安全訪問受密碼保護的ZIP檔案下載配置

目錄

問題

遷移到Cisco Secure Access後，使用者無法下載受密碼保護（加密）的ZIP檔案。嘗試通過Secure Access服務訪問加密檔案內容時，下載始終失敗。儘管在C8200裝置上配置了多個安全規則（包括基於類別的阻止、SSL檢查控制和沙盒功能）的網際網路繫結流量策略，但仍會發生此問題。

使用者嘗試訪問在Secure Access遷移之前可訪問的受密碼保護的ZIP檔案時，會遇到完全下載失敗。此問題在多個隧道組之間仍然存在，影響所有15個已配置的位置。

環境

- 思科安全訪問(安全訪問OrgID:8320925)
- 管理網際網路繫結流量策略的C8200裝置
- 跨15個地點的多個隧道組（TK-TG和其他）
- 同時具有啟用和禁用配置的SSL檢查策略
- 在某些策略上啟用的沙盒安全配置檔案
- 根據特定訪問規則配置的IPS配置檔案

解析

在Cisco Secure Access中，允許下載受密碼保護的ZIP檔案的解決方案涉及配置Allow access to encrypted files設定並在必要時實施適當的解決方法。

主要配置方法

步驟 1:訪問思科安全訪問策略配置

導航到處理Cisco Secure Access控制面板中受影響流量的特定訪問策略。

步驟 2:啟用加密檔案訪問

在Advanced Settings策略中，找到並啟用Allow access to encrypted files選項。此設定基於每個規則進行配置，並控制是否可以通過該特定策略訪問加密內容。

步驟 3:套用組態

儲存並應用策略更改，使其對使用者流量有效。

替代解決方法

如果主要方法不能解決此問題，請實施下一節中介紹的解決方法。

步驟 1:識別受影響的URL

確定託管受密碼保護的ZIP檔案並導致下載失敗的特定URL或域。

步驟 2:配置不解密清單

將識別的URL新增到Cisco Secure Access配置中的Do Not Decrypt清單中。這可防止對這些特定URL進行SSL檢查。

步驟 3:建立SSL檢查繞過策略

請確保已配置禁用SSL檢查的訪問策略以處理到這些URL的流量。

此策略必須具有：

- 已禁用SSL檢查
- 已禁用所有安全配置檔案
- 優先順序高於啟用SSL檢查的策略

策略配置參考

下一小節中概述的策略順序及其各自的配置可用作正確流量處理的參考。

策略1:類別型封鎖規則

- 策略名稱：IA到Internet內容塊
- IPS配置檔案：無
- 目的:阻止特定內容類別
- 目標：所有隧道組

策略2:SSL檢查禁用規則

- 策略名稱：IA-SSL-INSPECTION-MUKOU

- IPS配置檔案：已停用
- 安全配置檔案：所有已禁用
- 目標：所有隧道組

策略3:啟用SSL檢查的規則

- 策略名稱：IA-SSL-Inspection
- IPS配置檔案：已啟用
- 安全配置檔案：沙盒功能已啟用
- 目標：所有隧道組

重要配置說明

Allow access to encrypted files 功能不存在等效的全域性設定。此設定必須根據需要在各個訪問策略上配置。要求加密檔案訪問的每個策略都必須在其高級設定配置中顯式啟用此設定。

測試配置更改時，在驗證功能之前，請留出足夠的時間在思科安全訪問基礎設施中傳播策略。服務事件或維護視窗會影響測試結果，在排除故障時必須考慮這些因素。

原因

發生此問題的原因在於，思科安全訪問預設情況下會阻止對加密檔案的訪問，作為一項安全措施。啟用SSL檢查並遇到受密碼保護或加密的內容時，除非明確配置為允許此類訪問，否則服務將阻止下載。訪問策略的「高級設定」中的允許訪問加密檔案設定控制此行為，如果未啟用此設定，則會在下載過程中阻止加密的ZIP檔案和類似內容。

此外，當檢查過程無法正確處理加密內容時，SSL檢查策略可能會干擾加密檔案下載，需要對受影響的URL執行加密檔案訪問設定或SSL檢查繞行。

相關內容

- 高級安全控制
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。