配置警告规则操作

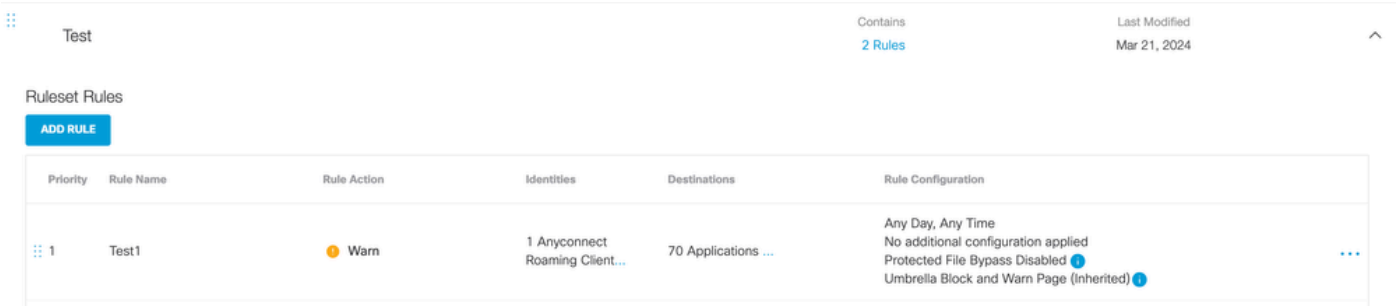
目录

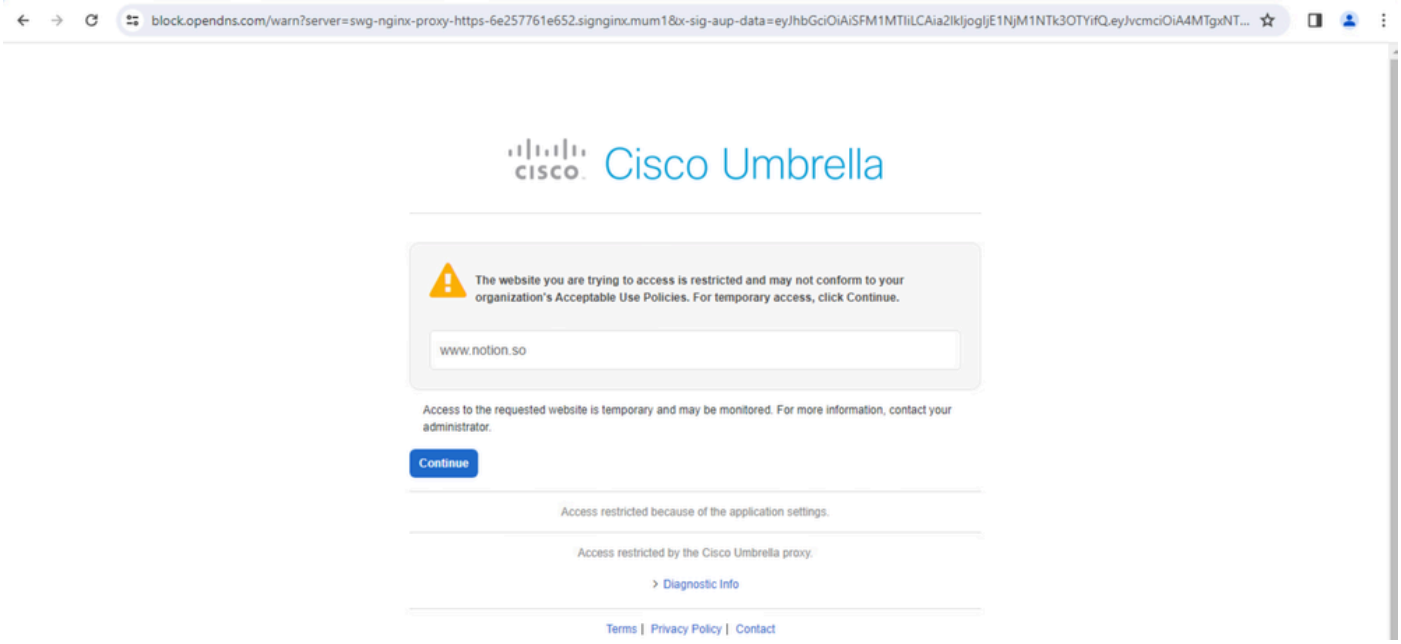
简介

本文档介绍对Cisco Umbrella中的警告规则操作功能、其配置和相关限制的全面了解。

概述

当用户尝试访问Cisco Umbrella中“警告”(Warn)类别下的网站时，会遇到“警告”(Warn)页面。要继续，用户必须单击浏览“警告”页面。



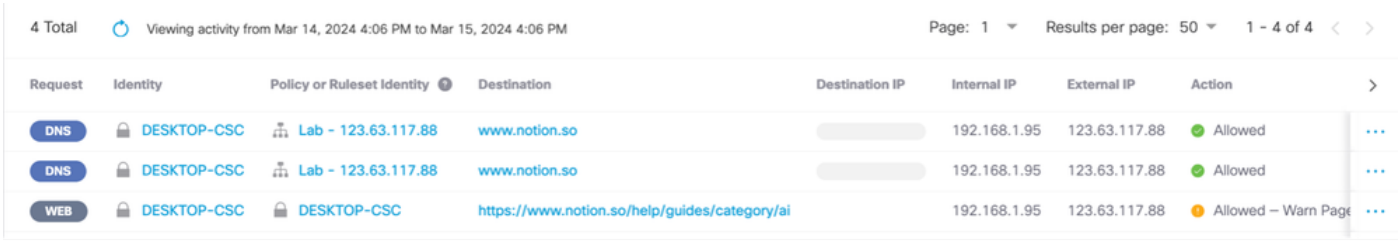


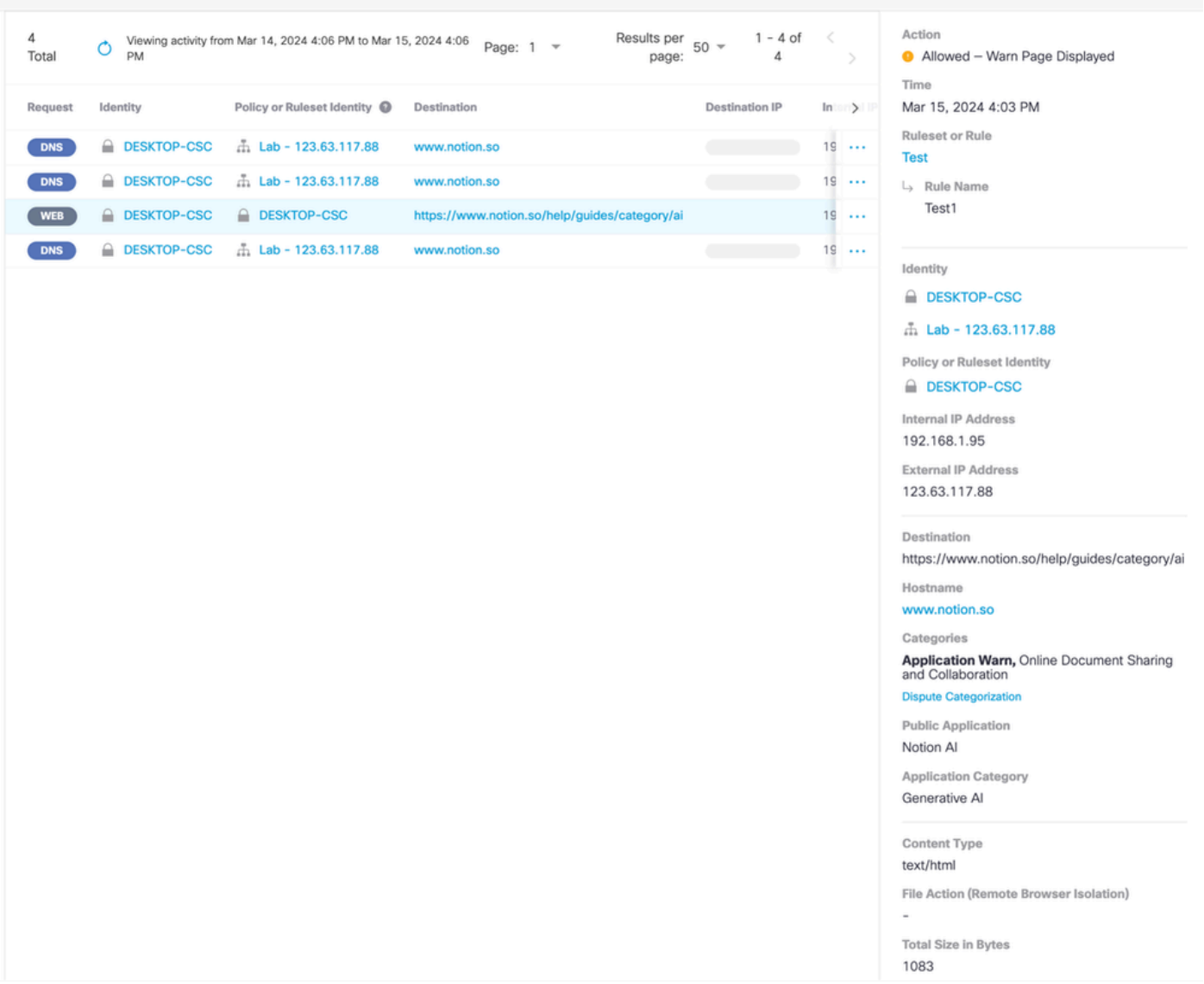
访问持续时间

