使用案例 - 在 Cisco Secure Fiewall Management Center 生成 Snort 3 建议

Snort 3 规则建议

规则建议使用特定于主机环境的规则自动调整入侵策略。您可以通过禁用网络中不存在的漏洞的规则来启用其他规则或调整当前规则集。有关详细信息，请参阅Cisco Secure Firewall 建议规则的概述。

该计划如何实施？

管理中心通过被动发现构建网络上的主机数据库，其中包含 IP 地址、主机名、操作系统、服务、用户和客户端应用等详细信息。根据此信息，系统会将漏洞映射到每个已发现的主机。建议功能使用此主机数据库来确定适用于您的环境的规则。

在 Snort 3 中，有四个安全级别，每个安全级别对应一个特定的 Talos 策略。它们是：

- 1 级 - 连接优先于安全
- 2 级 - 平衡安全性和连接性
- 3 级 - 安全优先于连接
- 4 级 - 最大检测

选中 **接受建议以禁用规则** 复选框，为网络中的主机上未找到的漏洞禁用规则。仅当由于大量警报而必须调整规则集或提高检查性能时，才选中此选项。

优势

- 通过配置建议，您可以定制入侵策略，以使用特定于主机环境的规则更有效地检测特定类型的威胁。
- 通过减少误报和漏报，建议有助于提高事件响应流程的效率和效力。

示例业务情景

一家大型企业网络使用 Snort 3 作为其主要的入侵检测和防御系统。在快速发展的威胁环境中，必须采用强大的网络安全措施。安全团队希望增强其事件响应能力。其中一种方法是根据在主机网络中检测到的漏洞生成建议或规则集。这有助于优化其入侵策略，从而更有效地保护网络。

最佳实践

- 您必须拥有高质量、准确的主机数据。

  由于网络发现的被动性质，您的威胁防御设备必须尽可能靠近受保护的主机。这允许威胁防御设备监控进出这些主机的网络流量，从而为您提供有关网络上存在的应用、服务和漏洞的准确数据。
- 设备应了解东西流量以及南北流量，以构建准确的主机配置文件。
- 您可以创建计划任务来自动更新建议。

