Resolución de Problemas de Dividido-Cerebro en Failover ASA

Contenido

Introducción

Este documento describe cómo resolver problemas comunes de división cerebral con fallas de Cisco Adaptive Security Appliance (ASA) o pares Firepower Threat Defense (FTD) High Availability (HA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre cómo funciona ASA/FTD High Availability Pair (Failover) - Acerca de la conmutación por fallas.

Componentes Utilizados

Este documento no se limita a versiones específicas de software o hardware y se aplica a todas las implementaciones ASA/FTD soportadas en Failover.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

¿Qué es Split-Brain?

El cerebro dividido es un escenario en el que las unidades de un ASA/FTD HA no pueden detectarse entre sí en la red y, por lo tanto, ambas asumen el rol activo. Esto hace que ambas unidades tengan la misma dirección IP de interfaz y dirección MAC y puede causar graves inconsistencias en su red, lo que resulta en la pérdida de servicios.

Para identificar si su HA está en el cerebro dividido, ejecute el comando **show failover state** en ambas unidades y verifique si ambas casillas están activas.

Un ejemplo de un cerebro dividido:

Unidad principal:

```
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==
```

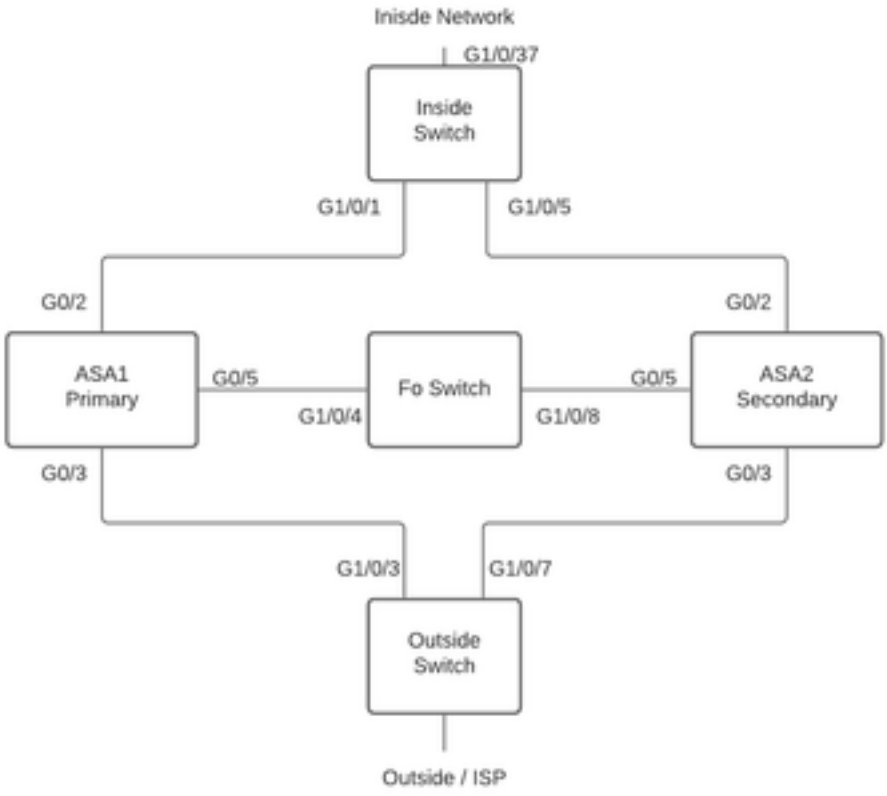
Unidad secundaria:

```
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==
```

El cerebro dividido puede provocar una interrupción si la dirección MAC aprendida para las direcciones IP activas en los dispositivos conectados no son todas las mismas unidades. Por ejemplo, considere la topología de red:



Topología de laboratorio

VMAC se ha asignado a la interfaz de la siguiente manera, esto se ha hecho para que la **tabla de direcciones mac** sea fácil de entender:

```
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
```

> **Nota:** Si los VMAC no están configurados, el dispositivo activo siempre toma el MAC para la interfaz de la unidad principal y el standby toma el MAC secundario.

