驗證安全訪問Microsoft 365相容性的旁路行為功能

目錄

問題

在啟用了Microsoft 365相容性功能的情況下配置Cisco安全訪問時，不確定是否從安全Web網關(SWG)處理和TLS解密自動繞過特定的Microsoft相關完全限定域名(FQDN)。具體來說，需要說明這些域的旁路行為：

- do.dsp.mp.microsoft.com
- dl.delivery.mp.microsoft.com
- manage.microsoft.com

主要關注點在於這些域是否需要手動新增到「不解密」清單，或者當啟用「Microsoft 365相容性」時是否自動排除這些域。此外，SWG級旁路和IPS級解密設定之間的互動也存在混淆，特別是對於manage.microsoft.com（出現在文檔中，說明仍需要手動設定不解密清單）。

環境

- Cisco Secure Access
- 已啟用Microsoft 365相容性功能
- 已配置安全Web網關(SWG)檢測和TLS解密
- 正在使用的IPS解密策略
- 需要連線的Microsoft管理和更新服務

解析

Microsoft 365相容性功能行為已通過實驗室測試驗證，結果如下：

Microsoft 365相容性功能範圍

Microsoft 365相容性功能免除了在Microsoft端點類別中標籤為「最佳化」和「允許」的Microsoft 365相關域，從而免除SWG檢查和策略實施。這樣可允許流向這些域的流量在SWG層未經更改地通過。

實驗室檢測結果

測試在已啟用Microsoft 365相容性的受控實驗室環境中進行。針對指定的FQDN觀察到此行為：

步驟 1:啟用Microsoft 365相容性功能

Microsoft 365相容性功能已在Secure Access配置中啟用。

步驟 2:測試到目標FQDN的流量

使用標準的Internet瀏覽器生成到三個FQDN中每個的Web流量：

- do.dsp.mp.microsoft.com
- dl.delivery.mp.microsoft.com
- manage.microsoft.com

步驟 3:驗證儀表板中的旁路行為

對安全訪問控制面板的分析確認，啟用Microsoft 365相容性功能時，不會對這些特定目標的流量進行Web流量檢測和解密。

步驟 4:確認DNS引導行為

到這些目的地的DNS流量繼續通過安全訪問引導，這符合記錄的行為，除非配置了特定DNS免除。

關鍵行為發現

根據測試結果和文檔分析：

- SWG旁路：啟用Microsoft 365相容性時，會從網路流量檢測繞過三個指定的FQDN。
- TLS解密：這些域的解密在SWG層被繞過。
- DNS引導：除非明確免除，否則DNS查詢將繼續通過安全訪問處理。
- 域覆蓋：雖然規範並未完全繞過「*.microsoft.com」作為一個完整域，但實際會繞開測試的特定URL。

IPS層注意事項

Microsoft 365相容性功能在SWG層運行。對於IPS級別解密繞行，仍需要手動配置：

- 如果這些域也需要IPS解密旁路，則可能需要手動新增到Do Not Decrypt List。
- 不解密清單主要影響IPS端解密，而不是SWG處理。
- 這解釋了為什麼即使啟用了Microsoft 365相容性，文檔仍可以參考將manage.microsoft.com新增到「不解密清單」。

原因

混淆源於思科安全訪問的分層架構，其中Microsoft 365相容性影響SWG級處理，而IPS解密則作為具有其自身配置要求的單獨層運行。Microsoft 365相容性功能會自動處理符合條件的Microsoft域的SWG旁路，但IPS解密策略可能需要通過Do Not Decrypt List進行單獨配置。

相關內容

- 思科安全訪問Microsoft 365相容性文檔

- 為思科安全訪問建立有效的「不解密」清單
- 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）。