

Omnissa Full Client Connectivity Issues Through Secure Access (通過安全訪問解決Omnissa完全客戶端連線問題)

目錄

問題

通過Cisco Secure Access連線時，Omnissa full客戶端無法載入虛擬案頭。使用者嘗試使用完整的客戶端應用程式建立與虛擬環境的連線時，會遇到連線故障。但是，通過HTML/Web客戶端的訪問繼續正常運行，這表明基礎虛擬案頭基礎設施已正常工作，但存在影響客戶端通過Cisco Secure Access解決方案建立連線的完整能力的特定問題。

環境

- 技術：解決方案支援 (SSPT — 需要合約)
- 子技術：Cisco Secure Access
- 產品系列：SEACACS
- 軟體版本:所有受影響的版本
- 客戶端應用程式：Omnissa完全客戶端
- 虛擬案頭環境：Omnissa虛擬案頭
- 網路基礎設施：IPsec通道和FTD (Firepower威脅防禦)

解析

解決方案涉及實施特定的網路配置更改，以便通過Cisco Secure Access為Omnissa完全客戶端實現

正確的路由。為了解決連線問題，採取了以下步驟：

- 配置拆分隧道設定。新增拆分隧道配置，以允許Omnissa full客戶端建立到所需目標主機的直接連線。此配置可確保通過適當的網路路徑正確路由發往特定虛擬案頭客戶端的流量。
- 實施靜態路由配置。為需要建立到虛擬案頭的連線的特定客戶端配置靜態路由。關鍵要求是，不僅要配置到下游匯聚伺服器的路由，還要配置直接到虛擬案頭客戶端需要到達的目標主機的路由。
- 清除IPsec隧道。實施組態變更後，清除FTD上的IPsec通道，以確保新路由組態正確生效。
- 驗證連線。實施更改後測試Omnissa完全客戶端連線，以確認可以通過Cisco Secure Access成功建立虛擬案頭連線。

實施計畫

必須在計畫維護時段實施配置更改，以儘量減少對使用者的影響。實施後，驗證可達性和Omnissa完全客戶端連線，以確保解決成功。

原因

連線問題是由思科安全訪問環境中的路由配置不足引起的。具體來說，網路配置的路由只到下游的聚合伺服器，但缺少Omnissa完全客戶端建立連線所需的特定客戶端所必需的分割隧道和靜態路由配置。此路由間隙使整個客戶端無法正確到達虛擬案頭主機，而HTML/Web客戶端仍然可以正常工作，因為它使用了正確配置的不同連線路徑。

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）。