



Cisco 安全防火墙管理中心 Snort 3 配置指南，版本 7.2

首次发布日期: 2022 年 6 月 6 日

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. 保留所有权利。



目录

第 1 章

网络分析和入侵策略概述 1

网络分析和入侵策略基础知识 1

Snort 检测引擎 2

Snort 3 2

策略如何检查流量是否存在入侵 4

解码、规范化和预处理：网络分析策略 5

访问控制规则：入侵策略选择 6

入侵检查：入侵策略、规则和变量集 6

入侵事件生成 8

系统提供的与自定义的网络分析和入侵策略 8

系统提供的网络分析和入侵策略 9

自定义网络分析和入侵策略的优势 10

自定义网络分析策略的优势 10

自定义入侵策略的优势 11

自定义策略的限制 12

网络分析和入侵策略的许可证要求 14

网络分析和入侵策略的要求和必备条件 14

第 2 章

从 Snort 2 迁移到 Snort 3 15

Snort 2 与 Snort 3 15

管理中心管理的威胁防御的 Snort 3 的功能限制 16

从 Snort 2 迁移到 Snort 3 17

Snort 2 自定义规则的转换工具 17

启用和禁用 Snort 3 17

- 在单个设备上启用和禁用 Snort 3 18
- 在多台设备上启用和禁用 Snort 3 18
- 查看 Snort 2 和 Snort 3 基本策略映射 19
- 将 Snort 2 规则与 Snort 3 同步 19

第 1 部分：**Snort 3 中入侵检测和预防 21**

第 3 章 **Snort 3 入侵策略入门 23**

- 入侵策略基础知识 23
- 入侵策略的要求和必备条件 24
- 创建自定义 Snort 3 入侵策略 25
- 编辑 Snort 3 入侵策略 25
 - 规则操作日志记录 28
- 更改入侵策略的基本策略 28
- 更改 Snort 2 和 Snort 3 版本的入侵策略检测模式 29
- 管理入侵策略 29
- 用于执行入侵防御的访问控制规则配置 30
 - 访问控制规则配置和入侵策略 31
 - 配置访问控制规则以执行入侵防御 31
- 部署配置更改 31

第 4 章 **使用规则调整入侵策略 33**

- 入侵规则调整基础知识 33
- 入侵规则类型 34
- 入侵规则的许可证要求 35
- 入侵规则的要求和必备条件 35
- Snort 3 中的自定义规则 35
- 查看入侵策略中的 Snort 3 入侵规则 36
- 入侵规则操作 36
 - 入侵规则操作选项 36
 - 设置入侵规则操作 37

入侵策略中的入侵事件通知过滤器	38
入侵事件阈值	38
入侵事件阈值配置	38
在 Snort 3 中为入侵规则设置阈值	40
查看和删除入侵事件阈值	40
入侵策略抑制配置	41
入侵策略抑制类型	41
在 Snort 3 中为入侵规则设置抑制	41
查看和删除抑制条件	42
添加入侵规则注释	42
将 Snort 2 自定义规则转换为 Snort 3	43
将所有入侵策略中的所有 Snort 2 自定义规则转换为 Snort 3	43
将单个入侵策略的 Snort 2 自定义规则转换为 Snort 3	44
上传自定义规则	44
将具有自定义规则的规则组添加到入侵策略	45
管理 Snort 3 中的自定义规则	46
删除自定义规则	47
删除规则组	47
<hr/>	
第 5 章	根据网络资产定制入侵防护 49
	LSP 更新中的 Snort 3 规则更改 49
	关于 安全防火墙 建议的规则 49
	为 Snort 3 生成新的 安全防火墙 建议 50
	为 Snort 3 生成 安全防火墙 建议：升级场景 52
<hr/>	
第 11 部分：	Snort 3 中的高级网络分析 55
<hr/>	
第 6 章	网络分析策略入门 57
	网络分析策略基础知识 57
	网络分析策略的许可证要求 58
	网络分析策略的要求和必备条件 58

管理网络分析策略	58
网络分析策略的 Snort 3 定义和术语	59
为 Snort 3 的自定义网络分析策略创建	61
网络分析策略映射	64
查看网络分析策略映射	65
创建网络分析策略	65
修改网络分析策略	65
在网络分析策略页面上搜索检查器	66
复制检查器配置	66
自定义网络分析策略	67
对检查器进行内联编辑以覆盖配置	70
在内联编辑期间恢复未保存的更改	70
查看具有覆盖的检查器列表	71
将覆盖的配置恢复为默认配置	71
验证 Snort 3 策略	72
自定义网络分析策略配置示例	73
网络分析策略设置和缓存的更改	84



第 1 章

网络分析和入侵策略概述

“网络分析和入侵策略概述”一章概述了 Snort 检测引擎以及网络分析和入侵策略。它可以让您深入了解系统提供的和自定义的网络分析和入侵策略，以及这些策略的要求和前提条件。

- [网络分析和入侵策略基础知识，第 1 页](#)
- [Snort 检测引擎，第 2 页](#)
- [Snort 3，第 2 页](#)
- [策略如何检查流量是否存在入侵，第 4 页](#)
- [系统提供的与自定义的网络分析和入侵策略，第 8 页](#)
- [网络分析和入侵策略的许可证要求，第 14 页](#)
- [网络分析和入侵策略的要求和必备条件，第 14 页](#)

网络分析和入侵策略基础知识

网络分析和入侵策略作为入侵检测和防御功能的一部分，共同发挥作用。

- 术语入侵检测通常是指被动监控并分析网络流量以查找潜在入侵，并存储攻击数据以进行安全分析的过程。这有时称为“IDS”。
- 术语入侵防御包括入侵检测的概念，但是增加了在恶意流量流经网络时对其进行拦截或更改的能力。这有时称为“IPS”。

在入侵防御部署中，当系统检测数据包时：

- **网络分析策略**监管如何解码和预处理流量，以便可进一步对其进行评估，尤其适用于可能表明入侵尝试的异常流量。
- **入侵策略**使用入侵和预处理程序规则（有时统称为入侵规则）根据模式检测已解码数据包是否存在攻击。入侵策略与变量集配对，这使您能够使用指定值准确反映网络环境。

网络分析和入侵策略均由父访问控制策略调用，但是在不同时间调用。在系统分析流量时，网络分析（解码和预处理）阶段发生在入侵防御（其他预处理和入侵规则）阶段之前并与其分隔开来。网络分析和入侵策略共同提供广泛且深入的数据包检测。它们可以帮助您检测、提醒和防范可能威胁主机及其数据的可用性、完整性和保密性的网络流量。

系统随附若干以类似方式命名的网络分析和入侵策略（例如，平衡安全性和连接），这些策略是相辅相成的。通过使用系统提供的策略，您可以利用思科 Talos 情报小组 (Talos) 的经验。对于这些策略，Talos 提供入侵和检查器规则状态及对检查器和其他高级设置的初始配置。

您还可以创建自定义网络分析和入侵策略。您可以调整自定义策略中的设置，以对您最重要的方式检查流量，从而能够提高受管设备的性能以及您有效响应其生成的事件的能力。

您可在网络界面中使用相似的策略编辑器创建、编辑、保存和管理网络分析和入侵策略。在您编辑任一类型的策略时，导航面板显示在网络界面的左侧；右侧显示各种配置页面。

有关其他支持和信息，请参阅视频：

- [Snort 3 简明概述](#)
- [Snort 3 扩展概述](#)

Snort 检测引擎

Snort 检测引擎是 Cisco Secure Firewall Threat Defense（前称 Firepower 威胁防御）设备不可或缺的一部分。检测引擎实时分析流量，以提供深度数据包检测。网络分析和入侵策略共同利用 Snort 检测引擎的功能来检测和防御入侵。

Snort 3

Snort 3 是最新版本的 Snort 检测引擎，与早期版本的 Snort 相比有很大改进。旧版本的 Snort 是 Snort 2。Snort 3 更高效，可提供更好的性能和可扩展性。

与 Snort 2 相比，Snort 3 在架构上进行了重新设计，以使用相同的资源检查更多流量。Snort 3 提供简化且灵活的流量解析器插入。Snort 3 还提供了新的规则语法，使规则编写更加容易，并且共享对象规则等效项可见。

Snort 3 的其他重大变化包括：

- 与使用多个 Snort 实例的 Snort 2 不同，Snort 3 将多个线程与单个 Snort 实例相关联。这会使用更少的内存，缩短 Snort 重新加载时间，并支持更多入侵规则和更大的网络映射。Snort 线程的数量因平台而异，与每个平台的 Snort 2 实例数量相同。使用几乎是透明的。
- Snort 版本 per 威胁防御 - Snort 检测引擎是威胁防御特定的，而不是 Cisco Secure Firewall Management Center（前称 Firepower Management Center）特定的。管理中心可以管理多个威胁防御，每个都使用任一版本的 Snort（Snort 2 和 Snort 3）。虽然管理中心的入侵策略是唯一的，但系统会应用 Snort 2 或 Snort 3 版本的入侵策略，具体取决于设备所选的检测引擎。有关设备上检测引擎的详细信息，请参阅 [启用和禁用 Snort 3，第 17 页](#)。
- 解码器规则 - 仅在默认入侵策略中触发数据包解码器规则。系统会忽略您在其他策略中启用的解码器规则。
- 共享对象规则 - Snort 3 支持部分但不是全部共享对象 (SO) 入侵规则（生成器 ID (GID) 为 3 的规则）。不支持的已启用共享对象规则不会触发。

- 安全情报的多层检测 - Snort 2 检测多层流量中的两层。Snort 3 会检测最内部的 IP 地址，而不考虑层。
- 硬件支持 - 仅 威胁防御 7.0 及更高版本支持 Snort 3。ASA 5500-X 或 Firepower 7000 和 8000 系列设备不支持 Snort 3。
- 受管设备 - 版本 7.0 的管理中心可以同时支持版本 6.4、6.5、6.6、6.7 和 7.0 Snort 2 威胁防御以及版本 7.0 Snort 3 威胁防御。
- 切换 Snort 版本时的流量中断 - 切换 Snort 版本会中断流量检查，并且在部署期间可能会丢弃一些数据包。
- 统一策略 - 无论受管 威胁防御中启用的底层 Snort 引擎版本如何，管理中心中配置的控制策略、入侵策略、网络访问策略均可在应用策略时无缝地工作。管理中心版本 7.0 及更高版本中的所有入侵策略都有两个可用版本：Snort 2 版本和 Snort 3 版本。虽然入侵策略有两个版本（Snort 2 版本和 Snort 3 版本），但它具有统一的名称、基本策略和检测模式。Snort 2 和 Snort 3 版本的入侵策略在规则设置方面可能不同。但是，在设备上应用入侵策略时，系统会自动识别设备上启用的 Snort 版本，并应用为该版本配置的规则设置。
- 轻量级安全软件包 (LSP) - 替换 Snort 3 下一代入侵规则和配置更新的 SRU。下载更新会同时下载 Snort 3 LSP 和 Snort 2 SRU。

LSP 更新提供新的和更新后的入侵规则和检查器规则、现有规则的修改后状态以及管理中心和威胁防御版本 7.0 或更高的修改后的默认入侵策略设置。当您从管理中心从 6.7 或更低版本升级到 7.0 时，它同时支持 LSP 和 SRU。LSP 更新还可能删除系统提供的规则，提供新规则类别和默认变量，并修改默认变量值。有关 LSP 更新的详细信息，请参阅最新版本的 *Firepower* 管理中心配置指南中的更新入侵规则主题。

- Snort 2 和 Snort 3 规则和预设的映射 - 映射 Snort 2 和 Snort 3 规则，并且映射由系统提供。但是，它不是一对一映射。系统提供的入侵基本策略是为 Snort 2 和 Snort 3 预配置的，它们提供相同的入侵防御，但规则集不同。系统为 Snort 2 和 Snort 3 提供的基本策略针对相同的入侵防御设置相互映射。有关详细信息，请参阅[查看 Snort 2 和 Snort 3 基本策略映射](#)，第 19 页。
- 同步 Snort 2 和 Snort 3 规则覆盖 - 威胁防御升级到 7.0 后，可以将威胁防御的检测引擎升级到 Snort 3 版本。管理中心使用 Talos 提供的映射将 Snort 2 版本入侵策略的现有规则中的所有覆盖映射到相应的 Snort 3 规则。但是，如果在升级后执行了其他覆盖，或者如果您安装了版本为 7.0 的新威胁防御，则必须手动进行同步。有关详细信息，请参阅[将 Snort 2 规则与 Snort 3 同步](#)，第 19 页。
- 自定义入侵规则 - 您可以在 Snort 3 中创建自定义入侵规则。您还可以将 Snort 2 的自定义入侵规则导入到 Snort 3。有关详细信息，请参阅[Snort 3 中的自定义规则](#)，第 35 页。
- 规则组-管理中心将属于系统提供的基本策略的 Snort 3 规则分组到规则组中。规则组是规则的逻辑组，提供简单的管理界面，以增强规则可访问性、规则导航以及对规则组安全级别的更好控制。
- 在 Snort 2 和 Snort 3 引擎之间切换-威胁防御支持 Snort3 的也可以支持 Snort 2。从效率的角度来看，不建议从 Snort 3 切换到 Snort 2。但是，如果需要交换机，请按照[启用和禁用 Snort 3](#)，第 17 页中的说明进行操作。

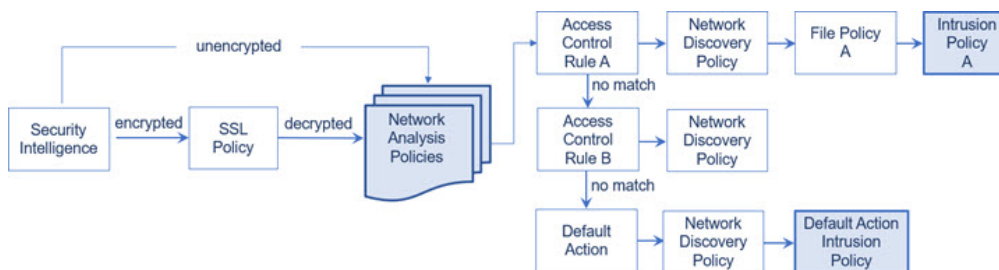


重要事项 虽然您可以自由切换 Snort 版本，但一个版本的 Snort 中的入侵规则更改不会自动更新到另一个版本中。如果在一个版本的 Snort 中更改规则的规则操作，请确保在切换 Snort 版本之前复制另一个版本中的更改。系统提供的同步选项仅将 Snort 2 版本的入侵策略更改同步到 Snort 3 版本，而不是相反。

策略如何检查流量是否存在入侵

当系统在访问控制部署过程中分析流量时，网络分析（解码和预处理）阶段发生在入侵防御（入侵规则和高级设置）阶段之前并与其分隔开来。

下图以简化方式显示网络部署的内联、入侵防御和 AMP 中的流量分析顺序。它说明访问控制策略如何调用其他策略来检测流量，以及这些策略的调用顺序。网络分析和入侵策略选择阶段突出显示。



在内联部署中（即，使用路由接口、交换接口、透明接口或内联接口对将相关配置部署到设备），系统可以在图示过程中的几乎任何步骤阻止流量而不进行进一步检查。安全智能、SSL 策略、网络分析策略、文件策略和入侵策略均可以丢弃或修改流量。只有网络发现策略（被动检测数据包）无法影响流量的流动。

类似地，在该过程的每个步骤中，数据包都可能会导致系统生成事件。入侵和预处理程序事件（有时统称为入侵事件）指示数据包或其内容可能表示安全风险。



提示 当您的 SSL 配置允许已加密流量通过，或者您未配置 SSL 检查时，此图未反映访问控制规则处理已加密流量。默认情况下，系统禁用对已加密负载的入侵和文件检查。当已加密连接与已配置入侵和文件检查的访问控制规则相匹配时，这有助于减少误报和提高性能。

请注意，对于单个连接而言，虽然系统在访问控制规则之前选择网络分析策略（如图所示），但是一些预处理（特别是应用层预处理）发生在访问控制规则选择之后。这不会影响您在自定义网络分析策略中配置预处理的方式。

解码、规范化和预处理：网络分析策略

如果没有解码和预处理，则系统无法适当评估流量是否存在入侵，因为协议差异使得无法进行模式匹配。网络分析策略在以下时机监管这些流量处理任务：

- 在流量由安全智能过滤之后
- 在加密流量由可选 SSL 策略解密之后
- 在流量可由文件或入侵策略检测之前

网络分析策略分阶段监管数据包处理。系统首先通过前三个 TCP/IP 层解码数据包，然后继续规范化、预处理和检测协议异常：

- 数据包解码器将数据包报头和负载转换为可由检查器并在以后由入侵规则轻松使用的格式。TCP/IP 堆栈的各层从数据链路层开始并持续到网络层和传输层依次解码。数据包解码器还会检测数据包报头中的各种异常行为。
- 在内联部署中，内联规范化预处理程序重新格式化（规范化）流量，以尽量降低攻击者逃避检测的可能性。它会准备数据包以供其他检查器和入侵规则进行检测，并且帮助确保系统处理的数据包与网络上主机接收的数据包相同。
- 各种网络层和传输层检查器检测利用 IP 分段的攻击，执行校验和验证并执行 TCP 和 UDP 会话预处理。

请注意，一些高级传输和网络检查器设置全局适用于由访问控制策略的目标设备处理的所有流量。您在访问控制策略中而不是在网络分析策略中配置这些高级设置。

- 各种应用层协议解码器将特定类型的数据包数据规范化为入侵规则引擎可以分析的格式。通过规范化应用层协议编码，系统可以将相同的内容相关的入侵规则有效地应用于以不同方式表示其数据的数据包，并且获取有意义的结果。
- Modbus、DNP3、CIP 和 s7commplus SCADA 检查器可检测流量异常并向入侵规则提供数据。监控与数据采集(SCADA)协议可监视和控制工业、基础设施以及工厂流程（例如制造、生产、水处理、配电、机场和运输系统等）并从中获取数据。
- 通过若干检查器，可以检测特定威胁，如 Back Orifice、端口扫描、SYN 泛洪和其他基于速率的攻击。

