用於安全訪問的F5負載平衡器DNS轉發配置

目錄

問題

在Umbrella to Secure Access遷移期間，將F5負載平衡器用作客戶端DNS伺服器時，DNS解析不起作用。當DNS請求命中虛擬IP(VIP)時，F5負載均衡器已成功將資料包轉發到後端DNS轉發器，但主機名未在終端電腦上解析。當將虛擬裝置直接用作客戶端DNS伺服器時，DNS解析工作正常，表明此問題特定於F5負載均衡器配置。

資料包捕獲顯示DNS應答使用虛擬裝置IP地址而不是預期的F5 VIP地址。客戶端電腦期待來自F5 VIP地址的DNS回覆，但實際上收到了來自後端虛擬裝置IP地址的回覆。

環境

- Cisco Umbrella用於安全訪問遷移環境
- 已配置DNS負載平衡VIP的F5負載均衡器
- 多個DNS轉發器作為後端伺服器
- 充當DNS伺服器的虛擬裝置
- 需要通過負載平衡器進行DNS解析的客戶端終端

解析

通過將F5負載均衡器配置為在客戶端電腦和虛擬裝置之間正確充當代理，解決了此問題。關鍵配置更改涉及使用自動對映功能啟用源網路地址轉換(SNAT)。

已執行的診斷步驟

步驟 1:驗證DNS解析行為

已使用F5負載均衡器VIP和直接虛擬裝置連線測試DNS解析，以隔離問題。

步驟 2:捕獲和分析DNS流量

已執行資料包捕獲，以分析通過F5負載均衡器的DNS請求和響應流。

步驟 3:標識源地址不匹配

分析顯示，DNS回覆包含虛擬裝置IP地址而不是F5 VIP地址，從而導致客戶端混亂。

配置更改

步驟 1:訪問F5負載平衡器配置

導航到F5負載均衡器管理介面以修改DNS VIP配置。

步驟 2:啟用SNAT自動對映

將SNAT（源網路地址轉換）配置為F5負載均衡器上的自動對映。這可確保F5裝置在客戶端和後端DNS伺服器之間正確代理DNS請求和響應。

步驟 3:驗證設定

實施SNAT自動對映配置後，DNS解析開始通過F5負載均衡器正常工作。

原因

根本原因是F5負載平衡器上的源網路地址轉換(SNAT)配置不正確。如果未啟用SNAT自動對映，則

F5裝置無法正確充當DNS流量的代理。這導致DNS響應直接從後端虛擬裝置傳送到客戶端電腦，使用虛擬裝置IP地址而不是預期的F5 VIP地址作為源。客戶端電腦希望收到的DNS響應來自它們向傳送請求的同一IP地址(F5 VIP)，但收到來自不同IP地址（後端伺服器）的響應，導致DNS解析失敗。

相關內容

- 配置F5 GTM負載均衡
- 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）。