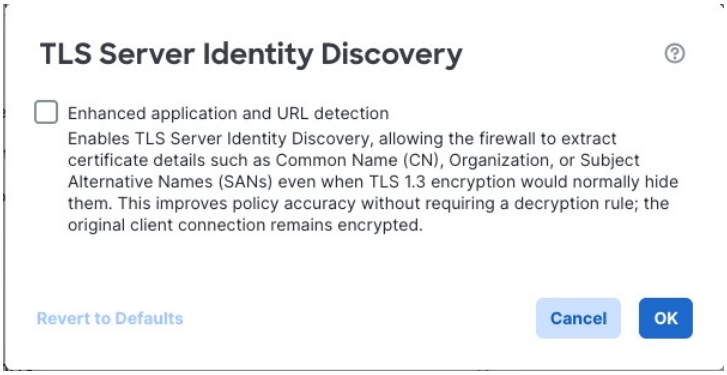
如果启用此选项，我们建议您同时启用解密策略的高级 TLS 自适应服务器身份探测选项。总之，这些选项可更有效地解密 TLS 1.3 流量。有关详细信息，请参阅TLS 1.3 解密最佳实践。

当新连接开始且受 TLS 服务器身份发现影响时，Firewall Threat Defense 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。Firewall Threat Defense 设备会从 Firewall Threat Defense 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，点击该设置旁的**编辑** (✎)，然后选择**增强应用和 URL 检测**。




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

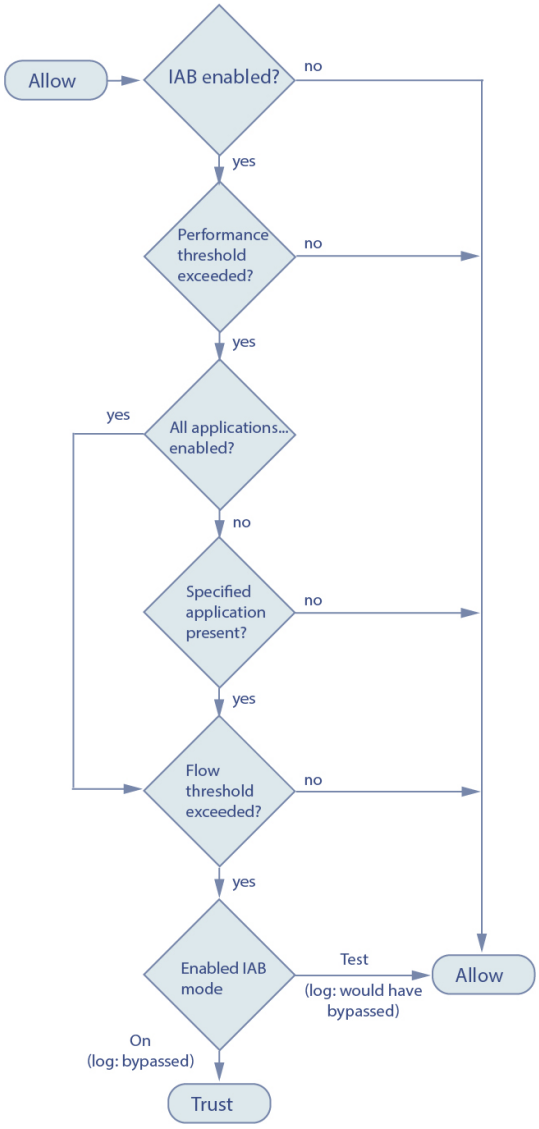
- TLS 服务器身份发现不能与以下任何一项配合使用：
  - STARTTLS 流量
  - HTTP CONNECT 方法
  - 已被网络上的其他设备解密的流量
- 由于证书是解密的，因此 TLS 服务器身份发现会降低性能，具体取决于硬件平台。
- 内联分路模式或被动模式部署不支持 TLS 服务器身份发现。
- 任何部署到 AWS 的 Secure Firewall Threat Defense Virtual 都不支持启用 TLS 服务器身份发现。如果您有任何由 Secure Firewall Management Center管理的此类托管设备，则每次设备尝试提取服务器证书时，连接事件 **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。

