Snort 3 入侵策略入门

本章提供有关为入侵检测和防御管理 Snort 3 入侵策略和访问控制规则配置的信息。

入侵策略概述

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 Cisco Talos 情报组 (Talos) 的经验。对于这些策略，Talos 设置入侵和检查器规则状态（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。

- 遵从安全防火墙的建议，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。

入侵策略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“阻止”。

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检查其，虽然该检查器在网络分析策略网络界面中保持禁用，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。

有关其他支持和信息，请参阅 Snort 3 入侵策略概述。

网络分析和入侵策略的前提条件

要允许Snort检测引擎处理流量以进行入侵和恶意软件分析，必须为 威胁防御 设备启用IPS许可证。

您必须是管理员用户，才能管理网络分析、入侵策略和执行迁移任务。

创建自定义 Snort 3 入侵策略

过程

步骤 1 依次选择**策略** > **入侵**。

步骤 2 点击**创建策略**。

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）。

注释
在选择预防模式之前，您可能希望阻止规则仅发出警报，以便识别导致大量误报的规则。

步骤 5 选择 **基本策略**。

您可以使用系统提供的策略或已存在的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。

下一步做什么

要自定义策略，请参阅 编辑 Snort 3 入侵策略，第 3 页。

编辑 Snort 3 入侵策略

编辑 Snort 3 策略时，所有更改都会立即保存。无需执行其他操作即可保存更改。

过程

步骤 1 依次选择**策略** > **入侵**。

步骤 2 确保选择**入侵策略**选项卡。

步骤 3 点击要配置的入侵策略旁边的 **Snort 3 版本**。

步骤 4 编辑策略：

- 更改模式 - 点击**模式**下拉列表以更改检测模式。

注意
仅 Snort 3 版本的策略会更改检测模式。现有检测模式在 Snort 2 版本中保持不变，这意味着您的 Snort 2 和 Snort 3 版本的策略将具有不同的检测模式。我们建议您谨慎使用此选项。

- **预防**-已触发的阻止规则创建事件（警报）并丢弃连接。
- **检测**-已触发阻止规则创建警报。

  您可以在进入防御之前选择检测模式。例如，在选择预防模式之前，您可能希望阻止规则仅发出警报，以便识别导致大量误报的规则。

步骤 5 点击 **基本策略** 层定义入侵策略的默认设置。

- 搜索规则 - 使用搜索字段过滤显示内容。您可以输入 GID、SID、规则消息或参考信息。例如，GID:1; SID:9621 - 仅显示规则 1:962；SID:9621,9622,9623 - 显示具有不同 SID 的多个规则。您还可以在“搜索”文本框中点击以选择以下任何选项：
  - 应用过滤器 **操作 = 警报**或 **操作：阻止**
  - 应用 **禁用规则** 过滤器

- 显示 **自定义/用户定义的规则**
- 按 GID、SID 或 GID:SID 过滤
- 按 CVE 过滤
- 按备注过滤

- 查看过滤的规则 - 点击任意 **预设** 以查看设置为警报、阻止、禁用等的规则。

  已覆盖的规则表示规则操作已从默认操作更改为其他操作的规则。请注意，一旦更改，规则操作状态即为已覆盖，即使您将其更改回其原始默认操作也是如此。但是，如果从 **规则操作** 下拉列表中选择 **恢复为默认**，则会删除覆盖状态。

  高级过滤器 根据轻量级安全软件包 (LSP) 版本、入侵分类和 Microsoft 漏洞提供过滤器选项。

- 查看规则文档 - 点击规则 ID 或 **规则文档** 图标可显示规则的 Talos 文档。
- 查看规则详细信息 - 点击规则行中的 **展开箭头**（ ） 图标可查看规则详细信息。
- 添加规则注释 - 点击“注释”列下的 **注释**（ ） 为规则添加注释。

步骤 6 **组覆盖**- 点击列出所有规则组类别的 **组覆盖** 层。系统将显示包含说明、覆盖和已启用组等内容的顶级父规则组。父规则组无法更新，且为只读。只能更新枝叶规则组。在每个规则组中，您可以遍历到最后一个枝叶组。在每个组中，您可以覆盖、包含和排除规则组。在枝叶规则组中，您可以：

