入侵策略使用入门

以下主题介绍如何开始使用入侵策略：

入侵策略基础知识

入侵策略是已定义的几组入侵检测和防护配置，用于检查流量是否存在安全违规，以及在内联部署中阻止或修改恶意流量。入侵策略供访问控制策略调用，是系统在允许流量到达目标之前的最后一道防线。

每个入侵策略的中心是入侵规则。启用的规则导致系统为匹配规则的流量生成入侵事件（或阻止该流量）。禁用规则将停止该规则的处理。

系统提供几种基本入侵策略，使您可以利用 Talos 情报小组的经验。对于这些策略，Talos 设置入侵和预处理器规则状态（启用或禁用），并提供其他高级设置的初始配置。

提示 系统提供的入侵和网络分析策略具有类似的名称，但包含不同的配置。例如，“平衡安全性和连接”(Balanced Security and Connectivity) 网络分析策略和“平衡安全性和连接”(Balanced Security and Connectivity) 入侵策略共同发挥作用，均可在入侵规则更新中更新。但是，网络分析策略管理的主要是预处理选项，而入侵策略管理的主要是入侵规则。

如果创建自定义入侵策略，您可以：

- 通过启用和禁用规则，以及撰写和添加您自己的规则来调整检测。
- 遵从思科 的建议，将您的网络中检测到的操作系统、服务器和客户端应用协议与为保护这些资产而特别编写的规则相关联。
- 配置各种高级设置，例如，外部警告，敏感数据预处理和全局规则阈值。
- 使用分层作为构建块，以有效地管理多个入侵策略。

在内联部署中，入侵策略可以阻止和修改流量：

- 丢弃规则可以丢弃匹配的数据包和生成入侵事件。要配置入侵或预处理器丢弃规则，请将其状态设置为“丢弃并生成事件”(Drop and Generate Events)。
- 入侵规则可使用 `replace` 关键字来替换恶意内容。

要使入侵规则影响流量，必须正确配置丢弃规则和内容替换规则，以及正确部署内联受管设备，也就是与内联接口集内联。最后，必须启用入侵策略的丢弃行为或 **Drop when Inline** 设置。

当定制入侵策略时，特别是在启用和添加规则时，请记住一些入侵规则要求首先以某种方式对流量进行解码或预处理。在入侵策略检查数据包之前，数据包根据网络分析策略中配置对其进行预处理。如果您禁用一个必需的预处理程序，虽然该预处理程序在网络分析策略 Web 界面中保持禁用，但系统仍自动通过其当前设置使用它。

⚠

注意 由于预处理和入侵检查密切相关，因此用于检查单个数据包的网络分析和入侵策略**必须**相互补充。定制预处理（特别是使用多个自定义网络分析策略）是一个**高级**任务。

在配置自定义入侵策略后，可以在访问控制配置过程中通过以下方式使用该策略：将入侵策略与一个或多个访问控制规则或访问控制策略的默认操作相关联。这会强制系统在某个允许的流量到达最终目的地之前使用入侵策略检查该流量。与入侵策略共同使用的变量集，用于准确地反映您的家庭和外部网络以及网络上的服务器（如果适当）。

请注意，默认情况下，系统禁用加密负载的入侵检查。当加密连接与已配置入侵检查的访问控制规则匹配时，这有助于减少误报和提高性能。

入侵策略的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

入侵策略的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 入侵管理员 (Intrusion Admin)

管理入侵策略

在“入侵策略”页面（**策略** > **访问控制** > **入侵**）上，可以查看当前自定义入侵策略以及下列信息：

- 最近一次修改策略的时间和日期（采用当地时间）以及执行此修改的用户。
- 是否已启用**内联时丢弃 (Drop when Inline)** 设置，该设置允许您在内联部署中丢弃和修改流量。内联部署可以是使用路由、交换或透明接口，或内联接口对部署到设备上的配置。
- 哪些访问控制策略和设备在使用入侵策略检查流量
- 策略是否有未保存的更改，以及有关何人（如果有任何人）当前正在编辑该策略的信息
- 在多域部署中，创建了策略的域

