在Web策略管理的基于规则的策略中配置规则操作

目录

简介

本文档介绍如何在基于规则的策略中为Web策略管理配置规则操作。

概述

基于规则的策略使用基于身份匹配的规则集。每个规则集包含规则，每个规则根据身份、目标和计划进行匹配。系统以自上而下的优先级顺序应用规则集和规则。标识与第一个适用的规则集匹配，然后应用与标识、目标和计划匹配的第一个规则。

通过基于规则的策略中的新功能，管理员可以将允许、警告、阻止或隔离操作分配给特定目标和应用的规则身份。

有关如何配置规则集和规则的说明，请参阅管理Web策略文档。

操作:允许、允许（安全）、警告、阻止和隔离

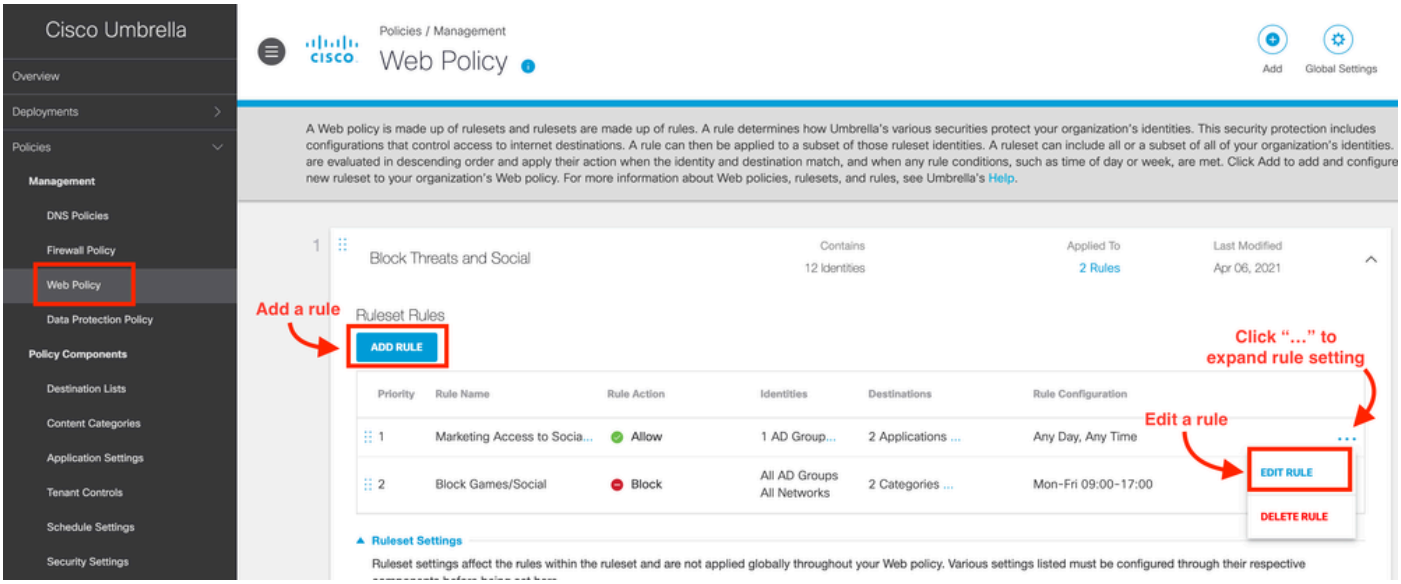
可以将以下操作之一分配给规则集中的单个规则：

允许（安全）	除非检测到安全问题，否则允许访问目标或应用。文件检测和安全类别仍然适用。除非选择安全覆盖，否则这是“允许”的默认操作。
允许	允许访问目标或应用程序，而不提供安全保护。不能覆盖整个内容类别的安全设置。
警告	通过警告页面和继续选项提供规则身份，而不是阻止访问。
阻止	拒绝对目标的访问。规则标识无法覆盖或继续超过阻止页面。
隔离	基于云的浏览器不阻止来自目标端点的身份，而是托管该目标的浏览会话。