请注意，您在入侵策略中配置敏感数据检查器，该预处理器用于检测敏感数据（例如，ASCII 文本中的信用卡号和社会安全保障号）。

在新建的访问控制策略中，一个默认网络分析策略监管对同一父访问控制策略调用的所有入侵策略的所有流量的预处理。最初，系统使用“平衡安全性和连接” (Balanced Security and Connectivity) 网络分析策略作为默认值，但是，可以将其更改为另一个系统提供的网络分析策略或自定义网络分析策略。在更复杂的部署中，高级用户可以分配自定义网络分析策略以预处理匹配流量，从而根据特定安全区域、网络和 VLAN 定制流量预处理选项。

访问控制规则：入侵策略选择

在初始预处理后，访问控制规则（如果存在）会评估流量。在大多数情况下，数据包匹配的第一条访问控制规则处理该流量；您可以监控、信任、阻止或允许匹配流量。

当使用访问控制规则允许流量时，系统可能按该顺序检查流量是否存在发现数据、恶意软件、受禁文件和入侵。不与任何访问控制规则匹配的流量由访问控制策略的默认操作进行处理，该操作还检查是否存在发现数据和入侵。



注释 所有数据包（无论哪个网络分析策略对其进行预处理）均与配置的访问控制规则相匹配，因此可能会由上而下受到入侵策略的检测。

[策略如何检查流量是否存在入侵，第 4 页](#) 中的图显示流经内联的入侵防御和 AMP 网络部署中的设备的流量，如下所示：

- Access Control Rule A 允许匹配流量通过。然后该流量由网络发现策略检查是否存在发现数据，由文件策略 A 检查是否存在受禁文件和恶意软件，最后由入侵策略 A 检查是否存在入侵。
- 访问控制规则 B 也允许匹配流量通过。但是，在此情景中，未检查流量是否存在入侵（或文件或恶意软件），因此没有与规则关联的入侵或文件策略。请注意，默认情况下，您允许通过的流量将由网络发现策略进行检查；您不需要配置此检查。
- 在此情景中，访问控制策略的默认操作允许匹配流量。然后该流量将依次由网络发现策略和入侵策略进行检查。将入侵策略与访问控制规则或默认操作相关联时，可以（但不必）使用其他入侵策略。

图中的示例不包括任何阻止或信任规则，因为系统不检测已阻止或信任的流量。

入侵检查：入侵策略、规则和变量集

在允许流量继续到达其目标之前，可以使用入侵防御作为系统的最后一道防线。入侵策略监管系统如何检测流量是否存在安全违规，并且在内联部署中可以阻止或修改恶意流量。入侵策略的主要功能是管理启用哪些入侵和预处理程序规则以及如何配置它们。

入侵和检查器规则

入侵规则是一组指定的关键字和参数，用于检测企图利用网络漏洞的行为；系统使用入侵规则来分析网络流量，以检测其是否与规则中的条件匹配。系统将数据包与每条规则中指定的条件进行比较，如果数据包数据与规则中指定的所有条件都匹配，则触发此规则。

系统包括以下由 Cisco Talos 情报组 (Talos) 创建的规则类型：

- 共享对象入侵规则，已编译且无法修改（规则标题信息除外，如源和目标端口及 IP 地址）
- 标准文本入侵规则，可以保存并修改为规则的新自定义实例。

- 预处理器规则，是指与网络分析策略中的检查器和数据包解码器检测选项关联的规则。不能复制或编辑检查器规则。默认情况下，大多数检查器规则均已禁用；您必须将其启用才能使用检查器生成事件，并在内联部署中丢弃有问题的数据包。

当系统根据入侵策略处理数据包时，首先，规则优化器会根据传输层、应用协议、受保护网络的方向等条件对子集中所有已激活的规则进行分类。然后，入侵规则引擎选择要应用于每个数据包的相应规则子集。最后，多规则搜索引擎执行三种不同类型的搜索以确定流量是否与规则匹配：

- 协议字段搜索在应用协议的特定字段中查找匹配项。
- 一般内容搜索在数据包负载中查找 ASCII 或二进制字节匹配项。
- 数据包异常搜索查找违反既定协议（而不是包含特定内容）的数据包报头和负载。

在自定义入侵策略中，您可以通过启用和禁用规则以及通过编写和添加自己的标准文本规则来调整检测。还可以遵从 Cisco 的建议，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。



注释 当没有足够的数据包根据阻止规则处理特定流量时，系统会继续根据其他规则评估剩余流量。如果任何剩余流量与设置为阻止的规则匹配，则会话将被阻止。但是，如果系统分析要传递的剩余流量，则流量状态在规则上显示为待处理，该规则因需要完整的数据包而被卡住。

变量集

只要系统使用入侵策略来评估流量，它便会使用关联的变量集。变量集中的大多数变量表示入侵规则中常用于识别源和目标 IP 地址及端口的值。您还可以在入侵策略中使用变量表示规则禁止和动态规则状态中的 IP 地址。

系统提供单个由预定义默认变量组成的默认变量集。大多数系统提供的共享对象规则和标准文本规则均使用这些预定义的默认变量来定义网络和端口号。例如，大部分规则使用变量 `$HOME_NET` 指定受保护网络，使用变量 `$EXTERNAL_NET` 指定未受保护（或外部）网络。此外，专用规则通常会使用其他预定义的变量。例如，检测针对网络服务器的漏洞攻击的规则使用 `$HTTP_SERVERS` 和 `$HTTP_PORTS` 变量。



提示 即使您使用系统提供的入侵策略，思科也**强烈**建议修改默认变量集中的关键默认变量。当使用准确反映网络环境的变量时，处理会得以优化，并且系统可以监控相关系统是否存在可疑活动。高级用户可以创建并使用自定义变量集与一个或多个自定义入侵策略配对。



重要事项 如果要创建自定义变量集，请勿使用数字作为自定义变量集名称（例如，3Snort）中的第一个字符。当您配置部署到 FMC 上的 FTD 防火墙时，这将导致 Snort 3 验证失败。

入侵事件生成

当系统识别可能的入侵时，它会生成入侵或预处理程序事件（有时统称为入侵事件）。受管设备将其事件传输到管理中心，在其中可以查看聚合数据并更好地了解针对网络资产的攻击。在内联部署中，受管设备还可以丢弃或替换已知有害的数据包。

数据库中的每个入侵事件均包括事件报头并包含有关事件名称和分类的信息；源和目标 IP 地址；端口；生成事件的进程；事件的日期和时间，以及有关攻击源及其目标的情景信息。对于基于数据包的事件，系统还会记录一个或多个已触发事件的数据包的已解码数据包报头和负载的副本。

数据包解码器、预处理程序和入侵规则引擎均会导致系统生成事件。例如：

- 如果数据包解码器（在网络分析策略中配置）接收少于 20 字节（没有任何选项或负载的 IP 数据报的大小）的 IP 数据包，解码器将此解释为异常流量。如果之后启用了用于检测数据包的入侵策略中的配套解码器规则，则系统会生成检查器事件。
- 如果 IP 分片重组检查器遇到一系列重叠的 IP 片段，则检查器会将此解释为可能的攻击，当启用了配套预处理程序规则时，系统会生成检查器事件。
- 在入侵规则引擎内，大多数标准文本规则和共享对象规则编写为在由数据包触发时会生成入侵事件。

随着数据库累计入侵事件，您可以开始分析潜在攻击。系统为您提供复审入侵事件和评估其在网络环境与安全策略情境中是否重要所需的工具。

系统提供的与自定义的网络分析和入侵策略

创建新的访问控制策略是使用系统管理流量过程中的头几个步骤之一。默认情况下，新创建的访问控制策略调用系统提供的网络分析和入侵策略来检测流量。

下图显示内联的入侵防御部署中新创建的访问控制策略最初如何处理流量。预处理和入侵防御阶段突出显示。



请注意以下各种操作的方式：

- 默认网络分析策略监管由访问控制策略处理的所有流量的预处理。最初，系统提供的 *Balanced Security and Connectivity* 网络分析策略是默认策略。
- 访问控制策略的默认操作允许由系统提供的 *Balanced Security and Connectivity* 入侵策略确定的所有非恶意流量。由于默认操作允许流量通过，在入侵策略能够检查并可能阻止恶意流量之前，发现功能可以检查流量中的主机、应用和用户数据。
- 策略使用默认的安全情报选项（仅全局阻止列表和非阻止列表），不使用 SSL 解密已加密的流量，并且不使用访问控制规则对网络流量执行特殊处理和检查。

可以采取用于调整入侵防御部署的一个简单步骤是使用系统提供的一组不同的网络分析和入侵策略作为默认值。Cisco 通过系统提供若干对策略。

或者，您可以通过创建和使用自定义策略来定制入侵防御部署。您可能会发现这些策略中配置的检查器选项、入侵规则和其他高级设置无法满足网络的安全需求。通过调整网络分析和入侵策略，可以非常精细地配置系统如何处理网络流量并检测其是否存在入侵。

系统提供的网络分析和入侵策略

Cisco 通过系统提供若干对网络分析和入侵策略。通过使用系统提供的网络分析和入侵策略，您可以利用 Cisco Talos 情报组 (Talos) 的经验。对于这些策略，Talos 提供入侵和检查器规则状态及对检查器和其他高级设置的初始配置。

没有哪一个系统提供的策略能够涵盖所有的网络配置文件、流量组合或防御安全状况。但每个此类策略都涵盖常见情况和网络设置，为提供精细调整的防御策略奠定基础。虽然您可以按原样使用系统提供的策略，但思科强烈建议您将其作为自定义策略的基础，对其进行调整以适合您的网络。



提示 即使您使用系统提供的网络分析和入侵策略，也应该配置系统的入侵变量，以准确反映网络环境。至少应修改默认变量集中的关键默认变量。

随着新的漏洞被发现，Talos 会发布入侵规则更新，又名轻量安全安装包 (LSP)。这些规则更新可以修改系统提供的任何网络分析或入侵策略，并且可以提供新的和已更新的入侵规则及检查器规则、现有规则的已修改状态，以及已修改的默认策略设置。规则更新还可以从系统提供的策略中删除规则，并且提供新规则类别，以及修改默认变量集。

如果规则更新影响您的部署，则网络界面将受影响的入侵和网络分析策略标记为已过期，并标记其父访问控制策略。您必须重新部署已更新的策略才能使其更改生效。

为方便起见，可以将规则更新配置为自动重新部署受影响的入侵策略（单独或与受影响的访问控制策略组合）。这使您能够轻松、自动保持部署为最新，以防范最近发现的漏洞和入侵。

为了确保获得最新的预处理设置，必须重新部署访问控制策略，该策略也会重新部署与当前运行的策略不同的所有关联的 SSL、网络分析和文件策略，同时还可以更新高级预处理和性能选项的默认值。

Cisco 通过系统提供以下网络分析和入侵策略：

“平衡安全和连接”网络分析和入侵策略

这些策略专为速度和检测而构建。共同使用时，这些策略充当大多数组织和部署类型的良好起点。系统在大多数情况下均使用 **Balanced Security and Connectivity** 策略和设置作为默认值。

Connectivity Over Security 网络分析和入侵策略

这些策略专为连接性（能够获取所有资源）优先于网络基础设施安全性的组织而构建。此入侵策略启用的规则远远少于“安全优先于连接”策略中启用的规则。仅会启用阻止流量的最重要规则。

“安全优先于连接”网络分析和入侵策略

这些策略专为网络基础设施安全性优先于用户便利性的组织而构建。此入侵策略将启用许多可能会提醒或丢弃合法流量的网络异常入侵规则。

“最大检测”网络分析和入侵策略

此类策略适用于网络基础设施安全性比在“安全性优先于连接”(Security Over Connectivity)策略中还要重要，有可能产生更大运营影响的组织。例如，入侵策略将启用大量威胁类别中的规则，包括恶意软件、攻击程序包、旧漏洞和常见漏洞及已知外部攻击程序。

No Rules Active 入侵策略

在“无活动规则”入侵策略中，所有入侵规则和所有高级设置（除入侵规则阈值外）均已禁用。如果您要创建自己的入侵策略而不是将其基于系统提供的其他策略之一的已启用规则，可以尝试使用此策略。



注释 根据所选的系统提供的基本策略，该策略的设置有所不同。要查看策略设置，请点击策略旁边的 **编辑** 图标，然后点击 **基本策略** 链接。

自定义网络分析和入侵策略的优势

您可能会发现系统提供的网络分析和入侵策略中配置的检查器选项、入侵规则和其他高级设置不完全满足贵组织的安全需要。

构建自定义策略可以提高环境中系统的性能，并且可以密切关注网络上发生的恶意流量和策略违例。通过创建和调整自定义策略，可以非常精细地配置系统如何处理和检查网络流量是否存在入侵。

所有自定义策略都具有基本策略（也称为基层），用于为策略中所有配置定义默认设置。层是可用于高效管理多个网络分析或入侵策略的构建块。

在大多数情况下，自定义策略基于系统提供的策略，但是可以使用其他自定义策略。不过，所有自定义策略在策略链中都以系统提供的策略作为最终基础。由于规则更新可能会修改系统提供的策略，因此导入规则更新可能会对您产生影响，即使使用自定义策略作为基础也如此。如果规则更新影响部署，则 Web 界面将受影响策略标记为过期。

自定义网络分析策略的优势

默认情况下，一个网络分析策略预处理访问控制策略处理的所有未加密流量。这意味着所有数据包都根据相同设置进行解码和预处理，无论后来使用哪种入侵策略（和因此使用的入侵规则集）对其进行检测。

最初，系统提供的 **Balanced Security and Connectivity** 网络分析策略是默认策略。调整预处理的一个简单方法是创建并使用自定义网络分析策略作为默认值。

可用的调整选项因检查器而异，但是可以调整检查器和解码器的一些方法包括：

- 可以禁用不适用于正在监控的流量的检查器。例如，HTTP Inspect 检查器规范化 HTTP 流量。如果确信网络中没有任何使用 Microsoft 互联网信息服务 (IIS) 的 Web 服务器，则可以禁用查找特定于 IIS 的流量的检查器选项，从而减少系统处理开销。



注释 如果禁用自定义网络分析策略中的检查器，但系统稍后需要使用该检查器利用已启用的入侵或检查器规则对数据包进行评估，系统会自动启用并使用检查器，不过它在网络分析策略 Web 界面中保持禁用。

- 指定端口（如果适用）以关注某些检查器的活动。例如，可以确定要对 DNS 服务器响应或加密 SSL 会话进行监控的其他端口，或者确定解码 telnet、HTTP 和 RPC 流量所在的端口

对于复杂部署的高级用户，可以创建多个网络分析策略，每个策略定制为以不同方式预处理流量。然后，可以配置系统使用这些策略管理使用不同的安全区域、网络或 VLAN 的流量的预处理。（请注意，ASA FirePOWER 模块无法通过 VLAN 限制预处理。）



注释 使用自定义网络分析策略（尤其是多个网络分析策略）定制预处理是一个高级任务。由于预处理和入侵检测密切相关，因此，您必须注意，要确保允许检测单个数据包的网络分析和入侵策略能够互补。

自定义入侵策略的优势

在新建的初始配置为执行入侵防御的访问控制策略中，默认操作允许所有流量，但是首先会使用系统提供的 **Balanced Security and Connectivity** 入侵策略对流量进行检测。除非添加访问控制规则或更改默认操作，否则所有流量都由该入侵策略进行检查。

要自定义入侵防御部署，可以创建多个入侵策略，每个策略定制为以不同方式检测流量。然后，使用指定哪个策略检测哪个流量的规则来配置访问控制策略。访问控制规则可能很简单，也可能很复杂，使用多个条件来匹配和检测流量，包括安全区域、网络或地理位置、VLAN、端口、应用、请求的 URL 或用户。

入侵策略的主要功能是管理启用哪些入侵和检查器规则及其如何配置，如下所示：

- 在每个入侵策略中，应该验证所有适用于环境的规则是否已启用，并且通过禁用不适用于环境的规则来提高性能。您可以指定哪些规则应该丢弃或修改恶意数据包。
- 如果遵从 Cisco 的建议，则可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。
- 您可以修改现有规则并根据需要编写新的标准文本规则，以捕获新的漏洞或强制实施安全策略。

您可能对入侵策略进行的其他自定义包括：

- 敏感数据预处理器检测敏感信息，例如 ASCII 文本格式的信用卡号和社会保障号。请注意，在网络分析策略中配置了用于检测特定威胁（back orifice 攻击、多种端口扫描类型以及尝试以过多流量淹没网络的基于速率的攻击）的其他检查器。

- 全局阈值导致系统根据与入侵规则匹配的流量在指定时间段内源自或流向特定地址或地址范围的次数来生成事件。这有助于防止系统被大量事件淹没。
- 禁止入侵事件通知和设置个别规则或全体入侵策略的阈值也可以防止系统被大量事件淹没。
- 除了网络界面中的各种入侵事件视图之外，您还可以启用将日志记录到系统日志工具或者将事件数据发送到 SNMP 陷阱服务器。根据策略，可以指定入侵事件通知限制，设置发送到外部日志记录工具的入侵事件通知，以及配置对入侵事件的外部响应。请注意，除了基于策略的这些警报配置，对于每个规则或规则组，您还可以在入侵事件上全局启用或禁用邮件警报。无论哪个入侵规则处理数据包，都会使用您的邮件警报设置。

自定义策略的限制

由于预处理和入侵检测如此密切相关，因此，您必须小心确保自己的配置允许网络网络分析和入侵策略处理和检测单个数据包，以实现互补。

默认情况下，系统使用一个网络分析策略预理由受管设备使用单个访问控制策略处理的所有流量。下图显示内联的入侵防御部署中新创建的访问控制策略最初如何处理流量。预处理和入侵防御阶段突出显示。



请留意默认网络分析策略如何监管访问控制策略处理的所有流量的预处理。最初，系统提供的 **Balanced Security and Connectivity** 网络分析策略是默认策略。

调整预处理的一个简单方法是创建并使用自定义网络分析策略作为默认值。但是，如果在自定义网络分析策略中禁用检查器，但系统需要根据已启用的入侵或检查器规则评估预处理的数据包，则系统会自动启用并使用该检查器，尽管其在网络分析策略 **Web** 界面中保持禁用。



注释 要获取禁用检查器的性能优势，您 **必须** 确保自己的入侵策略均未启用需要该检查器的规则。

如果使用多个自定义网络分析策略，则会引起其他问题。对于使用复杂部署的高级用户，可以分配自定义网络分析策略以预处理匹配流量，从而根据特定安全区域、网络和 VLAN 自定义预处理。

