



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，第 1 页](#)
- [网络分析策略的许可证要求，第 2 页](#)
- [网络分析策略的要求和必备条件，第 2 页](#)
- [管理网络分析策略，第 2 页](#)

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

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，然后点击 网络分析策略或策略 > 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**。

- 对于 Snort 2 版本，请按照为 [Snort 2 的自定义网络分析策略创建](#)，第 11 页中所述继续操作。
- 对于 Snort 3 版本，请按照[创建网络分析策略](#)，第 7 页中所述继续操作。
- 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 13 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](#)。

为 Snort 3 自定义网络分析策略的创建

默认网络分析策略针对典型的网络要求和最佳性能进行了调整。通常，默认网络分析策略足以满足大多数网络要求，您可能不需要自定义策略。但是，当您有特定的网络要求或遇到性能问题时，可以自定义默认网络分析策略。请注意，自定义网络分析策略是一种高级配置，应仅由高级用户或 Cisco 支持人员执行。

Snort 3 的网络分析策略配置是基于 JSON 和 JSO 的数据驱动模型。架构基于 OpenAPI 规范，可帮助您了解支持的检查器、设置、设置类型和有效值。Snort 3 检查器是处理数据包的插件（类似于 Snort 2 预处理器）。网络分析策略配置可以 JSON 格式下载。

在 Snort 3 中，检查器和设置列表与 Snort 2 预处理器和设置列表不存在一对一映射。此外，管理中心中可用的检查器和设置的数量是 Snort 3 支持的检查器和设置的子集。有关 Snort 3 的详细信息，请参阅<https://snort.org/snort3>。有关管理中心中的可用检查器的详细信息，请参阅<https://www.cisco.com/go/snort3-inspectors>。



注释

- 将管理中心升级到 7.0 版本时，在升级后，在 Snort 2 版本的网络分析策略中所做的更改不会迁移到 Snort 3。
- 与入侵策略不同，没有将 Snort 2 网络分析策略设置同步到 Snort 3 的选项。

默认检查器更新

轻量级安全包(LSP)更新可能包含新的检查器或对现有检查器配置的整数范围的修改。安装LSP后，新的检查器和/或更新的范围将在网络分析策略的 **Snort 3** 版本中的**检查器**下供使用。

绑定检查器

绑定检查器定义必须访问和考虑特定检查器时的流程。当流量与绑定程序检查器中定义的条件匹配时，只有该检查器的值/配置才会生效。例如：

对于 *imap* 检查器，当必须访问时，活页夹定义以下条件。即：

- 服务等于 *imap*。
- 角色均一致。

如果满足这些条件，则使用类型 *imap*。

```
▼ binder
185 {
186   "when": {
187     "service": "imap",
188     "role": "any"
189   },
190   "use": {
191     "type": "imap"
192   }
193 },
```

单例检查器

单例检查器包含一个实例。这些检查器不支持添加更多实例，例如多例检查器。单例检查器的设置应用于整个流量，而不是特定的流量段。

例如：

```
{
  "normalizer":{
    "enabled":true,
    "type":"singleton",
    "data":{
      "ip4":{
        "df":true
      }
    }
  }
}
```

多例检查器

多例检查器包含多个实例，您可以根据需要进行配置。这些检查器支持根据特定条件（例如网络、端口和 VLAN）配置设置。一组受支持的设置称为实例。有一个默认实例，您还可以根据特定条件添加其他实例。如果流量与该条件匹配，则应用该实例中的设置。否则，将应用默认实例中的设置。此外，默认实例的名称与检查器的名称相同。

对于多例检查器，当您上传覆盖的检查器配置时，您还需要为 JSON 文件中的每个实例包含/定义匹配的绑定程序条件（必须访问或使用检查器时的条件），否则上传将导致错误。您还可以创建新实例，但请确保为您创建的每个新实例包含绑定程序条件，以避免错误。

例如：

- 修改了默认实例的多例检查器。

```
{
  "http_inspect":{
    "enabled":true,
    "type":"multiton",
    "instances":[
      {
        "name":"http_inspect",
        "data":{
          "response_depth":5000
        }
      }
    ]
  }
}
```