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

步骤 2 管理入侵策略：

- 比较 - 点击**比较策略 (Compare Policies)**；请参阅比较策略。
- 创建 - 点击**创建策略 (Create Policy)**；请参阅：
  - Snort 2 策略的 创建自定义 Snort 2 入侵策略，第 4 页。
  - 最新版本的《Cisco Secure Firewall Management Center Snort 3 配置指南》中适用于 Snort 3 策略的创建自定义 *Snort 3* 入侵策略主题。

- 删除 - 点击要删除的策略旁边的 **删除**（ ）。如果另一用户在策略中有未保存的更改，则系统会提示您确认并进行通知。点击 **OK** 确认。

  如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

- 编辑 - 选择：
  - **Snort 2 版本 (Snort 2 Version)**；请参阅编辑 Snort 2 入侵策略，第 5 页。
  - **Snort 3 版本**；请参阅最新版本的《Cisco Secure Firewall Management Center Snort 3 配置指南》中的编辑 *Snort 3* 入侵策略主题。

  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。

- 导出 - 如果要导出入侵策略以在其他 Cisco Secure Firewall Management Center 上进行导入，请点击 **YouTube EDU**（ ）；请参阅《Cisco Secure Firewall Management Center 管理指南》中的导出配置。
- 部署 - 选择**部署** > **部署**；请参阅部署配置更改。
- 报告 - 点击**报告**（ ）；请参阅生成当前策略报告。

自定义入侵策略创建

当您创建新的入侵策略时，必须为其提供唯一的名称，指定基本策略并指定丢弃行为。

基本策略定义入侵策略的默认设置。修改新策略中的设置会覆盖（但不会更改）基本策略中的该设置。您可以使用系统提供的策略或自定义策略作为您的基本策略。

创建自定义 Snort 2 入侵策略

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

步骤 2 点击**创建策略**。如果您在另一策略中有未保存的更改，当系统提示您返回“入侵策略”(Intrusion Policy) 页面时，请点击**取消 (Cancel)**。

确保选择**入侵策略 (Intrusion Policies)** 选项卡。

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 选择**监测模式 (Inspection Mode)**。

所选操作确定是入侵规则阻止并发出警报（**防御** 模式）还是仅发出警报（**检测** 模式）。

步骤 5 选择初始**基本策略 (Base Policy)**。

您可以使用系统提供的策略或其他自定义策略作为您的基本策略。

步骤 6 点击**保存 (Save)**。

新策略的设置与其基本策略相同。

相关主题

层中的入侵规则
冲突和更改：网络分析和入侵策略

编辑 Snort 2 入侵策略

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

步骤 2 确保选择**入侵策略 (Intrusion Policies)** 选项卡。

步骤 3 点击要配置的入侵策略旁边的 **Snort 2 版本** 。

步骤 4 编辑策略：

- 更改基本策略 - 从**基本策略 (Base Policy)** 下拉列表中选择基本策略；请参阅更改基本策略。
- 配置高级设置 - 点击导航面板中的**高级设置 (Advanced Settings)**；请参阅入侵策略高级设置，第 9 页。
- 配置思科 配置 Firepower 建议的入侵规则 - 点击导航面板中的**思科建议 (Cisco Recommendations)**；请参阅生成和应用思科 建议。
- 丢弃内联部署中的行为 - 选中或取消选中**内联时丢弃 (Drop when Inline)**；请参阅设置内联部署中的丢弃行为，第 8 页。
- 按建议的规则状态过滤规则 - 生成建议后，点击每个建议类型旁边的**查看 (View)**。点击**查看建议的更改 (View Recommended Changes)** 以查看所有建议。
- 按当前规则状态过滤规则 - 点击每个规则状态类型（生成事件、丢弃和生成事件）旁边的**查看 (View)**；请参阅入侵策略中的入侵规则过滤器。
- 管理策略层 - 点击导航面板中的**策略层 (Policy Layers)**；请参阅层管理。
- 管理入侵规则 - 点击**管理规则 (Manage Rules)**；请参阅查看入侵策略中的入侵规则。
- 查看基本策略中的设置 - 点击**管理基本策略 (Manage Base Policy)**；请参阅基本层。

步骤 5 要保存自上次策略确认以来在此策略中进行的更改，请选择**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

