使用零信任訪問配置檔案配置排除MS Teams問題

目錄

問題

在零信任訪問(ZTA)配置檔案中為安全網際網路訪問註冊的使用者遇到了Microsoft Teams呼叫連線問題。將使用者新增到ZTA配置檔案時，Microsoft Teams呼叫意外斷開連線，其他使用者無法向受影響的使用者發起呼叫。但是，當受影響的使用者從其一側發起呼叫時，呼叫連線成功。

該問題被隔離到已註冊到ZTA配置檔案的使用者，表明ZTA策略或路由配置正在影響Teams呼叫連線。流量日誌顯示Microsoft Teams從ms-teams.exe等進程到IP地址(例如52.115.245.30:3480，屬於52.112.0.0/14)的流量被ZTA客戶端攔截，而不是直接進入網際網路。

環境

- 採用零信任訪問(ZTA)配置檔案的思科安全訪問
- 配置了「使用ZTA保護所有Internet目標」的ZTA配置檔案
- Microsoft Teams應用程式
- 具有ZTA功能的思科安全客戶端
- 在ZTA配置檔案中註冊Secure Internet訪問的使用者

解析

要解決此問題，請將Microsoft Teams流量異常新增到ZTA配置檔案配置中，以允許Teams流量繞過ZTA隧道並直接連線到網際網路：

1.定位至控制面板>終端使用者連線>零信任訪問，然後查詢受影響的ZTA配置檔案。

2.選擇ZTA配置檔案，然後選擇「編輯」>「安全Internet訪問」。

3.根據Microsoft的官方文檔，將這些IP範圍和FQDN新增到例外清單:

IP範圍：

```
52.112.0.0/14
52.122.0.0/15
2603:1063::/38
2603:1027::/48
2603:1037::/48
2603:1047::/48
2603:1057::/48
2620:1ec:6::/48
2620:1ec:40::/42
```

FQDN:

```
*.lync.com
*.teams.cloud.microsoft
*.teams.microsoft.com
teams.cloud.microsoft
teams.microsoft.com
*.keydelivery.mediaservices.windows.net
*.streaming.mediaservices.windows.net
aka.ms
```

4.新增例外說明，例如：

```
MS Teams exception as per: https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-addre
```

5.儲存配置更改。等待幾分鐘以應用更改。

6.確保在受影響的終端上重新同步ZTA客戶端策略。這可能需要重新啟動零信任訪問代理服務或重新啟動客戶端裝置。

7.測試團隊呼叫功能以確認：

- 現在已成功連線傳入給受影響使用者的呼叫
- Teams呼叫不再意外斷開連線
- Teams流量繞過ZTA隧道直接連線到Internet

附註：實施例外後，Teams流量不會出現在安全訪問活動日誌中，因為它完全繞過ZTA隧道。

原因

此問題是由通過ZTA安全網際網路訪問隧道而非直接連線到網際網路的Microsoft Teams流量導致的。當使用「Secure All Internet Destinations」選項配置ZTA配置檔案時，它將攔截Teams媒體流量，包括即時通訊所需的UDP流量。這會導致連線問題，尤其是對於傳入呼叫和媒體流。

Microsoft建議繞過來自代理伺服器的Microsoft Teams流量和SSL檢查，以實現最佳效能和呼叫品質。當ZTA配置缺少Teams流量的必要異常時，應用程式媒體流將通過ZTA客戶端進行處理，而不是採用即時通訊所需的直接路徑。

相關內容

- Microsoft 365 URL和IP地址範圍 — Microsoft Teams
- Microsoft Teams Proxy伺服器建議
- 排除故障並收集思科安全訪問的基本資訊
- 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）。