网络分析策略入门

“网络分析策略入门”一章深入介绍了网络分析策略基础知识、前提条件和管理网络分析策略。它提供有关创建自定义网络分析策略和网络分析策略设置的信息。

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，这些策略由思科 Talos 情报小组 (Talos) 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。（请注意，ASA FirePOWER无法通过 VLAN 限制预处理。）

网络分析策略的许可证要求

威胁防御 许可证

威胁

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
- 入侵管理员

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。

步骤 1 选择以下路径之一来访问网络分析策略。

- **策略** > **访问控制**，然后单击 **网络分析策略**
- **策略** > **访问控制** > **入侵**，然后单击 **网络分析策略**
- **策略** > **入侵** > **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**；请参阅 *Firepower* 管理中心配置指南中的 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**。

  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 *Firepower* 管理中心配置指南中的 *Snort 2* 自定义网络分析策略创建 中所述继续操作。
  - 对于 Snort 3 版本，请按照 为 Snort 3 的自定义网络分析策略创建，第 5 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** 图标，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。

- 编辑 - 如果要编辑现有网络分析策略，请点击 **编辑** 图标。

  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 - 请点击 **报告**；请参阅最新版本的 *Firepower* 管理中心配置指南中的 生成当前策略报告。

网络分析策略的 Snort 3 定义和术语

下表列出了网络分析策略中使用的 Snort 3 概念和术语。

表 *1:* 网络分析策略的 *Snort 3* 定义和术语

术语	说明
检查器	检查器是处理数据包的插件（类似于 Snort 2 预处理器）。
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，该检查器的值/配置才会生效。 有关详细信息，请参阅中 为 Snort 3 的自定义网络分析策略创建，第 5 页的 绑定检查器 。
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匹配该检查器的整个流量，而不是特定的流量段。 有关详细信息，请参阅 为 Snort 3 的自定义网络分析策略创建，第 5 页中的 单例检查器 。

术语	说明
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。 有关详细信息，请参阅 为 Snort 3 的自定义网络分析策略创建，第 5 页中的 多例检查器 。
架构 (Schema)	架构文件基于 OpenAPI JSON 规范，用于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（例如 Swagger 编辑器）将其打开。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。 有关详细信息，请参阅自定义网络分析策略，第 11 页。
示例文件	它是一个预先存在的模板，其中包含可帮助您配置检查器的示例配置。 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。 有关详细信息，请参阅自定义网络分析策略，第 11 页。
完整配置	您可以在一个文件中下载整个检查器配置。 此文件中提供有关检查器配置的所有信息。 完整配置是默认配置（由Cisco Talos 作为 LSP 更新的一部分推出）和自定义 NAP 检查器配置的合并配置。 有关详细信息，请参阅自定义网络分析策略，第 11 页。

术语	说明
覆盖的配置	在网络分析策略页面的 **Snort 3 版本** 中： • 在 **操作** > **上传**下，您可以点击 **覆盖配置** 以上传包含覆盖配置的 JSON 文件。 • 在 **操作** > **上传**下，您可以点击 **覆盖配置** 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。 有关详细信息，请参阅自定义网络分析策略，第 11 页。

相关主题

为 Snort 3 的自定义网络分析策略创建，第 5 页
自定义网络分析策略，第 11 页
网络分析策略映射，第 8 页

为 Snort 3 的自定义网络分析策略创建

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** 下可用。

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

步骤 1 转至 **策略** > **入侵** > **网络分析策略**。

步骤 2 点击 **添加映射**。

步骤 3 展开 **查看映射**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**。

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。

步骤 1 转至 **策略** > **入侵** > **网络分析策略**。

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** 。

- **检测**
- **防御**

步骤 5 选择 **基本策略** ，然后点击 **保存**。

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** 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。

