在FMC上配置其他Snort 3规则操作

目录

简介

本文档介绍Firepower管理中心(FMC)对7.1版本中添加的其他Snort 3规则操作功能的支持。

背景信息

虽然Firepower威胁防御(FTD)在7.0中支持七个入侵策略规则操作警报/禁用/阻止/拒绝/重写/传递/丢弃，但FMC仅支持三个Snort 3规则操作："警报"、"禁用"和"阻止"。

在Firepower 7.1.0中，FMC支持配置新规则操作。

先决条件

要求

Cisco 建议您了解以下主题：
·了解开源Snort
· Firepower管理中心(FMC)7.1.0+
· Firepower威胁防御(FTD)7.0.0+

使用的组件

本文档中的信息基于以下软件和硬件版本：
·本文档适用于运行Snort 3的所有Firepower平台
·运行软件版本7.4.2的思科Firepower威胁防御虚拟(FTD)
·运行软件版本7.4.2的Firepower管理中心虚拟(FMC)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

功能详细信息

添加的新Snort 3规则操作及其说明如下：

密码：不生成事件，允许数据包通过，无需任何后续Snort规则进行进一步评估。

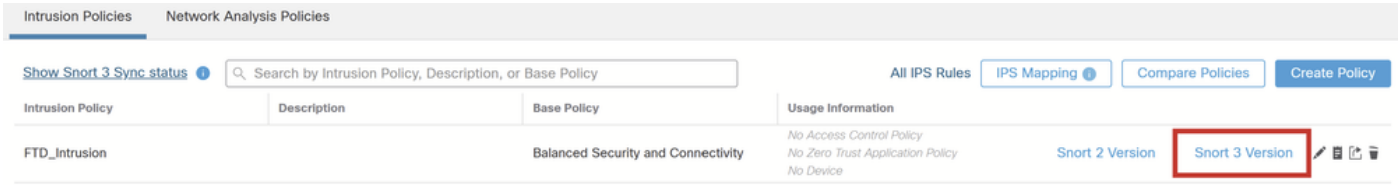
丢弃：生成事件，丢弃匹配的数据包，并且不阻止此连接中的其他流量。

拒绝：生成事件、丢弃匹配数据包、阻止此连接中的进一步流量，并向源主机和目的主机发送TCP重置或ICMP端口不可达。

重写：根据规则中的replace选项生成事件并覆盖数据包内容。

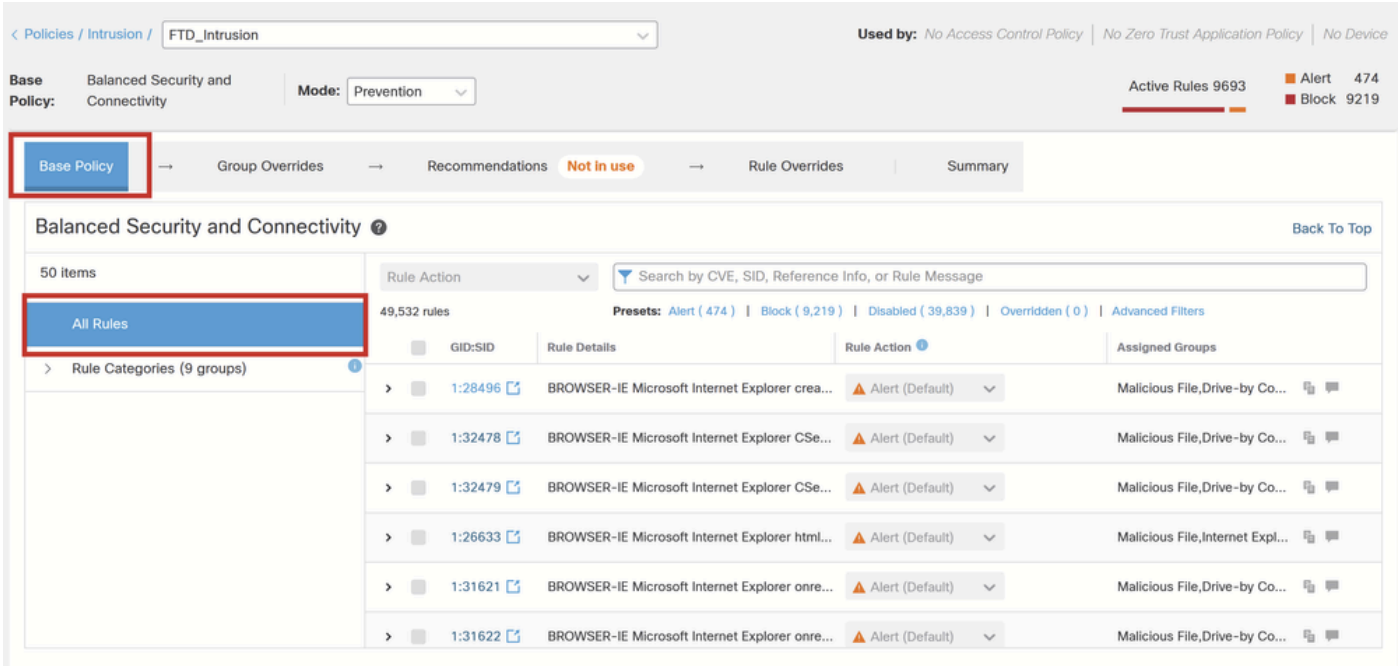
FMC演练

要查看入侵策略中的Snort 3规则，请导航至FMC Policies > Access Control > Intrusion,此，点击策略右上角的Snort 3版本选项，如图所示：



