排除ASA故障轉移上的大腦分割問題

目錄

簡介

本文描述如何解決思科自適應安全裝置(ASA)故障轉移或Firepower威脅防禦(FTD)高可用性(HA)對中遇到的常見拆分問題。

必要條件

需求

思科建議您瞭解ASA/FTD高可用性對（故障轉移）的運作方式 — 故障轉移。

採用元件

本文檔不限於特定軟體或硬體版本，並且適用於故障切換中所有支援的ASA/FTD部署。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

什麼是Split-Brain?

Split-brain是一種場景，其中ASA/FTD HA的單元無法在網路上檢測到對方，因此兩者都扮演主動角色。這會導致兩個裝置具有相同的介面IP地址和MAC地址，並且可能導致網路中的嚴重不一致而導致服務丟失。

要確定您的HA是否處於拆分腦，請在兩台裝置上運行命令**show failover state**，並檢查兩台裝置是否均處於活動狀態。

Split-brain示例：

主裝置：

```
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==
```

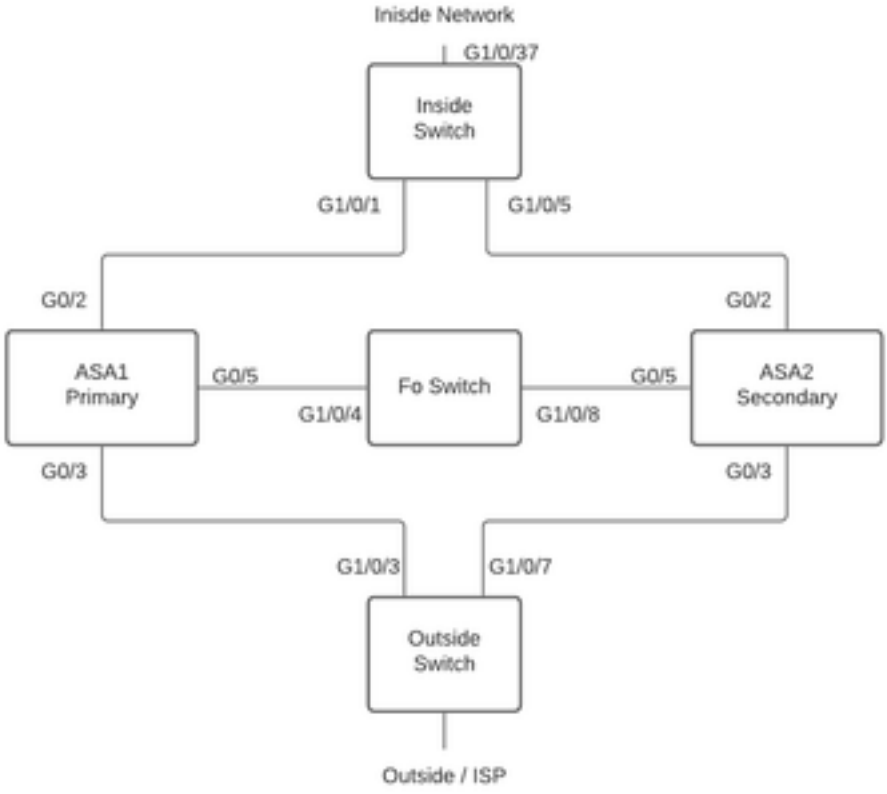
輔助裝置：

```
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==
```

如果為相連裝置上的活動IP地址獲取的MAC地址不是所有相同的裝置，則分頭可能會導致中斷。例如，考慮網路拓撲：



實驗拓撲

VMAC已按如下方式分配給介面，這樣做是為了使**mac address-table**易於理解：

```
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，則主用裝置始終採用主裝置介面的MAC，備用裝置採用輔助MAC。

HA正常時，交換器上的MAC位址表：