步骤 1 转至 **策略** > **入侵** > **网络分析策略**。

步骤 2 点击 **编辑** 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**。

在网络分析策略页面上搜索检查器

在 Snort 3 版本的网络分析策略页面上，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。

步骤 1 转至网络分析策略的 **Snort 3 版本** 。

步骤 2 在 **搜索** 栏中输入要搜索的检查器名称或任何相关文本。

系统将显示与您搜索的文本匹配的所有检查器。

例如，如果输入 **pop**，则弹出检查器和活页夹检查器在屏幕上显示为匹配结果。

相关主题

自定义网络分析策略配置示例 ， 第 17 页
查看具有覆盖的检查器列表 ， 第 15 页
网络分析策略的 Snort 3 定义和术语 ， 第 3 页
自定义网络分析策略 ， 第 11 页
对检查器进行内联编辑以覆盖配置 ， 第 14 页

复制检查器配置

您可以根据自己的要求复制网络分析策略的 Snort 3 版本的检查器配置。

步骤 1 在网络分析策略的 **Snort 3 版本** 中的 **检查器** 下，展开要为其复制配置的所需检查器。

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。

步骤 2 点击 **复制到剪贴板** 图标，将检查器配置复制到以下一项或两项的剪贴板。

- 左列的 **默认配置**
- 右列的 **覆盖的配置**

步骤 3 将复制的检查器配置粘贴到 JSON 编辑器，以进行您可能需要的任何编辑。

相关主题

自定义网络分析策略 ， 第 11 页

自定义网络分析策略

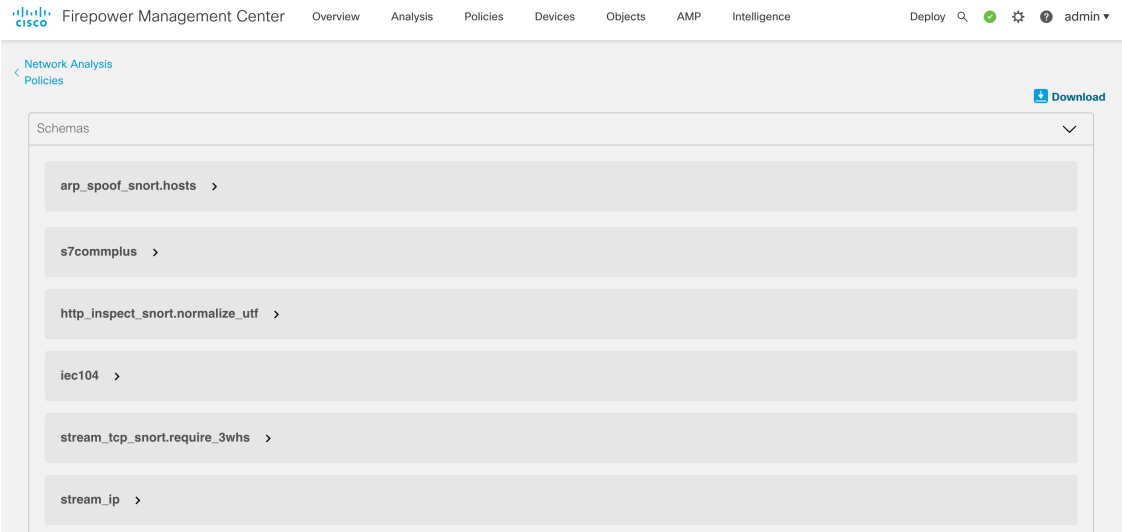
您可以根据自己的要求自定义 Snort 3 版本的网络分析策略。

步骤 1 点击网络分析策略的 **Snort 3 版本** 中的 **操作** 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** 可直接在浏览器中打开方案文件。



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

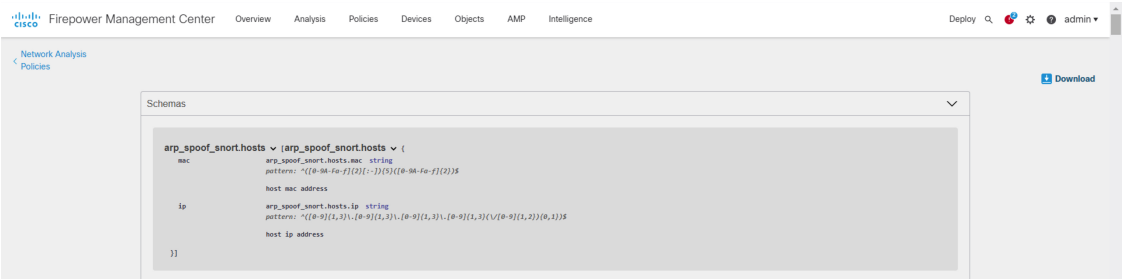
通过这些选项，您可以了解允许的值、范围和模式、现有和默认检查器配置以及覆盖的检查器配置。

