# 入侵和网络分析策略中的层

以下主题介绍如何使用入侵和网络分析策略中的层：



## 层基础知识

拥有众多受管设备的大型组织可能具有许多入侵策略和网络分析策略来支持不同部门、业务单位或（某些情况下）不同公司的独特需求。两种策略类型中的配置均包含在构建块（称为层）中，可用于高效管理多个策略。

入侵和网络分析策略中的层基本以相同方式工作。您可以创建和编辑任一策略类型，而无需刻意使用层。您也可以修改策略配置；如果您没有向策略中添加用户层，系统会自动将您的更改纳入单个可配置的层（初始名称为 *My Changes*）。您还可以最多添加 200 个层，在其中可以配置设置的任意组合。可以复制、合并、移动和删除用户层，并且最重要的是，可与同一类型的其他策略共享个别用户层。

## 网络分析和入侵策略层的许可证要求

**威胁防御 许可证**

IPS

**经典许可证**

保护

# 网络分析和入侵策略层的要求和必备条件

**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)

# 层堆栈

层堆栈由以下元素组成：

**用户层**

用户可配置层可以复制、合并、移动或删除任何用户可配置层，并将任何用户可配置层设置为由同一类型的其他策略共享。此层包括自动生成的层，其最初名为“我的更改”(My Changes)。

**内置层**

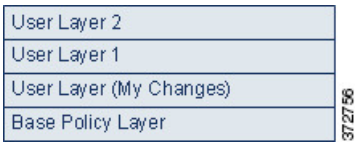
只读基本策略层。此层中的策略可以是系统提供的策略或您创建的自定义策略。

默认情况下，网络分析或入侵策略包括一个基本策略层和一个“我的更改”(My Changes) 层。可以根据需要添加用户层。

每个策略层均包含网络分析策略中所有预处理程序或入侵策略中所有入侵规则和高级设置的完整配置。最低基本策略层包含创建策略时选择的基本策略中的所有设置。较高层中的设置优先于较低层中的相同设置。在某一层中未明确设置的功能从对其进行了明确设置的下一最高层继承其设置。系统会将层平展，也就是说，它在处理网络流量时，仅应用所有设置的累积效果。

**提示** 可以仅根据基本策略中的默认设置创建入侵或网络分析策略。在创建入侵策略的情况下，如果要根据监控网络的特定需求定制入侵策略，您也可以使用 Firepower 规则陈述建议。

下图显示一个示例层堆栈，除基本策略层和初始My Changes层以外，还包括其他两个用户可配置层 *User Layer 1* 和 *User Layer 2*。请注意，图中添加的每个用户可配置层初始定位为堆栈中的最高层；因此，图中的 User Layer 2 最后添加并位于堆栈中的最高层。




无论是否允许规则更新修改策略，规则更新中的更改都绝不会覆盖您在层中所做的更改。这是因为规则更新中的更改是在基本策略中做出，基本策略会确定基本策略层中的默认设置；您的更改始终在更高层中做出，因此其会覆盖规则更新对基本策略所做出的任何更改。

# 基本层

入侵或网络分析策略的基本层（也称为基本策略）定义策略中所有配置的默认设置，并且是策略中的最低层。在不添加新层的情况下创建新策略以及更改设置，更改会存储在My Changes层中，并会覆盖（但不会更改）基本策略中的设置。

## 系统提供的基本策略

Firepower 系统提供若干对网络分析和入侵策略。通过使用系统提供的网络分析和入侵策略，您可以利用Talos 情报小组 的经验。对于这些策略，Talos 会设置入侵和预处理器规则状态，以及提供预处理器和其他高级设置的初始配置。可以按原样使用系统提供的这些策略，也可以将其用作自定义策略的基础。

如果使用系统提供的策略为基础，则导入规则更新可能会修改基本策略中的设置。但是，您可以配置自定义策略，以便系统不会自动对其系统提供的基本策略进行这些更改。这使您能够按照独立于规则更新的计划手动更新系统提供的基本策略。在任一情况下，规则更新对基本策略所做出的更改不会更改或覆盖 My Changes 或任何其他层中的设置。

