使用WCCP發現路徑MTU上的WSA行為

目錄

簡介

本文描述當您的配置包括Web快取通訊協定(WCCP)和路徑最大傳輸單元(MTU)發現時，路由器捨棄封包時遇到的問題，並且提供了問題的解決方案。

背景資訊

前期

單獨檢視時，許多功能在處理特定問題時非常出色。不過，有時候，如果將兩種或三種技術相結合，就會產生一些令人尷尬的行為，而您必須引入其他特徵或應對方法才能使其正常工作。例如，使用生成樹和開放最短路徑優先(OSPF)以及第2層(L2)收斂比OSPF（如果使用最小失效間隔，則為1）花費更長（20秒），但用多生成樹(MST)替換生成樹後，它再次正常工作。

在WCCP和路徑MTU發現之間觀察到相同的互操作性行為；許多人認為這就是通用路由封裝(GRE)標頭問題。但是本檔案將說明真正的原因。

路徑MTU發現和WCCP如何獨立工作

路徑MTU探索

每行對資料包的大小都有自己的限制。如果傳送的封包大於支援的封包，就會遭到捨棄。途中L3裝置（路由器）的角色之一是負責將大型資料包從一條線路分割到另一條線路，以確保端到端通訊對每條線路的功能透明。

但是，有時終端主機的配置方式使其資料包無法截斷（例如，加密檔案、語音呼叫）。 此資訊是透

過IP標頭中的「不分段(DF)」位元傳遞的。路由器捨棄此類封包，但路由器嘗試透過網際網路控制訊息通訊協定(ICMP)訊息（型別3 — 無法到達目的地，代碼4 — 需要分段，但已設定DF位元）向終端主機報告。 這樣，主機就知道將來會傳送較小的封包。

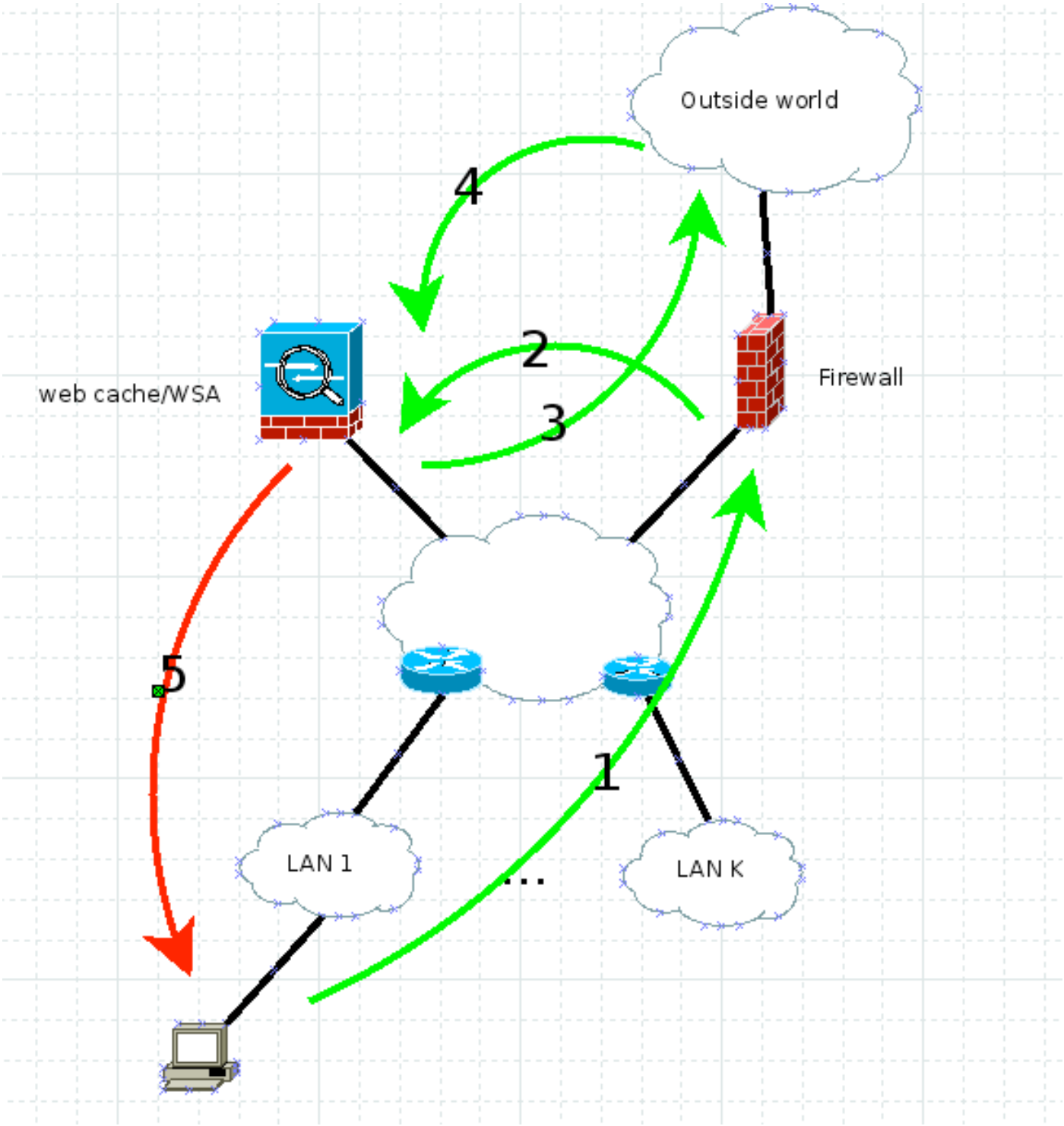
這是路徑MTU發現的核心。您可以傳送已設定DF位元的大型封包，以瞭解它們是朝著結尾傳送，還是如前所述接收ICMP報告。確定可行的最大資料包大小後，將其用於任何進一步的通訊。如需詳細資訊，請參閱RFC 1191。

