通過與Meraki整合的安全訪問解決Azure託管的FQDN連線問題

目錄

問題

當使用者流量通過Meraki路由到Cisco Secure Access時，儘管安全訪問日誌顯示流量為「允許」，但無法訪問特定的Azure託管的FQDN。 此問題主要影響使用非標準埠連線到這些FQDN的RDP連線。

在安全訪問門戶中按FQDN搜尋日誌時，僅顯示DNS安全日誌，顯示「允許」狀態。但是，RDP連線到非標準埠上的相同目的地失敗。當FQDN解析為IP地址且Activity Search使用目標IP時，會顯示已阻止流量的雲防火牆日誌。

環境

- 整合Meraki的Cisco Secure Access(SSE)
- 具有本地分支功能的Meraki儀表板
- Azure託管的開發資源需要在非標準埠上進行RDP訪問
- 通過Meraki隧道路由到安全訪問的流量

解析

即時解決方法

將受影響的FQDN新增到Meraki本地分支規則，以繞過特定目標的安全訪問，詳見以下各節。

步驟 1:訪問Meraki儀表板

導航到Meraki控制面板並找到本地分支配置部分。

步驟 2:配置本地分組規則

將有問題的FQDN新增到本地分流規則，以繞過Secure Access路由。此配置更改會繞過安全訪問隧道，將流量直接從Meraki路由到Internet，從而立即恢復受影響使用者的訪問。

疑難排解和分析

步驟 1:按FQDN進行日誌分析

使用FQDN搜尋安全訪問活動日誌。這主要顯示DNS安全日誌，並可顯示埠443上Web流量的「允許」狀態。

步驟 2:按目標IP顯示的日誌分析

將FQDN解析為其IP地址，使用目標IP而不是FQDN搜尋「活動」日誌。這將顯示顯示阻止的流量的雲防火牆日誌，從而提供實際的流量處置情況。

步驟 3:驗證流量

確認僅當流量沿著路徑傳播時才會出現問題：使用→ Meraki網→通道→安全訪→Internet的使用者。通

過本地分支進行旁路測試可解決連線問題。

長期解決方案

已將此觀察到的行為確定為當前安全訪問實施中的預期功能。已開啟功能請求(FR CSE-I-5543)，以解決與以下內容相關的可視性和功能問題：

- 基於FQDN的日誌搜尋與基於IP的日誌搜尋之間的差異
- DNS安全和雲防火牆日誌之間不一致的流量處置報告
- 提高了非標準埠上RDP流量的可見性

原因

此問題源於安全訪問處理和報告通過RDP訪問非標準埠上的Azure託管的FQDN流量的方式存在差異。按FQDN搜尋日誌時，系統主要顯示DNS安全日誌，顯示Web流量（通常為埠443）的「允許」狀態。 但是，非標準埠上的實際RDP流量正由雲防火牆規則處理，這些規則僅在按解析的目標IP地址而不是FQDN搜尋時才可見。

這造成了一個可視性差距，管理員在基於FQDN的搜尋中看到「允許」流量，而實際RDP連線被防火牆策略阻止，而這些策略僅在基於IP的日誌搜尋中很明顯。該行為當前被視為預期功能，但已提交功能請求，以提高不同搜尋方法中流量報告的可見性和一致性。

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）。