相关主题

生成和应用思科 建议
配置层中的入侵规则
冲突和更改：网络分析和入侵策略

入侵策略更改

当创建新的入侵策略时，它具有与其基本策略相同的入侵规则和高级设置。

系统为每个用户缓存一个入侵策略。在编辑入侵策略时，如果您选择任何菜单或指向另一页的其他路径，即使您离开此页，更改也会保留在系统缓存中。

用于执行入侵防御的访问控制规则配置

访问控制策略可能有多个与入侵策略相关联的访问控制规则。您可以为任何 Allow 或 Interactive Block 访问控制规则配置入侵检测，这样，您就可在网络中不同类型的流量到达最终目的地之前，使不同的入侵检测配置文件与其匹配。

只要系统使用入侵策略来评估流量，它便会使用关联的变量集。变量集中的变量代表通常在入侵规则中用来识别源 IP 地址、目标 IP 地址、源端口和目标端口的值。您还可以在入侵策略中使用变量表示规则禁止和动态规则状态中的 IP 地址。

提示 即使您使用系统提供的入侵策略，思科也**强烈**建议您配置系统的入侵变量以准确反映您的网络环境。至少，要修改默认变量集中的默认变量。

了解系统提供的入侵策略和自定义入侵策略

思科通过 Firepower 系统提供多种入侵策略。通过使用系统提供的入侵策略，您可以利用 Talos 情报小组 的经验。对于这些策略，Talos 会设置入侵和预处理器规则状态，并提供高级设置的初始配置。可以按现状使用系统提供的策略，也可以将其用作自定义策略的基础。构建自定义策略可以提高系统在您的环境中的性能，并提供网络上发生的恶意流量和策略违规行为的集中视图。

连接和入侵事件日志记录

当访问控制规则调用的入侵策略检测到入侵并生成入侵事件时，它会将此事件保存到 Cisco Secure Firewall Management Center。无论访问控制规则采用何种日志记录配置，系统都会将发生入侵的连接结束自动记录到 Cisco Secure Firewall Management Center数据库。

相关主题

预定义默认变量

访问控制规则配置和入侵策略

请注意，您在单个访问控制策略中可以使用的唯一入侵策略的数量取决于目标设备型号；设备的功能越强大，处理的策略就越多。每个唯一的入侵策略和变量集**对均**视为一个策略。虽然您可以将不同的入侵策略-变量集对与每条“允许”(Allow) 和“交互式阻止”(Interactive Block) 规则（以及默认操作）相关联，但是，如果目标设备没有足够的资源可按照配置执行检测，则无法部署访问控制策略。

配置访问控制规则以执行入侵防御

您必须是管理员，访问管理员或网络管理员用户才能执行此任务。

过程

步骤 1 在访问控制策略编辑器中，创建新规则或编辑现有规则；请参阅访问控制规则组成部分。

步骤 2 确保规则操作设置为 **Allow**、**Interactive Block** 或 **Interactive Block with reset**。

步骤 3 点击 **检测**。

步骤 4 选择系统提供的或自定义**入侵策略 (Intrusion Policy)**，或选择**无 (None)** 以禁用对与访问控制规则相匹配的流量进行的入侵检查。

步骤 5 如果要更改与入侵策略关联的变量集，请从**变量集 (Variable Set)** 下拉列表中选择值。

步骤 6 点击**保存 (Save)** 保存规则。

步骤 7 点击**保存 (Save)** 保存策略。

下一步做什么

- 部署配置更改。

相关主题

变量集
Snort® 重新启动场景

内联部署中的丢弃行为

如果要评估配置如何在内联部署中起作用（即，使用路由式、交换式或透明接口或内联接口对将相关配置部署到设备），而实际上不影响流量，则可以禁用丢弃行为。在这种情况下，系统生成入侵事件，但不会丢弃触发丢弃规则的数据包。当对结果满意时，可以启用丢弃行为。

请注意，在分流模式下，在被动部署或内联部署中，无论丢弃行为如何，系统都无法影响流量。在被动部署中，设置为**丢弃和生成事件 (Drop and Generate Events)** 的规则与设置为**生成事件 (Generate Events)** 的规则行为完全相同。系统生成入侵事件，但不能丢弃数据包。

注释 假设文件阻止操作导致对数据包的“阻止”或“待处理”文件策略判定，然后在同一数据包上生成 IPS 事件。在这种情况下，即使 IPS 策略处于检测模式 (IDS)，IPS 事件也会被标记为已丢弃，而不是将已丢弃。

