

Cisco Secure Firewall Management Center Snort 3 配置指南，版本 7.6

上次修改日期: 2026 年 1 月 5 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 NONINFRINGEMENT 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.

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)

© 2024 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

关于网络分析和入侵策略 1

Snort 检测引擎 2

Snort 3 2

网络分析和入侵策略的准则和限制 5

策略如何检查流量是否存在入侵 6

解码、规范化和预处理：网络分析策略 7

访问控制规则：入侵策略选择 8

入侵检查：入侵策略、规则和变量集 8

入侵事件生成 10

Snort 中的不对称流检查 10

系统提供的与自定义的网络分析和入侵策略 11

系统提供的网络分析和入侵策略 12

自定义网络分析和入侵策略的优势 13

自定义网络分析策略的优势 13

自定义入侵策略的优势 14

自定义策略的限制 15

网络分析和入侵策略的必备条件 17

第 2 章

从 Snort 2 迁移到 Snort 3 19

Snort 3 检测引擎 19

网络分析和入侵策略的必备条件 20

如何从 Snort 2 迁移到 Snort 3 20

从 Snort 2 迁移到 Snort 3 的必备条件 20

在单个设备上启用 Snort 3 21
在多台设备上启用 Snort 3 21
将 Snort 2 自定义规则转换为 Snort 3 22
将所有入侵策略中的所有 Snort 2 自定义规则转换为 Snort 3 22
将单个入侵策略的 Snort 2 自定义规则转换为 Snort 3 23
查看 Snort 2 和 Snort 3 基本策略映射 24
将 Snort 2 规则与 Snort 3 同步 24
部署配置更改 25

第 I 部分： **Snort 3 中入侵检测和预防** 29

第 3 章 **Snort 3 入侵策略入门** 31
入侵策略概述 31
网络分析和入侵策略的必备条件 32
创建自定义 Snort 3 入侵策略 32
编辑 Snort 3 入侵策略 33
规则组报告 37
规则操作日志记录 37
更改入侵策略的基本策略 38
管理入侵策略 38
用于执行入侵防御的访问控制规则配置 39
访问控制规则配置和入侵策略 39
配置访问控制规则以执行入侵防御 40
部署配置更改 40

第 4 章 **使用规则调整入侵策略** 43
调整入侵规则概述 43
入侵规则类型 44
网络分析和入侵策略的必备条件 45
Snort 3 中的自定义规则 45
查看入侵策略中的 Snort 3 入侵规则 48

入侵规则操作 49
入侵规则操作选项 49
设置入侵规则操作 49
入侵策略中的入侵事件通知过滤器 50
入侵事件阈值 50
设置入侵事件阈值 50
在 Snort 3 中为入侵规则设置阈值 52
查看和删除入侵事件阈值 53
入侵策略抑制配置 53
入侵策略抑制类型 53
在 Snort 3 中为入侵规则设置抑制 53
查看和删除抑制条件 54
添加入侵规则注释 55
将 Snort 2 自定义规则转换为 Snort 3 55
将所有入侵策略中的所有 Snort 2 自定义规则转换为 Snort 3 56
将单个入侵策略的 Snort 2 自定义规则转换为 Snort 3 56
将自定义规则添加到规则组 57
将具有自定义规则的规则组添加到入侵策略 58
管理 Snort 3 中的自定义规则 59
删除自定义规则 60
删除规则组 60

第 5 章 根据网络资产定制入侵防护 63
LSP 更新中的 Snort 3 规则更改 63
Cisco Secure Firewall 建议规则的概述 63
网络分析和入侵策略的必备条件 64
在 Snort 3 生成新的 Cisco Secure Firewall 建议 64

第 II 部分： Snort 3 中的高级网络分析 69

第 6 章 Snort 3 网络分析策略入门 71

网络分析策略概览 71
管理网络分析策略 72
网络分析策略的 Snort 3 定义和术语 72
网络分析和入侵策略的必备条件 74
为 Snort 3 自定义网络分析策略的创建 74
通用工业协议安全 78
检测和阻止 CIP 数据包中的安全分段 79
网络分析策略映射 79
查看网络分析策略映射 80
创建网络分析策略 80
修改网络分析策略 80
在网络分析策略页面上搜索检查器 81
复制检查器配置 82
自定义网络分析策略 82
对检查器进行内联编辑以覆盖配置 85
在内联编辑期间恢复未保存的更改 86
查看具有覆盖的检查器列表 87
将覆盖的配置恢复为默认配置 87
验证 Snort 3 策略 88
自定义网络分析策略配置示例 90
网络分析策略设置和缓存的更改 101

第 III 部分：
Snort 3 的加密可视性引擎 103

第 7 章
加密可视性引擎 105
加密可视性引擎概述 105
EVE 工作原理 106
危害事件表现 107
EVE 中的 QUIC 指纹识别 107
配置 EVE 107
查看 加密可视性引擎事件 109

查看 EVE 控制面板 109
配置 EVE 例外规则 110
从统一事件添加例外规则 111
事件扩充 111

第 IV 部分： Snort 3 的大象流检测 113

第 8 章 大象流检测 115
关于大象流检测和补救 115
从智能应用绕行升级大象流 115
配置大象流 116

第 V 部分： Snort 3 使用案例 119

第 9 章 使用案例 - 在 Cisco Secure Firewall Management Center 中从 Snort 2 迁移到 Snort 3 121
从 Snort 2 迁移到 Snort 3 121
迁移到 Snort 3 的优势 121
示例业务情景 122
从 Snort 2 迁移到 Snort 3 的最佳实践 122
前提条件 122
端到端迁移工作流程 122
在威胁防御上启用 Snort 3 123
将单个入侵策略的 Snort 2 规则转换为 Snort 3 124
部署配置更改 129

第 10 章 使用案例 - 在 Cisco Secure Fiewall Management Center 生成 Snort 3 建议 131
Snort 3 规则建议 131
优势 132
示例业务情景 132
最佳实践 132
前提条件 132

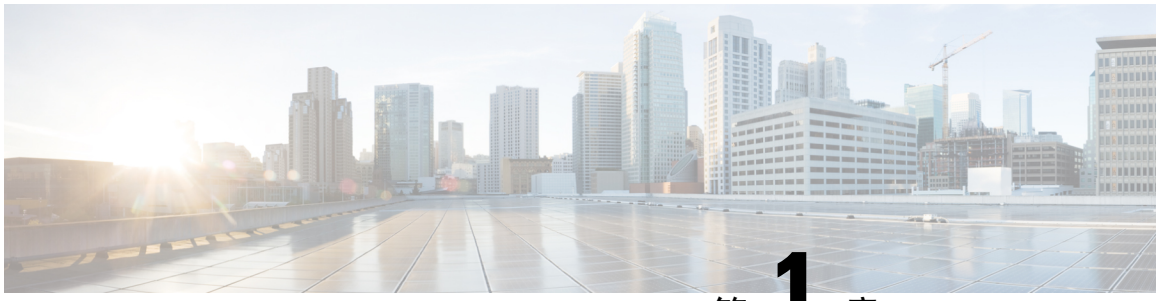
生成 Snort 3 建议 132
部署配置更改 135

第 11 章 使用案例 - 根据 EVE 威胁置信度评分阻止流量 139
关于加密可视性引擎 139
优势 139
示例业务情景 139
前提条件 140
高级工作流程 140
在 EVE 中配置阻止阈值 140
查看 EVE 事件 143
其他参考资料 144

第 12 章 使用案例 - 配置大象流检测结果 145
关于大象流 145
关于大象流检测和补救的优势 145
大象流工作流程 145
示例业务情景 146
前提条件 146
配置大象流参数 147
查看大象流的事件 149
配置大象流补救豁免 150
查看大象流补救豁免事件 153
其他参考资料 153

第 13 章 在 Snort 3 入侵策略中使用 MITRE 框架缓解威胁 155
关于 MITRE ATT&CK 框架 155
MITRE 框架的优势 156
MITRE 网络的业务场景示例 156
MITRE 框架的必备条件 156
查看和编辑 Snort 3 入侵策略 156

查看入侵事件 161
其他参考资料 163



第 1 章

网络分析和入侵策略概述

Snort 检测引擎是 Cisco Secure Firewall Threat Defense（前称 Firepower Threat Defense）设备不可或缺的一部分。本章提供 Snort 3 网络分析和入侵策略概述。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。

- 关于网络分析和入侵策略， 第 1 页
- Snort 检测引擎， 第 2 页
- Snort 3， 第 2 页
- 网络分析和入侵策略的准则和限制， 第 5 页
- 策略如何检查流量是否存在入侵， 第 6 页
- 系统提供的与自定义的网络分析和入侵策略， 第 11 页
- 网络分析和入侵策略的必备条件， 第 17 页

关于网络分析和入侵策略

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 智能小组 (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，从而能够提高托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

注意 **检测模式弃用**：从管理中心 7.4.0 版本开始，对于网络分析策略 (NAP)，**检测**检查模式已弃用，并将在后续版本中移除。

检测 模式旨在用作测试模式，以便您可以启用检测并查看它们在网络中的行为，然后再将其设置为丢弃流量，即显示将被丢弃的流量。

此行为已得到改进，其中所有检查器丢弃都由规则状态控制，并且您可以设置每个丢弃以生成事件。这样做是为了在配置规则状态以丢弃流量之前对其进行测试。由于我们现在可以对 Snort 3 中的流量丢弃进行精细控制，因此 **检测** 模式只会增加产品的复杂性，不需要，因此检测模式已弃用。

如果将**检测**模式下的 NAP 更改为**预防**，则处理入侵事件流量并具有结果 “会被丢弃”的 NAP 现在将为“已丢弃”，相应的流量将丢弃来自这些事件的流量。这适用于 GID 不是 1 或 3 的规则。GID 1 和 3 是文本/编译规则（通常由 Talos 提供或从您的自定义/导入规则中提供），所有其他 GID 都是异常检测。这些是在网络中触发的比较少见的规则。更改为 **预防** 模式不太可能对流量产生任何影响。您只需禁用适用于已丢弃流量的入侵规则，并将其设置为仅生成或禁用。

我们建议您选择 **预防** 作为检测模式，但如果您选择 **预防**，则无法恢复到 **检测** 模式。

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防火墙威胁防御 - Snort 检测引擎是 防火墙威胁防御 特定的，而不是 Cisco Secure Firewall Management Center （前称 Firepower Management Center） 特定的。防火墙管理中心 可以管理多个 防火墙威胁防御，每个都使用任一版本的 Snort（Snort 2 和 Snort 3）。虽然 防火墙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。
- 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。
- 安全智能的多层检测 - Snort 3 会检测最内部的 IP 地址，而不考虑层。
- 平台支持 - Snort 3 需要 防火墙威胁防御 7.0 或更高版本。ASA FirePOWER 或 NGIPSv 设备不支持此功能。
- 受管设备 - 版本 7.0 的 防火墙管理中心 可以同时支持版本 6.4、6.5、6.6、6.7 和 7.0 Snort 2 防火墙威胁防御以及版本 7.0 Snort 3 防火墙威胁防御。
- 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 防火墙威胁防御中启用的底层 Snort 引擎版本如何， 防火墙管理中心 中配置的访问控制策略、入侵策略、网络分析策略均可在应用策略时无缝地工作。 防火墙管理中心 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) - 替换适用于 Snort 3 下一代入侵规则的 Snort 规则更新 (SRU) 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 防火墙管理中心 和 防火墙威胁防御 版本 7.0 或更高的修改后的默认入侵策略设置。当您将 防火墙管理中心 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 24 页。

- 同步 Snort 2 和 Snort 3 规则覆盖 - 防火墙威胁防御 升级到 7.0 后，可以将 防火墙威胁防御 的检测引擎升级到 Snort 3 版本。防火墙管理中心 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 防火墙威胁防御，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 24 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 45 页。
- 规则组 - 防火墙管理中心 将所有 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。

  从防火墙管理中心7.3.0，支持多个级别的规则组的规则导航，这为规则提供了更大的灵活性和逻辑分组。添加了 MITRE 框架，使您能够使用 MITRE 框架浏览规则。MITRE 只是另一个类别的规则组，是 Talos 规则组的一部分。

注释 有关 MITRE 的信息，请参阅 https://attack.mitre.org 。

  一条规则可以是多个规则组的一部分，例如多个 MITRE ATT&CK 规则组、规则类别规则组、多个“资产类型”规则组、恶意软件活动等。入侵策略编辑器中列出了可用的规则组，可以选择这些规则组以增强策略。

  使用多级分层规则组的结构，您现在可以向下遍历到最后一个元素，即“枝叶规则组”。这些规则组包含彼此相关的规则集，例如特定类型的漏洞、类似的目标系统或类似的威胁类别。规则组有四个与其关联的安全级别。您可以更改安全级别，添加或删除规则组，并且可以更改与网络上看到的流量匹配的规则的规则操作。这样做是为了在安全性、性能和防误报之间取得令人满意的平衡。

  要编辑 Snort 3 入侵策略，请参阅编辑 Snort 3 入侵策略，第 33 页。

  有关入侵事件中的规则组报告，请参阅规则组报告，第 37 页。

- 在 Snort 2 和 Snort 3 引擎之间切换 - 防火墙威胁防御，支持 Snort 3 的版本也可以支持 Snort 2。从效率的角度来看，不建议从 Snort 3 切换到 Snort 2。

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。

网络分析和入侵策略的准则和限制

- 具有小数据包的流量百分比较高会导致Snort性能下降。即使禁用所有预处理器，也会观察到此行为。
- 当您尝试在内存不足的威胁防御设备上部署配置更改时，也会触发Snort部署。这会导致大量消耗RSS内存。如果在设备上部署大型配置（例如包含大量Snort IPS规则、网络对象和访问控制列表的多个IPS策略），Snort内存使用率也会受到影响。可以通过优化配置来缓解此类内存问题。有关如何配置访问控制规则以优化配置的最佳实践，请参阅 访问控制规则的最佳实践。
- 如果增加Threat Defense Virtual实例的内存，必须重新部署配置，Snort 3才能利用额外的内存。

注释 增加 Threat Defense Virtual 实例的内存时，Snort 3 的内存分配不会自动调整。必须重新部署配置，以重新生成相关配置文件（例如 `memory_allocation.lua`），这些文件会将更新后的资源限制应用于 Snort 3。

- 如果SIP流之后跟随来自同一连接的RTP流，Snort会检测用于建立连接的初始SIP通信，并允许SIP流量。默认情况下，SIP通信之后的RTP流也会被信任，并绕过已配置的规则。要防止此类情况，信任父SIP连接或将父SIP连接添加到预过滤器规则，可确保只有SIP流绕过Snort检测，并允许后续的RTP流分别根据相应规则进行评估。
- 通过系统日志或eStreamer完全限定事件源转发入侵数据包事件时，由于可用于系统日志生成和eStreamer的缓冲区大小限制，数据包数据字段可能会被截断。在这种情况下，数据包长度将不匹配实际发送的数据包数据。
- 不能同时进行策略更改、切换 Snort 版本并部署这两类更改。必须先进行所需的策略更改并部署，或先切换 Snort 版本并部署。

防火墙管理中心管理的 防火墙威胁防御 的 Snort 3 的功能限制

下表列出了 防火墙管理中心管理的 防火墙威胁防御 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

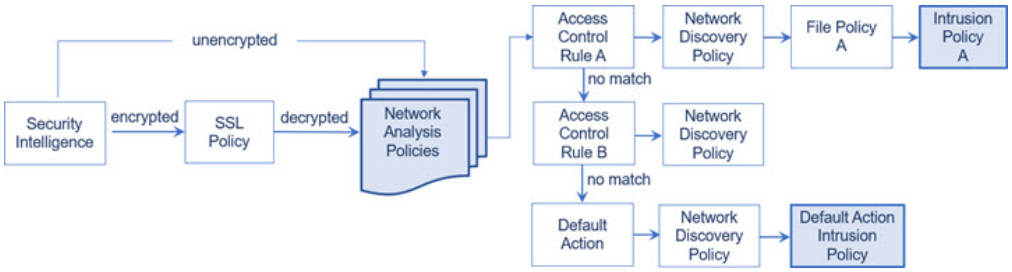
策略/区域	不支持的功能
访问控制策略	以下应用设置： • 安全搜索 • YouTube EDU

策略/区域	不支持的功能
入侵策略	• 全局规则阈值 • 日志记录配置： • SNMP • SRU 规则更新，因为 Snort 3 仅支持 LSP 规则更新
其他功能	使用 FQDN 名称进行事件日志记录

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）。



注释 禁用 TLS 服务器身份时，Snort 3 不会执行 SNI 不匹配检测。它仅评估客户端 Hello 数据包中的 SNI，并绕过服务器 Hello 数据包中证书的通用名称 (CN) 的验证。

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。

注释 对于规则操作为 **信任** 的访问控制策略和操作为 **快速路径** 的预过滤器规则并禁用日志记录选项，您将观察到仍在系统中生成流结束事件。这些事件在管理中心事件页面上不可见。

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 6 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 Cisoc Talos 智能组 (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 Firepower 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。当您将配置部署到 防火墙管理中心上的 防火墙威胁防御 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）。托管设备将其事件传输到防火墙管理中心，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，托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。

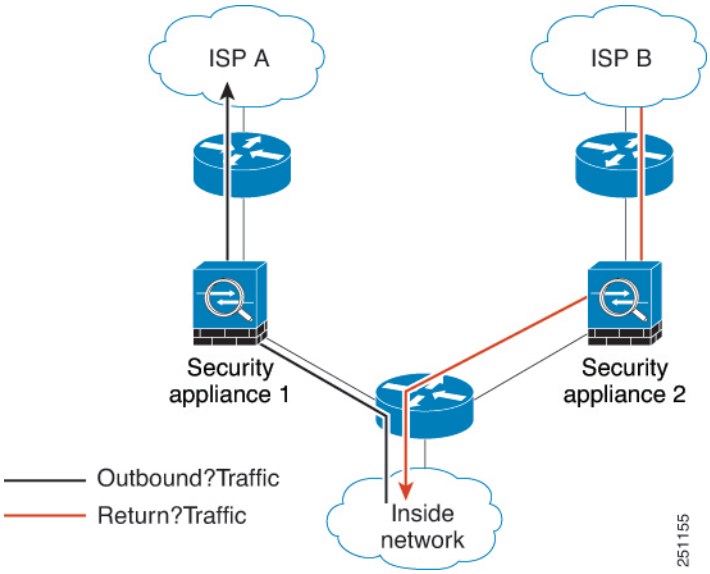
随着数据库累计入侵事件，您可以开始分析潜在攻击。系统为您提供复审入侵事件和评估其在网络环境与安全策略情境中是否重要所需的工具。

Snort 中的不对称流检查

在使用不对称路由的内联部署中，由于 Snort 的单向流量可视性有限，因此会损害数据包规范化。Snort 无法从未知流方向考虑 TCP 握手参数，例如窗口缩放或最大分段大小 (MSS)，这些参数可能导致主机接收大量数据包。

在下图中，两台设备都在运行 Snort 引擎。但是，引擎都未观察到完整的流量。未完全捕获流的 TCP 三次握手，这限制了可以应用的规范化类型。但是，在对 Snort 引擎可见的流侧会执行其他有效的规范化。

图 *1:* 非对称路由



在具有非对称路由的环境中，Snort可以无缝适应动态变化，而无需额外配置。它会根据流模式动态调整其操作。请注意，不对称流量可能会影响防火墙的有效性，可能不是最佳选择。但是，Snort旨在在必要时为此类部署提供支持。

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智能选项（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为作为默认值。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 智能组 (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“平衡安全和连接”策略和设置作为默认值。

连接优先于安全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。

无活动规则入侵策略

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中的已启用规则，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处理由托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。

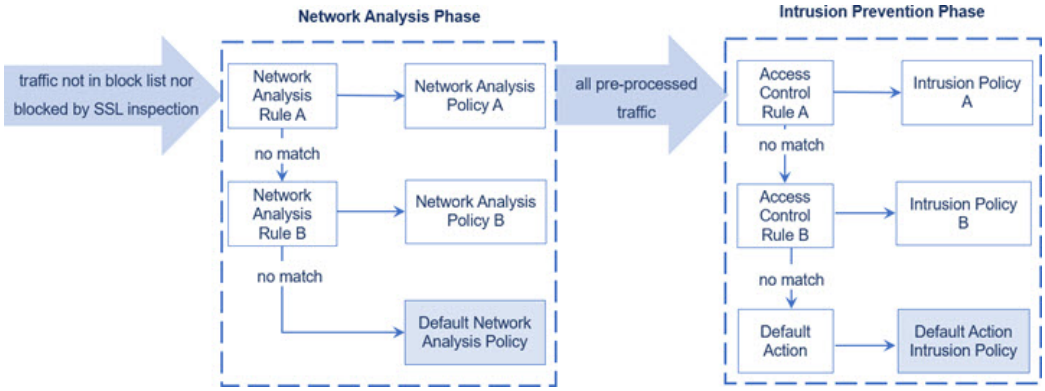
注释 要获取禁用检查器的性能优势，您 **必须** 确保自己的入侵策略均未启用需要该检查器的规则。

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。

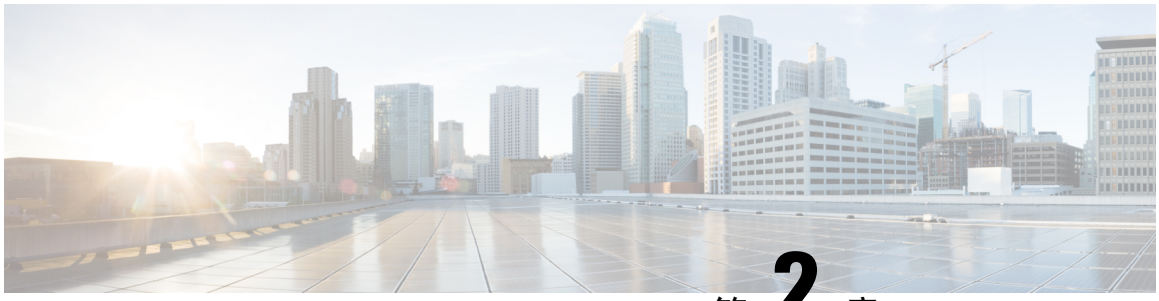
每个数据包的处理均由网络分析策略和入侵策略对进行监管，但系统**不**为您协调该对。请考虑以下情景：访问控制策略配置错误，以致网络分析规则 A 和访问控制规则 A 不处理相同流量。例如，您可能希望配对的策略监管特殊安全区域上流量的处理，但是在两条规则的条件中错误地使用不同的区域。这可能会导致错误地预处理流量。因此，使用网络分析规则和自定义策略定制预处理是一项**高级**任务。

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**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必备条件

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

您必须是管理员用户，才能管理网络分析、入侵策略和执行迁移任务。



第 2 章

从 Snort 2 迁移到 Snort 3

从版本 7.0 开始，Snort 3 是具有 防火墙管理中心 的新 防火墙威胁防御 部署的默认检测引擎。如果您仍在使用 Snort 2 检测引擎，请立即切换到 Snort 3 以提高检测和性能。

将 防火墙威胁防御 升级到版本 7.2 至 7.6 也会将符合条件的 Snort 2 设备升级到 Snort 3。对于因使用自定义入侵或网络分析策略而不符合条件的设备，可在此处手动升级到 Snort 3 以提高检测和性能。

虽然您可以切换回单个设备，但不应这样做。Snort 2 将在未来版本中弃用，最终将阻止 防火墙威胁防御 升级。

- Snort 3 检测引擎，第 19 页
- 网络分析和入侵策略的必备条件，第 20 页
- 如何从 Snort 2 迁移到 Snort 3，第 20 页
- 查看 Snort 2 和 Snort 3 基本策略映射，第 24 页
- 将 Snort 2 规则与 Snort 3 同步 ，第 24 页
- 部署配置更改，第 25 页

Snort 3 检测引擎

Snort 3 是版本 7.0 及更高版本的新注册 防火墙威胁防御 设备的默认检测引擎。但是，对于较低版本的 防火墙威胁防御 设备，Snort 2 是默认检测引擎。将受管 防火墙威胁防御 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 防火墙威胁防御的使用 Snort 3，必须明确启用它。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。

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 24 页。

网络分析和入侵策略的必备条件

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

您必须是管理员用户，才能管理网络分析、入侵策略和执行迁移任务。

如何从 Snort 2 迁移到 Snort 3

从 Snort 2 迁移到 Snort 3 需要将 防火墙威胁防御 设备的检测引擎从 Snort 2 切换到 Snort 3。

根据您的要求，下表列出了完成设备从 Snort 2 迁移到 Snort 3 的任务：

步骤	任务	程序链接
1	启用 Snort 3	• 在单个设备上启用 Snort 3，第 21 页 • 在多台设备上启用 Snort 3，第 21 页
2	将 Snort 2 自定义规则转换为 Snort 3	• 将所有入侵策略中的所有 Snort 2 自定义规则转换为 Snort 3，第 22 页 • 将单个入侵策略的 Snort 2 自定义规则转换为 Snort 3，第 23 页
3	将 Snort 2 规则与 Snort 3 同步	将 Snort 2 规则与 Snort 3 同步 ，第 24 页

从 Snort 2 迁移到 Snort 3 的必备条件

以下是在将设备从 Snort 2 迁移到 Snort 3 之前必须考虑的建议前提条件。

- 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。
- 克隆入侵策略。为此，您可以使用现有策略作为基本策略来创建入侵策略的副本。在**入侵策略**页面中，点击**创建策略**，然后从**基本策略**下拉列表中选择现有入侵策略。

在单个设备上启用 Snort 3

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。

过程

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 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)**。

注释
如果要禁用 Snort 3，请点击“检测引擎”部分中的 **恢复为 Snort 2** 。

步骤 5 点击**是**。

下一步做什么

在设备上部署更改。请参阅部署配置更改，第 25 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。

在多台设备上启用 Snort 3

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

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。

过程

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**选择批量操作**下拉列表，然后选择**升级到 Snort 3**。

步骤 4 点击**是**。

下一步做什么

在设备上部署更改。请参阅部署配置更改，第 25 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。

将 Snort 2 自定义规则转换为 Snort 3

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，请参阅以下程序。

- 将所有入侵策略中的所有 Snort 2 自定义规则转换为 Snort 3，第 22 页
- 将单个入侵策略的 Snort 2 自定义规则转换为 Snort 3，第 23 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。

