疑難排解Webex通話SIP中繼缺陷 — 防火牆阻止來自Webex對等體的傳入連線

目錄

問題

配置為連線到AudioCodes會話邊界控制器(SBC)的Webex呼叫SIP中繼顯示「已損壞」狀態。中繼已使用TCP埠5062配置為基於證書的信令。雖然從SBC到所有4個Webex對等體(peering1-4.eun.sipconnect.bcld.webex.com)的出站SIP選項均成功並收到正確的響應，但是對於某些對等體（尤其是標籤為「EUN 2和4」的對等體），從Webex到SBC的入站SIP選項失敗。

觀察到的特定錯誤為：

```
Failed to connect out to
atstesbc.bmd.com
./213.33.78.212:5062io.netty.channel.ConnectTimeoutException: connection timed out after 2000 ms:
atstesbc.bmd.com
./213.33.78.212:5062
```

防火牆封包擷取顯示來自Webex對等點的傳入TCP SYN封包抵達防火牆，但並未觀察到從SBC傳回的相應SYN-ACK或RST封包，因此未能成功完成TCP作業階段建立和後續SIP選項健康狀況檢查。

環境

- Webex通話憑證型SIP中繼
- AudioCodes作業階段邊界控制器
- 適用於SIP over TLS信令的TCP埠5062
- 四個Webex對等點：peering1-4.eun.sipconnect.bcld.webex.com
- Webex雲端和客戶SBC之間的防火牆基礎架構
- 組織ID:173b6146-6c50-4890-9ccc-43f73b6c85d5

解析

通過重置防火牆連線解決了此問題，該連線為所有Webex對等體和SBC之間的SIP選項運行狀況檢查恢復了正確的雙向連線。

已執行的診斷步驟

步驟 1:已驗證中繼配置和DNS解析。

已確認SBC能夠成功解析所有四個Webex對等體FQDN並建立到每個對等體的出站連線。

步驟 2:已分析防火牆資料包捕獲。

在SIP OPTIONS測試期間，從防火牆入口和出口介面收集了同步資料包捕獲。捕獲顯示：

- 來自Webex對等點的入站TCP SYN封包正在抵達防火牆。
- 沒有從SBC傳送回SYN-ACK或RST響應。
- 對於特定對等體連線，TCP握手無法完成。

步驟 3:已檢視SBC系統日誌和跟蹤。

SBC日誌顯示連線建立時的TLS握手成功，但沒有傳輸錯誤或證書故障可以解釋連線超時。

步驟 4:重置防火牆連線。

防火牆連線已重置，以清除任何過時的會話狀態或連線跟蹤條目，這些條目可能阻止了正確的雙向通訊。

驗證

在防火牆連線重置後，SIP中繼狀態從「已損壞」更改為可操作，所有四個Webex對等體都成功雙向完成SIP選項運行狀況檢查。

原因

根本原因是防火牆基礎設施阻止或丟棄從特定Webex對等IP地址到埠5062上的SBC的入站TCP連線。這阻止了通過TLS的SIP信令所需的TCP握手完成，從而導致中繼運行狀況檢查失敗並導致「已損壞」狀態。此問題可能是因為防火牆連線狀態過時、非對稱路由或安全策略干擾了某些Webex雲對等點的入站會話建立。

相關內容

- Webex Calling的埠參考資訊
- 配置Webex呼叫的中繼、路由組和撥號計畫
- Webex Calling的安全要求
- 本地網關入門
- 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）。