网络分析策略使用入门

以下主题介绍如何开始使用网络分析策略：

网络分析策略基础知识

网络分析策略管理许多流量预处理选项，并供访问控制策略中的高级设置调用。网络分析相关预处理发生在安全情报匹配和 SSL 解密之后进行，但在入侵或文件检查开始之前进行。

默认情况下，系统使用平衡的安全性和连接性网络分析策略预处理由访问控制策略处理的所有流量。但是，您可以选择不同的默认网络分析策略执行此预处理。为方便您使用，系统提供多种无法修改的网络分析策略供选择，这些策略由Talos情报小组针对安全性和连接的特定平衡专门进行过调整。您也可以用自定义预处理设置创建自定义网络分析策略。

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。网络分析和入侵策略相互配合，检查您的流量。

您也可以通过以下方式根据特定安全区域、网络和 VLAN 定制流量预处理选项：创建多个自定义网络分析策略，然后分配它们预处理不同流量。

网络分析策略的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

网络分析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)

管理网络分析策略

过程

步骤 1 选择**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 管理网络分析策略：

- 比较 - 点击**比较策略 (Compare Policies)**；请参阅比较策略。
- 创建 - 如果要创建新的网络分析策略，请点击**创建策略 (Create Policy)**。

  系统将创建两个版本的网络分析策略：**Snort 2 版本**和 **Snort 3 版本**。

- 删除 - 如果要删除网络分析策略，请点击 **删除**（）， 然后确认是否要删除策略。如果网络分析策略被访问控制策略引用，则无法删除该网络分析策略。

  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。

- 部署 - 选择**部署** > **部署**；请参阅部署配置更改。

- 编辑 - 如果要编辑现有网络分析策略，请点击 **编辑**（），然后如网络分析策略设置和缓存的更改，第 6 页中所述继续操作。

  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。

- 报告 - 点击**报告**（）；请参阅生成当前策略报告。

创建网络分析策略

所有 管理中心 现有的网络分析策略均可用于相应的 Snort 2 和 Snort 3 版本。当您创建新的网络分析策略时，会同时创建 Snort 2 版本和 Snort 3 版本。

过程

步骤 1 转至**策略 (Policies)** > **入侵 (Intrusion)** > **网络分析策略 (Network Analysis Policies)**。

步骤 2 点击**创建策略**。

步骤 3 输入**名称 (Name)** 和**描述 (Description)**。

步骤 4 选择**基本策略 (Base Policy)**，然后点击**保存 (Save)**。

新的网络分析策略使用其对应的 **Snort 2 版本**和 **Snort 3 版本**创建。

修改网络分析策略

您可以修改网络分析策略以更改其名称、说明或基本策略。

过程

步骤 1 转至 **策略** > **入侵** > **网络分析策略**。

步骤 2 点击**编辑 (Edit)** 以更改名称、说明、检测模式或基本策略。

注意 **检测模式弃用：** 从管理中心 7.4.0 开始，对于网络分析策略 (NAP)， **检测** 检查模式已弃用，并将在即将推出的版本中删除。

检测 模式旨在用作测试模式，以便您可以启用检测并查看它们在网络中的行为，然后再将其设置为丢弃流量，即显示将被丢弃的流量。

此行为已得到改进，其中所有检查器丢弃都由规则状态控制，并且您可以设置每个丢弃以生成事件。这样做是为了在配置规则状态以丢弃流量之前对其进行测试。由于我们现在可以对 Snort 3 中的流量丢弃进行精细控制，因此 **检测** 模式只会增加产品的复杂性，不需要，因此检测模式已弃用。

如果将**检测**模式下的 NAP 更改为**预防**，则处理入侵事件流量并具有结果 “会被丢弃” 的 NAP 现在将为“已丢弃”，相应的流量将丢弃来自这些事件的流量。这适用于 GID 不是 1 或 3 的规则。GID 1 和 3 是文本/编译规则（通常由 Talos 提供或从您的自定义/导入规则中提供），所有其他 GID 都是异常检测。这些是在网络中触发的比较少见的规则。更改为 **预防** 模式不太可能对流量产生任何影响。您只需禁用适用于已丢弃流量的入侵规则，并将其设置为仅生成或禁用。

我们建议您选择 **预防** 作为检测模式，但如果您选择 **预防**，则无法恢复到 **检测** 模式。

注释 如果编辑网络分析策略名称、说明、基本策略和检测模式，编辑内容将同时应用于Snort 2 和 Snort 3 版本。如果要更改特定版本的检测模式，可以在相应版本的网络分析策略页面中执行此操作。

