Solución de problemas de cerebro dividido en conmutación por fallo ASA

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados
- Convenciones

¿Qué es Split-Brain?

- Un ejemplo de un cerebro dividido

Cómo prepararse proactivamente contra problemas de failover

Posibles razones para el cerebro dividido

Procedimiento de localización de averías - Diagrama de flujo

Recuperación de Emergencia de Split-Cerebro

Datos para compartir con el TAC

Introducción

Este documento describe la solución de problemas de mente dividida en los pares de alta disponibilidad de failover del Cisco Adaptive Security Appliance o Firepower Threat Defence.

Prerequisites

Requirements

Cisco recomienda que conozca el funcionamiento del par de alta disponibilidad (failover) de ASA/FTD - Acerca del failover.

Componentes Utilizados

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). 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 desempeñan un papel activo. Esto hace que ambas unidades tengan la misma dirección IP y la dirección MAC de la interfaz y puede causar graves inconsistencias en su red que resulten en la pérdida de servicios.

Para identificar si su HA está en split-brain, ejecute el comando show failover state en ambas unidades y verifique si ambas casillas están activas.

Un ejemplo de un cerebro dividido

Unidad primaria:

```
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:

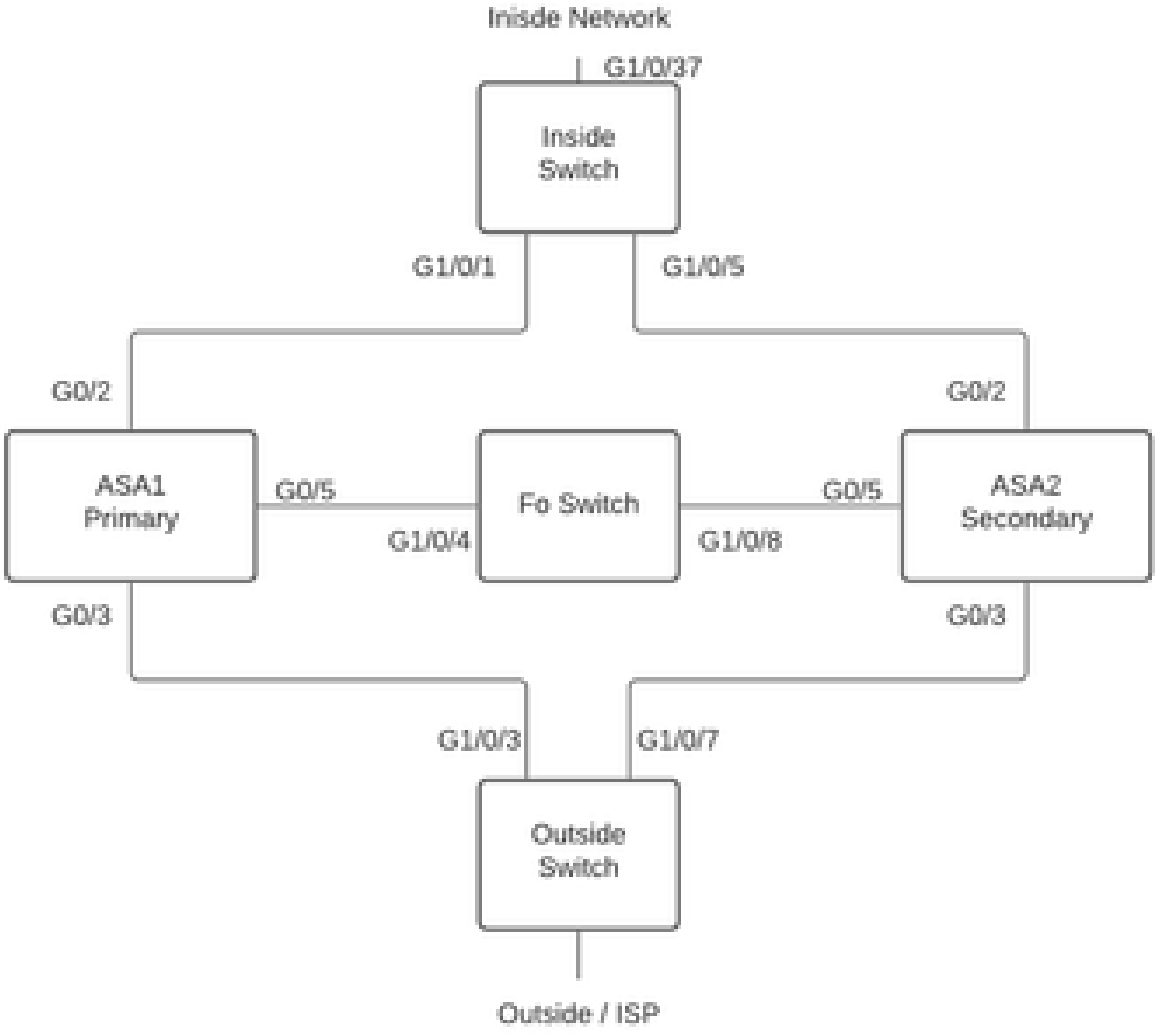
```
ciscoasa2/act/sec# show failover state