Tabla de direcciones MAC en el switch cuando HA está en buen estado:

```
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
```

Si falla el link de failover, la unidad activa permanecerá activa y el standby permanecerá en espera. Cuando una unidad no recibe tres mensajes HELLO consecutivos en el link Failover, la unidad envía mensajes LANTEST en cada interfaz de datos, incluido el link de failover, para validar si el par responde o no. La acción que realiza el ASA depende de la respuesta de la otra unidad.

Las posibles acciones son:

- Si el ASA recibe una respuesta en el link de failover, entonces no falla.
- Si el ASA no recibe una respuesta en el link de failover, pero sí recibe una respuesta en una interfaz de datos, entonces la unidad no falla. El link de failover está marcado como fallido. Debe restaurar el link de failover lo antes posible porque la unidad no puede conmutar por error a standby mientras el link de failover está inactivo.
- Si el ASA no recibe una respuesta en ninguna interfaz, entonces la unidad standby cambia al modo activo y clasifica la otra unidad como fallada. Esto llevará a un escenario de división cerebral.

En esta etapa, todas las interfaces de datos de ambos Firewalls actuarán como si fueran la unidad activa. Por lo tanto, las interfaces en el firewall activo y en espera utilizarán la misma dirección IP y MAC. Esto dará lugar a una tabla de direcciones MAC incoherente debido a una entrada arp envenenada y por lo tanto causará una interrupción.

> **Nota:** El enlace de conmutación por fallas es responsable de la comunicación de estos datos entre el par de conmutación por fallas: estado de unidad (activo/en espera), mensajes de saludo, estado del enlace de red, intercambio de direcciones MAC, replicación de configuración y sincronización.

Cómo prepararse de forma proactiva frente a los problemas de conmutación por fallo

Para prepararse de forma proactiva frente a una enfermedad del cerebro dividido:

- Participe en la versión dorada recomendada por Cisco. En ciertas condiciones, también puede producirse una división cerebral debido a problemas como una pérdida de memoria. Al estar en las versiones recomendadas por Cisco, reducirá en gran medida su exposición a tales situaciones.
- Topología de red - Se recomienda que las Interfaces de datos y los Links de conmutación por fallas tengan trayectorias diferentes para disminuir la probabilidad de que todas las interfaces fallen al mismo tiempo.
- Utilice una interfaz de canal de puerto para la interfaz de conmutación por fallo. Si tiene interfaces no utilizadas en su firewall, emparejételas para formar un canal de puerto y utilícelo como enlace de conmutación por fallo, esto aumentará la fiabilidad del enlace y eliminará un único punto de fallo (SPOF).
- Asegúrese de que la interfaz de conmutación por fallas no tenga demasiada latencia - Según la Guía de configuración de ASA "Para un rendimiento óptimo cuando se usa conmutación por fallas a larga distancia, la latencia para el link de estado debe ser menor a 10 milisegundos y no mayor a 250 milisegundos. Si la latencia es superior a 10 milisegundos, se

produce cierta degradación del rendimiento debido a la retransmisión de los mensajes de conmutación por fallas".
- Ajuste los valores del temporizador de sondeo/temporizador de espera según la implementación: no hay un tamaño que se ajuste a todos los tiempos de conmutación por fallas. En general, bajar un temporizador puede causar fallas innecesarias (especialmente si hay alguna latencia) y un valor demasiado alto puede conducir a un aumento del tiempo para que se produzca una conmutación por fallas. Lo que dará lugar a filovers notables. El valor del temporizador de espera debe ser 5x del temporizador de sondeo.
- Configuración de una Dirección MAC Virtual para las interfaces - Bajo una condición donde "la unidad secundaria se inicia sin detectar la unidad primaria, entonces la unidad secundaria se convierte en la unidad activa y utiliza sus propias direcciones MAC porque no conoce las direcciones MAC de la unidad primaria. Cuando la unidad primaria está disponible, la unidad secundaria (activa) cambia las direcciones MAC a las de la unidad primaria, lo que puede causar una interrupción en el tráfico de red. Asimismo, si cambia la unidad principal por un nuevo hardware, se utiliza una nueva dirección MAC". Las direcciones MAC virtuales protegen contra esta interrupción, porque las direcciones MAC activas son conocidas por la unidad secundaria al inicio y permanecen iguales en el caso del nuevo hardware de la unidad primaria. Si no configura las direcciones MAC virtuales, es posible que necesite borrar las tablas ARP en los routers conectados para restaurar el flujo de tráfico". Para obtener más detalles, consulte Direcciones MAC y Direcciones IP en Failover.
- Enviar registros ASA/FTD para ambas unidades a un servidor Syslog externo - Este paso es más para la facilidad de mantenimiento de los problemas.

