使用Kerberos身份驗證訪問專用資源時排除故障

目錄

簡介

本檔案將說明Kerberos與「安全存取零信任網路存取」(ZTNA)一起使用時的行為。

必要條件

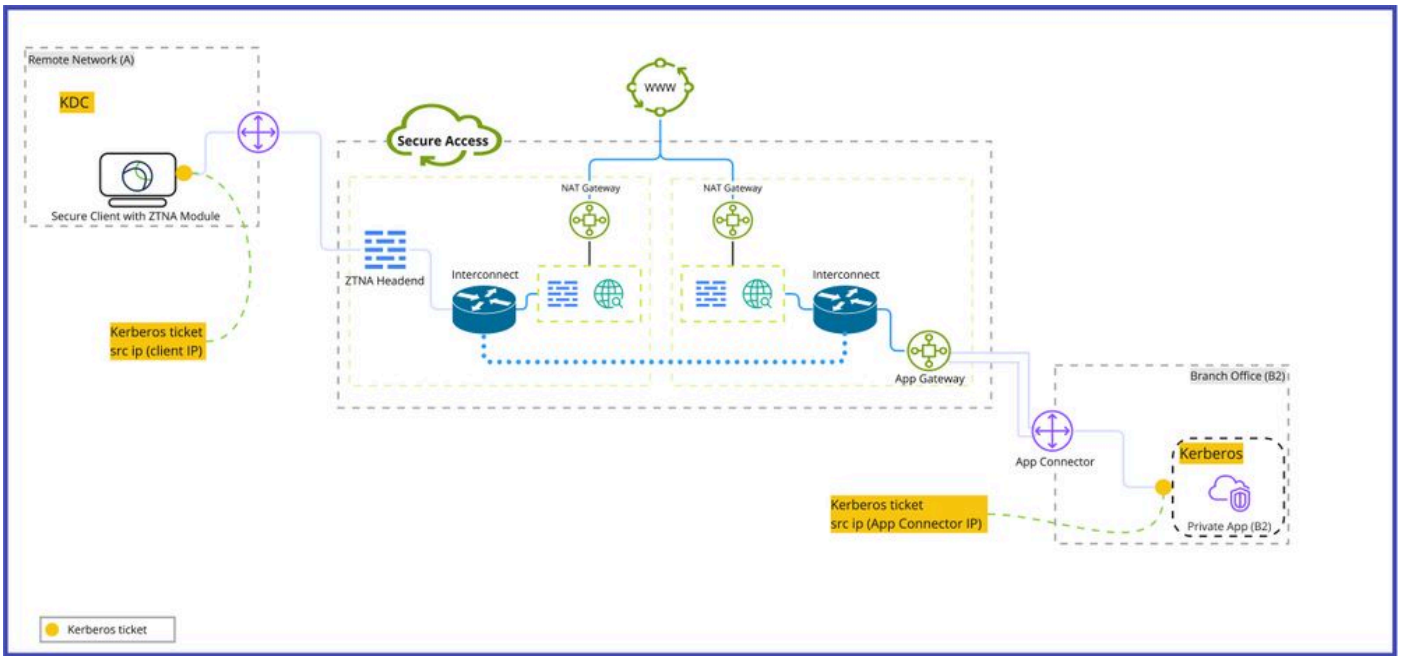
需求

思科建議您瞭解以下主題：

- 安全存取
- 思科安全使用者端
- 網際網路通訊協定安全(IPSEC)通道
- 遠端存取虛擬私人網路(RAVPN)
- 零信任網路存取(ZTNA)

背景資訊

安全訪問用於透過多種方案(包括安全客戶端上的零信任訪問模組(ZTNA)、IPSEC隧道或遠端訪問VPN)提供對私有應用的訪問。雖然私有應用程式提供其自己的身份驗證機制，但依賴Kerberos作為身份驗證機制的伺服器存在限制。