預設情況下，網路安全裝置(WSA)採用路徑MTU發現。因此，其所有產生的封包都使用預設組態設定DF位元。

WCCP

如果您需要在他人不知情的情況下對Web流量強制實施網路安全，則可以通過不可見的代理運行其流量。WCCP是用於攔截裝置（路由器/防火牆）和Web快取引擎/代理（本例中為WSA）之間通訊的協定。

此圖說明此場景中的流量傳輸方式：



工作原理如下：

1. 客戶端傳送帶有IP源、其IP地址（客戶端IP地址）和目標伺服器IP地址的HTTP GET。

2. 防火牆或路由器會攔截HTTP GET，並通過WCCP GRE或純L2將其轉送到Web快取/WSA。源仍是客戶端IP地址，目標仍是Web伺服器IP地址。

3. WSA檢查請求，如果請求合法，則將其映象到Web伺服器。根據您是否啟用了客戶端IP地址欺騙，這裡的目標IP地址是Web伺服器IP地址，而源IP地址可能是WSA或客戶端。在本範例中，這並不重要，因為兩種情況下的返回流量都必須命中WSA。

4. 在WSA處檢查返回流量。

5. WSA使用源IP地址、ALWAYS網路伺服器IP地址（因此客戶端不會受到懷疑）和目標客戶端IP地址將響應傳送到客戶端。

問題

如果圖中的一台路由器必須將流量分段，會發生什麼情況？WSA將DF位元放在封包編號5上，但必須將其分段。路由器將其捨棄，並告訴傳送者需要分段，但已設定DF位元（ICMP型別3代碼4）。畢竟，RFC 1191現在必須工作，傳送者必須降低其封包大小。

使用WCCP時，來源IP位址是Web伺服器IP位址，因此此ICMP永遠不會到達WSA;相反，它會嘗試訪問真正的Web伺服器（請記住，底部的此路由器並不知道WCCP）。 這就是將WCCP和路徑MTU發現結合在一起有時會破壞網路設計的方式。

解決方案

解決此問題有四種方法：

- 發現實際MTU，然後在WSA上使用**etherconfig**降低介面的MTU。請記住，TCP標頭是60,IP是20，而使用ICMP時，會將8位元組新增到IP標頭。
- 禁用路徑MTU發現(**路徑**發現CLI WSA命令)。 這會導致TCP MSS為536，這可能會導致效能問題。
- 更改網路，以便WSA和客戶端之間沒有L3分段。
- 在相關介面上的每台Cisco路由器上使用**ip tcp mss-adjust 1360**（或其他計算的數字）命令。

附加說明

調查此問題時，發現如果您將代理明確設定為客戶端幾分鐘，然後刪除，則問題會在接下來的4到5小時內得到解決。這是因為在WSA和客戶端之間的路徑MTU發現機制在顯式模式下工作這一事實。WSA發現路徑MTU後，會將其與發現的TCP MSS一起儲存到內部表以供參考。顯然，此表每4到5個小時刷新一次，這使得解決方案在經過這麼多時間後不再工作。