Snort 3版本

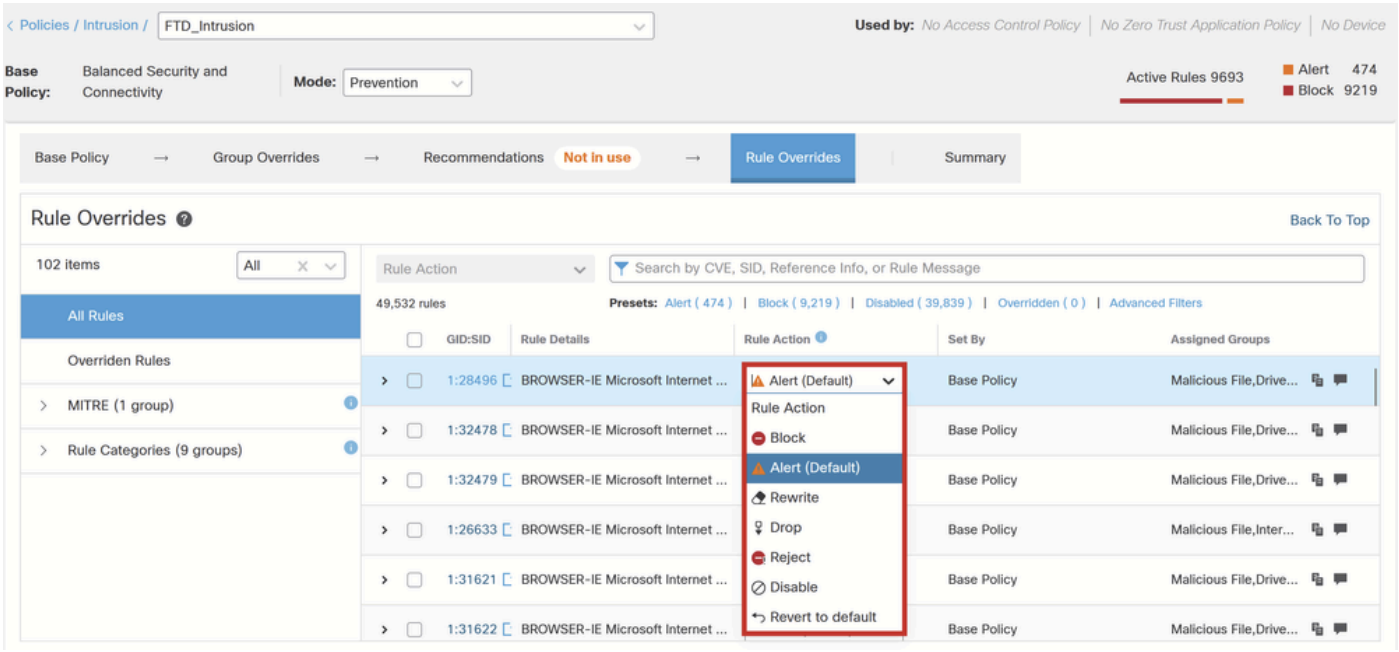
单击Base Policy > All Rules，可以看到所有系统定义的Snort 3规则的默认操作。