将所有入侵策略中的所有 Snort 2 自定义规则转换为 Snort 3

过程

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 Snort 2 规则和导入** - 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 防火墙管理中心 。

- **转换 Snort 2 规则并夏泽** - 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 点击**确定**。

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 将自定义规则添加到规则组，第 57 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 25 页。

将单个入侵策略的 Snort 2 自定义规则转换为 Snort 3

过程

步骤 1 选择**策略** > **访问控制标题** > **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 **Snort 不同步**（ ）。

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**Snort 同步**（ ）。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 防火墙管理中心 。
- **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 25 页。

查看 Snort 2 和 Snort 3 基本策略映射

过程

步骤 1 选择**策略** > **访问控制标题** > **入侵**。

步骤 2 确保选择**入侵策略**选项卡。

步骤 3 点击 **IPS 映射**。

步骤 4 在 **IPS 策略映射** 对话框中，点击 **查看映射** 以查看 Snort 3 到 Snort 2 的入侵策略映射。

步骤 5 点击**确定 (OK)**。

将 Snort 2 规则与 Snort 3 同步

为确保 Snort 2 版本设置和自定义规则保留并转移到 Snort 3， 防火墙管理中心 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。此实用程序帮助将 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 防火墙管理中心 从 6.0 之前的版本升级到 7.0 或更高版本，系统会同步配置。如果 防火墙管理中心 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。

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。

过程

步骤 1 选择**策略** > **访问控制标题** > **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**”**(Sync)** 图标 **Snort 不同步**（ ）。

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**Snort 同步**（ ）。

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 23 页。

下一步做什么

部署配置更改；请参阅部署配置更改，第 25 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 *Cisco Secure Firewall Management Center* 指南 中的 部署配置更改 主题，了解部署更改的前提条件和影响。

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

过程

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

GUI 页面列出了具有 **待处理** 状态的过期配置的设备。

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

  注释
  没有为已删除的策略和对象提供用户名。

- **检查中断** 列指示在部署过程中是否可能导致设备中的流量检查中断。

  如果设备的此为空白，则表明在部署过程中该设备上不会出现流量检查中断。

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

步骤 2 识别并选择要部署配置更改的设备。

- 搜索 - 在搜索框中搜索设备名称、类型、域、组或状态。
- 展开 - 点击 **展开箭头**（ ） 以查看要部署的设备特定的配置更改。

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

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

步骤 3 点击**部署 (Deploy)**。

步骤 4 如果系统在要部署的更改中发现错误或警告，则会在**验证消息**窗口中显示它们。要查看完整详细信息，请点击警告或错误前的箭头图标。

有以下选项可供选择：

- 部署 - 继续部署而无需解决警告情况。如果系统识别错误，则无法继续。

- 关闭 - 退出而不部署。解决错误和警告情况，并尝试重新部署该配置。

下一步做什么

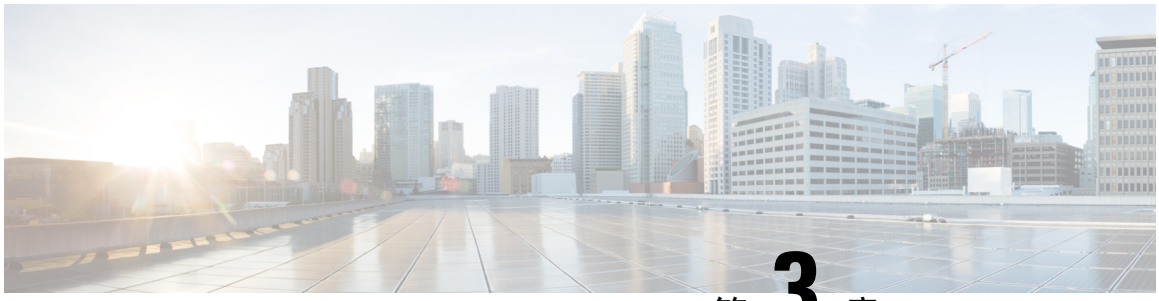
在部署过程中，如果有部署失败，则可能会影响流量。不过，这取决于某些条件。如果部署中存在特定的配置更改，则部署失败可能导致流量中断。有关部署过程的详细信息，请参阅 *Cisco Secure Firewall Management Center* 配置指南中的部署配置更改主题。



第 部分

Snort 3 中入侵检测和预防

- Snort 3 入侵策略入门， 第 31 页
- 使用规则调整入侵策略， 第 43 页
- 根据网络资产定制入侵防护， 第 63 页



第 3 章

Snort 3 入侵策略入门

本章提供有关为入侵检测和防御管理 Snort 3 入侵策略和访问控制规则配置的信息。

- 入侵策略概述， 第 31 页
- 网络分析和入侵策略的必备条件， 第 32 页
- 创建自定义 Snort 3 入侵策略 ， 第 32 页
- 编辑 Snort 3 入侵策略， 第 33 页
- 更改入侵策略的基本策略， 第 38 页
- 管理入侵策略， 第 38 页
- 用于执行入侵防御的访问控制规则配置， 第 39 页
- 部署配置更改， 第 40 页

入侵策略概述

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，以及在内联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 智能组 (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其，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。

网络分析和入侵策略的必备条件

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

您必须是管理员用户，才能管理网络分析、入侵策略和执行迁移任务。

创建自定义 Snort 3 入侵策略

过程

步骤 1 选择**策略** > **访问控制标题** > **入侵**。

步骤 2 点击**创建策略 (Create Policy)**。

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 (Inspection Mode)**。

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已存在的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 33 页。

编辑 Snort 3 入侵策略

编辑 Snort 3 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。

过程

步骤 1 选择**策略** > **访问控制标题** > **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。

注意
仅 Snort 3 版本的策略会更改检测模式。现有检测模式在 Snort 2 版本中保持不变，这意味着您的 Snort 2 和 Snort 3 版本的策略将具有不同的检测模式。我们建议您谨慎使用此选项。

- **预防**-已触发的阻止规则创建事件（警报）并丢弃连接。
- **检测**-已触发阻止规则创建警报。

  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。

步骤 5 点击 **基本策略** 层定义入侵策略的默认设置。

- 搜索规则 - 使用搜索字段过滤显示内容。您可以输入 GID、SID、规则消息或参考信息。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。您还可以在“搜索”文本框中点击以选择以下任何选项：
  - 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

- 查看过滤的规则 - 点击任意 **预设** 以查看设置为警报、阻止、禁用等的规则。

  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 Microsoft 漏洞提供过滤器选项。

- 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。

步骤 6 **组覆盖**- 点击列出所有规则组类别的 **组覆盖** 层。系统将显示包含说明、覆盖和已启用组等内容的顶级父规则组。父规则组无法更新，且为只读。只能更新枝叶规则组。在每个规则组中，您可以遍历到最后一个枝叶组。在每个组中，您可以覆盖、包含和排除规则组。在枝叶规则组中，您可以：

- 搜索规则组 - 使用搜索字段输入关键字并搜索规则组。
- 在左侧面板中，您可以选择任何预设过滤器选项来搜索规则组：
  - 全部 - 用于显示所有规则组。
  - 已排除 - 适用于已排除的组。
  - 已包含 - 适用于已包含的组。
  - 已覆盖 - 适用于已覆盖规则组配置。

- 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点击它。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。

  在 **编辑安全级别** 对话框中，您可以选择点击 **恢复为默认值**，这将恢复您所做的更改。

  防火墙管理中心 自动更改已配置安全级别的规则组规则的操作。在 **规则覆盖** 层，每次更改安全级别时，请注意 **预设** 中阻止规则和禁用规则的计数。

- 您可以对安全级别进行批量更改，以更改特定规则类别中所有规则组的安全级别。批量安全级别适用于具有多个规则组的规则组。批量更新规则组后，您仍然可以更新其中任何关联规则组的安全级别。

  规则组中可以有 **混合** 的安全级别； **混合** 表示子组包含父规则组内的混合安全级别。

- 已包括或排除规则组 - 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。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 防火墙管理中心中上传自定义规则的信息，请参阅 将自定义规则添加到规则组，第 57 页。

  排除规则组：

  1. 导航规则组窗格，然后选择要排除的规则组。
  2. 点击右侧窗格中的 **排除** 超链接。
  3. 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. 点击规则组过滤器下拉列表旁边的 **添加** (+) 。
  2. 选择要添加的所有规则组旁边的复选框。
  3. 点击**保存**。

- 对于枝叶规则组，点击 **覆盖** 列标题下的 图标可查看规则操作跟踪，其中描述了由于入侵规则的基本策略和组覆盖而可以分配的覆盖规则操作的顺序。可以从基本策略配置或用户组覆盖中获取规则操作。用户组覆盖优先级介于两者之间；优先级是指分配给规则组的最终覆盖操作。
- 点击 **规则计数** 列标题下的规则计数（数字），查看属于规则组的规则摘要。

步骤 7 **建议**- 如果要生成和应用思科建议的规则，请点击 **建议** 层。建议使用主机数据库来基于已知漏洞启用或禁用规则。

步骤 8 **规则覆盖** - 点击**规则覆盖 (Rule Overrides)** 层以选择任何预设来查看规则，这些预设设置为警报、阻止、禁用、覆盖、重写、通过、删除或拒绝。

- **设置方式** 列按状态（基本策略）显示默认设置，或按组覆盖、规则覆盖或建议显示修改后的规则状态。**所有规则** 中的 **设置者** 列（位于左侧窗格中）根据优先级顺序显示规则操作覆盖操作的轨迹。规则操作的优先级顺序为规则覆盖 > 建议 > 组覆盖 > 基本策略。
- 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** 栏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。

  注释
  “通过”操作仅适用于自定义规则，不适用于系统提供的规则。

- **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。

有关 IPS 规则操作日志记录，请参阅 规则操作日志记录，第 37 页。

如果有 **反应** 规则转换为警报操作。

步骤 9 点击 **摘要** 层可查看当前策略更改的整体视图。策略摘要页面包含以下信息：

- 策略的规则分布，即活动规则、禁用规则等。
- 用于导出策略并生成入侵策略报告的选项。
- 基础策略详细信息。
- 生成建议的选项。
- 显示已覆盖的组列表的组覆盖。
- 显示已覆盖的规则列表的规则覆盖。
- 在 **摘要** 层中，点击？图标可打开解释 Snort 分层概念的 Snort 帮助程序指南的弹出窗口。

要更改基本策略，请参阅 更改入侵策略的基本策略，第 38 页。

注释
您可以导航至 **对象** 入侵规则，然后点击 Snort 3 所有规则 选项卡并遍历所有入侵规则组。**对象** > **入侵规则**父规则组列出关联的子组和规则计数。

下一步做什么

部署配置更改；请参阅部署配置更改，第 25 页。

规则组报告

规则组反映在生成的入侵事件中，并且还会调出 MITRE 策略和技术。有用于 MITRE 策略和技术以及用于入侵事件的非 MITRE 规则组的列。要访问入侵事件，请在 防火墙管理中心 中导航至 **分析** > **入侵** > **事件**，然后点击**事件表格视图**选项卡。您还可以在 **统一事件** 查看器中查看入侵事件字段。在 **分析** 选项卡中，点击 **统一事件**。

在 **入侵事件** 页面中，为规则组报告添加了以下字段。请注意，您必须明确启用上述列。

- MITRE ATT&CK
- 规则组

有关这些字段的信息，请参阅 *Cisco Firepower Management Center* 管理指南， *7.3* 版中 入侵事件字段 的部分。

规则操作日志记录

从 防火墙管理中心 7.2.0 开始，在 **入侵事件** 页面中，**内联结果** 列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。

Snort 3 的 **IPS** 操作	内联结果 - 防火墙管理中心 **7.1.0** 及更早版本	内联结果 - 防火墙管理中心 **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（防火墙管理中心 7.2.0 管理 防火墙威胁防御 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， 防火墙管理中心 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。

过程

步骤 1 选择**策略** > **访问控制标题** > **入侵**。

步骤 2 点击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 (Save)**。

下一步做什么

部署配置更改；请参阅部署配置更改 ， 第 25 页。

管理入侵策略

在“入侵策略”页面（**策略** > **访问控制标题** > **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。

过程

步骤 1 选择**策略** > **访问控制标题** > **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 32 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**确定 (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 33 页。
- 导出 - 如果要导出入侵策略以在另一个 防火墙管理中心上导入，请点击导出；请参阅最新版本的 *Cisco Secure Firewall Management Center* 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 25 页。
- 报告 - 请点击 **报告**；请参阅最新版本的 *Cisco Secure Firewall Management Center* 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。

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 智能组 (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。

过程

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 *Cisco Secure Firewall Management Center* 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 点击**保存 (Save)** 保存规则。

步骤 7 点击**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 25 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 *Cisco Secure Firewall Management Center* 指南 中的 部署配置更改 主题，了解部署更改的前提条件和影响。

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

过程

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

GUI 页面列出了具有 **待处理** 状态的过期配置的设备。

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

  注释
  没有为已删除的策略和对象提供用户名。

- **检查中断** 列指示在部署过程中是否可能导致设备中的流量检查中断。

  如果设备的此为空白，则表明在部署过程中该设备上不会出现流量检查中断。

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

步骤 2 识别并选择要部署配置更改的设备。

- 搜索 - 在搜索框中搜索设备名称、类型、域、组或状态。
- 展开 - 点击 **展开箭头**（ ） 以查看要部署的设备特定的配置更改。

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

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

步骤 3 点击**部署 (Deploy)**。

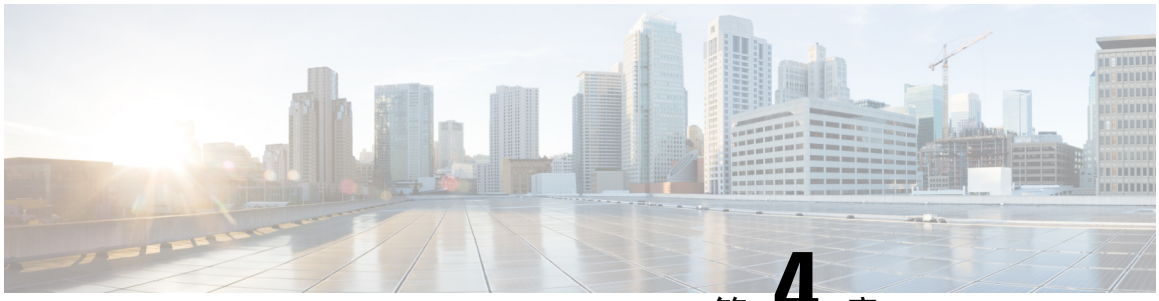
步骤 4 如果系统在要部署的更改中发现错误或警告，则会在**验证消息**窗口中显示它们。要查看完整详细信息，请点击警告或错误前的箭头图标。

有以下选项可供选择：

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

下一步做什么

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



第 4 章

使用规则调整入侵策略

本章提供有关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。

- 调整入侵规则概述， 第 43 页
- 入侵规则类型， 第 44 页
- 网络分析和入侵策略的必备条件， 第 45 页
- Snort 3 中的自定义规则， 第 45 页
- 查看入侵策略中的 Snort 3 入侵规则， 第 48 页
- 入侵规则操作， 第 49 页
- 入侵策略中的入侵事件通知过滤器， 第 50 页
- 添加入侵规则注释， 第 55 页
- 将 Snort 2 自定义规则转换为 Snort 3， 第 55 页
- 将自定义规则添加到规则组， 第 57 页
- 将具有自定义规则的规则组添加到入侵策略， 第 58 页
- 管理 Snort 3 中的自定义规则， 第 59 页
- 删除自定义规则， 第 60 页
- 删除规则组， 第 60 页

调整入侵规则概述

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。

注释 建议您不要修改共享对象规则，而建议仅为威胁防御设备启用或禁用这些规则。要创建自定义 Snort 规则，请联系思科支持部门。

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和标准文本规则
- 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 智能小组 (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的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。

网络分析和入侵策略的必备条件

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

您必须是管理员用户，才能管理网络分析、入侵策略和执行迁移任务。

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。

要检查 SID 是已启用还是已禁用，请验证 snort.lua 文件中的条目，该文件位于 `./file-contents/ngfw/var/sf/detection_engines/<id>/ips/<id>` 目录。

- 如果 SID 默认为禁用，则 文件中将不会有任何条目。
- 如果手动启用 SID，您将看到包含 **enable:yes** 的条目。
- 如果 SID 在手动启用后被禁用，该条目将保留在文件中，并将显示 **enable:no**。

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。
- 您可以使用 Snort 3 来创建自定义入侵规则。但是，目前不支持对这些规则进行调整和故障排除。
- Snort 规则中的 *classtype* 为规则分配分类，指示与事件关联的攻击类型。每个 *classtype* 还关联了一个 1-4 优先级。但是，威胁防御设备上某些类 类型 的优先级与 Snort 文档 中提到的开源 Snort 类类型优先级不匹配。例如， *tcp-connection* 在开源 Snort 中的优先级为 4，而在威胁防御设备上为其分配的优先级为 3。

Snort 3 中的敏感数据检测

社会保险号、信用卡号、电子邮件等敏感数据可能会被有意或无意地在互联网上泄露。敏感数据检测用于检测可能的敏感数据泄漏并生成事件。仅当传输大量个人身份信息 (PII) 数据时，才会生成事件。敏感数据检测可以屏蔽事件输出中的 PII。

sd_pattern 选项

使用 `sd_pattern` IPS 选项检测和过滤 PII。这些信息包括信用卡号、美国社会保险号、电话号码和电子邮件地址。正则表达式 (regex) 语法可用于定义您自己的 PII。

sd_pattern 选项具有以下设置：

- 模式 - 指定要在 PDU 中查找的正则表达式的隐式必需设置。正则表达式必须使用 PCRE 语法编写。
- 阈值 - 明确的可选设置，指定生成事件所需的 PDU 中的匹配数。

`sd_pattern` as IPS 规则选项在 Snort 中可用，对其他检查器没有要求。规则选项的语法为：

```
sd_pattern: "<pattern> "[, threshold<count> ];
```

例如：

```
sd_pattern:"credit_card", threshold 2;
```

内置模式

敏感数据有五种内置模式。要在"模式"设置中使用内置模式，必须指定需要匹配的 PII 类型的名称，并将其替换为必要的正则表达式。PII 名称和正则表达式映射或模式如下所述：

- credit_card—

```
\d{4}\D?\d{4}\D?\d{2}\D?\d{2}\D?\d{3,4}
```

- us_social—

```
[0-8]\d{2}-\d{2}-\d{4}
```

- us_social_nodashes—

```
[0-8]\d{8}
```

- Email—

```
[a-zA-Z0-9!#$%&'*+\/=?^_`{|}~-]+(?:\.[a-zA-Z0-9!#$%&'*+\/=?^_`{|}~-]+)*@(?:[a-zA-Z0-9]
(?:[a-zA-Z0-9-]*[a-zA-Z0-9])?\.)+[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?
```

- us_phone—

```
(?:\+?1[-\.\s]?)?\(?([2-9][0-8]\d)\)?[-\.\s]([2-9]\d{2})[-\.\s](\d{4})
```

PII Name	模式
credit_card	`\d{4}\D?\d{4}\D?\d{2}\D?\d{2}\D?\d{3,4}`
us_social	`[0-8]\d{2}-\d{2}-\d{4}`
us_social_nodashes	`[0-8]\d{8}`
邮件	`[a-zA-Z0-9!#$%&'*+\/=?^_`{\|}~-]+(?:\.[a-zA-Z0-9!#$%&'*+\/=?^_`{|}~-]+)*@(?:[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?\.)+[a-zA-Z0-9](?:[a-zA-Z0-9-]*[a-zA-Z0-9])?`
us_phone	`(?:\+?1[-\.\s]?)?\(?([2-9][0-8]\d)\)?[-\.\s]([2-9]\d{2})[-\.\s](\d{4})`

与这些模式匹配的数据的掩码仅适用于信用卡、美国社会保险号、邮箱和美国电话号码的系统提供的规则或内置模式。屏蔽不适用于自定义规则或用户定义的PII模式。敏感数据的轻量级安全包(LSP)中提供了规则，gid:13。默认情况下，它们在任何系统提供的策略中均未启用。

LSP 中的敏感数据规则涵盖所有内置模式，并具有以下阈值：

- credit_card: 2
- us_social: 2
- us_social_nodashes: 20
- email: 20
- us_phone: 20

您可以使用 sd_pattern 选项创建自定义规则并修改现有规则。要执行此操作，请使用 Snort 3 入侵策略接口。

具有自定义模式和阈值的 sd_pattern 规则示例：

*alert tcp (sid: 1000000001; sd_pattern:"[\w-\.]+@([\w-]+\.)+[\w-]{2,4}",threshold 4; msg: "email,*阈值 *4")*

示例

使用敏感数据检测的自定义规则示例：

具有内置模式的规则：

```
alert tcp (
        msg:"SENSITIVE-DATA Email";
        flow:only_stream;
        pkt_data;
        sd_pattern:"email", threshold 5;
```

```
        service:http, smtp, ftp-data, imap, pop3;
        gid:2000;
        sid:1000001;
)
```

具有自定义模式的规则

```
alert tcp (
        msg:"SENSITIVE-DATA US phone numbers";
        flow:only_stream;
        file_data;
        sd_pattern:"+?3?8?(0[\s\.-]\d{2}[\s\.-]\d{3}[\s\.-]\d{2}[\s\.-]\d{2})", threshold
2;
        service:http, smtp, ftp-data, imap, pop3;
        gid:2000;
        sid:1000002;
)
```

以下是具有内置敏感数据模式的完整 Snort IPS 规则的更多示例：

- alert tcp (sid:1; msg:"Credit Card"; sd_pattern:"credit_card", threshold 2;)
- alert tcp (sid:2; msg:"US Social Number"; sd_pattern:"us_social", threshold 2;)
- alert tcp (sid:3; msg:"US Social Number No Dashes"; sd_pattern:"us_social_nodashes", threshold 2;)
- alert tcp (sid:4; msg:"US Phone Number"; sd_pattern:"us_phone", threshold 2;)
- alert tcp (sid:5; msg:"Email"; sd_pattern:"email", threshold 2;)

Cisco Secure Firewall Management Center 和安全防火墙设备管理器不支持禁用数据屏蔽。

有关如何向规则组添加自定义规则的信息，请参阅将自定义规则添加到规则组 ， 第 57 页。

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细信息。

过程

步骤 1 选择**策略** > **访问控制标题** > **入侵**。

步骤 2 点击策略旁边的 **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。

有关执行这些任务的详细信息，请参阅 编辑 Snort 3 入侵策略 ， 第 33 页 。

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 智能组 (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

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。

我们 **强烈** 建议您 **不要** 启用入侵策略中的所有入侵规则。如果启用所有规则，则您的托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。

过程

步骤 1 选择策略 > 访问控制标题 > 入侵。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

提示
此页面显示以下总数：

- 已禁用的规则
- 已启用的规则设置为警报
- 已启用的规则设置为阻止
- 已覆盖的规则

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** 下拉框中选择规则操作之一：有关不同规则操作的详细信息，请参阅 编辑 Snort 3 入侵策略，第 33 页。

步骤 5 点击**保存 (Save)**。

下一步做什么

部署配置更改；请参阅部署配置更改，第 25 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。

设置入侵事件阈值

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	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。
双向	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： • 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）

其次，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。

选项	说明
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。您为入侵规则设置的阈值将应用于每个数据包线程。但是，该配置仅在唯一流的上下文中完全应用。不同的网络流上可能有更多警报，但警报数不会少于配置的数量。

过程

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 请点击 **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 点击**保存**。

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。

查看和删除入侵事件阈值

要查看或删除存在的规则的阈值设置，使用“规则详细信息”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。

过程

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 选择具有已配置阈值的规则，如 **警报配置** 列中所示（ **警报配置** 列将 **阈值** 显示为该规则的链接）。

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 (Save)**。

下一步做什么

部署配置更改；请参阅部署配置更改 ， 第 25 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**，点击**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。

过程

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 请点击 **编辑** ()。

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

- 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 25 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。

过程

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 点击抑制旁边的 **清除** () 以删除抑制。

步骤 8 点击**保存 (Save)**。

下一步做什么

部署配置更改；请参阅部署配置更改，第 25 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。

过程

步骤 1 选择**策略** > **访问控制标题** > **入侵**。

步骤 2 点击要编辑的策略旁边的 **Snort 2 版本 (Snort 2 Version)**。

步骤 3 在列出所有规则的页面右侧，选择要添加注释的规则。

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”(Comments) 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 25 页。

将 Snort 2 自定义规则转换为 Snort 3

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。

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。

将所有入侵策略中的所有 Snort 2 自定义规则转换为 Snort 3

过程

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 Snort 2 规则和导入** - 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 防火墙管理中心 。
- **转换 Snort 2 规则并夏泽** - 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 点击**确定**。

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 将自定义规则添加到规则组 ， 第 57 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 25 页。

将单个入侵策略的 Snort 2 自定义规则转换为 Snort 3

过程

步骤 1 选择**策略** > **访问控制标题** > **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 **Snort 不同步**（ ）。

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**Snort 同步**（）。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 防火墙管理中心 。
- **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 25 页。

将自定义规则添加到规则组

在 防火墙管理中心 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。

过程

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 Snort 3 规则**。

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

步骤 6 点击**确定 (OK)**。

注释
如果所选文件中有任何错误，则无法继续。修复错误后，您可以下载错误文件和**替换文件**链接，以上传文件的第 2 版。

步骤 7 将规则关联到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 (Next)**。

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 (Finish)**。

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 防火墙管理中心 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 58 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 59 页。
- 部署配置更改；请参阅部署配置更改，第 25 页。

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 防火墙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。

过程

步骤 1 选择**策略 > 访问控制标题 > 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 在**添加规则组**窗口中，点击规则组旁边的 **展开箭头**（ › ） 图标以展开本地规则组。

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 (Save)**。

下一步做什么

部署配置更改；请参阅部署配置更改，第 25 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：

过程

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 25 页。

删除自定义规则

过程

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 选中要删除的策略的复选框。

步骤 5 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 6 从 **规则操作** 下拉框中，选择 **删除**。

步骤 7 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 25 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 33 页。