a) 点击 **架构** 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})$`
- **ip** – 模式：`^([0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}() /[0-9]{1,2}){0,1})$`



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** 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** 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** 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** 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**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** 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** 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 的自定义网络分析策略创建，第 5 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**下，您可以点击 **覆盖配置** 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** - 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** - 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** 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** 弹出窗口中，点击 **导入** 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** 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** 复选框查看所有已覆盖的检查器。

注释 确保始终下载 **下载**下的 **覆盖配置** ，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，第 15 页
查看具有覆盖的检查器列表，第 15 页
自定义网络分析策略配置示例，第 17 页
在网络分析策略页面上搜索检查器，第 10 页
复制检查器配置 ，第 10 页

对检查器进行内联编辑以覆盖配置

对于 Snort 3 版本的网络分析策略，您可以对检查器配置进行内联编辑，以根据您的要求覆盖配置。

或者，您也可以使用**操作**下拉菜单上传覆盖的配置文件。有关详细信息，请参阅自定义网络分析策略，第 11 页。

步骤 1 在网络分析策略的 **Snort 3 版本** 中的 **检查器** 下，展开要覆盖其默认设置的所需检查器。

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。

步骤 2 在右侧列的 **覆盖配置** 下，点击 **编辑检查器** （铅笔）图标以更改检查器配置。

系统将显示覆盖配置弹出窗口，您可以在其中进行所需的编辑。

注释

- 确保仅保留要覆盖的设置。如果保留的某个设置具有相同值，该字段将变为粘滞状态，这意味着如果将来 Talos 团队更改该设置，系统将保留当前值。
- 如果要添加或删除任何自定义实例，请确保同时在绑定程序检查器中为该实例添加或删除绑定程序规则。

步骤 3 单击**确定 (OK)**。

如果根据 JSON 标准存在任何错误，则会显示错误消息。

步骤 4 点击 **Save** 保存所做的更改。

如果更改符合 OpenAPI 架构规范，则 管理中心 允许您保存配置，否则，系统将显示 **保存覆盖配置时出错** 的弹出窗口。您还可以下载包含错误的文件。

相关主题

自定义网络分析策略，第 11 页
在内联编辑期间恢复未保存的更改，第 14 页
将覆盖的配置恢复为默认配置，第 15 页
自定义网络分析策略配置示例，第 17 页

在内联编辑期间恢复未保存的更改

进行内联编辑以覆盖检查器的配置或恢复检查器的默认配置时，您可以恢复任何未保存的更改。请注意，此操作会将所有未保存的更改恢复为最近保存的值，但不会将配置恢复为检查器的默认配置。