# 智能应用绕行

智能应用绕行 (IAB) 可识别您信任的应用，当超出性能和流量阈值时，允许其流经网络而无需进一步检测。例如，如果每次晚间的备份会显著影响系统的性能，您可以配置某些阈值，当超过这些阈值时则信任备份应用产生的流量。（可选）可以配置 IAB，使其在超出检查性能阈值时，无论应用类型如何，IAB 都信任超出任何流绕过阈值的所有流量。

在对流量进行深度检查之前，系统会对访问控制规则或访问控制策略的默认操作所允许的流量实施 IAB。您可以通过一种测试模式确定是否已超过阈值，如果已超过，则识别出在您实际启用了 IAB 的情况下会被绕过的应用数据流（称为绕行模式）。

下图展示 IAB 决策过程：



# 配置智能应用旁路

并非所有部署都需要 IAB，而那些需要 IAB 的部署也仅以有限的方式进行使用。除非您具备网络流量（特别是应用流量）和系统性能（包括可预测的性能问题的原因）方面的专业知识，否则不要启用 IAB。在绕行模式下运行 IAB 之前，请确保信任指定的流量不会使您处于风险中。

### 开始之前

IAB 设置适用于 Snort2 设备或 7.2.0 版本之前的 Snort3 设备。对于 Snort 3 设备，请改用大象流量检测。

### 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** 下拉箭头中点击**高级设置**。然后，点击**智能应用绕行设置**旁边的 **编辑** (✎)。

**步骤 2** 为 IAB 设置启用**状态**。

**关闭**或**打开** IAB，或在**测试**模式下启用 IAB。

在测试模式下，连接事件和控制面板会告诉您在 IAB 开启时系统本会执行的操作，但流量不受影响。使用测试模式检查您的配置。

**步骤 3** 设置**性能采样间隔**。

**性能采样间隔**指定两次 IAB 性能采样扫描间隔的时间（秒），系统会在此期间收集系统性能指标以与 IAB 性能阈值进行比较。默认值为 5 秒。范围为 1 到 1000 秒。

**步骤 4** 选择**可绕行应用和过滤器**。

选项包括：

- ***X*应用/过滤器** — 点击链接，选择要绕过其流量的应用或应用过滤器。您可以按常规属性、特定应用或两者进行选择。例如，可以将可绕行的流量限制为仅允许流向风险极低的应用。
- **包括未识别应用在内的所有应用** — 不要限制旁路。超过检查性能阈值时，不管应用类型为何，IAB 都信任超过任何流绕行阈值的所有流量。这是默认值。

**步骤 5** 配置性能和流阈值。

您必须至少配置一个**检测性能阈值**和一个**流量旁路阈值**。但是，所有设置都有默认值，如果默认值适合您的网络，则无需更改设置。

当超过某一性能阈值时，系统会检查流阈值，并且如果超过某一阈值，则信任指定流量。如果启用其中一项以上，则只能超过其中一项。

a) 点击**检查性能阈值**下的**配置**并配置选项。

检查性能阈值提供入侵检查性能限值，如果超过该限值，则会触发流阈值检查。检查性能阈值设置为 0 时将被忽略。

您可以配置一个或多个以下阈值：

- **丢弃百分比** — 因昂贵入侵规则、文件策略、解压等引起的性能过载导致的数据包丢弃时，丢弃的平均数据包数占总数据包数的百分比。这并不是指入侵规则等正常配置丢弃的数据包数。

  请注意，当丢弃指定百分比的数据包时，指定大于 1 的整数会激活 IAB。指定 1 时，任何从 0 到 1 的百分比都会激活 IAB。这允许少量数据包激活 IAB。

