使用SSE NATaaS輸出IP時，Web應用程式防火牆阻止訪問地域限制的網站

目錄

問題

嘗試通過Cisco Secure Access(SSE)訪問特定網站會生成一條阻止消息「對不起，您已被阻止」。

使用常規家庭Wi-Fi連線時，可以訪問該站點。懷疑的原因是遠端網站僅允許從特定IP地址範圍進行訪問，而SSE出口IP似乎超出了允許範圍。

技術調查顯示，該網站的Web應用程式防火牆(Cloudflare)阻止了整個安全訪問NATaaS輸出IP範圍，而不考慮國家/地區。該問題可重複出現，在使用SSE輸出IP時始終存在。

環境

- 技術：思科安全接入(SSE)與統一策略（網際網路策略、私有策略、DLP策略、RBI、安全配置檔案）配合使用
- 訪問路徑：SSE的任何資料中心
- 地理限制網站
- 安全控制：目標網站上的Web應用程式防火牆(Cloudflare)
- 從遠端網路（SSE出口IP）到本地網路（家庭Wi-Fi）的網際網路訪問
- 出現問題時未對Secure Access部署進行任何更改
- 觀察到的錯誤消息：「對不起，您已被阻止」

解析

要解決遠端站點阻止Cisco安全訪問NATaaS輸出IP而引起的訪問問題，建議使用此工作流。這些步驟可確保使用一種系統方法來識別阻止的性質，並探索可能的變通方法或解決方案。

第1步：確認錯誤消息和阻止行為

通過SSE訪問站點時，請注意以下消息：

```
sorry you have been blocked
```

第2步：驗證來自不同網路的網站可訪問性

從以下網址訪問該網站：

- 任何SSE資料中心（已阻止）
- 常規家庭Wi-Fi連線（可訪問）

第3步：確定負責阻止的安全控制

技術觀察：Cloudflare Web應用程式防火牆(WAF)正在阻止整個安全訪問NATaaS輸出IP範圍。

第4步：確認終端使用者使用的訪問路徑

確定用於將流量傳送到安全訪問的方法：

- 漫遊安全模組
- RAVPN通道
- 站點到站點VPN隧道
- PAC部署

第5步：瀏覽旁路或允許清單選項

檢查以下選項中是否有任何可能：

- 與目標網站管理員建立業務關係或聯絡，請求允許SSE出口IP清單。
- SSE輸出IP在文檔中列出：
- 可以使用不同輸出IP的備用訪問路徑未被WAF阻止。
- 從SSE代理繞過有問題的網站（具體步驟取決於用於將流量傳送到安全訪問的方法）

第6步：記錄觀察結果和後續步驟

記錄這些意見：

錯誤消息

訪問路徑和相應結果

與遠端站點管理員的通訊（如果允許）。

原因

此問題的根本原因是目標網站的Web應用程式防火牆(Cloudflare)正在主動阻止Cisco Secure Access(SSE)NATaaS出口IP範圍。此阻止不限於非以色列IP或地理定位過濾。相反，它針對與Cisco Secure Access關聯的整個已知出口IP範圍，很可能是出於遠端網站上的策略或安全配置的原因。因此，源自這些IP的任何流量都會被拒絕，無論其實際來源國家/地區或終端使用者位置如何。

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）。