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。

## 自定义基本策略

您可以使用自定义策略作为基本策略。您可以调整自定义策略中的设置，以对您最重要的方式检查流量，从而能够提高受管设备的性能以及您有效响应其生成的事件的能力。

如果更改用作其他策略的基础的自定义策略，则这些更改会自动用作使用该基础的策略的默认设置。

此外，即使使用自定义基本策略，规则更新也可能会影响您的策略，因为在策略链中，所有策略都将系统提供的策略作为最终基础。如果链中的第一个自定义策略（即使用系统提供的策略作为其基础的策略）允许规则更新修改其基本策略，则您的策略可能会受影响。

无论如何对基本策略进行更改（通过规则更新或在修改用作基本策略的自定义策略时做出更改），都不会更改或覆盖“我的更改”(My Changes) 或任何其他层中的设置。

## 规则更新对基本策略的影响

导入规则更新时，系统会修改系统提供的入侵策略、访问控制策略和网络分析策略。规则更新可能包括：

- 经过修改的网络分析预处理器设置
- 入侵和访问控制策略中经过修改的高级设置
- 新增和更新的入侵规则
- 经过修改的现有规则状态
- 新的规则类别和默认变量

规则更新还可从系统提供的策略中删除现有规则。

对默认变量和规则类别的更改在系统级别处理。

如果将系统提供的策略用作入侵或网络分析基本策略，您可以允许规则更新修改基本策略，在此情况下，基本策略是系统提供的策略的副本。如果允许规则更新更新基本策略，则新规则更新在基本策略中所做的更改与其对用作基本策略的系统提供的策略所做出的更改相同。如果您未曾对相应的设置进行过修改，则基本策略中的设置会决定策略中的设置。但是，规则更新不会覆盖您在策略中所做出的更改。

如果不允许规则更新修改基本策略，则可以在导入一个或多个规则更新后手动更新基本策略。

无论入侵策略中的规则状态如何或者是否允许规则更新修改基本入侵策略，规则更新始终会删除 Talos 删除的入侵规则。

在将更改重新部署到网络流量之前，当前部署的入侵策略中的规则行为如下：

- 已禁用的入侵规则保持禁用。
- 设置为**生成事件 (Generate Events)** 的规则在触发时继续生成事件。
- 设置为**丢弃并生成事件 (Drop and Generate Events)** 的规则在触发时继续生成事件并丢弃有问题的数据包。

除非同时满足以下两个条件，否则规则更新不会修改自定义基本策略：

- 允许规则更新修改父策略（即用于创建自定义基本策略的策略）的系统提供的基本策略。
- 未曾在父策略中做出将覆盖父策略的基本策略中相应设置的更改。

如果同时满足两个条件，则在保存父策略时，规则更新中的更改会传递到子策略（即，使用自定义基本策略的策略）。

例如，如果规则更新启用以前禁用的入侵规则，并且您未曾修改该规则在父入侵策略中的状态，则在保存父策略时，已修改的规则状态会传递到基本策略。

同样，如果规则更新修改默认预处理程序设置，并且您未曾修改父网络分析策略中的设置，则在保存父策略时，已修改的设置会传递到基本策略。

## 更改基本策略

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** 选择**策略** > **访问控制** > **入侵**。

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

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 3** 点击所需的入侵策略行中的 **编辑**（）。

**步骤 4** 从**基本策略 (Base Policy)** 下拉列表中选择策略。

**步骤 5** 点击**保存 (Save)**。

### 下一步做什么

- 部署配置更改。

### 相关主题

冲突和更改：网络分析和入侵策略

# 思科 建议层

当在入侵策略中生成规则状态建议时，可以选择是否根据建议自动修改规则状态。

如下图所示，使用建议的规则状态会在紧挨基本层之上插入一个内置只读思科 建议层。


请注意，此层对于入侵策略是唯一的。

如果您随后选择不使用建议的规则状态，则系统将移除思科 建议层。您无法手动删除该层，但是，您可以通过选择使用或不使用建议的规则状态来添加和移除该层。

添加思科 建议层会在导航面板中的“策略层”(Policy Layers) 下添加一个思科 建议链接。此链接会引导您进入思科 建议层页面的只读视图，在其中您可以只读模式访问“规则”(Rules) 页面的建议过滤视图。

