

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

- •从 Snort 2 迁移到 Snort 3,第1页
- •迁移到 Snort 3 的优势,第1页
- •示例业务情景,第2页
- •从 Snort 2 迁移到 Snort 3 的最佳实践, 第 2 页
- 前提条件, 第2页
- 端到端迁移工作流程,第2页
- 在威胁防御上启用 Snort 3, 第3页
- •将单个入侵策略的 Snort 2 规则转换为 Snort 3,第4页
- •部署配置更改,第9页

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-Snort3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)。

Inspection Engine	
Inspection Engine:	Snort 2
Before you upgrade, read and understand the Snort 3 configuration guide for you version: https://www.cisco.com/go/fmc-snort3. Pay special attention to feature limitations and migration instructions. Although upgrading to Snort 3 is designed minimal impact, features do not map exactly. Custom intrusion rules are not autor migrated during upgrade but options are available to migrate. Careful planning a preparation can help you make sure that traffic is handled as expected.	ur for omatically nd
Upgrading to Snort 3 also deploys configuration changes to affected devices. The interrupts traffic flow and inspection on all devices, including those configured for availability/scalability. Interface configurations determine whether traffic drops or without inspection during the interruption. For details, see the Snort Restart Traffic Behavior section in the online help.	iis briefly ir high i passes ic
Upgrade to Snort3 should be done during a maintenance window.	

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。

Intrusion Policies	Network An	nalysis Policies	
Hide Snort 3 Sync st	tatus ()	्र Search by Intrusion Policy, Description, or Base	P
Intrusion Policy		Description	
_Intrusion_Policy_1 → Snort 3 is out of synd	c with Snort 2. 2	2023-07-	

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。

Snort 2 to Snort 3 Sync Summary	0
This is a utility to synchronize Snort 2 policy configuration with Snort 3 version to start with a similar coverage	ge.
 Snort 3 policy configuration is synched from Snort 2 version by the system when Firewall Management Center is upgraded from pre-7.0 version. Before upgrading a device to Snort 3, If changes are made in Snort 2 version, you can use this utility to have the latest synchronization from Snort 2 version to Snort 3 version so that you start with similar coverage. 	
Note: After moving to Snort 3, it is recommended that you manage the Snort 3 version of the policy independently and do not use this utility as a regular operation.	
Click here to learn more.	
Policy Name:Intrusion_Policy_1 → Snort 3 and Snort 2 Sync Pending 2023-07-09 21:16:51 EDT Used by: 1 Access Control Policy 1 Device	
Re-Sync Close	•

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。

	Policy Name:Intrusion_Policy_1
	→ Snort 3 is partially in sync with Snort 2, 2023-08-01 05:42:52 EDT
	Used by: 1 Access Control Policy 0 Devices (Snort 2), 1 Devices (Snort 3)
	Summary Details
	<u>Kule Overnoes</u>
	Based on tailor fulle-mapping 18639 Short 2 rule action overrides migrated to 18635 Short 2 rules. Builds migration stimped for 13 rules with threshold 15 rules with suppression as super 5 superssion
	and Threshold setting(s) are of supported.
	Rules migration skipped for 76 custom rules, as sync of Custom Rule setting(s) are not supported.You can
	manually convert the Snort 2 custom rules to Snort 3 using the snort2Lua tool.
	Download Summary Details
	Overridden Advanced Custom Rules
	The custom rules are not auto-converted to the Snort 3 version, as Snort 3 rules are written
	manually:
	要迁移具有阈值和抑制的规则,请转至步骤 6。
	Policy Name: _Intrusion_Policy_1
	→ Snort 3 is partially in sync with Snort 2, 2023-08-01 05:42:52 EDT
	Used by: 1 Access Control Policy 0 Devices (Snort 2), 1 Devices (Snort 3)
	Summary Details
	Rule Overrides
	Based on Talos rule-mapping 18639 Snort 2 rule action overrides migrated to 18635 Snort 3 rules.
	Rules migration skipped for 17 rules with threshold, 15 rules with suppression, as sync of Suppression
	and Threshold setting(s) are not supported.
	A Rules migration skipped for 76 custom rules, as sync of Custom Rule setting(s) are not supported.You can
	manually convert the Snort 2 custom rules to Snort 3 using the snort2Lua tool.
	Download Summary Details
	Overridden Advanced Custom Rules
	The custom rules are not auto-converted to the Snort 3 version, as Snort 3 rules are written
	ainerentity compared to Short 2 rules. Use one of the following options to convert the custom rules manually.
-	要迁移 76 条白完义抑则 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。

