Dépannage des problèmes de « split-cerveau » sur le basculement ASA

Table des matières

Introduction

Ce document décrit la résolution des problèmes de « split-brain » dans les paires haute disponibilité de basculement d'appliance de sécurité adaptatif Cisco ou de Firepower Threat Defense.

Conditions préalables

Exigences

Cisco recommande que vous connaissiez le fonctionnement de la paire haute disponibilité ASA/FTD (basculement) - À propos du basculement.

Composants utilisés

Ce document n'est pas limité à des versions logicielles ou matérielles spécifiques et s'applique à tous les déploiements ASA/FTD pris en charge dans le basculement.

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 votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Qu'est-ce que Split-Brain ?

Le « split-brain » est un scénario dans lequel les unités d'une HA ASA/FTD ne peuvent pas se détecter mutuellement sur le réseau et jouent donc toutes deux un rôle actif. Les deux unités ont donc la même adresse IP et la même adresse MAC d'interface, ce qui peut entraîner de graves incohérences dans votre réseau et entraîner une perte de services.

Pour déterminer si votre HA est en mode « split-brain », exécutez la commande show failover state sur les deux unités et vérifiez si les deux cases sont actives.

Un exemple de « Split-Brain »

Unité principale :

```
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==
```

Unité secondaire :

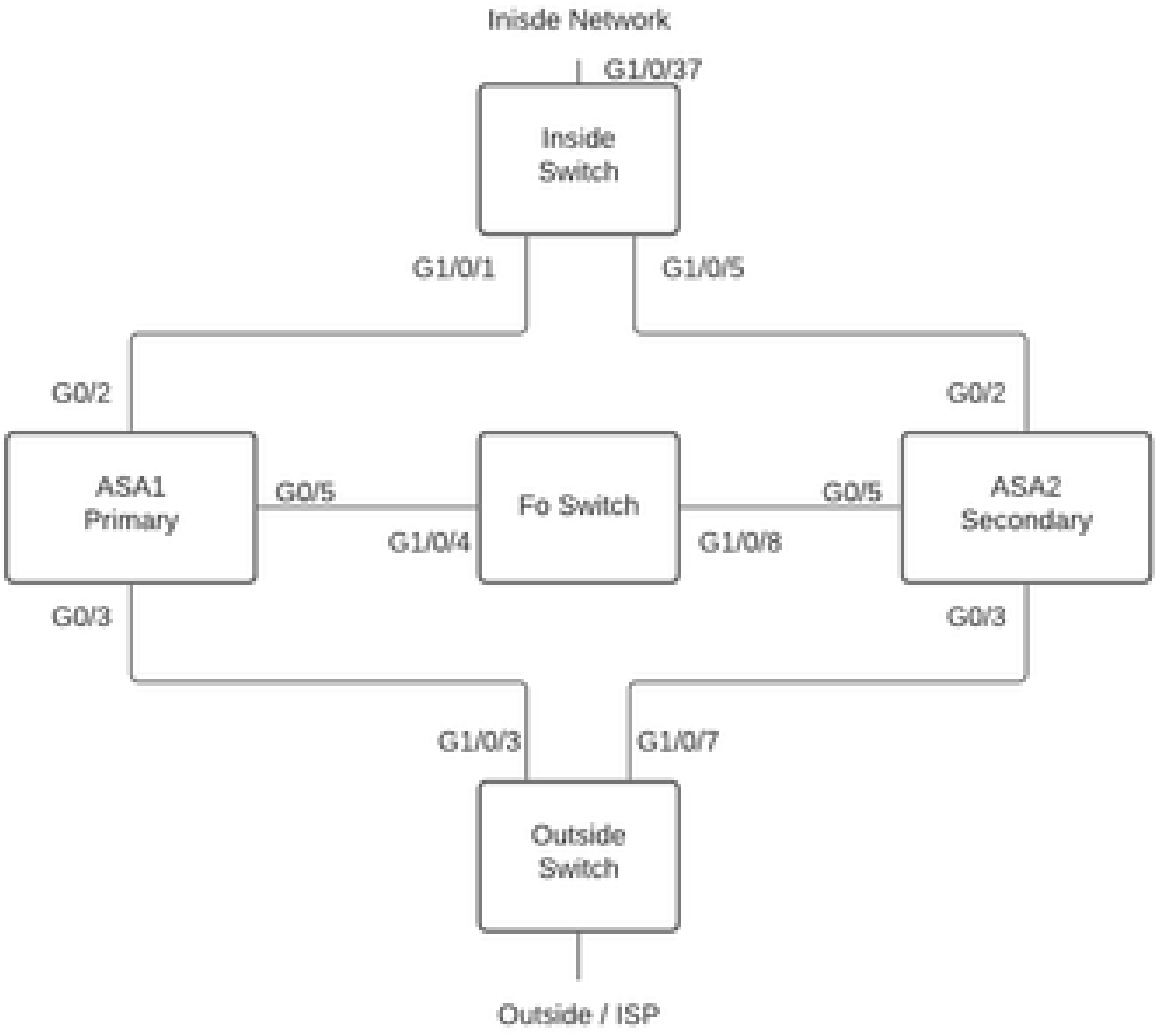
```
ciscoasa2/act/sec# show failover state

               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==
```

