Résolution des problèmes de fractionnement du cerveau sur le basculement ASA

Contenu

Introduction

Ce document décrit comment résoudre les problèmes courants de cerveau partagé rencontrés avec les paires haute disponibilité (HA) de Cisco Adaptive Security Appliance (ASA) Failover ou Firepower Threat Defense (FTD).

Conditions préalables

Conditions requises

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

Components Used

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

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

Qu'est-ce que Split-Brain ?

Le fractionnement du cerveau est un scénario dans lequel les unités d'une HA ASA/FTD ne peuvent pas se détecter mutuellement sur le réseau et donc les deux jouent le rôle actif. Les deux unités ont ainsi la même adresse IP et la même adresse MAC d'interface et peuvent provoquer de graves incohérences dans votre réseau, entraînant la perte de services.

Pour déterminer si votre HA est en mode fractionné, exécutez la commande **show failover state** sur les deux unités et vérifiez si les deux cases sont actives.

Exemple de cerveau fractionné :

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==
```

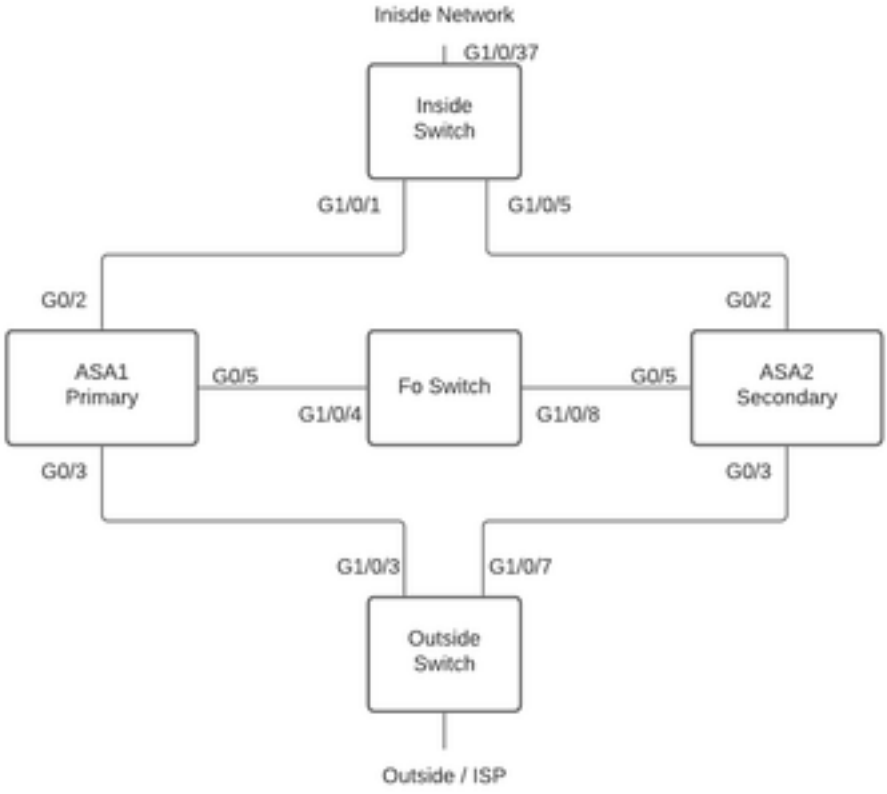
Unité secondaire :

```
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 fractionnement du cerveau peut provoquer une panne si l'adresse MAC apprise pour les adresses IP actives sur les périphériques connectés ne sont pas toutes des mêmes unités. Prenons par exemple la topologie du réseau :



Topologie des travaux pratiques

Les VMAC ont été attribués à l'interface comme suit, 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 HA 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 la veille reste en veille. Lorsqu'une unité ne reçoit pas trois messages HELLO consécutifs sur la liaison de basculement, elle envoie des messages LANTEST sur chaque interface de données, y compris la liaison de basculement, pour vérifier si l'homologue répond ou non. L'action que prend l'ASA dépend de la réponse de l'autre unité.

Les actions possibles sont les suivantes :

- 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 reçoit une réponse sur une interface de données, alors l'unité ne failover pas. Le lien de basculement est marqué comme ayant échoué. Vous devez restaurer le lien de basculement le plus tôt possible, car l'unité ne peut pas basculer en veille lorsque le lien de basculement est désactivé.
- Si l'ASA ne reçoit aucune réponse sur une interface, l'unité de secours passe en mode actif et classe l'autre unité comme ayant échoué. Cela mènera à un scénario de cerveau divisé.

