安全访问安全配置文件解密要求（用于警告操作）

目录

问题

用户需要思科安全访问的配置指南，内容涉及当Access Policy操作设置为Warning时，是否必须在Security Profile设置中启用Decryption。具体问题适用于以下安全配置文件功能：

- 威胁类别
- 文件检查
- Cisco Secure Malware Analytics
- 文件类型阻止
- 安全搜索

问题的核心是了解访问策略警告操作和安全配置文件解密要求之间的关系，以便这些安全功能正常运行。

环境

- 产品:思科安全互联网接入优势
- 技术：安全访问
- 软件版本:全部
- 配置:具有各种安全功能的安全配置文件
- 策略配置：具有警告操作设置的访问策略

分辨率

实验室验证确认，即使在安全配置文件中仅启用了解密，并且禁用所有其他功能，访问策略警告操作仍能正常工作。这意味着对于这些安全配置文件功能，在使用警告操作时，不需要为每个单独功能专门启用解密：

- 威胁类别
- 文件检查
- Cisco Secure Malware Analytics
- 文件类型阻止
- 安全搜索

配置指南

配置带有警告操作的访问策略时：

步骤 1：将所需策略规则的Access Policy操作配置为Warning。

步骤 2：在安全配置文件设置中，确保在配置文件级别启用解密。

步骤 3：单个安全功能（威胁类别、文件检查、思科安全恶意软件分析、文件类型阻止和安全搜索）可以在其特定解密设置中保持禁用状态，同时仍通过警告操作正常运行。

此配置方法允许警告操作正常运行，同时保持安全配置文件功能管理的灵活性。

原因

访问策略中的警告操作与单个安全配置文件功能解密要求不同。Warning操作可以在仅在Security Profile级别启用主解密设置的情况下运行，无需对每个特定安全功能单独启用解密。

相关内容

- 思科技术支持和下载

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）。