Kerberos資料包流

問題：使用Kerberos驗證存取私人資源失敗

從ZTNA模組後面的客戶端裝置向App Connector後面的私有應用程式發起身份驗證請求將導致源IP地址沿安全訪問網路的路徑發生更改。這會導致在使用由客戶端Kerberos分發中心(KDC)啟動的Kerberos票證時身份驗證失敗。

解決方案

客戶端源IP地址是從Kerberos分發中心(KDC)授予的Kerberos票證的一部分。通常，當Kerberos票證穿越網路時，要求源IP地址保持不變，否則，與源IP票證傳送源伺服器相比，我們正在驗證的目標伺服器不會接受票證。

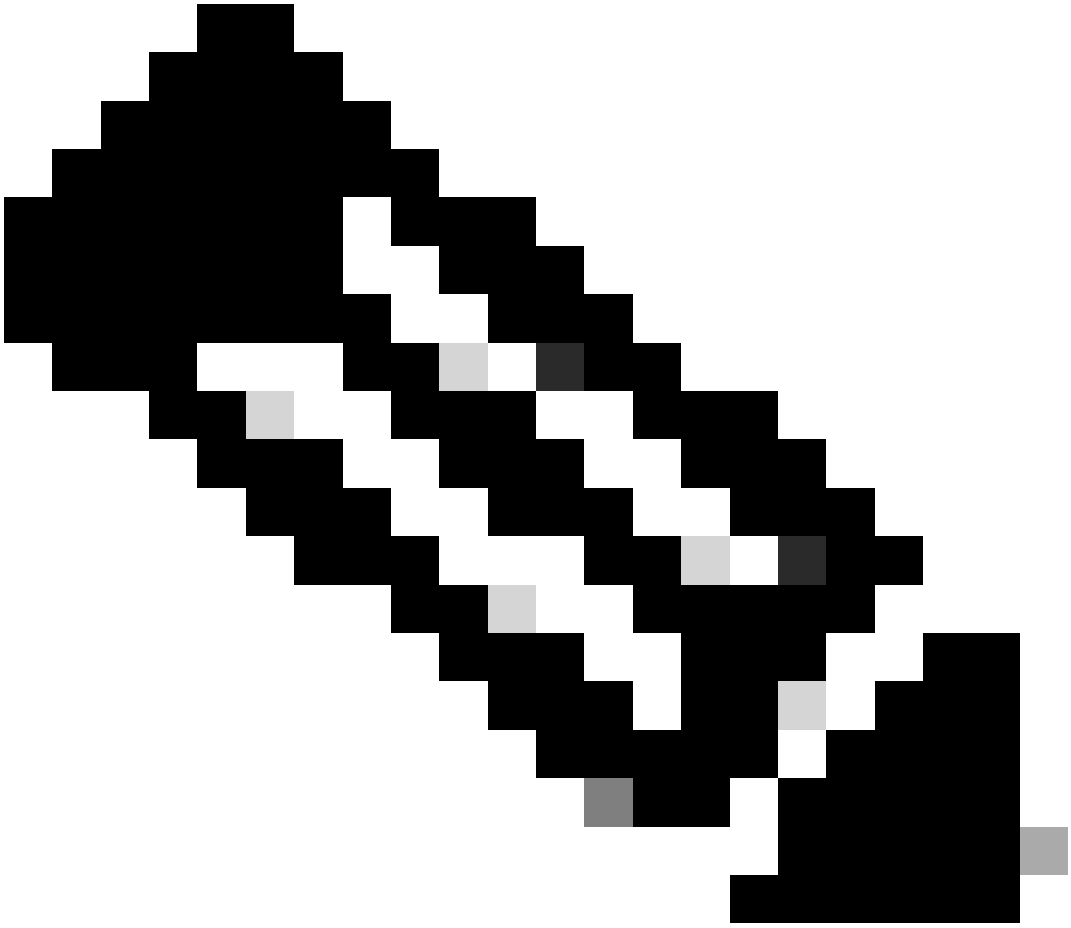
若要解決此問題，請使用以下選項之一：

選項 1:

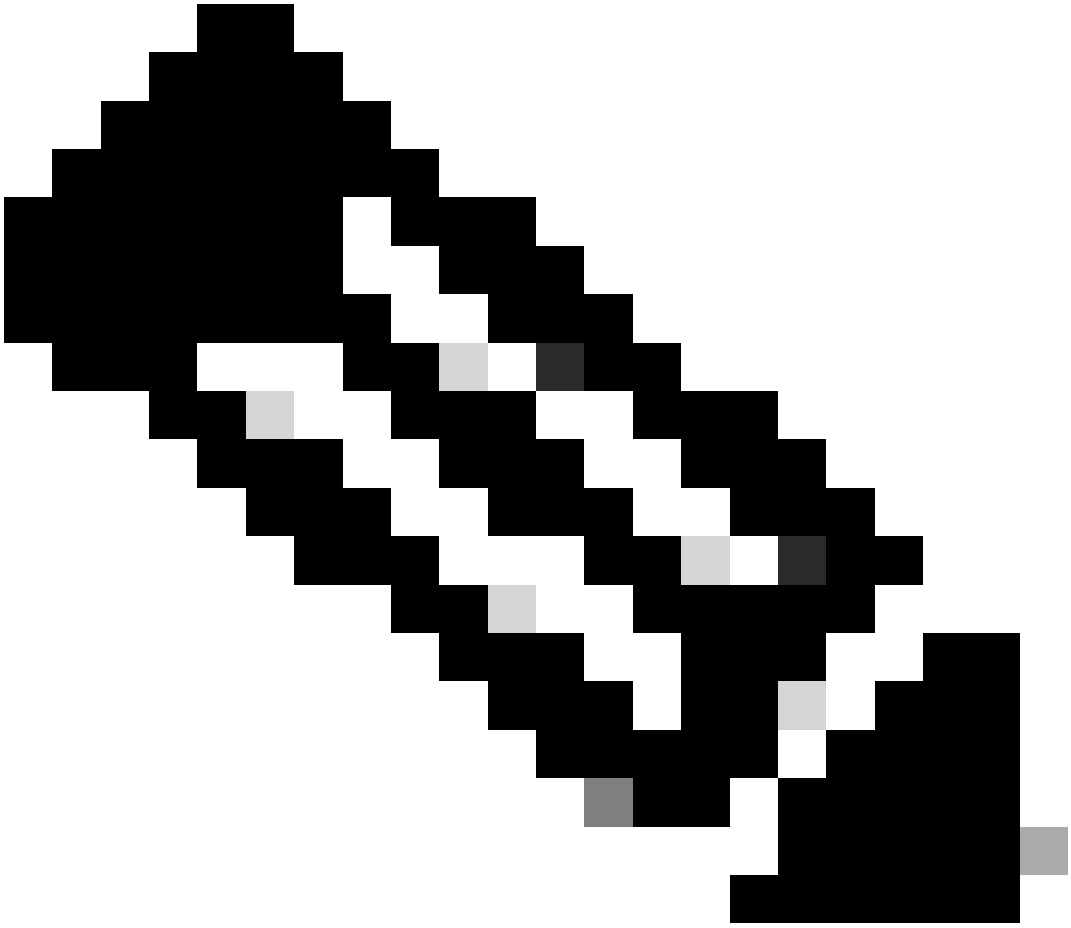
停用此選項以在客戶端Kerberos票證中包含源IP地址。

選項 2:

在IPSEC隧道後使用具有專用資源的安全訪問VPN，而不是在App Connector後使用專用應用程式。



注意：此行為只影響部署在App Connector之後的專用應用程式，並且資料流源自帶有ZTNA模組的客戶端（不帶VPN）。



注意：「安全訪問活動搜尋」顯示允許的事務處理操作，因為阻止發生在專用應用程式端（而非安全訪問端）。

相關資訊

- Secure Access使用手冊
- 技術支援與文件 - Cisco Systems

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）。