排除ASA故障切换上的脑分裂问题

目录

简介

本文档介绍如何排除思科自适应安全设备(ASA)故障切换或Firepower威胁防御(FTD)高可用性(HA)对遇到的常见脑分裂问题。

先决条件

要求

思科建议您了解ASA/FTD高可用性对（故障转移）的工作方 — 于故障转移。

使用的组件

本文档不限于特定软件或硬件版本，并适用于故障切换中支持的所有ASA/FTD部署。

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

规则

有关文件规则的更多信息请参见“ Cisco技术提示规则”。

什么是分裂大脑？

分裂脑是ASA/FTD HA的单元无法在网络上相互检测，因此两者都起主动作用的场景。这会导致两台设备具有相同的接口IP地址和MAC地址，并可能导致网络出现严重不一致，导致服务丢失。

要确定您的HA是否处于分裂脑区，请在两个设备上运行命令**show failover state**，并检查两个框是否都处于活动状态。

裂脑的一个示例：

主要单元:

```
ciscoasa1/act/pri# show failover state

State Last Failure Reason Date/Time
This host - Primary
 Active None
Other host - Secondary
Failed Comm Failure 02:39:43 UTC Jan 10 2022

====Configuration State===
 Sync Done - STANDBY
====Communication State==
```

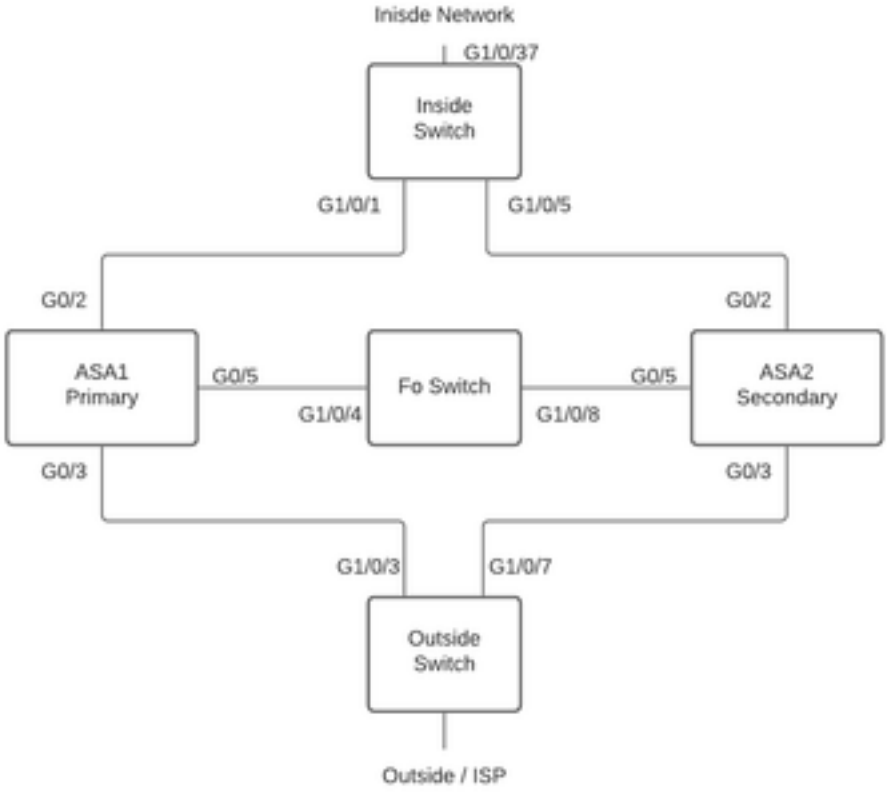
辅助单元:

```
ciscoasa2/act/sec# show failover state

State Last Failure Reason Date/Time
This host - Secondary
 Active None
Other host - Primary
Failed Comm Failure 02:39:40 UTC Jan 10 2022

====Configuration State===
  Sync Done
 Sync Done - STANDBY
====Communication State==
```

如果所连接设备上为活动IP地址学习的MAC地址并非全部相同单元，则脑分裂可能会导致中断。例如，请考虑网络拓扑：



实验室拓扑结构

VMAC已按如下方式分配给接口，这样做是为了使**MAC地址**表易于理解：

```
Inside (G0/2)    : Active MAC    - 00c1.1000.aaaa
                         Standby MAC - 00c1.1000.bbbb

Outside (G0/4) : Active MAC    - 00c1.2000.aaaa

                         Standby MAC - 00c1.2000.bbbb
```