步骤 3 点击**保存 (Save)**。

为 Snort 2 的自定义网络分析策略创建

当创建新的网络分析策略时，必须为其提供唯一的名称，指定基本策略并选择内联模式。

基本策略定义网络分析策略的默认设置。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。

网络分析策略的内联模式允许预处理器修改（标准化）和丢弃流量，从而使攻击者避开检测的可能性最小化。请注意，在被动部署中，无论内联模式如何设置，系统都无法影响流量传输。

相关主题

基本层
内联部署中预处理器流量的修改，第 8 页
创建自定义网络分析策略，第 4 页
编辑网络分析策略，第 6 页

创建自定义网络分析策略

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 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 点击**创建策略**。如果在另一策略中有未保存的更改，当系统提示您返回**网络分析策略 (Network Analysis Policy)** 页面时，请点击**取消 (Cancel)**。

步骤 3 在**名称 (Name)** 中输入唯一的名称。

在多域部署中，策略名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的策略名称的冲突。

步骤 4 输入**说明 (Description)**（可选）。

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自定义策略作为您的基本策略。

注意 在配置自定义 NAP 时，如果选择**最大检测 (Maximum Detection)** 作为**基本策略**，则性能可能会下降。建议在部署到生产环境之前检查并测试此设置。

步骤 6 如果要允许预处理器影响内联部署中的流量，请启用**内联模式 (Inline Mode)**。

步骤 7 要创建策略：

- 点击**创建策略 (Create Policy)**创建新策略并返回**网络分析策略 (Network Analysis Policy)** 页面。新策略的设置与其基本策略相同。
- 点击**创建并编辑策略 (Create and Edit Policy)**，创建策略并在高级网络分析策略编辑器中将其打开进行编辑。

Snort 2 的网络分析策略管理

在“网络分析策略”页面（或**策略 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)**或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**）上，可以查看当前的自定义网络分析策略以及以下信息：

- 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**内联模式 (Inline Mode)** 设置，该设置允许预处理器影响流量
- 哪些访问控制策略和设备使用网络分析策略来预处理流量
- 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

除了您创建的自定义策略之外，系统还提供两种自定义策略：初始内联策略和初始被动策略。这两个网络分析策略使用“平衡安全性和连接”(Balanced Security and Connectivity) 网络分析策略作为其

基本策略。两者之间的唯一区别在于其内联模式，在内联策略中允许预处理器影响流量，但在被动策略中禁用了该功能。您可以编辑并使用系统提供的这些自定义策略。

请注意，如果您的 Firepower 系统用户帐户的角色被限制为“入侵策略”(Intrusion Policy) 或“修改入侵策略”(Modify Intrusion Policy)，则您可以创建和编辑网络分析策略及入侵策略。

相关主题

创建自定义网络分析策略，第 4 页
编辑网络分析策略，第 6 页

网络分析策略设置和缓存的更改

当您创建新的网络分析策略时，它具有与其基本策略相同的设置。

当您定制网络分析策略时，特别是在禁用预处理器时，请记住某些预处理器和入侵规则要求首先以某种方式对流量进行解码或预处理。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。

注释 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。

系统为每个用户缓存一条网络分析策略。在编辑网络分析策略时，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。

相关主题

策略如何检查流量是否存在入侵
自定义策略的限制

编辑网络分析策略

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 (Policies)** > **访问控制 (Access Control)**，然后点击**网络分析策略 (Network Analysis Policy)** 或**策略** > **访问控制** > **入侵**，然后点击 **网络分析策略**。

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

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

步骤 3 点击想要配置的网络分析策略旁的 **编辑**（）。

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 4 编辑网络分析策略：

- 更改基本策略 - 如果要更改基本策略，请从“策略信息”(Policy Information) 页面上的**基本策略 (Base Policy)** 下拉列表中选择一个基本策略。
- 管理策略层 - 如果要管理策略层，请点击导航面板中的**策略层 (Policy Layers)**。
- 修改预处理器 - 如果要启用、禁用或编辑预处理器的设置，请点击导航面板中的**设置 (Settings)**。
- 修改流量 - 如果要允许预处理器修改或丢弃流量，请选中“策略信息”(Policy Information) 页面上的**内联模式 (Inline Mode)** 复选框。
- 查看设置 - 如果要查看基本策略中的设置，请点击“策略信息”(Policy Information) 页面上的**管理基本策略 (Manage Base Policy)**。