Àce stade, toutes les interfaces de données des deux pare-feu agissent comme si elles étaient l'unité active. Ainsi, les interfaces du pare-feu actif et de secours utilisent la même adresse IP et MAC. Cela entraînera une table d'adresses MAC incohérente en raison d'une entrée de l'arp empoisonnée et donc une panne.

> **Note:** La liaison de basculement est responsable de la communication de ces données entre la paire de basculement : état de l'unité (actif/en 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 se préparer de manière proactive à une condition de fractionnement du cerveau :

- Soyez sur la version d'or recommandée par Cisco - Dans certaines conditions, le fractionnement du cerveau peut également être dû à des problèmes tels qu'une fuite de mémoire. En faisant partie des versions recommandées par Cisco, vous réduisez considérablement votre exposition à de telles situations.
- Topologie du réseau : il est recommandé que les interfaces de données et les liaisons de basculement disposent de chemins différents pour diminuer 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 liaison de basculement, cela augmentera la fiabilité de la liaison et supprimera 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 de la liaison d'état doit être inférieure à 10 millisecondes et ne pas dépasser 250 millisecondes. Si la latence est supérieure à 10 millisecondes, une dégradation des performances se produit en raison de la retransmission des messages de basculement. »
- Ajuster les valeurs du minuteur de sondage/du minuteur de mise en attente en fonction de

votre déploiement : il n'existe aucune approche unique pour tous les minuteurs de basculement. En règle générale, le fait de réduire la durée d'un compteur peut entraîner des basculement inutiles (en particulier en cas de latence) et une valeur trop élevée peut entraîner une augmentation du temps de basculement. Ce qui mène à des basculement visibles. La valeur du minuteur d'attente doit être égale à 5x.

- Configuration d'une adresse MAC virtuelle pour les interfaces - Dans une condition où « l'unité secondaire démarre sans détecter l'unité principale, l'unité secondaire devient l'unité active et utilise ses propres adresses MAC parce qu'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 du nouveau matériel de l'unité principale. Si vous ne configurez pas d'adresses MAC virtuelles, vous devrez peut-être 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 le basculement.
- Envoyer des journaux ASA/FTD pour les deux unités à un serveur Syslog externe : cette étape est plus adaptée à la facilité de maintenance des problèmes.