前提条件

- 确保系统中存在主机以生成建议。
- 为建议配置的受保护网络应映射到系统中的主机。

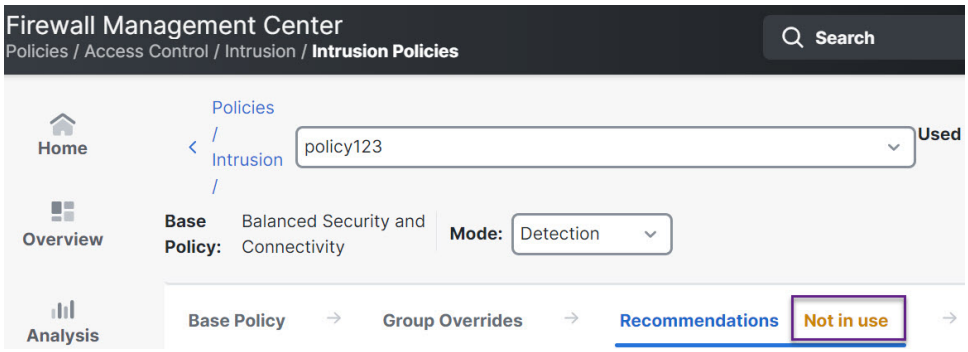
生成 Snort 3 建议

过程

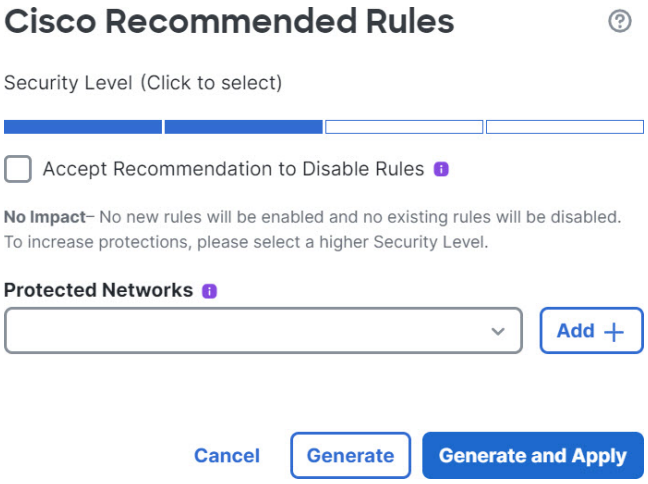
步骤 1 依次选择**策略** > **入侵**。

步骤 2 点击相应的入侵策略的 **Snort 3 版本** 按钮。

步骤 3 点击 **建议**（**未使用**） 层以配置规则建议。



在 **思科建议的规则** 窗口中，您可以设置安全级别。



步骤 4 点击以选择安全级别。

步骤 5 （可选）选中 **接受建议以禁用规则** 复选框，以禁用为网络中主机上未发现的漏洞编写的规则。

仅当由于大量警报或提高检查性能而必须调整规则集时，才使用此选项。

步骤 6 从 **受保护的网络** 下拉列表中，选择建议必须检查的网络对象。默认情况下，如果不进行选择，则选择任何 IPv4 或 IPv6 网络。

点击 **添加 +** 来创建类型为 **主机** 或 **网络** 的新网络对象，然后点击 **保存**。

步骤 7 生成并应用建议：

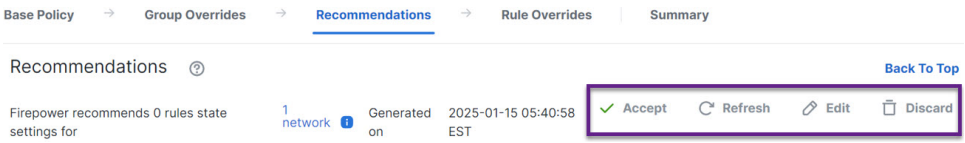
- **生成** - 生成入侵策略的建议。此操作列出了**建议的规则**（**未使用**）下的规则。
- **生成并应用** - 生成并应用入侵策略的建议。此操作列出了**建议的规则**（**未使用**）下的规则。

建议已成功生成。系统将显示一个新的建议选项卡，其中包含所有建议的规则及其相应的建议操作。规则操作预设过滤器也可用于此选项卡，此外还有新建议。

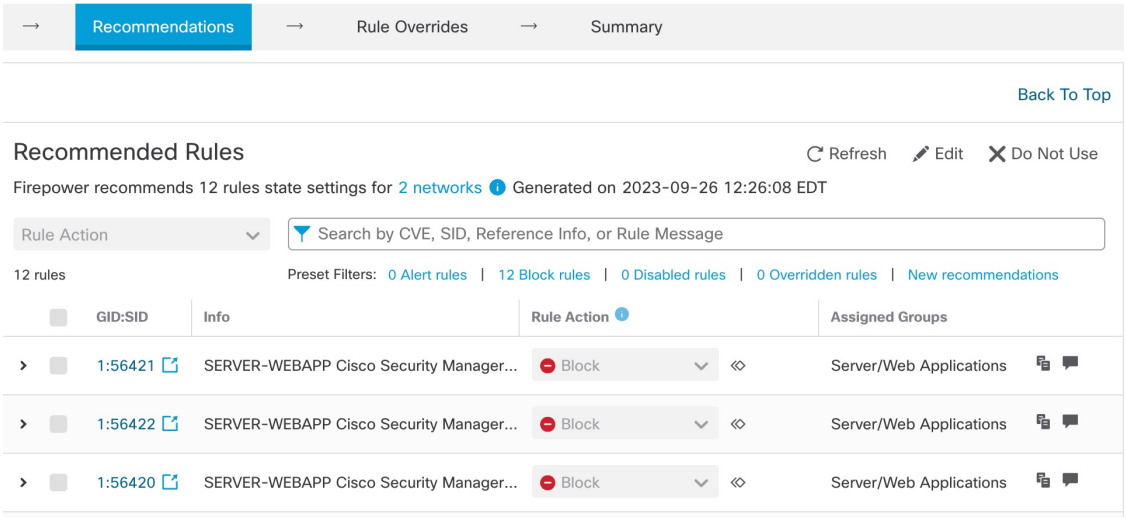
步骤 8 验证这些建议，然后相应地选择应用它们：

- **接受** - 应用先前为入侵策略生成的建议。
- **刷新** - 重新生成并更新入侵策略的规则建议。

- **编辑** - 打开 **建议** 对话框，您可以提供建议输入值，然后生成建议。
- **丢弃** - 从策略中恢复或删除已应用的建议规则，并删除 **建议** 选项卡。