  默认值为 5%。范围为 0 到 100。

- **处理器利用率百分比** — 使用的处理器资源的平均百分比。默认值为 95。范围为 0 到 100。
- — 平均数据包延迟（微秒）。默认值为 1000。范围为 0 到 1000000。
- **流速率** — 系统处理流的速率，以每秒的流数进行测量。请注意，此选项可配置 IAB 以测量流速率，而不是流计数。默认值为 0。范围为 0 到 1000000。

b) 点击**流绕行阈值**下的**配置**并配置选项。

流绕行阈值提供流限值，如果超过该限值，则会触发 IAB 信任绕行模式下的可绕行应用流量，或允许应用流量在测试模式下接受进一步检查。系统会忽略设置为 0 的流绕行阈值。

您可以配置一项或多项以下流绕行阈值：

- **单位流字节数** — 一个流可以包含的最大千字节数。默认值为 500000。范围为 0 至 2147483647。
- **单位流数据包数**—一个流可以包含的最大数据包数。默认值为 0。范围为 0 至 2147483647。
- **流持续时间** — 一个流保持开放的最大秒数。默认值为 0。范围为 0 至 2147483647。
- **流速**— 最高传输速率（千字节/秒）。默认值为 250000。范围为 0 至 2147483647。

**步骤 6** 点击**确定 (OK)** 保存 IAB 设置。

**步骤 7** 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。

## IAB 日志记录和分析

无论是否启用连接日志记录，IAB 都会强制连接结束事件记录已绕过的流和应已绕过的流。连接事件指示在绕行模式下绕过的流或在测试模式下应已绕过的流。基于连接事件的自定义控制面板构件和报告可以显示已绕过和应已绕过的流的长期统计信息。

### IAB 连接事件

#### 操作

当**原因 (Reason)** 包括 `Intelligent App Bypass` 时：

- **允许** — 指示已应用的 IAB 配置处于测试模式，并且**应用协议**指定的应用的流量仍可供检查。
- **信任** — 指示已应用的 IAB 配置处于绕行模式，并且**应用协议**指定的应用的流量受信任，可流经网络而不进行进一步检查。

**原因**

`Intelligent App Bypass` 指示 IAB 在绕行或测试模式下触发了事件。

**应用协议**

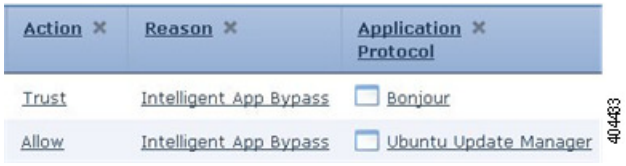
此字段显示触发了事件的应用协议。

### 示例 1

在以下截断的图形中，某些字段已省略。该图形显示根据两个单独访问控制策略中的不同 IAB 设置产生的两个连接事件的**操作 (Action)**、**原因 (Reason)** 和**应用协议 (Application Protocol)** 字段。

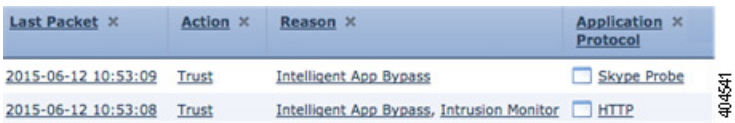
对于第一个事件，`Trust` 操作指示 IAB 在绕行模式下已启用，并且 Bonjour 协议流量受信任可通过而不进行进一步检查。

对于第二个事件，`Allow` 操作指示 IAB 在测试模式下已启用，因此 Ubuntu 更新管理器流量会接受进一步检查，但如果 IAB 在绕行模式下已启用，则应已绕过该流量。




### 示例 2

在以下截断的图形中，某些字段已省略。第二个事件中的流同时按照入侵规则（**原因 [Reason]**：`Intrusion Monitor`）进行绕过（**操作 [Action]**：`Trust`；**原因 [Reason]**：`Intelligent App Bypass`）和检查。`Intrusion Monitor` 原因指示检测到设置为**生成事件 (Generate Events)** 的入侵规则，但在连接过程中未阻止漏洞。在示例中，此情况发生在检测到应用之前。在检测到应用后，IAB 将应用识别为可绕过且受信任的流。




