在双ISP设置中，主ISP链路重新联机后，通过ASA的UDP流量发生故障

目录

[简介](#)
[开始使用前](#)
[要求](#)
[使用的组件](#)
[规则](#)
[问题](#)
[解决方案](#)
[相关信息](#)

简介

如果自适应安全设备(ASA)每个目标子网有两个出口接口，并且到目的地的首选路由从路由表中删除一段时间，则当首选路由重新添加到路由表时，用户数据报协议(UDP)连接可能会失败。TCP连接也可能受问题影响，但是由于TCP检测到丢包，这些连接会由终端自动断开，并在路由更改后使用更优的路由重新构建。

如果使用路由协议且拓扑更改触发ASA上路由表的更改，也可以看到此问题。

开始使用前

要求

要遇到此问题，ASA的路由表必须更改。当ASA通过IGP(OSPF、EIGRP、RIP)获取路由时，冗余方式的双ISP链路通常会出现这种情况。

当主ISP链路恢复联机或所述IGP发现重新收敛时，会发生此问题，因为ASA使用的较不首选的路由被首选的较低度量路由取代。然后，当主路由或首选路由重新安装到ASA的路由表中时，您将看到长期连接（如UDP SIP注册、GRE等）失败。

使用的组件

本文档中的信息基于下列硬件和软件版本：

- 任何Cisco ASA 5500系列自适应安全设备
- ASA版本8.2(5)、8.3(2)12、8.4(1)1、8.5(1)及更高版本

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

问题

如果路由表条目从ASA的路由表中删除，并且没有从接口到达目的地的路由，则通过防火墙构建的与该外部目的地的连接将被ASA删除。这样，就可以使用包含目的地路由条目的不同接口重新建立连接。

但是，如果将更具体的路由添加回表中，则连接不会更新为使用新的更具体的路由，并且会继续使用不太理想的接口。

例如，假设防火墙有两个面向Internet的接口 — “外部”和“备份”，并且ASA配置中存在这两个路由：

```
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
```

如果外部接口和备份接口都为“up”，则通过防火墙建立的出站连接将使用外部接口，因为它的首选度量为1。如果外部接口关闭（或跟踪路由的SLA监控功能遇到与跟踪的IP的连接丢失），则使用外部接口的连接将断开并使用备份接口重新建立，因为备份接口是唯一具有路由的接口目的地。

当外部接口重新打开或跟踪的路由再次成为首选路由时，就会出现问题。路由表会更新为首选原始路由，但现有连接仍然存在于ASA上并遍历备份接口，因此不会删除并使用首选度量在外部接口上重新创建。这是因为ASA的接口特定路由表中仍然存在备份默认路由。连接继续使用具有较不首选路由的接口，直到删除连接；在UDP中，这可能是不确定的。

这种情况可能导致长期连接出现问题，例如外部SIP注册或其他UDP连接。

解决方案

为了解决此特定问题，ASA中添加了一项新功能，如果向路由表中添加了通往目的地的更优先路由，该功能将导致连接断开并在新接口上重建。要激活该功能（默认情况下禁用此功能），请将非零超时设置为**timeout floating-conn** 命令。此超时（以HH:MM:SS指定）指定在将更首选的路由添加到路由表后，ASA在断开连接之前等待的时间：

这是启用该功能的CLI示例。使用此CLI时，如果在现有连接上收到数据包，而该连接现在有一条到目的地的不同、更优先的路由，则该连接将在1分钟后断开（并使用新的、更优先的路由重建）：

```
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#
```

此功能在版本8.2(5)、8.3(2)12、8.4(1)1和8.5(1)中添加到ASA平台，包括ASA软件的更高版本。

如果运行的ASA代码版本不实施此功能，则问题的解决方法是手动刷新继续采用较不首选路由的

UDP连接，**尽管通过clear local-host *<IP>*或*clear-conn* <IP>提供了更好的路由。**

命令参考在超时部分下列出此新功能。

相关信息

- 技术支持和文档 - Cisco Systems