使用建议的规则状态还会在导航面板中的思科 建议链接之下添加“规则”(Rules) 子链接。借助于“规则”(Rules) 子链接，可访问思科 建议层中“规则”(Rules) 页面的只读显示。在此视图中，请注意以下几点：

- 如果状态栏中没有规则状态图标，则从基本策略继承状态。
- 如果这个或其他“规则”(Rules) 页面视图的思科 建议列中没有规则状态图标，则没有适合此规则的建议。

**相关主题**

根据网络资产定制入侵防护

# 层管理

Policy Layers 页面提供网络分析或入侵策略的完整层堆栈的单页摘要。在此页面上，可以添加共享和非共享层，复制、合并、移动和删除层，访问每层的摘要页面，以及访问每层中已启用、禁用和覆盖的配置的配置页面。

对于每层，您均可查看以下信息：

- 层是内置层、共享用户层还是非共享用户层
- 哪些层包含最高（即最有效）预处理程序或高级设置配置（按功能名称）
- 在入侵策略中，在该层中设置了其状态的入侵规则的数量，以及设置为每个规则状态的规则的数量。

“策略层”(Policy Layers) 页面还提供所有已启用预处理器（网络分析）或高级设置（入侵）的实际效果的摘要，并为入侵策略提供入侵规则的实际效果的摘要。

每层的摘要中的功能名称指明在该层中已启用、禁用、覆盖或继承哪些配置，如下所示：

| 当功能..... | 功能名称..... |
|---|---|
| 在层中已启用 | 以纯文本编写 |
| 在层中已禁用 | 删除 |
| 被更高层中的配置覆盖 | 以斜体文本编写 |
| 从更低层继承 | 不存在 |

您最多可以向网络分析或入侵策略中添加 200 层。添加的层显示为策略中的最高层。初始状态对于所有功能都为 Inherit，并且在入侵策略中，未设置事件过滤、动态状态或警报规则操作。

在将用户可配置层添加到策略中时，可为该层提供唯一名称。之后，可以更改名称，或者可以在编辑层时添加或修改可视的说明。

您可以复制层，在“用户层”(User Layers) 页面区域中将层上移或下移，或删除用户层，包括初始“我的更改”(My Changes) 层。请注意以下考虑事项：

- 在复制层时，副本显示为最高层。
- 复制共享层会创建初始未共享且之后在选择时可共享的层。
- 不能删除共享层；已启用共享但未曾与其他策略共享的层不是共享层。

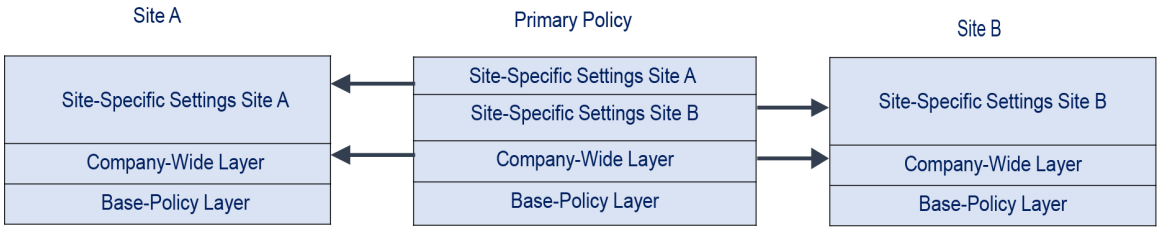
您可以将一个用户可配置层与其正下方的另一个用户可配置层合并。合并层保留任一层特有的所有设置，并且如果两层均包含同一预处理程序、入侵规则或高级设置的设置，则会接受更高层中的设

