安全访问受密码保护的ZIP文件下载配置

目录

问题

迁移到思科安全访问后，用户无法下载受密码保护（加密）的ZIP文件。尝试通过Secure Access服务访问加密文件内容时，下载始终失败。尽管在C8200设备上配置了多个安全规则（包括基于类别的阻止、SSL检查控制和沙盒功能）的互联网绑定流量策略，但仍会发生此问题。

用户尝试访问之前在Secure Access迁移之前可访问的受密码保护的ZIP文件时，会遇到完全下载失败。此问题在多个隧道组之间持续存在并影响所有15个已配置位置。

环境

- 思科安全访问(安全访问OrgID:8320925）
- 管理互联网绑定流量策略的C8200设备
- 跨15个位置（TK-TG和其他）的多个隧道组
- 同时具有启用和禁用配置的SSL检查策略
- 在某些策略上启用的沙盒安全配置文件
- 根据特定访问规则配置的IPS配置文件

分辨率

在Cisco Secure Access中允许使用密码保护的ZIP文件下载的解决方案包括配置Allow access to encrypted files设置并在必要时实施适当的解决方法。

主要配置方法

步骤 1：访问思科安全访问策略配置

导航到处理思科安全访问控制面板中受影响流量的特定访问策略。

步骤 2：启用加密文件访问

在Advanced Settings策略中，找到并启用Allow access to encrypted files选项。此设置基于每个规则进行配置，并控制是否可以通过该特定策略访问加密内容。

步骤 3：应用配置

保存并应用策略更改，使其对用户流量有效。

替代解决方法

如果主要方法不能解决问题，请实施以下各节中介绍的解决方法。

步骤 1：识别受影响的URL

确定托管密码保护ZIP文件并导致下载失败的特定URL或域。

步骤 2：配置不解密列表

将已识别的URL添加到Cisco安全访问配置中的Do Not Decrypt列表。这将阻止对这些特定URL进行SSL检查。

步骤 3：创建SSL检测旁路策略

确保已配置禁用了SSL检查的访问策略，以处理流向这些URL的流量。

此策略必须：

- 已禁用SSL检查
- 已禁用所有安全配置文件
- 比启用SSL检查的策略优先级更高

策略配置参考

以下各小节中概述的策略顺序及其各自的配置可用作正确处理流量的参考。

策略1:基于类别的阻止规则

- 策略名称：IA到InternetContentBlock
- IPS配置文件：无
- 目的:阻止特定内容类别
- 目标：所有隧道组

策略2:SSL检查禁用规则

- 策略名称：IA-SSL-Inspection-MUKOU

- IPS配置文件：禁用
- 安全配置文件：全部禁用
- 目标：所有隧道组

策略3:启用SSL检查的规则

- 策略名称：IA-SSL-Inspection
- IPS配置文件：启用
- 安全配置文件：沙盒功能已启用
- 目标：所有隧道组

重要配置说明

Allow access to encrypted files功能不存在等效的全局设置。此设置必须根据需要在各个访问策略上进行配置。要求加密文件访问的每个策略都必须在其高级设置配置中明确启用此设置。

测试配置更改时，在验证功能之前，请留出足够的时间在思科安全访问基础设施中传播策略。服务事件或维护窗口会影响测试结果，在排除故障时必须予以考虑。

原因

发生此问题的原因是，默认情况下，思科安全访问会阻止对加密文件的访问作为一项安全措施。启用SSL检查并遇到受密码保护或加密的内容时，除非明确配置为允许此类访问，否则服务将阻止下载。访问策略的Advanced Settings中的Allow access to encrypted files设置控制此行为，如果未启用此设置，则会在下载过程中阻止加密ZIP文件和类似内容。

此外，当检查进程无法正确处理加密内容时，SSL检查策略可能会干扰加密文件下载，需要对受影响的URL进行加密文件访问设置或SSL检查绕行。

相关内容

- 高级安全控制
- 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）。