Posibles razones para dividir el cerebro

Como ya se ha mencionado, la división cerebral ocurre cuando la comunicación entre las interfaces de link de failover está inactiva (unidireccional o bidireccionalmente). Las razones más comunes son:

- Problemas de L1 - Cable/SFP/interfaz defectuoso
- Un problema en un dispositivo intermedio
- Falta de memoria o recursos de CPU en ASA/FTD **Nota:** El motor ASA/Lina utiliza bloques de memoria de 1550 bytes para almacenar paquetes para su procesamiento. Si el número de bloques libres de este tamaño se agota, ASA/FTD ya no podrá procesar paquetes de conmutación por fallas. Ejecute el comando **show blocks** para comprobar si se ha agotado el bloque.

Procedimiento para la resolución de problemas - Diagrama de flujo

Para resolver problemas y resolver un Escenario de división cerebral, utilice este diagrama de flujo, comience en la caja marcada como **Principal**. Hay algunos problemas que podrían no resolverse aquí. En estos casos, se proporcionan enlaces al soporte técnico de Cisco. Para abrir una solicitud de servicio, debe tener un contrato de servicio válido.

Nota: En las implementaciones de FTD, los pasos de este gráfico se deben seguir desde "**system support diagnostics-cli**".

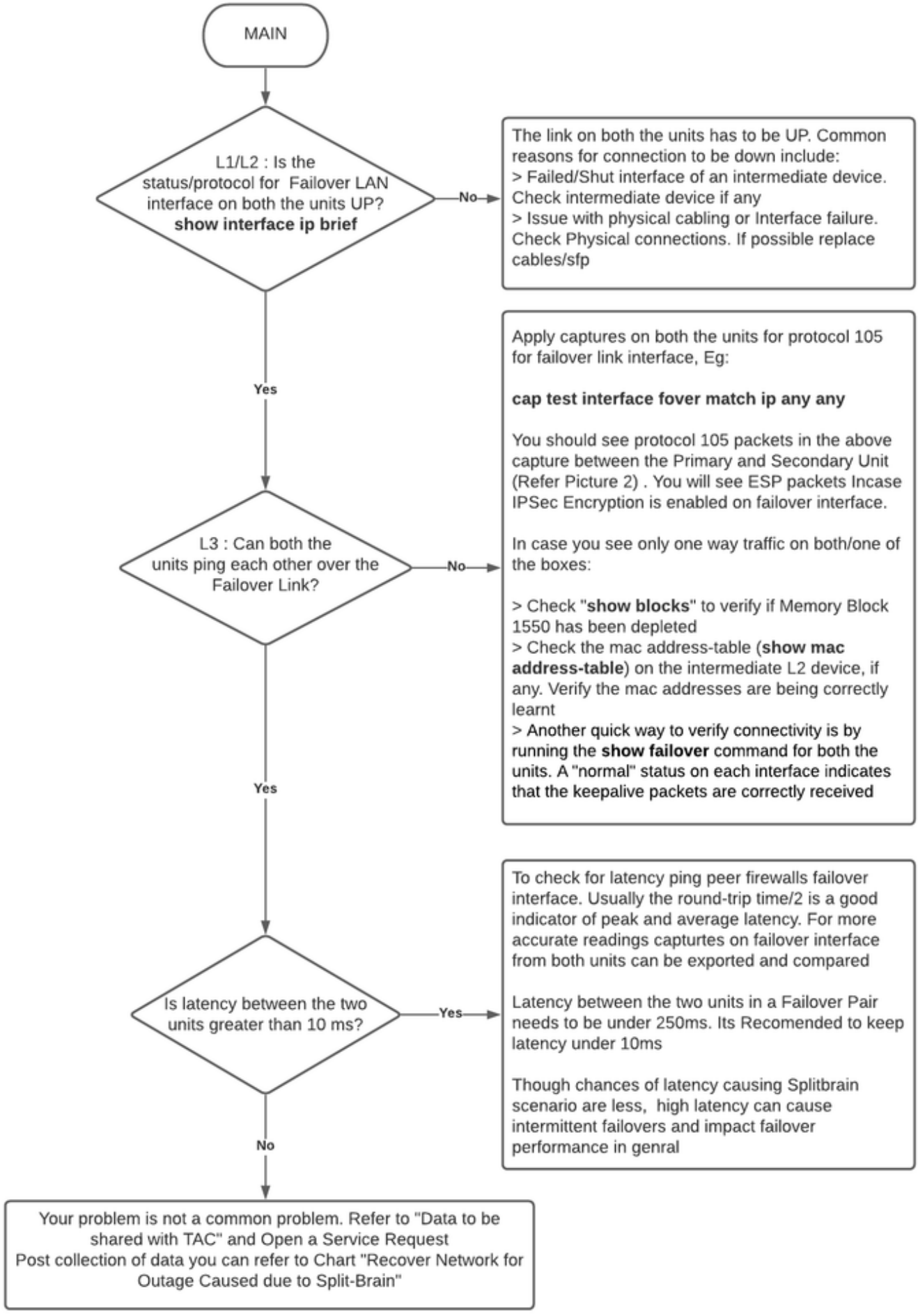


Diagrama de flujo de solución de problemas

Recuperación de emergencia del cerebro dividido

Para recuperar su red de un cerebro dividido, debe asegurarse de que el tráfico llegue a uno de los dos firewalls, es decir, las direcciones MAC aprendidas para las IP activas deben apuntar a una sola unidad. Para ello, puede inhabilitar la conmutación por fallas en la unidad o cortarla por completo de la red.

1. Desactivar conmutación por fallas en la unidad que no pasa tráfico: En la plataforma ASA, a través de la CLI, navegue hasta el terminal de configuración e ingrese el comando **no failover**.En la plataforma FTD, en el modo Clish, ingrese el comando **configure high-Availability suspender**.
