排除SWG網站訪問問題

目錄

簡介

本檔案介紹如何疑難排解使用Umbrella安全Web閘道(SWG)代理時出現的網站存取問題。

背景資訊

假設網站www.xyz.com無法通過SWG代理訪問，並且當使用者嘗試直接訪問Internet（圖片中沒有Umbrella SWG）時，該網站運行正常。 讓我們檢視通過SWG無法訪問網站時報告的各種症狀和不同型別的錯誤消息。最常見的是502網關錯誤，502無法轉發消息上游錯誤，撤銷上游證書，訪問被拒絕403被禁止，上游密碼不匹配，網站在旋轉一段時間後超時或類似情況。

由於上游塊而出現「Access Denied 403」錯誤

Web伺服器或上游端阻塞或限制SWG代理輸出IP範圍。例如，Akamai WAF的塊列出了幾個SWG輸出IP範圍。要解決此問題，唯一的選擇是聯絡網站管理員並讓其取消阻止我們的IP範圍。在此之前，使用外部域管理清單繞過SWG進行Anyconnect SWG和PAC檔案部署。簡而言之，此類問題並非由於代理本身，而是由於代理與Web伺服器之間的不相容所致。以下是專門針對因輸出IP地址塊而出現「拒絕訪問403」錯誤的連結參考知識庫的內容。

此外，以下連結還包含幾個可能的原因，說明Akamai具有阻止清單的IP地址。

由於Java問題而出現「Access Denied 403」錯誤

在已啟用檔案檢查設定的情況下，通過SWG MPS代理傳送請求時，無法訪問網站並引發「拒絕訪

問或403禁止 — Umbrella雲安全網關錯誤」。但是，如果禁用「檔案檢查」，則網站載入成功。或者，如果對網站進行旁路解密，網站載入成功。

問題的高級根本原因

什麼是MPS與Java相關的問題？

有問題的站點或Web伺服器在代理嘗試連線到伺服器後，將有關SNI或SSL警報的TLS警告返回給代理。基本上，這發生在客戶端hello傳送之後。MPS代理（基於Java等）在設計上，將描述欄位中帶有「無法識別的名稱」的任何TLS警報視為SNI分析過程中的錯誤，並終止事務。在此處找到更多詳細資訊

請注意，這不是SWG或MPS代理問題。這是與SWG或任何其他代理的不相容問題之一，原因是伺服器端配置錯誤。瀏覽器通常忽略此警告，但SWG或其他內容安全過濾器將SSL警告視為致命錯誤並終止會話，從而導致使用者獲得403個禁止的錯誤頁面。它還可以報告502 Bad Gateway錯誤，但通過我們看到的大多數示例是403禁止錯誤，如下圖所示。