置。合并层保留更低层的名称。如果在策略中创建的可共享层可以添加到其他策略，则可以将该可共享层正上方的非共享层与该可共享层合并，但是不能将该共享层与其下方的非共享层合并。如果在一个策略中添加的共享层在其他策略中已创建，则可以将该共享层合并到其正下方的非共享层中，所生成的层不再共享；不能将非共享层合并到其下方的共享层中。

# 共享层

当您在另一策略中创建层后，可以将该层添加到您的策略中并允许其共享，该层即为共享层。可共享的层是您允许共享的层。

下图显示一个主策略示例，您可在其中创建公司范围层，为站点 A 和 B 创建站点特定层，并允许进行共享。然后，将这些层作为共享层添加到站点 A 和 B 的策略中。




主策略中的公司范围层包含适用于站点 A 和 B 的设置。站点特定层包含特定于每个站点的设置。例如，如果使用网络分析策略，则 Site A 在受监控网络上可能没有 Web 服务器，并且不需要 HTTP Inspect 预处理程序的保护或处理开销，但两个站点均可能需要 TCP 数据流预处理。可在与两个站点共享的公司范围层启用 TCP 数据流处理，在与站点 A 共享的站点特定层禁用 HTTP 检查预处理器，在与站点 B 共享的站点特定层启用 HTTP 检查预处理器。通过编辑站点特定策略中的较高层配置，如果需要任何配置调整，您还可以进一步微调每个站点的策略。

示例主策略中的扁平化网络设置不大可能对流量监控有用，但配置和更新站点特定策略所节省的时间使得它成为策略层的一种有用应用。

也可使用许多其他层配置。例如，您可以按公司、部门、网络甚至用户来界定策略层。如果使用入侵策略，则还可以在一层中包含高级设置，在另一层中包含规则设置。

可以将用户可配置层与同一类型（入侵或网络分析）的其他策略共享。在可共享层中修改配置，然后确认更改时，系统会更新共享层的所有策略，并为您提供所有受影响策略的列表。您只能在已创建该层的策略中修改功能配置。

不能对添加到另一个策略的层禁用共享；必须先从另一个策略中删除该层，或者删除另一个策略。

当基本策略是在其中已创建要共享的层的自定义策略时，不能向策略中添加共享层。这样将为策略提供循环依赖。

在多域部署中，可以将来自祖先策略的共享层添加到后代域中的策略。

# 管理层

过程

**步骤 1** 在编辑 Snort 2 策略时，点击导航面板中的**策略层 (Policy Layers)**。

**步骤 2** 可以在“策略层”(Policy Layers) 页面上执行下列任意管理操作：

- 添加其他策略中的共享层 - 点击“用户层”(User Layers) 旁边的添加共享层 **添加**（+），从**添加共享层 (Add Shared Layer)** 下拉列表中选择层，然后点击**确定 (OK)**。
- 添加非共享层 - 点击“用户层”(User Layers) 旁边的添加层 **添加**（+），输入**名称 (Name)**，然后点击**确定 (OK)**。
- 添加或更改层说明 - 点击层旁边的 **编辑**（✎），然后添加或更改**说明 (Description)**。
- 允许与其他策略共享层 - 点击层旁边的 **编辑**（✎），然后清除**共享 (Sharing)** 复选框。
- 更改层名称 - 点击层旁边的 **编辑**（✎），然后更改**名称 (Name)**。
- 复制层 - 点击该层的 **复制**（⧉）。
- 删除层 - 点击该层的 **删除**（🗑），然后点击**确定 (OK)**。
- 合并两层 - 点击两层中上层的 **合并**（⧉），然后点击**确定 (OK)**。
- 移动层 - 点击层摘要中的任何开放区域并将其拖动，直至**位置箭头** 指向该层上方或下方要将该层移到的行。

