零信任訪問和VPN連線的地理訪問限制

目錄

問題

需要零信任訪問(ZTA)和VPN連線的地理訪問限制的組織可以發現，在嘗試實施基於國家/地區的訪問控制時，需要禁用現有的ZTA和VPN策略。當策略因無法在安全SSE產品介面中定位本地地理限制選項而被禁用時，使用者會完全失去對所需資源的訪問許可權。使用內建產品功能無法配置限制訪問僅源自特定國家/地區的連線的特定要求，導致當試圖實施此類限制而停用現有策略時，使用者受到廣泛影響。

環境

- Cisco Secure Access Service Edge(SASE)/Secure SSE產品
- 零信任訪問(ZTNA)實施
- 需要地理訪問控制的VPN服務
- 專用資源訪問策略
- 需要針對特定國家/地區訪問限制的組織

解析

思科安全SSE產品目前不提供本地功能，無法根據使用者地理位置或國家/地區限制私有資源訪問。可考慮在下一部分中描述的方法來克服這一限制。

功能請求提交

必須向Cisco提交功能請求，才能為ZTA和VPN訪問新增地理限制功能。此增強請求由產品團隊評估，以確定是否可能包含在未來的版本中。組織可以與其思科客戶經理合作，根據業務需求確定這些功能請求的優先順序。

手動解決方法注意事項

可能的手動解決方法涉及將特定國家/地區的公有IP地址範圍新增為訪問策略中的網路對象組。

步驟 1:從相應的區域網際網路登錄檔(RIR)獲取國家/地區的公共IP地址範圍。

步驟 2:建立包含已標識IP範圍的網路對象組。在訪問策略配置中配置網路對象組，以包括分配給目標國家/地區的特定IP地址範圍。

步驟 3:將網路對象組應用於訪問策略。修改現有訪問策略以引用建立的網路對象組，從而有效地限制對源自指定IP範圍的連線的訪問。

重要限制

此手動方法具有重大限制，因為它依賴於靜態IP範圍定義，無法考慮可繞過地理限制的動態IP分配、移動使用者或VPN服務。此外，此方法需要持續維護，以確保IP範圍的準確性。

臨時策略管理

在永久解決方案可用之前，組織必須避免同時禁用所有ZTA和VPN策略。相反，請考慮實施分階段方法，其中關鍵訪問策略保持有效，而地理限制要求通過替代方法解決，或者等待產品改進。

原因

Cisco Secure SSE產品架構不包括用於專用資源訪問的本地地理訪問控制功能。產品訪問策略框架圍繞使用者身份、裝置狀態和基於網路的控制而設計，但不將地理位置作為策略實施引數。這表示產品功能差距，而不是配置問題或軟體缺陷。

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）。