               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 causar una interrupción si la dirección MAC aprendida para las direcciones IP activas en los dispositivos conectados no son todas las unidades iguales. Por

ejemplo, piense en la topología de red:



Topología de laboratorio

Los VMAC se han asignado a la interfaz como se muestra. Esto se ha hecho para hacer 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 Primaria 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 modo de espera permanecerá en modo de espera. Cuando una unidad no recibe tres mensajes HELLO consecutivos en el link de failover, la unidad envía los mensajes LANTEST en cada interfaz de datos, incluyendo el link de failover, para validar si el peer responde o no. La acción que el ASA toma depende de la respuesta de la otra unidad.

Las acciones posibles son:

- Si el ASA recibe una respuesta en el link de failover, no falla.
- Si el ASA no recibe una respuesta en el link de failover, pero recibe una respuesta en una interfaz de datos, entonces la unidad no falla. El link de failover está marcado como fallado. Puede restaurar el link de failover tan pronto como sea posible porque la unidad no puede conmutar por error al modo en espera mientras el link de failover está inactivo.
- Si el ASA no recibe una respuesta en ninguna interfaz, la unidad standby cambia al modo activo y clasifica la otra unidad como fallada. Esto lleva a un escenario de cerebro partido.

En esta etapa, todas las interfaces de datos en ambos firewalls actúan como si fueran la unidad activa. Por lo tanto, las interfaces en el firewall activo y en espera utilizan la misma dirección IP y MAC. Esto conduce a una tabla de direcciones MAC inconsistente debido a la entrada de arp intoxicado y por lo tanto puede causar una interrupción.

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

Cómo prepararse proactivamente contra problemas de failover

Para prepararse de forma proactiva contra una enfermedad cerebral dividida:

- Tenga en cuenta la versión de oro recomendada por Cisco: en determinadas condiciones, la división del cerebro también puede deberse a problemas como una pérdida de memoria.

Las versiones recomendadas de Cisco reducen de forma significativa la exposición a este tipo de situaciones.

- Topología de red - Se recomienda que las interfaces de datos y los links de failover tengan diferentes trayectorias 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 sin utilizar en el firewall, vincúlelas para formar un canal de puerto y utilícelas como enlace de conmutación por fallo, lo que aumenta la fiabilidad del enlace y elimina un punto único de fallo (SPOF).
- Asegúrese de que la interfaz de conmutación por fallo no tenga demasiada latencia. Según la guía de configuración de ASA "Para obtener un rendimiento óptimo al utilizar conmutación por fallo a larga distancia, la latencia del enlace de estado puede ser inferior a 10 milisegundos y no superior 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 fallo".
- Ajuste los valores del temporizador de sondeo/temporizador de espera según su implementación: no existe un tamaño único para todos los enfoques de los temporizadores de conmutación por fallo. En general, cuando se baja un temporizador, puede causar fallas innecesarias (especialmente si hay cierta latencia), y un valor demasiado alto puede llevar a un aumento del tiempo para que se produzca una falla. Esto conduce a conmutaciones por error perceptibles. El valor del temporizador de espera debe ser 5 veces el valor del temporizador de sondeo.
- Configuración de una Dirección MAC Virtual para 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 vuelve a estar 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. Del mismo modo, si cambia la unidad principal por 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 direcciones MAC virtuales, debe borrar las tablas ARP en los routers conectados para restaurar el flujo de tráfico". Para obtener más detalles, consulte: Direcciones MAC e IP en Failover.

- Enviar registros de 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 el cerebro dividido