### IAB 自定义控制面板构件

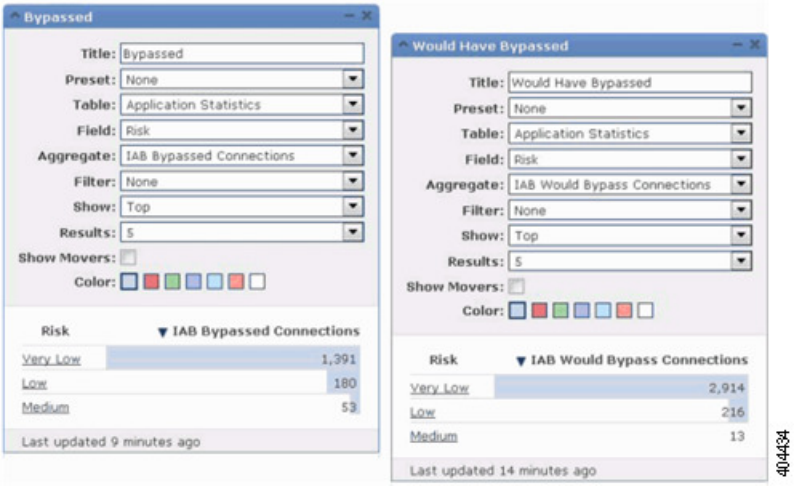
可以创建自定义分析控制面板构件以根据连接事件显示长期 IAB 统计信息。创建构件时，请指定以下信息：

- **预设**：无
- **表**：应用统计信息
- **字段 (Field)**：any
- **汇聚 (Aggregate)**：以下任一：
  - IAB Bypassed Connections
  - IAB Would Bypass Connections
- **过滤器 (Filter)**：any

### 控制面板示例

在以下自定义分析控制面板构件示例中：

- 已绕过示例显示由于在已部署的访问控制策略中应用指定为可绕过且 IAB 在绕行模式下已启用而绕过的应用流量的统计信息。
- 应已绕过示例显示由于在已部署的访问控制策略中应用指定为可绕过且 IAB 在测试模式下已启用而应已绕过的应用流量的统计信息。.




### IAB 自定义报告

可以创建自定义报告以根据连接事件显示长期 IAB 统计信息。创建报告时，请指定以下信息：

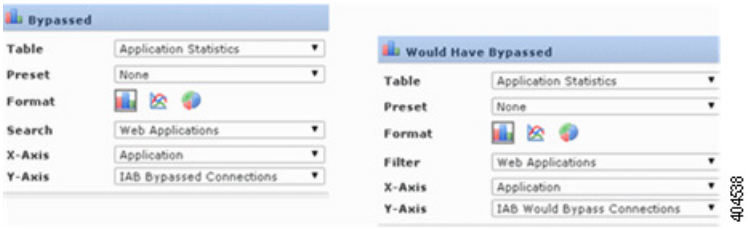
- **表**：应用统计信息
- **预设**：无
- **过滤器 (Filter)**：any
- **X 轴 (X-Axis)**：any

- **Y 轴 (Y-Axis)**：以下任一：
  - IAB Bypassed Connections
  - IAB Would Bypass Connections

### 报告示例

下图中显示两个缩写的报告示例：

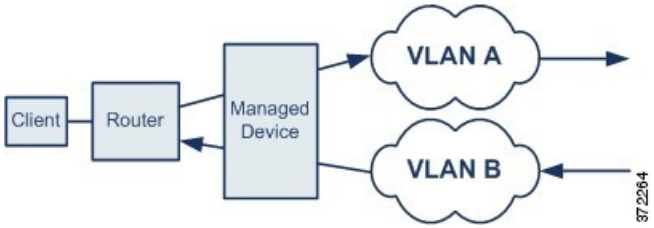
- 已绕过示例显示由于在已部署的访问控制策略中应用指定为可绕过且 IAB 在绕行模式下已启用而绕过的应用流量的统计信息。
- 应已绕过示例显示由于在已部署的访问控制策略中应用指定为可绕过且 IAB 在测试模式下已启用而应已绕过的应用流量的统计信息。




