配置文件检查器允许受密码保护的文件和其他非恶意文件

目录

简介

本文档介绍如何防止非恶意文件被文件检测阻止。

问题

在某些情况下，启用“文件检查”会阻止非恶意文件。这些文件类型包括：

- 受密码保护的文件
- 可能有害的应用程序（已损坏）文件

这些文件被Umbrella阻止，因为防病毒工具无法对这些文件进行解压缩和扫描。受密码保护的文件可能显示在“受保护文件”类别下。损坏的文件可能包括包含加密内容、无法提取的存档内容、无效的压缩数据或无效的存档标头，或者只是以不受支持的格式压缩或存档的文件。虽然这些文件可能是非恶意的，但默认情况下Umbrella会阻止这些文件以防万一，因为文件无法扫描。

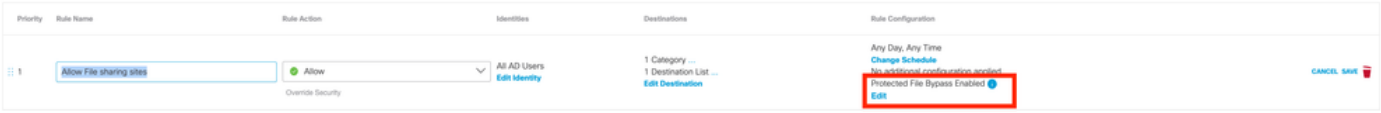
解决方案

如果您知道某个非恶意文件由于上述原因之一而被阻止，可以通过允许受保护的文件来解决此问题。现在可以在全局级别或在单个Web规则中更改阻止受保护文件的行为。

- Rule(Recommended) — 允许身份和/或目标的受保护文件。 如果要信任来自特定目标的受保护文件，或希望覆盖单个用户/组的行为，请执行此操作。
- 全局 — 允许所有规则/规则集中的所有用户使用受保护文件。 如果您接受下载受保护文件的风险，并宁愿选择此选项，而不愿承担进行更精细的例外处理的管理负担，请执行此操作。

规则

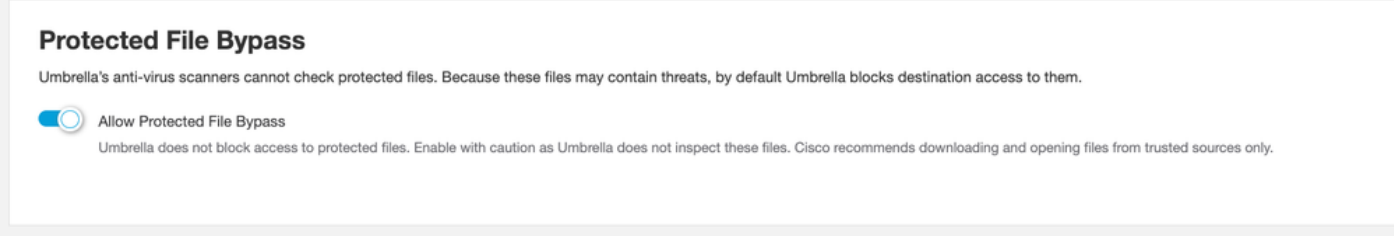
通过在Policies > Web Policies页面上编辑Web规则可以更改功能。



10588971481748

全局

可以在Policies > Web Policies > Global Settings中更改功能。

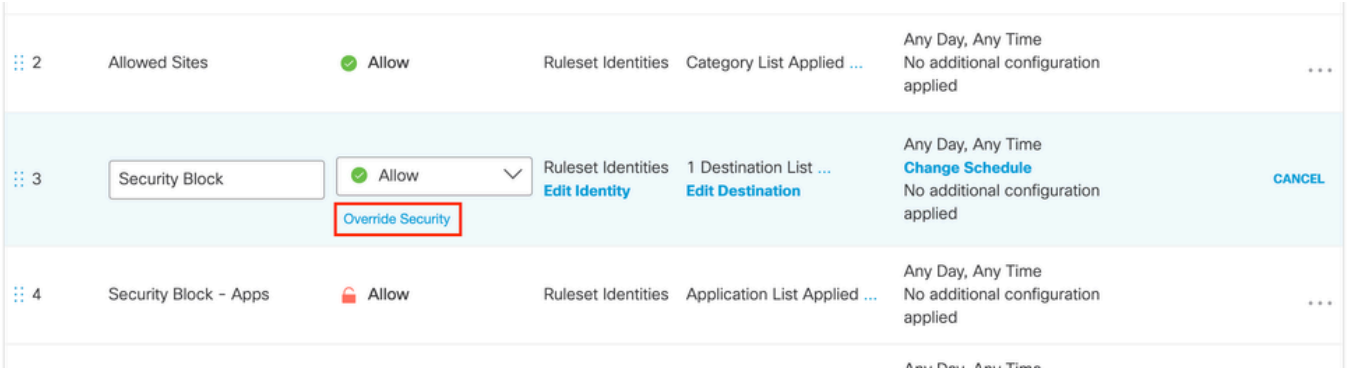


10589018672020

替代解决方案

还可以使用Override Security选项绕过任何Web策略中的文件检查问题。此选项必须谨慎使用，因为它会禁用所有其他安全设置，包括阻止恶意文件。

- 对于受保护文件，请使用本文档中介绍的解决方案之一。
- 仅在您完全信任目标且没有其他解决问题选项的情况下使用此选项。
- 对于防病毒误报，在实施任何变通方法之前，先从Cisco Talos中确认文件是安全的。



Screen_Shot_2021-10-07_at_2.59.04_PM.png

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）。