有关如何将配置恢复为默认配置的信息，请参阅将覆盖的配置恢复为默认配置。

步骤 1 在网络分析策略的 **Snort 3 版本** 中的 **检查器** 下，展开要恢复其未保存更改的所需检查器。

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。

步骤 2 在右侧列的 **覆盖配置** 下，点击 **叉号** (X) 图标可恢复检查器的任何未保存的更改。

或者，单击 **取消** 放弃更改。

如果您对检查器配置没有任何未保存的更改，则此选项不可见。

相关主题

将覆盖的配置恢复为默认配置，第 15 页
对检查器进行内联编辑以覆盖配置，第 14 页

查看具有覆盖的检查器列表

您可以使用“搜索”栏旁边的“仅显示覆盖”复选框查看所有已覆盖的检查器。

步骤 1 转至网络分析策略的 **Snort 3 版本** 。

步骤 2 点按 **仅显示覆盖** 复选框以查看已覆盖检查器的列表。

所有被覆盖的检查器都在其名称旁边显示一个橙色圆圈，以帮助您识别它们。

相关主题

在网络分析策略页面上搜索检查器，第 10 页
对检查器进行内联编辑以覆盖配置，第 14 页
自定义网络分析策略，第 11 页

将覆盖的配置恢复为默认配置

您可以恢复为覆盖检查器的默认配置所做的任何更改。此操作会将覆盖的配置恢复为检查器的默认配置。

步骤 1 在网络分析策略的 **Snort 3 版本** 中的 **检查器** 下，展开要为其恢复覆盖配置的所需检查器。

被覆盖的检查器在其名称旁边显示为橙色圆圈。

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。在右侧列的 **覆盖配置** 下，点击 **恢复默认配置** （后退箭头）图标，将检查器的覆盖配置恢复为默认配置。

如果未对检查器的默认配置进行任何更改，则此选项处于禁用状态。

步骤 2 点击 **恢复** 以确认决策。

步骤 3 点击 **Save** 保存所做的更改。

如果您不想保存更改，可以点击 **取消** 或 **叉号** (X) 图标。

相关主题

在内联编辑期间恢复未保存的更改 ，第 14 页
自定义网络分析策略 ，第 11 页
对检查器进行内联编辑以覆盖配置 ，第 14 页
自定义网络分析策略配置示例 ，第 17 页

验证 Snort 3 策略

要验证 Snort 3 策略，以下是用户可以记录的基本信息列表：

- 当前 管理中心 可以管理多个 威胁防御 版本。
- 当前版本的 管理中心 支持不适用于以前版本的 威胁防御 设备的 NAP 配置。
- 当前 NAP 策略和验证将基于当前版本支持工作。
- 更改可能包括对以前版本的 威胁防御无效的内容。
- 如果策略配置更改是当前版本的有效配置，并且使用当前 Snort 3 二进制文件和 NAP 方案执行，则接受策略配置更改。
- 对于以前的版本 威胁防御，在部署期间使用该特定版本的 NAP 架构和 Snort 3 二进制文件执行验证。如果有任何配置不适用于给定版本，系统会向用户提供信息或警告，告知我们不会部署给定版本不支持的配置，并将部署其余配置。

在此程序中，当我们将NAP策略关联到访问控制策略并将其部署在设备上时，例如速率过滤器配置等任何检查器都将应用于验证 Snort 3 策略。

步骤 1 **覆盖 NAP 策略配置的步骤：** 在网络分析策略的 **Snort 3 版本** 中的 **检查器** 下，展开要覆盖其默认设置的所需检查器。

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。

步骤 2 在右侧列的 **覆盖配置** 下，点击 **编辑检查器** （铅笔）图标以更改任何检查器，例如 rate_filter。

系统将显示覆盖配置弹出窗口，您可以在其中对 rate_filter 检查器进行所需的编辑。

步骤 3 单击**确定 (OK)**。

步骤 4 点击 **Save** 保存所做的更改。

或者，您也可以使用 **操作** 下拉菜单上传覆盖的配置文件。

步骤 5 点击网络分析策略的 **Snort 3 版本** 中的 **操作** 下拉菜单。

步骤 6 在 **上传**下，您可以点击 **覆盖配置** 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** - 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** - 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** 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 7 **将NAP策略关联到访问控制策略的步骤：** 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** 。

步骤 8 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 9 单击 **OK**。

步骤 10 单击**保存 (Save)** 保存策略。

步骤 11 或者，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** 。

步骤 12 单击**添加规则 (Add Rule)**。

步骤 13 通过点击与要添加的条件来配置规则条件。

步骤 14 点击 **网络分析** ，并选择要用于预处理匹配此规则的流量的 **网络分析策略** 。

步骤 15 单击**添加**。

步骤 16 **部署：** 在 管理中心 菜单栏中，点击 **部署** 并选择。**部署**。

步骤 17 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。

  选中设备复选框后，该设备下列出的设备的所有更改都会推送到部署中。但是，您可以使用 **策略选择** 来选择部署个别策略或配置，而保留其余的更改不予部署。

  （可选）使用 **显示或隐藏策略** 可选择性地查看或隐藏关联的未修改策略。

步骤 18 单击**部署 (Deploy)**。

步骤 19 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，请单击警告或错误前的箭头图标。

注释 显示警告，Snort 3 网络分析策略包含对于此 威胁防御 版本无效的检查器或属性，部署时将跳过以下无效设置：无效检查器： [“rate_filter”] 仅针对 7.1 版本或更低版本。

