針對特定應用協定的安全訪問策略實施

目錄

簡介

本文檔介紹使用某些應用協定時的安全訪問策略實施。

必要條件

需求

思科建議您瞭解以下主題：

- 安全存取
- 檔案傳輸通訊協定 (FTP)
- 傳輸控制通訊協定(TCP)
- 防火牆即服務(FWaaS)
- 安全殼層 (SSH)
- 超文字傳輸通訊協定(HTTP)
- 快速UDP網際網路連線(QUIC)
- 安全郵件傳輸通訊協定(SMTP)

背景資訊

用於評估基於應用協定的策略實施的典型FWaaS測試是一種協定誤用測試。

此案例的測試通常涉及在非標準埠上建立阻止特定應用協定（例如FTP/SSH）的策略。例如，僅允許FTP在TCP埠21上，並阻止FTP在TCP埠80上。

「安全存取」使用OpenAppID通訊協定偵測來偵測應用程式通訊協定，例如FTP、SSH、QUIC、SMTP和其他通訊協定。並使用安全Web閘道來保護HTTP(S)流量。

問題：TCP 80/443上某些應用協定的策略實施測試導致連線超時

，並且安全訪問中未生成任何日誌

在某些情況下，例如嘗試允許/阻塞TCP埠80/443上的FTP等特定協定，我們遇到客戶端和伺服器之間的初始連線被代理引擎擷取，TCP握手完成，然後安全訪問中的代理引擎等待客戶端傳送流量，但是協定需要伺服器端訊號才能到達客戶端。

這種情況會導致連線超時，因為客戶端等待伺服器訊號，並且代理最終斷開連線。而Secure Access不為此型別的會話生成任何日誌。

解決方案

這是由於「安全存取」架構保護Web流量的方式所導致的一種預期行為，而且因為這種測試涉及Web連線埠上的非Web流量（FTP、SSH、Telnet、SMTP、IMAP及其他最初依賴伺服器端訊號的通訊協定），所以不會為此類作業階段產生任何記錄。

相關資訊

- Secure Access使用手冊
- 安全存取社群頁面
- 技術支援與文件 - Cisco Systems

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）。