解決安全Web網關SWG網站訪問問題

目錄

簡介

本文描述的是診斷網站訪問問題的結構化方法，該方法用於診斷通過基於雲的代理（安全Web網關/SWG）路由時的問題，而不是在使用直接網際網路訪問(DIA)時的問題。

- 範圍：適用於Cisco Umbrella SIG和Cisco Secure Access。

前提條件和重要警告

- 驗證是否對可再現的問題執行所有故障排除。
- 收集HAR（HTTP存檔）檔案和同時資料包捕獲(PCAP)以提供準確的資料進行分析。
- 對代理策略的更改（例如，繞過解密或檢查）可能會影響安全狀態；僅用於故障排除或按照建議應用。

識別代理級錯誤

常見的代理干擾指示器包括：

- 502錯誤的網關
- 515上游證書不受信任
- 517上游證書已吊銷
- 403禁止
- 吊銷的證書
- 密碼套件不匹配
- 網站連線超時

故障排除方法

步驟 1:確認流量通過代理

- 資料收集：發生問題時生成HAR檔案和PCAP。
- 標題分析：檢查HTTP響應中的Via報頭。`s_proxy`（Nginx代理）或`m_proxy`（模組化代理服務/MPS）的存在可確認流量已代理。
- TCP資料流：在Wireshark中，遵循TCP資料流確保連線到代理的IP，而不是目標IP。

步驟 2:驗證TLS解密狀態

- 瀏覽器檢查：按一下瀏覽器位址列中的鎖定圖示。如果Cisco安全訪問根證書出現在證書鏈中，則HTTPS檢查處於活動狀態。
- 驗證：交叉引用HAR/PCAP檔案中的Via報頭。
- OpenSSL指令：檢查證書鏈：
  `openssl s_client -connect www.example.com:443 -showcerts`
  此命令檢查伺服器顯示的證書鏈。從遍歷代理的電腦運行它以進行直接驗證。

步驟 3:隔離與消除

1. 階段A — 測試HTTPS檢查（Nginx層）：
   - 將有問題的域新增到SWG「不解密」清單中。
   - 保持檔案檢查處於啟用狀態。
   - 如果問題得到解決：根本原因可能是Nginx SSL/TLS檢查。分析PCAP是否存在密碼不匹配或SNI問題。使用具有和不具有代理的`curl`來比較行為。
   - 如果問題仍然存在：進入B階段。
2. 階段B — 測試檔案檢查（掃描層）：
   - 禁用特定流量的檔案檢查。
   - 如果問題得到解決：根本原因存在於檔案掃描引擎中。檢查PCAP和HAR，在實驗室中複製，並確定特定檔案或掃描簽名是否觸發了問題。
   - 如果未解決：請與支持部門聯絡，提供全面的日誌和調查結果。

常見問題和錯誤代碼

515上游證書不受信任

當SWG代理無法驗證目標伺服器的證書時，會發生此錯誤。原因包括證書鏈已過期、自簽名或不完整。

- 上的HTTPS檢查+檔案檢查：網站工作；無證書錯誤。
- 開啟HTTPS檢查+關閉檔案檢查：發現515錯誤，匹配使用者報告。
- HTTPS檢查關閉+檔案檢查關閉（不解密清單中的域）：未發現問題。

技術詳細資訊：如果上游伺服器依靠授權資訊訪問(AIA)獲取丟失的中間證書，Nginx代理可能會失敗，因為Nginx對AIA的處理不如檔案掃描代理服務那麼優雅。在TLS握手期間的SNI和SAN不匹配也會觸發故障。

517上游證書已吊銷

517錯誤表示SWG代理的CRL或OCSP檢查發現上游伺服器的證書已吊銷。

- 疑難排解:使用SSL Labs或OpenSSL等外部工具確認撤銷狀態。
- 說明文件:
  - 思科故障排除錯誤517 — 上游證書已吊銷
  - 瞭解常見證書和協定錯誤

證書錯誤處理選項

Cisco Secure Access將引入稱為「證書錯誤處理選項」的新功能，用於無需完全禁用解密的精細錯誤繞過。可以使用此功能而不是廣泛的「不解密」清單來管理由於檢查而觸發證書錯誤的域。
截至今天，此功能在Umbrella SIG中存在。CSA的功能請求詳細資訊。

502錯誤的網關

502錯誤表示SWG代理作為中間伺服器時收到來自上游伺服器的無效響應。

— 下游：使用者端對SWG代理
— 上游：SWG代理到目標伺服器

該錯誤總是出現在上游連線中 — 由於協定錯誤、TCP重置或報頭格式不正確。

常見502個原因

- 不支援的SWG密碼套件

- 客戶端證書身份驗證請求
- SWG代理新增的標頭

不支援的密碼套件

原因：伺服器需要SWG不支援的密碼（例如TLS_CHACHA20_POLY1305_SHA256）。
解析度：將該域新增到Selective Decryption清單。

測試命令：
使用代理：

```
curl -x proxy.sig.umbrella.com:80 -v xyz.com:80
curl -x swg-url-proxy-https.sigproxy.qq.opendns.com:443 -vvv -k "https://www.cnn.com" >> null
```

無代理：

```
curl -v www.xyz.com:80
```

Mac/Linux:

```
curl -vv -o /dev/null -k -L www.cnn.com
```

Windows:

```
curl -vv -o null -k -L www.cnn.com
```

客戶端證書身份驗證請求

原因：上游伺服器需要客戶端證書，SWG不支援該證書。
解析度：使用外部域管理清單(Umbrella SIG)或繞過安全代理（思科安全訪問）從代理繞過域。 僅繞過HTTPS檢查是不夠的。

代理新增的標頭

原因：啟用HTTPS檢查後，某些伺服器會拒絕帶有SWG新增的X-Forwarded-For(XFF)標頭的請求。
解析度：比較具有/不具有HTTPS和檔案檢查的行為。如果錯誤僅在出現XFF時發生，則Web伺服器可能配置錯誤。

範例：

```
curl https://www.xyz.com -k –header 'X-Forwarded-For:1.1.1.1' -o /dev/null -w "狀態代碼：%{http_code}" -s
```

狀態代碼：502

```
curl https://www.xyz.com -k -o /dev/null -w "狀態代碼：%{http_code}" -s
```

狀態代碼：200

新增了XFF報頭進行地理定位。如果伺服器無法處理它，則會出現502錯誤。

可能有害的PUA或已損壞的檔案

如果SWG無法使用檔案檢查掃描檔案（例如，受保護、請求範圍或損壞的檔案），則會阻止下載並報告 — 已阻止 — 可能有害的應用程式（受保護的檔案）

- 疑難排解:在阻止事件期間捕獲HAR。使用「覆蓋安全性」作為臨時解決方法。如果檔案已損壞或惡意，則必須在源位置對其進行更正。

潛在有害的類別和信譽塊

- 使用Talos檢查Web信譽(WBRS)。 如果域分類錯誤，請向Talos提交COG Jira請求以供稽核。Talos被歸類為安全或有利但仍是SWG塊，然後我們需要從SWG的Beaker服務進行檢查。

Akamai拒絕訪問SWG輸出IP

- SWG使用共用輸出IP。如果這些站點被IP信譽服務（例如Brightcloud）列入黑名單，則可能會拒絕對某些站點的訪問。

已知的問題:Youtube登入Bot和影片不可用

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）。