- 搜索规则组 - 使用搜索字段输入关键字并搜索规则组。
- 在左侧面板中，您可以选择任何预设过滤器选项来搜索规则组：
  - 全部 - 用于显示所有规则组。
  - 已排除 - 适用于已排除的组。
  - 已包含 - 适用于已包含的组。
  - 已覆盖 - 适用于已覆盖规则组配置。
- 设置规则组的安全级别 - 在左侧窗格中导航到所需的规则组并点击它。点击规则组 **安全级别** 旁边的 **编辑**，以根据系统定义的规则设置提高或降低安全级别。

  在 **编辑安全级别** 对话框中，您可以选择点击 **恢复为默认值**，这将恢复您所做的更改。

  管理中心 自动更改已配置安全级别的规则组规则的操作。在 **规则覆盖** 层，每次更改安全级别时，请注意 **预设** 中阻止规则和禁用规则的计数。

- 您可以对安全级别进行批量更改，以更改特定规则类别中所有规则组的安全级别。批量安全级别适用于具有多个规则组的规则组。批量更新规则组后，您仍然可以更新其中任何关联规则组的安全级别。

  规则组中可以有 **混合** 的安全级别； **混合** 表示子组包含父规则组内的混合安全级别。

- 已包括或排除规则组 - 显示的规则组是与系统提供的基本入侵策略关联的默认规则组。可以在入侵策略中包括和排除规则组。已从入侵策略中删除已排除的规则组，并且其规则不会应用于流量。有关在 管理中心中上传自定义规则的信息，请参阅 将自定义规则添加到规则组。

  排除规则组：

  1. 导航规则组窗格，然后选择要排除的规则组。
  2. 点击右侧窗格中的 **排除** 超链接。
  3. 点击 **排除**。

  要包括具有上传的自定义规则的新规则组或先前排除的规则组，请执行以下操作：

  1. 点击规则组过滤器下拉列表旁边的 **添加** (+) 。
  2. 选择要添加的所有规则组旁边的复选框。
  3. 点击**保存**。

- 对于枝叶规则组，点击 **覆盖** 列标题下的 图标可查看规则操作跟踪，其中描述了由于入侵规则的基本策略和组覆盖而可以分配的覆盖规则操作的顺序。可以从基本策略配置或用户组覆盖中获取规则操作。用户组覆盖优先级介于两者之间；优先级是指分配给规则组的最终覆盖操作。
- 点击 **规则计数** 列标题下的规则计数（数字），查看属于规则组的规则摘要。

步骤 7 **建议**- 如果要生成和应用思科建议的规则，请点击 **建议** 层。建议使用主机数据库来基于已知漏洞启用或禁用规则。

步骤 8 **规则覆盖** - 点击**规则覆盖 (Rule Overrides)** 层以选择任何预设来查看规则，这些预设设置为警报、阻止、禁用、覆盖、重写、通过、删除或拒绝。

- **设置方式** 列按状态（基本策略）显示默认设置，或按组覆盖、规则覆盖或建议显示修改后的规则状态。**所有规则** 中的 **设置者** 列（位于左侧窗格中）根据优先级顺序显示规则操作覆盖操作的轨迹。规则操作的优先级顺序为规则覆盖 > 建议 > 组覆盖 > 基本策略。
- 修改 **规则操作**-要修改规则操作，请选择以下任一操作：
  - 批量编辑 - 选择一个或多个规则，然后从 **规则操作** 下拉列表中选择所需的操作；然后点击 **保存**。

    注释
    仅前 500 条规则支持批量规则操作更改。

  - 单个规则编辑-从 **规则操作** 栏的下拉框中选择规则的操作。

  规则操作是：

  - **阻止**-生成事件，阻止此连接中的当前匹配数据包和所有后续数据包。
  - **警报**-仅对匹配的数据包生成事件，而不丢弃数据包或连接。
  - **禁用**-不针对此规则匹配流量。不生成事件。

- **恢复为默认**-恢复为系统默认操作。
- **通过**-不生成事件，允许数据包通过，而且不使用任何后续 Snort 规则进行进一步评估。

  注释
  “通过”操作仅适用于自定义规则，不适用于系统提供的规则。

- **丢弃**-生成事件，丢弃匹配的数据包，但不阻止此连接上的后续流量。
- **反对**-生成事件，丢弃匹配的数据包，阻止此连接上的后续流量，并将 TCP 重置事件或无法连接的 ICMP 端口发送到源和目的主机。