**步骤 3** 要保存自上次策略确认以来在此策略中进行的更改，请点击**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

- 部署配置更改。

### 相关主题

冲突和更改：网络分析和入侵策略

# 导航层

过程

**步骤 1** 在编辑 Snort 2 策略时，点击导航面板中的**策略层 (Policy Layers)**。

**步骤 2** 可以执行下列任意操作以在各层间导航：

- 访问预处理器或高级设置页面 - 如果要访问层级别的预处理器或高级设置配置页面，请点击该层对应的行中的功能名称。配置页面在基本策略和共享层中为只读。
- 访问规则页面 - 如果要访问按规则状态类型过滤的层级别的规则配置页面，请在层摘要中点击**丢弃并生成事件 (Drop and Generate Events)**、**生成事件 (Generate Events)** 或**禁用 (Disabled)**。如果该层不包含设置为所选规则状态的规则，则不会显示任何规则。
- 显示“策略信息”(Policy Information) 页面 - 如果要显示“策略信息”(Policy Information) 页面，请点击导航面板中的**策略摘要 (Policy Summary)**。
- 显示层摘要页面 - 如果要显示某层的摘要页面，请点击该层对应的行中的层名称，或者点击用户层旁边的 **编辑**（）。您也可以点击 **视图**（） 来访问共享层的只读摘要页面。

**步骤 3** 要保存自上次策略确认以来在此策略中进行的更改，请点击**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

- 部署配置更改。

### 相关主题

冲突和更改：网络分析和入侵策略

# 层中的入侵规则

可以在该层的 Rules 页面上查看个别层设置，也可以在 Rules 页面的策略视图中查看所有设置的实际效果。在 Rules 页面的策略视图中修改规则设置时，修改的是策略中的最高用户可配置层。可以在任何 Rules 页面上使用层下拉列表切换到另一层。

下表描述在多个层中配置相同类型设置的效果。

**表 *1:* 层规则设置**

| 您可设置 | 设置类型 | 所需的操作… |
|---|---|---|
| 一条 | 规则状态 | 覆盖为更低层中的规则设置的规则状态，并忽略在更低层中为该规则配置的所有阈值、抑制、基于速率的规则状态和警报。<br>如果希望规则从基本策略或更低层继承其状态，请将规则状态设置为 Inherit。请注意，在入侵策略“规则”(Rules) 页面上操作时，不能将规则状态设置为“继承”(Inherit)，因为入侵策略“规则”(Rules) 页面是所有规则设置的实际效果的综合视图。 |
| 一条 | 阈值 SNMP 警报 | 对于下层中的规则，覆盖相同类型的设置。请注意，对于该层中的规则，设置阈值将改写所有现有阈值。 |

| 您可设置 | 设置类型 | 所需的操作… |
|---|---|---|
| 一个或多个 | 基于抑制率的规则状态 | 将为每个选定规则累积组合相同类型的设置，直到为规则设置了规则状态的第一层。系统会忽略设定规则状态所在层下方的设置。 |
| 一个或多个 | 注释 | 向规则中添加注释。注释特定于规则，而非特定于策略或层。您可以在任何层中为规则添加一个或多个注释。 |

例如，如在一层中将规则状态设置为“丢弃并生成事件”(Drop and Generate Events)，但在上层设置为“已禁用”(Disabled)，则入侵策略的“规则”(Rules) 页面将显示规则已被禁用。

又例如，如果在一层中为规则将基于源的抑制设置为 192.168.1.1，同时也为该规则将基于目标的抑制设置为 192.168.1.2，则“规则”(Rules) 页面显示：累积效应将为源地址 192.168.1.1 和目标地址 192.168.1.2 抑制事件。请注意，抑制和基于速率的规则状态设置将为每个选定规则累积组合相同类型的设置，直到为规则设置了规则状态的第一层。系统会忽略设定规则状态所在层下方的设置。