点击“警告”(Warn)页面后，系统授予对请求目标的访问时间为一小时。经过此阶段后，系统将重新显示“警告”(Warn)页面，要求用户再次点击以继续访问。

活动报告概述

警告页面交互记录在Umbrella的活动报告内，为管理员提供对用户交互和警告规则的操作功能触发的警告的见解。





目标列表限制

启用警告页面功能会限制对目标列表的访问。用户无法为分类在“警告”下的网站选择“目标列表”选项。

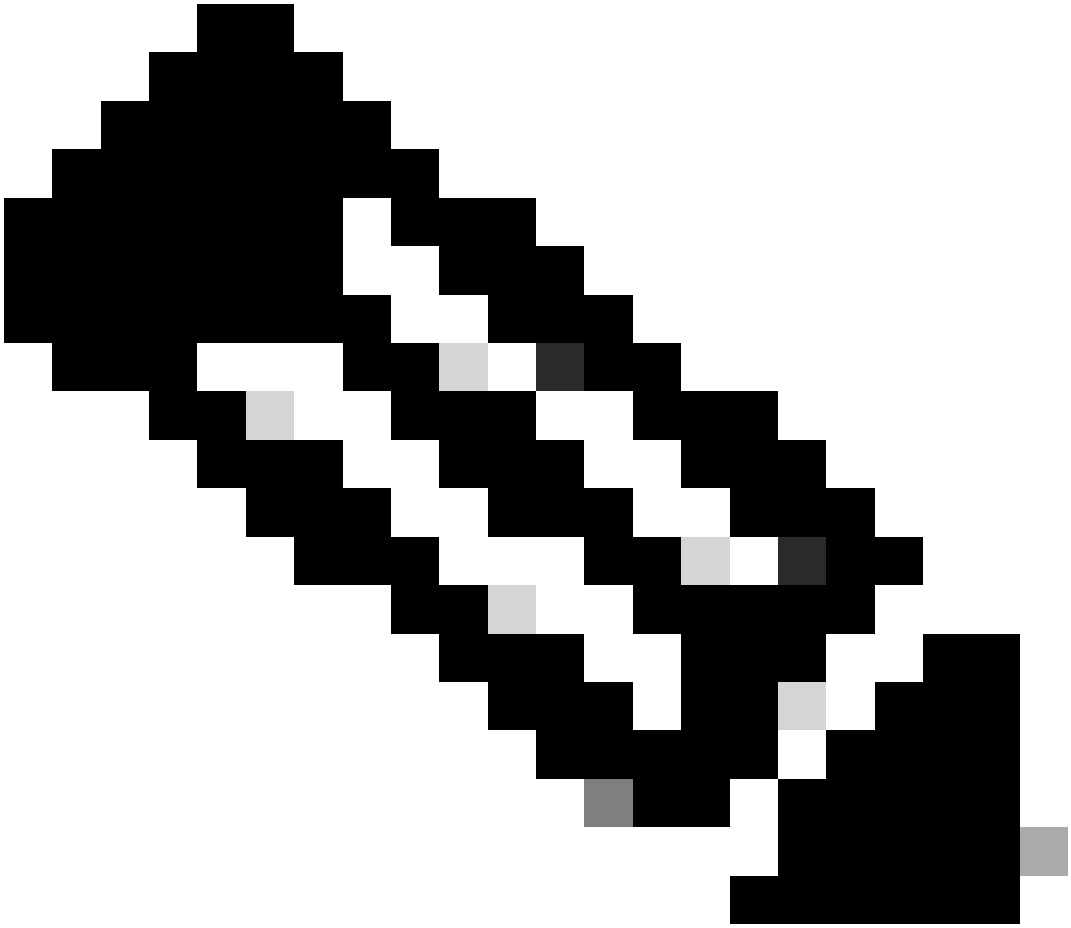
启用HTTPS检测

要有效实施“警告”页面功能，必须在Cisco Umbrella中启用HTTPS检查。HTTPS检测会解密并检测HTTPS流量，从而使Umbrella对加密连接强制执行“警告”页面。

创建自定义警告页面

管理员可以选择创建包含个性化消息传送的自定义“警告”页面。向规则集添加规则时，可以选择此自定义“警告”页面，为用户提供定制的警告体验。

有关创建自定义Warn页面的详细说明，以及有关Warn规则操作配置的详细信息，请参阅官方文档：创建自定义警告页面。



注意：任何选择性解密列表例外都会影响代理执行某些策略和功能的能力，警告页面就是其中之一。

结论

了解Warn规则操作配置和相关限制对于在Cisco Umbrella中实施有效的安全策略至关重要。通过利用警告页面和HTTPS检测，组织可以增强其安全状态并确保用户的安全浏览体验。

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）。