```
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
```

如果故障切換鏈路發生故障，主用裝置將保持主用狀態，備用裝置將保持備用狀態。當裝置在故障切換鏈路上未收到三個連續的HELLO消息時，該裝置會在每個資料介面（包括故障切換鏈路）上傳

送LANTEST消息，以驗證對等裝置是否響應。ASA採取的操作取決於來自其他裝置的響應。

可能的操作包括：

- 如果ASA在故障切換鏈路上收到響應，則它不會進行故障切換。
- 如果ASA未在故障轉移鏈路上收到響應，但在資料介面上收到響應，則裝置不會進行故障轉移。故障切換鏈路標籤為發生故障。您應儘快恢復故障切換鏈路，因為當故障切換鏈路關閉時，裝置無法故障切換至備用裝置。
- 如果ASA在任何介面上均未收到響應，則備用裝置會切換至主用模式並將其他裝置分類為故障。這將導致大腦分裂。

在這個階段，兩個防火牆上的所有資料介面都將像它們作為活動單元一樣工作。因此，主用和備用防火牆上的介面將使用相同的IP和MAC地址。由於毒素arp條目，這將導致不一致的MAC地址表，從而導致中斷。

> **附註：**故障轉移鏈路負責故障轉移對之間的資料通訊：裝置狀態（活動/備用）、Hello消息、網路鏈路狀態、MAC地址交換、配置複製和同步。

如何主動預防故障切換問題

要主動做好應對大腦分裂狀況的準備：

- 進入思科推薦的黃金版本 — 在某些情況下，也可能會由於記憶體洩露等問題導致大腦分裂。使用思科推薦的版本，您可以大大降低此類情況的風險。
- 網路拓撲 — 建議資料介面和故障轉移鏈路具有不同的路徑，以減少所有介面同時發生故障的可能性。
- 將埠通道介面用於故障切換介面 — 如果防火牆上有未使用的介面，請配對它們以形成埠通道並將其用作故障切換鏈路，這將提高鏈路可靠性並消除單點故障(SPOF)。
- 確保故障切換介面沒有太多延遲 — 根據ASA配置指南「要在使用遠距離故障切換時獲得最佳效能，狀態鏈路的延遲應小於10毫秒，不超過250毫秒。如果延遲超過10毫秒，則由於重新傳輸故障切換消息而導致某些效能下降。」
- 根據您的部署調整輪詢計時器/保持計時器值 — 沒有一種大小適合所有故障切換計時器的方法。通常，降低計時器會導致不必要的故障轉移（特別是在存在一些延遲時），而值太高則可能會導致發生故障轉移的時間增加。這將導致明顯的故障轉移。保持計時器值必須是「輪詢計時器」值的5倍。
- 為介面配置虛擬MAC地址 — 在「輔助裝置在不檢測主裝置的情況下啟動」的情況下，輔助裝置會成為主裝置，並使用自己的MAC地址，因為它不知道主裝置的MAC地址。當主裝置可用時，輔助（活動）裝置會將MAC地址更改為主裝置的MAC地址，這可能會導致網路流量中斷。同樣，如果您用新硬體替換主裝置，則使用新的MAC地址。」 虛擬MAC地址可防止這種中斷，因為主用MAC地址在啟動時已為輔助裝置所知，而在新主裝置硬體的情況下保持不變。如果不配置虛擬MAC地址，您可能需要清除相連路由器上的ARP表以恢復流量」。 有關詳細資訊，請參閱 — 故障切換中的MAC地址和IP地址。