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

- 如果希望预处理器生成事件并在内联部署中丢弃攻击性数据包，请启用该预处理器的规则。有关详细信息，请参阅 设置入侵规则状态。
- 部署配置更改；请参阅 部署配置更改。

相关主题

基本层
更改基本策略
Snort 2 的网络分析策略中的预处理器配置 ，第 7 页
内联部署中预处理器流量的修改 ，第 8 页
管理层
冲突和更改：网络分析和入侵策略

Snort 2 的网络分析策略中的预处理器配置

预处理器通过规范化流量和标识协议异常，准备要进行进一步检查的流量。预处理器可以在数据包触发配置的预处理器选项时生成预处理器事件。网络分析策略的基本策略决定了默认情况下启用哪些预处理器及各自的默认配置。

注释 在大多数情况下，配置预处理器要求特定专业知识，并且通常很少需要修改或不需要任何修改。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。

修改预处理器配置要求了解配置及其对网络的潜在影响。

请注意，某些高级传输和网络预处理器设置全局应用于您部署访问控制策略所在的所有网络、区域和 VLAN。可以在访问控制策略中而非网络分析策略中配置这些高级设置。

另请注意，您在入侵策略中配置敏感数据预处理器，用于检测 ASCII 文本形式的信用卡号和社会安全保障号等敏感数据。

相关主题

DCE/RPC 预处理器
DNP3 预处理器
DNS 预处理器
FTP/Telnet 解码器
GTP 预处理器
HTTP 检查预处理器
IMAP 预处理器
内联规范化预处理器
IP 分片重组预处理器
Modbus 预处理器
数据包解码器
POP 预处理器
敏感数据检测基础知识
SIP 预处理器
SMTP 预处理器
SSH 预处理器
SSL 预处理器
Sun RPC 预处理器
TCP 数据流预处理
UDP 数据流预处理
自定义策略的限制

内联部署中预处理器流量的修改

在内联部署中（即，使用路由接口、交换接口、透明接口或内联接口对将相关配置部署到设备），某些预处理器可以修改并阻止流量。例如：

- 内联规范化预处理器将数据包标准化为准备这些数据包，以便由其他预处理器和入侵规则引擎进行分析。您还可以使用预处理器的**允许这些 TCP 选项 (Allow These TCP Options)** 和**阻止无法解析的 TCP 报头异常 (Block Unresolvable TCP Header Anomalies)** 选项阻止某些数据包。
- 系统可以丢弃具有无效校验和的数据包。
- 系统可以丢弃匹配基于速率的攻击防护设置的数据包。

要使网络分析策略中配置的预处理器影响流量，还必须启用并正确配置预处理器，并正确部署内联的受管设备。最后，您必须启用网络分析策略的 **Inline Mode** 设置。

网络分析策略中的预处理器配置说明

当您在网络分析策略的导航面板中选择 **Settings** 时，策略将按类型列出其预处理器。在“设置”(Settings) 页面中，可以启用或禁用网络分析策略中的预处理器，以及访问预处理器配置页面。

必须启用预处理器，这样您才能对其进行配置。当启用预处理器时，该预处理器配置页面的子链接显示在导航面板中**设置 (Settings)** 链接下，并且到配置页的**编辑 (Edit)** 链接显示在“设置”(Settings) 页面上的预处理器旁边。

提示 将预处理器的配置恢复为基本策略中的设置，请点击预处理器配置页面上的**恢复为默认值 (Revert to Defaults)**。出现提示时，请确认您要恢复。

当禁用预处理器时，子链接和**编辑 (Edit)** 链接将不显示，但会保留您的配置。请注意，为了执行其特定分析，许多预处理器和入侵规则要求首先以某种方式对流量进行解码或预处理。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。

如果要评估配置如何在内联部署中起作用，而不会实际修改流量，您可以禁用内联模式。在被动部署或分路模式的内联部署中，系统无法影响流量，无论内联模式设置如何。

注释 禁用内联模式可能会影响入侵事件性能统计数据图表。在内联部署中启用内联模式时，“入侵事件性能”页面（**概述** > **摘要** > **入侵事件性能**）显示表示已规范化和阻止的数据包的图表。如果禁用内联模式，或者在被动部署中，许多图表显示有关系统应当已规范化或丢弃的流量的数据。

注释 在内联部署中，我们建议您启用内联模式并配置已启用 **Normalize TCP Payload** 选项的内联规范化预处理器。在被动部署中，我们建议您使用 自适应配置文件。

相关主题

高级传输/网络预处理器设置

校验和验证

内联规范化预处理器

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。