瀏覽到某些站點時出現502 / 504 GATEWAY_TIMEOUT錯誤

目錄

問題：

問題：

瀏覽特定站點時，為什麼會出現502 / 504 GATEWAY_TIMEOUT錯誤？

症狀:使用者在瀏覽某些網站時從Cisco WSA收到502或504個網關超時錯誤

使用者在瀏覽網站時收到502或504個網關超時錯誤。訪問日誌顯示「NONE/504」或「NONE/502」

訪問日誌行示例：

1233658928.496 153185 10.10.70.50 **NONE/504** 1729 GET http://www.example.com/ - DIRECT/www.example.com - .....

WSA可能返回502或504網關超時錯誤的原因有很多。雖然這些錯誤響應是相似的，但瞭解它們之間的細微差別非常重要。

以下是可能發生的情況型別的一些示例：

- **502:**WSA已嘗試與Web伺服器建立TCP連線，但尚未收到SYN/ACK。
- **504:**WSA正在接收TCP重設(RST)，該RST終止與Web伺服器的連線。
- **504:**在與Web伺服器通訊之前，WSA沒有從所需服務獲得響應，例如DNS失敗。
- **504:**WSA與Web伺服器建立了TCP連線並傳送了GET請求，但WSA從未收到HTTP響應。

下面是每個方案的示例以及有關潛在問題的更多詳細資訊：

502:WSA已嘗試與Web伺服器建立TCP連線，但尚未收到SYN/ACK。
如果Web伺服器沒有響應WSA的SYN資料包，在嘗試一定次數後，客戶端將收到502網關超時錯誤。 典型原因如下： 1. Web伺服器或Web伺服器網路出現問題。 2. WSA網路上的網路問題阻止SYN資料包進入Internet。 3.防火牆或類似裝置正在丟棄WSA SYN資料包或Web伺服器的SYN/ACK 4. WSA上啟用了IP欺騙，但未正確配置（無返迴路徑重新導向）

故障排除步驟：

第一步是驗證WSA是否能ICMP ping通Web伺服器。可以使用以下CLI命令完成此操作：
WSA> *ping www.example.com*
如果ping失敗，並不意味著伺服器已關閉。這可能表示ICMP封包在路徑中的某個位置遭封鎖。如果ping成功，我們可以確定WSA與Web伺服器之間具有基本的第3層連線。
Telnet測試將驗證WSA是否能夠在埠80上與Web伺服器建立TCP連線。有關執行telnet測試的資訊，請參閱本文中的詳細說明。

網路問題或防火牆阻止
如果ping成功，但telnet失敗，則很有可能是過濾裝置（如防火牆）阻止此流量通過網路。建議分析防火牆日誌和/或從防火牆捕獲的資料包以瞭解更多詳細資訊。
啟用IP欺騙，但未正確配置
如果通過WSA顯式代理或telnet測試成功，這表明WSA可以直接與Web伺服器通訊，但是當客戶端通過WSA進行IP欺騙時，會出現問題。

沒有客戶端IP欺騙：
- WSA使用自己的IP地址作為源向Web伺服器傳送SYN。封包傳回時，會直接傳回WSA。

使用客戶端IP欺騙：
- WSA傳送SYN，但使用客戶端的IP作為源。如果沒有特殊的網路設定，返回資料包將被傳送到客戶端，而不是WSA。
- 要使用客戶端IP欺騙，必須以非常特定的方式配置網路，以便正確重定向資料包。如果Web伺服器返迴路徑資料包被傳送到客戶端而不是WSA，則WSA將永遠不會看到伺服器SYN/ACK，並將向客戶端傳送502網關超時錯誤。

504:WSA正在接收TCP重設(RST)，該RST終止與Web伺服器的連線。

如果WSA在其與Web伺服器的上游連線上收到TCP重置資料包，則WSA將向客戶端傳送504網關超時錯誤。

典型原因如下：
1.思科第4層流量監控器(L4TM)正在封鎖WSA代理連線Web伺服器。
2.防火牆、IDS、IPS或其他資料包檢測裝置正在阻止WSA。

故障排除步驟：
首先確定TCP RST是來自L4TM還是來自其他裝置。
如果L4TM阻塞此流量，則該流量會顯示在GUI報告中「***Monitor -> L4流量監控***」下。 否則，RST來自其他裝置。
L4TM封鎖：
建議如果L4TM阻塞，不要在同樣運行WSA代理的連線埠上阻塞。原因有多種：
1.發生問題時，WSA代理會提供一個友好的錯誤消息，而不只是TCP重置連線。這將有助於在終端使用者被阻止時減少他們的困惑。
2. WSA代理能夠掃描和阻止特定內容，而L4TM阻止與列入黑名單的IP地址匹配的所有流量。
若要將L4TM設定為不在代理連線埠上封鎖，請前往「***GUI ->安全服務 — > L4流量監控***」。
如果該站點是一個已知錯誤的網站，但有原因允許流量，則該站點可以是中列出的白色：
"***GUI ->網路安全管理員 — > L4流量監控器 — >允許清單***"

防火牆/IDS/IPS阻止：
如果網路上的另一台裝置阻止了WSA連線到Web伺服器，建議分析以下內容：
1.防火牆阻止日誌

2.問題期間的輸入/輸出封包擷取

阻止日誌可以快速確認裝置是否正在阻止WSA。有時，防火牆、IPS或IDS會阻止流量，並且無法正確記錄流量。如果是這種情況，唯一能證明TCP RST來源的方法就是從裝置取得輸入和輸出擷取。如果將RST從輸入介面發出，並且沒有資料包通過輸出端，則絕對是由安全裝置導致的。

504:WSA與Web伺服器建立了TCP連線並傳送了GET請求，但WSA從未收到HTTP響應。

如果WSA傳送HTTP GET但從未收到響應，則會向客戶端傳送504網關超時錯誤。

典型原因如下：

- 防火牆、IDS、IPS或其他資料包檢測裝置允許TCP連線，但阻止HTTP內容到達Web伺服器。在這種情況下，telnet測試可能有助於隔離被阻止的哪種HTTP資料。

防火牆阻止日誌可以快速確認裝置是否阻止WSA/為什麼阻止。有時，防火牆、IPS或IDS會阻止流量，並且無法正確記錄流量。如果是這種情況，唯一能證明TCP RST來源的方法就是從裝置取得輸入和輸出擷取。如果將RST從輸入介面發出，並且沒有資料包通過輸出端，則絕對是由安全裝置導致的。

使用telnet測試與Web伺服器的連線

在WSA CLI中執行**telnet**命令：

WSA> **telnet**
請選擇您要從哪個介面telnet。
1.自動
2.管理(192.168.15.200/24:wsa.hostname.com)
3. P1(192.168.113.199/24:data.com)
[1]> **3**

輸入遠端主機名或IP地址。
[]> www.example.com

輸入遠端埠。
[25]> **80**

正在嘗試10.3.2.99...
已連線到www.example.com.
跳脫字元為「^]」。

附註:紅色的「已連線」消息表明WSA和Web伺服器之間已成功建立TCP。

也可以通過此telnet會話手動傳送HTTP請求。以下是可以在「已連線」消息後鍵入的請求示例：

獲取http://www.example.com **HTTP/1.1**
主機： www.example.com
{Enter}

附註：確保在結尾新增額外的回車，否則伺服器將不會響應請求。