Umbrella DNS安全與MacOS上Broadcom WSS的共存問題

目錄

問題

與Broadcom WSS（網路安全服務）共存時，Umbrella模組不會在macOS上攔截DNS流量。 當WSS代理配置為擷取特定Web埠（如80和443）時，Umbrella DNS安全功能無法捕獲所有DNS查詢。但是，當WSS被禁用時，Umbrella會按照預期繼續攔截DNS流量。啟用WSS時，Umbrella只處理某些DNS查詢，而不是攔截所有DNS流量。

環境

- 作業系統：macOS
- Cisco Umbrella DNS安全模組
- Broadcom WSS（網路安全服務）代理
- 配置為擷取Web埠80和443的WSS代理

解析

已分析此問題並確定為macOS的架構限制，其中DNS安全無法在當前macOS架構中與WSS共存。此限制適用於Infoblox和Cisco Umbrella DNS安全解決方案。

技術分析

根本原因與macOS DNS代理限制有關：

- 由於macOS限制，系統中一次只能有一個DNS代理處於活動狀態

- 如果DNS解析器繫結到utunX介面或代理注入的解析器，則macOS解析隧道中的DNS，而不是通過Umbrella
- 當另一個NEDnsProxyProvider在macOS上的系統上處於活動狀態時，Umbrella不會攔截DNS流量

診斷命令

要驗證哪個DNS解析程式在macOS上優先，請使用以下命令：

```
scutil --dns
```

此命令將顯示哪個解析程式標籤為：作用域、補充或介面：utunX，幫助識別DNS代理衝突。

解決方法選項

對於macOS環境，WSS將繼續在不使用任何獨立DNS代理的情況下攔截DNS。要繼續使用DNS安全覆蓋，一個選項是實施以支援被動旁路架構。使用此方法，提供商將完全繞過流，從而允許處理流量，就像提供商處於非活動狀態一樣。

原因

此問題是由於macOS架構限制導致的，在這種限制下，系統一次只能啟用一個NEDnsProxyProvider。當同時安裝Umbrella DNS Security和Broadcom WSS時，它們會爭奪DNS代理控制，導致WSS優先處理並阻止Umbrella攔截DNS流量。這是macOS網路堆疊的基本限制，會影響所有DNS安全解決方案，而不僅僅是Cisco Umbrella。

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）。