15151734443924

由於MPS工作在應用層，因此TLS層很少甚至完全不控制TLS層如何根據TLS協定產生的警報處理事務。伺服器有責任確保其TLS端點/證書配置正確。請參閱此連結。

要縮小範圍或排除故障，可以很容易從SSL實驗中指出。

15152060146964

如果訪問網站時中間沒有SWG代理，或者繞過SWG的HTTPS檢查，則網站工作正常，因為瀏覽器忽略SNI無法識別的名稱警報，並繼續與Web伺服器通訊。

在撰寫本文時，我們向您建議的最佳緩解措施是推薦的解決方法。在不久的將來，使用新的代理架構，我們能夠更妥善地處理這些問題。

解析

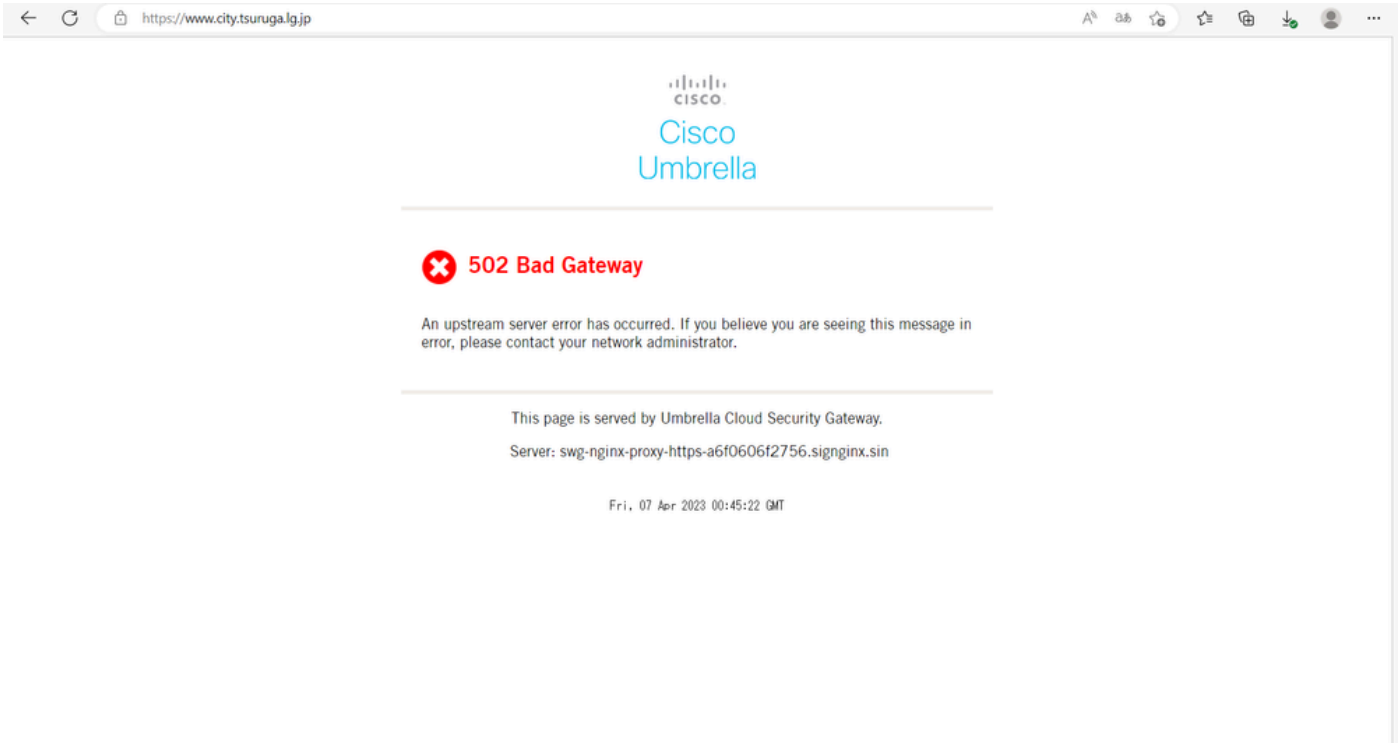
1.對受影響的域禁用解密 — 或
2.將域新增到目標清單並關聯允許規則（如果信任該站點）

什麼是502 Bad Gateway?

502 Bad Gateway Error表示伺服器正在充當網關或代理，並且從上游伺服器收到無效響應。當使用者嘗試通過SWG Proxy訪問網站時，會出現兩個通訊流。

a)客戶端 — >代理連線（下行）
b)代理 — >結束Web伺服器連線（上行）

502 SWG代理(MPS、Nginx)與終端伺服器連線之間發生錯誤的網關錯誤。



15026978020884

502壞網關的常見因素

1.不受支援的SWG密碼套件

2.客戶端證書身份驗證請求

3. SWG代理新增或刪除的標頭

不支援的SWG密碼套件

讓我們假設在TLS協商期間報告不受支援的SWG密碼套件的Web伺服器。請注意，SWG MPS（模組化代理服務）代理不支援TLS_CHACHA20_POLY1305_SHA256密碼套件。請注意，有單獨的文章介紹支援SWG的密碼套件和TLS。我們可以通過檢視客戶端hello和伺服器hello中在密碼套件交換期間捕獲的資料包來輕鬆查明此問題。作為疑難排解步驟，請使用CURL命令強制使用特定密碼來

縮小問題範圍並確認這是由密碼套件引起的，如範例1和2所示。

Curl命令示例:

<#root>

```
curl -vvv "" --ciphers TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 >> /dev/null
curl -vvv "" --ciphers ECDHE-RSA-AES256-GCM-SHA384 >> /dev/null
```

Testing website With Proxy:

```
 - 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
```

Testing website without Proxy

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

Mac/Linux:

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

Windows:

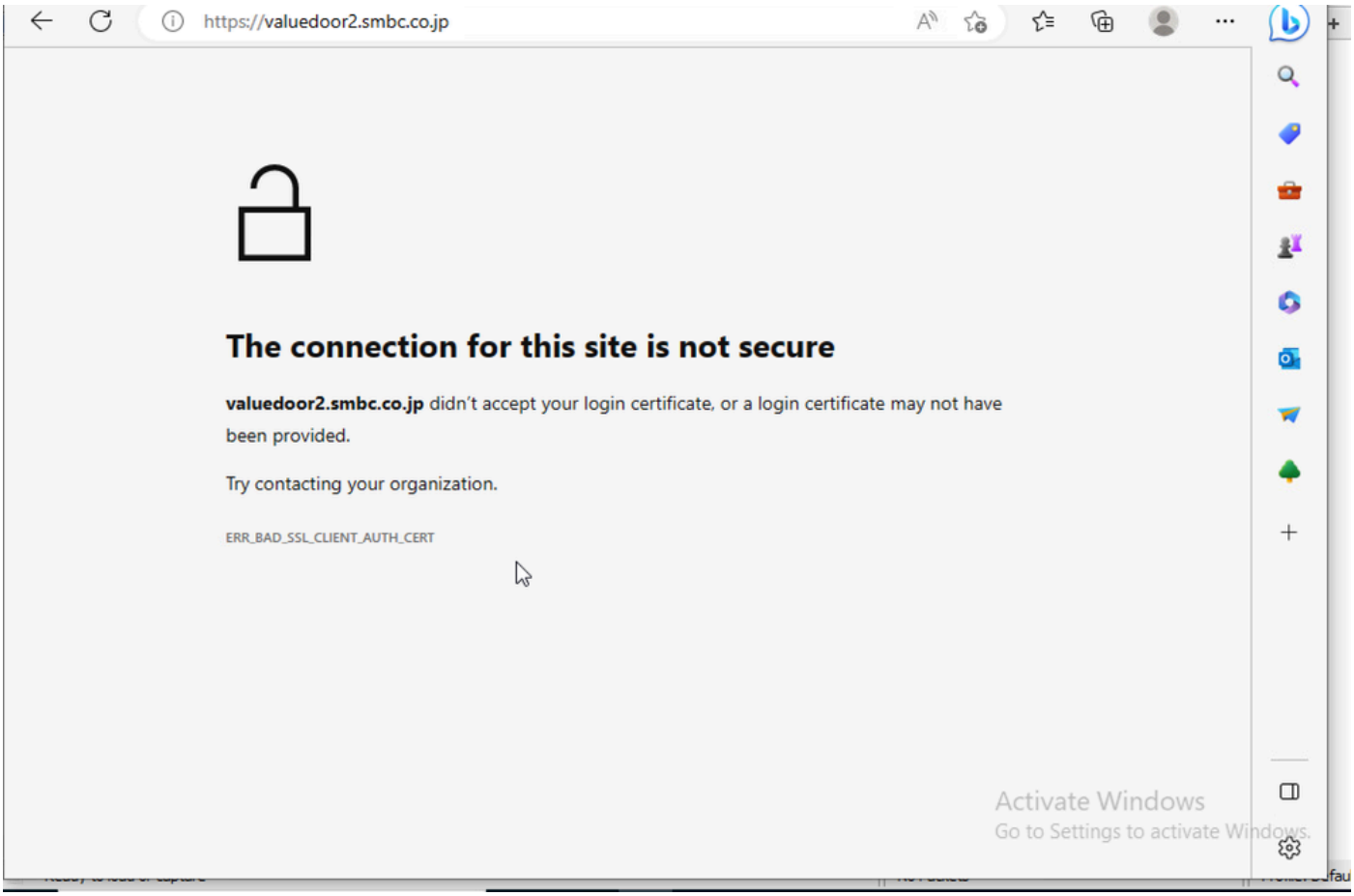
```
 - curl -vvv -o null -k -L www.cnn.com
```