2. Para ASA, cierre las interfaces de datos. Para FTD, cierre las interfaces en el dispositivo conectado. Alternativamente, también puede desconectar físicamente las interfaces. Además, puede apagar el dispositivo, pero esto le limitará a administrar el dispositivo. Consulte la guía de configuración del dispositivo sobre los pasos para hacerlo.

   Nota: Si observa problemas de conectividad incluso después de realizar los pasos mencionados, es probable que los dispositivos conectados tengan entradas ARP obsoletas. Verifique las entradas ARP en los dispositivos ascendentes y descendentes. Para solucionar el problema, puede vaciar estos o forzar al ASA/FTD en funcionamiento a enviar un paquete garp para la IP de interfaz que tiene el problema. Para hacerlo, ejecute el comando en modo habilitar (para FTD en el sistema soporta diagnostics-cli) - **debug menu ipaddrutl 6 <interface ip address>**.

   Precaución: En caso de que abra un ticket de soporte con TAC para problemas relacionados con Split-cerebro, por favor comparta la información mencionada en la sección **Datos que se recopilarán para la Solicitud de Servicio TAC** en este documento.

Datos que se compartirán con el TAC

Comparta los datos mencionados en caso de que necesite abrir una solicitud de servicio del TAC.

1. Diagrama de topología que muestra ASA/FTD-HA y sus conexiones físicas con los dispositivos vecinos (incluidas las interfaces de conmutación por fallo).
2. Salida para **show tech-support** en ASA o archivo de resolución de problemas en plataformas que ejecutan FTD.
3. Los registros del sistema junto con las marcas de tiempo durante +/- 5 minutos cuando ocurrió el problema.
4. Archivos de resolución de problemas de FXOS, si el hardware es un dispositivo FPR.

Para generar los archivos de resolución de problemas para FTD o FXOS, consulte Procedimientos de generación de archivos Firepower Troubleshooting. Abra un TAC SR.