在 Cisco Secure Firewall Management Center 中从 Snort 2 迁移到 Snort 3

从 Snort 2 迁移到 Snort 3

Snort 是一种入侵检测和防御系统，从第 2 版到第 3 版发生了重大变化。要利用 Snort 3 的增强特性和功能，从 Snort 2 迁移现有规则集变得至关重要。此迁移过程涉及将 Snort 2 规则转换并调整为 Snort 3 规则语法，并对其进行优化以提高检测和性能。

在某些情况下，组织可以由 Cisco Secure Firewall Management Center 管理威胁防御设备。在从 Snort 2 迁移到 Snort 3 期间，组织可以选择混合部署方法。此方法允许逐步过渡，并最大限度地减少潜在的中断（如果有）。

迁移到 Snort 3 的优势

- **增强的协议支持**- Snort 3 提供改进的协议支持，允许您跨各种现代协议监控和检测威胁，包括加密流量。
- **简化的规则管理**- Snort 3 提供更用户友好的规则语言和规则管理系统，使其更容易有效地创建、修改和管理规则。
- **提高性能**- Snort 3 已经过优化，可以更高效地处理更高的流量，从而降低性能瓶颈风险并确保及时检测到威胁。

示例业务情景

Alice 是一家大型组织的安全分析师，该组织严重依赖 Snort 检测引擎来监控和保护其网络基础设施。该组织多年来一直在使用 Snort 版本 2，但遇到了一些限制和挑战。

网络管理员 Bob 希望从 Snort 2 迁移到 Snort 3，以克服这些问题并增强其组织的网络安全功能。

此迁移还将改进网络安全监控，增强性能并简化规则管理。

从 Snort 2 迁移到 Snort 3 的最佳实践

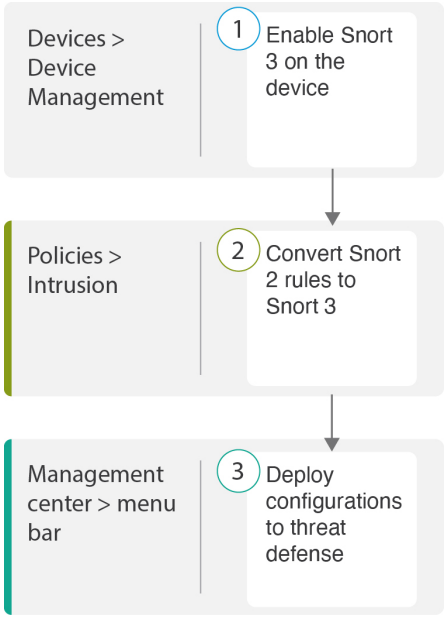
- 在执行迁移之前备份入侵策略。请参阅 *Cisco Secure Firewall Management Center* 管理指南 中的导出配置任务。
- 在将设备升级到 Snort 3 之前，如果在 Snort 2 中进行了更改，请使用同步实用程序包括从 Snort 2 到 Snort 3 的最新同步，以便您可以从类似的覆盖范围开始。请参阅将 Snort 2 规则与 Snort 3 同步。
- Snort 2 自定义规则不会自动转换为 Snort 3，必须手动迁移。请参阅将 Snort 2 自定义规则转换为 Snort 3。
- 同步不会迁移具有阈值或抑制的 Snort 2 规则。必须在 Snort 3 中重新创建这些规则。

前提条件

- 具备 Snort 的应用知识。要了解有关 Snort 3 架构的信息，请参阅 Snort 3 采用。
- 备份您的管理中心。请参阅 备份管理中心。
- 备份您的入侵策略。请参阅 导出配置。

端到端迁移工作流程

以下流程图说明了在Cisco Secure Firewall Management Center 中迁移 Snort 2 到 Snort 3 的工作流程。



步骤	说明
1	在设备上启用 Snort 3。请参阅在威胁防御上启用 Snort 3，第 3 页。
2	将 Snort 2 规则转换为 Snort 3。请参阅将单个入侵策略的 Snort 2 规则转换为 Snort 3，第 4 页。
3	部署配置。请参阅部署配置更改。