> **注意：**如果未配置VMAC，则主用设备始终为主设备接口使用MAC，备用设备则为辅助MAC。

当HA正常时，交换机上的MAC地址表：

```
Switch#show mac address-table

Mac Address Table
-------------------------------------------
Vlan Mac Address Type Ports
---- ----------- -------- -----
100 00c1.1000.aaaa DYNAMIC Gi1/0/5
100 00c1.1000.bbbb DYNAMIC Gi1/0/1
300 00c1.64bc.c508 DYNAMIC Gi1/0/4
300 00d7.8f38.8424 DYNAMIC Gi1/0/8
200 00c1.2000.aaaa DYNAMIC Gi1/0/7
200 00c1.2000.bbbb DYNAMIC Gi1/0/3
```

如果故障切换链路发生故障，主用设备将保持主用状态，备用设备将保持备用状态。当设备未在故障切换链路上收到三个连续的HELLO消息时，设备会在每个数据接口（包括故障切换链路）上发送

LANTEST消息，以验证对等设备是否响应。ASA执行的操作取决于来自另一设备的响应。

可能的操作包括：

- 如果ASA在故障切换链路上收到响应，则不进行故障切换。
- 如果ASA在故障切换链路上未收到响应，但在数据接口上确实收到响应，则设备不会进行故障切换。故障切换链路被标记为失败。您应尽快恢复故障切换链路，因为当故障切换链路关闭时，设备无法故障切换到备用。
- 如果ASA 未在任何接口上收到响应，则备用设备会切换到主用模式，并将另一设备分类为故障。这将导致脑分裂。

在此阶段，两个防火墙上的所有数据接口都将充当活动单元。因此，主用和备用防火墙上的接口将使用相同的IP和MAC地址。这将导致因毒性ARP条目而导致MAC地址表不一致，从而导致中断。

> **注意**：故障切换链路负责在故障切换对(Failover Pair)之间通信此数据：设备状态（主用/备用）、Hello消息、网络链路状态、MAC地址交换、配置复制和同步。

如何主动准备应对故障切换问题

要主动针对脑分裂状况做准备，请执行以下操作：

- 加入思科推荐的黄金版 — 在某些情况下，脑分裂也可能由内存泄漏等问题引起。通过加入思科推荐的版本，您可以大大减少此类情况的暴露。
- 网络拓扑 — 建议数据接口和故障切换链路使用不同的路径，以降低所有接口同时发生故障的可能性。
- 将端口通道接口用于故障切换接口 — 如果防火墙上有未使用的接口，请将其配对以形成端口通道并将其用作故障切换链路，这将提高链路可靠性并删除单点故障(SPOF)。
- 确保故障切换接口的延迟不会太长 — 如《ASA配置指南》中所述，为了在使用长距离故障切换时获得最佳性能，状态链路的延迟应小于10毫秒且不超过250毫秒。如果延迟超过10毫秒，则会因重新传输故障切换消息而导致某些性能下降。”
- 根据部署调整轮询计时器/保持计时器值 — 对于故障切换计时器，没有一种方法适合所有方法。通常，计时器低可能导致不必要的故障切换（特别是当有延迟时），而值过高可能导致故障切换发生时间延长。这会导致明显的故障切换。保持计时器值必须为5x轮询计时器值。
- 为接口配置虚拟MAC地址 — 在“辅助设备在不检测主设备的情况下启动，辅助设备将成为主用设备并使用其自己的MAC地址，因为它不知道主设备MAC地址。当主设备可用时，辅助（主用）设备会将MAC地址更改为主设备的MAC地址，这可能导致网络流量中断。同样，如果用新硬件替换主设备，则会使用新的MAC地址。” 虚拟MAC地址可防止此中断，因为主用MAC地址在启动时已为辅助设备所知，在新的主设备硬件情况下保持不变。如果不配置虚拟MAC地址，则可能需要清除相连路由器上的ARP表以恢复流量”。 有关详细信息，请参阅 — 故障切换中的MAC地址和IP地址。
- 将两台设备的ASA/FTD日志发送到外部系统日志服务器 — 此步骤更适合问题的可维护性。

