网络分析和入侵策略的高级访问控制设置

以下主题介绍如何配置网络分析和入侵策略的高级访问控制设置：

关于网络分析和入侵策略的高级访问控制设置

访问控制策略中的多项高级设置可监管需要特定专门技术才能做出的入侵检测和防御配置。高级设置通常几乎不需要修改，并非在每个部署中都出现。

网络分析和入侵策略的高级访问控制设置的要求和前提条件

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

在识别流量之前检查通过的数据包

对于某些功能（包括 URL 过滤、应用检测、 速率限制 和智能应用绕行），必须通过几个数据包才能建立连接，并使系统能够识别流量并确定哪个访问控制规则（如果任何）将处理该流量。

您必须明确配置访问控制策略，以检查这些数据包，防止其到达目的地并生成任何事件。请参阅指定策略以处理在流量识别之前通过的数据包，第 2 页。

一旦系统识别应处理连接的访问控制规则或默认操作后，相应地处理和检测连接中剩余的数据包。

处理在流量识别之前通过的数据包的最佳实践

- 为访问控制策略指定的默认操作不会应用于这些数据包。
- 相反，请使用以下准则为访问控制策略的“高级”设置中的“在**确定访问控制规则之前使用的入侵策略设置**选择值。
  - 您可以选择系统创建或自定义入侵策略。例如，您可以选择 **平衡安全和连接**。
  - 出于性能原因，除非您有充分的理由，否则此设置应与访问控制策略的默认操作集匹配。
  - 如果系统不执行入侵检查（例如，在仅发现部署中），请选择 **无活动规则**。系统不会检查这些初始数据包，并且允许它们通过。
  - 默认情况下，此设置使用默认变量集。确保这符合您的用途。有关信息，请参阅变量集。
  - 与第一个匹配网络分析规则关联的网络分析策略预处理您选择的策略的流量。如果没有网络分析规则，或者无任何网络分析规则匹配，则使用默认网络分析策略。

指定策略以处理在流量识别之前通过的数据包

注释 此设置有时称为 默认入侵策略。（这与访问控制策略的默认操作不同。）

开始之前

查看这些设置的最佳实践。请参阅处理在流量识别之前通过的数据包的最佳实践，第 2 页。

过程

步骤 1 在访问控制策略编辑器中，点击 **高级**，然后点击 **网络分析** 和 **入侵策略** 旁边的 **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。如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 2 从**确定访问控制规则之前使用的入侵策略 (Intrusion Policy used before Access Control rule is determined)** 下拉列表中选择入侵策略。

如果选择用户创建的策略，则可以点击 **编辑** (✎) 在新窗口中编辑该策略。无法编辑系统提供的策略。

步骤 3 或者，从**入侵策略变量集 (Intrusion Policy Variable Set)** 下拉列表中选择其他变量集。您还可以点击变量集旁边的 **编辑** (✎) 以创建和编辑变量集。如果您未更改变量集，系统会使用默认的变量集。

步骤 4 点击**确定 (OK)**。

步骤 5 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。

相关主题

变量集

网络分析策略的高级设置

网络分析策略监管如何解码和预处理流量，以便进一步对其进行评估，特别适用于可能表明入侵尝试的异常流量。此流量预处理发生在安全智能匹配和流量解密之后，但是，发生在入侵策略对数据包进行详细检查之前。默认情况下，系统提供的“平衡安全性和连接”(Balanced Security and Connectivity) 网络分析策略是默认网络分析策略。

提示 系统提供的 Balanced Security and Connectivity 网络分析策略和 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。

调整预处理的一个简单方法是创建并使用自定义网络分析策略作为默认值。对于复杂部署的高级用户，可以创建多个网络分析策略，每个策略定制为以不同方式预处理流量。然后，可以配置系统使用这些策略管理使用不同的安全区域、网络或 VLAN 的流量的预处理。

为此，请向访问控制策略中添加自定义网络分析规则。网络分析规则只是指定如何预处理与这些限制条件匹配的流量的一组配置和条件。可在现有访问控制策略的高级选项中创建和编辑网络分析规则。每条规则只属于一个策略。

每条规则均有：

- 一组规则条件，用于识别想要预处理的特定流量
- 一条关联的网络分析策略，想要用来预处理符合所有规则条件的流量

在系统预处理流量时，其将数据包按照规则编号自上而下的顺序与网络分析规则相匹配。不与任何网络分析规则匹配的流量由默认网络分析策略预处理。

设置默认网络分析策略

您可以选择系统或用户创建的策略。

注释 如果禁用预处理器，但是系统需要根据已启用的入侵或预处理器规则评估预处理的数据包，则系统将自动启用和使用预处理器，尽管它在网络分析策略 Web 界面中保持禁用。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。由于预处理和入侵检测如此密切相关，因此，请**务必**小心确保允许网络和入侵策略检测每个数据包，以实现互补。

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)**，然后点击“网络分析和入侵策略”(Network Analysis and Intrusion Policies) 旁边的 **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。如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 2 从 **Default Network Analysis Policy** 下拉列表中，选择一条默认网络分析策略。

如果选择用户创建的策略，则可以点击 **编辑** () 在新窗口中编辑该策略。无法编辑系统提供的策略。

步骤 3 点击**确定 (OK)**。

步骤 4 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。

相关主题

自定义策略的限制

网络分析规则

在访问控制策略的高级设置中，您可以使用网络分析规则定制网络流量的预处理配置。

网络分析规则从 1 开始进行编号。在系统预处理流量时，它将数据包按照升序规则编号自上而下的顺序与网络分析规则相匹配，然后根据所有条件都匹配的第一个规则预处理流量。