自定义网络分析策略配置示例

此示例文件包含 JSON 片段，用于说明如何为 Snort 3 自定义网络分析策略。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。请参阅。
- 使用 **操作** 下拉菜单上传覆盖的配置文件。请参阅自定义网络分析策略，第 11 页。

在选择任何这些选项之前，请查看以下所有详细信息和示例，这些详细信息和示例将帮助您成功定义网络分析策略覆盖。您必须阅读并理解此处介绍的各种场景的示例，以避免任何风险和错误。

如果您选择从 **操作** 下拉菜单覆盖检查器配置，则需要为网络分析策略覆盖构建一个 JSON 文件并上传该文件。

要覆盖网络分析策略中的检查器配置，您应只上传您需要的更改。不应上传整个配置，因为它会使覆盖本质上具有粘性，因此，将不会应用对默认值或配置的任何后续更改作为 LSP 更新的一部分。

以下是各种场景的示例：

当基本策略中的默认状态为“禁用”时启用单例检查器

```
{
  "rate_filter": {
    "enabled": true,
    "type": "singleton",
    "data": []
  }
}
```

当基本策略中的默认状态为“已启用”时禁用单例检查器

```
{
  "rate_filter": {
    "enabled": false,
    "type": "singleton",
    "data": []
  }
}
```

当基本策略中的默认状态为“禁用”时启用多例检查器

```
{
  "ssh": {
    "enabled": true,
    "type": "multiton",
    "instances": []
  }
}
```

基本策略中的“默认状态”为“已启用”时禁用多例检查器

```
{
  "ssh": {
    "enabled": false,
    "type": "multiton",
    "instances": []
  },
  "iec104": {
    "type": "multiton",
    "enabled": false,
    "instances": []
  }
}
```

覆盖单例检查器特定设置的默认值

```
{
  "normalizer": {
    "enabled": true,
    "type": "singleton",
    "data": {
      "tcp": {
        "block": true
      },
      "ip6": true
    }
  }
}
```

覆盖多例检查器中默认实例的特定设置（其中实例名称与检查器类型匹配）

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

为具有所需更改的默认实例添加绑定程序规则

注释 无法编辑默认绑定程序规则，它们始终附加在末尾。

```
{
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "use": {
          "type": "http_inspect"
        },
        "when": {
          "role": "server",
          "service": "http",
          "dst_nets": "10.1.1.0/24"
        }
      }
    ]
  }
}
```

添加新的自定义实例

注释 必须在绑定程序检查器中定义相应的绑定程序规则条目。

```
{
  "telnet": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "name": "telnet_my_instance",
        "data": {
          "encrypted_traffic": true
        }
      }
    ]
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_my_instance"
        }
      }
    ]
  }
}
```

在单个 JSON 覆盖中覆盖单个实例、多例默认实例和创建新的多例实例

在单个 JSON 覆盖中显示以下内容的示例：

- 覆盖单例实例（**规范器** 检查器）
- 覆盖多例默认实例 **(http_inspect** 检查器)
- 创建新的多例实例（**Telnet** 检查器）

```
{
  "normalizer": {
    "enabled": true,
    "type": "singleton",
    "data": {
      "tcp": {
        "block": true
      },
      "ip6": true
    }
  },
  "http_inspect": {
    "enabled": true,
    "type": "multiton",
```

```
    "instances": [
      {
        "data": {
          "unzip": false,
          "xff_headers": "x-forwarded-for true-client-ip x-another-forwarding-header"
        },
        "name": "http_inspect"
      }
    ]
  },
  "telnet": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "name": "telnet_my_instance",
        "data": {
          "encrypted_traffic": true
        }
      }
    ]
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_my_instance"
        }
      },
      {
        "use": {
          "type": "http_inspect"
        },
        "when": {
          "role": "server",
          "service": "http",
          "dst_nets": "10.1.1.0/24"
        }
      }
    ]
  }
}
```

