對Umbrella元件使用埠地址轉換時排除埠耗盡故障

目錄

簡介

本檔案介紹使用漫遊使用者端和/或虛擬裝置的Umbrella客戶，以及在使用連線埠位址轉譯的防火牆中遇到連線埠耗盡問題。在擁有大量漫遊客戶端和/或通過VA的大量流量的環境中，這種情況最有可能發生。症狀包括返回緩慢或超時的DNS查詢。

原因

漫遊客戶端和虛擬裝置都不會快取對DNS查詢的響應。此外，漫遊客戶端會傳送頻繁的「探測」DNS請求，以分析網路環境並檢查運行狀況。

行動

- 確保在Umbrella控制面板上的「域管理」中正確配置您的內部域。它們必須包含Active Directory區域（和/或其他內部區域），才能減少高頻查詢的量。
- 檢查防火牆上的某些PAT設定：
  - 長UDP會話超時可能是一個問題。我們通常建議大約15秒的UDP會話超時。但是，請注意，如果UDP被網路中的其他應用程式大量使用，則它們可能會有更長的超時時間，您必須考慮這些超時時間。
  - 根據您的防火牆，可以增加其PAT池的大小以增加同時連線的數量。
- 如果您的IP地址可以專用於虛擬主機，請在防火牆上使用1:1 NAT而不是PAT。附註：「1:1 NAT」有時也稱為「直接NAT」，但這是用詞不當；正確的技術術語是「1:1 NAT」。
- 檢視每個IP的連線限制。通常情況下，一項本不應適用於相關裝置的政策實際上是在實施限制。請參見下一節瞭解如何進行確認。

檢查ASA上的每個IP連線限制

使用以下步驟：

- 使用捕獲配置ASA以檢視防火牆丟棄資料包的原因：

```
capture asp type asp-drop all match ip any host 208.67.222.222
```

- 尋找針對相關IP的遭捨棄封包。連線限制原因顯示為「Drop-reason:(conn-limit)"
- 使用命令檢查主機連線限制：

```
show local-host detail | begin <IP Address of VA or roaming client>
```

  - 此數字是否在某個限制（即999）下保持靜態並且從不增加？如果是，則表示連線限制。
- 檢查應用此命令的服務策略；如果找到，請檢查其策略對映：

```
show run service-policy, show policy-map NAME
```

  - 如果找到將每主機連線限制設定為1000（例如）的策略對映「名稱」，則會導致從裝置丟棄所有新DNS資料包，直到有更多連線可用。UDP是無狀態且不會重試。
- 要解決此問題，請刪除該服務策略（內部沒有服務策略名稱）。 連線必須開始超出1K限制（從我們的示例中）。 VA比漫遊客戶端更易發生這種情況。

進一步建議

如果這些建議不起作用，則可能的解決方法是：

1. 使用「Umbrella dashboard —> Reporting —> Top Destinations」報告可以識別在過去24小時內具有大量請求的一個或多個域。
2. 在Umbrella dashboard —> Configuration —> Domain Management中，將一個或多個高容量域新增到清單中，將「Apply to」設定為「All Appliances and Devices」。
3. 之後，這些域的查詢由VA轉發到本地DNS。理想情況下，本地DNS必須配置為轉發到位於208.67.220.220/208.67.222.222的Umbrella DNS，但可以配置為轉發到任何外部DNS。
4. 本地DNS處理其授權的任何域的查詢。
5. 假設本地DNS接受非本地域的查詢，則這些其他域的查詢將轉發到外部DNS。

這是因為本地DNS可以快取DNS結果，而漫遊客戶端和虛擬裝置不進行快取。請注意，使用此變通方法會導致內部DNS上的流量增加和負載增加，因此請仔細監控這些流量，以確保它們不會過載。

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）。