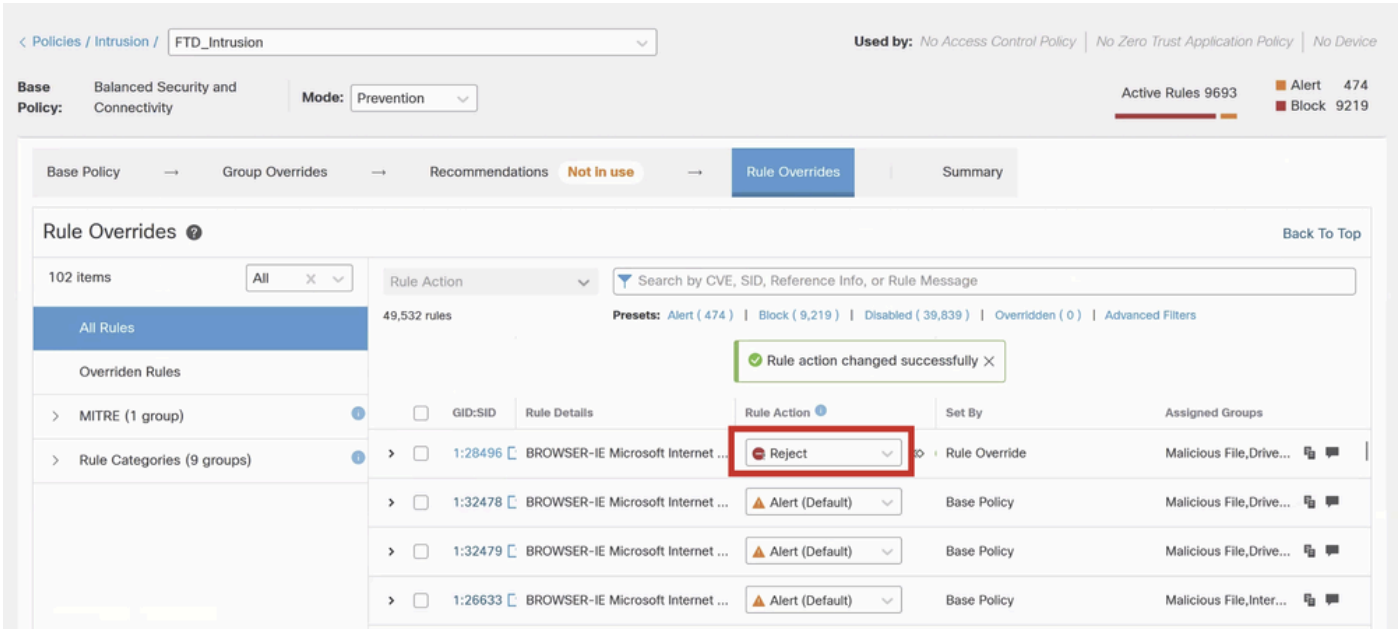
基本策略

要将规则操作更改为任何这些新规则操作，请导航到规则覆盖>所有规则，然后从所选规则的下拉列

表中选择规则操作。

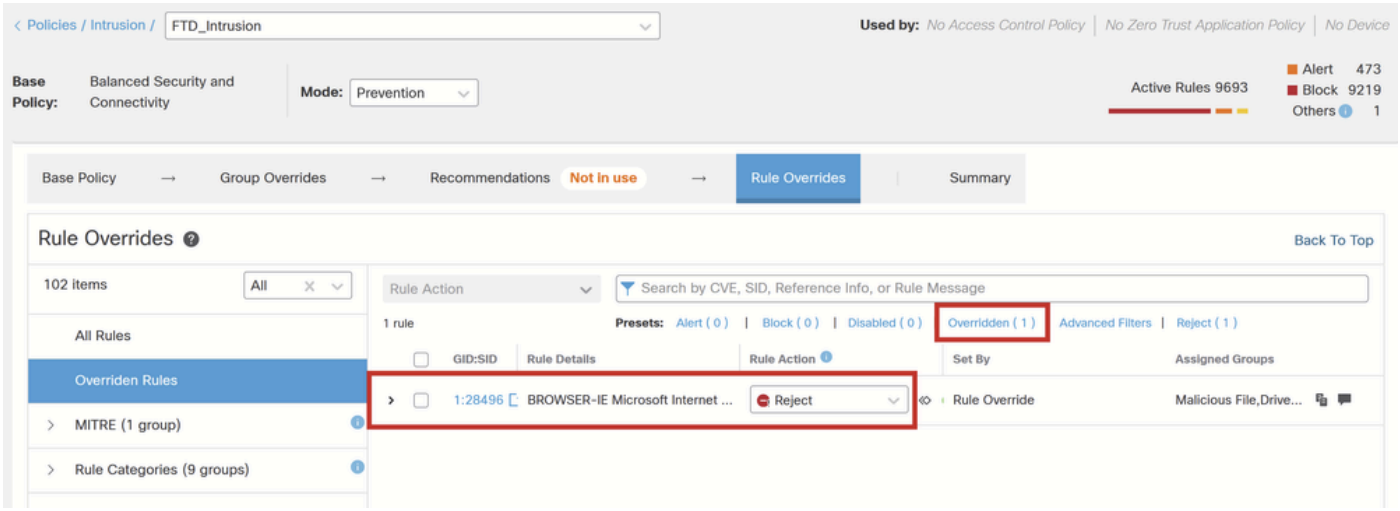


其他规则操作



更改规则操作

在Rule Overrides > Overridden Rules下可以找到被覆盖的规则。


Policies / Intrusion /
FTD_Intrusion
Used by: No Access Control Policy | No Zero Trust Application Policy | No Device
Base Policy: Balanced Security and Connectivity
Mode: Prevention
Active Rules 9693
Alert 473
Block 9219
Others 1
Base Policy → Group Overrides → Recommendations Not in use → Rule Overrides | Summary
Rule Overrides
Back To Top
102 items
All
All Rules
Overriden Rules
MITRE (1 group)
Rule Categories (9 groups)
Rule Action
Search by CVE, SID, Reference Info, or Rule Message
1 rule
Presets: Alert (0) | Block (0) | Disabled (0) | Overridden (1) | Advanced Filters | Reject (1)
GID:SID
Rule Details
Rule Action
Set By
Assigned Groups
1:28496
BROWSER-IE Microsoft Internet ...
Reject
Rule Override
Malicious File,Drive...

覆盖规则

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。