注释 您不需要为绑定程序规则中的默认实例提供 **名称** 属性。

配置 arp_spoof

配置 **arp_spoof** 的示例：

arp_spoof 检查器没有任何属性的任何默认配置。这演示了可以提供覆盖的情况。

```
{
  "arp_spoof": {
```

```
    "type": "singleton",
    "data": {
      "hosts": [
        {
          "ip": "1.1.1.1",
          "mac": "ff:0f:f1:0f:0f:ff"
        },
        {
          "ip": "2.2.2.2",
          "mac": "ff:0f:f2:0f:0f:ff"
        }
      ]
    },
    "enabled": true
  }
}
```

配置 rate_filter

```
{
  "rate_filter": {
    "data": [
      {
        "apply_to": "[10.1.2.100, 10.1.2.101]",
        "count": 5,
        "gid": 135,
        "new_action": "alert",
        "seconds": 1,
        "sid": 1,
        "timeout": 5,
        "track": "by_src"
      }
    ],
    "enabled": true,
    "type": "singleton"
  }
}
```

使用多层次结构网络分析策略时配置绑定器规则

此示例说明在子策略中添加新的自定义实例以及应如何编写绑定程序规则。绑定器规则定义为一个列表，因此，必须选择父策略中定义的规则并在此基础上构建新规则，因为规则不会自动合并。子策略中可用的绑定程序规则是整体真实性的来源。

在 威胁防御上，默认 Cisco Talos 策略规则将附加到这些用户定义的覆盖上。

父策略:

我们已通过名称 **telnet_parent_instance** 和相应的绑定程序规则定义了一个自定义实例。

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": true
        },
        "name": "telnet_parent_instance"
      }
    ],
```

```
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

子策略:

此网络分析策略将上述策略作为其基本策略。我们定义了一个名为 **telnet_child_instance** 的自定义实例，并为此实例定义了绑定程序规则。需要在此处复制来自父策略的绑定程序规则，然后可以根据规则的性质将子策略绑定程序规则附加或附加在其之上。

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": false
        },
        "name": "telnet_child_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet",
          "nets": "10.2.2.0/24"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_child_instance"
        }
      },
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
```

```
      }
    ]
  }
}
```

常规配置列表检查器属性

更改列表类型的任何属性的覆盖时，必须传递完整内容而不是部分覆盖。这意味着，如果基本策略属性定义为：

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1"
      }
    },
    {
      "entry2": {
        "key2": "value2"
      }
    }
  ]
}
```

如果要将 **value1** 修改为 **value1-new**，则覆盖负载必须如下所示：

正确方法：

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1-new"
      }
    },
    {
      "entry2": {
        "key2": "value2"
      }
    }
  ]
}
```

不正确的方式：

```
{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1-new"
      }
    }
  ]
}
```

您可以通过获取 **smtp** 检查器中 **alt_max_command_line_len** 属性的修整值来了解此配置。假设 **smtp** 检查器的默认（基本）策略配置如下：