在威胁防御上启用 Snort 3

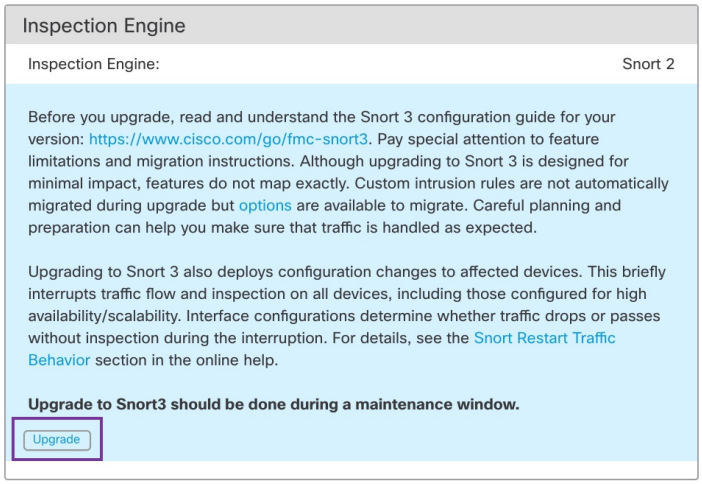
注意 在部署过程中，由于需要关闭当前检测引擎，因此会出现短暂的流量丢失。

步骤 1 选择**设备** > **设备管理**。

步骤 2 点击相应的设备以转到设备主页。

步骤 3 点击**设备 (Device)** 选项卡。

步骤 4 在 **检测引擎 (Inspection Engine)** 部分中，点击 **升级 (Upgrade)**。



步骤 5 点击 **Yes**。

下一步做什么

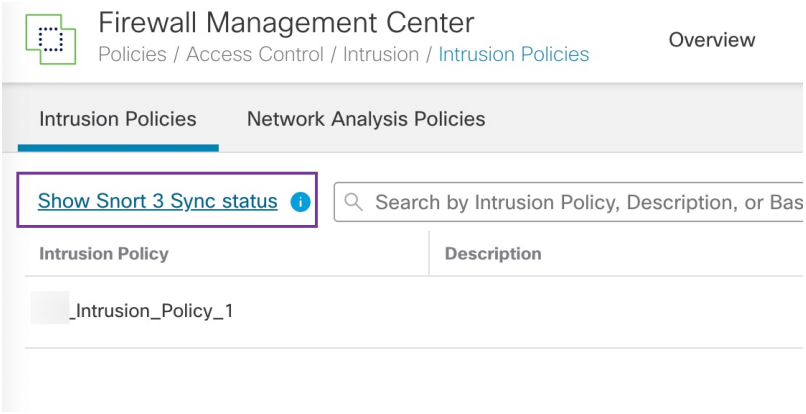
在设备上部署更改。请参阅部署配置更改。

系统会在部署过程中转换您的策略配置，使其与所选的 Snort 版本兼容。

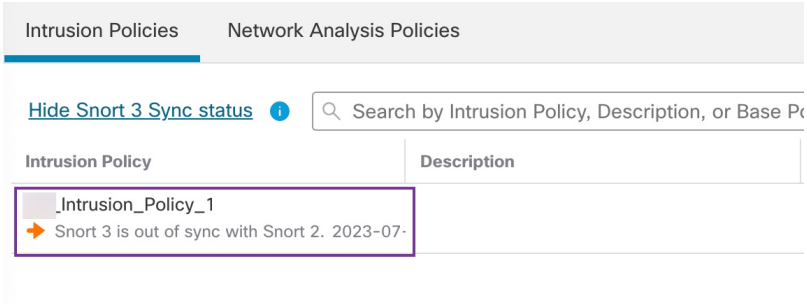
将单个入侵策略的 Snort 2 规则转换为 Snort 3

步骤 1 依次选择**策略** > **入侵**。