- 修改默认实例和默认绑定程序的多例检查器。

```
{
  "http_inspect":{
    "enabled":true,
    "type":"multiton",
    "instances":[
      {
        "name":"http_inspect",
        "data":{
          "response_depth":5000
        }
      }
    ]
  },
  "binder":{
```

```

    "type": "binder",
    "enabled": true,
    "rules": [
      {
        "use": {
          "type": "http_inspect"
        },
        "when": {
          "role": "any",
          "ports": "8080",
          "proto": "tcp",
          "service": "http"
        }
      }
    ]
  }
}

```

- 多例检查器，其中添加了自定义实例和自定义绑定程序。

```

{
  "http_inspect": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "name": "http_inspect1",
        "data": {
          "response_depth": 5000
        }
      }
    ]
  },
  "binder": {
    "type": "binder",
    "enabled": true,
    "rules": [
      {
        "use": {
          "type": "http_inspect",
          "name": "http_inspect1"
        },
        "when": {
          "role": "any",
          "ports": "8080",
          "proto": "tcp",
          "service": "http"
        }
      }
    ]
  }
}

```

网络分析策略映射

对于网络分析策略，Cisco Talos 提供了映射信息，用于为 Snort 3 版本找到对应的 Snort 2 版本的策略。

此映射可确保 Snort 3 版本的策略具有对应的 Snort 2 版本。

查看网络分析策略映射

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NAP 映射 (**NAP Mapping**)。

步骤 3 展开查看映射 (**View Mappings**) 的箭头。

系统将显示自动映射到 Snort 2 等效策略的 Snort 3 网络分析策略。

步骤 4 点击确定 (**OK**)。

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 从可用选项中选择检测模式 (**Inspection Mode**) 。