“规则”(Rules) 页面上特定层的颜色编码表示有效状态位于较高层、较低层还是当前层中，如下所示：

- 红色 - 有效状态位于较高层
- 黄色 - 有效状态位于较低层
- 无光度 - 有效状态位于当前层

由于入侵策略 Rules 页面是所有规则设置的实际效果的综合视图，因此规则状态在此页面上未进行颜色编码。

## 配置层中的入侵规则

在入侵策略中，可以为任何用户可配置层中的规则设置规则状态、事件过滤、动态状态、警报和规则注释。访问要更改的层后，可按照在入侵策略 Rules 页面上所用的相同方法在该层的 Rules 页面添加设置。

### 过程

**步骤 1** 编辑 Snort 2 入侵策略时，展开导航面板中的**策略层 (Policy Layers)**。

**步骤 2** 展开要修改的策略层。

**步骤 3** 点击要修改的策略层正下方的 **Rules**。

**步骤 4** 修改使用规则调整入侵策略中所述的任意设置。

**提示** 要从可编辑层删除单项设置，请双击该层“规则”页面上的规则消息，以显示规则详细信息。点击要删除的设置旁边的 **Delete**，然后双击 **OK**。

**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，请点击**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

- 部署配置更改。

### 相关主题

冲突和更改：网络分析和入侵策略

## 从多个层中删除规则设置

可以从入侵策略中的多个层同时删除特定类型的事件过滤器、动态状态或警报。系统移除所选设置并将规则的剩余设置复制到策略中的最高可编辑层。

系统将向下移除每层中设置的设置类型，直至移除所有设置或遇到为规则设置了规则状态的层。在后一种情况下，系统会从该层中删除设置并停止删除设置类型。

当系统在共享层或在基本策略中遇到该设置类型时，如果策略中的最高层可以编辑，则系统会将该规则的剩余设置和规则状态复制到该可编辑层。否则，如果策略中的最高层是共享层，系统会在该共享层上方创建新的可编辑层，并将该规则的剩余设置和规则状态复制到该可编辑层。

**注释** 删除从共享层或基本策略派生的规则设置会导致忽略从更低层或基本策略中对该规则做出的任何更改。要停止忽略从更低层或基本策略做出的更改，请在最高层的摘要页面上将规则状态设置为 **Inherit**。

### 过程

**步骤 1** 在编辑 Snort 2 入侵策略时，点击导航面板中**策略信息 (Policy Information)** 正下方的**规则 (Rules)**。

**提示** 也可为所有层在“规则”(Rules) 页面的层下拉列表中选择**策略 (Policy)**，或在“策略信息”(Policy Information) 页面选择**管理规则 (Manage Rules)**。

**步骤 2** 选择要从中删除多个设置的规则：

- 选择特定 - 如果要选择特定规则，请选中每条规则旁边的复选框。
- 选择全部 - 如果要选择当前列表中的所有规则，请选中列顶部的复选框。

**步骤 3** 选择以下选项之一：

- **事件过滤 > 删除阈值**
- **事件过滤 > 删除抑制**
- **动态状态 > 删除基于速率的规则状态**
- **警报 > 删除 SNMP 警报**

注释　删除从共享层或基本策略派生的规则设置会导致忽略从更低层或基本策略中对该规则做出的任何更改。要停止忽略从更低层或基本策略做出的更改，请在最高层的摘要页面上将规则状态设置为 **Inherit**。