过程

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：

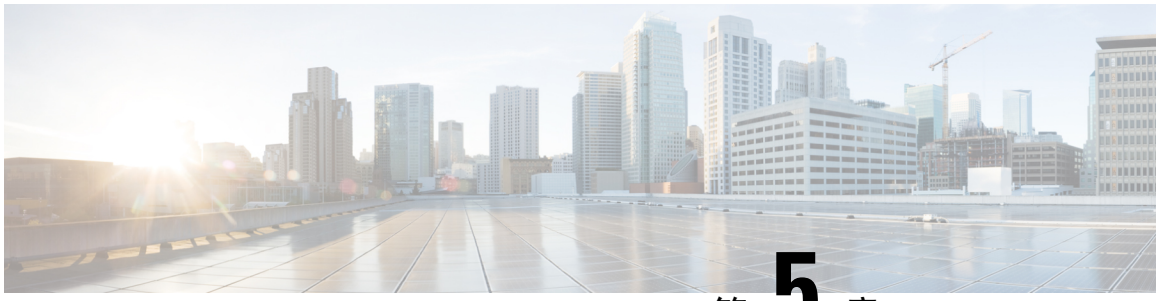
a) 选中 **规则操作** 下拉列表下方的复选框，以选择组中的所有规则。
b) 从 **规则操作** 下拉框中，选择按 **入侵策略**。
c) 选择 **所有策略** 单选按钮。
d) 从 **选择覆盖状态** 下拉列表中选择 **禁用** 。
e) 点击**保存**。

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 25 页。



第 5 章

根据网络资产定制入侵防护

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

- LSP 更新中的 Snort 3 规则更改 ， 第 63 页
- Cisco Secure Firewall 建议规则的概述， 第 63 页
- 网络分析和入侵策略的必备条件， 第 64 页
- 在 Snort 3 生成新的 Cisco Secure Firewall 建议， 第 64 页

LSP 更新中的 Snort 3 规则更改

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

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

要导航至**保留已删除 Snort 3 规则的用户覆盖 (Retain user overrides for deleted Snort 3 rules)** 复选框，请点击 **系统** (⚙) > **配置** > **入侵策略首选项**，然后选择配置 (Configuration)入侵策略首选项 (Intrusion Policy Preferences)。

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 **系统** (⚙) 旁边的“通知”(Notifications) 图标下的**任务 (Tasks)** 选项卡中。

Cisco Secure Firewall 建议规则的概述

您可以使用入侵规则建议来锁定与在网络中检测到的主机资产相关联的漏洞。例如，操作系统、服务器和客户端应用协议。这样，您就可根据自己的受监控网络的特定需求定制您的入侵策略。

系统为每个入侵策略制定一组单独的建议。它通常会建议标准文本规则和共享对象规则的规则状态更改。但是，它也可建议检查器和解码器规则的更改。

当生成规则状态建议时，可以使用默认设置或配置高级设置。通过高级设置，可以执行以下操作：

- 重新定义系统监控网络上的哪些主机以查找漏洞
- 影响系统根据规则开销建议哪些规则
- 指定是否生成建议以禁用规则

您还可以选择是要立即使用建议还是在接受之前审核建议（和受影响规则）。

选择使用建议规则状态会向入侵策略中添加只读 Cisco Secure Firewall 建议层，并且随后选择不使用建议规则状态会删除该层。

您可以安排任务来根据入侵策略中最近保存的配置设置自动生成建议。

系统不会更改手动设置的规则状态，如：

- 在生成建议之前手动设置指定规则的状态可防止系统将来修改这些规则的状态。
- 在生成建议之后手动设置指定规则的状态可覆盖这些规则的建议状态。

提示 入侵策略报告可能包含具有与建议状态不同的规则状态的规则列表。

在显示对建议过滤后的 Rules 页面时，或者从导航面板或 Policy Information 页面直接访问 Rules 页面后，可以手动设置规则状态、对规则排序并执行 Rules 页面中的任何其他可用操作，例如抑制规则、设置规则阈值等。

注释 Cisco Talos 智能组 (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 Cisco Secure Firewall 建议规则状态，则入侵策略中的规则与为网络资产建议的设置相匹配。

网络分析和入侵策略的必备条件

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

您必须是管理员用户，才能管理网络分析、入侵策略和执行迁移任务。

在 Snort 3 生成新的 Cisco Secure Firewall 建议

为入侵策略生成 Cisco Secure Firewall 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 Cisco Secure Firewall 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

Cisco Secure Firewall 建议具有以下要求：

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

过程

步骤 1 选择**策略** > **访问控制标题** > **入侵**。

步骤 2 点击入侵策略的 **Snort 3 版本** 按钮。

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

在 Cisco Secure Firewall 建议窗口中，您可以设置以下内容：

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

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

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

  - 安全级别 2：平衡安全性优先于连接

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

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

- 安全级别 3：安全优先于连接

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

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

- 安全级别 4：最大检测

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

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

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

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

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

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

步骤 4 生成并应用建议：

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

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

步骤 5 您可以验证这些建议，然后相应地选择应用它们：

- **接受** - 应用先前为入侵策略生成的建议。
- **刷新** - 重新生成并更新入侵策略的规则建议。
- **编辑** - 它会打开“建议”对话框，您可以提供建议输入值，然后生成建议。
- **全部删除** - 从策略中恢复或删除已应用的建议规则，并删除建议选项卡。

在 **所有规则**下，有一个建议的规则部分，其中显示建议的规则。

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

规则覆盖 > 生成的建议 > 组覆盖 > 基本 策略默认操作

对于已启用的建议，防火墙管理中心 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

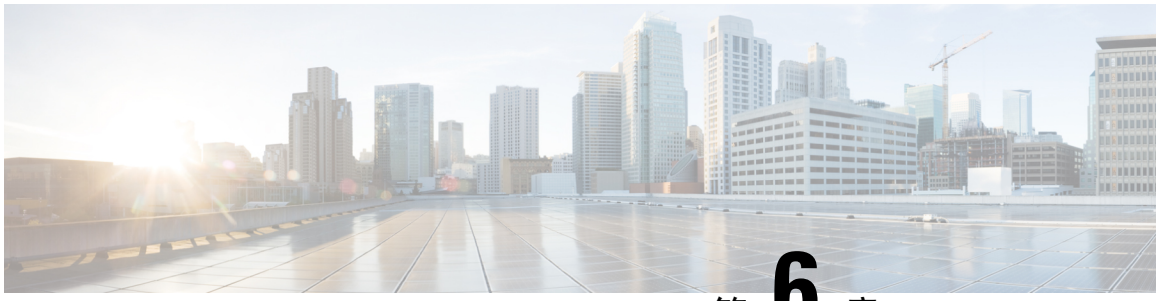
部署配置更改；请参阅部署配置更改，第 25 页。



第 II 部分

Snort 3 中的高级网络分析

- Snort 3 网络分析策略入门，第 71 页



第 6 章

Snort 3 网络分析策略入门

本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。它也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。

- 网络分析策略概览， 第 71 页
- 管理网络分析策略， 第 72 页
- 网络分析策略的 Snort 3 定义和术语， 第 72 页
- 网络分析和入侵策略的必备条件， 第 74 页
- 为 Snort 3 自定义网络分析策略的创建， 第 74 页
- 网络分析策略设置和缓存的更改， 第 101 页

网络分析策略概览

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智能匹配和 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处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 智能小组 (Talos) 针对安全性和连接的特定平衡专门进行过调整。您也可以用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。）

管理网络分析策略

在工具栏中的用户名下，系统会显示可用域的树。要切换域，请选择要访问的域。

过程

步骤 1 选择以下路径之一来访问网络分析策略。

- **策略** > **访问控制标题** > **访问控制**，然后点击**网络分析策略**
- **策略** > **访问控制标题** > **入侵**，然后点击**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：

- 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，请参阅 *Cisco Secure Firewall Management Center* 设备配置指南中 为 *Snort 2* 自定义网络分析策略创建 章节。
  - 对于 Snort 3 版本，请参阅 为 Snort 3 自定义网络分析策略的创建 ，第 74 页。

- 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** 图标；请参阅 *Cisco Secure Firewall Management Center* 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 自定义网络分析策略的创建，第 74 页中的绑定检查器。
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 自定义网络分析策略的创建，第 74 页中的单例检查器。
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。 有关详细信息，请参阅为 Snort 3 自定义网络分析策略的创建，第 74 页中的多例检查器。
架构 (Schema)	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。 有关详细信息，请参阅自定义网络分析策略，第 82 页。
示例文件	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。 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。 有关详细信息，请参阅自定义网络分析策略，第 82 页。

术语	说明
完整配置	您可以在一个文件中下载整个检查器配置。 此文件中提供有关检查器配置的所有信息。 完整配置是默认配置（由思科 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。 有关详细信息，请参阅自定义网络分析策略，第 82 页。
覆盖的配置	在网络分析策略页面的 **Snort 3 版本**中： • 在**操作 (Actions)** > **上传 (Actions)** 下，您可以点击**覆盖配置 (Overridden Configuration)** 以上传包含覆盖配置的 JSON 文件。 • 在 **操作 (Actions)** > **下载 (Download)** 下，您可以点击**覆盖配置 (Overridden Configuration)** 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。 有关详细信息，请参阅自定义网络分析策略，第 82 页。

相关主题

为 Snort 3 自定义网络分析策略的创建，第 74 页
自定义网络分析策略，第 82 页
网络分析策略映射，第 79 页

网络分析和入侵策略的必备条件

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

您必须是管理员用户，才能管理网络分析、入侵策略和执行迁移任务。

为 Snort 3 自定义网络分析策略的创建

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， 防火墙管理中心 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 防火墙管理中心 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 防火墙管理中心 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**下供使用。

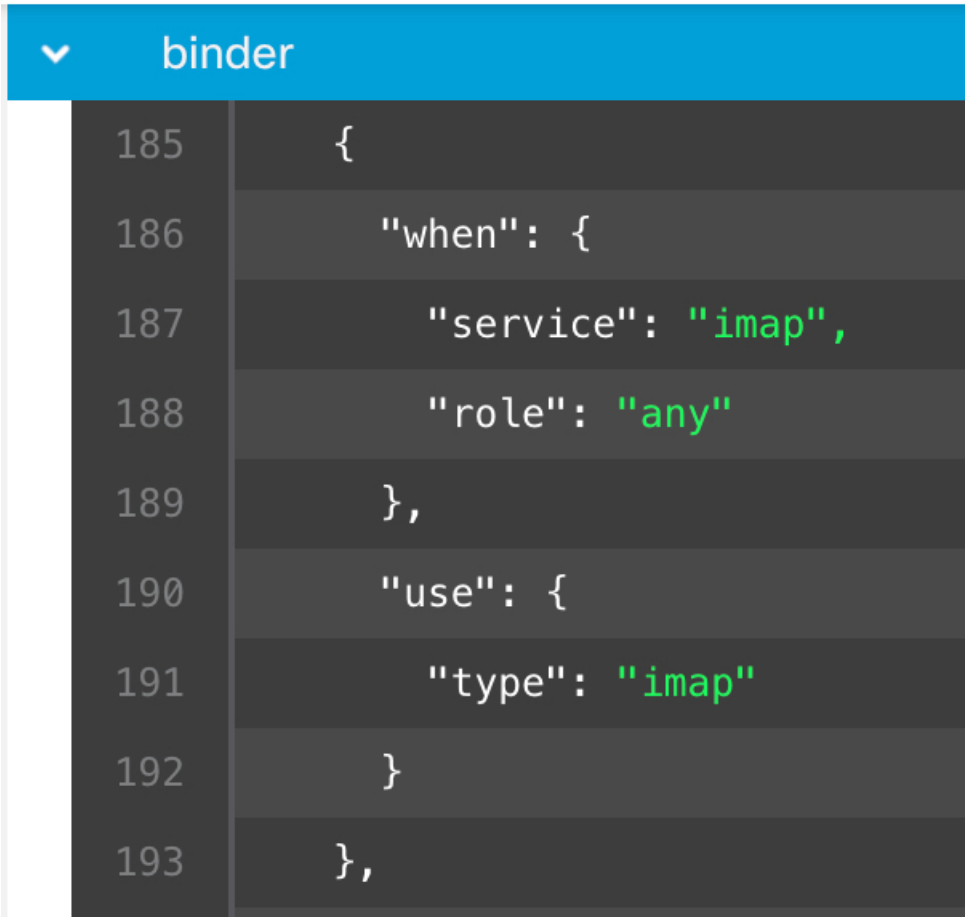
绑定检查器

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。



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"
            }
         }
      ]
   }
}
```

通用工业协议安全

通用工业协议 (CIP) 安全是 CIP 的一组扩展，可确保设备的安全运行。它还提供 CIP 网络上不同节点之间的故障安全通信。

CIP 安全协议包括两个主要组成部分：

- CIP 安全网段 - 用于转发打开消息，为后续安全会话交换安全参数。
- CIP 安全消息 - 用于交换实际安全信息。

CIP 检测器检测并识别：

- CIP 即服务和客户端
- 负载，例如 CIP Read、CIP Admin、CIP Infrastructure 和 CIP Write

  CIP 检查器可以解析 CIP 数据段并检测 Forward Open 请求中的 CIP 安全数据段。

要测试 CIP 安全功能，必须启用 CIP 检测器。请参阅检测和阻止 CIP 数据包中的安全分段，第 79 页。

检测和阻止 CIP 数据包中的安全分段

使用案例：要检测和阻止 CIP 安全分段，同时允许其他 CIP 数据包，请执行以下操作：

- 创建名为 **cip_safety**的自定义网络分析策略。
- 在访问控制策略中创建访问控制规则，以阻止 CIP 安全并允许所有其他数据包。

要测试 CIP 安全功能，请在管理中心启用 CIP 检查器并将其分配给访问控制策略。

过程

步骤 1 转至**策略** > **访问控制标题** > **入侵** > **网络分析策略**。

步骤 2 点击您创建的网络分析策略 **cip_safety** 的 **Snort 3 版本** 。

步骤 3 在 **检查器**下，点击 **cip** 将其展开。

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 4 在右侧列的 **覆盖配置** 下，点击 **编辑检查器** 图标，并将 **cip** 中的“已启用”字段从 false（默认）更改为 true。

步骤 5 点击**确定 (OK)**。

步骤 6 点击**保存 (Save)**。

步骤 7 要将 **cip** 检查器分配给访问控制策略，请依次选择 **策略 访问控制 编辑** ，然后从数据包流行末尾的更多 下拉箭头中选择 高级设置 选项。**策略** > **访问控制标题** > **访问控制**

步骤 8 点击 **网络分析和入侵策略** 旁边的 **编辑** ()。

步骤 9 在 **网络分析和入侵策略** 窗口中，从 **默认网络分析策略** 下拉列表中选择您创建的访问控制策略 **cip_safety** 。

CIP 检查器现已在管理中心启用，您可以创建自定义访问控制规则来阻止 CIP 安全并允许所有其他 CIP 数据包。

步骤 10 发送包含 CIP 安全数据包流的实时流量后，请转至 **连接事件** 以验证负载是否为包含此程序中所述检测和阻止使用案例的 CIP 安全数据包日志的预期负载。**CIP** 被检测为应用协议和客户端（请参阅 **应用协议** 和 **客户端** 字段），并且 **CIP 安全** 显示在 **Web 应用** 字段下。

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

过程

步骤 1 转至策略 > 访问控制标题 > 入侵 > 网络分析策略。

步骤 2 点击**NAP 映射 (NAP Mapping)**。

步骤 3 展开**查看映射 (View Mappings)** 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 (OK)**。

创建网络分析策略

所有 防火墙管理中心 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。

过程

步骤 1 转至策略 > 访问控制标题 > 入侵 > 网络分析策略。

步骤 2 点击**创建策略 (Create Policy)**。

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

步骤 4 选择**基本策略**，然后点击**保存**。

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。

过程

步骤 1 转至策略 > 访问控制标题 > 入侵 > 网络分析策略。

步骤 2 点击**编辑 (Edit)** 以更改名称、说明、检测模式或基本策略。

注意
检测模式弃用： 从管理中心 7.4.0 开始，对于网络分析策略 (NAP)，**检测** 检查模式已弃用，并将在即将推出的版本中删除。

检测 模式旨在用作测试模式，以便您可以启用检测并查看它们在网络中的行为，然后再将其设置为丢弃流量，即显示将被丢弃的流量。

此行为已得到改进，其中所有检查器丢弃都由规则状态控制，并且您可以设置每个丢弃以生成事件。这样做是为了在配置规则状态以丢弃流量之前对其进行测试。由于我们现在可以对 Snort 3 中的流量丢弃进行精细控制，因此 **检测** 模式只会增加产品的复杂性，不需要，因此检测模式已弃用。

如果将**检测**模式下的 NAP 更改为**预防**，则处理入侵事件流量并具有结果 “会被丢弃”的 NAP 现在将为“已丢弃”，相应的流量将丢弃来自这些事件的流量。这适用于 GID 不是 1 或 3 的规则。GID 1 和 3 是文本/编译规则（通常由 Talos 提供或从您的自定义/导入规则中提供），所有其他 GID 都是异常检测。这些是在网络中触发的比较少见的规则。更改为 **预防** 模式不太可能对流量产生任何影响。您只需禁用适用于已丢弃流量的入侵规则，并将其设置为仅生成或禁用。

我们建议您选择 **预防** 作为检测模式，但如果您选择 **预防**，则无法恢复到 **检测** 模式。

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。

过程

步骤 1 转至**策略** > **访问控制标题** > **入侵** > **网络分析策略**。

步骤 2 转至网络分析策略的 **Snort 3 版本** 。

步骤 3 在**搜索 (Search)** 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 90 页
查看具有覆盖的检查器列表 ， 第 87 页
网络分析策略的 Snort 3 定义和术语 ， 第 72 页
自定义网络分析策略 ， 第 82 页
对检查器进行内联编辑以覆盖配置 ， 第 85 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。

过程

步骤 1 转至**策略** > **访问控制标题** > **入侵** > **网络分析策略**。

步骤 2 转至网络分析策略的 **Snort 3 版本** 。

步骤 3 在 **检查器** 下，展开要复制其配置的所需检查器。

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 4 点击**复制到剪贴板 (Copy to clipboard)** 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 5 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 82 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。

过程

步骤 1 转至**策略** > **访问控制标题** > **入侵** > **网络分析策略**。

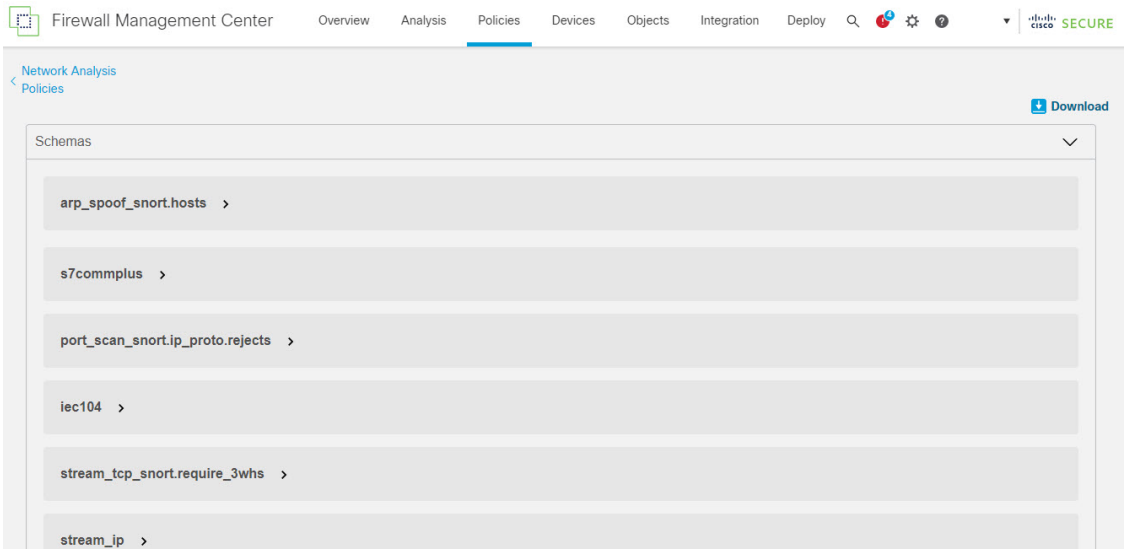
步骤 2 转至网络分析策略的 **Snort 3 版本** 。

步骤 3 点击 **操作** 下拉菜单。

系统将显示以下选项：

- 查看架构
- 下载方案 / 下载示例文件 / 模板
- 下载完整配置
- 下载覆盖配置文件
- 上传覆盖配置文件

步骤 4 点击**查看方案 (View Schema)** 可直接在浏览器中打开方案文件。



步骤 5 您可以根据需要来下载方案文件、示例文件 / 模板、完整配置或覆盖配置。

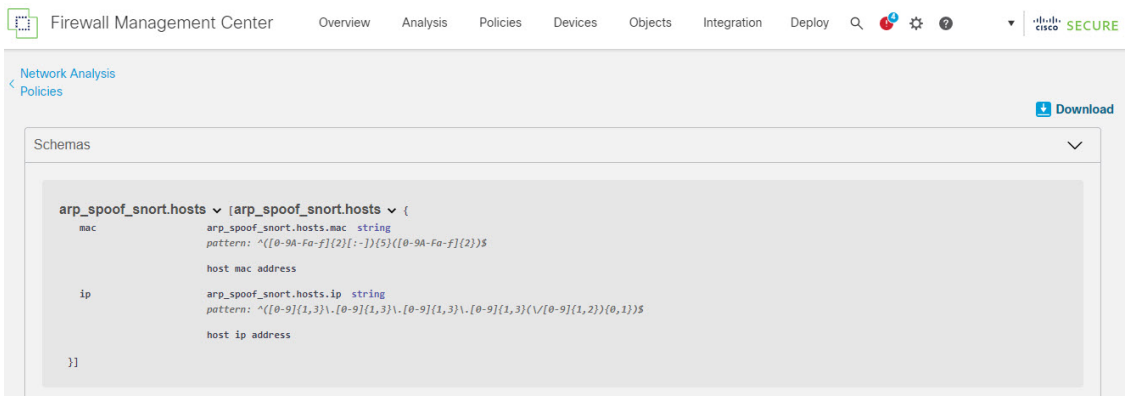
通过这些选项，您可以了解允许的值、范围和模式、现有和默认检查器配置以及覆盖的检查器配置。

a) 点击 **下载方案** 以下载架构文件。

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。

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})$`
- **ip** – 模式：`^([0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}()/[0-9]{1,2}){0,1})$`



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 **下载示例文件/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。

c) 点击 **下载完整配置** 以将整个检查器配置下载到一个 JSON 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 **下载覆盖的配置** 以下载已覆盖的检查器配置。

步骤 6 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 防火墙管理中心上对检查器进行内联编辑。请参阅 *Cisco Secure Firewall Management Center Snort 3* 配置指南的 **网络分析策略入门** 一章中的 **对检查器进行内联编辑以覆盖配置** 主题。
- 继续按照当前程序使用**操作 (Actions)** 下拉菜单上传覆盖的配置文件。

如果您选择直接在 防火墙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 (Inspectors)** 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 (Copy to clipboard)** 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 (Sample File / Template)** 来了解如何覆盖默认配置。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。

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 *Cisco Secure Firewall Management Center Snort 3* 配置指南中 **Snort 3 的自定义网络分析策略创建** 主题中的 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。

步骤 7 从 **操作** 下拉餐单，选择上传覆盖配置 以上传包含覆盖配置的 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 (Merge inspector overrides)** - 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 (Replace inspector overrides)** - 删除所有之前的覆盖并替换为上传文件中的新内容。

  注意
  选择此选项将删除所有以前的覆盖。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，修复错误并重新上传文件。

步骤 8 在 **上传覆盖的配置文件** 弹出窗口中，点击 **导入** 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图标，表示它是一个覆盖的检查器。

此外，检查器下的**覆盖配置 (Overridden Configuration)** 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 (Show Overrides Only)** 复选框查看所有已覆盖的检查器。

注释
确保始终下载覆盖配置，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 9 （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 87 页
查看具有覆盖的检查器列表，第 87 页
在网络分析策略页面上搜索检查器，第 81 页
复制检查器配置，第 82 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 (Actions)** 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 82 页。

过程

步骤 1 转至**策略** > **访问控制标题** > **入侵** > **网络分析策略**。

步骤 2 转至网络分析策略的 **Snort 3 版本** 。

步骤 3 在 **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 4 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 5 点击**确定**。

如果根据 JSON 标准存在任何错误，则会显示错误消息。

步骤 6 点击**保存**保存所做的更改。

如果更改符合 OpenAPI 架构规范，则 防火墙管理中心 允许您保存配置，否则，系统将显示**保存覆盖配置时出错 (Error saving overridden configuration)** 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 82 页
在内联编辑期间恢复未保存的更改 ， 第 86 页
将覆盖的配置恢复为默认配置 ， 第 87 页
自定义网络分析策略配置示例 ， 第 90 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，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。

过程

步骤 1 转至**策略 > 访问控制标题 > 入侵 > 网络分析策略**。

步骤 2 转至网络分析策略的 **Snort 3 版本** 。

步骤 3 在 **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 4 在右侧列的**覆盖配置 (Overridden Configuration)** 下，点击**叉号** ✕ 图标可恢复检查器的任何未保存的更改。

或者，点击**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 87 页
对检查器进行内联编辑以覆盖配置，第 85 页

查看具有覆盖的检查器列表

您可以查看所有覆盖的检查器的列表。

过程

步骤 1 转至**策略** > **访问控制标题** > **入侵** > **网络分析策略**。

步骤 2 转至网络分析策略的 **Snort 3 版本** 。

步骤 3 选中搜索栏旁的 **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图标，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 81 页
对检查器进行内联编辑以覆盖配置，第 85 页
自定义网络分析策略，第 82 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。

过程

步骤 1 转至**策略** > **访问控制标题** > **入侵** > **网络分析策略**。

步骤 2 转至网络分析策略的 **Snort 3 版本** 。

步骤 3 在 **检查器** 下，展开要恢复覆盖配置所需的检查器。

被覆盖的检查器在其名称旁边显示为橙色图标。

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 (Overridden Configuration)** 下，点击**恢复默认配置 (Revert to default configuration)**（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 4 点击**恢复 (Revert)** 以确认决策。

步骤 5 点击**保存**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** ✕ 图标。

相关主题

在内联编辑期间恢复未保存的更改 ， 第 86 页
自定义网络分析策略 ， 第 82 页
对检查器进行内联编辑以覆盖配置 ， 第 85 页
自定义网络分析策略配置示例 ， 第 90 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 防火墙管理中心 的版本可以管理多个 防火墙威胁防御 版本。
- 当前版本的 防火墙管理中心 支持不适用于以前版本的 防火墙威胁防御 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 防火墙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 防火墙威胁防御，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。

过程

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 点击**确定**。

步骤 4 点击**保存**保存所做的更改。

或者，您也可以使用**操作 (Actions)** 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 (Merge inspector overrides)** - 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 (Replace inspector overrides)** - 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 (Upload Overridden Configuration File)** 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 点击**确定 (OK)**。

步骤 10 点击**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 点击**添加规则**。

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 点击**添加 (Add)**。

步骤 16 **部署：** 在 防火墙管理中心 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 点击**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，请点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防火墙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：

- 直接在防火墙管理中心上对检查器进行内联编辑。请参阅对检查器进行内联编辑以覆盖配置，第 85 页。
- 使用**操作 (Actions)** 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 82 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 (Actions)** 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": []
  },
  "iec104": {
    "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（**normalizer** 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 **name** 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应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 防火墙威胁防御上，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"
      }
    }
  ]
}
```