# 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。

- **跟踪连接时忽略 VLAN 报头** -识别流量时忽略还是包含 VLAN 报头。同一连接中行进方向不同的流量中的 VLAN 标记不同，可能影响流量重组和规则处理。例如，对于同一连接，流量可以通过 VLAN A 传输，而通过 VLAN B 接收。如果设备可能为同一连接识别到不同的 VLAN，请选择此选项。该选项默认为关闭。




- **最大活动响应数** - 对于触发配置为提供活动响应的预处理器/入侵丢弃规则的 TCP 连接，是指每个 TCP 连接的最大活动响应数。如果已启动活动响应的连接上出现其他流量，并且在先前活动响应后流量出现超过**最小响应秒数 (Minimum Response Seconds)**，系统会发送其他活动响应，除非已达到指定的最大数量。设置为 0 将禁用由主动响应规则触发的额外主动响应。默认值为无限制。范围为 0 到 25。

注释 您必须专门配置丢弃规则，以提供主动响应。对于TCP连接，主动响应是RESET 数据包。对于 UDP 连接，系统会向连接源发送 ICMP 不可达数据包。

- **最小响应秒数** - 指定在系统已启动活动响应的连接上的任何其他流量都会产生后续活动响应之前等待的秒数，直至出现**最大活动响应数**。默认值为无限制。范围为 1 到 300。
- **会话终止日志记录阈值** - 请勿修改此选项，除非支持人员指示执行此操作。

  支持人员可能会在故障排除呼叫期间要求您配置系统，以在单个连接超过指定阈值时记录消息。更改此选项的设置会影响性能，应仅在支持人员的指导下进行操作。此选项指定一个字节数，当会话终止并超过该指定数字时，将会记录消息。上限为 1GB。

# 检测增强设置

检测增强设置确定自适应配置文件是否用于访问控制策略中的应用检测和入侵规则。通常，系统使用网络分析策略中的静态设置预处理和分析流量。通过自适应配置文件，系统可以使用由网络发现检测或从第三方导入的主机信息适应处理行为。

注释 要在 Snort 3 中启用自适应配置文件，必须同时选择**启用**和**启用配置文件更新**选项。

- **启用** - 您必须启用自适应分析功能（其默认状态），以便访问控制规则执行应用程序和文件控制（包括恶意软件防护 (AMP)），并使入侵规则能够使用服务元数据。
- **启用配置文件更新** - 配置文件更新（例如可在网络分析策略中配置的基于目标的配置文件）有助于通过与目标主机上的操作系统相同的方式对IP数据包进行分片重组并重组数据流。然后入侵规则引擎使用与目标主机所用的相同格式分析数据。配置文件更新还会将入侵规则中的元数据与主机信息进行比对，以确定该规则是否应适用于特定主机。有关详细信息，请参阅：
  - 自适应配置文件更新，第 14 页
  - 自适应配置文件更新和建议的规则，第 14 页
- **自适应配置文件-属性更新间隔** - 启用配置文件更新后，您可以控制从管理中心向受管设备同步网络地图数据的频率（以分钟为单位）。系统使用该数据确定处理流量时应使用哪些配置文件。增大此选项的值可提升大型网络的性能。
- **自适应配置文件-网络** - 或者，启用配置文件更新后，您可以通过将限制在逗号分隔的IP地址、地址块和网络变量列表中来提高性能。如果使用网络变量，则系统会为您的访问控制策略使用与默认入侵策略相关联的变量集中的变量值。例如，可以输入：192.168.1.101, 192.168.4.0/24, $HOME_NET。支持 IPv4 和 IPv6。