步骤 2 在 **入侵策略** 选项卡中，点击 **显示 Snort 3 同步状态**。

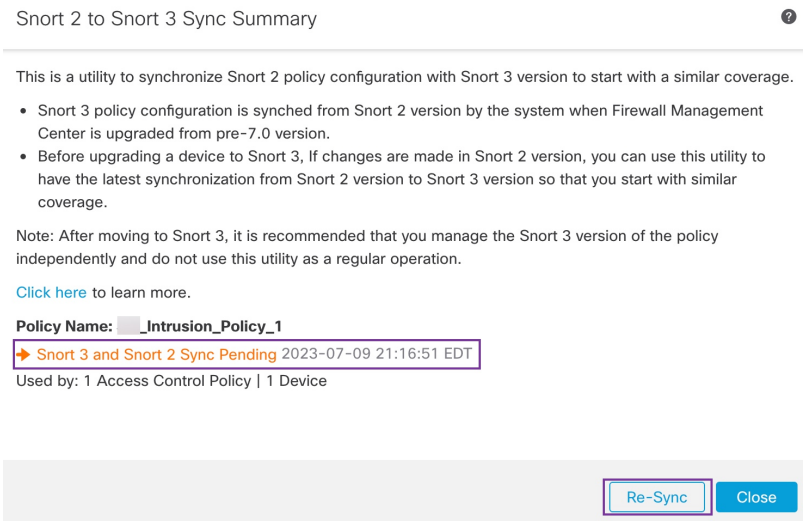


如果策略显示橙色箭头，则表示入侵策略的 Snort 2 和 Snort 3 版本未同步。



步骤 3 点击橙色箭头。

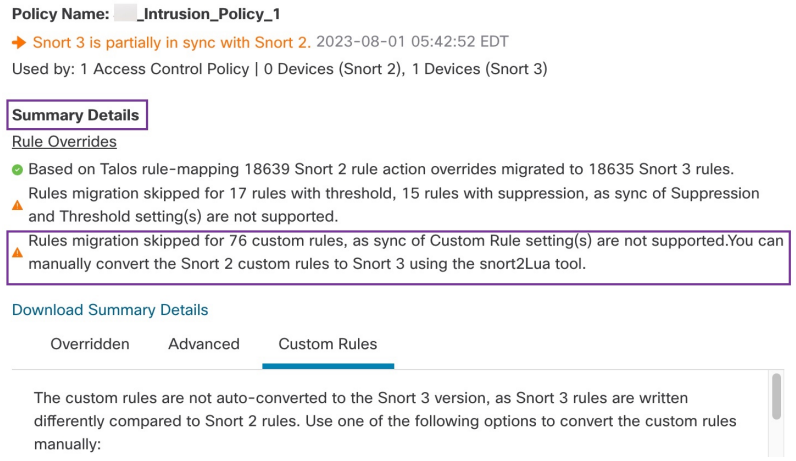
Snort 2 到 Snort 3 同步摘要 页面显示 Snort 2 到 Snort 3 的同步正在等待处理。



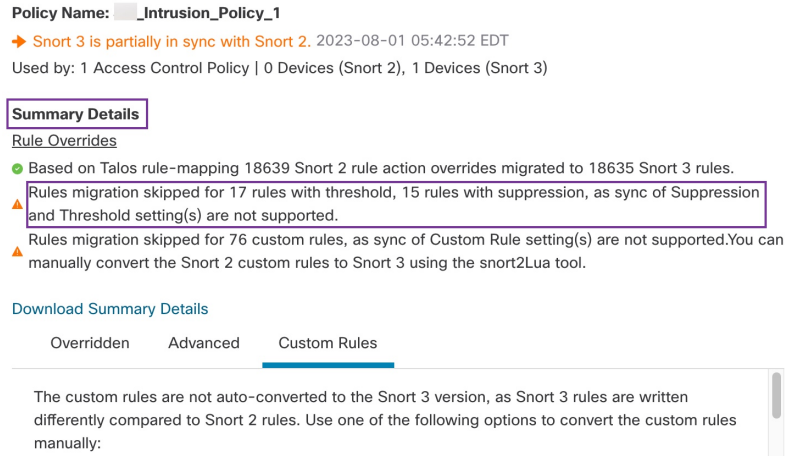
步骤 4 点击 **重新同步** 以开始同步。

注释 点击 **重新同步**时，snort2Lua 工具会将规则从 Snort 2 转换为 Snort 3。

摘要详细信息 部分列出已迁移或跳过的规则。在我们的使用案例中，有 76 个自定义 Snort 2 规则、17 个具有阈值的规则和 15 个在同步过程中跳过的规则。要迁移自定义规则，请转至下一步。