不正确方法：

```
{
  "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 (Replace inspector overrides)**选项。

```
{
}
```

相关主题

网络分析策略的 Snort 3 定义和术语，第 72 页
网络分析策略映射，第 79 页
为 Snort 3 自定义网络分析策略的创建，第 74 页
在网络分析策略页面上搜索检查器，第 81 页
复制检查器配置，第 82 页
自定义网络分析策略，第 82 页
查看具有覆盖的检查器列表，第 87 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其，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。

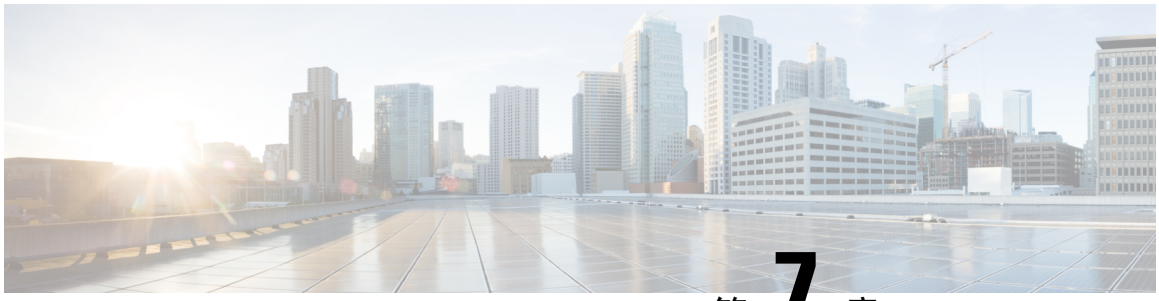
系统为每个用户缓存一条网络分析策略。在编辑网络分析策略时，如果您选择任何菜单或指向另一页的其他路径，即使您离开此页，更改也会保留在系统缓存中。



第 III 部分

Snort 3 的加密可视性引擎

- 加密可视性引擎， 第 105 页



第 7 章

加密可视性引擎

加密可视性引擎 (EVE) 用于识别使用 TLS 加密的客户端应用和进程。它支持可视性，并允许管理员在其环境中采取行动并实施策略。EVE 技术还可用于识别和阻止恶意软件。

- 加密可视性引擎概述， 第 105 页
- EVE 工作原理， 第 106 页
- 危害事件表现， 第 107 页
- EVE 中的 QUIC 指纹识别， 第 107 页
- 配置 EVE， 第 107 页
- 配置 EVE 例外规则， 第 110 页
- 事件扩充， 第 111 页

加密可视性引擎概述

加密可视性引擎 (EVE)用于提供对加密会话的更多可视性，而无需对其进行解密。对 TLS 连接的见解源自思科的开源库，该库包含在思科的漏洞数据库 (VDB) 中。库指纹并分析传入的加密会话，并将其与一组已知指纹进行匹配。已知指纹的数据库在思科 VDB 中也可用。

注释 只有运行 Snort 3 的 防火墙管理中心管理的设备才支持加密可视性引擎功能。Snort 2 设备和防火墙设备管理器受管设备不支持此功能。

EVE 的一些重要功能如下：

- 您可以使用从 EVE 派生的信息对流量执行访问控制策略操作。
- Cisco Secure Firewall 中包含的 VDB 能够以高置信度值将应用分配给 EVE 检测到的某些进程。或者，您可以创建自定义应用检测器，以便：
  - 将 EVE 检测到的进程映射到用户定义的新应用。
  - 覆盖用于将应用分配给 EVE 检测到的进程的进程置信度的内置值。

  请参阅 Cisco Secure Firewall Management Center 设备配置指南的**应用检测**一章中的**配置自定义应用检测器**和**指定 EVE 进程分配**部分。

- EVE 可以检测在加密流量中创建客户端 Hello 数据包的客户端的操作系统类型和版本。
- EVE 也支持快速 UDP 互联网连接 (QUIC) 流量的指纹识别和分析。来自客户端 Hello 数据包的服务器名称显示在 **连接事件** 页面的 URL 字段中。

注意 要在 防火墙管理中心上使用 EVE，您的设备上必须具有有效的 IPS 许可证。在没有 IPS 许可证的情况下，策略会显示警告，并且不允许部署。

注释

- EVE 可以检测 SSL 会话的操作系统类型和版本。操作系统的正常使用（例如运行应用、软件包管理软件等）可以触发操作系统检测。要查看客户端操作系统检测，除了启用 EVE 切换按钮，您还必须在 **策略 (Policies)** > **网络发现 (Network Discovery)** 下启用 **主机 (Hosts)** 。要查看主机 IP 地址上可能的操作系统的列表，请点击 **分析** > **主机标题** > **网络映射**，然后选择所需的主机。
- 为访问控制策略启用 EVE 后，确保已为该策略中的访问控制规则开启日志记录，以便在满足任何特定规则条件时，能在 EVE 控制面板上显示预期结果。有关如何开启日志记录的详细信息，请参阅创建和编辑访问控制规则。
- EVE 无法提供对封装流量的可视性或洞察力。

相关链接

配置 EVE，第 107 页

配置 EVE 例外规则，第 110 页

EVE 工作原理

加密可视性引擎 (EVE) 检查 TLS 握手的客户端 Hello 部分，以识别客户端进程。客户端 Hello 是发送到服务器的初始数据包。这可以很好地指示主机上的客户端进程。此指纹与其他数据（例如目的 IP 地址）相结合，为 EVE 的应用识别提供基础。通过识别 TLS 会话建立中的特定应用指纹，系统可以识别客户端进程并采取适当的操作（允许/阻止）。

EVE 可以识别 5,000 多个客户端进程。系统将许多此类进程映射到客户端应用，以用作访问控制规则中的条件。这使得系统能够在不启用 TLS 解密的情况下识别和控制这些应用。通过使用已知恶意进程的指纹，EVE 技术还可用于识别和阻止加密的恶意流量，而无需出站解密。

通过机器学习 (ML) 技术，思科每天要处理超过 10 亿个 TLS 指纹和超过 10000 个恶意软件样本，以创建和更新 EVE 指纹。然后，使用思科漏洞数据库 (VDB) 软件包将这些更新交付给客户。

如果 EVE 无法识别某个指纹，它会识别客户端应用，并使用目标详细信息（例如 IP 地址、端口和服务器名称）估算第一个数据流的威胁评分。此时，指纹的状态已随机化，可以在调试日志中查看状态。对于具有相同指纹的后续流，EVE 会跳过重新分析并将指纹状态标记为未标记。如果您打算基于 EVE 的“低”或“非常低”分数阈值阻止流量，应阻止初始流。但是，一旦应用的指纹被缓存，将允许以后的流。

危害事件表现

用于加密可视性引擎检测的主机危害表现 (IoC) 事件允许您检查恶意软件置信度非常高的连接事件，如 EVE 所报告的那样。使用恶意客户端从主机生成的加密会话会触发 IoC 事件。您可以查看恶意主机的 IP 地址、MAC 地址和操作系统信息等信息，以及可疑活动的时间戳。

如连接事件中所示，加密可视性威胁置信度评分为“非常高”的会话将 IoC 事件类型化。您必须从**策略** > **网络发现**启用 **主机** 。在 防火墙管理中心中，您可以从以下位置查看 IoC 事件的存在情况：

- **分析** > **危害表现**。**分析** > **主机标题** > **“危害指标”**
- **分析** > **主机标题** > **网络映射** >选择必须检查的主机。

  您可以在**连接事件 (Connection Events)** 页面查看产生该 IoC 的会话的进程信息。点击**分析** > **连接** > **事件**以访问**统一事件**页面。请注意，您必须从**“连接事件表视图”**选项卡中手动选择“加密可见性”字段和“IoC”字段。

EVE 中的 QUIC 指纹识别

Snort 可以根据 EVE 识别快速 UDP Internet 连接（QUIC 会话）中的客户端应用程序。QUIC 指纹识别可以：

- 通过 QUIC 检测应用而不启用解密。
- 在不启用解密的情况下识别恶意软件。
- 检测服务应用。您可以根据通过 QUIC 协议检测到的服务分配访问控制规则。

配置 EVE

过程

步骤 1 选择**策略** > **访问控制标题** > **访问控制**。

步骤 2 点击要编辑的访问控制策略旁边的 **编辑** (✎) 。

步骤 3 从数据包流末尾的 **更多** 下拉箭头中选择 **高级设置** 。

步骤 4 点击**加密可视性引擎 (Encrypted Visibility Engine)**旁边的 **编辑** (✎)。

步骤 5 在**加密可视性引擎 (Encrypted Visibility Engine)** 页面中，启用**加密可视性引擎 (EVE) (Encrypted Visibility Engine [EVE])** 切换按钮。

步骤 6 **使用 EVE 进行应用检测 (Use EVE for Application Detection)** - 默认情况下启用此切换开关，这意味着允许 EVE 将客户端应用分配给进程。

将在连接事件或统一事件的**加密可视性指纹 (Encrypted Visibility Fingerprint)** 列标题中添加 EVE 的指纹信息。要对收集的 EVE 数据进行进一步分析，可以右键点击指纹信息以打开下拉菜单。在菜单中，点击**查看加密可视性引擎进程分析 (View Encrypted Visibility Engine Process Analysis)** 以转至 Cisco Secure Firewall 应用检测器站点，然后查看详细信息，例如指纹、VDB 版本等。系统将显示具有相同指纹字符串的不同行，以及与其关联的潜在进程名称及其普遍性。普遍性表示与数据收集系统中的特定指纹关联的进程的频率。您可以选择进程名称，然后点击 **提交请求 (Submit Request)**，以提供有关 EVE 进程检测中任何差异的反馈。例如，如果检测到的进程名称与正在发送的流量不匹配，或者根本没有检测到特定指纹的进程名称，则可以提交请求。

具有非思科电子邮件地址的用户当前无法访问 Cisco Secure Firewall 应用检测器 (Secure Firewall Application Detectors) 页面上查看其他详细信息的权限。

如果禁用 **使用 EVE 进行应用检测** 切换按钮：

- AppID 识别的客户端将分配给进程，您可以看到 EVE 进程和分数，但没有将 EVE 检测到的进程映射到应用，也不会执行任何操作。您可以在**连接事件 (Connection Events)** 或**统一事件 (Unified Events)** 下查看事件的详细信息。要查看连接事件的差异（有和没有应用分配），请参阅**客户端应用 (Client Application)** 列标题。
- 连接事件或统一事件中的 **已加密可视性指纹 (Encrypted Visibility Fingerprint)** 字段为空。

步骤 7 启用**基于威胁置信度阻止恶意软件进程 (Block Malware Processes Based on Threat Confidence Level)** 切换按钮，以根据 EVE 的威胁置信度阻止前缀为 *Malware_* 的恶意客户端进程。

默认阻止阈值为 99%，这意味着：

- 如果 EVE 检测到流量为恶意软件且置信度为 99% 或更高，则流量会被阻止。
- 如果 EVE 检测到流量为恶意软件且其置信度低于 99%，则 EVE 不会采取任何措施。

注释
如果 EVE 已阻止流量，则在**连接事件 (Connection Events)** 页面中，**原因 (Reason)** 列标题会显示**加密可视性阻止 (Encrypted Visiblity Block)**。

步骤 8 使用滑块根据 EVE 的威胁置信度调整阻止阈值，范围从 **非常低** 到 **非常高**。

步骤 9 要进行进一步精细控制，请启用**高级模式 (Advanced Mode)** 切换按钮。现在，您可以为阻止流量分配特定的 EVE 威胁置信度。默认阻止阈值为 99%。

注意
为了获得最佳性能，我们建议不要将阈值设置为低于 50%。

步骤 10 点击**确定 (OK)**。

步骤 11 点击**保存 (Save)**。

下一步做什么

部署配置更改。

查看 加密可视性引擎事件

启用**加密可视性引擎 (Encrypted Visibility Engine)** 并部署访问控制策略后，您可以开始通过系统发送实时流量。**您可以在“连接事件”**页面或**“统一事件”**页面查看已记录的连接事件。

执行此过程以访问防火墙管理中心中的连接事件。

过程

步骤 1 请点击 **分析** > **连接** > **事件**。

步骤 2 点击**连接事件的表视图 (Table View of Connection Events)** 选项卡。

您也可以在**统一事件**页面中查看连接事件。点击**分析** > **统一事件**以访问**统一事件**页面。

加密可视性引擎可以识别发起连接的客户端进程和客户端中的操作系统，并指示该进程是否包含恶意软件。

在**连接事件**页面上，您必须显式启用为 加密可视性引擎添加的这些列：

- **加密可视性进程名称**
- **加密可视性进程置信度分数**
- **加密可视性威胁置信度**
- **加密可视性威胁置信度分数**
- **检测类型**

有关这些字段的信息，请参阅《Cisco Secure Firewall Management Center 管理指南》中的 连接和安全相关的连接事件字段。

注释