Overridden	Advanced	Custom Rules	
Convert the rules	and auto-imp	ort them to the Sno	rt 3 version of the policy 🔄
OR			
Download conver	rted rules 🛃 Y	ou can upload the	file after you have reviewed the converted rules 🚹

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。

< Intrusion Policy					Back To To			
All Rules	All Rules							
Local Rules	All rules assigned to cur	Il rules assigned to current intrusion policy irrespective of rule group						
> Browser (6 groups)	Rule Actions 🗸 🗸	Rule Actions V Search by CVE, SID, Reference Info, or Rule Message						
	49,218 rules				Upload Snort 3 rules			
> Server (9 groups)	GID:SID	Info	Rule Action	Assigned Groups	Convert Snort 2 rules and import			
> Policy (4 groups)	> 🗌 112:1 🖬	(arp_spoof) unicast ARP request	🖉 Disable (Default) 🗸	Protocol/Builtins	Convert Snort 2 rules and download			

3. 点击确定 (OK)。

Snort 2 All Rules Snort 3 All Rules								
< Intrusion Policy	Intrusion Policy B							
All Rules		All Rules						
V Local Rules (2 groups)		All rules assigned to curr	ent intrusion policy irrespective of rule	group				
All Snort 2 Converted Global	0	Rule Actions V	Search by CVE, SID, Reference Inf	o, or Rule Message			Tasks 🔻	
Intrusion_Policy_1_custom_rules	0	43,21010163						
> Browser (6 groups)				he custom rules were successfully impor	ied ×			
> Server (9 groups)		GID:SID	Info	Rule Action	Assigned Groups	Alert Configuration		
> Policy (4 groups)		> 🗌 112:1 🖸	(arp_spoof) unicast ARP request	🖉 Disable (Default) 🗸 🗸	Protocol/Builtins	None	5 V	
> Indicator (4 groups)		> 🗌 105:3 Ґ	(back_orifice) Back Orifice server traffic	c detec 🖉 Disable (Default) 🗸	Protocol/Builtins	None	¶a ₩	

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。

< Intrusion Policy								Back To Top
All Rules	Local Rul	ocal Rules /Intrusion_Policy_1_custom_rules						
✓ Local Rules (2 groups)	Description	Group cre	eated for custom rules enabled	in snort 2 versio	on			
All Snort 2 Converted Global	Rule Action	ns 🗸 🤇	Y Search by CVE, SID, Referen	nce Info, or Rule	e Message			Tasks 🔻
_Intrusion_Policy_1_custom_rules 🖍 🗑 🕕				The custor	m rules were successfully imported	×		
> Browser (6 groups)				• The custo	The succession montee			
> Server (9 groups)		GID:SID	Info		Rule Action	Assigned Groups	Alert Configuration	
> Policy (4 groups)	> 🗆 2	2000:1000143	http://mischa5xyix2mrhd.onion/	MZ2MMJ_2	🔺 Alert (Default) 🗸	All Snort 2 Converted	None	11
> Indicator (4 groups)	> 🗌 2	2000:1000139	CERT-In MALWARE THREAT EX	CHANGE (CM	🔺 Alert (Default) 🗸 🗸	All Snort 2 Converted	None	11

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",
    "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,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:1000146=alert,1:
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** (こ)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。