Cisco安全存取分段的ICMP封包處理

目錄

問題

在停用DF（不分段）位元的情況下傳送時，大於MTU的ICMP回應要求不會接收回覆。此行為發生在兩個特定場景中：

- 在清除DF位元的情況下，傳送超過VPN介面MTU大小的ICMP資料包時，通過VPN介面從RAVPN終端
- 在傳送超過IPsec通道介面MTU大小且已清除DF位元的ICMP封包時，透過站點路由器和Cisco安全存取(CSA)之間的IPsec通道從內部端點

在這兩種情況下，系統都沒有收到ICMP回應，因此會產生CSA是否捨棄已停用DF位元的分段封包的問題。

環境

- 思科安全存取(CSA)
- RAVPN（遠端訪問VPN）終端
- 站點路由器和CSA之間的IPsec隧道
- 超出介面MTU大小的ICMP流量
- 已清除DF位元的分段封包情境

解析

在底層和重疊方案中，思科安全存取都會捨棄分段封包。此行為記錄在Cisco Secure Access幫助文檔中，其中明確指出："底層或重疊中的分段資料包將被丟棄。"

預期行為

思科安全存取旨在捨棄分段封包，無論這些封包是發生在底層網路還是重疊網路中。這適用於：

- 從RAVPN端點傳送的ICMP封包超過VPN介面MTU，且已清除DF位元
- 從內部部署終端透過IPsec通道傳送的ICMP封包超過通道介面MTU，且已清除DF位元

此行為在涉及思科安全訪問基礎設施內分段資料包的所有場景中都是一致的。

已為此建立功能請求CSE-I-5739。

原因

思科安全訪問的架構旨在丟棄分段的資料包，作為安全和效能設計決策。實施此行為是為了防止底層網路方案和重疊網路方案中與資料包重組相關的潛在安全漏洞和處理開銷。

相關內容

- 思科安全存取幫助檔案 — 分段封包處理
- 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）。