在**连接事件**页面上，如果进程被分配了应用程序，**检测类型**列会显示**加密可视性引擎**，表明客户端应用程序是由 加密可视性引擎识别的。如果没有为进程名称分配应用，**检测类型**列会显示 **AppID**，表示识别客户端应用的引擎是 AppID。

查看 EVE 控制面板

您可以在以下控制面板中查看 EVE 分析信息：

开始之前

- 在访问控制策略中，必须在 **高级设置** 下启用 **加密可视性引擎（EVE）**。

过程

步骤 1 转至概述 > 控制 > 面板。

步骤 2 在摘要控制面板 (Summary Dashboard) 窗口中，点击交换机控制面板链接，然后从下拉框中选择应用统计信息 (Application Statistics)。

步骤 3 选择 加密可视性引擎 (Encrypted Visibility Engine) 选项卡以查看以下两个控制面板：

- 排名靠前的加密可视化引擎发现进程 - 显示网络中使用的排名靠前的 TLS 进程名称和连接计数。您可以点击表中的进程名称，查看 连接事件 页面的过滤视图，该视图按进程名称进行过滤。
- 按加密可视化引擎威胁置信度的连接 - 按恶意软件置信度级别（非常高，非常低等）显示连接。您可以点击表中的 威胁 置信度级别，查看 ”连接事件“ 页面的过滤视图，该视图按置信度级别进行过滤。

配置 EVE 例外规则

您可以创建加密可视性引擎 (EVE) 例外规则来绕过 EVE 的阻止操作，从而确保可信连接和服务的连续性。您可以在例外规则中添加进程名称和目标 IP 地址等属性。例如，您可能希望绕过受信任网络的 EVE 阻止判定。根据威胁置信度，绕过网络中的所有连接都免于执行 EVE 阻止判定。

过程

步骤 1 选择策略 > 访问控制标题 > 访问控制。

步骤 2 点击要编辑的访问控制策略旁边的 编辑 (✎) 。

步骤 3 从数据包流行末尾的更多下拉箭头选择高级设置 (Advanced Settings)。

步骤 4 在加密可视性引擎 (EVE) (Encrypted Visibility Engine [EVE]) 旁边，点击 编辑 (✎)。

步骤 5 在加密可视性引擎 (Encrypted Visibility Engine) 页面中，点击加密可视性引擎 (EVE) (Encrypted Visibility Engine [EVE]) 切换按钮以启用 EVE。

步骤 6 启用根据 EVE 分数阻止流量 (Block Traffic Based on EVE Score) 开关来根据 EVE 的威胁置信度来阻止流量。

步骤 7 点击添加例外规则 (Add Exception Rule) 并添加以下一个或多个属性。

a) 在进程名称 (Process Name) 选项卡下，输入 EVE 识别的进程名称，然后点击窗口右侧的添加到进程 (Add to Process)。

可以将多个进程名称添加到同一例外规则。基于进程名称的 EVE 例外列表仅适用于 EVE 识别的进程名称，这些进程名称区分大小写和空格。

b) 在网络对象 (Network Objects) 选项卡下，执行以下操作之一：

- 从列表中选择一个或多个 IP 地址，并将其添加到**选定网络 (Selected Networks)** 列表中。
- 在**选定网络 (Selected Networks)** 下，手动输入 IP 地址，然后点击 **+** 以将其添加到选定网络列表中。

c) （可选）在所有选项卡上提供的**注释 (Comment)** 字段中，您可以输入将所需属性添加到 EVE 例外规则的原因。

步骤 8 点击**保存**保存 EVE 例外规则。

步骤 9 在设备上保存并部署访问控制策略。



注释 当连接匹配例外规则时，它会绕过EVE的阻止判定。您可以在**连接事件**或**统一事件**页面中查看EVE的操作。**原因 (Reason)** 列标题显示 **EVE 已豁免 (EVE Exempted)**，用于识别此类绕过 EVE 的流量。

从统一事件添加例外规则

使用**统一事件**页面为被 EVE 阻止的连接添加例外规则。

开始之前

仅 Threat Defense 版本 7.6.0 及更高版本支持例外列表。

过程

步骤 1 请点击 **分析** > **统一事件**。

步骤 2 在**原因**为“**加密可见性块**”的原因列中，点击单元格内的**省略号**(⋮)图标。

步骤 3 从下拉列表中选择**添加 EVE 例外规则 (Add EVE Exception Rule)**。

步骤 4 在显示的**加密可视性引擎 (Encrypted Visibility Engine)** 窗口中，规则会自动添加到例外列表的底部。您可以在保存和部署配置之前查看并更改添加的规则。

事件扩充

Talos 分类法和加密可视性引擎 (EVE) 可丰富 MITRE ATT&CK 的情景。Talos 和 EVE 扩充都使用 Talos 分类法进行传达。启用 EVE 时，EVE 扩充有效。有关启用 EVE 的详细信息，请参阅配置 EVE，第 107 页。

在**连接事件 (Connection Events)** 页面上，可以查看作为扩充事件内容的一部分添加的以下列标题。您必须明确启用这些列。

- **MITRE ATT&CK**
- **其他扩充**

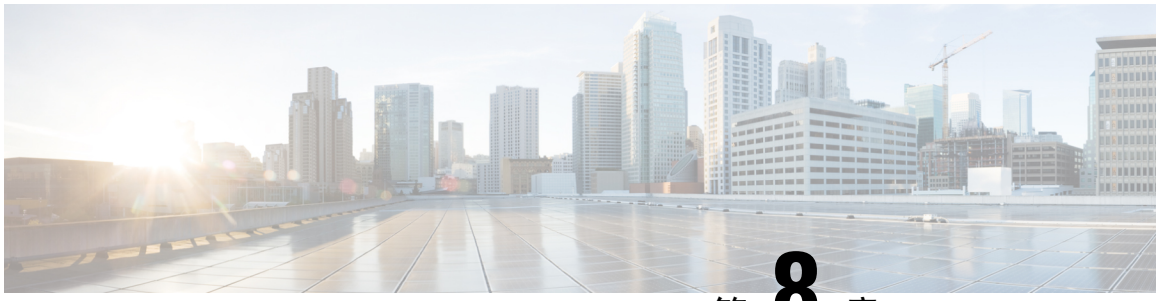
有关这些字段的信息，请参阅 《Cisco Secure Firewall Management Center 管理指南》中的“连接和中的“安全相关连接 事 件字段” 。



第 IV 部分

Snort 3 的大象流检测

- 大象流检测， 第 115 页



第 8 章

大象流检测

大象流非常大（以总字节数为单位），由 TCP（或其他协议）设置的连续流通过网络链路测量。默认情况下，大象流是速率大于每 10 秒 1GB 的流。它们可能会在 Snort 核心中造成性能威胁。大象流并不多，但它们可以在一段时间内占总带宽的不成比例。它们可能导致问题，例如CPU 占用、丢包等。

从 防火墙管理中心 7.2.0 开始（仅限 Snort 3 设备），您可以使用象流检测功能对象流进行监测和补救，这有助于减少系统压力并解决上述问题。

- 关于大象流检测和补救，第 115 页
- 从智能应用绕行升级大象流，第 115 页
- 配置大象流，第 116 页

关于大象流检测和补救

您可以使用大象流检测功能来检测和补救大象流。可应用以下补救操作：

- **绕过大象流 (Bypass elephant flow)** - 您可以配置大象流以绕过 Snort 检测。如已配置，则 Snort 不会收到来自该流的任何数据包。
- **限制大象流 (Throttle elephant flow)** – 您可以对流应用速率限制并继续检查流。流速会以动态方式进行计算，流速会降低 10%。Snort 会将判定（流量减少 10% 的 QoS 流）发送到防火墙引擎。如果选择绕过所有应用，包括未识别的应用，您将无法为任何流配置限制操作（速率限制）。

注释 要使大象流检测正常工作，Snort 3 必须是检测引擎。

从智能应用绕行升级大象流

从 7.2.0 版开始，在 Snort 3 设备中已弃用智能应用绕行 (IAB)。

对于运行 7.2.0 或更高版本的设备，您必须在 AC 策略（高级设置选项卡）的**大象流设置 (Elephant Flow Settings)** 部分下配置象流设置。

在升级到 7.2.0（或更高版本）后，如果您使用的是 Snort 3 设备，则将从**大象流设置**部分而不是从**智能应用绕行设置**部分中挑选和部署大象流配置设置，这样，如果您没有迁移到大象流配置设置，那么您的设备在下次部署时将失去大象流配置。

下表显示了可应用于运行 Snort 3 或 Snort 2 引擎的版本 7.2.0 或更高版本以及版本 7.1.0 或更早版本的 IAB 或大象流配置。

防火墙管理中心	防火墙威胁防御	大象流或 IAB 配置
防火墙管理中心 7.0 或 7.1	Snort 2 设备	来自 IAB 的配置将适用。
	Snort 3 设备	来自 IAB 的配置将适用。
防火墙管理中心 7.2.0	Snort 2 设备	来自 IAB 的配置将适用。
	Snort 3 设备（7.1.0 及更早版本）	来自 IAB 的配置将适用。
	Snort 3 设备（7.2.0 及更高版本）	大象流中的配置将适用。

配置大象流

您可以配置大象流以便对大象流执行操作，这有助于解决系统强制、高 CPU 使用率、丢包等问题。

注意 大象流检测不适用于不通过 Snort 处理的预过滤流、受信任流或快速转发流。由于大象流由 Snort 检测，因此大象流检测不适用于加密流量。

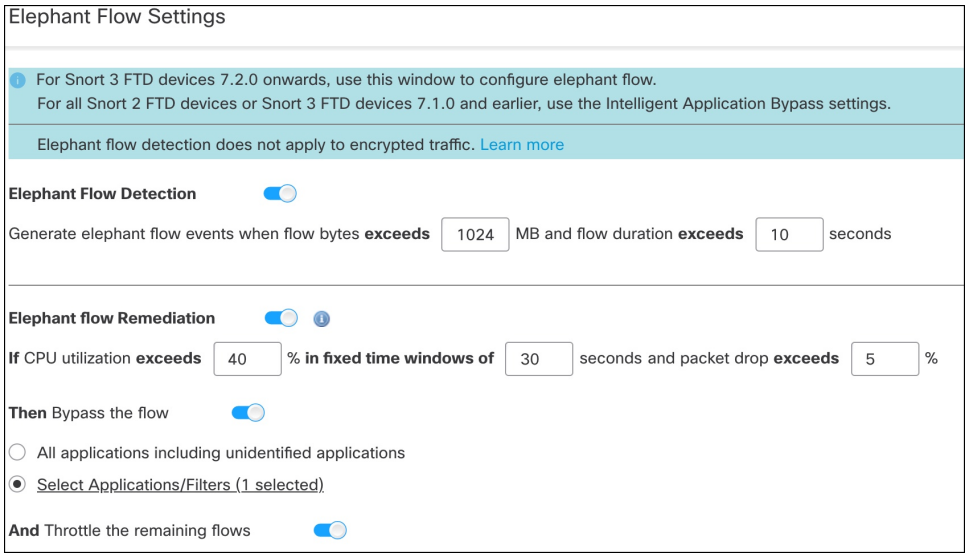
过程

步骤 1 在访问控制策略编辑器中，从数据包流行末尾的 **更多** 下拉箭头中点击 **高级设置** 。然后，点击 **大象流设置**旁边的 **编辑** (✎) 。

如果显示**视图**(👁)，则表明设置继承自祖先策略，或者您没有修改设置的权限。如果配置已解锁，请取消选中**从基本策略继承**以启用编辑。

图 2: 配置大象流检测

图 3: 配置大象流检测



步骤 2 默认情况下，**大象流检测 (Elephant Flow Detection)** 切换按钮处于启用状态。您可以配置流字节和流持续时间的值。当它们超过配置的值时，就会生成大象流事件。

步骤 3 要补救大象流，请启用 **大象流补救** 切换按钮。

步骤 4 要设置大象流补救标准，请配置 CPU 利用率 %、固定时间窗口的持续时间和丢包百分比的值。

CPU利用率是根据流延迟计算的每个大象流。如果CPU使用率超出配置的阈值，并且也匹配其他配置（例如固定时间窗口和丢包），则会应用大象流补救操作。同样，丢包计算基于每个CPU丢弃的数据包。当丢包百分比超过特定CPU上的配置值后，系统将应用补救操作。例如，假设配置设置为默认值，即 CPU 使用率为 40%，固定时间窗口为 30 秒，丢包率为 5%。在特定 CPU 上，如果检测到的丢包数超过 5%，并且每个数据流的 CPU 使用率在 30 秒的固定时间范围内超过 40%，则会绕过或限制这些数据流。

步骤 5 当大象流补救符合配置的条件时，您可以对其执行以下操作：

1. **绕过流 (Bypass the flow)** - 启用此按钮可绕过所选应用或过滤器的 Snort 检查。选项包括：
   - **包括未识别应用在内的所有应用 (All applications including unidentified applications)** - 选择此选项可绕过所有应用流量。如果配置此选项，则无法为任何流配置限制操作（速率限制）。
   - **选择应用/过滤器** - 选择此选项可选择要绕过其流量的应用或过滤器；请参阅《Cisco Secure Firewall Management Center 设备配置指南》的**访问控制规则**一章中的**配置应用条件和过滤器**主题。
2. **限制流 (Throttle the flow)** - 启用此按钮可对流应用速率限制并继续检查流。请注意，您可以选择应用或过滤器来绕过 Snort 检查，同时限制剩余流量。

注释

当系统摆脱压力时，即 Snort 数据包丢弃的百分比小于配置的阈值时，会自动从已限制的大象流中删除限制。因此，速率限制也会被删除。

您还可以使用以下威胁防御命令从已限制的流量中手动删除限制：

- **clear efd-throttle <5-tuple/all> bypass** - 此命令从已限制的大象流中删除限制并绕过 Snort 检查。
- **clear efd-throttle <5-tuple/all>** - 此命令从已限制的大象流中删除限制，Snort 检测将继续。使用此命令后，系统将跳过大象流补救。

有关这些命令的详细信息，请参阅《Cisco Secure Firewall Threat Defense 命令参考》。

步骤 6 在 **补救豁免规则** 部分，点击 **添加规则** 为必须豁免补救的流配置 L4 访问控制列表 (ACL) 规则。

步骤 7 在 **添加规则** 窗口中，使用 **网络** 选项卡添加网络详细信息，即源网络和目的网络。使用 **端口** 选项卡添加源端口和目的端口。

如果检测到象流并且它与定义的规则相匹配，则会在 **连接事件**的 **原因** 列标题中生成一个事件，其原因为 **象流豁免** 。

步骤 8 在 **补救豁免规则** 部分，可以查看免于执行补救操作的流。

步骤 9 点击**确定 (OK)** 以保存大象流设置。

步骤 10 点击**保存**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。

配置大流设置后，监控连接事件以查看是否检测到、绕过或限制了任何流。您可以在连接事件的 **原因** 字段中查看此信息。出现大象流连接的三个原因是：

- 大象流
- 受限制的大象流
- 受信任的大象流