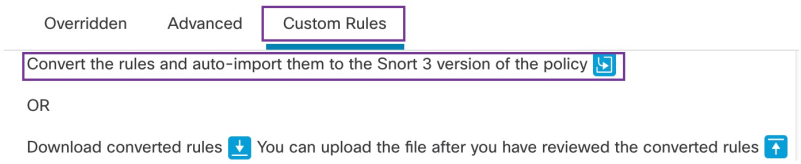


要迁移具有阈值和抑制的规则，请转至 步骤 6。



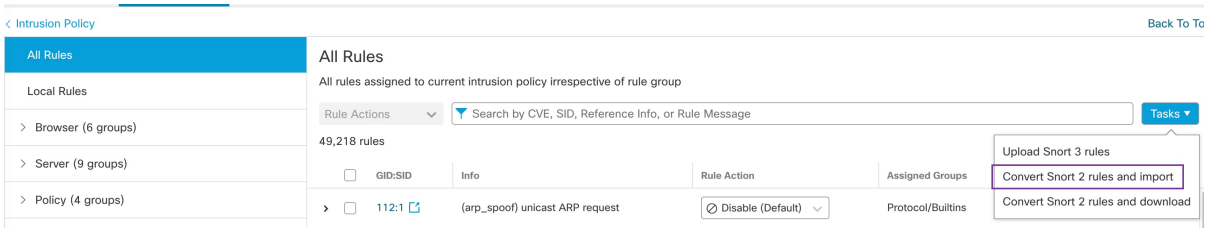
步骤 5 要迁移 76 条自定义规则，请执行以下任一步骤：

- 在 **自定义规则** 选项卡中，点击 **导入** 图标以将本地规则转换并自动导入到 Snort 3 版本的策略。

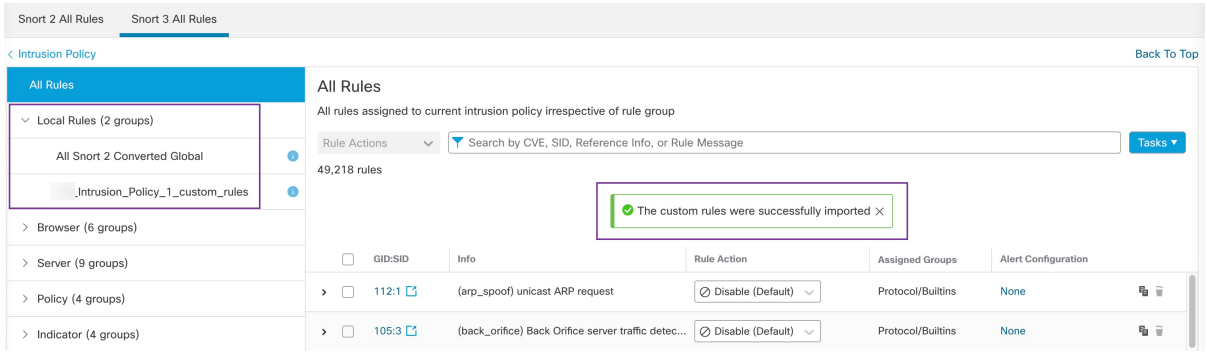


  成功导入规则后，系统将显示确认消息。

- 选择 **对象 > 入侵规则** 并点击 **Snort 3 所有规则**。
  1. 点击左侧面板中的 **本地规则** ，检查是否已迁移任何规则。请注意，尚未迁移 Snort 2 中的任何自定义规则。
  2. 从 **任务** 下拉列表中，选择 **转换 Snort 2 规则并导入**。

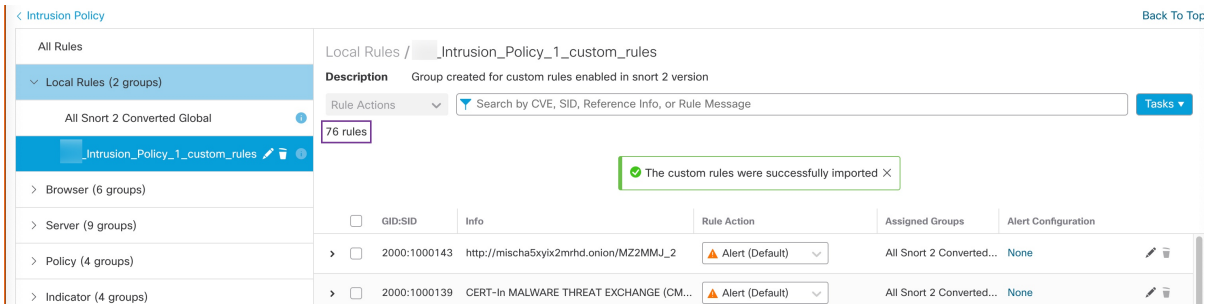


3. 点击**确定 (OK)**。



系统将在左侧面板的 **本地规则**下创建新创建的规则组（**所有 Snort 2 已转换的全局** 规则）。

请注意，所有 76 条自定义规则均已迁移，如下图所示。



或者，您可以在上一步中选择 **转换 Snort 2 规则并下载**，以在本地保存规则文件。您可以在下载的文件中查看转换后的规则，然后通过使用 **上传 Snort 3 规则** 选项上传文件。