  与客户端或服务器相关的不同防火墙模式和 *IP* 地址或源或目标中的拒绝行为：在路由、内联和桥接接口的情况下，Snort 会向客户端和服务器发送 RST 数据包。Snort 发送两个 RST 数据包。客户端方向的 RST 数据包将源设置为服务器的 IP，目的设置为客户端的 IP。服务器方向的 RST 数据包将源设置为客户端的 IP，目的设置为服务器的 IP。

- **重写**-生成事件，并根据规则中的替代选项覆盖数据包内容。

有关 IPS 规则操作日志记录，请参阅 规则操作日志记录，第 7 页。

如果有 **反应** 规则转换为警报操作。

步骤 9 点击 **摘要** 层可查看当前策略更改的整体视图。策略摘要页面包含以下信息：

- 策略的规则分布，即活动规则、禁用规则等。
- 用于导出策略并生成入侵策略报告的选项。
- 基础策略详细信息。
- 生成建议的选项。
- 显示已覆盖的组列表的组覆盖。
- 显示已覆盖的规则列表的规则覆盖。
- 在 **摘要** 层中，点击？图标可打开解释 Snort 分层概念的 Snort 帮助程序指南的弹出窗口。

要更改基本策略，请参阅 更改入侵策略的基本策略，第 8 页。

注释
您可以导航至 **对象** > **入侵规则**，然后点击 **Snort 3 所有规则** 选项卡并遍历所有入侵规则组。父规则组列出关联的子组和规则计数。

下一步做什么

部署配置更改；请参阅部署配置更改。

规则组报告

规则组反映在生成的入侵事件中，并且还会调出 MITRE 策略和技术。有用于 MITRE 策略和技术以及用于入侵事件的非 MITRE 规则组的列。要访问入侵事件，请在 管理中心 中转到**分析 (Analysis)** > **入侵 (Intrusions)** > **事件 (Events)**，然后点击**事件表视图 (Table View of Events)** 选项卡。您还可以在 **统一事件** 查看器中查看入侵事件字段。在 **分析** 选项卡中，点击 **统一事件**。

在 **入侵事件** 页面中，为规则组报告添加了以下字段。请注意，您必须明确启用上述列。

- MITRE ATT&CK
- 规则组

有关这些字段的信息，请参阅 *Cisco Firepower Management Center* 管理指南， *7.3* 版中 入侵事件字段 的部分。

规则操作日志记录

从 管理中心 7.2.0 开始，在 **入侵事件** 页面中，**内联结果** 列显示与应用于规则的 IPS 操作相同的名称，以便您可以查看应用于匹配规则的流量的操作。

对于 IPS 操作，下表显示了 **入侵事件** 页面的 **内联结果** 列中显示的事件，以及 **统一事件** 页面中 **入侵事件** 类型的 **操作** 列中显示的事件。

Snort 3 的 **IPS** 操作	内联结果 - 管理中心 **7.1.0** 及更早版本	内联结果 -管理中心 **7.2.0** 及更高版本
警报	通过	警报
阻止	已丢弃/将已丢弃/部分丢弃	阻止/将阻止/部分阻止
丢弃 (Drop)	已丢弃/将已丢弃	丢弃/将丢弃
拒绝	已丢弃/将已丢弃	拒绝/将拒绝
重写	允许	重写

重要事项

- 如果规则没有“替换”选项，则 **重写** 操作显示为 **将重写**。
- 如果指定了“替换”选项，但 IPS 策略处于检测模式或设备处于内联 TAP/被动模式，则 **重写** 操作也将显示为 **将重写** 。

注释 在向后兼容的情况下（管理中心 7.2.0 管理 威胁防御 7.1.0 设备），所提及的事件仅适用于警报 IPS 操作，其中 **通过** 显示为事件的 **警报** 。对于所有其他操作， 管理中心 7.1.0 的事件适用。

更改入侵策略的基本策略

可以选择其他系统提供的策略或自定义策略作为基本策略。

可以链接最多五个自定义策略，这五个策略中有四个使用其余四个之一以前创建的策略作为其基本策略；第五个策略必须使用系统提供的策略作为其基础。

过程

步骤 1 依次选择**策略** > **入侵**。

步骤 2 点击要配置的入侵策略旁边的 **编辑** ( )。

步骤 3 从 **基本策略** 下拉列表中选择策略。

步骤 4 点击**保存 (Save)**。

下一步做什么

部署配置更改；请参阅部署配置更改。

管理入侵策略

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

- 一些访问控制策略和设备使用入侵策略来检查流量
- 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 依次选择**策略** > **入侵**。