（请注意，ASA FirePOWER 模块无法通过 VLAN 限制预处理。）为此，请向访问控制策略中添加自定义网络分析规则。每条规则均具有关联的网络分析策略，用于监管与该规则匹配的流量的预处理。

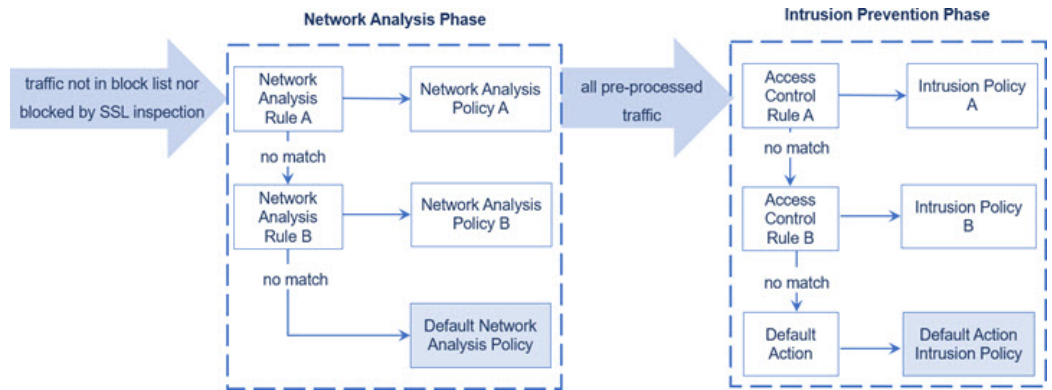


提示 可以将网络分析规则配置为访问控制策略中的高级设置。与其他类型的规则不同，网络分析规则调用网络分析策略，而不是被其包含。

系统按规则号由上而下将数据包与任何已配置的网络分析规则相匹配。不与任何网络分析规则相匹配的流量由默认网络分析策略预处理。虽然这使您在预处理流量时具有极大灵活性，但请记住，所有数据包 **无论** 由哪个网络分析策略进行了预处理，后来都会在各自的进程中与访问控制规则匹配，从而可能会接受入侵策略的检查。换句话说，使用特定网络分析策略预处理数据包不保证将通过任

何特殊入侵策略检测该数据包。您必须仔细配置访问控制策略，以使其调用正确的网络分析和入侵策略来评估特殊数据包。

下图集中细解了网络分析策略（预处理）选择阶段如何在入侵防御（规则）阶段之前发生并与其分隔开来。为简单起见，此图省去了发现和文件/恶意软件检查阶段。它还突出显示默认网络分析和默认操作入侵策略。



在此情景中，访问控制策略配置有两条网络分析规则和一个默认网络分析策略：

- 网络分析规则 A 使用网络分析策略 A 预处理匹配流量。之后，您希望此流量由入侵策略 A 进行检测。
- 网络分析规则 B 使用网络分析策略 B 预处理匹配流量。之后，您希望此流量由入侵策略 B 进行检测。
- 所有剩余流量都使用默认网络分析策略进行预处理。之后，您希望此流量由与访问控制策略的默认操作关联的入侵策略进行检测。

系统在预处理流量之后，可以检测流量是否存在入侵。该图显示具有两条访问控制规则和一个默认操作的访问控制策略：

- 访问控制规则 A 允许匹配流量。然后，流量由入侵策略 A 进行检测。
- 访问控制规则 B 允许匹配流量。然后，流量由入侵策略 B 进行检测。
- 访问控制策略的默认操作允许匹配流量。然后，流量由默认操作的入侵策略进行检测。

每个数据包的处理均由网络分析策略和入侵策略对进行监管，但系统不为您协调该对。请考虑以下情景：访问控制策略配置错误，以致网络分析规则 A 和访问控制规则 A 不处理相同流量。例如，您可能希望配对的策略监管特殊安全区域上流量的处理，但是在两条规则的条件中错误地使用不同的区域。这可能会导致错误地预处理流量。因此，使用网络分析规则和自定义策略定制预处理是一项高级任务。

请注意，对于单个连接而言，虽然系统在访问控制规则之前选择网络分析策略，但是一些预处理（特别是应用层预处理）发生在访问控制规则选择之后。这不会影响您在自定义网络分析策略中配置预处理的方式。

网络分析和入侵策略的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

网络分析和入侵策略的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 支持的域



第 2 章

从 Snort 2 迁移到 Snort 3

从 Snort 2 迁移到 Snort 3 一章涵盖了从 Snort 2 迁移到 Snort 3 的各个方面。它还提供有关启用和禁用 Snort 3 以及将 Snort 2 规则与 Snort 3 同步的信息。

- [Snort 2 与 Snort 3](#)，第 15 页
- [管理中心管理的威胁防御的 Snort 3 的功能限制](#)，第 16 页
- [从 Snort 2 迁移到 Snort 3](#)，第 17 页
- [启用和禁用 Snort 3](#)，第 17 页
- [查看 Snort 2 和 Snort 3 基本策略映射](#)，第 19 页
- [将 Snort 2 规则与 Snort 3 同步](#)，第 19 页

Snort 2 与 Snort 3

与 Snort 2 相比，Snort 3 在架构上进行了重新设计，以使用相同的资源检查更多流量。Snort 3 提供简化且灵活的流量解析器插入。Snort 3 还提供了新的规则语法，使规则编写更加容易，并且共享对象规则等效项可见。

下表列出了 Snort 2 和 Snort 3 版本在检测引擎功能方面的差异。

特性	Snort 2	Snort 3
数据包线程	每个进程一个	每个进程的任意数量
配置内存分配	进程数 * x GB	x GB 总计；更多内存可用于数据包
配置重新加载	较慢	更快；一个线程可以固定到单独的核心
规则语法	不一致，需要换行	具有任意空格的统一系统
规则注释	仅注释	#、#begin 和 #end 标记；C 语言风格

其他参考：[Firepower 中 Snort 2 和 Snort 3 之间的差异](#)。

管理中心管理的 威胁防御 的 Snort 3 的功能限制

下表列出了 管理中心管理的 威胁防御 设备的 Snort 2 支持但 Snort 3 不支持的功能。

表 1: Snort 3 的功能限制

策略/区域	不支持的功能
访问控制策略	以下应用设置： <ul style="list-style-type: none"> • 安全搜索 • YouTube EDU
威胁情报检测器	当 IPv4 或 IPv6 流量为： <ul style="list-style-type: none"> • 已阻止： <ul style="list-style-type: none"> • 无 TID 事件 • 无 SI 事件 • 受监控： <ul style="list-style-type: none"> • 无 ITD 事件
入侵策略	<ul style="list-style-type: none"> • 策略层 • 全局规则阈值 • 日志记录配置： <ul style="list-style-type: none"> • SNMP • SRU 规则更新，因为 Snort 3 仅支持 LSP 规则更新
应用检测	在 Snort 3 中，默认情况下为所有网络启用应用检测。与 Snort 2 不同的是，您无法使用网络发现策略的网络过滤器控制仅对特定网络启用或禁用应用检测。有关详细信息，请参阅最新版本的 <i>Firepower</i> 管理中心配置指南中的 <i>Snort 2</i> 和 <i>Snort 3</i> 中的应用检测 主题。
网络发现/RNA	<ul style="list-style-type: none"> • 主机端口/服务标识（如网络映射所示） • 操作系统指纹（您无法根据网络映射调整入侵策略）

策略/区域	不支持的功能
其他功能	使用 FQDN 名称进行事件日志记录

从 Snort 2 迁移到 Snort 3

从 Snort 2 迁移到 Snort 3 需要将威胁防御设备的检测引擎从 Snort 2 切换到 Snort 3。请注意，只有 7.0 及更高版本的设备支持 Snort 3。

当启用 Snort 3 作为设备的检测引擎时，在设备上应用（通过访问控制策略）的入侵策略的 Snort 3 版本将被激活并应用于通过该设备的所有流量。要在受支持的设备上启用 Snort 3，请参阅 [启用和禁用 Snort 3](#)，第 17 页。

Snort 2 自定义规则的转换工具

如果您使用的是自定义规则，请确保在从 Snort 2 转换为 Snort 3 之前准备好管理 Snort 3 的规则集。如果您使用的是来自第三方供应商的规则集，请联系该供应商以确认其规则将成功转换为 Snort 3 或获取为 Snort 3 编写的本地规则集。如果您有自己编写的自定义规则，请在转换之前熟悉如何编写 Snort 3 规则，以便在转换后更新规则以优化 Snort 3 检测。请参阅下面的链接，了解有关在 Snort 3 中编写规则的更多信息。

- <https://blog.snort.org/2020/08/how-rules-are-improving-in-snort-3.html>
- <https://blog.snort.org/2020/10/talos-transition-to-snort-3.html>

您可以参阅 <https://blog.snort.org/> 上的其他博客，了解有关 Snort 3 规则的更多信息。

要使用系统提供的工具将 Snort 2 规则转换为 Snort 3 规则，请参阅 [将 Snort 2 自定义规则转换为 Snort 3](#)，第 43 页。



重要事项 Snort 2 网络分析策略 (NAP) 设置无法自动复制到 Snort3。必须在 Snort 3 中手动复制 NAP 设置。

启用和禁用 Snort 3

Snort 3 是版本 7.0 及更高版本的新注册威胁防御设备的默认检测引擎。但是，对于较低版本的威胁防御设备，Snort 2 是默认检测引擎。将受管威胁防御设备升级到版本 7.0 或更高版本时，检测引擎仍保留在 Snort 2 上。要在 7.0 及更高版本的升级后威胁防御的使用 Snort 3，必须明确启用它。请注意，您可以随时从 Snort 3 切换回 Snort 2。

您可以根据需要切换 Snort 版本。映射 Snort 2 和 Snort 3 入侵规则，映射由系统提供。但是，您可能无法在 Snort 2 和 Snort 3 中找到所有入侵规则的一对一映射。如果更改 Snort 2 中的一条规则的规则操作，则在切换到 Snort 3 的情况下，不会保留 Snort 2 与 Snort 3 的同步。有关同步的详细信息，请参阅 [将 Snort 2 规则与 Snort 3 同步](#)，第 19 页。

在单个设备上启用和禁用 Snort 3

开始之前

可以执行这些步骤的受支持用户角色包括：

- 管理
- 入侵管理员

步骤 1 选择设备 > 设备管理。

步骤 2 点击设备以转到设备主页。

注释 设备被标记为 Snort 2 或 Snort 3，显示设备上的当前版本。

步骤 3 单击设备 (Device) 选项卡。

步骤 4 在检测引擎部分，点击 **升级**。

注释 要禁用 Snort 3，请点击检测引擎部分中的 **恢复为 Snort 2**。

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](#)，第 31 页。

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。



重要事项 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。

在多台设备上启用和禁用 Snort 3

要在多台设备上启用 Snort 3，请确保所有所需 **威胁防御** 设备的版本均为 7.0 或更高版本。

开始之前

可以执行这些步骤的受支持用户角色包括：

- 管理
- 入侵管理员

步骤 1 选择设备 > 设备管理。

步骤 2 选择要启用或禁用 Snort 3 的所有设备。

注释 设备被标记为 Snort 2 或 Snort 3，显示设备上的当前版本。

步骤 3 点击 **选择操作** 下拉列表。

步骤 4 点击 **升级到 Snort 3**。

注释 要禁用 Snort 3，请点击 **降级到 Snort 2**。

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](#)，第 31 页。

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。



重要事项 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。

查看 Snort 2 和 Snort 3 基本策略映射

步骤 1 依次选择策略 > 入侵。

步骤 2 确保选择 **入侵策略** 选项卡。

步骤 3 点击 **IPS 映射**。

将 Snort 2 规则与 Snort 3 同步

此实用程序用于将 Snort 2 版本策略配置与 Snort 3 版本同步，以便从相似的覆盖范围开始。

- 如果管理中心从 7.0 之前的版本升级到 7.0 或更高版本，系统会同步配置。如果管理中心是新的 7.0 版本或更高版本，您可以升级到更高版本，并且系统在升级过程中不会同步任何内容。

在将设备升级到 Snort 3 之前，如果在 Snort 2 版本中进行了更改，可以使用此实用程序将最新 Snort 2 版本同步到 Snort 3 版本，以便从相似的覆盖范围开始。



注释 迁移到 Snort 3 后，建议单独管理 Snort 3 版本的策略，且不要将此实用程序用作常规操作。

为确保 Snort 2 版本设置和自定义规则保留并转移到 Snort 3，管理中心 提供了同步功能。同步可帮助 Snort 2 规则覆盖设置和自定义规则，这些设置和自定义规则可能是您在过去几个月或几年内更改和添加的，以便在 Snort 3 版本上进行复制。

**重要事项**

- 只有 Snort 2 规则覆盖和自定义规则会复制到 Snort 3，而不会反过来。您可能无法在 Snort 2 和 Snort 3 中找到所有入侵规则的一对一映射。当您执行以下程序时，您对两个版本中存在的规则的规则操作更改会同步。
- 同步 不会 将任何自定义或系统提供的规则的阈值和抑制设置从 Snort 2 迁移到 Snort 3。

步骤 1 依次选择策略 > 入侵。

步骤 2 确保选择 入侵策略 选项卡。

步骤 3 点击 显示 Snort 3 同步状态。

步骤 4 确定不同步的入侵策略。

步骤 5 点击 同步 图标 (↻)。

注释 如果入侵策略的 Snort 2 和 Snort 3 版本已同步，则 同步 图标为绿色 (↻)。

步骤 6 仔细阅读摘要，并根据需要下载摘要副本。

步骤 7 点击 重新同步。

- 注释**
- 仅当在设备上应用并成功部署后，同步设置才适用于 Snort 3 入侵引擎。
 - 可以使用系统提供的工具将 Snort 2 自定义规则转换为 Snort 3。如果您有任何 Snort 2 自定义规则，请点击自定义规则选项卡，然后按照屏幕上的说明转换规则。有关详细信息，请参阅[将单个入侵策略的 Snort 2 自定义规则转换为 Snort 3](#)，第 44 页。

下一步做什么

部署配置更改：请参阅[部署配置更改](#)，第 31 页。



第 I 部分

Snort 3 中入侵检测和预防

- [Snort 3 入侵策略入门，第 23 页](#)
- [使用规则调整入侵策略，第 33 页](#)
- [根据网络资产定制入侵防护，第 49 页](#)



第 3 章

Snort 3 入侵策略入门

“Snort 3 入侵策略”一章深入介绍入侵策略的基础知识。它提供有关创建自定义 Snort 3 入侵策略、更改入侵策略的检测模式以及访问控制规则配置以执行入侵防御的信息。

- [入侵策略基础知识，第 23 页](#)
- [入侵策略的要求和必备条件，第 24 页](#)
- [创建自定义 Snort 3 入侵策略，第 25 页](#)
- [编辑 Snort 3 入侵策略，第 25 页](#)
- [更改入侵策略的基本策略，第 28 页](#)
- [更改 Snort 2 和 Snort 3 版本的入侵策略检测模式，第 29 页](#)
- [管理入侵策略，第 29 页](#)
- [用于执行入侵防御的访问控制规则配置，第 30 页](#)
- [部署配置更改，第 31 页](#)

入侵策略基础知识

入侵策略是已定义的几组入侵检测和防护配置，用于检查流量是否存在安全违规，以及在内部署中阻止或修改恶意流量。入侵策略供访问控制策略调用，是系统在允许流量到达目标之前的最后一道防线。

每个入侵策略的中心是入侵规则。启用的规则导致系统为匹配规则的流量生成入侵事件（或阻止该流量）。禁用规则将停止该规则的处理。

系统提供几种基本入侵策略，使您可以利用 Cisco Talos 情报组 (Talos) 的经验。对于这些策略，Talos 设置入侵和检查器规则状态（启用或禁用），并提供其他高级设置的初始配置。



提示 系统提供的入侵和网络分析策略具有类似的名称，但包含不同的配置。例如，“平衡安全性和连接” (Balanced Security and Connectivity) 网络分析策略和“平衡安全性和连接” (Balanced Security and Connectivity) 入侵策略共同发挥作用，均可在入侵规则更新中更新。但是，网络分析策略管理的主要是预处理选项，而入侵策略管理的主要是入侵规则。

如果创建自定义入侵策略，您可以：

- 通过启用和禁用规则，以及撰写和添加您自己的规则来调整检测。
- 遵从安全防火墙的建议，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。

入侵策略以丢弃匹配的数据包和生成入侵事件。要配置入侵或预处理器丢弃规则，请将其状态设置为“阻止”。

当定制入侵策略时，特别是在启用和添加规则时，请记住一些入侵规则要求首先以某种方式对流量进行解码或预处理。在入侵策略检查数据包之前，数据包根据网络分析策略中配置对其进行预处理。如果您禁用一个必需的检查器，虽然该检查器在网络分析策略网络界面中保持禁用，但系统仍自动通过其当前设置使用它。



注意 由于预处理和入侵检查密切相关，因此用于检查单个数据包的网络分析和入侵策略**必须**相互补充。定制预处理（特别是使用多个自定义网络分析策略）是一个**高级**任务。

在配置自定义入侵策略后，可以在访问控制配置过程中通过以下方式使用该策略：将入侵策略与一个或多个访问控制规则或访问控制策略的默认操作相关联。这会强制系统在某个允许的流量到达最终目的地之前使用入侵策略检查该流量。与入侵策略共同使用的变量集，用于准确地反映您的家庭和外部网络以及网络上的服务器（如果适当）。

请注意，默认情况下，系统禁用加密负载的入侵检查。当加密连接与已配置入侵检查的访问控制规则匹配时，这有助于减少误报和提高性能。

有关其他支持和信息，请参阅 [Snort 3 入侵策略概述](#)。

入侵策略的要求和必备条件

型号支持

威胁防御

支持的域

任意

用户角色

- 管理员
- 入侵管理员 (Intrusion Admin)

创建自定义 Snort 3 入侵策略

步骤 1 依次选择策略 > 入侵。

步骤 2 点击创建策略。

步骤 3 在名称 (**Name**) 和说明 (**Description**) (可选) 中输入唯一名称和说明。

步骤 4 选择 **监测模式**。

所选操作确定是入侵规则阻止并发出警报 (**防御模式**) 还是仅发出警报 (**检测模式**)。

注释 在选择预防模式之前, 您可能希望阻止规则仅发出警报, 以便识别导致大量误报的规则。

步骤 5 选择 **基本策略**。

您可以使用系统提供的策略或其他自定义策略作为您的基本策略。

步骤 6 点击保存。

新策略的设置与其基本策略相同。

下一步做什么

要自定义策略, 请参阅 [编辑 Snort 3 入侵策略, 第 25 页](#)。

编辑 Snort 3 入侵策略

从 Snort 2 版本到 Snort 3 版本编辑策略时, 所有更改都会立即保存。无需执行其他操作即可保存更改。

步骤 1 依次选择策略 > 入侵。

步骤 2 确保选择 **入侵策略** 选项卡。

步骤 3 点击要配置的入侵策略旁边的 **Snort 3 版本**。

步骤 4 编辑策略:

- 更改模式 - 点击 **模式** 下拉列表以更改检测模式。
 - **预防**-已触发的阻止规则创建事件 (警报) 并丢弃连接。
 - **检测**-已触发阻止规则警报。

您可以在进入防御之前选择检测模式。例如, 在选择预防模式之前, 您可能希望阻止规则仅发出警报, 以便识别导致大量误报的规则。

仅 Snort 3 版本的策略会更改检测模式。现有检测模式在 Snort 2 版本中按原样保留。

- **修改 规则操作**-要修改规则操作，请选择以下任一操作：
 - **批量编辑** - 选择一个或多个规则，然后从 **规则操作** 下拉列表中选择所需的操作；然后点击 **保存**。
 注释 仅前 500 条规则支持批量规则操作更改。
 - **单个规则编辑**-从 **规则操作** 列的下拉框中选择规则的操作。

规则操作是：

- **阻止**-生成事件，阻止此连接中的当前匹配数据包和所有后续数据包。
- **警报**-仅对匹配的数据包生成事件，而不丢弃数据包或连接。
- **禁用**-不针对此规则匹配流量。不生成事件。
- **恢复为默认**-恢复为系统默认操作。
- **通过**-不生成事件，允许数据包通过，而且不使用任何后续 Snort 规则进行进一步评估。
- **丢弃**-生成事件，丢弃匹配的数据包，但不阻止此连接上的后续流量。
- **反对**-生成事件，丢弃匹配的数据包，阻止此连接上的后续流量，并将 TCP 重置事件或无法连接的 ICMP 端口发送到源和目的主机。

与客户端或服务器相关的不同防火墙模式和 IP 地址或源或目标中的拒绝行为：在路由、内联和桥接接口的情况下，Snort 会向客户端和服务器发送 RST 数据包。Snort 发送两个 RST 数据包。客户端方向的 RST 数据包将源设置为服务器的 IP，目的设置为客户端的 IP。服务器方向的 RST 数据包将源设置为客户端的 IP，目的设置为服务器的 IP。

- **重写**-生成事件，并根据规则中的替代选项覆盖数据包内容。

如果有任何 **反应** 规则转换为警报操作。

- **搜索规则** - 使用搜索字段过滤显示内容。您可以输入 **GID**、**SID** 或参考信息。例如，**GID:1;SID:9621** - 仅显示规则 1:962; **SID:9621,9622,9623** - 显示具有不同 **SID** 的多个规则。您可以选择以下其中一个选项：
 - 应用过滤器 **操作 = 警报或 操作：阻止**
 - 应用 **禁用规则** 过滤器
 - 显示 **自定义/用户定义的规则**
 - 按 **GID**、**SID** 或 **GID:SID** 过滤
 - 按 **cve** 过滤
 - 按备注过滤
- **搜索规则组** - 输入关键字以搜索规则组，或选择搜索栏下方的以下任何预设过滤器选项：
 - **已排除** - 适用于已排除的规则组
 - **包含** - 适用于包含的规则组

- 覆盖 - 覆盖规则组配置

- 设置规则组的安全级别 - 在左侧窗格中导航到所需的规则组并选择它。点击规则组 **安全级别** 旁边的 **编辑**，以根据系统定义的规则设置提高或降低安全级别。

管理中心自动更改已配置安全级别的规则组规则的操作。每次更改安全级别时，请注意 **预设过滤器** 中阻止规则和禁用规则的计数。

- 查看过滤的规则 - 选择任何 **预设过滤器** 以查看设置为警报、阻止、禁用、覆盖、重写、通过、丢弃或拒绝的规则。

已覆盖的规则表示规则操作已从默认操作更改为其他操作的规则。请注意，一旦更改，规则操作状态即为已覆盖，即使您将其更改回其原始默认操作也是如此。但是，如果从 **规则操作** 下拉列表中选择 **恢复为默认**，则会删除覆盖状态。

高级过滤器 根据轻量级安全软件包 (LSP) 版本、入侵分类和漏洞 (CVE) 提供过滤器选项。

- 包括或排除规则组 - 显示的规则组是与系统提供的基本入侵策略关联的默认规则组。可以在入侵策略中包括和排除规则组。包含的规则组需要包含在组中才能实施策略中的规则。已从入侵策略中删除已排除的规则组，并且其规则不会应用于流量。有关在管理中心中上传自定义规则的信息，请参阅 [上传自定义规则](#)，第 44 页。


排除规则组：



1. 导航规则组窗格并选择规则组。
2. 点击右侧窗格中的 **排除** 链接。
3. 或者，如果要将规则组中的规则覆盖恢复为默认设置，选中 **是否要删除规则覆盖?** 复选框。

注释 仅当存在任何已覆盖的规则时，才会显示此复选框。

4. 点击 **排除**。

要包括具有上传的自定义规则的新规则组或先前排除的规则组，请执行以下操作：

1. 点击规则组搜索栏旁边的 **添加** () 。
2. 选中要添加的所有规则组旁边的复选框。
3. 点击**保存**。

- 查看规则文档 - 点击规则 ID 或 **规则文档** 图标可显示规则的 TALOS 文档。
- 查看规则详细信息 - 点击规则行中的 **展开箭头** () 图标可查看规则详细信息。
- 添加规则注释 - 点击“注释”列下的 **注释** () ，为规则添加注释。

要更改基本策略，请参阅 [更改入侵策略的基本策略](#)，第 28 页。

下一步做什么

部署配置更改；请参阅 [部署配置更改](#)，第 31 页。

规则操作日志记录

从管理中心 7.2.0 开始，内联结果列中的事件显示与应用于规则的 IPS 操作相同的名称，以便您可以查看应用于匹配规则的流量的操作。

对于 IPS 操作，下表显示了入侵事件页面的内联结果列中显示的事件，以及统一事件页面中入侵事件类型的操作列中显示的事件。

IPS 操作 (Snort 2)	内联结果 管理中心 7.1.0 及更早版本	内联结果 - 管理中心 7.2.0 及更高版本
警报	通过	警报

IPS 操作 (Snort 3)	内联结果 管理中心 7.1.0 及更早版本	内联结果 - 管理中心 7.2.0 及更高版本
警报	通过	警报
阻止	已丢弃/将已丢弃/部分丢弃	阻止/将阻止/部分阻止
丢弃 (Drop)	已丢弃/将已丢弃	丢弃/将丢弃
拒绝	已丢弃/将已丢弃	拒绝/将拒绝
重写	允许	重写



重要事项

- 如果规则没有“替换”选项，则 **重写** 操作显示为 **将重写**。
- 如果指定了“替换”选项，但 IPS 策略处于检测模式或设备处于内联 TAP/被动模式，则 **重写** 操作也将显示为 **将重写**。



注释

在向后兼容的情况下（管理中心 7.2.0 管理 威胁防御 7.1.0 设备），所提及的事件仅适用于警报 IPS 操作，其中 **通过** 显示为事件的 **警报**。对于所有其他操作，管理中心 7.1.0 的事件适用。

更改入侵策略的基本策略

可以选择其他系统提供的策略或自定义策略作为基本策略。

可以链接最多五个自定义策略，这五个策略中有四个使用其余四个之一以前创建的策略作为其基本策略；第五个策略必须使用系统提供的策略作为其基础。

步骤 1 依次选择策略 > 入侵。

步骤 2 点击想要配置的入侵策略旁边的 **编辑** (✎)。

步骤 3 从 **基本策略** 下拉列表中选择策略。

步骤 4 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](#)，第 31 页。

更改 Snort 2 和 Snort 3 版本的入侵策略检测模式

可以为现有入侵策略选择不同的检测模式。成功部署后，更改将应用于设备。遵循本主题中的步骤更改 Snort 2 和 Snort 3 版本的入侵策略的检测模式。

步骤 1 依次选择**策略 > 入侵**。

步骤 2 点击想要更改的入侵策略旁边的 **编辑** (✎)。

步骤 3 选择要应用策略的 **检测类型**。

步骤 4 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](#)，第 31 页。

管理入侵策略

在“入侵策略”页面 (**策略 > 入侵**) 上，可以查看当前自定义入侵策略以及下列信息：

- 一些访问控制策略和设备使用入侵策略来检查流量
- 在多域部署中，创建了策略的域


在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

步骤 1 依次选择**策略 > 入侵**。

步骤 2 管理入侵策略：

- 创建 - 点击**创建策略 (Create Policy)**；请参阅 [创建自定义 Snort 3 入侵策略](#)，第 25 页。
- 删除 - 点击要删除的策略旁边的 **删除** (🗑)。如果另一用户在策略中有未保存的更改，则系统会提示您确认并进行通知。点击 **OK** 确认。

如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。

- 编辑入侵策略详细信息 - 点击要编辑的策略旁边的 **编辑** ()。您可以编辑入侵策略的 **名称**、**检测模式**和**基本策略**。
- 编辑入侵策略设置 - 点击 **Snort 3 版本**；请参阅 [编辑 Snort 3 入侵策略，第 25 页](#)。
- 导出 - 如果要导出入侵策略以在另一个管理中心上导入，请点击导出；请参阅最新版本的 *Firepower* 管理中心配置指南中的 [导出配置](#) 主题。
- 部署 - 选择 **部署 > 部署**；请参阅 [部署配置更改，第 31 页](#)。
- 报告 - 请点击 **报告**；请参阅最新版本的 *Firepower* 管理中心配置指南中的 [生成当前策略报告](#) 主题。生成两个报告，每个策略版本一个。

用于执行入侵防御的访问控制规则配置

访问控制策略可能有多个与入侵策略相关联的访问控制规则。您可以为任何 **Allow** 或 **Interactive Block** 访问控制规则配置入侵检测，这样，您就可在网络中不同类型的流量到达最终目的地之前，使不同的入侵检测配置文件与其匹配。

只要系统使用入侵策略来评估流量，它便会使用关联的变量集。变量集中的变量代表通常在入侵规则中用来识别源 IP 地址、目标 IP 地址、源端口和目标端口的值。您还可以在入侵策略中使用变量表示规则禁止和动态规则状态中的 IP 地址。



提示 即使您使用系统提供的入侵策略，思科也**强烈**建议您配置系统的入侵变量以准确反映您的网络环境。至少，要修改默认变量集中的默认变量。

了解系统提供的入侵策略和自定义入侵策略

Cisco 通过系统提供多种入侵策略。通过使用系统提供的入侵策略，您可以利用 Cisco Talos 情报组 (Talos) 的经验。对于这些策略，Talos 会设置入侵和预处理器规则状态，并提供高级设置的初始配置。可以按现状使用系统提供的策略，也可以将其用作自定义策略的基础。构建自定义策略可以提高系统在您的环境中的性能，并提供网络上发生的恶意流量和策略违规行为的集中视图。

连接和入侵事件日志记录

当访问控制规则调用的入侵策略检测到入侵并生成入侵事件时，它会将此事件保存到管理中心。无论访问控制规则采用何种日志记录配置，系统都会将发生入侵的连接结束自动记录到管理中心数据库。

访问控制规则配置和入侵策略

请注意，您在单个访问控制策略中可以使用的唯一入侵策略的数量取决于目标设备型号；设备的功能越强大，处理的策略就越多。每个唯一的入侵策略和变量集对均视为一个策略。虽然您可以将不同的入侵策略-变量集对与每条“允许”(Allow)和“交互式阻止”(Interactive Block)规则（以及默认操作）相关联，但是，如果目标设备没有足够的资源可按照配置执行检测，则无法部署访问控制策略。

配置访问控制规则以执行入侵防御

您必须是管理员，访问管理员或网络管理员用户才能执行此任务。

- 步骤 1 在访问控制策略编辑器中，创建新规则或编辑现有规则；请参阅最新版本的 *Firepower* 管理中心配置指南中的 访问控制规则组件 主题。
- 步骤 2 确保规则操作设置为 **Allow**、**Interactive Block** 或 **Interactive Block with reset**。
- 步骤 3 点击 **检测**。
- 步骤 4 选择系统提供的或自定义入侵策略，或选择 **无** 以禁用对与访问控制规则相匹配的流量进行的入侵检查。
- 步骤 5 如果要更改与入侵策略关联的变量集，请从 **变量集 (Variable Set)** 下拉列表中选择值。
- 步骤 6 单击 **Save** 保存规则。
- 步骤 7 单击 **保存 (Save)** 保存策略。

下一步做什么

部署配置更改；请参阅 [部署配置更改](#)，第 31 页。

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 *Firepower* 管理中心配置指南 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，单击**部署 (Deploy)**，然后选择**部署 (Deployment)**。

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。展开设备列表时，您可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。

如果设备的此列中这一条为空白，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** - 单击 **展开箭头** (▶) 以查看要部署的设备特定的配置更改。

选中设备复选框后，该设备下列出的设备的所有更改都会推送到部署中。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 单击**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，请单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，如果由于任何原因导致部署失败，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 *Firepower* 管理中心配置指南中的 **部署配置更改** 主题。



第 4 章

使用规则调整入侵策略

“使用规则调整入侵策略”一章深入介绍入侵规则调整基础知识和规则类型。它提供有关 Snort 3 中的自定义规则、入侵规则操作、入侵策略中的入侵事件通知过滤器、将 Snort 2 自定义规则转换为 Snort 3 以及将具有自定义规则的规则组添加到入侵策略的信息。

- [入侵规则调整基础知识，第 33 页](#)
- [入侵规则类型，第 34 页](#)
- [入侵规则的许可证要求，第 35 页](#)
- [入侵规则的要求和必备条件，第 35 页](#)
- [Snort 3 中的自定义规则，第 35 页](#)
- [查看入侵策略中的 Snort 3 入侵规则，第 36 页](#)
- [入侵规则操作，第 36 页](#)
- [入侵策略中的入侵事件通知过滤器，第 38 页](#)
- [添加入侵规则注释，第 42 页](#)
- [将 Snort 2 自定义规则转换为 Snort 3，第 43 页](#)
- [上传自定义规则，第 44 页](#)
- [将具有自定义规则的规则组添加到入侵策略，第 45 页](#)
- [管理 Snort 3 中的自定义规则，第 46 页](#)
- [删除自定义规则，第 47 页](#)
- [删除规则组，第 47 页](#)

入侵规则调整基础知识

您可以为共享对象规则、标准文本规则和检查器规则配置规则状态和其他设置。

通过将规则状态设置为“警报”或“阻止”来启用规则。启用规则后，系统将对与该规则匹配的流量生成事件。禁用规则将停止该规则的处理。您还可以设置入侵策略，以便在内联部署中设置为阻止的规则在匹配流量时生成事件并丢弃该匹配流量。

您可以对规则进行过滤来显示规则的一个子集，这样就能选择要更改其规则状态或规则设置的确切规则集。

当入侵规则或规则参数要求禁用的检查器时，系统会自动使用其当前设置，即使其在网络分析策略网络界面中保持禁用状态。

入侵规则类型

入侵规则是系统用于检测利用网络漏洞企图的一组指定关键字和参数。当系统分析网络流量时，它将数据包与每个规则中指定的条件相比较，并在数据包满足规则中指定的所有条件的情况下触发规则。

入侵策略包含：

- 入侵规则，可细分为共享对象规则 and 标准文本规则
- 检查器规则，与数据包解码器的检测选项或与系统随附的检查器相关联

下表总结了这些规则类型的属性：

表 2: 入侵规则类型

类型	生成器 ID (GID)	Snort ID (SID)	来源	可以复制?	可以编辑?
共享对象规则	3	低于 1000000	思科 Talos 情报小组 (Talos)	是	有限
标准文本规则	1 (全局域或旧式 GID)	低于 1000000	Talos 协作	是	有限
	1000 - 2000 (后代域)	1000000 或更高	由用户创建或导入	是	是
预处理器规则	特定于解码器或预处理器	低于 1000000	Talos 协作	否	否
		1000000 或更高	由系统在选项配置期间生成	否	否

无法保存对 Talos 创建的任何规则所做的更改，但是可以将已修改的规则副本另存为自定义规则。可以修改在规则或规则报头信息中使用的变量（例如源和目标端口及 IP 地址）。在多域部署中，Talos 所创建的规则属于全局域。后代域中的管理员可以保存随后可编辑的规则的本地副本。

对于所创建的规则，Talos 在每个默认入侵策略中分配默认规则状态。大多数预处理器规则在默认情况下已禁用，如果希望系统为预处理器规则生成事件并在内联部署中丢弃违规的数据包，则必须启用这些规则。

入侵规则的许可证要求

威胁防御 许可证

IPS

经典许可证

保护

入侵规则的要求和必备条件

型号支持

任意。

支持的域

任意

用户角色

- 管理员
- 入侵管理员 (Intrusion Admin)

Snort 3 中的自定义规则

您可以通过以下方式创建自定义入侵规则。规则文件可以具有 `.txt` 或 `.rules` 扩展名。无论您使用哪种创建方法，系统都会将自定义规则保存在本地规则类别中。自定义规则必须属于规则组。但是，自定义规则也可以是两个或多个组的一部分。

当您创建自定义入侵规则时，系统会为它分配唯一的规则编号（其格式为 `GID:SID:Rev`）。此编号的元素如下：

- **GID**—生成器 ID。对于自定义规则，无需指定 **GID**。上传规则时，系统会根据您是在全局域还是子域中自动生成 **GID**。对于所有标准文本规则，此值为 2000。
- **SID**—Snort ID。指示规则是否为系统规则的本地规则。创建新规则时，请为该规则分配唯一的 **SID**。
本地规则的 Snort ID 号从 1000000 开始，且每个本地新规则的 **SID** 号以 1 递增。
- **Rev**—修订号。对于新规则，修订号为 1。每修改一次自定义规则，修订号就增加一。

在自定义标准文本规则中，可以设置规则报头设置、规则关键字和规则参数。您可以通过规则报头设置将规则设置为仅匹配使用特定协议以及发往或来自特定 IP 地址或端口的流量。