步骤 6 点击 **下载摘要详细信息** 链接，以 .txt 格式下载规则。

以下是显示的摘要示例。

```
"id": "00505691-15DC-0ed3-0000-004294988561",
"name": "_Intrusion_Policy_1",
"type": "IntrusionPolicy",
"syncStatus": {
  "source": {
    "id": "bdce2d6a-1ebe-11ee-8e88-220032eb1fb5",
    "type": "IntrusionPolicy"
  },
  "status": "WARN",
  "description": "Migration is partially successful. Some of the rules are not copied to Snort3.",
  "timestamp": 1690883954814,
  "lastUser": {
```

```
      "name": "admin"
    },
    "details": [
      {
        "type": "Summary",
        "status": "INFO",
        "description": "Based on Talos rule-mapping 18639 Snort 2 rule action overrides migrated to
18635 Snort 3 rules."
      },
      {
        "id":
"1:1000156=alert,1:1000114=alert,1:1000160=alert,1:1000135=alert,1:1000115=alert,1:1000118=alert,

1:1000092=alert,1:1000139=alert,1:1000123=alert,1:1000159=alert,1:1000149=disabled,1:1000167=alert,

1:1000133=alert,1:1000095=alert,1:1000143=alert,1:1000106=alert,1:1000153=alert,1:1000097=alert,1:1000141=alert,


1:1000148=alert,1:1000090=alert,1:1000119=alert,1:1000112=alert,1:1000138=alert,1:1000128=alert,1:1000132=alert,


1:1000134=alert,1:1000145=disabled,1:1000110=disabled,1:1000107=alert,1:1000163=alert,1:1000124=alert,1:1000125=alert,


1:1000094=alert,1:1000113=disabled,1:1000147=alert,1:1000161=alert,1:1000105=disabled,1:1000140=alert,1:1000111=alert,


1:1000102=alert,1:1000129=disabled,1:1000108=alert,1:1000144=disabled,1:1000088=alert,1:1000091=alert,1:1000131=alert,


1:1000157=alert,1:1000120=alert,1:1000126=alert,1:1000165=alert,1:1000146=alert,1:1000162=alert,1:1000116=alert,1:1000142=alert,


1:1000170=disabled,1:1000169=alert,1:1000104=alert,1:1000099=disabled,1:1000171=alert,1:1000093=alert,1:1000087=alert,1:1000100=alert,


1:1000137=alert,1:1000158=alert,1:1000103=alert,1:1000098=alert,1:1000127=disabled,1:1000130=alert,1:1000164=alert,1:1000089=alert,

         1:1000109=alert,1:1000136=alert,1:1000117=alert,1:1000166=alert,1:1000168=alert",
        "type": "PolicyInfo",
        "description": "Corresponding Snort 2 policy overridden custom (local) rules."
      },
      {
        "type": "AssignedDevices",
        "status": "INFO",
        "description": "Snort3:0 , Snort2:0"
      },
      {
        "id": "122:6",
        "type": "Threshold",
        "status": "ERROR",
        "description": "PSNG_TCP_FILTERED_DECOY_PORTSCAN"
      },
      {
        "id": "122:15",
        "type": "Threshold",
        "status": "ERROR",
        "description": "PSNG_IP_PORTSWEEP_FILTERED"
       },
      {
        "id": "122:1",
        "type": "Threshold",
        "status": "ERROR",
```

```
    "description": "PSNG_TCP_PORTSCAN"
  },
```

步骤 7 点击 **关闭** 以关闭 **同步摘要** 对话框。

步骤 8 要检查状态为 ERROR 的规则，请依次选择 **策略 > 入侵** ，然后点击入侵策略的 **Snort 2** 版本。

步骤 9 在 **策略信息**下，点击 **规则** 并过滤规则。例如，在 **过滤器** 字段中输入 **PSNG_TCP_PORTSCAN**以查找规则。

步骤 10 点击 **显示详细信息** 以查看规则的详细版本。

步骤 11 使用 Snort 3 规则准则在 Snort 3 中再次创建规则，并将文件另存为 .txt 或 .rules 文件。有关详细信息，请参阅 www.snort3.org。

步骤 12 将您在本地创建的自定义规则上传到所有 Snort 3 规则的列表中。请参阅 将自定义规则添加到规则组。

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。

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 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 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 管理中心的 **预览**页上显示为过期。

步骤 3 点击 **部署**。

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。