步骤 2 管理入侵策略：

- 创建 - 点击**创建策略 (Create Policy)**；请参阅创建自定义 Snort 3 入侵策略 ， 第 2 页。
- 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。

- 编辑入侵策略详细信息 - 点击要编辑的策略旁边的 **编辑** (✎)。您可以编辑入侵策略的 **名称**、**检测模式**和 **基本策略** 。
- 编辑入侵策略设置 - 点击 **Snort 3 版本**；请参阅 编辑 Snort 3 入侵策略，第 3 页。
- 导出 - 如果要导出入侵策略以在另一个 管理中心上导入，请点击导出；请参阅最新版本的 *Cisco Secure Firewall Management Center* 配置指南中的 导出配置 主题。
- 部署 - 选择 **部署** > **部署**；请参阅 部署配置更改。
- 报告 - 请点击 **报告**；请参阅最新版本的 *Cisco Secure Firewall Management Center* 配置指南中的 生成当前策略报告 主题。生成两个报告，每个策略版本一个。

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

Cisco 通过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 Cisco Talos 情报组 (Talos) 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管理中心。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管理中心数据库。

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；请参阅最新版本的 *Cisco Secure Firewall Management Center* 配置指南中的 访问控制规则组件 主题。

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，或选择 **无** 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；请参阅部署配置更改。

部署配置更改

更改配置后，将其部署到受影响的设备。

注释 本主题介绍部署配置更改的基本步骤。我们强烈建议您在继续执行这些步骤之前，参考最新版本的 *Cisco Secure Firewall Management Center* 指南 中的 部署配置更改 主题，了解部署更改的前提条件和影响。

注意 在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。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不进一步检查而直接通过，取决于目标设备处理流量的方式。

过程

步骤 1 在 Cisco Secure Firewall Management Center 菜单栏中，点击 **部署** ，然后选择 **部署**。

GUI 页面列出了具有 **待处理** 状态的过期配置的设备。

- **修改者**列列出了修改策略或对象的用户。展开设备列表以参照每个策略列表查看修改了策略的用户。

  注释
  没有为已删除的策略和对象提供用户名。

- **检查中断** 列指示在部署过程中是否可能导致设备中的流量检查中断。

  如果设备的此为空白，则表明在部署过程中该设备上不会出现流量检查中断。

- **上次修改时间** 列指定上次更改配置的时间。
- **预览**列允许您预览下一次要部署的更改。
- **状态**列提供每个部署的状态。

步骤 2 识别并选择要部署配置更改的设备。

- 搜索 - 在搜索框中搜索设备名称、类型、域、组或状态。
- 展开 - 点击 **展开箭头**（ ） 以查看要部署的设备特定的配置更改。

  选中设备旁边的复选框时，系统会推送对设备进行的所有更改并在设备下列出这些更改以进行部署。但是，您可以使用 **策略选择**（ ） 选择部署个别或指定策略或配置，而保留其余的更改不予部署。

  注释
  - 当 **检查中断** 列中的状态指示（**是**）部署会中断威胁防御 设备上的检查并可能中断流量时，展开的列表将用 **检查中断**（ ）指示导致中断的特定配置。
  - 当接口组、安全区或对象发生更改时，受影响的设备在 管理中心中显示为过期。为确保这些更改生效，包含这些接口组、安全区或对象的策略也需要随这些更改一起部署。受影响的策略在 管理中心的 **预览**页上显示为过期。

步骤 3 点击 **部署**。

步骤 4 如果系统在要部署的更改中发现错误或警告，则会在**验证消息**窗口中显示它们。要查看完整详细信息，请点击警告或错误前的箭头图标。

有以下选项可供选择：

- 部署 - 继续部署而无需解决警告情况。如果系统识别错误，则无法继续。

- 关闭 - 退出而不部署。解决错误和警告情况，并尝试重新部署该配置。

下一步做什么

在部署过程中，如果有部署失败，则可能会影响流量。不过，这取决于某些条件。如果部署中存在特定的配置更改，则部署失败可能导致流量中断。有关部署过程的详细信息，请参阅 *Cisco Secure Firewall Management Center* 配置指南中的部署配置更改主题。

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。