- 检测
- 防御

步骤 5 选择基本策略 (**Base Policy**) ， 然后点击保存 (**Save**)。

注释 如果您使用的是 Snort 3 和 SSL 解密或 TLS 服务器身份，请在预防 (**Prevention**) 模式下配置网络分析策略 (NAP)。

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)**。

自定义网络分析策略

您可以根据自己的要求自定义 Snort 3 版本的网络分析策略。

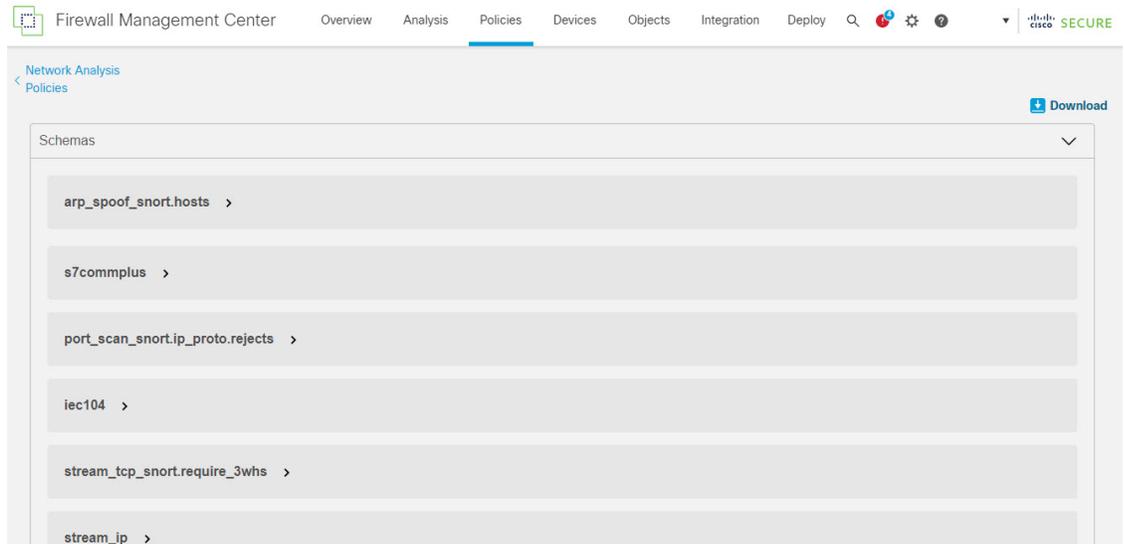
过程

步骤 1 点击网络分析策略的 **Snort 3 版本 (Snort 3 Version)** 中的**操作 (Actions)** 下拉菜单。

系统将显示以下选项：

- 查看架构
- 下载
 - 架构 (Schema)
 - 示例文件/模板
 - 完整配置
 - 覆盖的配置
- 上传
 - 覆盖的配置

步骤 2 点击**查看方案 (View Schema)** 可直接在浏览器中打开方案文件。



步骤 3 在下载 (**Download**) 下，您可以根据需要使用以下选项来下载架构文件、示例文件、完整配置或覆盖配置。

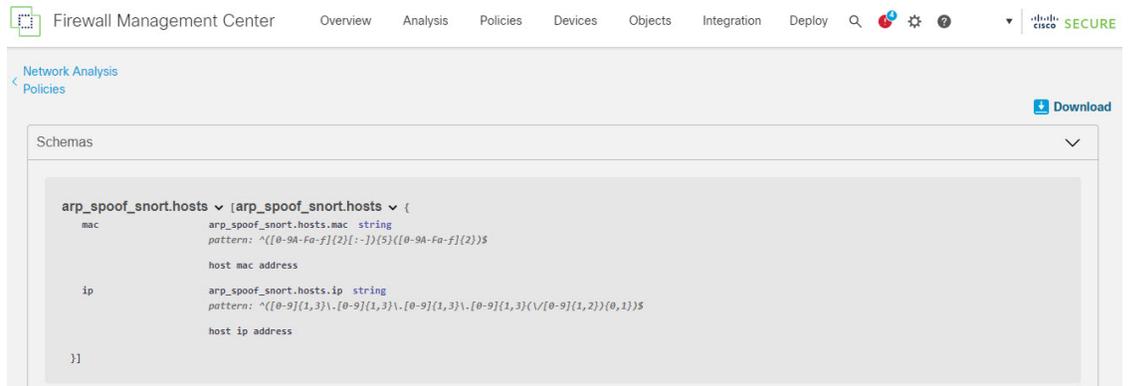
通过这些选项，您可以了解允许的值、范围和模式、现有和默认检查器配置以及覆盖的检查器配置。

a) 点击架构 (**Schema**) 以下载架构文件。

架构文件验证您上传或下载的内容。您可以下载架构文件并使用任何第三方 JSON 编辑器打开它。架构文件可帮助您确定可以为检查器配置的参数及其相应的允许值、范围和要使用的接受模式。

例如，对于 *arp_spoof_snort* 检查器，您可以配置主机。主机包括 *mac* 和 *ip* 地址值。架构文件显示这些值的以下可接受模式。

- **mac** - 模式: `^([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})$`
- **ip** - 模式: `^([0-9]{1,3}\. [0-9]{1,3}\. [0-9]{1,3}\. [0-9]{1,3})|([0-9]{1,3}/[0-9]{1,2}){0,1}$`



您必须根据架构文件中接受的值、范围和模式，才能成功覆盖检查器配置，否则会收到错误消息。

- b) 点击**示例文件/模板 (Sample File / Template)** 以使用包含示例配置的预先存在的模板来帮助您配置检查器。
您可以参考示例文件中包含的示例配置，并进行您可能需要的任何更改。有关信息，请参阅。
- c) 点击**完整配置 (Full Configuration)** 以将整个检查器配置下载到一个文件中。
您可以下载完整配置来查找所需的信息，而不是单独展开检查器。此文件中提供有关检查器配置的所有信息。
- d) 点击**覆盖的配置 (Overridden Configuration)** 以下载已覆盖的检查器配置。
如果尚未覆盖任何检查器配置，则此选项处于禁用状态。当您覆盖检查器配置时，此选项会自动启用，以允许您下载。

步骤 4 要覆盖现有配置，请按照以下步骤操作。

您可以选择使用以下方式覆盖检查器配置。

- 直接在 **管理中心** 上对检查器进行内联编辑。有关如何进行内联编辑的步骤，请参阅。
- 继续按照当前程序使用 **操作 (Actions)** 下拉菜单上传覆盖的配置文件。

