根据网络资产定制入侵防护

以下主题介绍如何使用 Cisco 建议规则：

关于思科 建议的规则

可以遵从入侵规则建议，将您的网络中检测到的操作系统、服务器和客户端应用协议与为保护这些资产而特别编写的规则相关联。这样，您就可根据自己的受监控网络的特定需求定制您的入侵策略。

系统为每个入侵策略制定一组单独的建议。它通常会建议标准文本规则和共享对象规则的规则状态更改。但是，它也可建议预处理器和解码器规则的更改。

当生成规则状态建议时，可以使用默认设置或配置高级设置。通过高级设置，可以执行以下操作：

- 重新定义系统监控网络上的哪些主机以查找漏洞
- 影响系统根据规则开销建议哪些规则
- 指定是否生成建议以禁用规则

您还可以选择是要立即使用建议还是在接受之前审核建议（和受影响规则）。

选择使用建议规则状态会向入侵策略中添加只读思科 建议层，并且随后选择不使用建议规则状态会删除该层。

系统不会更改手动设置的规则状态：

- 在生成建议之前手动设置指定规则的状态可防止系统将来修改这些规则的状态。
- 在生成建议之后手动设置指定规则的状态可覆盖这些规则的建议状态。

提示 入侵策略报告可能包含具有与建议状态不同的规则状态的规则列表。

在显示对建议过滤后的 Rules 页面时，或者从导航面板或 Policy Information 页面直接访问 Rules 页面后，可以手动设置规则状态、对规则排序并执行 Rules 页面中的任何其他可用操作，例如抑制规则、设置规则阈值等。

注释 Talos 情报小组 确定系统提供的策略中的各规则的相应状态。如果使用系统提供的策略作为基本策略，并且允许系统将规则设置为思科 建议规则状态，则入侵策略中的规则与思科为网络资产建议的设置相匹配。

建议规则和多租户

系统会为每个枝叶域构建单独的网络映射。在多域部署中，如果您在祖先域的入侵策略中启用此功能，则系统会使用来自所有后代枝叶域的数据生成建议。这可能使得入侵规则针对可能不存在于所有枝叶域的资产进行定制，从而影响性能。

思科 建议的默认设置

当生成思科 建议时，系统会搜索基本策略以查找防范与网络资产关联的漏洞的规则，并识别基本策略中的规则的当前状态。然后，系统会建议规则状态，如果选择如此，则会将规则设置为建议状态。

系统执行以下基本分析来生成建议：

表 *1:* 基于漏洞的规则状态建议

规则是否保护发现的资产？	基本策略规则状态	建议的规则状态
是	禁用	Generate Events
	Generate Events	Generate Events
	Drop and Generate Events	Drop and Generate Events
否	任意	禁用

请注意表中的以下内容：

- 如果某个规则在基本策略中处于禁用状态或设置为“生成事件”，则建议的状态始终是“生成事件”。

  例如，如果基本策略是“无活动规则”，其中的所有规则均处于禁用状态，则不会建议“丢弃并生成事件”。

- 只有对于已在基本策略中设置为“丢弃并生成事件”的规则，才会建议“丢弃并生成事件”。

  如果您要将某个规则设置为“丢弃并生成事件”，且该规则在基本策略中处于禁用状态或已设置为“生成事件”，您必须手动重置该规则的状态。

当生成建议而不更改思科 建议规则的高级设置时，系统会建议更改所发现的整个网络中所有主机的规则状态。

默认情况下，系统仅为低开销或中等开销的规则生成建议，并生成禁用规则的建议。

系统不会为基于使用“影响限定条件”(Impact Qualification) 功能禁用的漏洞的入侵规则建议规则状态。

系统始终建议启用与映射到主机的第三方漏洞相关联的本地规则。

对于未映射的本地规则，系统不会给出状态建议。

相关主题

第三方产品映射

思科 建议的高级设置

在策略报告中包括建议和规则状态之间的所有差异

默认情况下，入侵策略报告列出策略中已启用的规则，即设置为“生成事件”(Generate Events) 或“丢弃并生成事件”(Drop and Generate Events) 的规则。启用**包括所有差异 (Include all differences)** 选项还会列出其建议状态与已保存状态不同的规则。有关策略报告的信息，请参阅策略报告。