注释 无法编辑 Snort 3 自定义规则。确保自定义规则在规则文本中具有 classtype 的有效分类消息。如果导入没有分类或错误分类的规则，请删除并重新创建该规则。

查看入侵策略中的 Snort 3 入侵规则

您可以调整规则在入侵策略中的显示方式。也可以显示特定规则的详细信息，以便查看规则设置、规则文档和其他规则详情。

步骤 1 依次选择策略 > 入侵。

步骤 2 单击策略旁边的 **Snort 3 版本**。

步骤 3 查看规则时，您可以执行以下操作：

- 过滤器规则。
- 选择其他规则组以查看与该组相关的规则。
- 查看入侵规则的详细信息。
- 查看规则备注。
- 查看规则文档。

入侵规则操作

通过入侵规则操作，您可在个别入侵策略中启用或禁用规则，以及指定受监控条件触发该规则时系统采取的操作。

Cisco Talos 情报组 (Talos) 设置每个默认策略中每个入侵和检查器规则的默认操作。例如，一条规则可能会在 Security over Connectivity 默认策略中启用而在 Connectivity over Security 默认策略中禁用。Talos 有时会使用规则更新来更改默认策略中一条或多条规则的默认策略。如果允许规则更新对基本策略进行更新，则意味着当用于创建策略的默认策略中的默认操作发生更改时，也允许规则更新更改策略中的规则默认操作。但请注意，如果您已经更改了规则操作，规则更新不会覆盖您的更改。

创建入侵规则时，它会继承用于创建策略的默认策略中相应规则的默认操作。

入侵规则操作选项

在入侵策略中，可以将规则的状态设置为以下值：

警报

您希望系统检测特定入侵企图，并在其发现匹配流量时生成入侵事件。当恶意数据包通过网络并触发该规则时，数据包被发送到其目标，系统生成入侵事件。该恶意数据包到达其目标，但是您通过事件日志记录收到通知。

阻止

您希望系统检测特定入侵企图，丢弃包含攻击的数据包，并在其发现匹配流量时生成入侵事件。该恶意数据包永远不会到达其目标，并且您通过事件日志记录收到通知。

禁用 (Disable)

您不希望系统评估匹配流量。



注释 选择 **警报** 或 **阻止** 选项可启用规则。选择 **禁用 (Disable)** 会禁用规则。

思科强烈建议不要启用入侵策略中的所有入侵规则。如果启用所有规则，则您的受管设备的性能可能会下降。相反，应调整规则集，使之与网络环境尽可能匹配。

设置入侵规则操作

入侵规则操作为策略特定的。

步骤 1 依次选择策略 > 入侵。

步骤 2 单击要编辑的策略旁边的 **Snort 3 版本**。

提示 此页面指示已禁用规则的总数、设置为“警报”的已启用规则总数、设置为“阻止”的已启用规则总数以及已覆盖规则的总数。

步骤 3 选择要在其中设置规则操作的一条或多条规则。

步骤 4 从 **规则操作** 下拉框中选择以下选项之一：

- 警报
- 阻止
- 禁用 (Disable)

步骤 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](#)，第 31 页。

入侵策略中的入侵事件通知过滤器

入侵事件的重要性可根据发生频率或者源或目标 IP 地址而定。在某些情况下，直至事件发生一定次数后您可能才会会在意。例如，如果有人企图登录服务器，在其失败达到一定次数之前，您可能不会担心。但在其他情况下，也许只需要发生几次，就能让您知道存在普遍性问题。例如，如果有人对网络服务器发动 DoS 攻击，可能只需要发生区区数次入侵事件，您就会明白需要解决这种情况。发生数百次相同事件只会让系统不堪重负。

入侵事件阈值

您可以为各条规则设置阈值，根据事件在指定时间段内生成的次数来限制系统记录和显示入侵事件的次数。这可以防止因相同事件数量过多而使系统不堪重负。您可以根据共享对象规则、标准文本规则或检查器规则设置阈值。

入侵事件阈值配置

要设置阈值，请先指定阈值类型。

表 3: 阈值选项

选项	说明
限制	为指定时间段内触发规则的指定数量的数据包（由“计数” [Count] 参数指定）记录并显示事件。例如，如果将类型设置为限制 (Limit)，将计数 (Count) 设置为 10，并将秒数 (Seconds) 设置为 60，而同一分钟内有 14 个数据包触发规则，则系统在显示发生的前 10 个违反该规则的事件后将停止记录违反该规则的事件。
阈值 (Threshold)	在指定时间段内，当指定数量的数据包（由“计数” [Count] 参数指定）触发规则时，记录并显示一个事件。请注意，达到事件阈值计数且系统记录该事件之后，时间计数器将重新开始计数。例如，将类型设置为阈值 (Threshold)，将计数 (Count) 设置为 10，并将秒数 (Seconds) 设置为 60 时，如果到 33 秒时规则触发 10 次，系统将生成一个事件，然后将“秒数” (Seconds) 和“计数” (Count) 计数器重置为 0。其后，该规则在接下来 25 秒内又触发 10 次。由于计数器在第 33 秒时已重置为 0，因此，系统此时会记录另一个事件。

选项	说明
双向	<p>每个指定时间段在指定数量（计数）的数据包触发规则后记录并显示一次事件。例如，如果将类型设置为两者 (Both)，将计数 (Count) 设置为 2，并将秒数 (Seconds) 设置为 10，则事件计数结果如下：</p> <ul style="list-style-type: none"> • 如果 10 秒内触发规则一次，系统不会生成任何事件（未达到阈值） • 如果 10 秒内触发规则两次，系统将生成一个事件（第二次触发规则时达到阈值） • 如果 10 秒内触发规则四次，系统将生成一个事件（第二次触发规则时达到阈值，忽略其后的事件）

接下来，指定跟踪，从而确定事件阈值是按源 IP 地址计算还是按目标 IP 地址计算。

表 4: 阈值 IP 选项

选项	说明
来源	按源 IP 地址计算事件实例计数。
目标	按目标 IP 地址计算事件实例计数。

最后，指定用于定义阈值的实例数和时间段。

表 5: 阈值实例/时间选项

选项	说明
计数	每个跟踪 IP 地址在每个指定时间段内达到阈值所需的事件实例数量。
秒	计数重置之前经过的秒数。如果将阈值类型设置为 限制 (limit) ，将跟踪设置为 源 IP (Source IP) ，将 计数 (count) 设置为 10，并将 秒数 (seconds) 设置为 10，则系统将记录并显示 10 秒钟内发生的来自指定源端口的前 10 个事件。如果前 10 秒内只发生了 7 个事件，系统将记录并显示这些事件，而如果前 10 秒内发生了 40 个事件，系统将记录并显示 10 个事件，然后在为期 10 秒的时间段过后重新开始计数。


请注意，入侵事件阈值可单独使用，也可与基于速率的攻击防御、`detection_filter` 关键字和入侵事件抑制的任意组合配合使用。



提示 也可以在入侵事件的数据包视图中添加阈值。

在 Snort 3 中为入侵规则设置阈值

您可以在“规则详细信息”(Rule Detail)页面中为规则设置一个阈值。添加阈值将覆盖该规则的任何现有阈值。

- 步骤 1 选择 **对象 > 入侵规则**。
 - 步骤 2 点击 **Snort 3 所有规则** 选项卡。
 - 步骤 3 从入侵规则的警报配置列中，点击 **无** 链接。
 - 步骤 4 点击 **编辑** ()。
 - 步骤 5 在警报配置窗口中，点击 **阈值** 选项卡。
 - 步骤 6 从**类型 (Type)** 下拉列表中，选择要设置的阈值的类型：
 - 选择**限制 (Limit)** 以将通知限于每个时间段的指定数量的事件实例。
 - 选择**阈值 (Threshold)** 以在每个时间段内每次事件实例数达到指定数量时提供通知
 - 选择**两者 (Both)** 以在每个时间段内事件实例数达到指定数量后提供一次通知。
 - 步骤 7 从**跟踪方式** 下拉列表中，选择 **源** 或 **目标** 以指示希望按源 IP 地址还是目标 IP 地址跟踪事件实例。
 - 步骤 8 在**计数** 字段中，输入要用作阈值的事件实例数。
 - 步骤 9 在**秒** 字段中，输入用于指定跟踪事件实例的时间段的数字（以秒为单位）。
 - 步骤 10 单击**确定 (OK)**。
- 有关其他支持和信息，请参阅视频 [Snort 3 抑制和阈值](#)。


下一步做什么

部署配置更改；请参阅[部署配置更改](#)，第 31 页。

查看和删除入侵事件阈值

您可能需要查看或删除一个规则的现有阈值设置。可以使用“规则详细信息”(Rules Details)视图显示为阈值配置的设置，看其是否适合系统。如果不适合，可以添加新的阈值来覆盖现有值。

- 步骤 1 选择 **对象 > 入侵规则**。
- 步骤 2 点击 **Snort 3 所有规则** 选项卡。
- 步骤 3 选择具有 **警报配置** 列中所述已配置阈值的规则。
- 步骤 4 要删除规则的阈值，请点击 **警报配置** 列中的 **阈值** 链接。

步骤 5 请点击 **编辑** ()。

步骤 6 点击 **阈值** 选项卡。

步骤 7 点击 **重置**。

步骤 8 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](#)，第 31 页。

入侵策略抑制配置

您可以在特定 IP 地址或 IP 地址范围触发特定规则或检查器时抑制入侵事件通知。这对杜绝误报十分有用。例如，如果邮件服务器传输的数据包看起来像某种特定的漏洞，则可能会在邮件服务器触发该事件时抑制对其发出的事件通知。所有数据包都会触发该规则，但您只会看到真正的攻击事件。

入侵策略抑制类型

请注意，入侵事件抑制可单独使用，也可与基于速率的攻击防御、`detection_filter` 关键字和入侵事件阈值的任意组合配合使用。



提示 可以在入侵事件的数据包视图中添加抑制。您还可以使用入侵规则编辑器页面上的 **警报配置列** (**对象** > **入侵规则** > **Snort 3 所有规则**) 访问抑制设置。

在 Snort 3 中为入侵规则设置抑制

可以为入侵策略中的规则设置一个或多个抑制。


开始之前

确保创建要添加用于源或目标抑制的所需网络对象。

步骤 1 选择 **对象** > **入侵规则**。

步骤 2 点击 **Snort 3 所有规则** 选项卡。

步骤 3 点击入侵规则的警报配置列中的 **无** 链接。

步骤 4 点击 **编辑** ()。

步骤 5 在 **抑制** 选项卡中，点击以下任何选项旁边的添加图标 (+):

- 选择 **源** 将抑制由指定源 IP 地址发出的数据包生成的事件。
- 选择 **目标网络** 将抑制由发往指定目标 IP 地址的数据包生成的事件。

步骤 6 在 **网络** 下拉列表中选择任何预设网络。

步骤 7 点击保存。

步骤 8 （可选）如果需要，请重复最后三个步骤。

步骤 9 点击警报配置窗口中的 保存。

下一步做什么

部署配置更改；请参阅[部署配置更改](#)，第 31 页。

查看和删除抑制条件

您可能需要查看或删除现有抑制条件。例如，由于某个邮件服务器通常会传输看起来像漏洞的数据包，因此可以抑制由该邮件服务器 IP 地址发出的数据包的事件通知。如果以后停用该邮件服务器并将此 IP 地址重新分配给其他主机，应删除对该源 IP 地址的抑制条件。

步骤 1 选择 对象 > 入侵规则。

步骤 2 点击 **Snort 3 所有规则** 选项卡。

步骤 3 选择要查看或删除其抑制的规则。

步骤 4 点击 警报配置 列中的 抑制。

步骤 5 请点击 编辑 (✎)。

步骤 6 点击 抑制 选项卡。

步骤 7 通过点击抑制旁边的 清除 (✕) 删除 抑制。

步骤 8 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](#)，第 31 页。

添加入侵规则注释

可以向入侵策略中的规则添加注释。按这种方式添加的注释是策略特定的；即添加到一个入侵策略的规则中的注释在其他入侵策略中不可见。

步骤 1 依次选择策略 > 入侵。

步骤 2 单击要编辑的策略旁边的 **Snort 3 版本**。

步骤 3 选择要在其中添加注释的一条规则。

步骤 4 点击 注释 列下方的 注释 (🗨)。

步骤 5 在 注释 字段中，输入规则注释。

步骤 6 点击添加注释 (Add Comment)。

步骤 7 点击保存。

提示 系统将并在注释列中的规则旁显示 注释 (🗨️)。

下一步做什么

部署配置更改；请参阅[部署配置更改](#)，第 31 页。

将 Snort 2 自定义规则转换为 Snort 3

您可以一次性将管理中心中所有不同入侵策略的所有自定义 Snort 2 规则转换为 Snort 3，也可以将每个入侵策略的 Snort 2 自定义规则单独转换为 Snort 3。按照适合您的步骤操作。

将所有入侵策略中的所有 Snort 2 自定义规则转换为 Snort 3

步骤 1 选择 **对象** > 入侵规则。

步骤 2 点击 **Snort 3 所有规则** 选项卡。

步骤 3 确保在左侧窗格中选择 **更新**。

步骤 4 点击 **任务** 下拉列表，然后选择：

- **转换并导入** - 将所有入侵策略中的所有 Snort 2 自定义规则自动转换为 Snort 3，并将其作为 Snort 3 自定义规则导入管理中心。
- **转换并下载** - 将所有入侵策略中的所有 Snort 2 自定义规则自动转换为 Snort 3，并将其下载到本地系统。

步骤 5 单击确定 (OK)。

- 注释
- 如果在上一步中选择了 **转换并导入**，则所有转换后的规则都将保存在 **本地规则** 下新创建的规则组 **所有 Snort 2 转换后的全局** 下。
 - 如果在上一步中选择了 **转换并下载**，则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，然后按照 [上传自定义规则](#)，第 44 页中的步骤进行上传。

有关其他支持和信息，请参阅视频 [将 Snort 2 规则转换为 Snort 3](#)。

下一步做什么

部署配置更改；请参阅[部署配置更改](#)，第 31 页。

将单个入侵策略的 Snort 2 自定义规则转换为 Snort 3

步骤 1 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**。

步骤 3 点击入侵策略的 **同步** 图标 (↻)。

注释 如果入侵策略的 Snort 2 和 Snort 3 版本已同步，则 **同步** 图标为绿色 (↻)。它表示没有要转换的自定义规则。

步骤 4 仔细阅读摘要，然后点击 **自定义规则** 选项卡。

步骤 5 选择：

- **将转换后的规则导入到此策略**-将入侵策略中的 Snort 2 自定义规则转换为 Snort 3，并将其作为 Snort 3 自定义规则导入 **管理中心**。
- **下载转换后的规则**-将入侵策略中的 Snort 2 自定义规则转换为 Snort 3，并将其下载到本地系统中。您可以在下载的文件中查看转换后的规则，然后通过点击上传图标上传文件。

步骤 6 点击 **重新同步**。

下一步做什么

部署配置更改；请参阅[部署配置更改](#)，第 31 页。

上传自定义规则

在 **管理中心** 中上传自定义规则会将您在本地创建的自定义规则添加到所有 Snort 3 规则的列表中。

步骤 1 选择 **对象 > 入侵规则**。

步骤 2 点击 **Snort 3 所有规则** 选项卡。

步骤 3 点击 **任务** 下拉列表。

步骤 4 点击上传。

步骤 5 拖放包含已创建的 Snort 3 自定义规则的 `.txt` 或 `.rules` 文件。

注释 您也可以点击虚线框浏览到本地文件夹以选择文件。

步骤 6 单击**确定 (OK)**。

注释 如果所选文件中有任何错误，则无法继续。您可以下载有错误的文件，并在修复错误后将其 **替换**。

步骤 7 选择本地规则组以将新规则添加到该组。

您还可以创建新的自定义规则组（通过点击 [创建新的自定义规则组](#) 链接），然后将规则添加到新组。

注释 如果没有现有的本地规则组，请点击 [创建新的自定义规则组](#) 以继续。为该搜索输入一个 **名称**，然后点击 **保存**。

步骤 8 选择以下其中一个选项：

- **合并规则** 以合并您要添加的新规则与规则组中的现有规则。
- **将组中的所有规则替换为文件内容** 以将所有现有规则替换为您添加的新规则。

注释 如果在上一步中选择了多个规则组，则只有 **合并规则** 选项可用。

步骤 9 点击下一步。

查看摘要以了解正在添加的新规则 ID，并可选择下载。

步骤 10 点击完成。



重要事项 所有已上传规则的规则操作均处于禁用状态。您必须将其更改为所需的状态，以确保规则处于活动状态。

下一步做什么

- 在 **管理中心** 中上传自定义规则会将您创建的自定义规则添加到所有 **Snort 3** 规则的列表中。要对流量实施这些自定义规则，请在所需的入侵策略中添加并启用这些规则。有关将具有自定义规则的规则组添加到入侵策略的信息，请参阅 [将具有自定义规则的规则组添加到入侵策略](#)，第 45 页。有关启用自定义规则的详细信息，请参阅 [管理 Snort 3 中的自定义规则](#)，第 46 页。
- 部署配置更改；请参阅 [部署配置更改](#)，第 31 页。

有关其他支持和信息，请参阅 [Snort 3 自定义规则导入](#) 视频。

将具有自定义规则的规则组添加到入侵策略

必须在入侵策略中启用系统中上传的自定义规则，才能对流量实施这些规则。在 **管理中心** 上传自定义规则后，在入侵策略中添加具有新自定义规则的规则组。

步骤 1 依次选择 **策略 > 入侵**。

步骤 2 在 **入侵策略选项卡** 中，点击入侵策略的 **Snort 3 版本**。

步骤 3 点击规则组搜索栏旁边的 **添加 (+)**。

步骤 4 展开 **本地规则组**。

步骤 5 选中已上传的自定义规则组旁边的复选框。

步骤 6 点击 **保存**。

有关其他支持和信息，请参阅视频 [Snort 3 入侵规则组](#)。

下一步做什么

部署配置更改：请参阅[部署配置更改](#)，第 31 页。

管理 Snort 3 中的自定义规则

系统中上传的自定义规则必须添加到入侵策略并启用，以启用对流量实施这些规则。您可以跨所有策略或选择性地对单个策略启用已上传的自定义规则。

按照以下步骤在一个或多个入侵策略中启用自定义规则：

步骤 1 选择 **对象 > 入侵规则**。

步骤 2 点击 **Snort 3 所有规则** 选项卡。

步骤 3 展开 **本地规则**。

步骤 4 选择所需的规则组。

步骤 5 通过选中规则旁边的复选框来选择规则。

步骤 6 从 **规则操作** 下拉框中，选择 **按照入侵策略**。

步骤 7 选择：

- **所有策略**-对要添加的所有规则具有相同的规则操作。
- **按入侵策略**-为每个入侵策略设置不同的规则操作。

步骤 8 设置规则操作：

- 如果在上一步中选择了所有策略，请从 **选择覆盖状态** 下拉列表中选择所需的规则操作。
- 如果在上一步中选择了按入侵策略，则根据策略名称选择 **规则操作**。要添加更多策略，请点击 **添加其他**。

