ZTNA無客戶端源IP地址限制

目錄

問題

當嘗試對通過ZTNA無客戶端發佈的基於瀏覽器的應用程式實施訪問控制時，管理員會發現根據特定允許的公共IP地址限制訪問不能作為配置選項。要求是僅允許從指定的源IP地址進行訪問，同時阻止通過具有自定義域的ZTNA無客戶端訪問的應用程式的所有其他源IP。

環境

- 思科安全存取 — 零信任網路存取(ZTNA)
- ZTNA無客戶端（基於瀏覽器的訪問）
- 使用自定義域發佈的應用程式
- 所有受影響的軟體版本

解析

Cisco安全訪問平台不支援ZTNA無客戶端URL的源IP地址型訪問限制。此限制適用於通過ZTNA Clientless發佈的所有應用程式，無論它們使用的是自定義域還是標準ZTNA URL。

ZTNA無客戶端體系結構不提供在應用級別實施基於IP的訪問控制清單或允許清單功能的功能。訪問控制通過零信任框架內的其他身份驗證和授權機制進行管理，例如：

- 使用者身份驗證
- 裝置狀況評估
- 多重身份驗證

- 特定於應用程式的策略

需要基於IP的源訪問控制的組織可能需要考慮其他方法，或者等待將來可以包含此功能的產品增強功能。
請諮詢思科客戶團隊，以提出功能增強請求。

原因

ZTNA無客戶端服務架構的當前功能集不包括源IP地址過濾功能。這是產品限制，而不是配置問題。

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）。