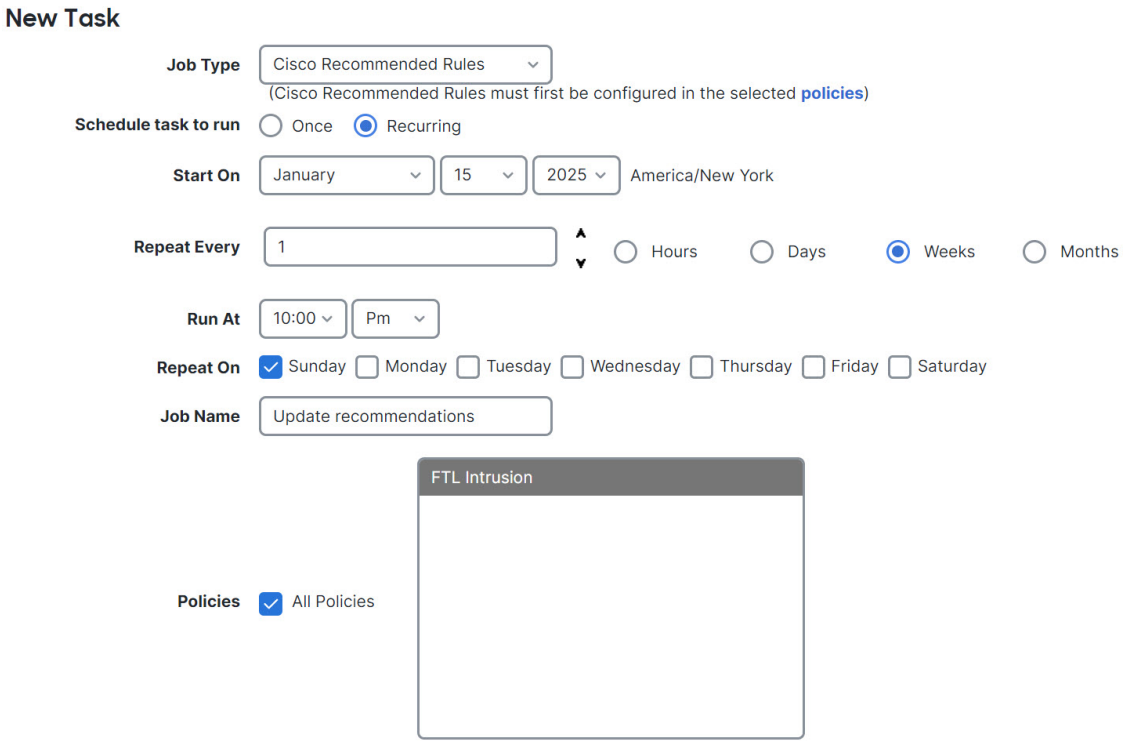


在 **所有规则**下，有一个建议的规则部分，其中显示建议的规则。



步骤 9 要有效地使用建议，必须定期更新。请按以下步骤操作：

1. 选择 **系统** (⚙) > **工具** > **计划**。
2. 点击**添加任务 (Add Task)**。
3. 从 **作业类型** 下拉列表中选择 **思科建议的规则** 。
4. 根据需要更新必填字段。



5. 点击**保存**。

下一步做什么

部署配置更改。请参阅部署配置更改。

部署配置更改

更改配置后，将其部署到受影响的设备。

注释 本主题介绍部署配置更改的基本步骤。我们强烈建议您在继续执行这些步骤之前，参考最新版本的 *Cisco Secure Firewall Management Center* 指南 中的 部署配置更改 主题，了解部署更改的前提条件和影响。

注意 在部署时，资源需求可能会导致少量数据包未经检测而被丢弃。此外，部署某些配置会重新启动 Snort 进程，这会中断流量检测。流量在此中断期间丢弃还是不进一步检查而直接通过，取决于目标设备处理流量的方式。

过程

步骤 1 在 Cisco Secure Firewall Management Center 菜单栏中，点击 **部署** ，然后选择 **部署**。

GUI 页面列出了具有 **待处理** 状态的过期配置的设备。

- **修改者**列列出了修改策略或对象的用户。展开设备列表以参照每个策略列表查看修改了策略的用户。

  注释
  没有为已删除的策略和对象提供用户名。

- **检查中断** 列指示在部署过程中是否可能导致设备中的流量检查中断。

  如果设备的此为空白，则表明在部署过程中该设备上不会出现流量检查中断。

- **上次修改时间** 列指定上次更改配置的时间。
- **预览**列允许您预览下一次要部署的更改。
- **状态**列提供每个部署的状态。

步骤 2 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。

  选中设备旁边的复选框时，系统会推送对设备进行的所有更改并在设备下列出这些更改以进行部署。但是，您可以使用 **策略选择**（ ） 选择部署个别或指定策略或配置，而保留其余的更改不予部署。

  注释
  - 当 **检查中断** 列中的状态指示（**是**）部署会中断 防火墙威胁防御 设备上的检查并可能中断流量时，展开的列表将用 **检查中断**（ ）指示导致中断的特定配置。
  - 当接口组、安全区或对象发生更改时，受影响的设备在 防火墙管理中心中显示为过期。为确保这些更改生效，包含这些接口组、安全区或对象的策略也需要随这些更改一起部署。受影响的策略在 防火墙管理中心的 **预览**页上显示为过期。

步骤 3 点击**部署 (Deploy)**。

步骤 4 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，请点击警告或错误前的箭头图标。

有以下选项可供选择：

- 部署 - 继续部署而无需解决警告情况。如果系统识别错误，则无法继续。
- 关闭 - 退出而不部署。解决错误和警告情况，并尝试重新部署该配置。

下一步做什么

在部署过程中，如果有部署失败，则可能会影响流量。不过，这取决于某些条件。如果部署中存在特定的配置更改，则部署失败可能导致流量中断。有关部署过程的详细信息，请参阅 *Cisco Secure Firewall Management Center* 配置指南中的部署配置更改主题。

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。