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

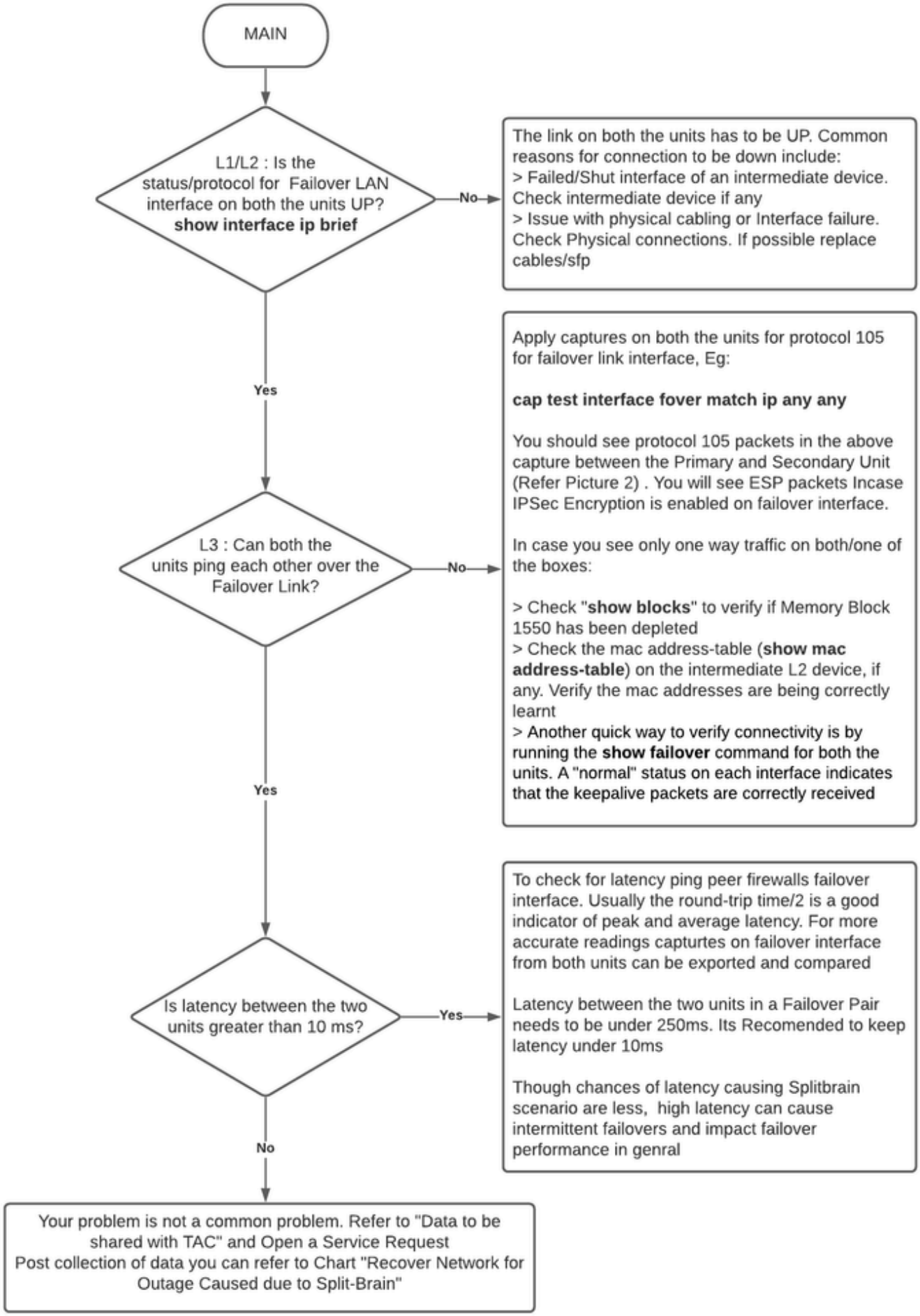
- Problemas de L1 - Cable/SFP/Interfaz defectuosos
- Un problema en un dispositivo intermedio
- Falta de memoria o recursos de CPU en ASA/FTD

> Nota: ASA/Line Engine utiliza bloques de memoria de 1550 bytes para almacenar paquetes para su procesamiento. Si el número de bloques libres de este tamaño agota el ASA/FTD, itl ya no es capaz de procesar paquetes de failover. Ejecute el comando show blocks para verificar si se ha agotado el bloque.

Procedimiento de localización de averías - Diagrama de flujo

Para resolver problemas y resolver un escenario de mente dividida, utilice este diagrama de flujo, comience en el cuadro marcado como Main. Hay algunos problemas que no se pueden resolver 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, siga los pasos de este diagrama de "system support diagnostics-cli".


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.
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
L3 : Can both the units ping each other over the Failover Link?
No
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
Is latency between the two units greater than 10 ms?
Yes
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"

Recuperación de Emergencia de Split-Cerebro

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

1. Inhabilite el failover en la unidad que no pasa el tráfico:
   - En la plataforma ASA, a través de CLI, navegue hasta el terminal de configuración e ingrese el comando no failover.
   - En la plataforma FTD, en el modo de nube, ingrese el comando configure high-availability suspend.
2. Para ASA, cierre las interfaces de datos. Para FTD, cierre las interfaces del dispositivo conectado. Como alternativa, también puede desconectar físicamente las interfaces. Además, puede apagar el dispositivo, pero esto le impide administrarlo. Consulte la guía de configuración del dispositivo para obtener información sobre los pasos necesarios.

   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 de flujo ascendente y descendente. 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 hacer esto, ejecute el comando en el modo enable (para FTD en System support diagnostics-cli) - debug menu ipaddrutl 6 <interface ip address>.

⚠ Precaución: En caso de que abra un ticket de soporte con el TAC para problemas relacionados con la mente dividida, comparta la información mencionada en la sección Datos que se deben recopilar para la solicitud de servicio del TAC en este documento.

Datos para compartir 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 dispositivos vecinos (incluidas las interfaces de conmutación por fallo).
2. Salida para show tech-support en ASA o archivo de solución de problemas en plataformas que ejecutan FTD.
3. Registros del sistema junto con marcas de tiempo durante +/- 5 minutos cuando se produjo el problema.
4. Archivos de resolución de problemas de FXOS, si el hardware es un dispositivo FPR.

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).