注意 仅启用大象流检测不会导致为大象流生成连接事件。如果由于其他原因已记录连接事件，并且流也是大象流，则 **原因** 字段包含此信息。但是，要确保记录所有大象流，必须在适用的访问控制规则中启用连接日志记录。

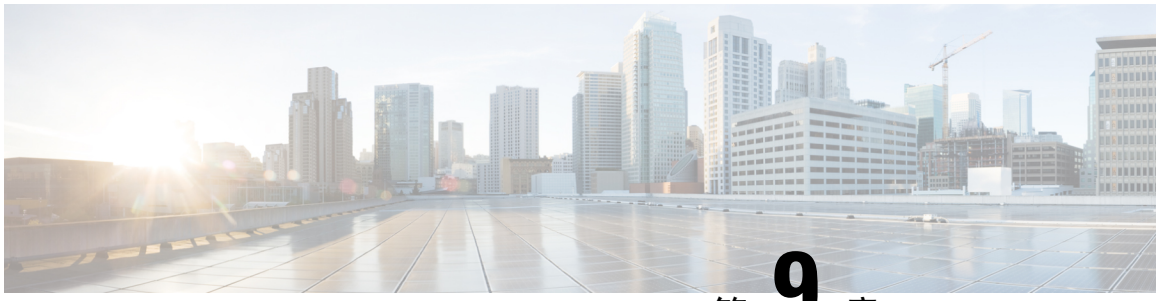
有关详细信息，请参阅 Cisco Secure Firewall 大象流检测 。



第 V 部分

Snort 3 使用案例

- 使用案例 - 在 Cisco Secure Firewall Management Center 中从 Snort 2 迁移到 Snort 3， 第 121 页
- 使用案例 - 在 Cisco Secure Fiewall Management Center 生成 Snort 3 建议， 第 131 页
- 使用案例 - 根据 EVE 威胁置信度评分阻止流量， 第 139 页
- 使用案例 - 配置大象流检测结果， 第 145 页
- 在 Snort 3 入侵策略中使用 MITRE 框架缓解威胁， 第 155 页



第 9 章

使用案例 - 在 Cisco Secure Firewall Management Center 中从 Snort 2 迁移到 Snort 3

- 从 Snort 2 迁移到 Snort 3， 第 121 页
- 迁移到 Snort 3 的优势， 第 121 页
- 示例业务情景， 第 122 页
- 从 Snort 2 迁移到 Snort 3 的最佳实践， 第 122 页
- 前提条件， 第 122 页
- 端到端迁移工作流程， 第 122 页
- 在威胁防御上启用 Snort 3， 第 123 页
- 将单个入侵策略的 Snort 2 规则转换为 Snort 3， 第 124 页
- 部署配置更改， 第 129 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**- 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

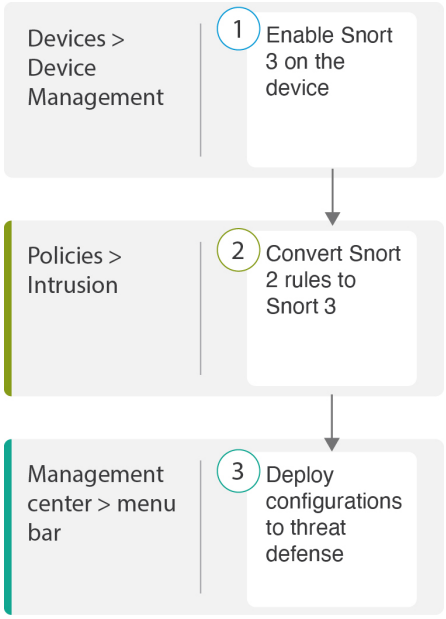
- 在执行迁移之前备份入侵策略。请参阅 *Cisco Secure Firewall Management Center* 管理指南 中的导出配置任务。
- 在将设备升级到 Snort 3 之前，如果在 Snort 2 中进行了更改，请使用同步实用程序包括从 Snort 2 到 Snort 3 的最新同步，以便您可以从类似的覆盖范围开始。请参阅将 Snort 2 规则与 Snort 3 同步 ， 第 24 页。
- Snort 2 自定义规则不会自动转换为 Snort 3，必须手动迁移。请参阅将 Snort 2 自定义规则转换为 Snort 3 ， 第 22 页。
- 同步不会迁移具有阈值或抑制的 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 123 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 124 页。
3	部署配置。请参阅部署配置更改，第 25 页。

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。

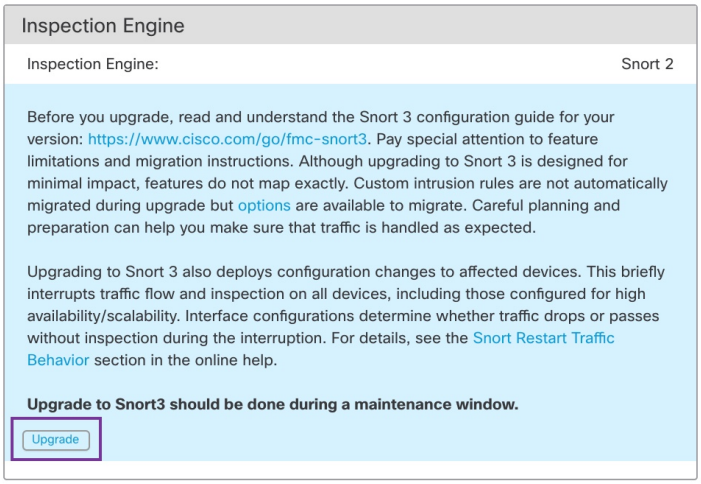
过程

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 点击是。

下一步做什么

在设备上部署更改。请参阅部署配置更改，第 25 页。

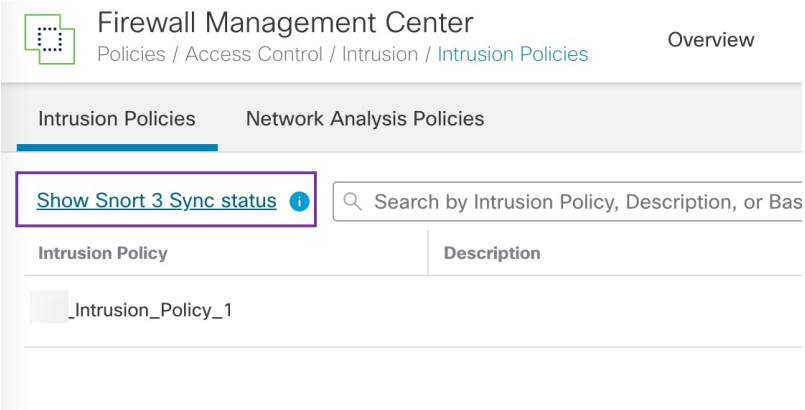
系统会在部署过程中转换您的策略配置，使其与所选的 Snort 版本兼容。

将单个入侵策略的 Snort 2 规则转换为 Snort 3

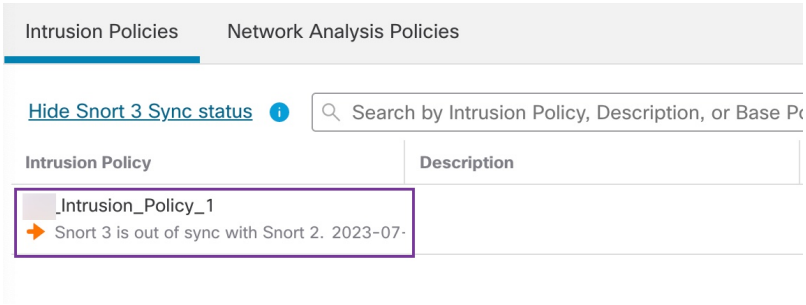
过程

步骤 1 选择策略 > 访问控制标题 > 入侵 > 入侵策略。

步骤 2 在 入侵策略 选项卡中，点击 显示 Snort 3 同步状态。

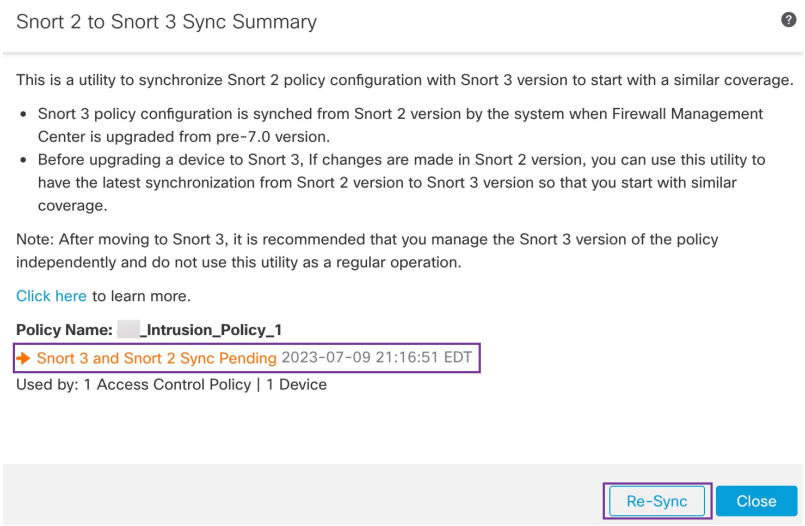


如果策略显示橙色箭头，则表示入侵策略的 Snort 2 和 Snort 3 版本未同步。



步骤 3 点击橙色箭头。

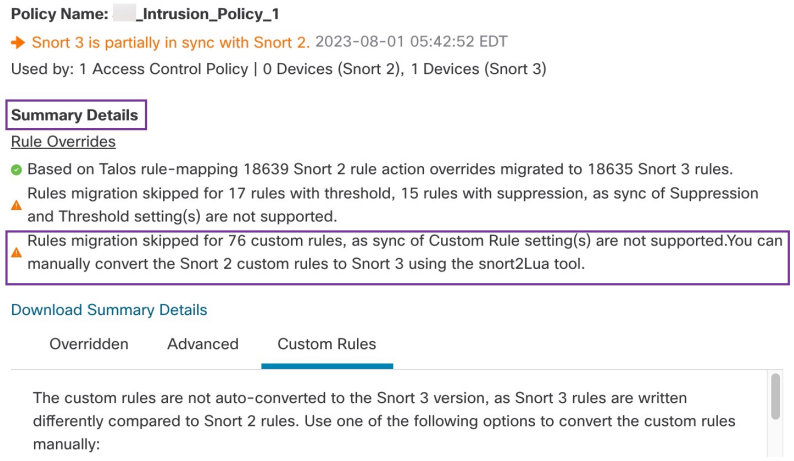
Snort 2 到 Snort 3 同步摘要 页面显示 Snort 2 到 Snort 3 的同步正在等待处理。



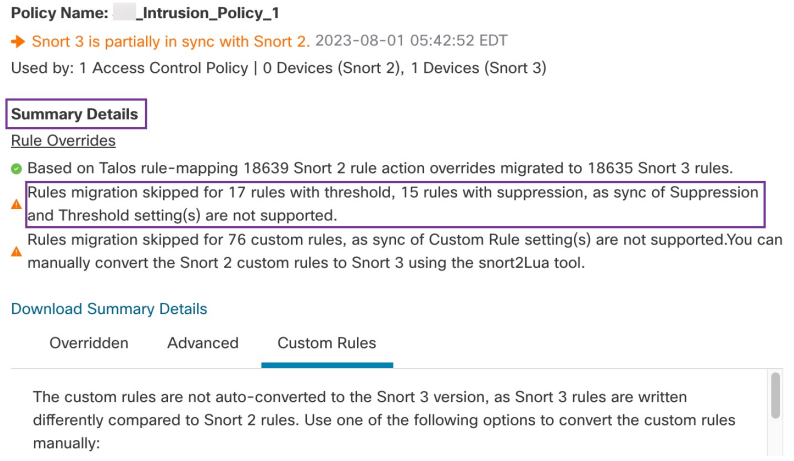
步骤 4 点击 **重新同步** 以开始同步。

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。

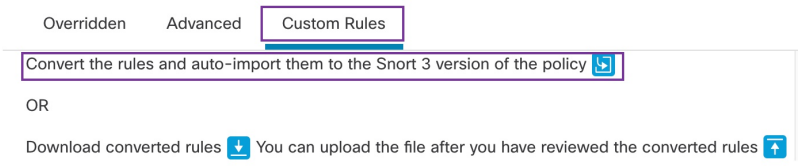


要迁移具有阈值和抑制的规则，请转至 步骤 6。



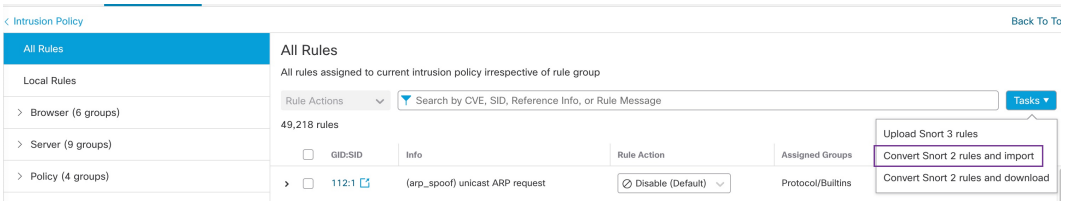
步骤 5 要迁移 76 条自定义规则，请执行以下任一步骤：

- 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。

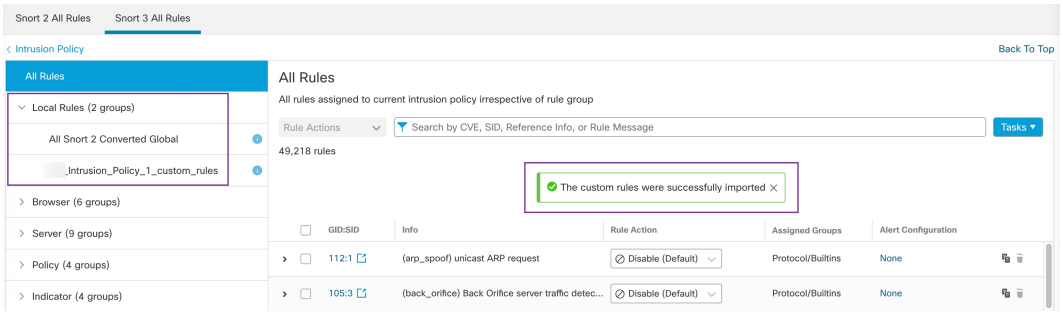


成功导入规则后，系统将显示确认消息。

- 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**。

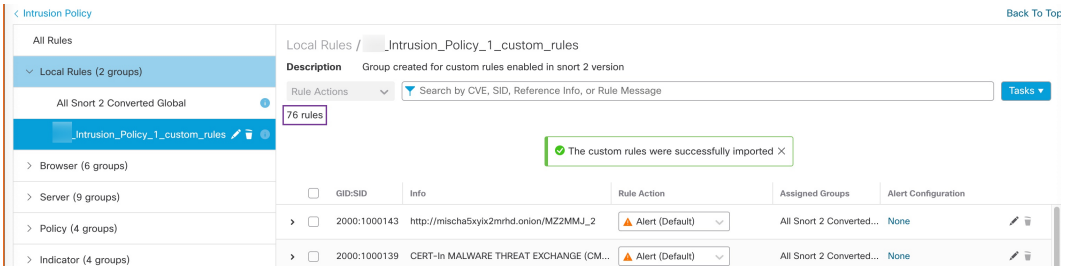


3. 点击**确定**。



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。**策略 > 访问控制标题 > 入侵**

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，第 25 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 *Cisco Secure Firewall Management Center* 指南 中的 部署配置更改 主题，了解部署更改的前提条件和影响。

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

过程

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

GUI 页面列出了具有 **待处理** 状态的过期配置的设备。

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

  注释
  没有为已删除的策略和对象提供用户名。

- **检查中断** 列指示在部署过程中是否可能导致设备中的流量检查中断。

  如果设备的此为空白，则表明在部署过程中该设备上不会出现流量检查中断。

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

步骤 2 识别并选择要部署配置更改的设备。

- 搜索 - 在搜索框中搜索设备名称、类型、域、组或状态。
- 展开 - 点击 **展开箭头**（ ） 以查看要部署的设备特定的配置更改。

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

  注释

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

步骤 3 点击**部署 (Deploy)**。

步骤 4 如果系统在要部署的更改中发现错误或警告，则会在**验证消息**窗口中显示它们。要查看完整详细信息，请点击警告或错误前的箭头图标。

有以下选项可供选择：

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

下一步做什么

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



第 10 章

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

- Snort 3 规则建议，第 131 页
- 优势，第 132 页
- 示例业务情景，第 132 页
- 最佳实践，第 132 页
- 前提条件，第 132 页
- 生成 Snort 3 建议，第 132 页
- 部署配置更改，第 135 页

Snort 3 规则建议

规则建议使用特定于主机环境的规则自动调整入侵策略。您可以通过禁用网络中不存在的漏洞的规则来启用其他规则或调整当前规则集。有关详细信息，请参阅Cisco Secure Firewall 建议规则的概述，第 63 页。

该计划如何实施？

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

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

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

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

优势

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

示例业务情景

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

最佳实践

- 您必须拥有高质量、准确的主机数据。

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

前提条件

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

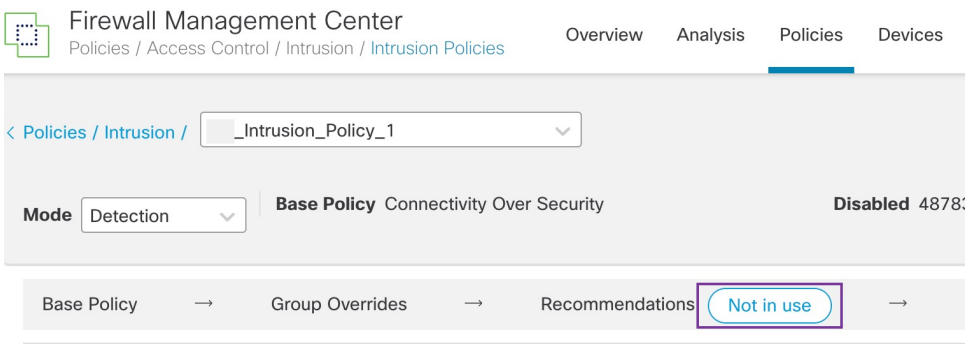
生成 Snort 3 建议

过程

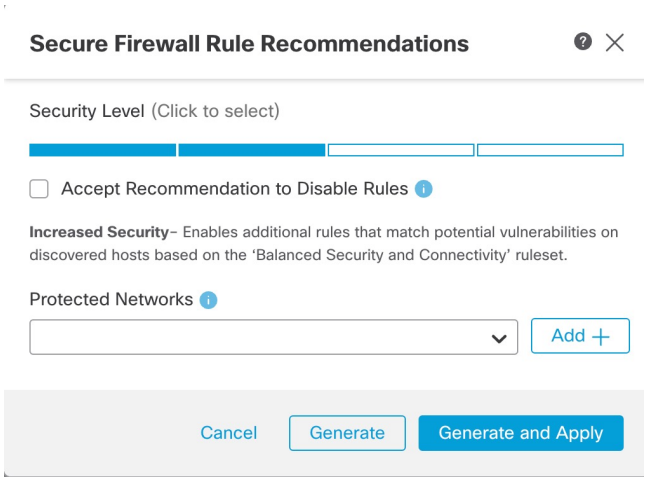
步骤 1 选择**策略** > **访问控制标题** > **入侵**。

步骤 2 点击相应的入侵策略的 **Snort 3 版本** 按钮。

步骤 3 点击 **建议**（**未使用**） 层以配置规则建议。



在 **思科建议的规则** 窗口中，您可以设置安全级别。



步骤 4 点击以选择安全级别。

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

仅当由于大量警报或提高检查性能而必须调整规则集时，才使用此选项。

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

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

步骤 7 生成并应用建议：

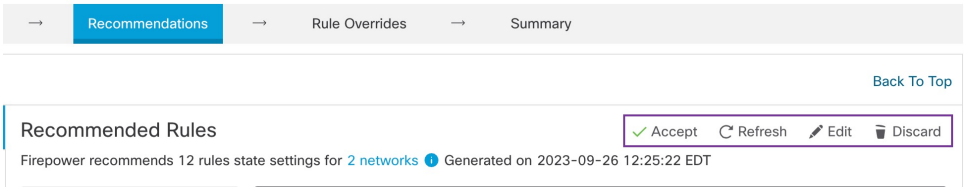
- **生成** - 生成入侵策略的建议。此操作列出了**建议的规则**（**未使用**）下的规则。
- **生成并应用** - 生成并应用入侵策略的建议。此操作列出了**建议的规则**（**未使用**）下的规则。

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

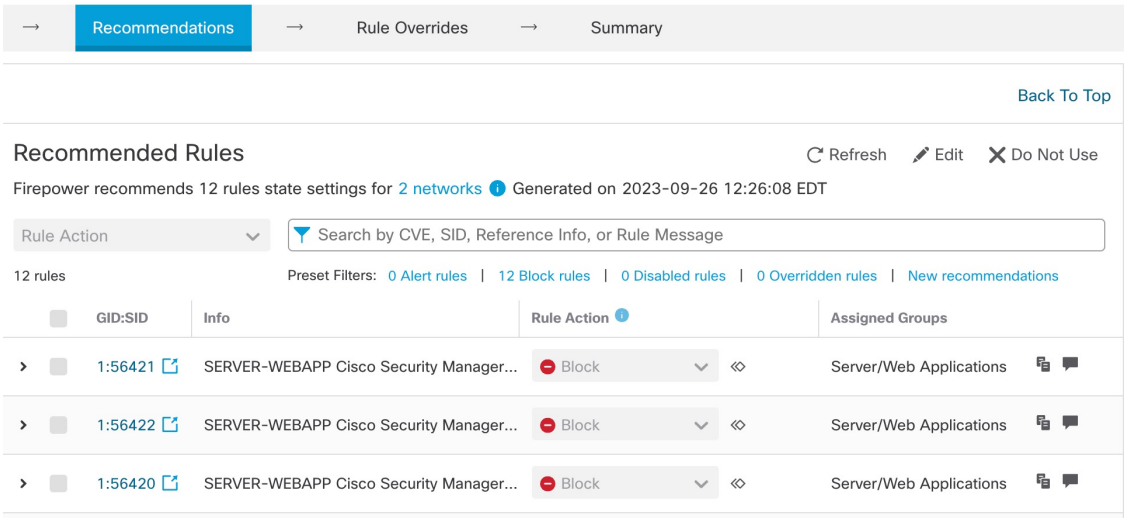
步骤 8 验证这些建议，然后相应地选择应用它们：

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

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

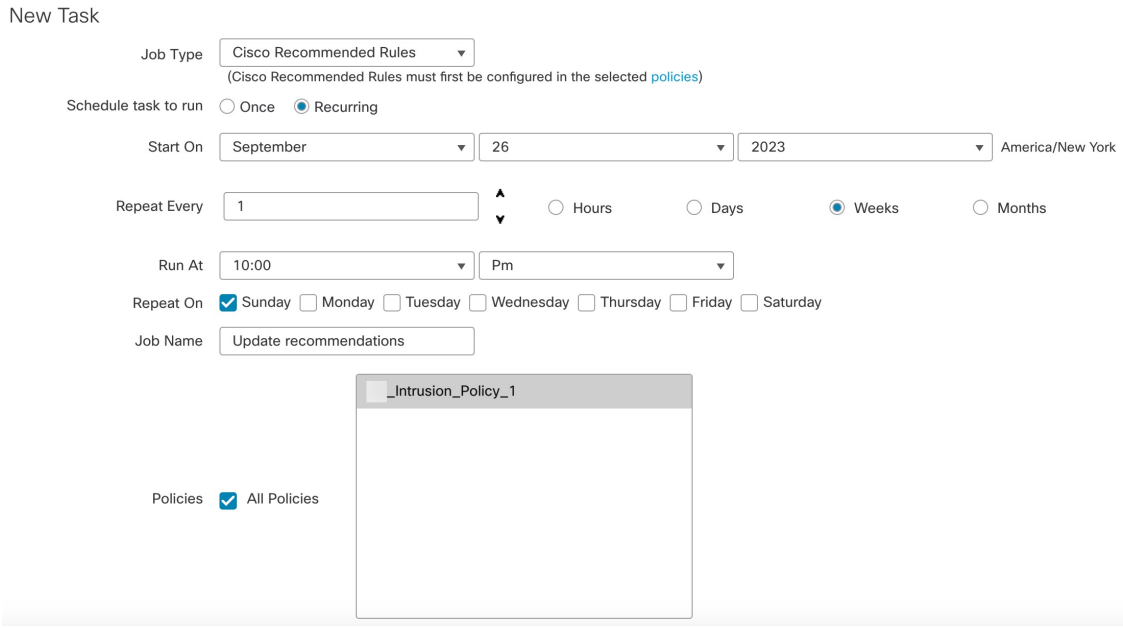


在 **所有规则**下，有一个建议的规则部分，其中显示建议的规则。



步骤 9 要有效地使用建议，必须定期更新。请按以下步骤操作：

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



5. 点击**保存 (Save)**。

下一步做什么

部署配置更改。请参阅部署配置更改，第 25 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 *Cisco Secure Firewall Management Center* 指南 中的 部署配置更改 主题，了解部署更改的前提条件和影响。

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

过程

