在雙ISP設定中，主ISP鏈路恢復聯機後，通過ASA的UDP流量出現故障

目錄

簡介

如果自適應安全裝置(ASA)的每個目標子網具有兩個出口介面，並且通往目標的首選路由從路由表中刪除一段時間，則當首選路由重新新增到路由表中時，使用者資料包協定(UDP)連線可能會失敗。TCP連線也可能受此問題影響，但由於TCP偵測到封包遺失，這些連線會被端點自動關閉，並在路由變更後使用更佳的路由重新建立。

如果使用路由協定，並且拓撲更改觸發ASA上的路由表發生更改時，也會出現此問題。

開始之前

需求

為了解決此問題，ASA的路由表必須更改。這在雙ISP鏈路冗餘方式或ASA通過IGP(OSPF、EIGRP、RIP)學習路由時很常見。

當主ISP鏈路恢復聯機或所述IGP發現重新收斂時，就會發生此問題，因為重新收斂導致ASA使用的較不優先的路由被替換為較優先的低度量路由。一旦主路由或首選路由重新安裝到ASA的路由表中，您就會看到長時間運行的連線（如UDP SIP註冊、GRE等）失敗。

採用元件

本檔案中的資訊是根據以下硬體和軟體版本：

- 任何Cisco ASA 5500系列自適應安全裝置
- ASA 8.2(5)、8.3(2)12、8.4(1)1、8.5(1)及更高版本

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

問題

如果從ASA的路由表中刪除了路由表條目，並且沒有來自要到達目標的介面的路由，則ASA將刪除通過防火牆建立的與該外部目標的連線。發生此情況時，可以使用另一個介面重新建立連線，同時存在目的地的路由條目。

但是，如果將更具體的路由新增回表中，則連線將不會更新為使用新的、更具體的路由，並且將繼續使用不太理想的介面。

例如，假設防火牆有兩個面向Internet的介面 — 「outside」和「backup」，並且這兩個路由存在於ASA的配置中：

```
route outside 0.0.0.0 0.0.0.0 10.1.1.1 1 track 1
route backup 0.0.0.0 0.0.0.0 172.16.1.1 254
```

如果外部介面和備份介面均為「up」，則通過防火牆出站構建的連線將使用外部介面，因為它的首選度量是1。如果外部介面關閉（或者跟蹤路由的SLA監控功能遇到與跟蹤的IP的連線斷開的情況），則使用外部介面的連線將斷開，並使用備份介面重新構建，因為備份介面是唯一具有到達目標的路由的介面。

當重新開啟外部介面或跟蹤的路由再次成為首選路由時，會出現此問題。路由表更新為優先使用原始路由，但現有連線仍存在於ASA上並遍歷備份介面，不會刪除這些連線，也不會在外部介面上使用更優先的度量重新建立。這是因為備份預設路由仍存在於ASA的特定於介面的路由表中。連線會繼續使用具有較少首選路由的介面，直到連線被刪除；對於UDP，這可能是不確定的。

這種情況可能會導致長時間使用的連線出現問題，例如外部SIP註冊或其他UDP連線。

解決方案

為了解決此特定問題，ASA新增了一項新功能，如果路由表中新增了更優先的通往目的地的路由，該功能將導致連線中斷並在新介面上重建。若要啟用該功能（預設為停用），請對**timeout floating-conn**命令設定非零逾時。此超時（以HH:MM:SS指定）指定ASA在將更多首選路由新增到路由表後斷開連線之前等待的時間：

以下是啟用此功能的CLI範例。使用此CLI時，如果現有連線上接收到資料包，並且此連線現在有通向目的地的更首選的另外一條路由，則連線將在1分鐘後斷開（並使用更首選的新路由重建）：

```
ASA# config terminal
ASA(config)# timeout floating-conn 0:01:00
ASA(config)# end
ASA# show run timeout
timeout conn 1:00:00 half-closed 0:10:00 udp 0:50:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout sip-provisional-media 0:02:00 uauth 0:01:00 absolute
timeout tcp-proxy-reassembly 0:01:00
timeout xlate 0:01:00
timeout pat-xlate 0:00:30
timeout floating-conn 0:01:00
ASA#
```

8.2(5)、8.3(2)12、8.4(1)1和8.5(1)版（包括ASA軟體的較新版本）將此功能新增到ASA平台。

如果運行不實施此功能的ASA代碼版本，問題的解決方法是手動刷新繼續採用不太首選路由的UDP連線，儘管通過**clear local-host *<IP>***或**clear-conn *<IP>***提供了更好的路由。

命令參考在timeout部分下列出此新功能。

相關資訊

- 技術支援與文件 - Cisco Systems