智能应用绕行

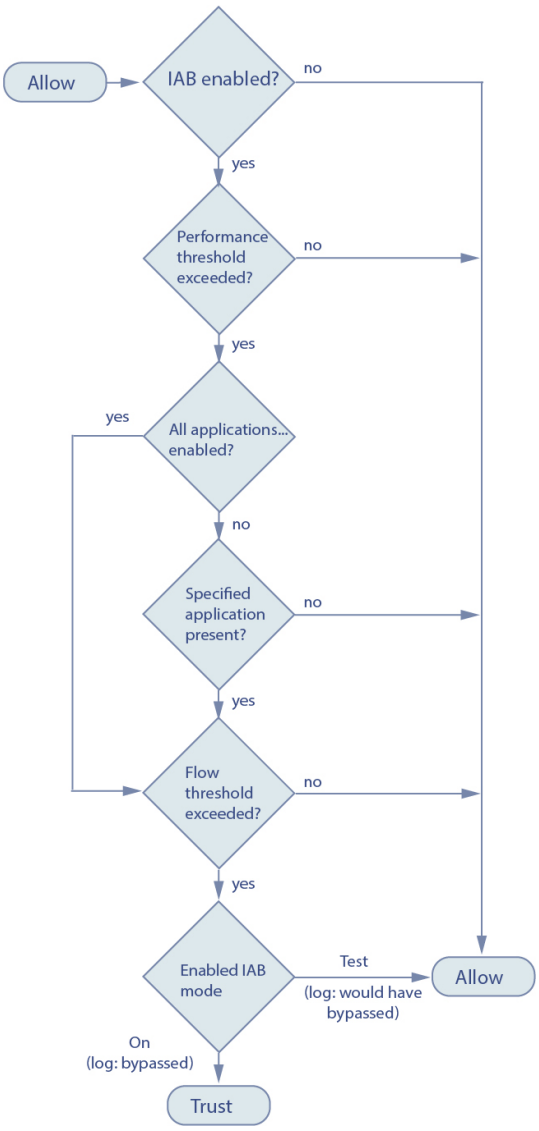
以下主题介绍如何配置访问控制策略以使用智能应用旁路 (IAB)

IAB 简介

IAB 可识别您信任其流经您的网络而无需进一步检查是否超出性能和数据流阈值的应用。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）您可以配置 IAB，以便在超过检查性能阈值时，无论应用类型如何，IAB 都信任超过任何流绕行阈值的所有流量。

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：



IAB 选项

状态

启用或禁用 IAB。

性能采样间隔 (Performance Sample Interval)

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。值 **0** 会禁用 IAB。

可绕行应用和过滤器 (Bypassable Applications and Filters)

此功能提供两个互斥的选项：

应用/过滤器
提供您可以在其中指定可绕行应用和应用集（过滤器）的编辑器。请参阅应用规则条件。

包括未识别应用在内的所有应用
超过检查性能阈值时，不管应用类型为何，都信任超过任何流绕行阈值的所有流量。

性能和流阈值

您必须配置至少一个检查性能阈值和一个流绕过阈值。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。

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。IAB 不使用设置为 **0** 的检查性能阈值。您可以配置一项或多项以下检查性能阈值：

丢弃百分比 (Drop Percentage)

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。

处理器利用率百分比 (Processor Utilization Percentage)

使用的处理器资源的平均百分比。

数据包延迟

平均数据包延迟（微秒）。

流量

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。

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。IAB 不使用设置为 **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 (Bytes per Flow)

一个流可以包含的最大千字节数。

单位流数据包数 (Packets per Flow)

一个流可以包含的最大数据包数。

流持续时间 (Flow Duration)

一个流保持开放的最大秒数。

流速 (Flow Velocity)

最高传输速率（千字节/秒）。

智能应用绕行的要求和前提条件

型号支持

任意

支持的域

任意

用户角色

- 管理员
- 访问管理员
- 网络管理员

配置智能应用旁路

⚠

注意 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

对于经典设备，您必须拥有控制许可证。

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 配置 IAB 选项：

- **状态 (State)** - **关闭**或**打开** IAB，或在**测试**模式下启用 IAB。
- **性能采样间隔 (Performance Sample Interval)** - 输入 IAB 性能采样扫描之间的间隔时间（以秒为单位）。如果启用 IAB，即使在测试模式下，也请输入非零值。输入 **0** 可禁用 IAB。
- **可绕过的应用和过滤器 (Bypassable Applications and Filters)** - 从以下项中选择：
  - 点击绕过的应用和过滤器数量并指定要绕过其流量的应用；请参阅配置应用条件和过滤器。

