身份驗證後銀行站點安全訪問502錯誤

目錄

問題

使用者報告在成功對FCBanking進行身份驗證後收到502個錯誤的網關HTTP錯誤代碼。身份驗證過程已成功完成，允許使用者輸入其登入憑據，但是，在身份驗證之後，瀏覽器立即顯示一個502錯誤網關錯誤。

FCBanking的網域及其相關類別免除了SSL和IPS解密，並且此組態變更未解決502 HTTP錯誤。此問題間歇性發生，僅在完全繞過FCBanking域的安全訪問之後才得到解決。HAR檔案分析顯示「my.fcbanking.com」的目標位置存在502個錯誤，活動搜尋日誌未顯示HAR檔案中捕獲的502個錯誤，這表明這些錯誤發生在中間裝置級別。

環境

- Cisco Secure Access - Internet Access（漫遊模組、VA、DNS、SWG、PAC、IPS、證書）
- 網路拓撲:使用者PC >交換機> Catalyst SD-WAN路由器>本地網際網路或CSA隧道
- Catalyst SD-WAN邊緣配置了應用策略規則，通過直接網際網路接入(DIA)繞過網路隧道組(NTG)傳送埠80和443上的所有流量
- 思科安全客戶端依靠旁路清單來確定流量路由到安全訪問
- 銀行業務領域：fcbanking.com和相關子域(my.fcbanking.com、treasury.fcbanking.com)

解析

主要解決方法涉及新增銀行域以完全繞過安全訪問，允許流量直接流到網際網路，同時維護DNS層安全性。

步驟 1:將主域新增到旁路清單

- 將fcbanking.com新增到Secure Access配置中的僅繞過代理清單。這可確保當DNS層安全性保持實施並記錄在「活動搜尋」中時，Web流量繞過安全訪問代理。

步驟 2:標識和新增域別名

- 銀行站點通常使用多個別名，這些別名也必須新增到旁路清單中。使用快取檢查標識銀行域的所有別名。
- 對於fcbanking.com，已標識這些別名並將其新增到旁路清單中：
  - treasury.fcbanking.com(別名：treasuryvanity.jackhenry.com)
  - my.fcbanking.com(別名：banno-online.jackhenry.bank)
  - treasuryvanity.jackhenry.com
  - banno-online.jackhenry.bank

步驟 3:使用IP地址進行替代解析

- 作為基於域的旁路方案的替代方案，可以將銀行站點的已解析IP地址新增到旁路清單中。思科安全客戶端將旁路清單中的FQDN轉換為IP地址，並將網路流量直接路由到網際網路。

步驟 4:啟用調試日誌記錄以進行故障排除

- 要捕獲詳細日誌以進行進一步分析，請啟用最大調試日誌記錄：
- 使用以下內容建立名為「SWGConfigOverride.json」的檔案：

```
{"logLevel": "1"}
```

將SWGConfigOverride.json檔案放在SWG資料夾中：

```
C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\SWG\
```

重新啟動SWG或Umbrella服務，或重新啟動系統以應用調試日誌記錄配置。

附註：調試日誌記錄不影響系統效能，但可能會增加日誌檔案大小。獲取DART捆綁包後刪除SWGConfigOverride.json檔案以返回正常日誌記錄級別。

步驟 5:驗證

- 實施旁路配置後，使用者在訪問銀行站點時不再報告502個錯誤。DNS流量繼續記錄在Activity Search中，而Web流量直接流向Internet。

原因

銀行站點通常實施安全措施，檢測並阻止來自代理伺服器或共用IP地址範圍的流量。Cisco Secure Access使用共用IP範圍(151.186.144.0/20和151.186.176.0/20)來傳送代理流量，銀行站點可以檢測這些流量，並以靜默方式丟棄或響應HTTP 502錯誤。

當域放在do not decrypt清單中時，源IP似乎仍來自Secure Access共用IP範圍，從而觸發銀行站點的安全機制。此外，未正確排除的銀行流量和域別名的IPS檢測會導致連線故障。此問題的間歇性以及出現在HAR檔案但不出現在活動搜尋日誌中的502個錯誤都表明這些錯誤是由中間代理處理而不是目標銀行伺服器生成的。

相關內容

- 排除SWG網站訪問問題
- 禁用QUIC協定以確保正確的網路流量檢測
- Cisco安全存取IP範圍檔案
- 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）。