步骤 9 或者，在 **注释** 文本框中添加注释。

步骤 10 点击**保存**。

下一步做什么

在设备上部署更改。请参阅[部署配置更改](#)，第 31 页。

删除自定义规则

步骤 1 选择 **对象 > 入侵规则**。

步骤 2 点击 **Snort 3 所有规则** 选项卡。

步骤 3 展开左侧窗格中的 **本地规则**。

步骤 4 选择包含规则的文件夹。

步骤 5 选中要删除的策略的复选框。

步骤 6 确保所选的所有规则的规则操作均为 **禁用**。

如果需要，请按照以下步骤为多个选定规则禁用规则操作：

- a) 从 **规则操作** 下拉框中，选择按 **入侵策略**。
- b) 选择 **所有策略** 单选按钮。
- c) 从 **选择覆盖状态** 下拉列表中选择 **禁用**。
- d) 点击**保存**。
- e) 选中要删除的策略的复选框。

步骤 7 从 **规则操作** 下拉框中，选择 **删除**。

步骤 8 在删除规则弹出窗口中点击 **删除**。

下一步做什么

部署配置更改；请参阅 [部署配置更改](#)，第 31 页。

删除规则组

开始之前

从包含该规则组的所有入侵策略中排除要删除的规则组。有关从入侵策略中排除规则组的步骤，请参阅 [编辑 Snort 3 入侵策略](#)，第 25 页。

步骤 1 选择 **对象 > 入侵规则**。

步骤 2 点击 **Snort 3 所有规则** 选项卡。

步骤 3 展开左侧窗格中的 **本地规则**。


步骤 4 选择要删除的规则组。

步骤 5 在继续之前，请确保将组中所有规则的规则操作设置为 **禁用**。

如果任何规则的规则操作不是 **禁用**，则无法删除规则组。如果需要，请按照以下步骤禁用所有规则的规则操作：

- a) 选中 **规则操作** 下拉列表下方的复选框，以选择组中的所有规则。

- b) 从 **规则操作** 下拉框中，选择按 **入侵策略**。
- c) 选择 **所有策略** 单选按钮。
- d) 从 **选择覆盖状态** 下拉列表中选择 **禁用**。
- e) 点击**保存**。

步骤 6 点击规则组旁边的 **删除** () 。

步骤 7 在 Delete Rule Group 弹出窗口中点击 **OK** 。

下一步做什么

部署配置更改；请参阅[部署配置更改](#)，第 31 页。



第 5 章

根据网络资产定制入侵防护

根据网络资产定制入侵保护一章，深入了解 安全防火墙 建议的规则以及生成和应用 安全防火墙 建议的规则。

- [LSP 更新中的 Snort 3 规则更改](#)，第 49 页
- [关于 安全防火墙 建议的规则](#)，第 49 页
- [为 Snort 3 生成新的 安全防火墙 建议](#)，第 50 页
- [为 Snort 3 生成 安全防火墙 建议：升级场景](#)，第 52 页

LSP 更新中的 Snort 3 规则更改

在常规 Snort 3 入侵规则 (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。系统默认情况下，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。

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。

关于 安全防火墙 建议的规则

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：

- 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 Cisco 为网络资产建议的设置相匹配。

为 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：

- 威胁防御 许可证 - 威胁
- 经典许可证 - 保护
- 用户角色 - 管理员或入侵管理员
- 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 点击左侧面板中的 **建议** 以配置规则建议。

在 安全防火墙 建议窗口中，您可以设置以下内容：

- **安全级别：**选择安全级别并结合选择或不选择此复选框：
 - **安全级别与基本策略匹配或低于基本策略，**并取消选中“禁用”复选框。
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。
 - **安全级别与基本策略匹配，**并已选中禁用复选框。
更高效 - 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。
 - **高于基本策略的安全级别（不是最大检测）**和禁用复选框处于未选中状态。
增强安全性 - 启用与基于 **Security Over Connectivity** 规则集的已发现主机上的潜在漏洞匹配的其他规则。
 - **选中安全级别高于基本策略（不是最大检测）**和禁用复选框。
重点安全性 - 启用与基于 **Security Over Connectivity** 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。
 - **安全级别增加到“最大检测”（使用较低的基本策略）**并取消选中或选中“禁用”复选框。
增强保护 - 启用大量规则，可能会影响性能。建议在部署到生产环境之前检查并测试此设置。
 - **安全级别低于基本策略**并已选中禁用复选框。
更低安全性 - 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。建议不调整基本策略。

- **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 和任何 IPv6 网络。

重要事项 安全防火墙规则建议取决于网络发现。受保护的网路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 Firepower* 管理中心配置指南中 [网络发现策略](#) 章节。

点击 + 按钮创建类型为主机或网络的新网络对象，然后点击 **保存**。

- **接受建议以禁用规则**：指定系统是否禁用基于 安全防火墙 建议的入侵规则。

步骤 4 生成并应用建议：

- **生成**：生成入侵策略的建议。生成操作列出了建议规则（未使用）下的规则。
- **生成并应用**：生成并应用入侵策略的建议。“生成并应用”操作会列出“建议的规则（使用中）”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 **mew** 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](#)，第 31 页。

为 Snort 3 生成 安全防火墙 建议：升级场景

开始或停止使用 安全防火墙 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。

为入侵策略生成 安全防火墙 建议。按照列出的步骤将建议的规则设置升级到 Snort 3。

开始之前

安全防火墙 建议具有以下要求：

- 威胁防御 许可证 - 威胁
- 经典许可证 - 保护
- 用户角色 - 管理员或入侵管理员
- 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 考虑升级场景 1： 从 6.5+ 升级到 7.1 - 考虑 7.0 中没有更改

步骤 2 使用现有 Snort 2 建议配置在 7.1 中生成 Snort 3 建议。

步骤 3 显示 Snort 2 到 Snort 3 同步摘要详细信息：

- 为以下入侵策略的 Snort 3 版本生成的建议。
- 相同的基本策略和检测模式更新为 Snort 3 策略。

您还可以下载摘要详细信息。

步骤 4 考虑升级场景 2： 从 6.5+ 升级到 7.0 再到 7.1 - 首先升级到 7.0：

步骤 5 选择 **策略 > 入侵** 并确定不同步的入侵策略。

步骤 6 点击 **同步** 图标 (↻)。

注释 如果入侵策略的 Snort 2 和 Snort 3 版本已同步，则 **同步** 图标为绿色 (↻)。

在从 7.0 之前的版本升级到 7.0 期间，任何现有的 Snort 2 建议都将同步到 Snort 3。但是，如果您在升级到 7.0 后生成了 Snort 2 建议，**则可以将**所有这些建议同步到 Snort 3 版本。

步骤 7 仔细阅读摘要，并根据需要下载摘要副本。

步骤 8 考虑到 7.0 中没有建议，Snort 2 建议将迁移为 7.0 中的规则覆盖。

步骤 9 显示迁移的覆盖详细信息：

- 此策略具有在先前升级中作为覆盖迁移的 Snort 2 建议。选择 Snort 3 版本，为 **Snort 3** 生成建议。

在生成 Snort 3 建议之前，请点击 **查看** 以查看覆盖，或点击 **删除** 以删除覆盖，或点击 **忽略并生成** 以忽略覆盖并生成建议。

- 相同的基本策略和检测模式更新为 Snort 3 策略。

您还可以下载摘要详细信息。

步骤 10 从 7.0 升级到 7.1：

步骤 11 对于具有 Snort 2 规则建议的 7.0 管理中心，升级到 7.1 后，您将收到同步摘要消息通知。

下一步做什么

部署配置更改；请参阅[部署配置更改](#)，第 31 页。



第 **II** 部分

Snort 3 中的高级网络分析

• [网络分析策略入门](#)，第 57 页



第 6 章

网络分析策略入门

“网络分析策略入门”一章深入介绍了网络分析策略基础知识、前提条件和管理网络分析策略。它提供有关创建自定义网络分析策略和网络分析策略设置的信息。

- [网络分析策略基础知识，第 57 页](#)
- [网络分析策略的许可证要求，第 58 页](#)
- [网络分析策略的要求和必备条件，第 58 页](#)
- [管理网络分析策略，第 58 页](#)
- [网络分析策略的 Snort 3 定义和术语，第 59 页](#)
- [为 Snort 3 的自定义网络分析策略创建，第 61 页](#)
- [网络分析策略设置和缓存的更改，第 84 页](#)

网络分析策略基础知识

网络分析策略管理许多流量预处理选项，并供访问控制策略中的高级设置调用。网络分析相关预处理发生在安全情报匹配和 SSL 解密之后进行，但在入侵或文件检查开始之前进行。

默认情况下，系统使用平衡的安全性和连接性网络分析策略预理由访问控制策略处理的所有流量。但是，您可以选择不同的默认网络分析策略执行此预处理。为方便您使用，系统提供多种无法修改的网络分析策略供选择，这些策略由思科 Talos 情报小组 (Talos) 针对安全性和连接的特定平衡专门进行过调整。您也可以自定义预处理设置创建自定义网络分析策略。



提示 系统提供的入侵和网络分析策略具有类似的名称，但包含不同的配置。例如，“平衡安全性和连接” (Balanced Security and Connectivity) 网络分析策略和“平衡安全性和连接” (Balanced Security and Connectivity) 入侵策略共同发挥作用，均可在入侵规则更新中更新。但是，网络分析策略管理的主要是预处理选项，而入侵策略管理的主要是入侵规则。网络分析和入侵策略相互配合，检查您的流量。

您也可以通过以下方式根据特定安全区域、网络和 VLAN 定制流量预处理选项：创建多个自定义网络分析策略，然后分配它们预处理不同流量。（请注意，ASA FirePOWER 无法通过 VLAN 限制预处理。）

网络分析策略的许可证要求

威胁防御 许可证

威胁

经典许可证

保护

网络分析策略的要求和必备条件

型号支持

任意

支持的域

任意

用户角色

- 管理
- 入侵管理员

管理网络分析策略

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

步骤 1 选择以下路径之一来访问网络分析策略。

- 策略 > 访问控制，然后单击 **网络分析策略**
- 策略 > 访问控制 > 入侵，然后单击 **网络分析策略**
- 策略 > 入侵 > **网络分析策略**

注释 如果自定义用户角色限制对此处列出的第一个路径的访问，请使用第二个路径访问该策略。

步骤 2 管理网络分析策略：

- 比较-单击 **比较策略**；请参阅 *Firepower* 管理中心配置指南中的 **比较策略**。

- 创建 - 如果要创建新的网络分析策略，请点击 [创建策略](#)。

系统将创建两个版本的网络分析策略：**Snort 2 版本** 和 **Snort 3 版本**。

- 对于 Snort 2 版本，请按照 *Firepower* 管理中心配置指南中的 *Snort 2* 自定义网络分析策略创建 中所述继续操作。
 - 对于 Snort 3 版本，请按照 [为 Snort 3 的自定义网络分析策略创建](#)，第 61 页中所述继续操作。
- 删除 - 如果要删除网络分析策略，请点击 [删除](#) 图标，然后确认是否要删除策略。如果网络分析策略被访问控制策略引用，则无法删除该网络分析策略。
如果控件呈灰色显示，则表明配置属于祖先域，或者您没有修改配置的权限。
 - 编辑 - 如果要编辑现有网络分析策略，请点击 [编辑](#) 图标。
如果显示视图（），则表明配置属于祖先域，或者您没有修改配置的权限。
 - 报告 - 请点击 [报告](#)；请参阅最新版本的 *Firepower* 管理中心配置指南中的 [生成当前策略报告](#)。

网络分析策略的 Snort 3 定义和术语

下表列出了网络分析策略中使用的 Snort 3 概念和术语。

表 6: 网络分析策略的 **Snort 3** 定义和术语

术语	说明
检查器	检查器是处理数据包的插件（类似于 Snort 2 预处理器）。
绑定检查器	绑定检查器定义必须访问和考虑特定检查器时的流程。 当流量与绑定程序检查器中定义的条件匹配时，该检查器的值/配置才会生效。 有关详细信息，请参阅 为 Snort 3 的自定义网络分析策略创建 ，第 61 页的 绑定检查器 。
单例检查器	单例检查器包含一个实例。这些检查器不支持添加更多实例，例如多例检查器。单例检查器的设置应用于匹配该检查器的整个流量，而不是特定的流量段。 有关详细信息，请参阅 为 Snort 3 的自定义网络分析策略创建 ，第 61 页中的 单例检查器 。

术语	说明
多例检查器	<p>多例检查器包含多个实例，您可以根据需要进行配置。这些检查器支持根据特定条件（例如网络、端口和 VLAN）配置设置。一组受支持的设置称为实例。</p> <p>有关详细信息，请参阅 为 Snort 3 的自定义网络分析策略创建，第 61 页中的 多例检查器。</p>
架构 (Schema)	<p>架构文件基于 OpenAPI JSON 规范，用于验证您上传或下载的内容。您可以下载架构文件并使用任何第三方 JSON 编辑器（例如 Swagger 编辑器）将其打开。架构文件可帮助您确定可以为检查器配置的参数及其相应的允许值、范围和要使用的接受模式。</p> <p>有关详细信息，请参阅 自定义网络分析策略，第 67 页。</p>
示例文件	<p>它是一个预先存在的模板，其中包含可帮助您配置检查器的示例配置。</p> <p>您可以参考示例文件中包含的示例配置，并进行您可能需要的任何更改。</p> <p>有关详细信息，请参阅 自定义网络分析策略，第 67 页。</p>
完整配置	<p>您可以在一个文件中下载整个检查器配置。</p> <p>此文件中提供有关检查器配置的所有信息。</p> <p>完整配置是默认配置（由 Cisco Talos 作为 LSP 更新的一部分推出）和自定义 NAP 检查器配置的合并配置。</p> <p>有关详细信息，请参阅 自定义网络分析策略，第 67 页。</p>

术语	说明
覆盖的配置	<p>在网络分析策略页面的 Snort 3 版本 中：</p> <ul style="list-style-type: none"> 在 操作 > 上传 下，您可以点击 覆盖配置 以上传包含覆盖配置的 JSON 文件。 在 操作 > 上传 下，您可以点击 覆盖配置 以下载已覆盖的检查器配置。 <p>如果尚未覆盖任何检查器配置，则此选项处于禁用状态。当您覆盖检查器配置时，此选项会自动启用，以允许您下载。</p> <p>有关详细信息，请参阅 自定义网络分析策略，第 67 页。</p>

相关主题

[为 Snort 3 的自定义网络分析策略创建](#)，第 61 页

[自定义网络分析策略](#)，第 67 页

[网络分析策略映射](#)，第 64 页

为 Snort 3 的自定义网络分析策略创建

默认网络分析策略针对典型的网络要求和最佳性能进行了调整。通常，默认网络分析策略足以满足大多数网络要求，您可能不需要自定义策略。但是，当您有特定的网络要求或遇到性能问题时，可以自定义默认网络分析策略。请注意，自定义网络分析策略是一种高级配置，应仅由高级用户或 Cisco 支持人员执行。

Snort 3 的网络分析策略配置是基于 JSON 和 JSO 的数据驱动模型。架构基于 OpenAPI 规范，可帮助您了解支持的检查器、设置、设置类型和有效值。Snort 3 检查器是处理数据包的插件（类似于 Snort 2 预处理器）。网络分析策略配置可以 JSON 格式下载。

在 Snort 3 中，检查器和设置列表与 Snort 2 预处理器和设置列表不存在一对一映射。此外，管理中心中可用的检查器和设置的数量是 Snort 3 支持的检查器和设置的子集。有关 Snort 3 的详细信息，请参阅 <https://snort.org/snort3>。有关管理中心中的可用检查器的详细信息，请参阅 <https://www.cisco.com/go/snort3-inspectors>。



注释

- 将管理中心升级到 7.0 版本时，在升级后，在 Snort 2 版本的网络分析策略中所做的更改不会迁移到 Snort 3。
- 与入侵策略不同，没有将 Snort 2 网络分析策略设置同步到 Snort 3 的选项。

默认检查器更新

轻量级安全包 (LSP) 更新可能包含新的检查器或对现有检查器配置的整数范围的修改。安装 LSP 后，新的检查器和/或更新的范围将在网络分析策略的 **Snort 3 版本** 中的 **检查器** 下可用。

绑定检查器

绑定检查器定义必须访问和考虑特定检查器时的流程。当流量与绑定程序检查器中定义的条件匹配时，只有该检查器的值/配置才会生效。例如：

对于 *imap* 检查器，当必须访问时，活页夹定义以下条件。即：

- 服务等于 *imap*。
- 角色均一致。

如果满足这些条件，则使用类型 *imap*。

```
▼ binder
185 {
186   "when": {
187     "service": "imap",
188     "role": "any"
189   },
190   "use": {
191     "type": "imap"
192   }
193 },
```

单例检查器

单例检查器包含一个实例。这些检查器不支持添加更多实例，例如多例检查器。单例检查器的设置应用于整个流量，而不是特定的流量段。

例如：

```
{
  "normalizer":{
    "enabled":true,
    "type":"singleton",
    "data":{
      "ip4":{
        "df":true
      }
    }
  }
}
```

多例检查器

多例检查器包含多个实例，您可以根据需要进行配置。这些检查器支持根据特定条件（例如网络、端口和 VLAN）配置设置。一组受支持的设置称为实例。有一个默认实例，您还可以根据特定条件添加其他实例。如果流量与该条件匹配，则应用该实例中的设置。否则，将应用默认实例中的设置。此外，默认实例的名称与检查器的名称相同。