- 点击**所有应用 (包括未识别的应用)**，以便在超过检查性能阈值时，IAB 信任超过任何流绕行阈值的所有流量，不管应用类型如何都是如此。

- **检查性能阈值 (Inspection Performance Thresholds)** - 点击**配置 (Configure)** 并输入至少一个阈值。
- **流绕行阈值 (Flow Bypass Thresholds)** - 点击**配置 (Configure)** 并输入至少一个阈值。

必须指定至少一个检查性能阈值和一个流绕行阈值；必须超过这两个阈值，IAB 才可信任流量。如果为每种类型输入多个阈值，则仅必须超过每种类型的一个阈值。有关详细信息，请参阅IAB 选项，第 2 页。

步骤 3 点击**确定 (OK)** 保存 IAB 设置。

步骤 4 点击**保存**保存策略。

下一步做什么

- 由于在检测应用之前必须允许一些数据包通过，因此必须配置系统以便检查这些数据包。
- 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：

`Allow` -

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。

`Trust` -

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

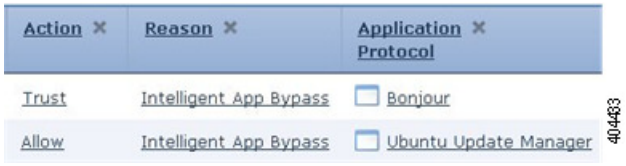
此字段显示触发了事件的应用协议。

示例

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

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

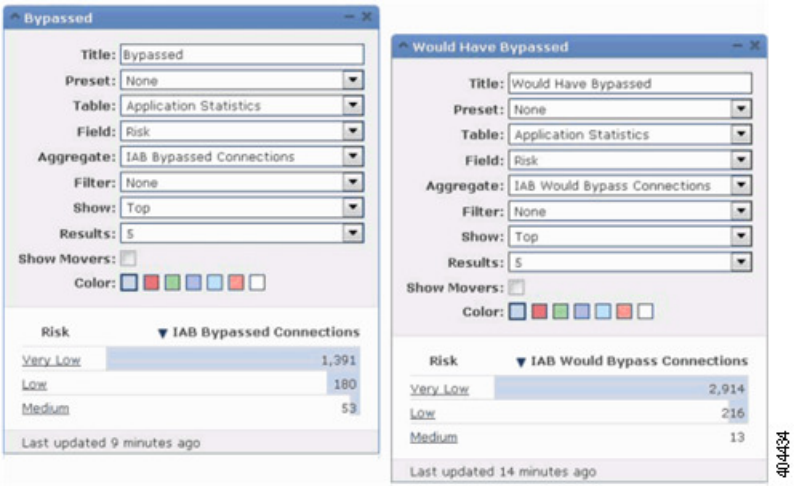
可以创建自定义分析控制面板构件以根据连接事件显示长期 IAB 统计信息。创建构件时，请指定以下信息：

- **预设 (Preset)**：`None`
- **表 (Table)**：`Application Statistics`
- **字段 (Field)**：any
- **汇聚 (Aggregate)**：以下任一：
  - `IAB Bypassed Connections`
  - `IAB Would Bypass Connections`
- **过滤器 (Filter)**：any

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：

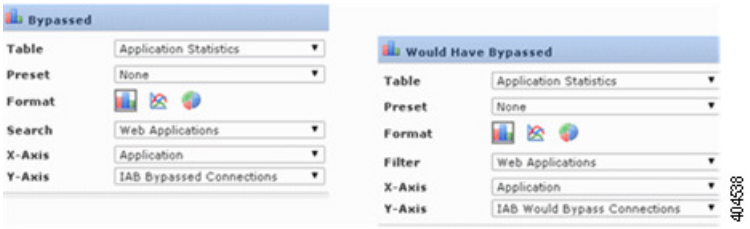
- **表 (Table)**：`Application Statistics`
- **预设 (Preset)**：`None`
- **过滤器 (Filter)**：any
- **X 轴 (X-Axis)**：any
- **Y 轴 (Y-Axis)**：以下任一：
  - `IAB Bypassed Connections`
  - `IAB Would Bypass Connections`

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。



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。