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

GUI 页面列出了具有 **待处理** 状态的过期配置的设备。

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

  注释
  没有为已删除的策略和对象提供用户名。

- **检查中断** 列指示在部署过程中是否可能导致设备中的流量检查中断。

  如果设备的此为空白，则表明在部署过程中该设备上不会出现流量检查中断。

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

步骤 2 识别并选择要部署配置更改的设备。

- 搜索 - 在搜索框中搜索设备名称、类型、域、组或状态。
- 展开 - 点击 **展开箭头**（ ） 以查看要部署的设备特定的配置更改。

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

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

步骤 3 点击**部署 (Deploy)**。

步骤 4 如果系统在要部署的更改中发现错误或警告，则会在**验证消息**窗口中显示它们。要查看完整详细信息，请点击警告或错误前的箭头图标。

有以下选项可供选择：

- 部署 - 继续部署而无需解决警告情况。如果系统识别错误，则无法继续。

- 关闭 - 退出而不部署。解决错误和警告情况，并尝试重新部署该配置。

下一步做什么

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



第 11 章

使用案例 - 根据 EVE 威胁置信度评分阻止流量

- 关于加密可视性引擎， 第 139 页
- 优势， 第 139 页
- 示例业务情景， 第 139 页
- 前提条件， 第 140 页
- 高级工作流程， 第 140 页
- 在 EVE 中配置阻止阈值， 第 140 页
- 其他参考资料， 第 144 页

关于加密可视性引擎

您可以使用加密可视性引擎 (EVE) 来识别使用传输层安全 (TLS) 加密的客户端应用和进程。EVE 无需解密即可提供对加密会话的更多可视性。根据 EVE 的调查结果，管理员可以对其环境中的流量实施策略操作。您还可以使用 EVE 识别和阻止恶意软件。

优势

管理员可以利用和调整 EVE 的威胁评分来阻止恶意加密流量。如果传入流量是恶意的，则可以根据威胁评分将 EVE 配置为阻止连接。

示例业务情景

一家大型企业网络使用 Snort 3 作为其主要的入侵检测和防御系统。在快速发展的威胁环境中，采用强大的网络安全措施是必要且重要的。安全团队使用加密可视性引擎 (EVE) 来增强加密流量检查，而无需实施完整的中间人 (MITM) 解密。EVE 技术使用已知恶意进程的指纹来识别和阻止恶意软件。网络管理员必须能够灵活地配置 EVE 的阻止流量阈值，以阻止基于其配置的阻止阈值的潜在恶意连接。

前提条件

- 您必须运行管理中心 7.4.0 或更高版本，并且托管威胁防御也必须是 7.4.0 或更高版本。
- 确保您拥有有效的入侵防御系统 (IPS) 许可证，并且 Snort 3 是检测引擎。

高级工作流程

1. EVE 分析传入流量，并判定传入流量是否为恶意软件的可能性。
2. 如果 EVE 以一定的置信度检测到传入流量为恶意软件，则可以将 EVE 配置为阻止该流量。
3. 首先检查数据包的恶意软件概率或威胁评分，然后将威胁评分与您设置的阻止阈值进行比较。
4. 如果威胁评分高于配置的阈值，EVE 将阻止流量。
5. 如果威胁评分低于配置的阈值，EVE 不采取任何措施。

在 EVE 中配置阻止阈值

此程序显示如何根据 90% 或更高的 EVE 威胁置信度分数阻止潜在的恶意流量。

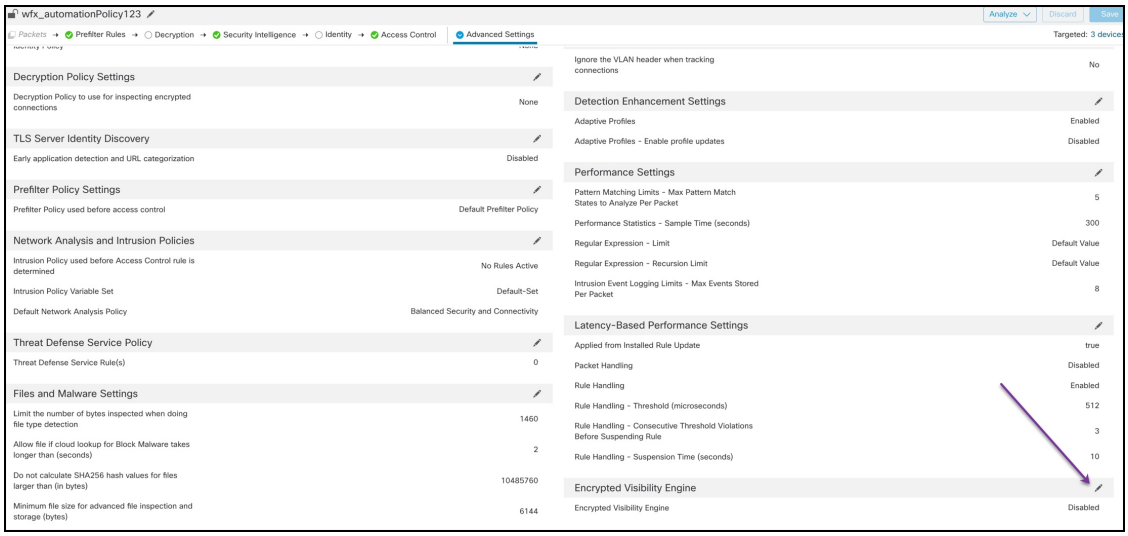
过程

步骤 1 选择**策略** > **访问控制标题** > **访问控制**。

步骤 2 点击要编辑的访问控制策略旁边的 **编辑** ( ) 。

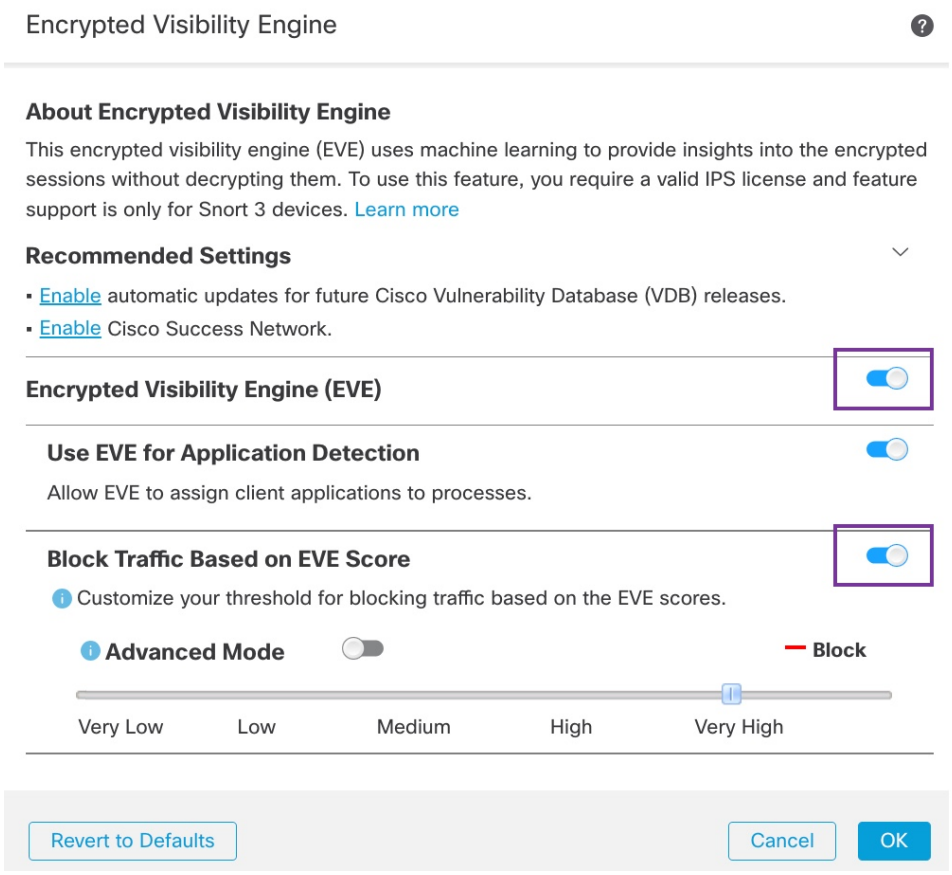
步骤 3 从数据包流末尾的 **更多** 下拉箭头中选择 **高级设置** 。

步骤 4 点击**加密可视性引擎 (Encrypted Visibility Engine)** 旁边的 **编辑** ( )。



步骤 5 在 **加密可视性引擎** 页面中，启用 **加密可视性引擎 (EVE)** 切换按钮。

步骤 6 启用 **基于 EVE 分数阻止流量** 切换按钮。默认情况下，任何可能构成威胁的传入流量都会被阻止。

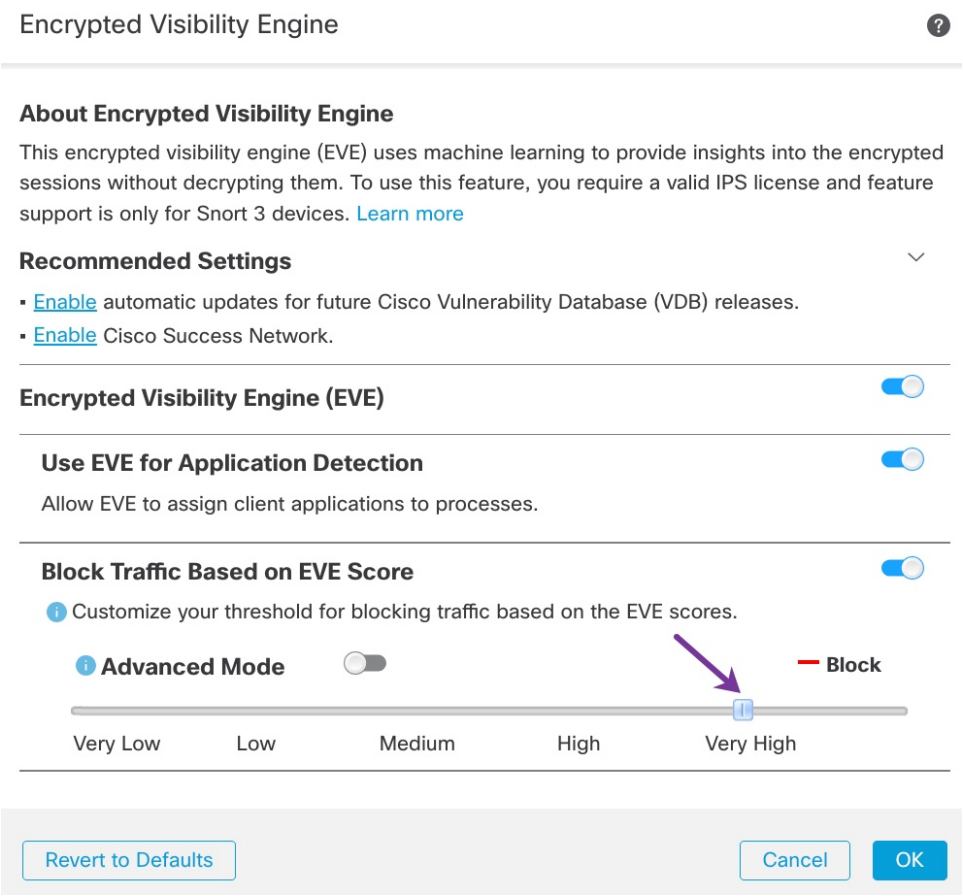


注释

默认情况下，阻止恶意软件的阈值为 99%，这意味着：

- 如果 EVE 检测到流量为恶意软件且置信度为 99% 或更高，则 EVE 会被阻止流量。
- 如果 EVE 检测到流量为恶意软件且其置信度低于 99%，则 EVE 不会采取任何措施。

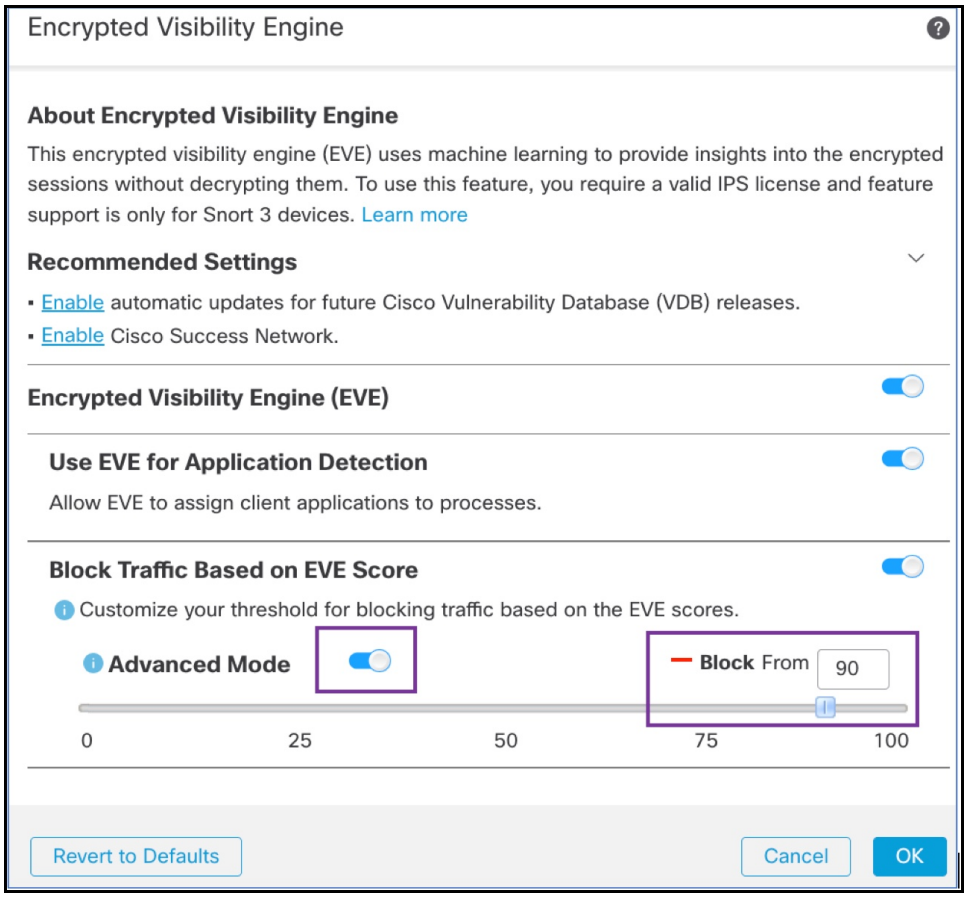
步骤 7 使用滑块根据 EVE 威胁置信度调整阻止阈值。范围从 **非常低** 到 **非常高**。在本例中，滑块设置为 **非常高**。



步骤 8 要进行进一步精细控制，请启用**高级模式 (Advanced Mode)** 切换按钮。现在，您可以为阻止流量分配特定的 EVE 威胁置信度评分。默认阈值为 99%。

步骤 9 在本例中，将阻止阈值更改为 **90**%。

注意
作为最佳实践，我们建议您不要将阻止阈值设置为低于 50%，以确保最佳性能。



步骤 10 点击确定 (OK)。

步骤 11 点击保存 (Save)。

下一步做什么

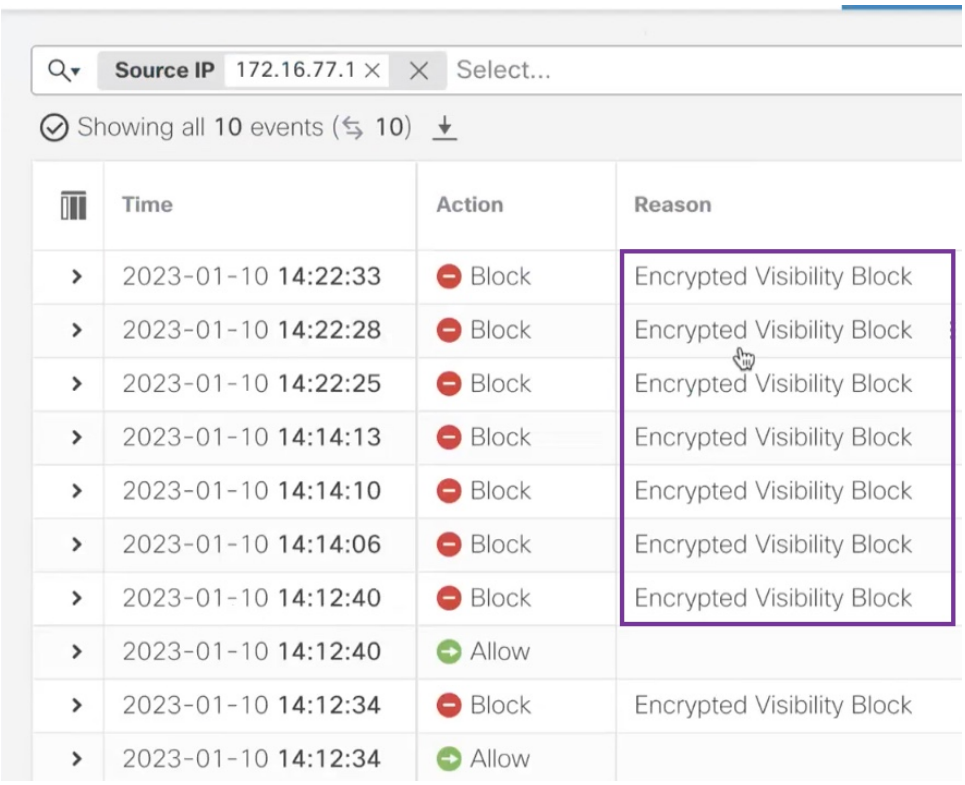
部署配置更改。请参阅部署配置更改，第 25 页。

查看 EVE 事件

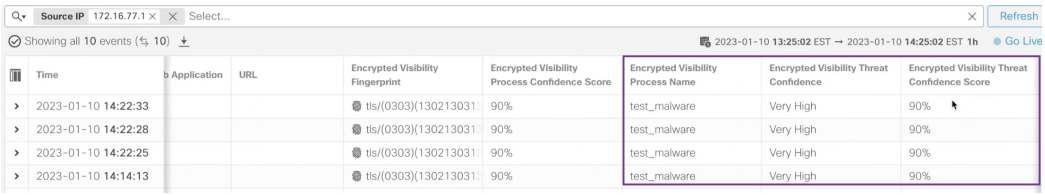
过程

步骤 1 要验证阻止操作，请选择 分析 > 连接 > 事件。您还可以在 统一事件 查看器中查看事件。

步骤 2 如果您已将 EVE 配置为阻止流量，则 原因 字段将显示 加密可视性阻止。



步骤 3 以下是 加密可视性进程名称 为 **test_malware**、 加密可视性威胁置信度 为 非常高、 加密可视性威胁置信度 为 **90** % 的示例。



其他参考资料

有关详细的概念信息，请参阅本指南中的“Snort 3 加密可视性引擎”一章或以下链接中的内容：

加密可视性引擎



第 12 章

使用案例 - 配置大象流检测结果

- 关于大象流，第 145 页
- 关于大象流检测和补救的优势，第 145 页
- 大象流工作流程，第 145 页
- 示例业务情景，第 146 页
- 前提条件，第 146 页
- 配置大象流参数，第 147 页
- 配置大象流补救豁免，第 150 页
- 其他参考资料，第 153 页

关于大象流

大象流非常大（以总字节数为单位），由 TCP（或其他协议）设置的相对长运行的网络连接通过网络链路测量。默认情况下，大象流是速率大于每 10 秒 1GB 的流。它们可能会在 Snort 核心中造成性能威胁或问题。大象流很重要，因为它们可能会消耗过多的CPU资源，并影响检测资源的其他竞争流，并导致延迟增加或丢包等问题。

关于大象流检测和补救的优势

- 大象流配置允许自定义和绕过甚至限制大象流的选项。
- 您可以选择绕过或限制基于所选应用的流量，以提供可疑流量的Snort检查，同时绕过更受信任的流量。
- 大象流补救有助于根据您的特定要求确定优先级并为内部应用释放更多带宽。

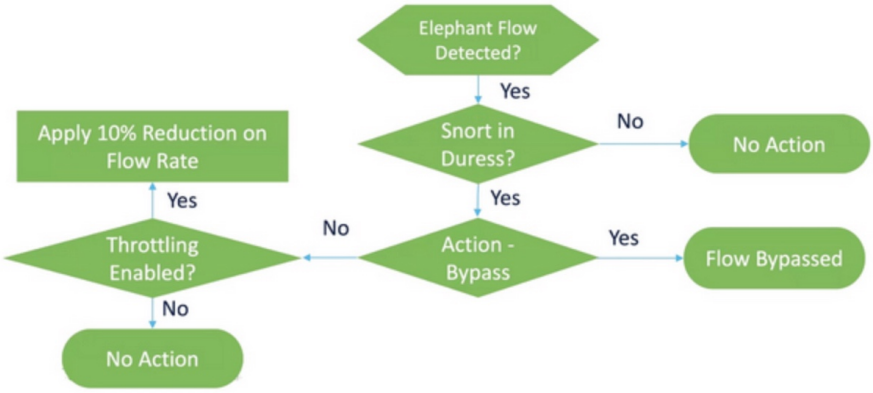
大象流工作流程

当根据配置的参数检测到大量流时，您可以选择绕过或限制该流。当流量被绕过时，允许流量通过而不进行 Snort 检查。限制表示流量吞吐量降低。以 10% 的增量降低流量，直到 CPU 使用率降至配

置的阈值以下。在识别大流并满足额外的CPU和时间窗口参数后，会发生绕行或限制。在识别大流之前，入侵策略会处理流，假设您已在“允许”规则中配置此流。这意味着不允许大量流在完全未经检查的情况下通过系统，因为大多数攻击都是在连接中很早就被检测到的。

要了解如何处理流，请参阅以下流程图。

图 *4:* 大象流工作流程



除非系统检测到Snort强制条件（性能问题），否则不会执行任何操作。系统不会仅仅因为流量大而限制或绕过流量。此外，限制和旁路的操作是相互排斥的。这意味着您可以绕过或限制流，但不能同时绕过或限制流。

如果您不想绕过导致威胁的所有大流，可以将绕过选项限制为仅适用于特定应用。您可以优先考虑您信任的应用的连接，而不会限制性能。您可以配置必须绕过的应用，但剩余流量（导致威胁）将受到限制。这可确保其他不受信任的应用流仍会收到完整的 Snort 检测，尽管其带宽已减少。

示例业务情景

在数据中心中，会发生多项活动，例如集群之间的数据复制、虚拟机集成和数据库备份。组织中的用户可能正在OTT上观看或下载视频。此类活动的带宽利用率可能会导致大量流量，降低网络速度并影响重要任务的性能。作为网络管理员（根据您的特定要求），您希望了解导致带宽问题的大型数据流并进行补救。

例如，让我们看看如何配置大流参数来绕过WebEx流量（您的组织用于实时视频会议）并限制其余应用或连接，包括视频、电影等。

前提条件

- 确保您运行的是管理中心 7.2.0 或更高版本，并且托管威胁防御也是 7.2.0 或更高版本。
- 仅启用大象流检测不会生成其他连接事件。大象流检测将大象流表示法添加到已记录到管理中心的匹配连接。**要记录这些事件，必须在访问控制策略中启用连接日志记录**。您可以对特定规则执行此操作，也可以添加记录所有连接（包括大流）的监控规则。

配置大象流参数

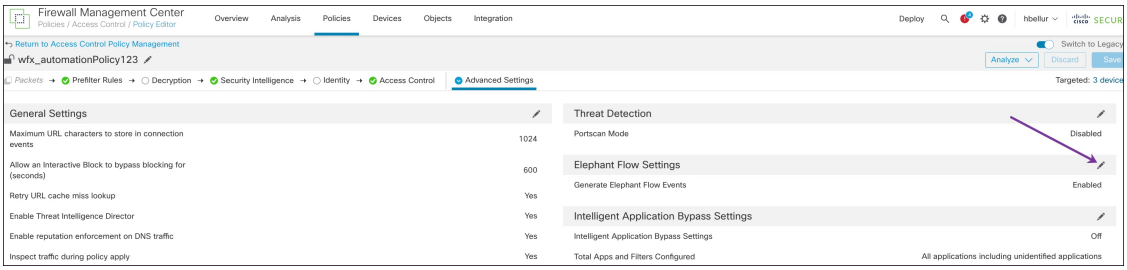
过程

步骤 1 选择**策略** > **访问控制标题** > **访问控制**。

步骤 2 点击要编辑的访问控制策略旁边的 **编辑** ()。

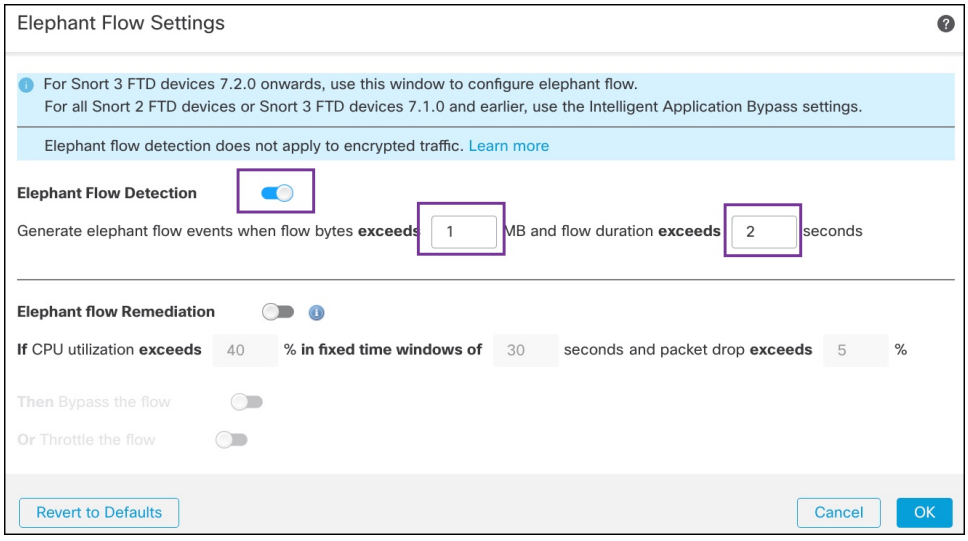
步骤 3 从数据包流末尾的 **更多** 下拉箭头中选择 **高级设置** 。

步骤 4 点击**大象流设置 (Elephant Flow Settings)** 旁边的 **编辑** ()。



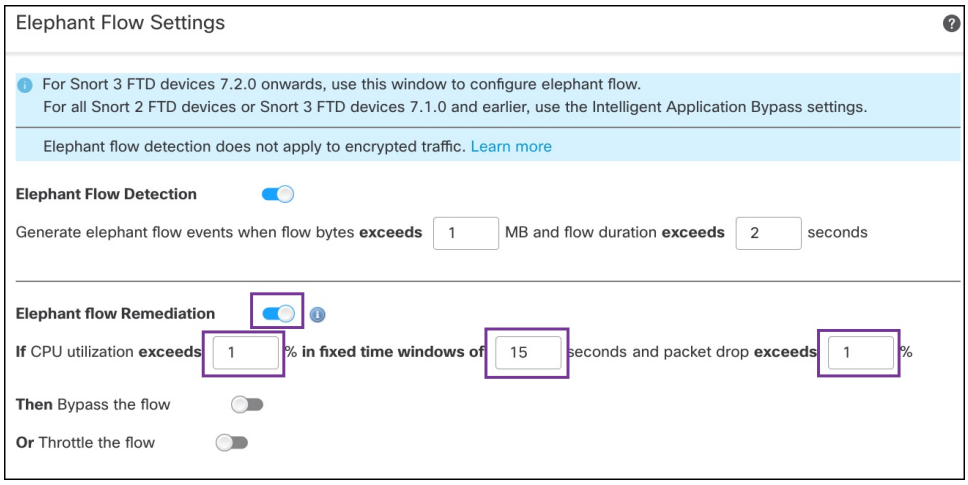
步骤 5 默认情况下，**大象流检测 (Elephant Flow Detection)** 切换按钮处于启用状态。默认设置仅启用检测，不配置默认操作。检测设置允许您调整流字节和持续时间，以便可以识别系统中的大象流。

作为测试设置，配置流字节和持续时间参数，如下图所示。

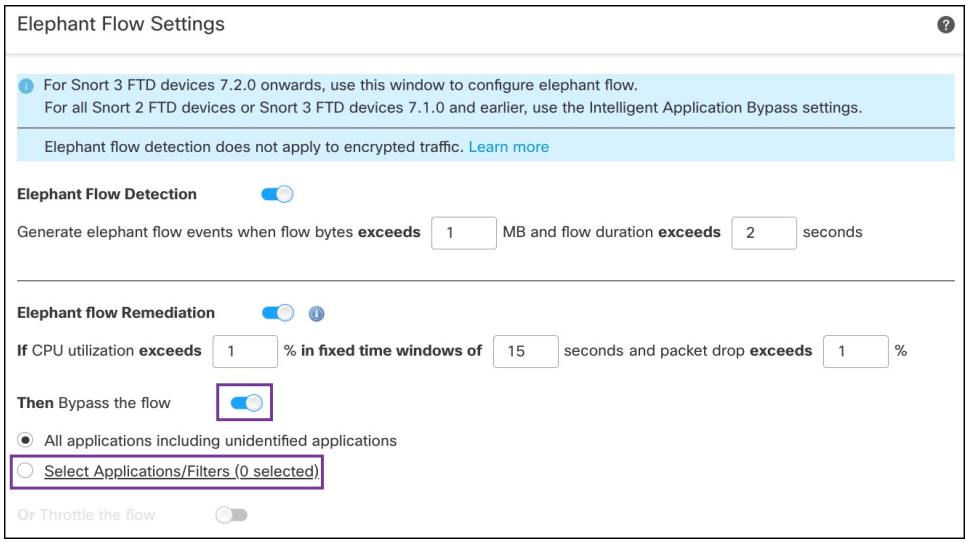


步骤 6 启用 **大象流补救** 切换按钮。当检测到大象流时，您可以选择绕过或限制该流。绕过流意味着允许流量通过而无需 Snort 检查。限制表示流量吞吐量降低。此速率降低以 10% 为增量，直到 CPU 使用率降至低于配置的阈值。

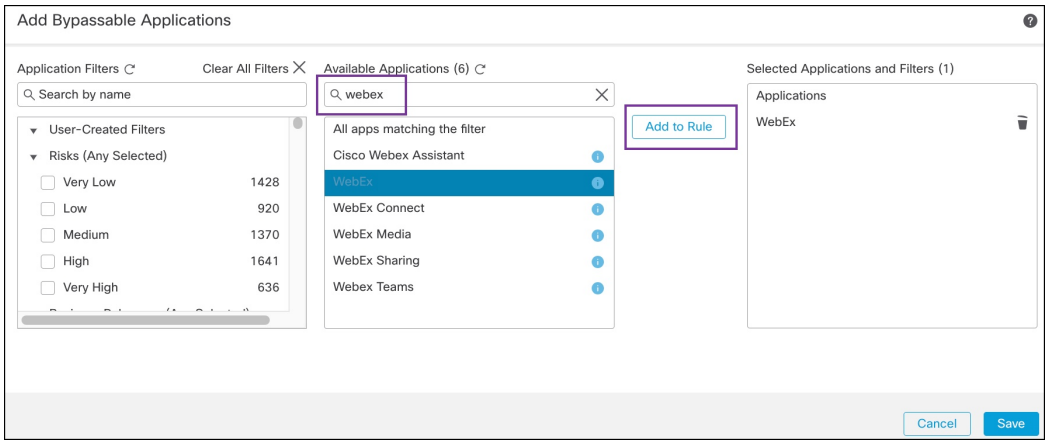
作为测试设置，配置大象流补救参数，如下图所示。



步骤 7 启用 **绕过流** 切换按钮，然后点击 **选择应用/过滤器** 单选按钮。



步骤 8 在 **应用过滤器**下，搜索并选择 **WebEx** 应用，将其添加到规则中，然后点击 **保存**。这意味着 WebEx 连接是受信任的和优先的，如果这些 WebEx 连接被检测为大象流，则将根据配置的参数跳过 Snort 检查。



步骤 9 启用 **限制** 切换按钮以限制剩余流量（导致强制）。这可确保所有其他流量以 10% 的增量减慢，直到满足 Snort 强制条件。

步骤 10 点击**确定 (OK)**。

步骤 11 点击**保存 (Save)**。

下一步做什么

部署配置更改。请参阅部署配置更改，第 25 页。

查看大象流的事件

配置大流设置后，监控连接事件以查看是否检测到、绕过或限制了任何流。您可以在连接事件的 **原因** 字段中查看此信息。大象流连接的三种类型为：

- 大象流
- 受限制的大象流
- 受信任的大象流

过程

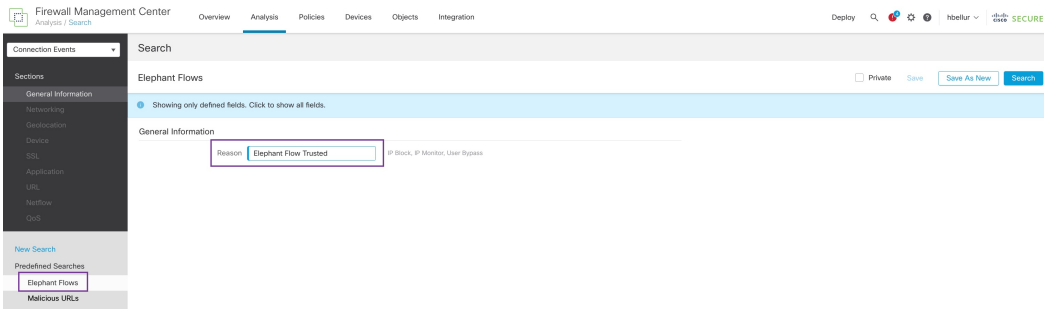
步骤 1 选择**分析** > **连接** > **事件**。您还可以在 **统一事件** 查看器中查看事件。

步骤 2 在 **连接事件** 页面中，从 **预定义搜索** 下拉列表中选择 **大象流** 以显示象形流事件。

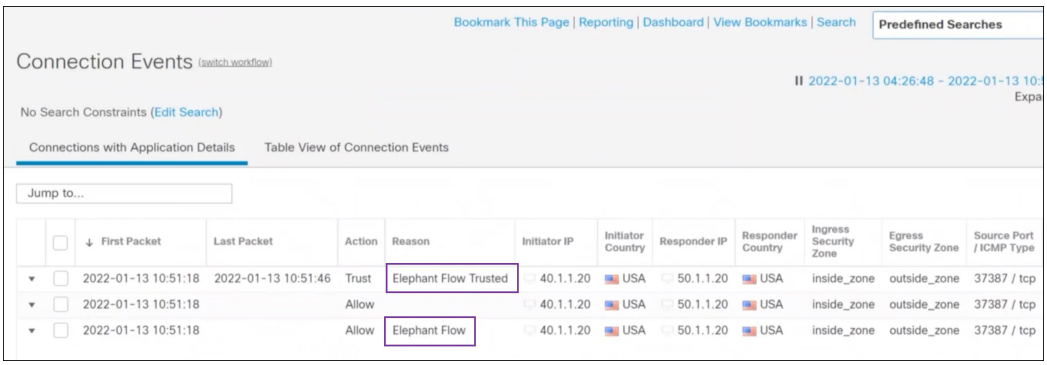


提示