Le « split-brain » peut provoquer une panne si les adresses MAC apprises pour les adresses IP

actives sur les périphériques connectés ne sont pas toutes les mêmes unités. Prenons l'exemple de la topologie du réseau :



Topologie de TP

Les VMAC ont été attribués à l'interface comme indiqué. Ceci a été fait pour rendre la table d'adresses mac facile à comprendre :

```
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
```

Remarque : si les VMAC ne sont pas configurés, le périphérique actif prend toujours

l'adresse MAC de l'interface de l'unité principale et le périphérique de secours prend l'adresse MAC secondaire.

Table d’adresses MAC sur le commutateur lorsque la haute disponibilité est saine :

```
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
```

En cas de défaillance de la liaison de basculement, l'unité active reste active et l'unité en veille reste en veille. Lorsqu'une unité ne reçoit pas trois messages HELLO consécutifs sur le lien de basculement, elle envoie des messages LANTEST sur chaque interface de données, y compris le lien de basculement, pour vérifier si l'homologue répond ou non. L'action entreprise par l'ASA dépend de la réponse de l'autre unité.

Les actions possibles sont :

- Si l'ASA reçoit une réponse sur le lien de basculement, alors il ne bascule pas.
- Si l'ASA ne reçoit pas de réponse sur la liaison de basculement, mais qu'il reçoit une réponse sur une interface de données, alors l'unité ne bascule pas. Le lien de basculement est marqué comme ayant échoué. Vous pouvez restaurer le lien de basculement dès que possible, car l'unité ne peut pas basculer en veille tant que le lien de basculement est en panne.
- Si l'ASA ne reçoit pas de réponse sur aucune interface, alors l'unité en veille passe en mode actif et classe l'autre unité comme défaillante. Cela conduit à un scénario de « split-brain ».

À ce stade, toutes les interfaces de données des deux pare-feu agissent comme si elles étaient l'unité active. Ainsi, les interfaces sur le pare-feu actif et en veille utilisent les mêmes adresses IP et MAC. Cela entraîne une table d'adresses MAC incohérente en raison de l'entrée poison arp et peut donc provoquer une panne.

> Remarque : le lien de basculement est responsable de la communication de ces données entre la paire de basculement : état de l'unité (actif/veille), messages Hello, état de la liaison réseau, échange d'adresses MAC, réplication de configuration et synchronisation.

Comment se préparer de manière proactive aux problèmes de basculement

Pour vous préparer de manière proactive à une fracture du cerveau :

- Soyez sur la version d'or recommandée par Cisco - Dans certaines conditions, le « split-brain » peut également être causé par des problèmes tels qu'une fuite de mémoire. Les versions recommandées par Cisco réduisent considérablement votre exposition à de telles situations.
- Topologie du réseau : il est recommandé que les interfaces de données et les liaisons de basculement aient des chemins différents pour réduire le risque de défaillance simultanée de toutes les interfaces.
- Utiliser une interface port-channel pour l'interface de basculement : si vous avez des interfaces inutilisées sur votre pare-feu, associez-les pour former un port-channel et utilisez-le comme lien de basculement, ceci augmente la fiabilité de la liaison et supprime un point de défaillance unique (SPOF).
- Assurez-vous que l'interface de basculement n'a pas trop de latence - Selon le Guide de configuration ASA « Pour des performances optimales lors de l'utilisation du basculement longue distance, la latence pour la liaison d'état peut être inférieure à 10 millisecondes et inférieure à 250 millisecondes. Si la latence est supérieure à 10 millisecondes, une certaine dégradation des performances se produit en raison de la retransmission des messages de basculement."
- Ajuster les valeurs des compteurs d'interrogation/de mise en attente en fonction de votre déploiement - Il n'existe pas d'approche unique pour tous les compteurs de basculement. En général, lorsque vous abaissez un minuteur, cela peut entraîner des basculements inutiles (en particulier s'il y a une certaine latence), et une valeur trop élevée peut entraîner une augmentation du temps de basculement. Cela entraîne des basculements visibles. La valeur du minuteur de mise en attente doit être égale à 5 fois la valeur du minuteur d'interrogation.
- Configuration d'une adresse MAC virtuelle pour les interfaces : dans une situation où « l'unité secondaire démarre sans détecter l'unité principale, l'unité secondaire devient l'unité active et utilise ses propres adresses MAC car elle ne connaît pas les adresses MAC de l'unité principale. Lorsque l'unité principale devient disponible, l'unité secondaire (active) remplace les adresses MAC par celles de l'unité principale, ce qui peut entraîner une interruption du trafic réseau. De même, si vous remplacez l'unité principale par un nouveau matériel, une nouvelle adresse MAC est utilisée."

