

# 在主ISP林克回来联机在一个双重ISP设置后，UDP流量通过ASA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

如果可适应安全工具(ASA)有每个目的地子网两出口接口和首选路由对目的地从路由表有一段时间了删除，用户数据报协议(UDP)连接可以发生故障，当首选路由获得重新加写了对路由表。TCP连接也许受问题的也影响，但是，因为TCP检测包丢失，这些连接由终端自动地切断，并且被重建使用更多最佳路由在路由更改以后。

此问题能也被看到是否使用路由协议，并且拓扑更改触发在路由表上的一个变化在ASA。

## 开始使用前

### 要求

为了遇到此问题，ASA的路由表必须更改。这是普通与双重ISP链路在冗余方式或，当ASA通过IGP (OSPF学习路由，EIGRP，RIP)。

此问题出现，当主ISP链路回来联机或前述IGP看到再收敛由于哪些由ASA使用的一较少首选路由用首选的更低量度路由替换。一旦主要的或首选路由被重新安装到ASA的路由表，您然后会看到长寿的连接，例如UDP SIP注册，GRE等等，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系列可适应安全工具
- ASA版本8.2(5)，8.3(2)12，8.4(1)1，8.5(1)及以后

### 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的路由表删除，并且没有路由在到达目的地的接口外面，通过与该外国目的地的防火墙被建立连接将由ASA删除。这发生，以便连接可以再被建立使用与路由条目的一个不同的接口目的地存在的。

然而，如果更加特定的路由被添加回到表，连接不会更新使用新，更加特定的路由和继续使用少最佳的接口。

例如，请考虑防火墙有面对互联网的两个接口-“外部”，并且“请备份”-，并且这两个路由在ASA的配置里存在：

```
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
```

如果外部和备份接口“”，则连接通过防火墙构件出站将使用外部接口，因为有首选的量度1。如果外部接口被关闭(或跟踪路由的SLA监控功能遇到失去连接对被跟踪的IP)，使用备份接口，连接使用外部接口将被切断并且被重建了，因为备份接口是唯一的接口用路由对目的地。

问题发生，当外部接口带来备份时或被跟踪的路由再变为支持的路由。路由表更新偏好原始路由，但是现有连接在ASA在与更多首选的量度的外部接口继续存在和横断备份接口和没有删除并且被再创。这是因为备用默认路由在ASA的特定接口的路由表里仍然存在。连接继续以较少首选路由使用接口，直到连接删除;一旦UDP，这也许不确定。

此情况能引起问题由于长寿的连接，例如外部SIP注册或其他UDP连接。

## 解决方案

为了涉及此特定问题，新特性被添加了到在新接口将造成连接被切断和重建的ASA，如果对目的地的更多首选路由被添加到路由表。为了激活功能(默认情况下禁用)，设置一非零超时为**超时浮动CONN**命令。此超时(指定在HH : MM:SS)指定ASA等待的时间，在切断连接前更多首选路由一次被添加回到路由表：

这是启用功能CLI示例。使用此CLI，如果数据包在当前有一不同的现有连接接收，对目的地的更多首选路由，连接将扯下1分钟后(和重建使用新，更多首选路由)：

```
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#
```

此功能被添加到版本8.2(5)的ASA平台，8.3(2)12，8.4(1)1和8.5(1)，包括ASA软件最新版本。

如果运行的ASA代码版本不实现此功能，对问题的一应急方案是手工冲洗继续上尽管佳路由的较少首选路由使可用通过**结算local-host <IP>**或**clear conn <IP>**的UDP连接。

命令参考参考目录在[超时](#)部分下的此新特性。

## 相关信息

- [技术支持和文档 - Cisco Systems](#)