```
{
  "smtp": {
    "type": "multiton",
    "instances": [
      {
```

```
        "name": "smtp",
        "data": {
          "decompress_zip": false,
          "normalize_cmds": "ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO
           EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL
           NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML STARTTLS TICK
           TIME TURN TURNME VERB VRFY X-ADAT XADR XAUTH XCIR X-DRCP X-
           ERCP XEXCH50 X-EXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE
           XSTA XTRN XUSR",
          "ignore_data": false,
          "max_command_line_len": 512,
          "max_header_line_len": 1000,
          "log_rcptto": false,
          "decompress_swf": false,
          "max_response_line_len": 512,
          "b64_decode_depth": -1,
          "max_auth_command_line_len": 1000,
          "log_email_hdrs": false,
          "xlink2state": "alert",
          "binary_data_cmds": "BDAT XEXCH50",
          "auth_cmds": "AUTH XAUTH X-EXPS",
          "log_filename": false,
          "uu_decode_depth": -1,
          "ignore_tls_data": false,
          "data_cmds": "DATA",
          "bitenc_decode_depth": -1,
          "alt_max_command_line_len": [
            {
              "length": 255,
              "command": "ATRN"
            },
            {
              "command": "AUTH",
              "length": 246
            },
            {
              "length": 255,
              "command": "BDAT"
            },
            {
              "length": 246,
              "command": "DATA"
            }
          ],
          "log_mailfrom": false,
          "decompress_pdf": false,
          "normalize": "none",
          "email_hdrs_log_depth": 1464,
          "valid_cmds": "ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO
           EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL
           NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML STARTTLS TICK
           TIME TURN TURNME VERB VRFY X-ADAT XADR XAUTH XCIR X-DRCP X-
           ERCP XEXCH50 X-EXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE
           XSTA XTRN XUSR",
          "qp_decode_depth": -1
        }
      }
    ],
    "enabled": true
  }
}
```

现在，如果要向 **alt_max_command_line_len** 列表添加另外两个对象：

```
{
    "length": 246,
    "command": "XEXCH50"
},
{
    "length": 246,
    "command": "X-EXPS"
}
```

然后，自定义网络分析策略覆盖 JSON 如下所示：

```
{
  "smtp": {
    "type": "multiton",
    "instances": [
      {
        "name": "smtp",
        "data": {
          "alt_max_command_line_len": [
            {
              "length": 255,
              "command": "ATRN"
            },
            {
              "command": "AUTH",
              "length": 246
            },
            {
              "length": 255,
              "command": "BDAT"
            },
            {
              "length": 246,
              "command": "DATA"
            },
            {
              "length": 246,
              "command": "XEXCH50"
            },
            {
              "length": 246,
              "command": "X-EXPS"
            }
          ]
        }
      }
    ],
    "enabled": true
  }
}
```

在多例检查器中使用多层次结构网络分析策略时配置覆盖

此示例说明如何覆盖子策略中的属性，以及如何在任何实例的子策略中使用合并的配置。子策略中定义的任何覆盖都将与父策略合并。因此，如果属性 1 和属性 2 在父策略中被覆盖，而属性 2 和属性 3 在子策略中被覆盖，则合并的配置适用于子策略。这意味着将在设备上配置属性 1（在父策略中定义）、属性 2（在子策略中定义）和属性 3（在子策略中定义）。

父策略:

在这里，我们通过名称 **telnet_parent_instance** 定义了一个自定义实例，并覆盖了自定义实例中的 2 个属性，即 **normalize** 和 **encrypted_traffic** 。

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": false
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

子策略:

此网络分析策略将上述策略作为其基本策略。我们覆盖了父策略中的**encrypted_traffic**属性，还覆盖了新属性 **ayt_attack_thresh**。

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "encrypted_traffic": true,
          "ayt_attack_thresh": 1
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  }
}
```

使用上述策略 JSON 时，当您部署网络分析策略时，将在设备上配置以下合并 JSON。

```
{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": true,
          "ayt_attack_thresh": 1
```

```
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}
```

此示例说明自定义网络分析策略的详细信息。默认实例中也会出现相同的行为。此外，还将对单例检查器执行类似的合并。

删除网络分析策略的所有检查器覆盖：

每当要删除特定网络分析策略的所有覆盖时，都可以上传空 JSON。上传覆盖时，请选择 **替换检查器覆盖**选项。

```
{
}
```

相关主题

网络分析策略的 Snort 3 定义和术语，第 3 页
网络分析策略映射，第 8 页
为 Snort 3 的自定义网络分析策略创建，第 5 页
在网络分析策略页面上搜索检查器，第 10 页
复制检查器配置，第 10 页
自定义网络分析策略，第 11 页
对检查器进行内联编辑以覆盖配置，第 14 页
查看具有覆盖的检查器列表，第 15 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，特别是在禁用检查器时，请记住某些检查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。