**步骤 4** 点击 **OK**。

**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，请点击**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

- 部署配置更改。

### 相关主题

冲突和更改：网络分析和入侵策略

## 接受来自自定义基本策略的规则更改

当未曾添加层的自定义网络分析或入侵策略使用另一个自定义策略作为其基本策略时，在以下情况下，必须将规则设置为继承其规则状态：

- 删除为基本策略中的规则设置的事件过滤器、动态状态或 SNMP 警报，以及
- 您希望规则接受在用作基本策略的另一个自定义策略中对其做出的后续更改

### 过程

**步骤 1** 编辑 Snort 2 入侵策略时，展开导航面板中的**策略层 (Policy Layers)**。

**步骤 2** 展开**我的更改 (My Changes)**。

**步骤 3** 点击**我的更改 (My Changes)** 正下方的**规则 (Rules)** 链接。

**步骤 4** 选择要接受其设置的规则。有以下选项可供选择：

- 选择特定规则 - 如果要选择特定规则，请选中每条规则旁边的复选框。
- 选择所有规则 - 如果要选择当前列表中的所有规则，请选中列顶部的复选框。

**步骤 5** 从**规则状态 (Rule State)** 下拉列表选择**继承 (Inherit)**。

**步骤 6** 要保存自上次策略确认以来在此策略中进行的更改，请点击**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

- 部署配置更改。

### 相关主题

冲突和更改：网络分析和入侵策略

# 层中的预处理器和高级设置

您使用类似的机制在网络分析策略中配置预处理程序和在入侵策略中配置高级设置。您可以启用和禁用预处理器（在网络分析设置页面上）和入侵策略高级设置（在入侵策略“高级设置”[Advanced Settings] 页面上）。这些页面还提供所有相关功能的有效状态的摘要。例如，如果网络分析 SSL 预处理器在一层中已禁用但在更高层中已启用，则“设置”(Settings) 页面将其显示为已启用。在这些页面上做出的更改显示在策略的顶层中。请注意，Back Orifice 预处理程序没有用户可配置选项。

您也可以在用户可配置层的摘要页面上启用或禁用预处理程序或高级设置并访问其配置页面。在此页面上，可以修改层名称和说明，并配置是否将该层与同一类型的其他策略共享。可以通过选择导航面板中 **Policy Layers** 下方的层名称来切换到另一层的摘要页面。

启用预处理器或高级设置时，在导航面板中的层名称下方会显示指向该功能的配置页面的子链接，并且在层的摘要页面上的功能旁边会显示 **编辑**（）；在层中禁用该功能或将其设置为“继承”(Inherit) 时，这些图标会消失。

设置预处理器或高级设置的状态（已启用或已禁用）会覆盖更低层中该功能的状态和配置设置。如果希望预处理器或高级设置从基本策略或更低层继承其状态和配置，请将其设置为“**继承**”**(Inherit)**。请注意，当在 Settings 或 Advanced Settings 页面上操作时，无法选择 Inherit。另请注意，如果继承当前启用的功能，则导航面板中的功能子链接和配置页面上的编辑图标不再显示。

系统使用已启用该功能的最高层中的配置。除非明确修改配置，否则系统使用默认配置。例如，如果在一层中启用并修改网络分析 DCE/RPC 预处理程序，并且还在更高层中将其启用但不修改，则系统使用更高层中的默认配置。

每个层摘要页面上的颜色编码指示有效配置位于较高层、较低层还是当前层中，如下所示：

- 红色 - 有效配置位于较高层
- 黄色 - 有效配置位于较低层
- 无光度 - 有效配置位于当前层

由于 Settings 和 Advanced Settings 页面是所有相关设置的综合视图，因此，这些页面不使用颜色编码指明有效配置的位置。

## 配置层中的预处理器和高级设置

### 过程

**步骤 1** 编辑 Snort 2 策略时，请展开导航面板中的**策略层 (Policy Layers)**，然后点击要修改的层的名称。

**步骤 2** 有以下选项可供选择：

- 更改层**名称 (Name)**。
- 添加或更改**说明 (Description)**。
- 选中或清除**共享 (Sharing)** 复选框以指定层是否可以与其他策略共享。
- 要访问已启用的预处理器/高级设置的配置页面，请点击 **编辑**（ ） 或功能子链接。
- 要禁用当前层中的预处理器/高级设置，请点击功能旁边的**已禁用 (Disabled)**。
- 要启用当前层中的预处理器/高级设置，请点击功能旁边的**已启用 (Enabled)**。
- 要从当前层下方的最高层中的设置继承预处理器/高级设置，请点击**继承 (Inherit)**。

**步骤 3** 要保存自上次策略确认以来在此策略中进行的更改，请点击**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

- 部署配置更改。

### 相关主题

冲突和更改：网络分析和入侵策略

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。