如果您选择直接在 **管理中心** 上进行内联编辑，则无需进一步执行当前程序。否则，您必须完全遵循此程序。

- a) 在**检查器 (Inspectors)** 下，展开要覆盖其默认配置的所需检查器。
默认配置显示在左侧列中，被覆盖的配置显示在检查器下的右侧列中。
您可能需要通过在搜索栏中输入任何相关文本来搜索检查器。
- b) 点击**复制到剪贴板 (Copy to clipboard)** 图标，将默认检查器配置复制到剪贴板。
- c) 创建一个 JSON 文件并将默认配置粘贴到其中。
- d) 保留要覆盖的检查器配置，并从 JSON 文件中删除所有其他配置和实例。
您还可以使用**示例文件/模板 (Sample File / Template)** 来了解如何覆盖默认配置。这是一个包含 JSON 片段的示例文件，说明如何为 Snort 3 自定义网络分析策略。有关详细信息，请参阅。
- e) 根据需要对检查器配置进行更改。
验证更改并确保它们符合架构文件。对于多例检查器，请确保所有实例的绑定器条件都包含在 JSON 文件中。有关详细信息，请参阅[为 Snort 3 自定义网络分析策略的创建](#)，第 3 页中的多例检查器。
- f) 如果要复制任何其他默认检查器配置，请将该检查器配置附加到包含覆盖配置的现有文件。
注释 复制的检查器配置必须符合 JSON 标准。
- g) 将覆盖的配置文件保存到您的系统。
- h) 将覆盖的配置上传到 **管理中心**，如下一步中所述。

步骤 5 在**上传 (Upload)** 下，您可以点击**覆盖配置 (Overridden Configuration)** 以上传包含已覆盖配置的 JSON 文件。

注意 仅上传您需要的更改。不应上传整个配置，因为它会使覆盖本质上具有粘性，因此，将不会应用对默认配置的任何后续更改作为 LSP 更新的一部分。

您可以拖放文件，也可以点击浏览到系统中保存的包含覆盖检查器配置的 JSON 文件。

- **合并检查器覆盖 (Merge inspector overrides)** - 如果没有通用检查器，上传文件中的内容会与现有配置合并。如果有通用检查器，则上传文件（用于通用检查器）中的内容优先于之前的内容，并将替换这些检查器的先前配置。
- **替换检查器覆盖 (Replace inspector overrides)** - 删除所有之前的覆盖并替换为上传文件中的新内容。

注意 由于选择此选项会删除之前的所有覆盖，因此请在使用此选项覆盖配置之前做出明智的决定。

如果在上传覆盖的检查器时发生任何错误，您会在上传覆盖的配置文件 (**Upload Overridden Configuration File**) 弹出窗口中看到错误。您还可以下载存在错误的文件，然后修复错误并重新上传文件。

步骤 6 在上传覆盖的配置文件 (**Upload Overridden Configuration File**) 弹出窗口中，点击导入 (**Import**) 按钮以上传覆盖的检查器配置。

上传覆盖的检查器配置后，您会在检查器旁边看到一个橙色圆圈，表示它是一个覆盖的检查器。

此外，检查器下的覆盖配置 (**Overridden Configuration**) 列会显示覆盖的值。

您还可以使用搜索栏旁边的仅显示覆盖 (**Show Overrides Only**) 复选框查看所有已覆盖的检查器。

注释 确保始终下载下载 (**Download**) 下的覆盖配置 (**Overridden Configurations**)，然后打开 JSON 文件并将对检查器配置的任何新更改/覆盖附加到此文件。需要执行此操作，以免丢失旧的覆盖配置。

步骤 7 (可选) 在进行任何新的检查器配置更改之前，备份系统上的覆盖配置文件。

提示 我们建议您在覆盖检查器配置时不时进行备份。

相关主题

[将覆盖的配置恢复为默认配置](#)

[查看具有覆盖的检查器列表](#)

[自定义网络分析策略配置示例](#)

[在网络分析策略页面上搜索检查器](#)

[复制检查器配置](#)

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 16 页

[创建自定义网络分析策略](#)，第 12 页

[编辑网络分析策略](#)，第 13 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 > 访问控制，然后单击 **网络分析策略或策略 > 访问控制 > 入侵**，然后单击 **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**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：

- 单击**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。
- 单击**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 > 访问控制，然后点击 **网络分析策略** 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 12 页

[编辑网络分析策略](#)，第 13 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 > 访问控制，然后点击 网络分析策略或策略 > 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。

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 15 页

[内联部署中预处理器流量的修改](#)，第 16 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。