  默认值 (0.0.0.0/0) 将自适应配置文件更新应用于所有网络。

## 自适应配置文件更新

通常，系统使用网络分析策略中的静态设置预处理和分析流量。通过自适应配置文件，系统可以使用由网络发现检测或从第三方导入的主机信息适应处理行为。

配置文件更新（就像可在网络分析策略中手动配置的基于目标的配置文件一样）有助于以与目标主机上操作系统相同的方式对 IP 数据包进行分片重组并重组数据流。然后入侵规则引擎使用与目标主机所用的相同格式分析数据。

手动配置的基于目标的配置文件应用您选择的默认操作系统配置文件，或绑定到特定主机的配置文件。但是，配置文件更新会根据目标主机的主机配置文件中的操作系统切换到相应的操作系统配置文件。

假设您为 10.6.0.0/16 子网配置配置文件更新，并将默认 IP 分片重组基于目标的策略设置为 Linux。配置设置的防火墙管理中心中有一个包括 10.6.0.0/16 子网的网络映射。

- 当系统检测到来自主机 A（不在 10.6.0.0/16 子网中）的流量时，它使用基于 Linux 目标的策略重组 IP 分片。
- 当系统检测到来自主机 B（在 10.6.0.0/16 子网中）的流量时，它从网络映射检索主机 B 的操作系统数据。系统使用基于该操作系统的配置文件对传送到主机 B 的流量进行分片重组。

## 自适应配置文件更新和建议的规则

自适应配置文件功能是访问控制策略中的高级设置，它全局应用于由该访问控制策略调用的所有入侵策略。思科 建议的规则功能适用于您在其中配置该功能的各个入侵策略。

与建议的入侵规则一样，配置文件更新将规则中的元数据与主机信息进行比较，确定是否应为特定主机应用该规则。然而，建议的入侵规则会基于该信息提供规则启用或禁用的建议，而配置文件更新则利用这些信息将特定规则应用于特定流量。

建议的入侵规则需要您手动执行规则状态的建议更改。另一方面，配置文件更新不会修改入侵策略。基于配置文件更新的规则处理以逐包方式进行。

此外，建议的入侵规则可启用已禁用的规则。相比之下，配置文件更新仅影响入侵策略中已启用规则的应用，且配置文件更新从不更改规则状态。

您可以将配置文件更新与建议的入侵规则结合使用。部署入侵策略时，配置文件更新会使用规则的当前状态来确定是否将其列为应用候选规则，而您接受或拒绝建议的选择会反映在该规则状态中。您可以同时使用这两个功能来确保您已启用或禁用每个监测网络中最合适的规则，然后应用对特定流量最为有效的已启用规则。

# 性能设置

以下设置用于在系统分析流量入侵企图时优化性能。各组设置均有独立选项卡。

这些设置适用于 Snort，仅当您在规则中或作为默认动作应用入侵策略时才相关。仅当您是 Snort 入侵规则专家，或在思科技术支持指导下才更改这些设置。

### 模式匹配限制

- **每个数据包要分析的最大模式状态数** — 要排队的最大事件数。默认值为 5。
- **禁用对未来将进行重组的流量的内容检查** — 是否在重组前检测 TCP 负载。它包括数据流重组前后的数据包检测。这一过程需要更多的处理开销，并且可能会降低性能。如果未选中该选项，则在重组后检测 TCP 负载。默认为关闭。

### 性能统计数据

当过了所指定的性能统计数据更新之间的秒数时，系统验证其已分析的数据包是否到达指定数量。如果到达，则系统更新性能统计数据。否则，系统等待，直到其分析的数据包到达指定的数量。

- **采样时间（秒）**— 进行性能采样的时间范围。默认值为 300 秒。

  为采样时间配置非常低的值（例如 1 秒）可能会对设备造成巨大影响；设备上记录的性能统计信息可能会导致磁盘空间问题并影响设备的运行。因此，建议您不要配置非常低的值。