要检查的网络

指定为给出建议而要检查的受监控网络或单独主机。可以指定单个 IP 地址或地址块，也可以指定由单个地址和/或地址块组成并以逗号分隔的列表。

指定主机中的地址列表与一个逻辑或运算关联，但逻辑非除外，逻辑非在所有逻辑或运算计算完之后与一个逻辑与运算关联。

如果要根据主机信息动态调整对特定数据包的主动规则处理，也可以启用自适应配置文件。

建议阈值（就规则开销而言）

防止系统推荐或自动启用开销高于您选择的阈值的入侵规则。

开销基于规则对系统性能的潜在影响以及规则产生误报的可能性。允许开销较高的规则通常会得到更多的建议，但会影响系统性能。在“入侵规则”(Intrusion Rules) 页面的规则详细信息视图中，可以查看规则的开销级别。

请注意，系统在给出禁用规则的建议时，不会将规则开销作为一项考虑因素。此外，本地规则没有开销，除非被映射到第三方漏洞。

为开销级别为特定设置的规则生成建议并不会妨碍您使用不同的开销生成建议后再重新为原来的开销设置生成建议。每次为同一规则集生成建议时，无论生成多少次建议或者生成多少不同的开销设置，为每个开销设置获得的规则状态建议都相同。例如，您可以将开销依次设置为中、

高，并最终设置为中来生成建议，如果网络中的主机和应用尚未更改，对于该规则集给出的开销设置为中的两组建议均相同。

接受禁用规则的建议

指定系统是否根据 思科 建议禁用入侵规则。

接受禁用规则的建议会限制规则的覆盖范围。忽略禁用规则的建议会扩大规则的覆盖范围。

相关主题

自适应配置文件更新和思科 建议规则

生成和应用思科 建议

开始或停止使用思科 建议可能需要几分钟的时间，具体取决于网络和入侵规则集的大小。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，如果您在祖先域的入侵策略中启用此功能，则系统会使用来自所有后代枝叶域的数据生成建议。这可能使得入侵规则针对可能不存在于所有枝叶域的资产进行定制，从而影响性能。

开始之前

- 思科 建议具有以下要求：
  - 威胁防御 许可证-IPS
  - 经典许可证-保护
  - 用户角色-管理员 或 入侵管理员 (Intrusion Admin)
- 在开始执行这些步骤之前，请配置网络发现策略。配置网络发现策略以定义内部主机，以便适合思科 建议。请参阅网络发现自定义。

过程

步骤 1 在 Snort 2 入侵策略编辑器的导航窗格中，点击**思科建议 (Cisco Recommendations)**。

步骤 2 （可选）配置高级设置；请参阅思科 建议的高级设置 ，第 3 页。

步骤 3 生成并应用建议。

- **生成并使用建议**-生成建议并更改规则状态以使其匹配。仅在您从未生成过建议时可用。
- **生成建议**-无论您是否在使用建议，生成新的建议，但不更改规则状态使其匹配。
- **更新建议**-如果您正在使用建议，生成建议并更改规则状态以使其匹配。否则，生成新的建议，但不更改规则状态。
- **使用建议**-更改规则状态以匹配任何未实施的建议。
- **不使用建议**-停止使用建议。如果您在应用建议前手动更改了规则状态，则规则状态会恢复为您为其指定的值。否则，规则状态会恢复为其默认值。

在您生成建议时，系统会显示建议更改的摘要。要查看系统建议更改状态的规则列表，请点击最近建议的规则状态旁边的**查看 (View)**。

步骤 4 评估并调整您实施的建议。

即使您接受大多数思科 建议，也可以通过手动设置规则状态覆盖个别建议；请参阅设置入侵规则状态。

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。

脚本检测

脚本检测可通过部分检测来防止 Snort 过晚阻止入侵失败。在客户端和服务器之间传输 HTML 文件时，这些文件可能会包含用于发起攻击的恶意脚本（例如 JavaScript）。当发现此类恶意脚本时，部分检查允许任何 IPS 规则匹配恶意脚本，并且检查器会通过检查和检测来刷新该数据段。恶意文件永远不会到达其目的地。此功能同时支持 HTTP/1 和 HTTP/2 流量。

默认情况下始终启用此功能。要关闭此功能，请将 **`http_inspect.script_detection=true`** 设为 false。

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。