- 將兩台裝置的ASA/FTD日誌傳送到外部Syslog伺服器 — 此步驟更多用於說明問題的可維護性。

大腦分裂的可能原因

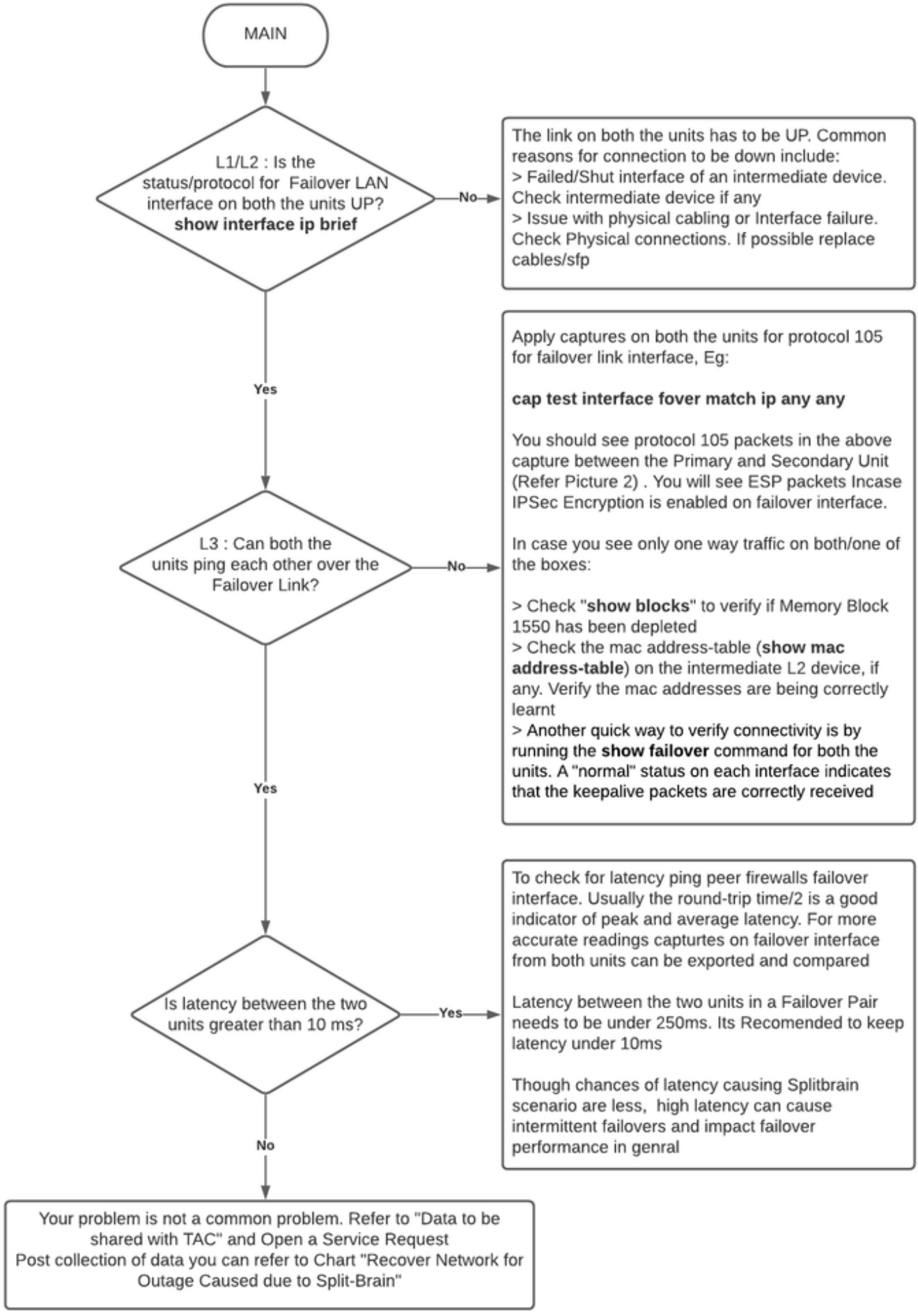
如前所述，當故障切換鏈路介面之間的通訊發生故障時（單向或雙向），將發生拆分。 最常見的原因包括：

- L1問題 — 電纜/SFP/介面故障
- 中間裝置上的問題
- ASA/FTD上缺少記憶體或CPU資源 **注意**：ASA/Lina引擎使用1550位元組記憶體塊來儲存資料包以進行處理。如果此大小的可用塊數量減少，ASA/FTD將無法再處理故障轉移資料包。運行show blocks以檢查塊耗盡。

故障排除過程 — 流程圖

若要疑難排解和解決大腦分裂的情況，請使用此流程圖，從標籤為Main的框開始。有些問題在此可能無法解決。在這些情況下，會提供指向思科技術支援的連結。若要開啟服務請求，您必須擁有有效的服務合約。

注意：在FTD部署中，必須從「system support diagnostics-cli」中執行此圖表中的步驟。


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"

故障排除流程圖

從腦裂傷急救

要從拆分頭腦中恢復網路，您需要確保流量僅到達兩個防火牆中的一個，也就是說，為活動IP學習的MAC地址應全部指向單個裝置。為此，您可以在裝置上禁用故障轉移，或將其完全切斷網路。

1. 在不傳遞流量的裝置上禁用故障轉移： 在ASA平台上，通過CLI導航到配置終端並輸入**no failover**命令。在FTD平台上，在Clish模式下，輸入**configure high-availability suspend**命令。
2. 對於ASA，關閉資料介面。若是FTD，請關閉已連線裝置上的介面。或者，您也可以斷開介面的物理連線。此外，您可以關閉裝置電源，但這會限制您管理裝置。有關執行此操作的步驟，請參閱裝置配置指南。

注意：即使執行上述步驟後，如果您發現連線問題，所連線的裝置很可能具有過時的ARP條目。檢查上游和下游裝置上的arp條目。要解決此問題，您可以刷新這些資料包，或強制正在運行的ASA/FTD為有問題的介面IP傳送garp資料包。為此，請在啟用模式下運行命令（對於系統支援診斷 — cli中的FTD） — **debug menu ipaddrutl 6 <interface ip address>**。

注意：如果您針對Split-brain相關問題向TAC開啟支援票證，請共用本文檔中**為TAC服務請求收集的資料**部分中提到的資訊。

要與TAC共用的資料

如果需要開啟TAC服務請求，請共用提及的資料。

1. 顯示ASA/FTD-HA及其與相鄰裝置（包括故障轉移介面）的物理連線的拓撲圖。
2. ASA上的**show tech-support**輸出或運行FTD的平台上的故障排除檔案輸出。
3. 系統日誌以及發生問題的時間戳+/- 5分鐘。
4. 如果硬體是FPR裝置，則FXOS故障排除檔案。

若要產生有關FTD或FXOS的疑難排解檔案，請參閱Firepower疑難排解檔案產生程式。開啟TAC SR。