脑分裂的可能原因

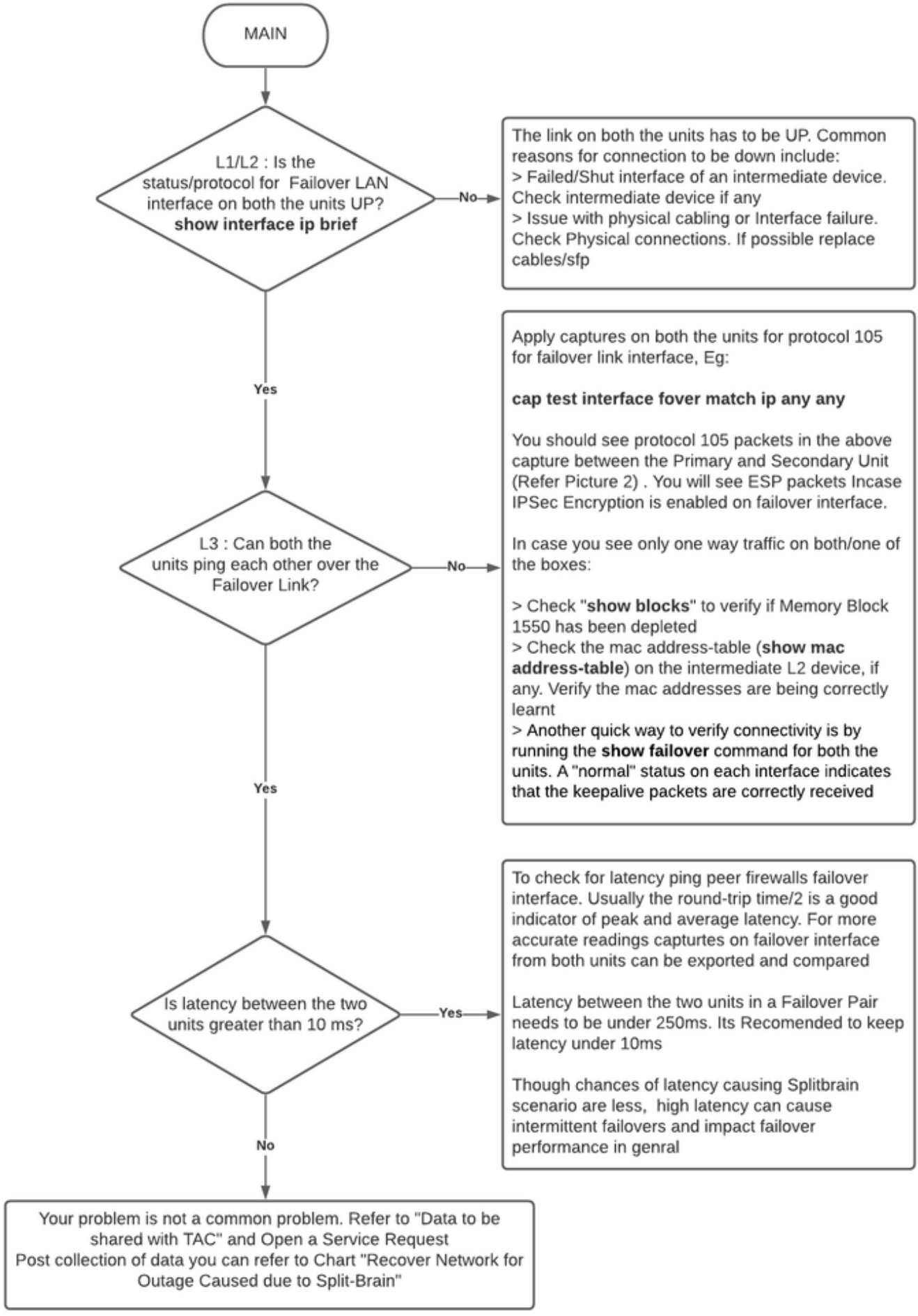
如前所述，当故障切换链路接口之间的通信（单向或双向）中断时，会发生脑分裂。 最常见的原因是：

