

疑難排解"452可疑的重播攻擊"CSC SWG模組中的錯誤

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[問題](#)

[解決方案](#)

[原因](#)

簡介

本檔案介紹如何疑難排解CSC SWG模組中的「452疑似重播攻擊」錯誤。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據Cisco Secure Client(CSC)和Secure Web Gateway(SWG)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

問題

嘗試連線到[Cisco Secure Client\(CSC\) \(前身為AnyConnect \) 安全Web網關\(SWG\)模組時，您遇到「452可疑重播攻擊」錯誤：](#)



360073322452

解決方案

請注意，消息「重播攻擊」是時間差異的一般警告，因為攻擊加密連線的一種方法是重複重播舊資料包。但是，在這種情況下，實際上不會發生重播攻擊。更改電腦上的時間後，就可以解決該錯誤。

原因

如果終端上的系統時鐘漂移4分鐘以上，則可能發生此錯誤。由於當前時間用於協商加密，因此如果客戶端和伺服器之間存在大量時間差，它們無法相互協商安全的加密連線。



附註：思科宣佈Cisco AnyConnect於2023年停用，Umbrella漫遊客戶端於2024年停用。許多Cisco Umbrella客戶已經從遷移到Cisco Secure Client中受益，我們鼓勵您儘快開始遷移，以獲得更好的漫遊體驗。閱讀此知識庫文章中的詳細資訊：[如何在Umbrella模組中安裝Cisco Secure Client?](#)

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）。