- **最小数据包数** — 将多少个数据包视为有效性能统计信息的最小值。默认值为 0。
- **故障排除选项：**
  - **记录会话/协议分布** — 思科技术支持可能会在故障排除电话中要求您启用此选项，以配置系统仅在 Snort 进程关闭或重启时计算性能统计信息。
  - **摘要** — 仅当思科技术支持指示时才启用此选项。

### 正则表达式限制

默认的 Perl 兼容正则表达式 (PCRE) 限制确保了最低水平的性能。覆盖这些限制可能会提高安全性，但也会因允许根据低效的正则表达式对数据包进行评估而严重影响性能。

- **匹配限制状态** — 匹配正则表达式的限制。您可以选择**默认值**（即 3500）、**无限制**或**自定义**。如果您选择自定义，请在**匹配限制**中指定尝试匹配 PCRE 正则表达式中定义的模式的次数。指定 0 以完全禁用 PCRE 匹配评估。
- **匹配递归限制状态** — 匹配正则表达式递归的限制。您可以选择**默认值**（即 3500）、**无限制**或**自定义**。如果您选择自定义，请在**匹配递归限制**中指定评估数据包负载中的 PCRE 正则表达式时的递归次数。指定 0 以完全禁用 PCRE 递归。

**注释** 要使自定义匹配递归限制有意义，它必须小于匹配限制。

### 入侵事件日志记录限制

当入侵规则引擎根据规则评估流量时，它会将针对给定数据包或数据包流生成的事件放在事件队列中，然后将队列顶部的事件报告至用户界面。配置入侵事件日志记录限制时，可指定队列中可放置的事件数量及要记录的事件数量，并可选择确定队列中事件顺序的条件。

- **每个数据包存储的最大事件数** — 可以为给定数据包或数据包流存储的最大事件数。默认值为 8。
- **每个数据包记录的最大事件数**—为给定数据包或数据包流记录的事件数。这不能超过**每个数据包存储的最大事件数量 (Maximum Events Stored Per Packet)** 的值。默认值为 5。
- **事件日志记录优先级依据**—用于确定事件队列中事件排序的值。通过用户界面报告排序最靠前的事件。您可以选择：
  - **内容长度**（默认），按最长识别内容匹配对事件进行排序。当事件按内容长度排序时，规则事件始终优先于解码器和预处理程序事件。
  - **优先级**，按事件优先级对队列中的事件进行排序。

# 基于延迟的性能设置

每个访问控制策略都具有基于延迟的设置，这些设置使用阈值来管理数据包和规则处理性能。

这些设置适用于 Snort，仅当您在规则中或作为默认动作应用入侵策略时才相关。默认情况下，数据包和规则处理的基于延迟的性能设置由最新部署的入侵规则更新自动填充，我们建议您不要更改默认设置。仅当您是 Snort 入侵规则专家，或在思科技术支持指导下才更改这些设置。

应用的延迟设置取决于与访问控制策略关联的网络分析策略 (NAP) 的安全级别。通常，这是指默认 NAP 策略。但是，如果已配置自定义网络分析规则，并且其中任意一个规则指定的 NAP 策略安全级别都高于默认 NAP 策略，则延迟设置取决于自定义规则中安全级别最高的 NAP 策略。如果默认 NAP 策略或任何自定义规则调用自定义 NAP 策略，则评估中使用的安全级别是每个自定义 NAP 策略所基于的系统提供的基本策略。