要查看 **受信任的大象流** 或 **受限制的大象流** 事件类型，请点击页面左上角的 **编辑搜索** 链接，然后在 **原因** 字段中，选择左侧面板中的 **大象流** 。根据要搜索的内容，输入 **受信任的大象流** 或 **受限制的大象流**。



步骤 3 查看在流中检测到的大象流，并且 **原因** 字段显示 **大象流**。在流结束时，它被绕过，并且 **原因** 字段显示 **受信任的大象流**。



配置大象流补救豁免

您可以为必须豁免补救的流配置 L4 访问控制列表 (ACL) 规则。如果检测到大型流，并且该流与为必须豁免补救操作的流定义的规则匹配。

开始之前

您必须运行管理中心 7.4.0 或更高版本，并且托管威胁防御也必须是 7.4.0 或更高版本。

过程

步骤 1 选择**策略** > **访问控制标题** > **访问控制**。

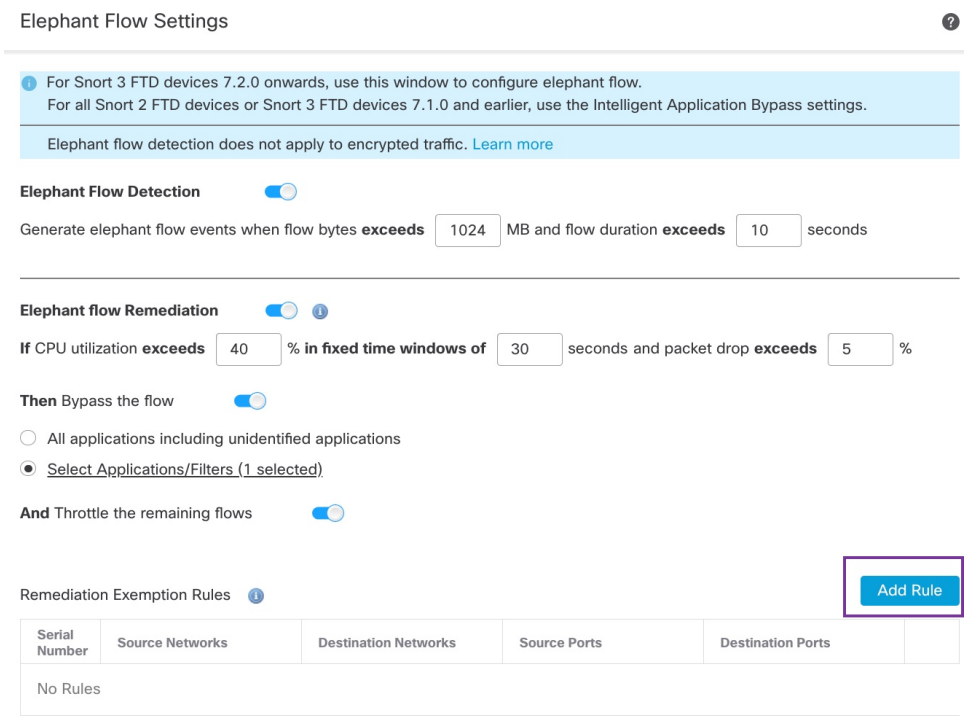
步骤 2 点击要编辑的访问控制策略旁边的 **编辑** ( ) 。

步骤 3 从数据包流末尾的 **更多** 下拉箭头中选择 **高级设置** 。

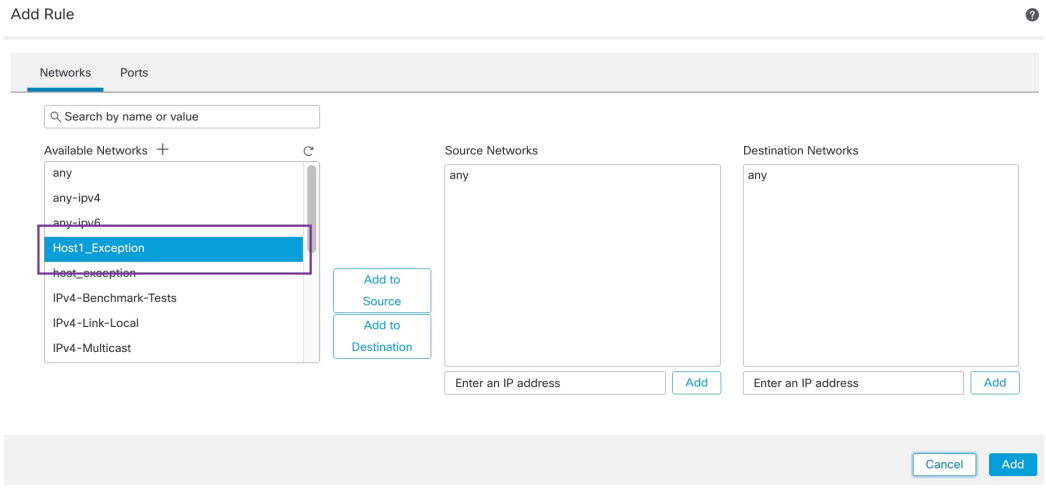
步骤 4 点击**大象流设置 (Elephant Flow Settings)** 旁边的 **编辑** ()。

步骤 5 确保您已配置大象流检测和补救参数。请参阅配置大象流参数，第 147 页。

步骤 6 点击 **补救豁免规则**旁边的 **添加规则** 按钮。



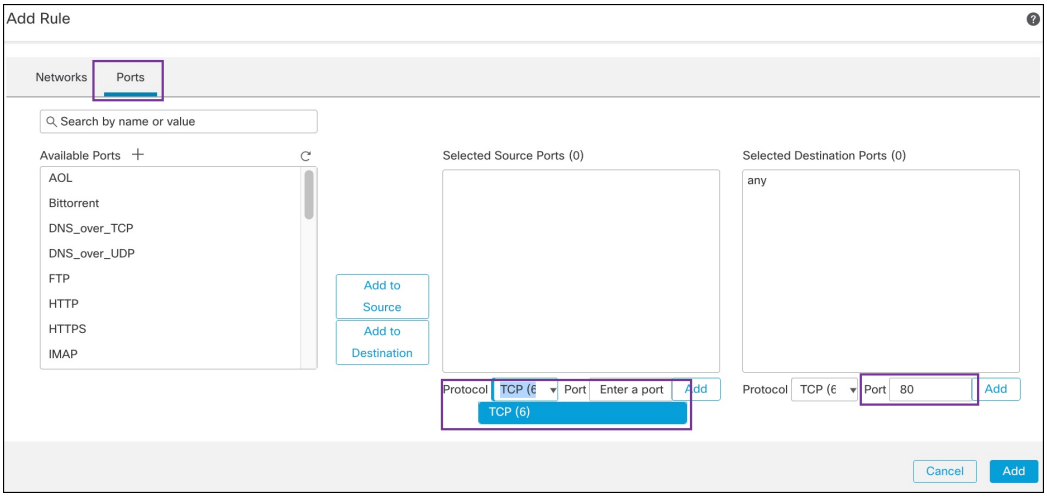
步骤 7 从 **可用网络**列表中，选择要免于执行大象流补救的已配置主机。在本示例中，我们创建了一个名为“Host1_Exception”的主机。



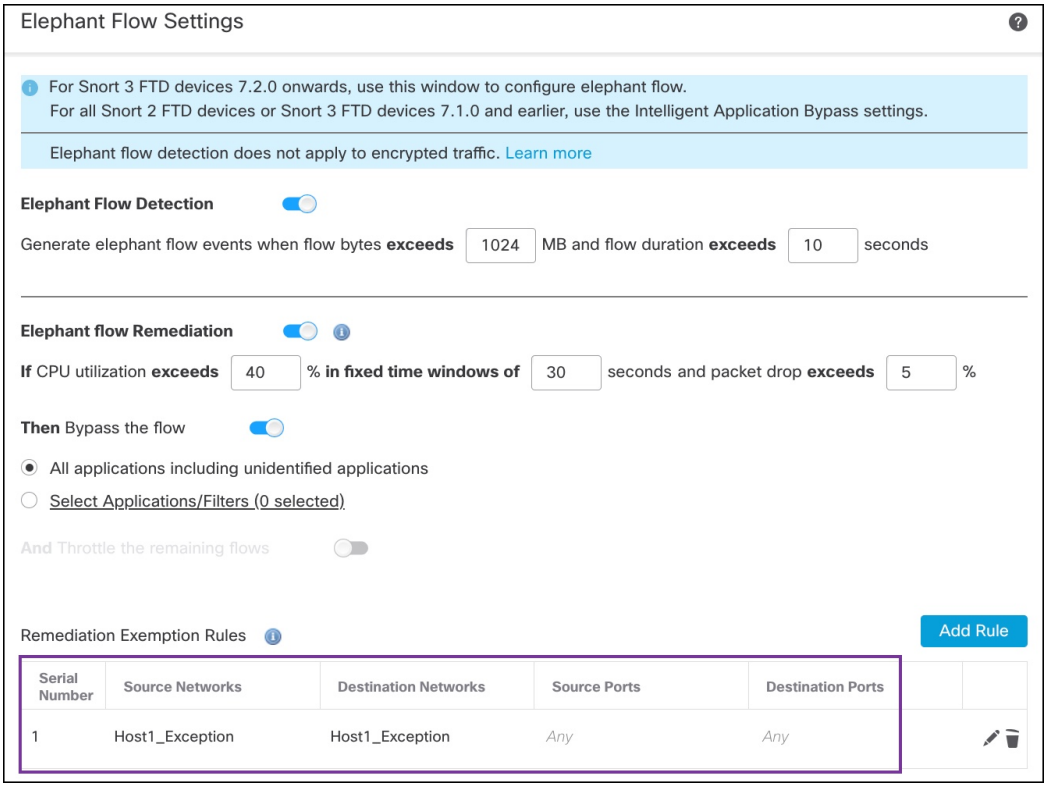
步骤 8 点击 **添加到源** 或 **添加到目标** （根据需要），将此主机添加到源或目标。

步骤 9 点击**端口**选项卡。

步骤 10 对于源端口，选择 **协议** 作为 TCP 并输入 **80** 作为目的端口，然后点击 **添加**。



步骤 11 点击**确定 (OK)**。



步骤 12 点击**保存 (Save)**。

下一步做什么

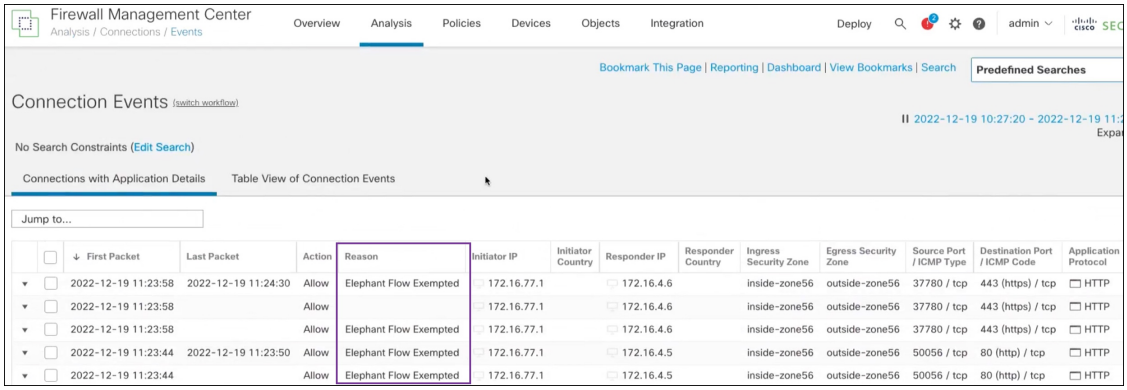
部署配置更改。请参阅部署配置更改，第 25 页。

查看大象流补救豁免事件

过程

步骤 1 选择**分析** > **连接** > **事件**。您还可以在 **统一事件** 查看器中查看事件。

步骤 2 查看免于补救的大象流。 **理由** 字段显示 **免于补救的大象流**。



其他参考资料

有关详细的概念信息，请参阅本指南中的“Snort 3 大象流检测”一章或以下链接中的内容：

- 大象流检测



第 13 章

在 Snort 3 入侵策略中使用 MITRE 框架缓解威胁

- 关于 MITRE ATT&CK 框架，第 155 页
- MITRE 框架的优势，第 156 页
- MITRE 网络的业务场景示例，第 156 页
- MITRE 框架的必备条件，第 156 页
- 查看和编辑 Snort 3 入侵策略，第 156 页
- 查看入侵事件，第 161 页
- 其他参考资料，第 163 页

关于 MITRE ATT&CK 框架

MITRE ATT&CK 框架是一个全面的知识库，其中概述了威胁发起者用来破坏系统的战术、技术和程序 (TTP)。它将这些 TTP 组织到不同操作系统和平台的矩阵中，将每个攻击阶段（战术）映射到特定方法（技术）。每种技术都包括有关执行、程序、防御、检测和实际示例的信息。

注释 有关 MITRE ATT&CK 的其他信息，请参阅 https://attack.mitre.org。

管理中心使用 MITRE ATT&CK 框架来增强威胁检测和响应，并纳入以下功能：

- 入侵事件包括 TTP，允许管理员根据漏洞类型、目标系统或威胁类别对规则进行分组，从而更精细地管理流量。
- 选择恶意软件事件使用 TTP，从而增强检测和响应威胁的能力。
- 统一和经典事件查看器显示 Talos 分类中的战术、技术、攻击生命周期图和情景扩充内容。这些扩充内容包括 MITRE 标记以及关联的策略、技术和子技术的分层视图。您还可以使用 MITRE 标识符过滤事件。

MITRE 框架的优势

- MITRE 策略、技术和程序 (TTP) 添加到入侵事件中，使管理员能够根据 MITRE ATT&CK 框架对流量执行操作。这让管理员能够以更精细的方式查看和处理流量，并按漏洞类型、目标系统或威胁类别对规则进行分组。
- 您可以根据 MITRE ATT&CK 框架组织入侵规则。这使您可以根据特定的攻击者战术和技术自定义策略。

MITRE 网络的业务场景示例

一家大型企业网络使用 Snort 3 作为其主要的入侵检测和防御系统。在快速发展的威胁环境中，采用强大的网络安全措施是必要且重要的。网络管理员需要知道配置的策略是否正在查找感兴趣的流量，以及他们是否在跟踪已知的攻击组。例如，您可能想知道攻击者是否试图利用您的系统或应用中的弱点来导致意外行为。系统中的弱点可能是漏洞、故障或设计漏洞。应用可以是网站、数据库、标准服务（例如服务器消息块 (SMB) 或安全外壳 (SSH)）、网络设备管理和管理协议或应用（例如 Web 服务器和相关服务）。

MITRE 框架提供的见解为管理员提供了一个更精确的机会来指定对特定资产的保护并保护其网络免受特定威胁组的侵害。

MITRE 框架的必备条件

- 您必须运行 Cisco Secure Firewall Management Center 和带有 Snort 3 的 Cisco Secure Firewall 威胁防御 7.3.0 或更高版本。
- 必须至少有一个入侵策略。请参阅创建自定义 Snort 3 入侵策略 ，第 32 页。

查看和编辑 Snort 3 入侵策略

过程

步骤 1 选择**策略** > **访问控制标题** > **入侵**。

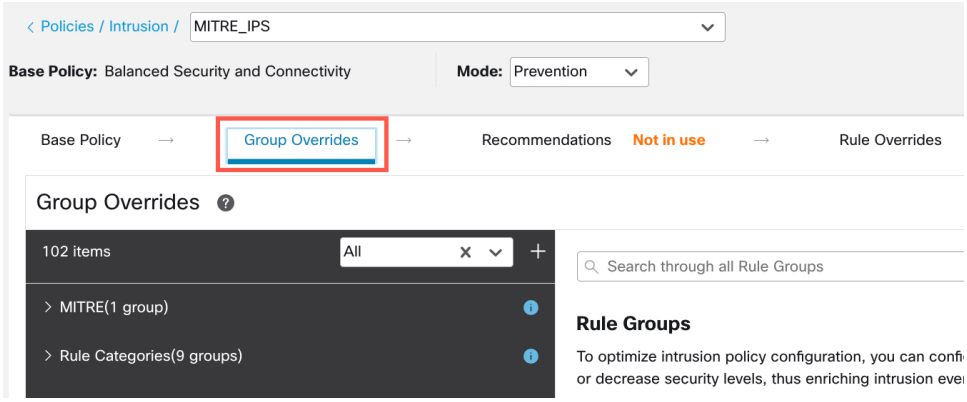
步骤 2 确保选择**入侵策略 (Intrusion Policies)** 选项卡。

步骤 3 点击要查看或编辑的入侵策略旁边的 **Snort 3 版本 (Snort 3 Version)**。

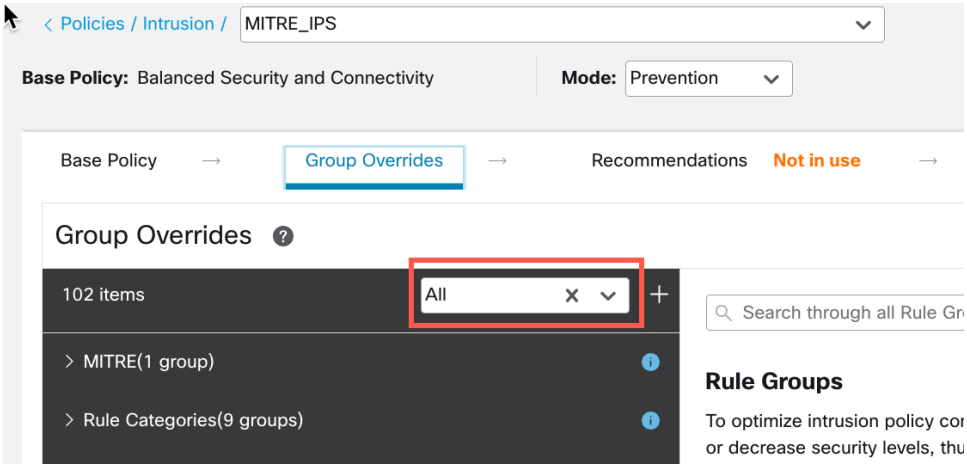
步骤 4 关闭显示的 Snort 助手指南。

步骤 5 点击**组覆盖 (Group Overrides)** 层。

此层以分层结构列出规则组的所有类别。您可以向下展开到每个规则组下的最后一个枝叶规则组。

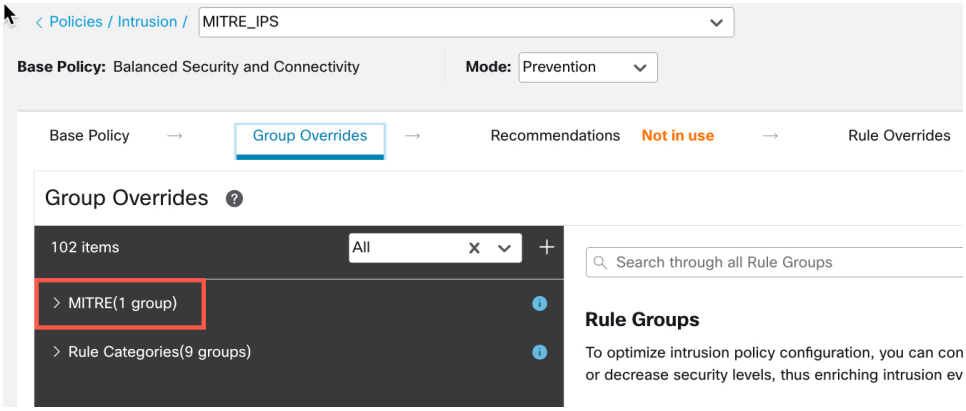


步骤 6 在**组覆盖 (Group Overrides)** 下，确保在下拉列表中选择**全部 (All)**，以便相应入侵策略的所有规则组在左侧窗格中可见。

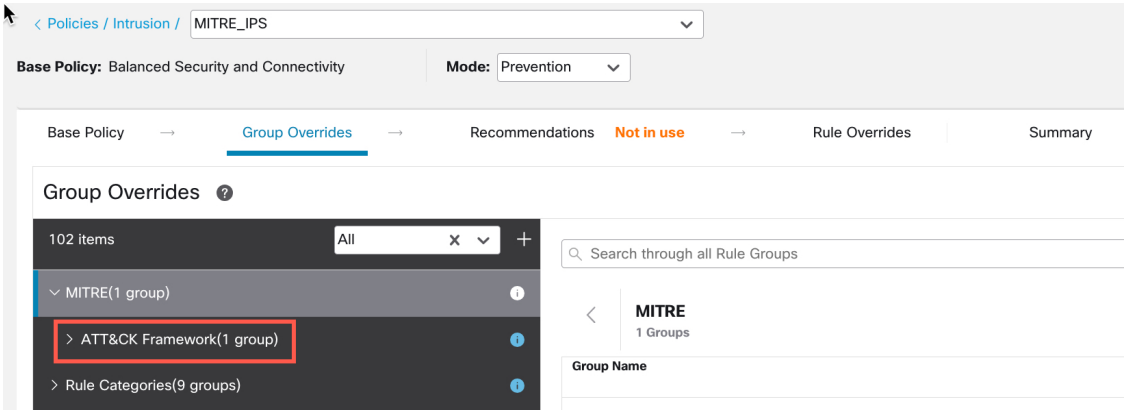


步骤 7 点击左窗格中的 **MITRE**。

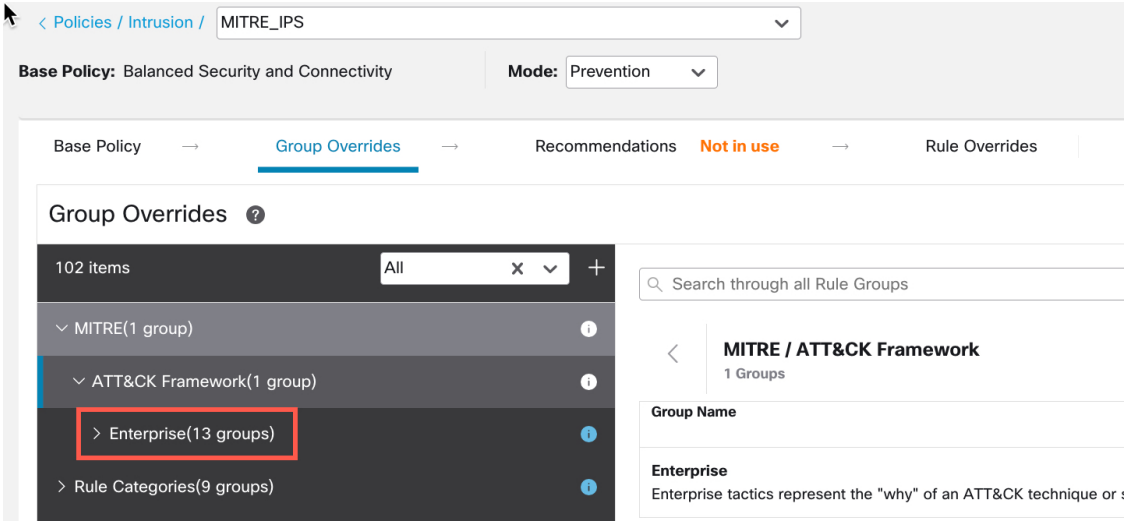
注释
根据您的特定要求，您可以选择**规则类别 (Rule Categories)** 规则组或其下的任何其他规则组和子规则组。所有规则组都使用 MITRE 框架。



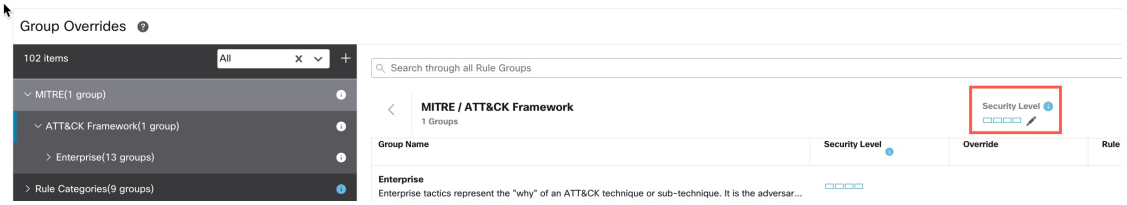
步骤 8 在 **MITRE**下，点击 **ATT&CK 框架 (ATT&CK Framework)** 向下展开。



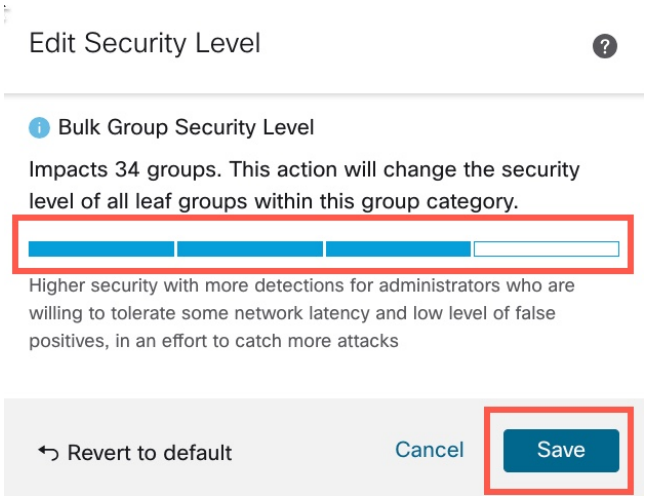
步骤 9 在 **ATT&CK 框架 (ATT&CK Framework)** 下，点击**企业 (Enterprise)** 以将其展开。



步骤 10 点击规则组安全级别 (Security Level) 旁边的 **编辑** (✎) 图标，对**企业 (Enterprise)** 规则组类别下的所有关联规则组的**安全级别**进行批量更改。

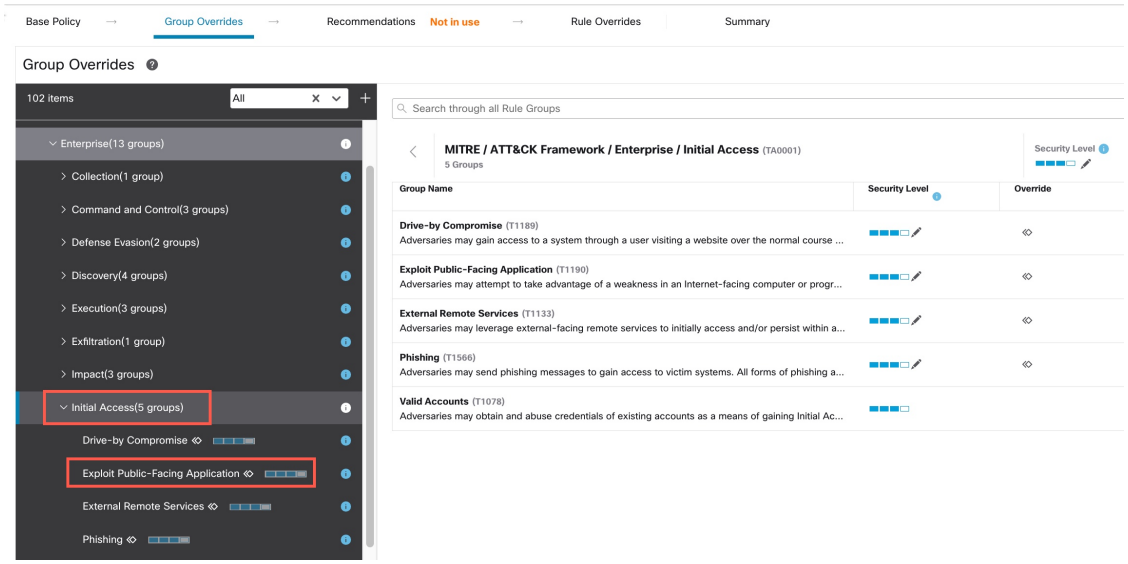


步骤 11 在**编辑安全级别**窗口中，选择**安全级别** （在本例中为 **3**），然后点击**保存**。

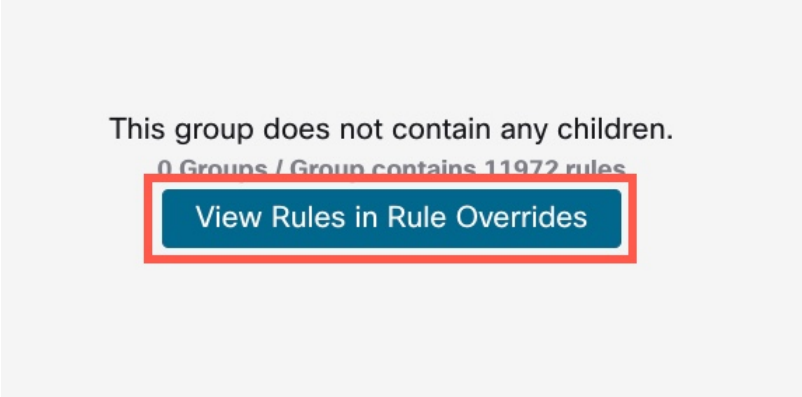


步骤 12 在**企业 (Enterprise)** 下，点击**初始访问权限 (Enterprise)** 将其展开。

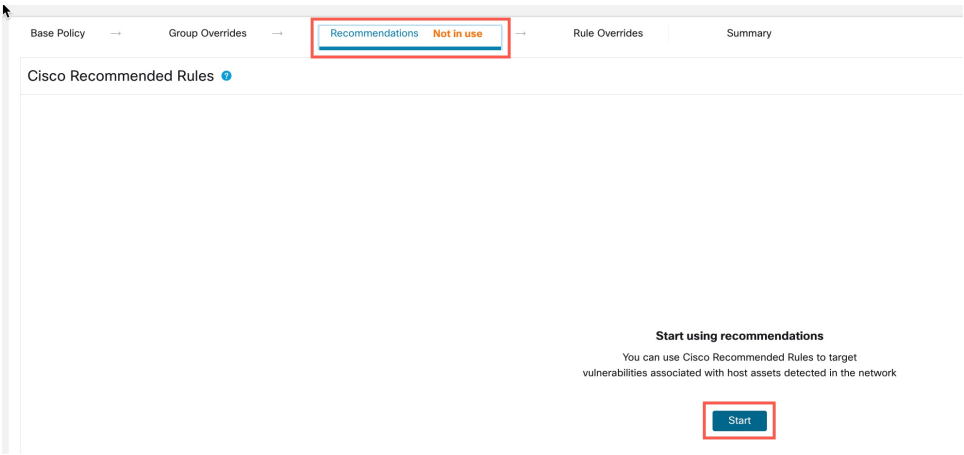
步骤 13 在**初始访问权限 (Initial Access)**下，点击**漏洞攻击面向公众的应用 (Exploit Public-Facing Application)**，这是最后一个枝叶组。



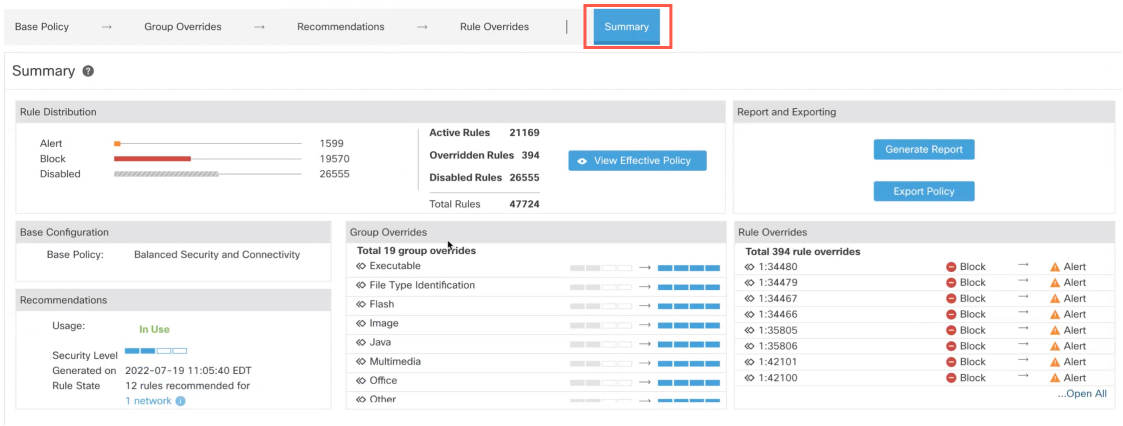
步骤 14 点击**查看规则覆盖中的规则 (View Rules in Rule Overrides)** 以查看不同规则的不同规则、规则详细信息、规则操作等。您可以在**规则覆盖 (Rule Overrides)** 层中更改一个或多个规则的规则操作。



步骤 15 点击**推荐 (Recommendations)** 层，然后点击**开始 (Start)** 以开始使用思科推荐的规则。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。有关详细信息，请参阅在 Snort 3 生成新的 Cisco Secure Firewall 建议，第 64 页。



步骤 16 点击 **摘要** 层可查看当前策略更改的整体视图。根据规则覆盖、安全级别更改和思科推荐规则的生成，您可以查看策略的规则分布、组覆盖、规则覆盖、规则建议等，以验证更改。



下一步做什么

部署入侵策略以检测和记录 Snort 规则触发的事件。请参阅部署配置更改，第 25 页。

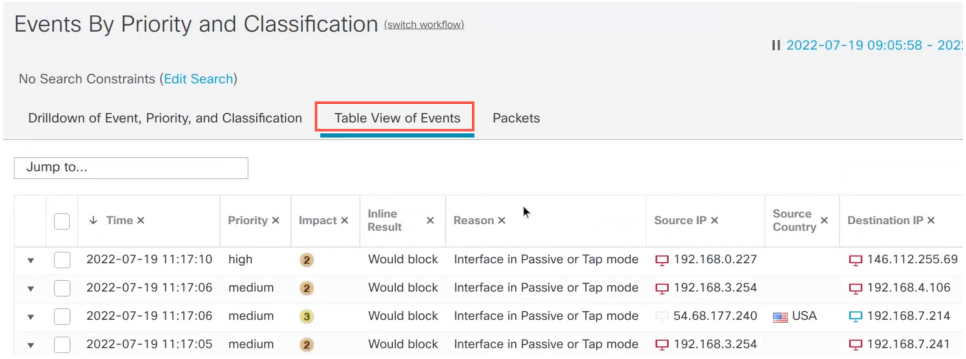
查看入侵事件

您可以在**经典事件查看器 (Classic Event Viewer)** 和**统一事件查看器 (Unified Event Viewer)** 页面上查看入侵事件中的 MITRE ATT&CK 技术和规则组。Talos 提供从 Snort 规则 (GID:SID) 到 MITRE ATT&CK 技术和规则组的映射。这些映射作为轻量级安全软件包 (LSP) 的一部分安装。

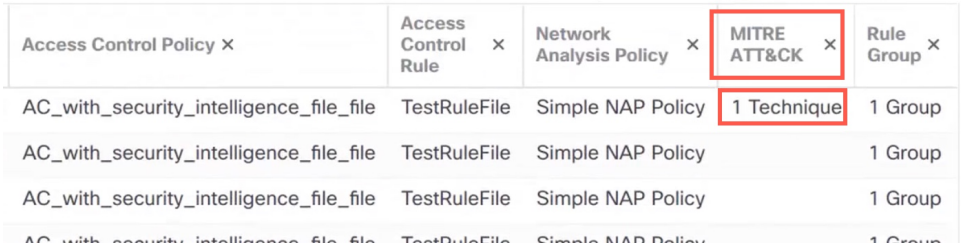
过程

步骤 1 点击**分析 (Analysis)**，然后选择**入侵 (Intrusions)** 下的**事件 (Events)**。

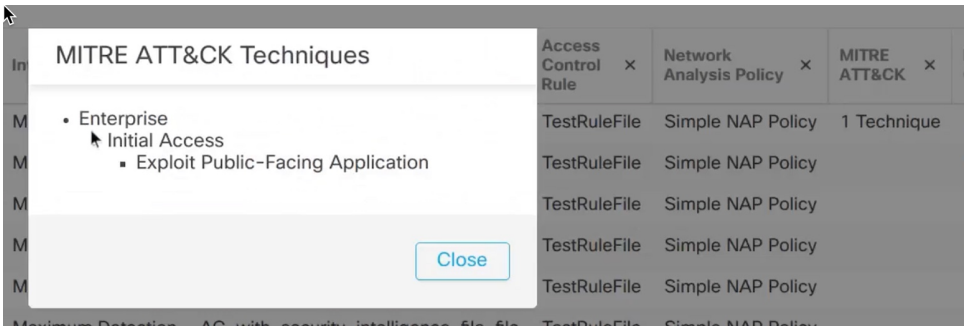
步骤 2 点击**事件的表视图 (Table View of Events)** 选项卡。



步骤 3 在 **MITRE ATT&CK**下，您可以看到入侵事件的技术。点击 **1 技术 (1 Technique)** 以查看 MITRE ATT&CK 技术。



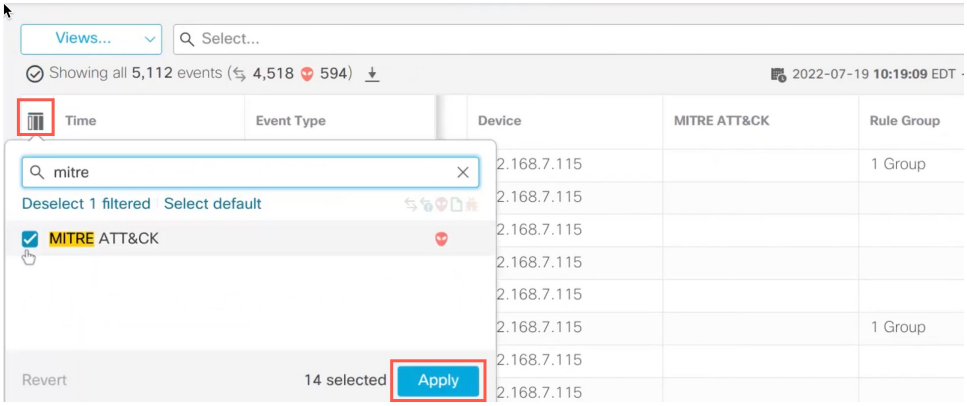
在本例中，攻击技术是**面向公众的应用 (Exploit Public-Facing Application)**。



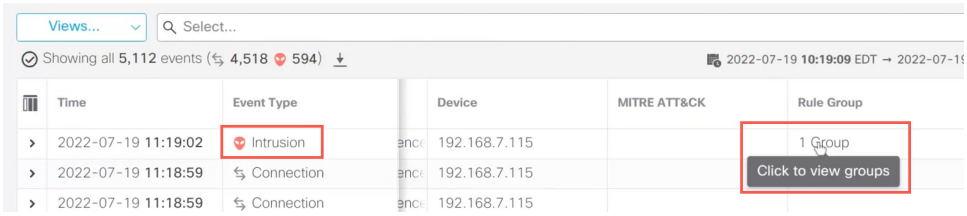
步骤 4 点击**关闭 (Close)**。

步骤 5 点击**分析 (Analysis)**，然后选择**统一事件 (Unified Events)**。

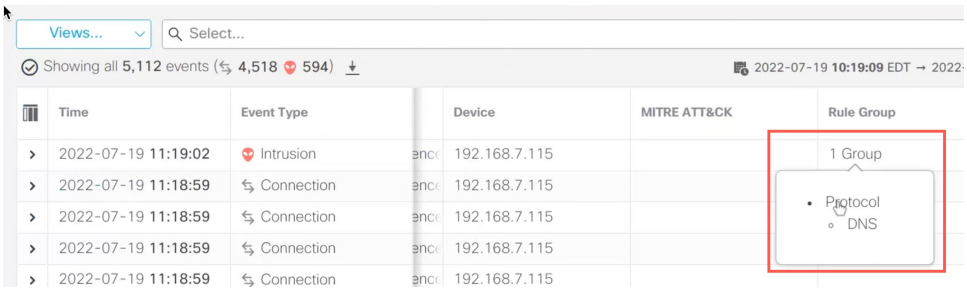
步骤 6 如果未启用，请点击列选择器图标以启用 **MITRE ATT&CK** 和**规则组 (Rule Group)** 列。



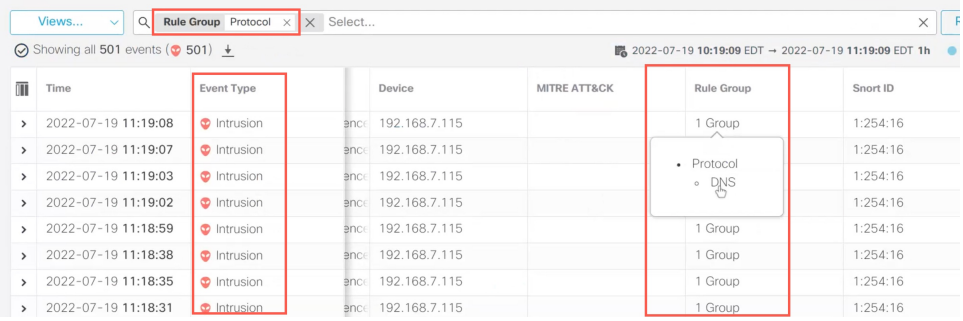
步骤 7 在本示例中，入侵事件由映射到一个规则组的事件触发。点击**规则组 (Rule Group)** 列下的 **1 组 (1 Group)**。



步骤 8 您可以查看**协议 (Protocol)**（父规则组）及其下的 DNS 规则组。选择**协议 (Protocol)** > **DNS** 以搜索具有至少一个规则组的所有入侵事件。



屏幕上会显示搜索结果。



其他参考资料

- Snort 3 中的入侵策略
- 编辑 Snort 3 入侵策略， 第 33 页
- 恶意软件事件中的 MITRE 信息

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。