排除強制網路門戶與Umbrella漫遊客戶端的互動故障

目錄

簡介

本文檔介紹強制網路門戶與Umbrella漫遊客戶端的互動。

概觀

強制網路門戶是公共或「即服務」Internet連線的常用名稱，此類連線要求付款、身份驗證或服務條款/可接受使用策略(TOS/AUP)接受，然後才允許連線到裝置。

人工門戶通常出現在機場、酒店、咖啡店或者任何提供免費或付費的WiFi的地方。您也可以在公司或學校環境中的訪客wifi網路中看到它們。

強制網路門戶在瀏覽器中通常顯示為「入口」或彈出視窗，終端使用者需要執行操作來提供憑證、付款或接受服務條款，才能訪問Internet。在清除強制網路門戶之前，使用者無法瀏覽除該門戶所在的子網內的資源以外的任何資源。

預期行為和場景

大多數強制網路門戶將所有瀏覽器請求(HTTP/HTTPS)重定向至其本地Web門戶。本地Web入口通常基於IP，而不是基於DNS。這表示在連線到強制網路門戶的電腦上使用Umbrella漫遊客戶端時，不會出現行為問題。

在強制網路門戶以某種方式使用DNS來為其服務提供便利的極少數情況下，此行為發生在完成強制網路門戶的要求之前（支付、TOS/AUP接受等）。]

基於DNS的強制網路門戶可能只能重定向無故障的HTTP查詢。現代瀏覽器會自動處理已知請求，例如google.com到https://www.google.com/，這些請求可能會破壞一些強制網路門戶。嘗試使用Apple強制網路門戶檢查站點訪問僅http的強制網路門戶登入頁面。要執行此操作，請訪問http://captive.apple.com。

思科安全聯結器(CSC)

與漫遊客戶端一樣，如果強制網路門戶後允許UDP 443，則CSC會保持受保護狀態並加密。這會導致強制網路門戶的本地DNS無法解析為本地結果。因此，要訪問強制網路門戶，必須訪問這些半強制網路門戶的內部域清單中的域。

要允許iOS自動強制網路門戶檢測正常工作，請執行以下操作：

- 將這些域新增到內部域清單
  - captive.apple.com
  - www.airport.us
  - www.thinkdifferent.us

已阻止第三方DNS

如果強制網路門戶阻止發往Umbrella的DNS請求，則Umbrella漫遊客戶端會阻止DNS連線大約六秒。6秒後，Umbrella漫遊客戶端將轉換為未保護/未加密狀態，直到可以再次與Umbrella通訊。

已重定向第三方DNS

如果強制網路門戶重定向目的地為Umbrella的DNS請求，則Umbrella漫遊客戶端會阻止DNS連線大約2到6秒。此後，Umbrella漫遊客戶端將轉換到未保護/未加密狀態，直到可以再次與Umbrella通訊。

允許第三方DNS

如果強制網路門戶沒有操縱或阻止發往Umbrella的DNS請求，則Umbrella漫遊客戶端按預期工作，可能導致完全繞過強制網路門戶的登入部分。

解決方案：訪問內部域清單中的域。即使允許第三方DNS，這仍允許強制網路門戶重定向。當漫遊客戶端在強制網路門戶後保持受保護狀態時執行此操作。

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）。