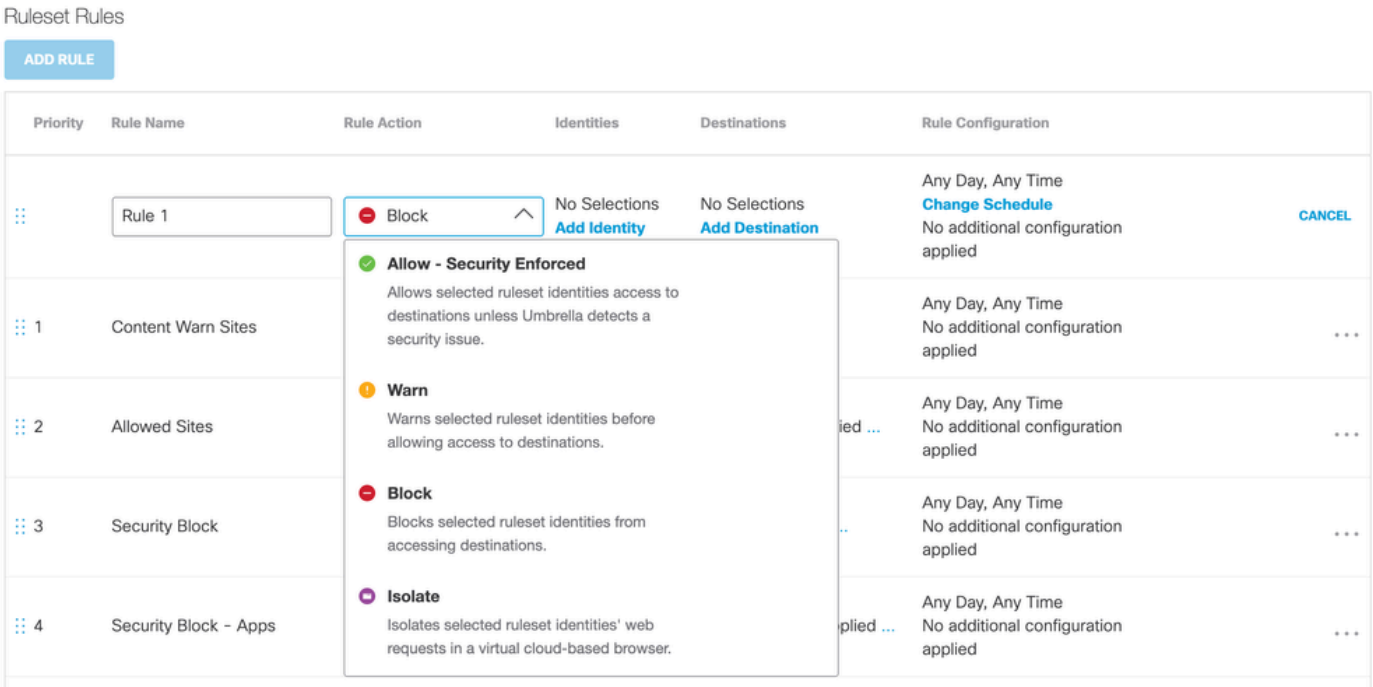
设置规则操作

创建或编辑规则时选择规则操作。

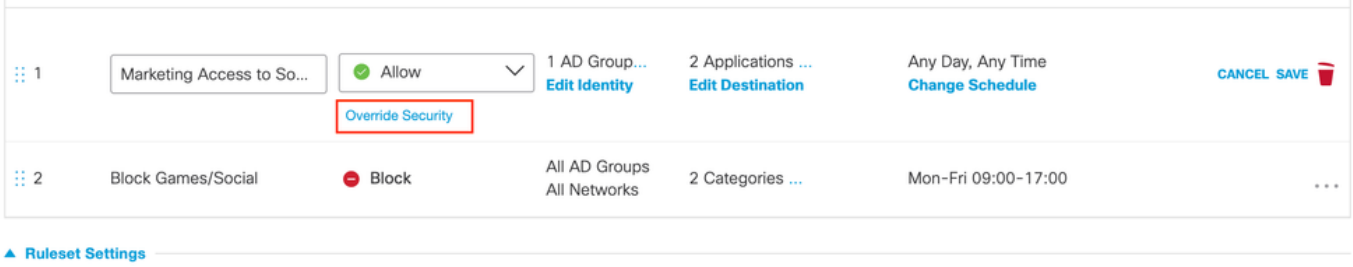
1. 转至Web Policy > [选择适当的规则集]。
2. 点击Add Rule或Edit Rule。



3. 在下拉菜单中，为目标选择Allow、Warn、Block或Isolates。



- “allow”的默认设置应用安全策略，并在检测到威胁时阻止目标。
- 要允许无安全保护的访问，请选择“覆盖安全”选项。



有关详细信息，请访问Umbrella Learning Hub，观看有关基于规则的策略的视频。

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）。