根据网络资产定制入侵防护

本章供您深入了解 Cisco Secure Firewall 建议的规则以及生成和应用 Cisco Secure Firewall 建议的规则。

LSP 更新中的 Snort 3 规则更改

在常规 Snort 3 轻量安全软件包 (LSP) 更新期间，现有系统定义的入侵规则可能会替换为新的入侵规则。一个规则可能被多个规则替换，或者多个规则被一个规则替换。如果可以对合并或扩展的规则进行更好的检测，则会发生这种情况。为了更好地进行管理，在 LSP 更新过程中，也可以删除一些现有的系统定义的规则。

要在 LSP 更新期间获取任何 已覆盖的 系统定义的规则更改的通知，请确保选中 **保留已删除的 Snort 3 规则** 的用户覆盖复选框。

要导航至 **保留已删除 Snort 3 规则的用户覆盖** 复选框，请点击 **齿轮**（ ），然后选择 **配置** > **入侵策略首选项** 。

默认情况下，此复选框为选中状态。选中此复选框时，系统会在作为 LSP 更新的一部分添加的新替换规则中保留规则覆盖。通知显示在 **齿轮**（ ）旁边的通知图标下的 **任务** 选项卡中。

安全防火墙 建议规则的概述

您可以使用入侵规则建议来锁定与在网络中检测到的主机资产相关联的漏洞。例如，操作系统、服务器和客户端应用协议。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，它也可建议检查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 安全防火墙 建议层，并且随后选择不使用建议规则状态会删除该层。

您可以安排任务来根据入侵策略中最近保存的配置设置自动生成建议。

系统不会更改手动设置的规则状态，如：

- 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 Cisco Talos 情报组 (Talos) 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 安全防火墙 建议规则状态，则入侵策略中的规则与为网络资产建议的设置相匹配。

网络分析和入侵策略的必备条件

要允许 Snort 检测引擎处理流量以进行入侵和恶意软件分析，必须为 威胁防御 设备启用 IPS 许可证。

您必须是管理员用户，才能管理网络分析、入侵策略和执行迁移任务。

在 Snort 3 生成新的 安全防火墙 建议

为入侵策略生成 安全防火墙 建议，然后按照此处列出的步骤为 Snort 3 创建新的建议规则设置根据您在 Snort 3 中选择的阈值策略，规则开销被解释为 **安全级别** 。建议的操作基于所选的安全级别，如果安全级别高于基本策略，则建议不仅限于生成事件。

在设置 安全防火墙 建议之前，您应该询问以下哪三点与目标非常匹配：

- 增强保护 - 根据主机数据库中发现的漏洞启用其他规则，并且不会自动禁用任何规则。这可能会导致更大的规则集。

- 重点保护 - 基于主机数据库中发现的漏洞启用其他规则并禁用现有规则。这可以根据发现的漏洞增加或减少规则的数量。
- 更高的效率 - 使用当前启用的规则集，并禁用主机数据库中未找到的任何漏洞规则。这可能会导致启用的规则集更小。

根据响应，建议操作如下：

- 将建议设置为下一个最高安全级别，并取消选中禁用规则。
- 将建议设置为下一个最高安全级别，并选中禁用规则。
- 将建议设置为当前安全级别，并选中禁用规则。

开始之前

安全防火墙 建议具有以下要求：

- 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

步骤 1 依次选择**策略** > **入侵**。

步骤 2 点击入侵策略的 **Snort 3 版本** 按钮。

步骤 3 点击 **建议**（**未使用**） 层以配置规则建议。点击**开始**。

在 安全防火墙 建议窗口中，您可以设置以下内容：

- **安全级别**：点击以选择安全级别。或者，您可以选中 **接受建议以禁用规则** 复选框，以禁用未在输入安全级别和受保护网络中启用的规则。仅当由于大量警报或提高检测性能而需要调整规则集时，才启用此选项。安全级别为：
  - 安全级别 1：连接优先于安全

    无影响 - 不会启用任何新规则，也不会禁用任何现有规则。如需增加保护，请选择更高的安全级别。

    更低安全性（选中复选框）- 除 Connectivity Over Security 规则集中与已发现主机上的潜在漏洞匹配的规则外，所有规则都将被禁用。建议改为调整基本策略。
  - 安全级别 2：平衡安全性优先于连接

    无影响 - 不会启用任何新规则，也不会禁用任何现有规则。如需增加保护，请选择更高的安全级别。

    更高效率（选中复选框）- 保留与已发现主机上的潜在漏洞匹配的现有规则，并禁用网络上未发现的漏洞的规则。
  - 安全级别 3：安全优先于连接

    增强安全性 - 启用与基于“最大检测”规则集的已发现主机上的潜在漏洞匹配的其他规则。

    重点安全性（选中复选框）- 启用与基于“安全优先于连接”规则集的已发现主机上的漏洞匹配的其他规则，同时禁用与已发现主机上的潜在漏洞不匹配的现有规则。

- 安全级别 4：最大检测

  增强安全性 - 启用与基于“安全优先于连接”规则集的已发现主机上的潜在漏洞匹配的其他规则。

  重点安全性（选中复选框）- 启用与基于“最大检测”规则集的已发现主机上的漏洞匹配的其他规则，同时禁用与已发现主机上的潜在漏洞不匹配的现有规则。

  注释 “最大检测”启用了大量规则，可能会影响性能。我们建议在部署到生产环境之前检查并测试此设置。

- **受保护网络**：指定为给出建议而要检查的受监控网络或单独主机。您可以从下拉列表中选择一个或多个系统或自定义定义的网络对象。默认情况下，如果未进行选择，则选择任何 IPv4 或 IPv6 网络。

  重要事项 安全防火墙规则建议取决于网络发现。受保护的网络适用于在网络发现策略中配置的范围内发现的任何主机。有关详细信息，请参阅 *Cisco Secure Firewall Management Center* 设备配置指南中 网络发现策略 章节。

点击 **添加 +** 按钮创建类型为主机或网络的新网络对象，然后点击 **保存**。

步骤 4 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（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 5 您可以验证这些建议，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** - 它会打开“建议”对话框，您可以提供建议输入值，然后生成建议。
- **全部删除** - 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。

注释 基于规则操作优先级顺序应用入侵规则的最终操作，以下是规则操作优先级顺序：

规则覆盖 > 生成的建议 > 组覆盖 > 基本 策略默认操作

对于已启用的建议，管理中心 会考虑当前状态：组覆盖、基本策略和建议配置以及操作的优先级顺序：

通过> 阻止 > 反对 > 丢弃 > 重写 > 警报

下一步做什么

部署配置更改；请参阅部署配置更改。

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。