安全訪問VPN — 無法訪問Jabber

目錄

問題

使用專用訪問策略時，安全客戶端使用者無法通過安全訪問VPN隧道訪問內部和專用應用程式（如Jabber和Epic）。使用者嘗試通過VPN連線訪問這些關鍵業務應用程式時遇到了連線故障。在故障排除期間，觀察到Epic資源存在單向流量，其中ping和TCP SYN流量通過安全訪問VPN隧道，但返回流量驗證問題在Palo Alto防火牆上被發現。此外，記錄了Jabber可訪問性問題，其中CUCM FQDN是通過內部DNS解析的，而流量控制配置為基於IP的路由，從而導致流量不匹配。

環境

- 使用VPN隧道配置的Cisco安全訪問
- 用於VPN連線的安全客戶端
- 私有訪問策略實施
- 適用於Jabber服務的思科整合通訊管理員(CUCM)
- Epic應用程式資源
- 適用於網路安全的Palo Alto防火牆
- CUCM FQDN的內部DNS解析

解析

解決方案涉及多個配置更改和故障排除步驟，以通過安全接入VPN隧道恢復與內部應用程式的連線：

子網配置和隧道修改

步驟 1:向VPN隧道新增其他子網

已將其他子網新增到受影響資源的VPN隧道配置中。實施此更改後，以前無法訪問的資源開始成功載入。

CUCM IP地址引導配置

步驟 2:配置CUCM IP引導

為了解決在流量控制基於IP時通過內部DNS解析CUCM FQDN的Jabber連線問題，將CUCM IP地址引導到安全客戶端。此配置更改使DNS解析與流量控制機制保持一致。

步驟 3:建立訪問策略規則

建立了一個訪問策略規則，以允許訪問CUCM IP地址。此規則恢復到CUCM基礎設施的正確連線，從而通過VPN隧道啟用Jabber功能。

靜態路由配置

步驟 4:配置CUCM子網的靜態路由

確保CUCM IP地址和整個CUCM子網包括在網路隧道的靜態路由表中。此配置可確保正確路由安全客戶端使用者池和CUCM基礎設施之間的流量。

返回流量驗證

步驟 5:驗證資料包流和返回流量

驗證資料包流配置，確認返回流量可以到達安全客戶端使用者池。這包括檢視Palo Alto防火牆配置，以確保對所有內部資源進行正確的返迴路徑驗證，特別是對於觀察到單向流量的Epic連線。

原因

連線問題是由安全接入VPN實施中的多個配置缺口引起的：

- VPN隧道中缺少子網配置，無法正確路由到內部應用程式資源
- CUCM服務的DNS解析（基於FQDN）和流量控制配置（基於IP）之間不匹配，導致Jabber連

線失敗
- 不允許流量到達CUCM IP地址的不完整訪問策略規則
- 網路隧道配置中缺少CUCM子網的靜態路由條目
- 影響雙向通訊的Palo Alto防火牆上的返回流量路徑驗證問題

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）。