对于多例检查器，当您上传覆盖的检查器配置时，您还需要为 JSON 文件中的每个实例包含/定义匹配的绑定程序条件（必须访问或使用检查器时的条件），否则上传将导致错误。您还可以创建新实例，但请确保为您创建的每个新实例包含绑定程序条件，以避免错误。

例如：

- 修改了默认实例的多例检查器。

```
{
  "http_inspect":{
    "enabled":true,
    "type":"multiton",
    "instances":[
      {
        "name":"http_inspect",
        "data":{
          "response_depth":5000
        }
      }
    ]
  }
}
```

- 修改默认实例和默认绑定程序的多例检查器。

```
{
  "http_inspect":{
    "enabled":true,
    "type":"multiton",
    "instances":[
      {
        "name":"http_inspect",
        "data":{
          "response_depth":5000
        }
      }
    ]
  },
  "binder":{
```

```

    "type": "binder",
    "enabled": true,
    "rules": [
      {
        "use": {
          "type": "http_inspect"
        },
        "when": {
          "role": "any",
          "ports": "8080",
          "proto": "tcp",
          "service": "http"
        }
      }
    ]
  }
}

```

- 多例检查器，其中添加了自定义实例和自定义绑定程序。

```

{
  "http_inspect": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "name": "http_inspect1",
        "data": {
          "response_depth": 5000
        }
      }
    ]
  },
  "binder": {
    "type": "binder",
    "enabled": true,
    "rules": [
      {
        "use": {
          "type": "http_inspect",
          "name": "http_inspect1"
        },
        "when": {
          "role": "any",
          "ports": "8080",
          "proto": "tcp",
          "service": "http"
        }
      }
    ]
  }
}

```

网络分析策略映射

对于网络分析策略，Cisco Talos 提供了映射信息，用于为 Snort 3 版本找到对应的 Snort 2 版本的策略。

此映射可确保 Snort 3 版本的策略具有对应的 Snort 2 版本。

查看网络分析策略映射

步骤 1 转至 **策略 > 入侵 > 网络分析策略**。

步骤 2 点击 **添加映射**。

步骤 3 展开 **查看映射** 的箭头。

系统将显示自动映射到 Snort 2 等效策略的 Snort 3 网络分析策略。

步骤 4 点击 **确定**。

创建网络分析策略

所有管理中心现有的网络分析策略均可用于相应的 Snort 2 和 Snort 3 版本。当您创建新的网络分析策略时，会同时创建 Snort 2 版本和 Snort 3 版本。

步骤 1 转至 **策略 > 入侵 > 网络分析策略**。

步骤 2 点击 **创建策略**。

步骤 3 输入 **名称 (Name)** 和 **描述 (Description)**。

步骤 4 从可用选项中选择 **检测模式**。

- 检测
- 防御

步骤 5 选择 **基本策略**，然后点击 **保存**。

注释 如果您使用的是 Snort 3 和 SSL 解密或 TLS 服务器身份，请在 **预防** 模式下配置网络分析策略 (NAP)。

新的网络分析策略使用其对应的 **Snort 2 版本** 和 **Snort 3 版本** 创建。

修改网络分析策略

您可以修改网络分析策略以更改其名称、说明或基本策略。

步骤 1 转至 **策略 > 入侵 > 网络分析策略**。

步骤 2 点击 **编辑** 以更改名称、说明、检测模式或基本策略。

注释 如果编辑网络分析策略名称、说明、基本策略和检测模式，编辑内容将同时应用于 Snort 2 和 Snort 3 版本。如果要更改特定版本的检测模式，可以在相应版本的网络分析策略页面中执行此操作。

步骤 3 点击保存。

在网络分析策略页面上搜索检查器

在 Snort 3 版本的网络分析策略页面上，您可能需要通过在搜索栏中输入任何相关文本来搜索检查器。

步骤 1 转至网络分析策略的 **Snort 3 版本**。

步骤 2 在 **搜索** 栏中输入要搜索的检查器名称或任何相关文本。

系统将显示与您搜索的文本匹配的所有检查器。

例如，如果输入 **pop**，则弹出检查器和活页夹检查器在屏幕上显示为匹配结果。

相关主题

[自定义网络分析策略配置示例](#)，第 73 页

[查看具有覆盖的检查器列表](#)，第 71 页

[网络分析策略的 Snort 3 定义和术语](#)，第 59 页

[自定义网络分析策略](#)，第 67 页

[对检查器进行内联编辑以覆盖配置](#)，第 70 页

复制检查器配置

您可以根据自己的要求复制网络分析策略的 Snort 3 版本的检查器配置。

步骤 1 在网络分析策略的 **Snort 3 版本** 中的 **检查器** 下，展开要为其复制配置的所需检查器。

默认配置显示在左侧列中，被覆盖的配置显示在检查器下的右侧列中。

步骤 2 点击 **复制到剪贴板** 图标，将检查器配置复制到以下一项或两项的剪贴板。

- 左列的 **默认配置**
- 右列的 **覆盖的配置**

步骤 3 将复制的检查器配置粘贴到 JSON 编辑器，以进行您可能需要的任何编辑。

相关主题

[自定义网络分析策略](#)，第 67 页

自定义网络分析策略

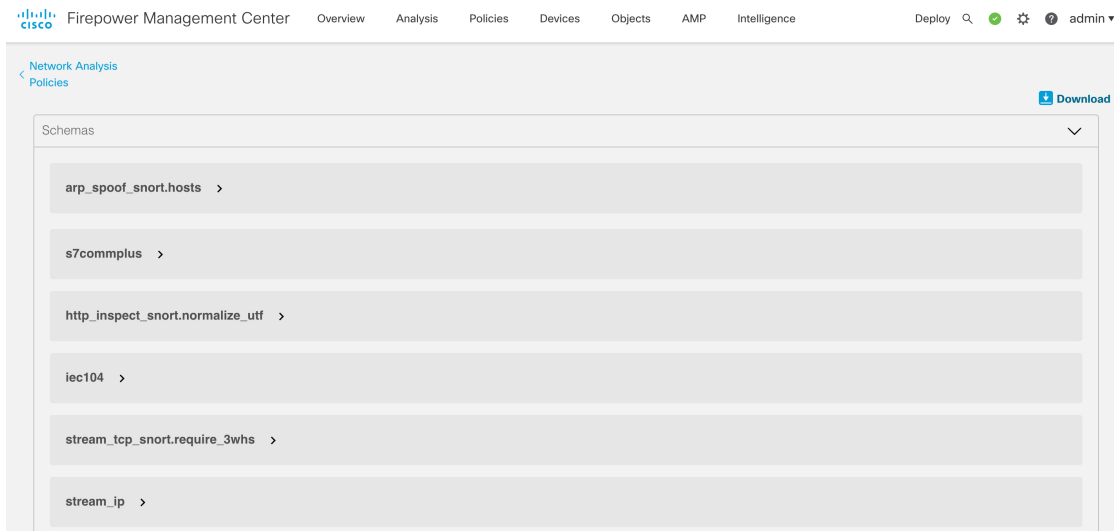
您可以根据自己的要求自定义 Snort 3 版本的网络分析策略。

步骤 1 点击网络分析策略的 **Snort 3 版本** 中的 **操作** 下拉菜单。

系统将显示以下选项：

- 查看架构
- 下载
 - 架构 (Schema)
 - 示例文件/模板
 - 完整配置
 - 覆盖的配置
- 上传
 - 覆盖的配置

步骤 2 点击 **查看方案** 可直接在浏览器中打开方案文件。



步骤 3 在 **下载** 下，您可以根据需要使用以下选项下载架构文件、示例文件、完整配置或覆盖配置。

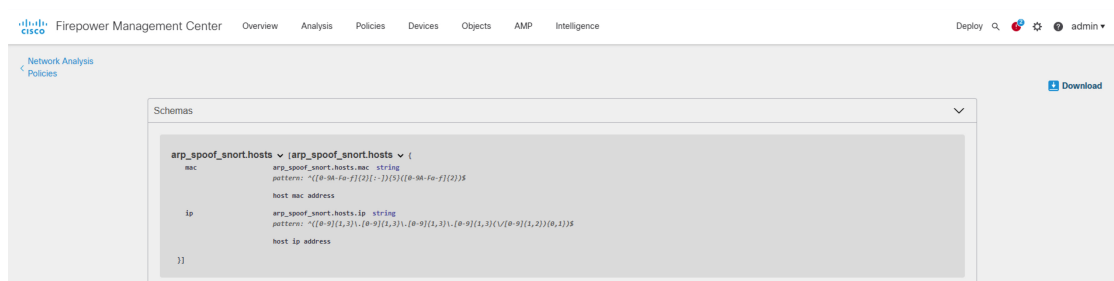
通过这些选项，您可以了解允许的值、范围和模式、现有和默认检查器配置以及覆盖的检查器配置。

a) 点击 **架构** 以下载架构文件。

架构文件验证您上传或下载的内容。您可以下载架构文件并使用任何第三方 JSON 编辑器打开它。架构文件可帮助您确定可以为检查器配置的参数及其相应的允许值、范围和要使用的接受模式。

例如，对于 `arp_spoof_snort` 检查器，您可以配置主机。主机包括 `mac` 和 `ip` 地址值。架构文件显示这些值的以下可接受模式。

- `mac` - 模式: `^([0-9A-Fa-f]{2}[:-]){5}([0-9A-Fa-f]{2})$`
- `ip` - 模式: `^([0-9]{1,3}\.){3}[0-9]{1,3}(\.)/[0-9]{1,2}([0,1])$`



您必须根据架构文件中接受的值、范围和模式，才能成功覆盖检查器配置，否则会收到错误消息。

- b) 点击 **示例文件 / 模板** 以使用包含示例配置的预先存在的模板来帮助您配置检查器。

您可以参考示例文件中包含的示例配置，并进行您可能需要的任何更改。有关信息，请参阅。

- c) 点击 **完整配置** 以将整个检查器配置下载到一个文件中。

您可以下载完整配置来查找所需的信息，而不是单独展开检查器。此文件中提供有关检查器配置的所有信息。

- d) 点击 **覆盖的配置** 以下载已覆盖的检查器配置。

如果尚未覆盖任何检查器配置，则此选项处于禁用状态。当您覆盖检查器配置时，此选项会自动启用，以允许您下载。

步骤 4 要覆盖现有配置，请按照以下步骤操作。

您可以选择使用以下方式覆盖检查器配置。

- 直接在 **管理中心** 上对检查器进行内联编辑。有关如何进行内联编辑的步骤，请参阅。
- 继续按照当前程序使用 **操作** 下拉菜单上传覆盖的配置文件。

如果您选择直接在 **管理中心** 上进行内联编辑，则无需进一步执行当前程序。否则，您必须完全遵循此程序。

- a) 在 **检查器** 下，展开要覆盖其默认配置的所需检查器。

默认配置显示在左侧列中，被覆盖的配置显示在检查器下的右侧列中。

您可能需要通过在搜索栏中输入任何相关文本来搜索检查器。

- b) 点击 **复制到剪贴板** 图标，将默认检查器配置复制到剪贴板。
- c) 创建一个 JSON 文件并将默认配置粘贴到其中。
- d) 保留要覆盖的检查器配置，并从 JSON 文件中删除所有其他配置和实例。

您还可以使用 **示例文件 / 模板** 来了解如何覆盖默认配置。这是一个包含 JSON 片段的示例文件，说明如何为 Snort 3 自定义网络分析策略。有关详细信息，请参阅。

- e) 根据需要对检查器配置进行更改。

验证更改并确保它们符合架构文件。对于多例检查器，请确保所有实例的绑定器条件都包含在 JSON 文件中。有关详细信息，请参阅 [为 Snort 3 的自定义网络分析策略创建，第 61 页](#) 中的多例检查器。

- f) 如果要复制任何其他默认检查器配置，请将该检查器配置附加到包含覆盖配置的现有文件。

注释 复制的检查器配置必须符合 JSON 标准。

- g) 将覆盖的配置文件保存到您的系统。

- h) 将覆盖的配置上传到管理中心，如下一步中所述。

步骤 5 在上传下，您可以点击 **覆盖配置** 以上传包含已覆盖配置的 JSON 文件。

注意 仅上传您需要的更改。不应上传整个配置，因为它会使覆盖本质上具有粘性，因此，将不会应用对默认配置的任何后续更改作为 LSP 更新的一部分。

您可以拖放文件，也可以点击浏览到系统中保存的包含覆盖检查器配置的 JSON 文件。

- **合并检查器覆盖** - 如果没有通用检查器，上传文件中的内容会与现有配置合并。如果有通用检查器，则上传文件（用于通用检查器）中的内容优先于之前的内容，并将替换这些检查器的先前配置。
- **替换检查器覆盖** - 删除所有之前的覆盖并替换为上传文件中的新内容。

注意 由于选择此选项会删除之前的所有覆盖，因此请在使用此选项覆盖配置之前做出明智的决定。

如果在上传覆盖的检查器时发生任何错误，您会在 **上传覆盖的配置** 弹出窗口中看到错误。您还可以下载存在错误的文件，然后修复错误并重新上传文件。

步骤 6 在 **上传覆盖的配置** 弹出窗口中，点击 **导入** 按钮以上传覆盖的检查器配置。

上传覆盖的检查器配置后，您会在检查器旁边看到一个橙色圆圈，表示它是一个覆盖的检查器。

此外，检查器下的 **覆盖配置** 列会显示覆盖的值。

您还可以使用“搜索”栏旁边的 **仅显示覆盖** 复选框查看所有已覆盖的检查器。

注释 确保始终下载 **下载** 下的 **覆盖配置**，然后打开 JSON 文件并将对检查器配置的任何新更改/覆盖附加到此文件。需要执行此操作，以免丢失旧的覆盖配置。

步骤 7（可选）在进行任何新的检查器配置更改之前，备份系统上的覆盖配置文件。

提示 我们建议您在覆盖检查器配置时不时进行备份。

相关主题

[将覆盖的配置恢复为默认配置](#)，第 71 页

[查看具有覆盖的检查器列表](#)，第 71 页

[自定义网络分析策略配置示例](#)，第 73 页

[在网络分析策略页面上搜索检查器](#)，第 66 页

[复制检查器配置](#)，第 66 页

对检查器进行内联编辑以覆盖配置

对于 Snort 3 版本的网络分析策略，您可以对检查器配置进行内联编辑，以根据您的要求覆盖配置。

或者，您也可以使用操作下拉菜单上传覆盖的配置文件。有关详细信息，请参阅[自定义网络分析策略，第 67 页](#)。

步骤 1 在网络分析策略的 **Snort 3 版本** 中的 **检查器** 下，展开要覆盖其默认设置的所需检查器。

默认配置显示在左侧列中，被覆盖的配置显示在检查器下的右侧列中。

步骤 2 在右侧列的 **覆盖配置** 下，点击 **编辑检查器**（铅笔）图标以更改检查器配置。

系统将显示覆盖配置弹出窗口，您可以在其中进行所需的编辑。

- 注释**
- 确保仅保留要覆盖的设置。如果保留的某个设置具有相同值，该字段将变为粘滞状态，这意味着如果将来 Talos 团队更改该设置，系统将保留当前值。
 - 如果要添加或删除任何自定义实例，请确保同时在绑定程序检查器中为该实例添加或删除绑定程序规则。

步骤 3 单击确定 (OK)。

如果根据 JSON 标准存在任何错误，则会显示错误消息。

步骤 4 点击 **Save** 保存所做的更改。

如果更改符合 OpenAPI 架构规范，则管理中心允许您保存配置，否则，系统将显示 **保存覆盖配置时出错** 的弹出窗口。您还可以下载包含错误的文件。

相关主题

[自定义网络分析策略，第 67 页](#)

[在内联编辑期间恢复未保存的更改，第 70 页](#)

[将覆盖的配置恢复为默认配置，第 71 页](#)

[自定义网络分析策略配置示例，第 73 页](#)

在内联编辑期间恢复未保存的更改

进行内联编辑以覆盖检查器的配置或恢复检查器的默认配置时，您可以恢复任何未保存的更改。请注意，此操作会将所有未保存的更改恢复为最近保存的值，但不会将配置恢复为检查器的默认配置。

有关如何将配置恢复为默认配置的信息，请参阅 [将覆盖的配置恢复为默认配置](#)。

步骤 1 在网络分析策略的 **Snort 3 版本** 中的 **检查器** 下，展开要恢复其未保存更改的所需检查器。

默认配置显示在左侧列中，被覆盖的配置显示在检查器下的右侧列中。

步骤 2 在右侧列的 **覆盖配置** 下，点击 **叉号 (X)** 图标可恢复检查器的任何未保存的更改。

或者，单击 **取消** 放弃更改。

如果您对检查器配置没有任何未保存的更改，则此选项不可见。

相关主题

[将覆盖的配置恢复为默认配置](#)，第 71 页

[对检查器进行内联编辑以覆盖配置](#)，第 70 页

查看具有覆盖的检查器列表

您可以使用“搜索”栏旁边的“仅显示覆盖”复选框查看所有已覆盖的检查器。

步骤 1 转至网络分析策略的 **Snort 3 版本**。

步骤 2 点按 **仅显示覆盖** 复选框以查看已覆盖检查器的列表。

所有被覆盖的检查器都在其名称旁边显示一个橙色圆圈，以帮助您识别它们。

相关主题

[在网络分析策略页面上搜索检查器](#)，第 66 页

[对检查器进行内联编辑以覆盖配置](#)，第 70 页

[自定义网络分析策略](#)，第 67 页

将覆盖的配置恢复为默认配置

您可以恢复为覆盖检查器的默认配置所做的任何更改。此操作会将覆盖的配置恢复为检查器的默认配置。

步骤 1 在网络分析策略的 **Snort 3 版本** 中的 **检查器** 下，展开要为其恢复覆盖配置的所需检查器。

被覆盖的检查器在其名称旁边显示为橙色圆圈。

默认配置显示在左侧列中，被覆盖的配置显示在检查器下的右侧列中。在右侧列的 **覆盖配置** 下，点击 **恢复默认配置**（后退箭头）图标，将检查器的覆盖配置恢复为默认配置。