解析

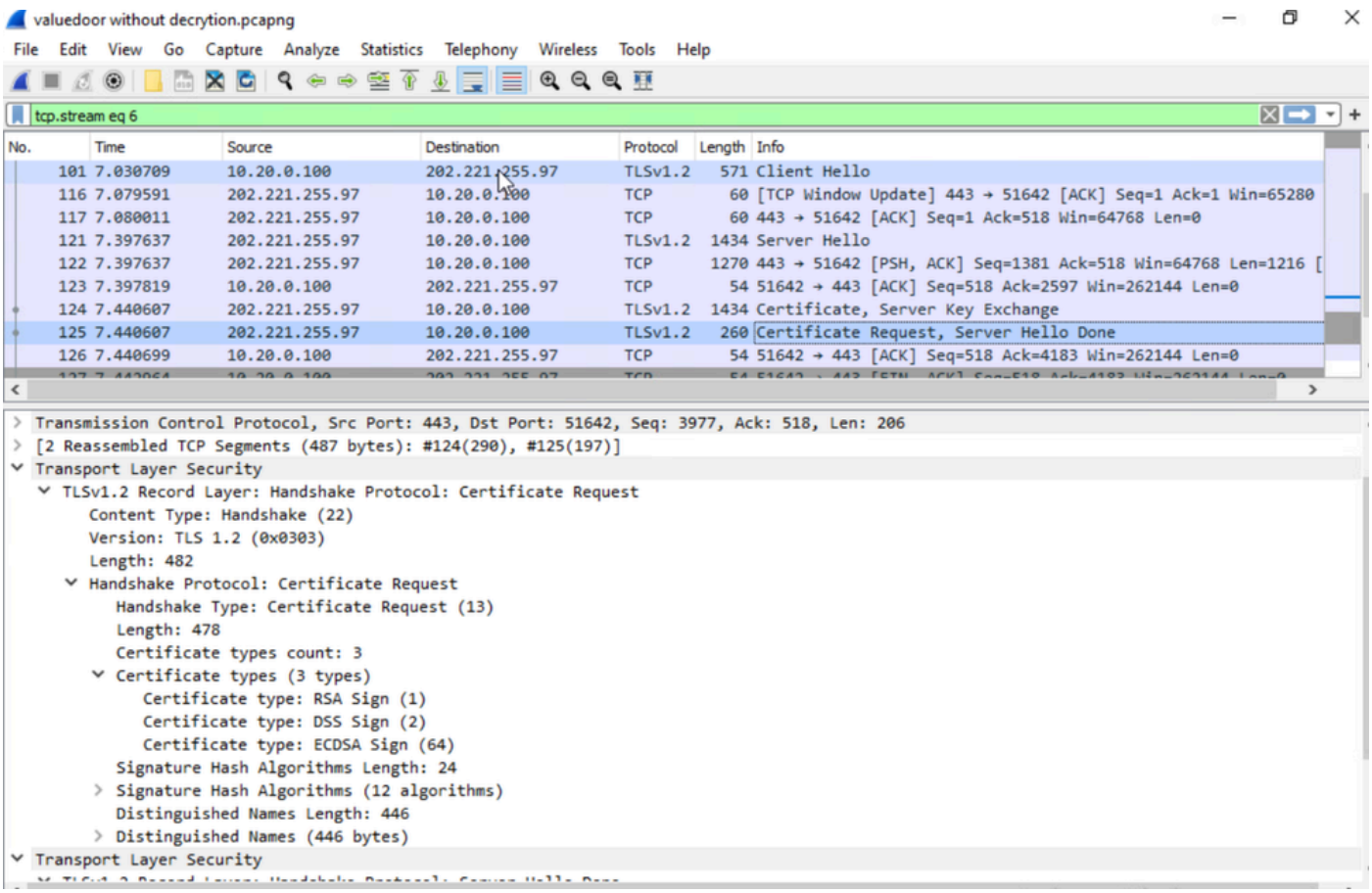
要解決此問題，請使用選擇性解密清單跳過有問題的網站的檢查。

客戶端證書身份驗證請求

在SWG代理和上游之間的TLS握手期間，上游Web伺服器需要客戶端證書身份驗證。由於客戶端證書身份驗證不受支援，我們需要使用外部域管理清單從代理繞過這些域，僅繞過https檢查是不夠的。舉例來說：https://valuedoor2.smbc.co.jp。



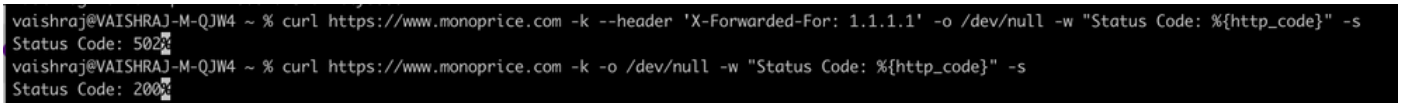
15027182308884



15027192992276

代理新增的標頭

啟用https檢查時，SWG代理新增了X-Forward-For標頭(XFF)，因此Web伺服器報告502錯誤網關錯誤。我們可以輕鬆地縮小502個壞網關問題中的大部分，方法是：首先使用https檢查或不使用https檢查來解決問題，然後使用或不使用檔案檢查來通過MPS代理排除檔案掃描問題。



15123666760340

```
curl https://www.xyz.com -k --header 'X-Forwarded-For: 1.1.1.1' -o /dev/null -w "Status Code: %{http_co
Status Code: 502
curl https://www.xyz.com -k -o /dev/null -w "Status Code: %{http_code}" -s
Status Code: 200
```

我們使用XFF報頭來啟用HTTPS檢查，以便上游伺服器基於客戶端IP（提供使用者的物理位置）提供最佳地理位置內容。

如果未啟用HTTPS檢查，則代理不會新增此標頭，因此不會出現502 Bad Gateway錯誤。這不是SWG代理問題。此錯誤是因為上游Web伺服器配置錯誤，不支援標準XFF標頭。

解析

要解決此問題，請使用選擇性解密清單繞過特定域的HTTPS檢查。

- 517上游證書已吊銷
- 證書和TLS協定錯誤
- 手動選擇SWG DC進行內部測試

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）。