  Les adresses MAC virtuelles protègent contre cette interruption, car les adresses MAC actives sont connues de l'unité secondaire au démarrage et restent les mêmes dans le cas d'un nouveau matériel d'unité principale. Si vous ne configurez pas d'adresses MAC virtuelles, vous devez effacer les tables ARP sur les routeurs connectés pour restaurer le flux de trafic. Pour plus de détails, reportez-vous à la section - Adresses MAC et adresses IP dans Failover.

- Envoi des journaux ASA/FTD pour les deux unités à un serveur Syslog externe - Cette étape est plus pour la facilité de maintenance des problèmes.

Raisons possibles du « split-cerveau »

Comme nous l'avons déjà mentionné, le « split-brain » se produit lorsque la communication entre les interfaces de liaison de basculement est désactivée (de manière unidirectionnelle ou bidirectionnelle). Les raisons les plus courantes sont les suivantes :

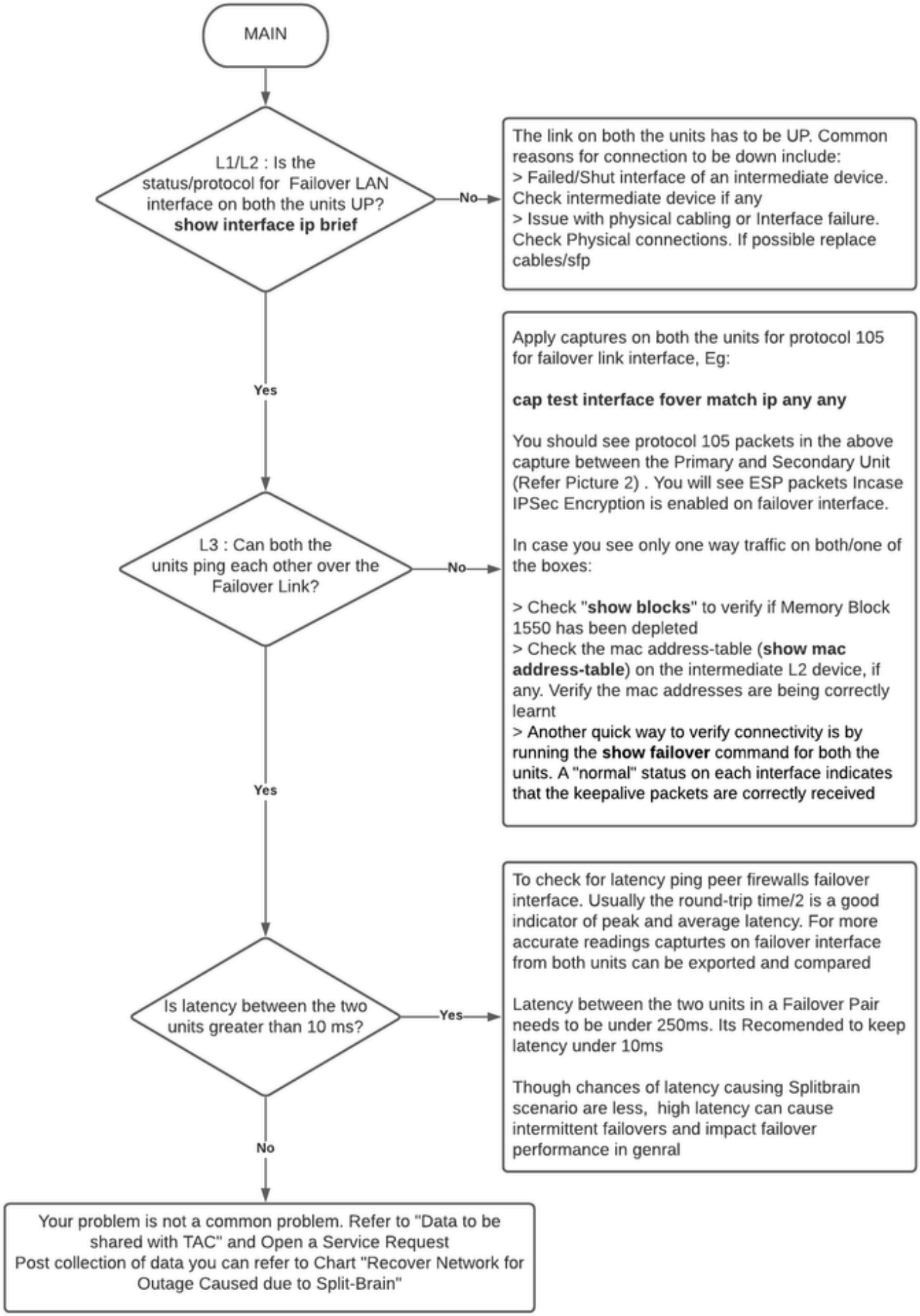
- Problèmes L1 - Câble/SFP/Interface défectueux
- Problème sur un périphérique intermédiaire
- Manque de mémoire ou de ressources processeur sur ASA/FTD