- L1问题 — 电缆/SFP/接口故障
- 中间设备上的问题
- ASA/FTD上内存或CPU资源不足 **注意**：ASA/Lina引擎利用1550字节内存块存储数据包以进行处理。如果此大小的空闲块数量减少，ASA/FTD将无法再处理故障转移数据包。运行show blocks 以检查块耗尽。

故障排除步骤 — 流程图

要排除并解决脑分裂场景故障，请使用此流程图，从标有“主”的框开**始**。有些问题在此可能无法解决。在这些情况下，文档提供指向 Cisco 技术支持的链接。要打开服务请求，必须有有效的服务合同。

> **注：在**FTD部署中，必须从“system support diagnostics-cli”中**执行此图表中的**步骤。


MAIN
L1/L2 : Is the status/protocol for Failover LAN interface on both the units UP? show interface ip brief
No
The link on both the units has to be UP. Common reasons for connection to be down include:
> Failed/Shut interface of an intermediate device. Check intermediate device if any
> Issue with physical cabling or Interface failure. Check Physical connections. If possible replace cables/sfp
Yes
Apply captures on both the units for protocol 105 for failover link interface, Eg:
cap test interface fover match ip any any
You should see protocol 105 packets in the above capture between the Primary and Secondary Unit (Refer Picture 2) . You will see ESP packets Incase IPSec Encryption is enabled on failover interface.
L3 : Can both the units ping each other over the Failover Link?
No
In case you see only one way traffic on both/one of the boxes:
> Check "show blocks" to verify if Memory Block 1550 has been depleted
> Check the mac address-table (show mac address-table) on the intermediate L2 device, if any. Verify the mac addresses are being correctly learnt
> Another quick way to verify connectivity is by running the show failover command for both the units. A "normal" status on each interface indicates that the keepalive packets are correctly received
Yes
Is latency between the two units greater than 10 ms?
Yes
To check for latency ping peer firewalls failover interface. Usually the round-trip time/2 is a good indicator of peak and average latency. For more accurate readings capturtes on failover interface from both units can be exported and compared
Latency between the two units in a Failover Pair needs to be under 250ms. Its Recomended to keep latency under 10ms
Though chances of latency causing Splitbrain scenario are less, high latency can cause intermittent failovers and impact failover performance in genral
No
Your problem is not a common problem. Refer to "Data to be shared with TAC" and Open a Service Request
Post collection of data you can refer to Chart "Recover Network for Outage Caused due to Split-Brain"

故障排除流程图

脑裂的急救

要从裂脑中恢复网络，您需要确保流量仅到达两个防火墙中的一个，即为活动IP学习的MAC地址应全部指向一个单元。为此，您可以禁用设备上的故障切换，或将其完全切断网络。

1. 在未传递流量的设备上禁用故障切换： 在ASA平台上，通过CLI导航至配置终端并输入**no failover**命令。在FTD平台上，在Clish模式下，输**入configure high-availability suspend**命令。
2. 对于ASA，关闭数据接口。对于FTD，关闭连接设备上的接口。或者，您也可以物理断开接口。此外，您可以关闭设备，但这会限制您管理设备。请参阅设备配置指南，了解执行此操作的步骤。

   注意：如果您注意到连接问题，即使在执行上述步骤后，连接的设备也可能有过时的arp条目。检查上游和下游设备上的arp条目。要解决该问题，您可以刷新这些，或强制工作的ASA/FTD为存在问题的接口IP发送garp数据包。为此，请在启用模式下运行命令（对于系统中的FTD，支持diagnostics-cli） — **debug menu ipaddrutl 6 <interface ip address>**。

   警告：如果您向TAC提交与拆分脑相关问题的支持票证，请共享本文档中要为TAC服务请求收集的**数据部分中提**及的信息。

要与TAC共享的数据

如果您需要打开TAC服务请求，请共享所提到的数据。

1. 拓扑图，显示ASA/FTD-HA及其与相邻设备（包括故障切换接口）的物理连接。
2. ASA上**的show tech-support或**运行FTD的平台上的故障排除文件的输出。
3. 出现问题时，系统日志和时间戳会持续+/- 5分钟。
4. FXOS故障排除文件（如果硬件是FPR设备）。

要为FTD或FXOS生成故障排除文件，请参[阅Firepower故障排除文件生](#)成过程。[打开TAC SR。](#)