如果未对检查器的默认配置进行任何更改，则此选项处于禁用状态。

步骤 2 点击 **恢复** 以确认决策。

步骤 3 点击 **Save** 保存所做的更改。

如果您不想保存更改，可以点击 **取消** 或 **叉号 (X)** 图标。

相关主题

[在内联编辑期间恢复未保存的更改](#)，第 70 页

[自定义网络分析策略](#)，第 67 页

[对检查器进行内联编辑以覆盖配置](#)，第 70 页

[自定义网络分析策略配置示例](#)，第 73 页

验证 Snort 3 策略

要验证 Snort 3 策略，以下是用户可以记录的基本信息列表：

- 当前管理中心可以管理多个威胁防御版本。
- 当前版本的管理中心支持不适用于以前版本的威胁防御设备的 NAP 配置。
- 当前 NAP 策略和验证将基于当前版本支持工作。
- 更改可能包括对以前版本的威胁防御无效的内容。
- 如果策略配置更改是当前版本的有效配置，并且使用当前 Snort 3 二进制文件和 NAP 方案执行，则接受策略配置更改。
- 对于以前的版本威胁防御，在部署期间使用该特定版本的 NAP 架构和 Snort 3 二进制文件执行验证。如果有任何配置不适用于给定版本，系统会向用户提供信息或警告，告知我们不会部署给定版本不支持的配置，并将部署其余配置。

在此程序中，当我们将 NAP 策略关联到访问控制策略并将其部署在设备上时，例如速率过滤器配置等任何检查器都将应用于验证 Snort 3 策略。

步骤 1 覆盖 NAP 策略配置的步骤：在网络分析策略的 **Snort 3 版本** 中的 **检查器** 下，展开要覆盖其默认设置的所需检查器。

默认配置显示在左侧列中，被覆盖的配置显示在检查器下的右侧列中。

步骤 2 在右侧列的 **覆盖配置** 下，点击 **编辑检查器**（铅笔）图标以更改任何检查器，例如 `rate_filter`。

系统将显示覆盖配置弹出窗口，您可以在其中对 `rate_filter` 检查器进行所需的编辑。

步骤 3 单击 **确定 (OK)**。

步骤 4 单击 **Save** 保存所做的更改。

或者，您也可以使用 **操作** 下拉菜单上传覆盖的配置文件。

步骤 5 点击网络分析策略的 **Snort 3 版本** 中的 **操作** 下拉菜单。

步骤 6 在 **上传** 下，您可以点击 **覆盖配置** 以上传包含已覆盖配置的 JSON 文件。

注意 仅上传您需要的更改。不应上传整个配置，因为它会使覆盖本质上具有粘性，因此，将不会应用对默认配置的任何后续更改作为 LSP 更新的一部分。

您可以拖放文件，也可以点击浏览到系统中保存的包含覆盖检查器配置的 JSON 文件。

- **合并检查器覆盖** - 如果没有通用检查器，上传文件中的内容会与现有配置合并。如果有通用检查器，则上传文件（用于通用检查器）中的内容优先于之前的内容，并将替换这些检查器的先前配置。
- **替换检查器覆盖** - 删除所有之前的覆盖并替换为上传文件中的新内容。

注意 由于选择此选项会删除之前的所有覆盖，因此请在使用此选项覆盖配置之前做出明智的决定。

如果在上传覆盖的检查器时发生任何错误，您会在 **上传覆盖的配置文件** 弹出窗口中看到错误。您还可以下载存在错误的文件，然后修复错误并重新上传文件。

步骤 7 将 NAP 策略关联到访问控制策略的步骤： 在访问控制策略编辑器中，点击 **高级**，然后点击网络分析和入侵策略旁边的 **编辑**。

步骤 8 从 Default Network Analysis Policy 下拉列表中，选择一条默认网络分析策略。

如果选择用户创建的策略，则可以点击 **编辑** 在新窗口中编辑该策略。无法编辑系统提供的策略。

步骤 9 单击 OK。

步骤 10 单击保存 (Save) 保存策略。

步骤 11 或者，在访问控制策略编辑器中，点击 高级，然后点击网络分析和入侵策略旁边的 编辑。

步骤 12 单击添加规则 (Add Rule)。

步骤 13 通过点击与要添加的条件来配置规则条件。

步骤 14 点击 网络分析，并选择要用于预处理匹配此规则的流量的 网络分析策略。

步骤 15 单击添加。

步骤 16 部署： 在管理中心 菜单栏中，点击 **部署** 并选择。**部署**。

步骤 17 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。

选中设备复选框后，该设备下列出的设备的所有更改都会推送到部署中。但是，您可以使用 **策略选择** 来选择部署个别策略或配置，而保留其余的更改不予部署。

(可选) 使用 **显示或隐藏策略** 可选择性地查看或隐藏关联的未修改策略。

步骤 18 单击部署 (Deploy)。

步骤 19 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，请单击警告或错误前的箭头图标。

注释 显示警告，Snort 3 网络分析策略包含对于此 威胁防御 版本无效的检查器或属性，部署时将跳过以下无效设置：无效检查器：[“rate_filter”] 仅针对 7.1 版本或更低版本。

自定义网络分析策略配置示例

此示例文件包含 JSON 片段，用于说明如何为 Snort 3 自定义网络分析策略。您可以选择使用以下方式覆盖检查器配置：

- 直接在 管理中心上对检查器进行内联编辑。请参阅。
- 使用 **操作** 下拉菜单上传覆盖的配置文件。请参阅[自定义网络分析策略](#)，第 67 页。

在选择任何这些选项之前，请查看以下所有详细信息和示例，这些详细信息和示例将帮助您成功定义网络分析策略覆盖。您必须阅读并理解此处介绍的各种场景的示例，以避免任何风险和错误。

如果您选择从 **操作** 下拉菜单覆盖检查器配置，则需要为网络分析策略覆盖构建一个 JSON 文件并上传该文件。

要覆盖网络分析策略中的检查器配置，您应只上传您需要的更改。不应上传整个配置，因为它会使覆盖本质上具有粘性，因此，将不会应用对默认值或配置的任何后续更改作为 LSP 更新的一部分。

以下是各种场景的示例：

当基本策略中的默认状态为“禁用”时启用单例检查器

```
{
  "rate_filter": {
    "enabled": true,
    "type": "singleton",
    "data": []
  }
}
```

当基本策略中的默认状态为“已启用”时禁用单例检查器

```
{
  "rate_filter": {
    "enabled": false,
    "type": "singleton",
    "data": []
  }
}
```

当基本策略中的默认状态为“禁用”时启用多例检查器

```
{
  "ssh": {
    "enabled": true,
    "type": "multiton",
    "instances": []
  }
}
```

基本策略中的“默认状态”为“已启用”时禁用多例检查器

```
{
  "ssh": {
    "enabled": false,
    "type": "multiton",
    "instances": []
  },
  "iecl04": {
    "type": "multiton",
    "enabled": false,
    "instances": []
  }
}
```

覆盖单例检查器特定设置的默认值

```
{
  "normalizer": {
    "enabled": true,
    "type": "singleton",
    "data": {
      "tcp": {
        "block": true
      },
      "ip6": true
    }
  }
}
```

覆盖多例检查器中默认实例的特定设置（其中实例名称与检查器类型匹配）

```
{
  "http_inspect": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "data": {
          "unzip": false
        },
        "name": "http_inspect"
      }
    ]
  }
}
```

为具有所需更改的默认实例添加绑定程序规则



注释 无法编辑默认绑定程序规则，它们始终附加在末尾。

```
{
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "use": {
          "type": "http_inspect"
        },
        "when": {
          "role": "server",
          "service": "http",
          "dst_nets": "10.1.1.0/24"
        }
      }
    ]
  }
}
```


添加新的自定义实例



注释 必须在绑定程序检查器中定义相应的绑定程序规则条目。

```
{
  "telnet": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "name": "telnet_my_instance",
        "data": {
          "encrypted_traffic": true
        }
      }
    ]
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_my_instance"
        }
      }
    ]
  }
}
```

在单个 JSON 覆盖中覆盖单个实例、多例默认实例和创建新的多例实例

在单个 JSON 覆盖中显示以下内容的示例：

- 覆盖单例实例（规范器 检查器）
- 覆盖多例默认实例（`http_inspect` 检查器）
- 创建新的多例实例（`Telnet` 检查器）

```
{
  "normalizer": {
    "enabled": true,
    "type": "singleton",
    "data": {
      "tcp": {
        "block": true
      },
      "ip6": true
    }
  },
  "http_inspect": {
    "enabled": true,
    "type": "multiton",
```

```

    "instances": [
      {
        "data": {
          "unzip": false,
          "xff_headers": "x-forwarded-for true-client-ip x-another-forwarding-header"
        },
        "name": "http_inspect"
      }
    ]
  },
  "telnet": {
    "enabled": true,
    "type": "multiton",
    "instances": [
      {
        "name": "telnet_my_instance",
        "data": {
          "encrypted_traffic": true
        }
      }
    ]
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_my_instance"
        }
      },
      {
        "use": {
          "type": "http_inspect"
        },
        "when": {
          "role": "server",
          "service": "http",
          "dst_nets": "10.1.1.0/24"
        }
      }
    ]
  }
}

```



注释 您不需要为绑定程序规则中的默认实例提供 **名称** 属性。

配置 arp_spoof

配置 **arp_spoof** 的示例:

arp_spoof 检查器没有任何属性的任何默认配置。这演示了可以提供覆盖的情况。

```

{
  "arp_spoof": {

```

```

    "type": "singleton",
    "data": {
      "hosts": [
        {
          "ip": "1.1.1.1",
          "mac": "ff:0f:f1:0f:0f:ff"
        },
        {
          "ip": "2.2.2.2",
          "mac": "ff:0f:f2:0f:0f:ff"
        }
      ]
    },
    "enabled": true
  }
}

```

配置 `rate_filter`

```

{
  "rate_filter": {
    "data": [
      {
        "apply_to": "[10.1.2.100, 10.1.2.101]",
        "count": 5,
        "gid": 135,
        "new_action": "alert",
        "seconds": 1,
        "sid": 1,
        "timeout": 5,
        "track": "by_src"
      }
    ],
    "enabled": true,
    "type": "singleton"
  }
}

```

使用多层次结构网络分析策略时配置绑定器规则

此示例说明在子策略中添加新的自定义实例以及如何编写绑定程序规则。绑定器规则定义为一个列表，因此，必须选择父策略中定义的规则并在此基础上构建新规则，因为规则不会自动合并。子策略中可用的绑定程序规则是整体真实性的来源。

在威胁防御上，默认 Cisco Talos 策略规则将附加到这些用户定义的覆盖上。

父策略:

我们已通过名称 `telnet_parent_instance` 和相应的绑定程序规则定义了一个自定义实例。

```

{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": true
        },
        "name": "telnet_parent_instance"
      }
    ],
  },
}

```

```

    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}

```

子策略:

此网络分析策略将上述策略作为其基本策略。我们定义了一个名为 **telnet_child_instance** 的自定义实例，并为此实例定义了绑定程序规则。需要在此处复制来自父策略的绑定程序规则，然后可以根据规则的性质将子策略绑定程序规则附加或附加在其之上。

```

{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": false
        },
        "name": "telnet_child_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet",
          "nets": "10.2.2.0/24"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_child_instance"
        }
      },
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}

```

```

    }
  ]
}

```

常规配置列表检查器属性

更改列表类型的任何属性的覆盖时，必须传递完整内容而不是部分覆盖。这意味着，如果基本策略属性定义为：

```

{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1"
      }
    },
    {
      "entry2": {
        "key2": "value2"
      }
    }
  ]
}

```

如果要将 **value1** 修改为 **value1-new**，则覆盖负载必须如下所示：

正确方法：

```

{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1-new"
      }
    },
    {
      "entry2": {
        "key2": "value2"
      }
    }
  ]
}

```

不正确的方式：

```

{
  "list-attribute": [
    {
      "entry1": {
        "key1": "value1-new"
      }
    }
  ]
}

```

您可以通过获取 **smtp** 检查器中 **alt_max_command_line_len** 属性的修整值来了解此配置。假设 **smtp** 检查器的默认（基本）策略配置如下：

```

{
  "smtp": {
    "type": "multiton",
    "instances": [
      {

```

```

"name": "smtp",
"data": {
  "decompress_zip": false,
  "normalize_cmds": "ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO
EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL
NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML STARTTLS TICK
TIME TURN TURNME VERB VRFY X-ADAT XADR XAUTH XCIR X-DRCP X-
ERCP XEXCH50 X-EXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE
XSTA XTRN XUSR",
  "ignore_data": false,
  "max_command_line_len": 512,
  "max_header_line_len": 1000,
  "log_rcptto": false,
  "decompress_swf": false,
  "max_response_line_len": 512,
  "b64_decode_depth": -1,
  "max_auth_command_line_len": 1000,
  "log_email_hdrs": false,
  "xlink2state": "alert",
  "binary_data_cmds": "BDAT XEXCH50",
  "auth_cmds": "AUTH XAUTH X-EXPS",
  "log_filename": false,
  "uu_decode_depth": -1,
  "ignore_tls_data": false,
  "data_cmds": "DATA",
  "bitenc_decode_depth": -1,
  "alt_max_command_line_len": [
    {
      "length": 255,
      "command": "ATRN"
    },
    {
      "command": "AUTH",
      "length": 246
    },
    {
      "length": 255,
      "command": "BDAT"
    },
    {
      "length": 246,
      "command": "DATA"
    }
  ],
  "log_mailfrom": false,
  "decompress_pdf": false,
  "normalize": "none",
  "email_hdrs_log_depth": 1464,
  "valid_cmds": "ATRN AUTH BDAT CHUNKING DATA DEBUG EHLO
EMAL ESAM ESND ESOM ETRN EVFY EXPN HELO HELP IDENT MAIL
NOOP ONEX QUEU QUIT RCPT RSET SAML SEND SOML STARTTLS TICK
TIME TURN TURNME VERB VRFY X-ADAT XADR XAUTH XCIR X-DRCP X-
ERCP XEXCH50 X-EXCH50 X-EXPS XGEN XLICENSE X-LINK2STATE XQUE
XSTA XTRN XUSR",
  "qp_decode_depth": -1
}
},
"enabled": true
}
}

```

现在，如果要向 `alt_max_command_line_len` 列表添加另外两个对象：

```
{
  "length": 246,
  "command": "XEXCH50"
},
{
  "length": 246,
  "command": "X-EXPS"
}
```

然后，自定义网络分析策略覆盖 JSON 如下所示：

```
{
  "smtp": {
    "type": "multiton",
    "instances": [
      {
        "name": "smtp",
        "data": {
          "alt_max_command_line_len": [
            {
              "length": 255,
              "command": "ATRN"
            },
            {
              "command": "AUTH",
              "length": 246
            },
            {
              "length": 255,
              "command": "BDAT"
            },
            {
              "length": 246,
              "command": "DATA"
            },
            {
              "length": 246,
              "command": "XEXCH50"
            },
            {
              "length": 246,
              "command": "X-EXPS"
            }
          ]
        }
      }
    ],
    "enabled": true
  }
}
```

在多例检查器中使用多层次结构网络分析策略时配置覆盖

此示例说明如何覆盖子策略中的属性，以及如何在任何实例的子策略中使用合并的配置。子策略中定义的任何覆盖都将与父策略合并。因此，如果属性 1 和属性 2 在父策略中被覆盖，而属性 2 和属性 3 在子策略中被覆盖，则合并的配置适用于子策略。这意味着将在设备上配置属性 1（在父策略中定义）、属性 2（在子策略中定义）和属性 3（在子策略中定义）。

父策略：

在这里，我们通过名称 `telnet_parent_instance` 定义了一个自定义实例，并覆盖了自定义实例中的 2 个属性，即 `normalize` 和 `encrypted_traffic`。

```

{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": false
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  },
  "binder": {
    "enabled": true,
    "type": "binder",
    "rules": [
      {
        "when": {
          "role": "any",
          "service": "telnet"
        },
        "use": {
          "type": "telnet",
          "name": "telnet_parent_instance"
        }
      }
    ]
  }
}

```

子策略:

此网络分析策略将上述策略作为其基本策略。我们覆盖了父策略中的 **encrypted_traffic** 属性，还覆盖了新属性 **ayt_attack_thresh**。

```

{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "encrypted_traffic": true,
          "ayt_attack_thresh": 1
        },
        "name": "telnet_parent_instance"
      }
    ],
    "enabled": true
  }
}

```

使用上述策略 JSON 时，当您部署网络分析策略时，将在设备上配置以下合并 JSON。

```

{
  "telnet": {
    "type": "multiton",
    "instances": [
      {
        "data": {
          "normalize": true,
          "encrypted_traffic": true,
          "ayt_attack_thresh": 1
        }
      }
    ]
  }
}

```



```

    },
    "name": "telnet_parent_instance"
  }
],
"enabled": true
},
"binder": {
  "enabled": true,
  "type": "binder",
  "rules": [
    {
      "when": {
        "role": "any",
        "service": "telnet"
      },
      "use": {
        "type": "telnet",
        "name": "telnet_parent_instance"
      }
    }
  ]
}
}
}

```

此示例说明自定义网络分析策略的详细信息。默认实例中也会出现相同的行为。此外，还将对单例检查器执行类似的合并。

删除网络分析策略的所有检查器覆盖：

每当要删除特定网络分析策略的所有覆盖时，都可以上传空 JSON。上传覆盖时，请选择 **替换检查器覆盖** 选项。

```

{
}

```

相关主题

- [网络分析策略的 Snort 3 定义和术语](#)，第 59 页
- [网络分析策略映射](#)，第 64 页
- [为 Snort 3 的自定义网络分析策略创建](#)，第 61 页
- [在网络分析策略页面上搜索检查器](#)，第 66 页
- [复制检查器配置](#)，第 66 页
- [自定义网络分析策略](#)，第 67 页
- [对检查器进行内联编辑以覆盖配置](#)，第 70 页
- [查看具有覆盖的检查器列表](#)，第 71 页

网络分析策略设置和缓存的更改

当您创建新的网络分析策略时，它具有与其基本策略相同的设置。

当您定制网络分析策略时，特别是在禁用检查器时，请记住某些检查器和入侵规则要求首先以某种方式对流量进行解码或预处理。如果您禁用一个必需的检查器，虽然该检查器在网络分析策略网络界面中保持禁用，但系统仍自动通过其当前设置使用它。



注释 由于预处理和入侵检查密切相关，因此用于检查单个数据包的网络分析和入侵策略**必须**相互补充。定制预处理（特别是使用多个自定义网络分析策略）是一个**高级**任务。

系统为每个用户缓存一条网络分析策略。在编辑网络分析策略时，如果您选择任何菜单或指向另一页的其他路径，即使您离开此页，更改也会保留在系统缓存中。