> Remarque : le moteur ASA/Lina utilise des blocs de mémoire de 1 550 octets pour stocker les paquets à traiter. Si le nombre de blocs libres de cette taille épuise l'ASA/FTD, il ne peut plus traiter les paquets de basculement. Exécutez la commande show blocks pour vérifier l'épuisement des blocs.

Procédure de dépannage - Organigramme

Afin de dépanner et de résoudre un scénario de split-brain, utilisez cet organigramme, commencez à la case marquée Main. Certains problèmes ne peuvent pas être résolus ici. Dans ce cas, des liens vers l'Assistance technique Cisco sont fournies. Afin de pouvoir effectuer une demande de service, vous devez disposer d'un contrat de service valide.

> Remarque : dans Déploiements FTD, suivez les étapes de ce tableau dans « 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"

Récupération d'urgence à partir d'un cerveau divisé

Pour récupérer votre réseau à partir d'un « split-brain », vous devez vous assurer que le trafic n'atteint qu'un des deux pare-feu, c'est-à-dire que les adresses MAC apprises pour les adresses IP actives pointent toutes vers une seule unité. Pour ce faire, vous pouvez désactiver le basculement sur l'unité ou la couper entièrement du réseau.

1. Désactivez le basculement sur l'unité qui ne transmet pas le trafic :
   - Sur la plate-forme ASA, sur CLI, accédez au terminal de configuration et entrez la commande no failover.
   - Sur la plate-forme FTD, en mode Clish, entrez la commande configure high-availability suspend.
2. Pour ASA, fermez les interfaces de données. Pour FTD, fermez les interfaces sur le périphérique connecté. Vous pouvez également déconnecter physiquement les interfaces. Vous pouvez également mettre le périphérique hors tension, mais cela vous empêche de le gérer. Reportez-vous au guide de configuration de votre périphérique pour connaître les étapes à suivre.

   Remarque : si vous remarquez des problèmes de connectivité même après avoir effectué la ou les étapes mentionnées, il est probable que les périphériques connectés disposent d'entrées ARP périmées. Vérifiez les entrées ARP sur les périphériques en amont et en aval. Pour résoudre le problème, vous pouvez soit vider ceux-ci ou forcer l'ASA/FTD en fonctionnement à envoyer un paquet garp pour l'interface IP qui a le problème. Pour ce faire, exécutez la commande en mode enable (pour FTD dans le système prend en charge diagnostics-cli) - debug menu ipaddrutl 6 <interface ip address>.

⚠ Attention : Si vous ouvrez un ticket d'assistance auprès du TAC pour des problèmes liés au « split brain », veuillez partager les informations mentionnées dans la section Données à collecter pour la demande de service du TAC dans ce document.

Données à partager avec le TAC

Veuillez partager les données mentionnées au cas où vous auriez besoin d'ouvrir une demande de service TAC.

1. Schéma de topologie montrant ASA/FTD-HA et ses connexions physiques avec les périphériques voisins (y compris les interfaces de basculement).
2. Sortie pour show tech-support sur ASA ou Troubleshooting File sur les plates-formes exécutant FTD.
3. Syslogs et horodatages pendant +/- 5 minutes lorsque le problème s'est produit.
4. Fichiers de dépannage FXOS, si le matériel est un appareil FPR.

Pour générer des fichiers de dépannage pour FTD ou FXOS, veuillez vous référer à Firepower Troubleshoot File Generation Procedures. Ouvrez un TAC SR.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.