您可以向规则中添加区域、网络和 VLAN 标记条件。如果不为规则配置特定条件，系统将不基于此标准匹配流量。例如，一条包含网络条件但不含区域条件的规则根据其源 IP 地址或目标 IP 地址评估流量，不管其进出接口如何。不与任何网络分析规则匹配的流量由默认网络分析策略预处理。

网络分析策略规则条件

通过规则条件，您可以微调网络分析策略，以您要控制的用户和网络为目标。有关详细信息，请参阅以下各节之一：

相关主题

安全区域规则条件
网络规则条件
VLAN 标记规则条件

安全区域规则条件

安全区域可对网络进行分段，以通过跨多个设备将接口分组来帮助管理和分类流量。

安全区域可根据其源和目标安全区域控制流量。如果将源区域和目标区域均添加到区域条件中，则匹配流量必须源自其中一个源区域的接口，并通过其中一个目标区域的接口流出。

正如区域中的所有接口都必须为同一类型（均为内联、被动、交换或路由），区域条件中使用的所有区域也必须为同一类型。由于被动部署的设备不会传输流量，因此不能使用具有被动接口的区域作为目标区域。

尽可能将匹配条件减少，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的 各 组合。

提示 按区域限制规则是提高系统性能的一种最佳方式。如果规则不适用于通过设备任意接口的流量，则该规则不影响该设备的性能。

安全区域条件和多租户

在多域部署中，在祖先域中创建的区域可以包含位于不同域中的设备上的接口。在后代域中配置区域条件时，您的配置仅适用于可以看到的接口。

网络规则条件

网络使用内部信头按流量的源和目标 IP 地址来控制流量。使用外部报头的隧道规则具有隧道终端条件而不是网络条件。

您可以使用预定义对象构建网络条件，或手动指定单个 IP 地址或地址块。

尽可能将匹配条件减少，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的 各 组合。

注释 您 不能 在身份规则中使用 FDQN 网络对象。

VLAN 标记规则条件

注释 访问规则中的 VLAN 标记仅适用于内联集。带 VLAN 标记的访问规则与防火墙接口上的流量不匹配。

VLAN 规则条件可控制 VLAN 标记的流量，包括 Q-in-Q（堆栈 VLAN）流量。系统使用最内层的 VLAN 标记过滤 VLAN 流量，但不包括预过滤器策略，因为它在其规则中使用最外层的 VLAN 标记。

请注意以下 Q-in-Q 支持：

- Firepower 4100/9300 上的威胁防御 -不支持 Q-in-Q （仅支持一个 VLAN 标记）。
- 所有其他型号上的威胁防御 ：
  - 内联集和被动接口-支持 Q-in-Q，最多2个 VLAN 标记。
  - 防火墙接口-不支持 Q-in-Q （仅支持一个 VLAN 标记）。

可以使用预定义对象构建 VLAN 条件，或手动输入从 1 到 4094 之间的任意 VLAN 标记。使用连字符可指定 VLAN 标记范围。

在集群中，如果遇到 VLAN 匹配问题，请编辑访问控制策略高级选项“传输/网络预处理器设置”(Transport/Network Preprocessor Settings)，然后选择**跟踪连接时忽略 VLAN 信头 (Ignore the VLAN header when tracking connections)** 选项。

配置网络分析规则

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)**，然后点击“网络分析和入侵策略”(Network Analysis and Intrusion Policies) 旁边的 **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。如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

提示
点击**网络分析策略列表 (Network Analysis Policy List)** 以查看和编辑现有自定义网络分析策略。

步骤 2 在 **Network Analysis Rules** 旁，点击指明您所拥有的自定义规则数量的语句。

步骤 3 点击**添加规则 (Add Rule)**。

步骤 4 通过点击与要添加的条件来配置规则条件。

步骤 5 点击**网络分析 (Network Analysis)**，并选择要用于预处理匹配此规则的流量的**网络分析策略 (Network Analysis Policy)**。

点击 **编辑** (✎)，在新窗口中编辑自定义策略。无法编辑系统提供的策略。

步骤 6 点击**添加 (Add)**。

下一步做什么

- 部署配置更改；请参阅 部署配置更改。

管理网络分析规则

网络分析规则只是指定如何预处理与这些限制条件匹配的流量的一组配置和条件。可在现有访问控制策略的高级选项中创建和编辑网络分析规则。每条规则只属于一个策略。

过程

步骤 1 在访问控制策略编辑器中，点击**高级 (Advanced)**，然后点击“入侵和网络分析策略”(Intrusion and Network Analysis Policies) 部分旁边的 **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。如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

步骤 2 在 **Network Analysis Rules** 旁，点击指明您所拥有的自定义规则数量的语句。

步骤 3 编辑您的自定义规则。您有以下选择：

- 要编辑某条规则的条件或更改该规则调用的网络分析策略，请点击该规则旁的 **编辑** ()。
- 要更改某条规则的评估顺序，请点击该规则并将其拖至正确的位置。要选择多条规则，请使用 Shift 和 Ctrl 键。
- 要删除规则，点击规则旁边的 **删除** ()。

提示
右键点击规则会显示情景菜单，通过该菜单可剪切、复制、粘贴、编辑、删除网络分析规则和添加新的网络分析规则。

步骤 4 点击**确定 (OK)**。

步骤 5 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。

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。