注释 要阻止恶意软件通过 FTP 传输，不仅要正确配置恶意软件防护，还必须在访问控制策略的默认入侵策略中启用**内联时丢弃**。

当您查看入侵事件时，工作流可以包括内联结果，以指示流量是否确实已丢弃，或者它是否仅仅应该已丢弃。

设置内联部署中的丢弃行为

过程

步骤 1 选择**策略** > **访问控制** > **入侵**。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

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 设置策略的丢弃行为：

- 选中**内联时丢弃 (Drop when Inline)** 复选框，以允许入侵规则影响流量并生成事件。
- 清除**内联时丢弃 (Drop when Inline)** 复选框，以防止入侵规则在生成事件时影响流量。

步骤 4 点击**确认更改 (Commit Changes)** 以保存自上次策略确认后在此策略中做出的更改。

如果在不确认更改的情况下退出策略，则编辑其他策略时，将会放弃自从上次确认以来的更改。

下一步做什么

- 部署配置更改。

双系统部署中的丢弃行为

当网络中有两个背靠背连接的系统时，通常可以看到第一个系统丢弃多个事件，并且仍会在第二个系统上记录一次丢弃或“将已丢弃”事件。第一个系统决定到其扫描文件的最后一个数据包时丢弃数据包，而第二个系统还将开展调查并将流量标识为“将被丢弃”。

例如，一个 5 数据包 HTTP GET 请求，其第一个数据包将触发一条规则，被第一个系统阻止，并且仅丢弃最后一个数据包。第二个系统只能收到 4 个数据包，并将丢弃连接，但当第二个系统在其修剪会话的同时最后刷新部分 GET 请求时，由于内联结果，它将触发与“将已丢弃”相同的规则。

入侵策略高级设置

配置入侵策略的高级设置需要特定专业知识。入侵策略的基本策略决定了默认情况下启用哪些高级设置及各自的默认配置。

在入侵策略的导航面板中选择**高级设置 (Advanced Settings)** 时，策略将按类型列出其高级设置。在 Advanced Settings 页面中，您可以启用或禁用入侵策略中的高级设置，以及访问高级设置配置页面。高级设置必须在启用后才能配置。

当禁用高级设置时，子链接和 **Edit** 链接将不显示，但会保留您的配置。请注意，某些入侵策略配置（敏感数据规则、入侵规则的 SNMP 警报）需要启用和正确配置高级设置。

修改高级设置的配置要求了解正在进行的修改及其对网络的潜在影响。

具体威胁检测

敏感数据预处理器检测敏感信息，例如 ASCII 文本格式的信用卡号和社会保障号。

请注意，在网络分析策略中配置了用于检测特定威胁（back orifice 攻击、多种端口扫描类型以及尝试以过多流量淹没网络的基于速率的攻击）的其他预处理程序。

入侵规则阈值

全局规则阈值允许使用阈值来限制系统记录和显示的入侵事件数量，从而可以防止您的系统由于无法应付大量事件而崩溃。

外部响应

除了网络界面中的各种入侵事件视图之外，您还可以启用记录到系统日志 (syslog) 工具或者将事件数据发送到 SNMP 陷阱服务器。根据策略，可以指定入侵事件通知限制，设置发送到外部日志记录工具的入侵事件通知，以及配置对入侵事件的外部响应。

请注意，除了基于策略的这些警报配置，对于每个规则或规则组，您还可以在入侵事件上全局启用或禁用邮件警报。无论哪个入侵规则处理数据包，都会使用您的邮件警报设置。

相关主题

敏感数据检测基础知识
全局规则阈值基础知识

优化入侵检测和防御的性能

如果要让 Firepower 系统执行入侵检测和防御，但不需要利用发现数据，则可以通过禁用新发现来优化性能，如下所述。

开始之前

要执行此任务，您必须具有以下用户角色之一：

- 访问控制的管理员、访问管理员或网络管理员。
- 网络发现的管理员或发现管理员。

过程

步骤 1 修改或删除与部署在目标设备的访问控制策略关联的规则。与该设备关联的任何访问控制规则均没有用户、应用或 URL 条件；请参阅创建和编辑访问控制规则。

步骤 2 从目标设备的网络发现策略中删除所有规则；请参阅配置网络发现规则。

步骤 3 将已更改的配置部署到目标设备；请参阅部署配置更改。

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。