Raisons possibles du fractionnement du cerveau

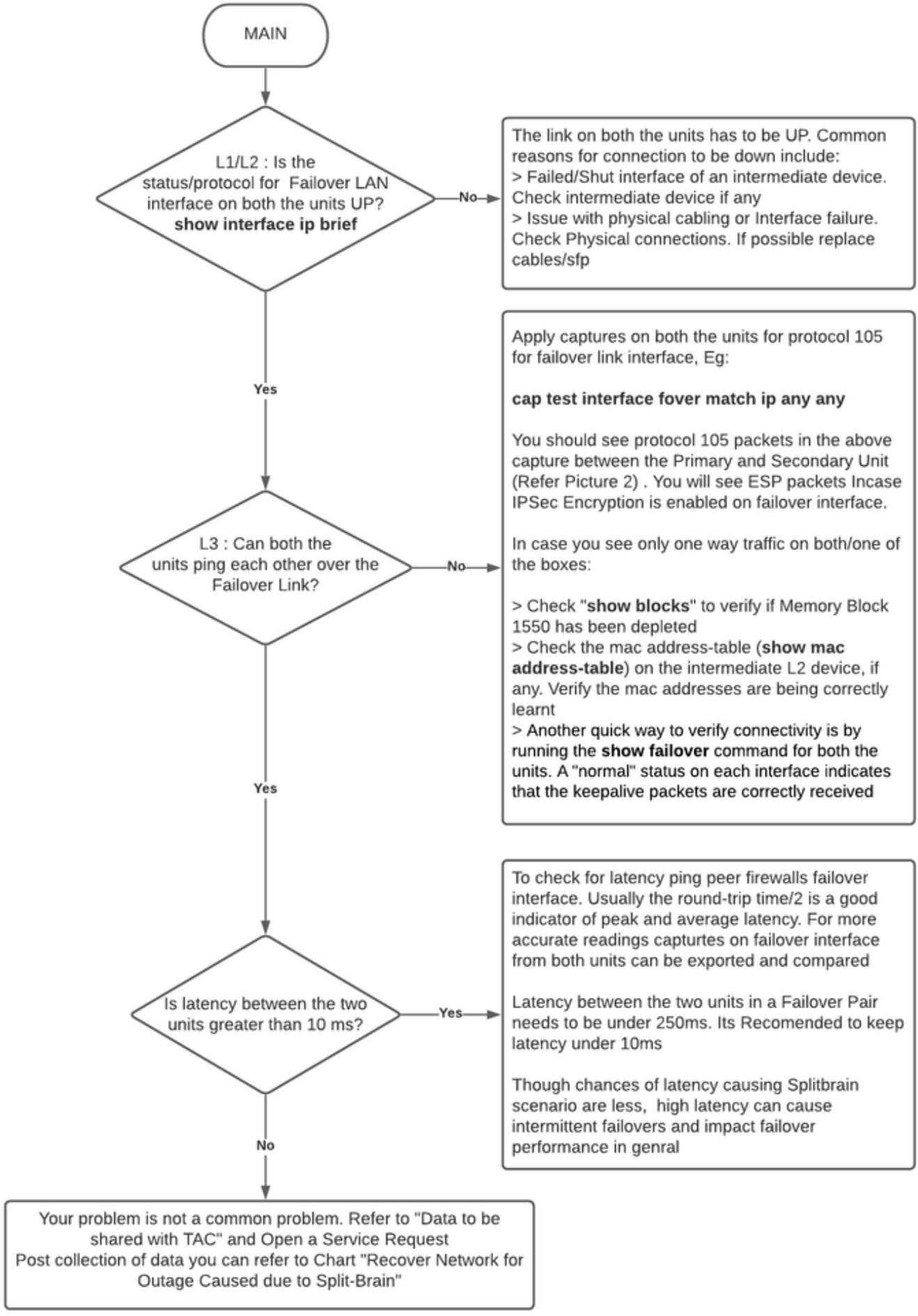
Comme indiqué précédemment, le fractionnement du cerveau se produit lorsque la communication entre les interfaces de liaison de basculement est interrompue (de manière unidirectionnelle ou bidirectionnelle). Les raisons les plus courantes sont les suivantes :

- Problèmes de couche 1 - 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 diminue, ASA/FTD ne pourra 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 résoudre un scénario de fractionnement du cerveau, utilisez ce diagramme de flux, commencez à la case marquée **Principal**. Certains problèmes sont susceptibles de ne pouvoir 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 les déploiements FTD, les étapes de ce tableau doivent être suivies à partir de “ **diagnostic-cli support** ”.



Graphique de flux de dépannage

Récupération d'urgence à partir de fractionnement du cerveau

Pour récupérer votre réseau à partir d'un cerveau partagé, vous devez vous assurer que le trafic ne touche qu'un des deux pare-feu, c'est-à-dire que les adresses MAC apprises pour les adresses IP actives doivent toutes pointer vers une seule unité. Pour ce faire, vous pouvez désactiver le basculement sur l'unité ou l'interrompre entièrement sur le réseau.

1. Désactivez le basculement sur l'unité qui ne transmet pas le trafic : Sur la plate-forme ASA, via l'interface de ligne de commande, 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 suspense**.
2. Pour ASA, arrêtez les interfaces de données. Pour FTD, arrêtez les interfaces sur le périphérique connecté. Vous pouvez également déconnecter physiquement les interfaces. Vous pouvez également mettre le périphérique hors tension, mais cela vous empêchera de gérer le périphérique. 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 les étapes mentionnées, il est probable que les périphériques connectés aient des entrées arp obsolètes. Vérifiez les entrées ARP sur les périphériques en amont et en aval. Pour résoudre le problème, vous pouvez soit les vider, soit forcer l'ASA/FTD fonctionnel à envoyer un paquet de paquets pour l'adresse IP de l'interface qui a le problème. Pour ce faire, exécutez la commande en mode enable (pour FTD dans le système prend en charge diagnostics-cli) - **menu debug ipaddrutl 6 <adresse ip de l'interface>**.

   Attention : Si vous ouvrez un ticket d'assistance avec le TAC pour les problèmes liés au cerveau partagé, 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

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

1. Schéma de topologie qui montre 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 avec horodatages pendant +/- 5 minutes lorsque le problème est survenu.
4. Fichiers de dépannage FXOS, si le matériel est un appareil FPR.

Pour générer des fichiers de dépannage pour FTD ou FXOS, référez-vous à Procédures de dépannage de Firepower pour la génération de fichiers. Ouvrez une demande de service TAC.