当ASA重新启动时，无线移动性连接发生故障和不恢复

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[规则](#)
[问题](#)
[示例网络结构](#)
[问题触发](#)
[解决方案](#)
[解决方案 1](#)
[解决方案 2](#)
[相关信息](#)

简介

本文描述移动性路径连接的问题(使用用户数据报协议(UDP)和IP协议93)该横断可适应安全工具(ASA)也许断开和继续发生故障，直到移动性设备重新加载，或者移动性路径流量被终止并且短时间被留下非激活然后重新启动。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科可适应安全工具(ASA)
- 无线局域网控制器(WLC)

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的信息，请参阅 Cisco 技术提示规则。

问题

在这种情况下一个无线局域网控制器(WLC) 10.10.1.2的尝试通信与WLC在10.10.9.3，但是通信发生故障。

此问题可以由任何这些事件触发：

- ASA重新启动。
- 管理员或路由协议修改路由表。
- 接口由管理员关闭，然后带来备份。

除移动性流量以外，此问题也许是有经验的为所有UDP或非TCP IP协议。

此问题是没有bug，然而网络拓扑和ASA配置的结果。下面请参阅关于原因和解决方案对此问题。

示例网络结构

ASA路由配置：

```
!
route outside 0.0.0.0 0.0.0.0 192.168.4.3 1
route inside 10.0.0.0 255.0.0.0 192.168.254.1 1
!
same-security-traffic permit intra-interface
!
```

ASA dmz接口配置：

```
!
interface Gigabit-Ethernet0/1.10
vlan 10
nameif dmz
security-level 75
ip address 10.10.9.1 255.255.255.240 standby 10.10.9.2
!
```

问题触发

当在10.10.1.2的WLC发送流量被注定对WLC在10.10.9.3时，问题被触发。这些数据包在发送移动性流量错误的ASA接口的其连接表里造成ASA建立连接(里面)。

此问题由目的地接口“dmz是”导致的ASA的down/down状态，在连接被建立了时候，导致被构件一个不同的连接，非最优接口。dmz接口也许下降由于电缆问题、以太网或者Port-Channel协商问题，或者也许管理性被关闭的。

在问题时，移动性路径连接能被看到和创建作为“接口内” ASA，路由他们到达的数据包取消同一个内部接口：

```
ASA# show conn address 10.10.1.2
15579 in use, 133142 most used
97 inside 10.10.9.3 inside 10.10.1.2, idle 0:00:00, bytes 32210
UDP inside 10.10.9.3:16666 inside 10.10.1.2:16666, idle 0:00:00, bytes 4338, flags -
97 inside 10.10.9.3 inside 10.10.1.2, idle 0:00:00, bytes 157240
ASA#
```

在10.10.1.2的移动性终端继续发送被注定的流量到10.10.9.3，匹配这些现有连接。即使dmz接口是进步对UP/UP状态，从10.10.1.2发出的移动性流量在重置连接超时在ASA的，延长问题的表里将匹配现有连接(而不是建立对dmz接口的一个新连接)。

总之，这些事件能触发问题：

1. 在10.10.1.2的设备发送协议97或UDP数据包对10.10.9.3。
2. ASA收到在内部接口的数据包，但是dmz接口发生故障，导致具体的路由对目的地网络丢失从路由表。因为**intra-interface命令相同的安全性的permit**在ASA启用，在连接表里跟随为10.0.0.0/8网络上一步配置的一条静态小路通过内部接口，建立连接，然后发送数据包取消往内部网络的内部接口。
3. 有时dmz接口也许恢复，并且路由被添加回到表;然而，因为协议97流量的连接在步骤#2已经被建立了，后续信息包将匹配连接，并且路由表覆盖，并且流量不到达在dmz的服务器。

解决方案

解决方案 1

此问题的一个可能的解决方案将删除**intra-interface命令相同的安全性的permit**从ASA。此解决方案防止U字型转向连接被构件取消原始信息包接收，允许将被构件的正确连接的同一个接口，当接口出来时。然而，根据ASA的路由表，此解决方案也许不工作(流量也许路由到另一个接口除根据路由表的有意目的地之外)，并且**intra-interface命令相同的安全性的permit**也许是必要的为在ASA的其他连接。

解决方案 2

对于此特定实例，问题通过启用**超时浮动CONN**功能顺利地减轻。此功能，默认情况下没有启用，造成ASA切断这些连接一分钟，在更多首选路由到其中一个终端被添加到路由表ASA的新接口后，发生，当dmz接口出来时。连接立即然后重建，当下一个信息包到达在ASA，使用更多首选的接口时(dmz，而不是10.10.9.3主机的里面)。

```
ASA(config)# timeout floating-conn 0:01:00
```

当问题被减轻时，正确连接在ASA连接表里被建立，并且连接自动地恢复：

```
ASA# show conn address 10.10.1.2
15329 in use, 133142 most used
97 dmz 10.10.9.3 inside10.10.1.2, idle 0:00:00, bytes 3175742510
UDP dmz 10.10.9.3:16666 inside 10.10.1.2:16666, idle 0:00:00, bytes 40651338, flags -
```

```
97 dmz 10.10.9.3 inside10.10.1.2, idle 0:00:00, bytes 1593457240
ASA#
```

相关信息

- ASA 9.1命令参考-超时浮动CONN命令
- 技术支持和文档 - Cisco Systems