安全訪問應用協定阻止阻止網際網路連線

目錄

- 問題
- 環境
- 解析
  - 步驟 1:確定阻止規則
  - 步驟 2:修改應用程式設定
  - 步驟 3:應用並驗證更改
- 原因
- 相關內容

問題

遷移到Cisco Secure Access後，使用者在嘗試訪問Web服務時遇到了網際網路連線被阻止的情況。特定症狀包括HTTP流量被安全策略阻止，從而阻止對合法網站和應用的訪問。

阻止事件詳細資訊顯示以下特性：

- Action:已阻止
- 事件阻止原因：AC_RULE_MATCH_LOCK
- 目標：http://www.bing.com/api/shopping/v1/user/shoppingsettings
- 目的地連線埠：443
- 類別：未分類

- 應用程式類別：搜尋
- 應用協定：超文字傳輸通訊協定
- 通訊協定：TCP

環境

- 思科安全訪問部署
- 具有應用協定限制的活動安全策略

解析

解決方法涉及修改安全規則配置以允許HTTP應用協定流量，同時維護真正不可信應用的安全狀態。

步驟 1:確定阻止規則

在安全訪問管理介面中查詢導致阻止的特定規則：

- 規則名稱:測試
- 當前配置:使用應用程式設定塊作為目標。

步驟 2:修改應用程式設定

訪問規則配置並檢查目標中的應用程式設定的名稱：

- 導航到資源>Internet和SaaS資源>應用程式清單。然後，按一下應用程式。
- 找到應用協定設定。

- 取消選中或從阻止的應用程式協定清單中刪除HTTP。
- 確保為實際不可信應用程式保留其他安全控制。

步驟 3:應用並驗證更改

儲存規則修改並測試連通性：

1. — 將配置更改應用於活動策略。

2. — 測試到以前被阻止的目的地的Internet連線。

3. — 監控安全日誌，確保現在允許合法的HTTP流量。

4. — 驗證其他安全保護是否仍然有效。

原因

根本原因是思科安全訪問中的安全規則配置過於嚴格。規則配置為阻止所有HTTP應用協定流量，從而阻止合法的Web瀏覽和應用訪問。HTTP協定阻止的廣泛應用影響了正常的Internet連線，使使用者可以訪問合法的Web服務和使用HTTP/HTTPS協定的應用。

相關內容

- 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）。