不论有效阈值和/或网络分析配置直接在策略中继承还是配置，上述情况均成立。

使用以下设置来调整系统的基于延迟的性能。

- **应用设置来源** — 是否从**已安装规则更新**（默认）或您的**自定义**设置中应用基于延迟的性能设置。
- **数据包处理**—数据包延迟阈值用于度量适用的解码器、预处理程序和规则在处理数据包时所需的总时间，并在处理时间超过可配置阈值时停止对数据包的检测。默认情况下，数据包处理的基于延迟的性能设置处于禁用状态。您可以选择将其启用。但是，思科建议您不要更改阈值设置的默认值。选择**已启用**以开启它。如果您选择了**自定义**，还需输入检查数据包应停止的**阈值**时间（微秒）。默认值为 256。
- **规则处理**—规则延迟阈值功能可以衡量每个规则处理各个数据包所花费的时间、将超过阈值的规则及一系列相关规则暂停指定的时间（如果处理时间连续超过规则延迟阈值一定次数 [可配置]），以及在暂停到期后恢复规则。仅当您选择**自定义**时才可以配置这些选项。
  - **启用**—如果您选择自定义，此选项会自动选中。如果您不想使用此功能，请取消选择该选项。此选项卡上的所有其他设置都需要启用该功能。
  - **阈值（微秒）**— 指定规则检查数据包时不应超过的时间（微秒）。默认值为 512。

- **暂停规则前的连续阈值违规次数**—指定规则在被暂停前检查数据包所用时间可以超过阈值时间的连续次数。默认值为 3。
- **暂停时间** — 暂停的规则应保持暂停多长时间。默认值为 10。

# 访问控制策略的高级设置历史记录

| 功能 | 防火墙管理中心最低版本 | **Firewall Threat Defense**最低版本 | 详细信息 |
|---|---|---|---|
| 影子流量监控 | 10.0.0 | 10.0.0 | 监控源自未经批准的隐私技术的流量（称为影子流量）。<br>新增/修改的屏幕：<br>• **策略** > **访问控制** > **编辑策略** > **更多** > **高级设置** > **影子流量**<br>• **洞察与报告** > **控制面板** > **影子流量** |
| 改进了端口扫描检测。 | 7.2 | 7.2 运行 Snort 3 | 通过改进的端口扫描检测器，您可以轻松地配置系统以检测或防止端口扫描。您可以细化要保护的网络，设置灵敏度等。对于运行 Snort 2 的设备以及运行版本 7.1 及更早版本的设备，请继续使用网络分析策略进行端口扫描检测。<br>新增/修改的屏幕：我们向访问控制策略的高级选项卡添加了 **威胁检测** 。<br>新增/修改的命令： **clear threat-detection portscan**、 **show threat-detection portscan**。 |
| 在 Snort 3 设备上绕过检查或限制大流量。 | 7.2.0 | 使用 Snort 3 的 7.2.0 | 您现在可以检测并选择性地绕过检查或限制大流量。默认情况下，访问控制策略设置为在系统发现大于 1 GB/10 秒的未加密连接时生成事件；速率限制可配置。<br>对于 Firepower 2100 系列，您可以检测象流，但不能绕过检查或限制。对于运行 Snort 2 的设备以及运行 7.1 及更低版本的设备，请继续使用智能应用绕行 (IAB)。<br>新增/修改的屏幕：我们在访问控制策略的“高级”选项卡中添加了 **象流设置** 。<br>有关更多信息，请参阅 象流检测。 |

| 功能 | 防火墙管理中心最低版本 | Firewall Threat Defense最低版本 | 详细信息 |
|---|---|---|---|
| DNS 过滤 | 7.0.0<br>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。<br>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。<br>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 | 6.7.0 | 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。<br>启用此功能可能会影响设备性能，但具体取决于型号。<br>访问控制策略的“高级”(Advanced) 选项卡页面具有新选项：<br>• 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。<br>• “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)**。 |
| 威胁防御服务策略。 | 6.3 | 任意 | 现在您可以将威胁防御服务策略配置为访问控制策略高级选项的一部分。您可以使用威胁防御服务策略将服务应用于特定流量类。支持的功能包括 TCP 状态绕行、随机生成 TCP 序列号、递减数据包的生存时间 (TTL) 值、失效连接检测、设置每个流量类和每个客户端的最大连接数和初期连接数限制以及初期、半闭和空闲连接的超时时间。<br>新屏幕： **策略** > **访问控制** > **访问控制**、 **高级** 选项卡， **威胁防御服务策略**。<br>支持的平台： Cisco Secure Firewall Threat Defense |

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。