Probleemoplossing met splitter/brein-problemen bij ASA-failover

Inhoud

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen bij uw gebruikelijke problemen met gesplitste hersenen die u hebt ondervonden met lucht-over-Cisco adaptieve security applicatie (ASA) of Firepower Threat Defense (FTD) Hoge beschikbaarheid (HA) telefoons.

Voorwaarden

Vereisten

Cisco raadt u aan om kennis te hebben over hoe ASA/FTD High Availability Pair (failover) werkt - About failover.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- of hardwareversies en is van toepassing op alle ondersteunde ASA/FTD-implementaties in failover.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Wat is Split-Brain?

Split-brain is een scenario waarin de eenheden van een ASA/FTD HA elkaar niet kunnen detecteren op het netwerk en dus beide de actieve rol kunnen spelen. Dit veroorzaakt dat beide eenheden hetzelfde IP-adres en hetzelfde MAC-adres hebben en kan ernstige inconsistenties in uw netwerk veroorzaken wat leidt tot verlies van services.

Om te identificeren of uw HA in gespleten brein is, **laat** de opdracht **de** status **van** de **failover** op zowel de eenheden **zien** en controleer of beide boxen actief zijn.

Een voorbeeld van een splitter-brein:

Primaire eenheid:

```
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==
```

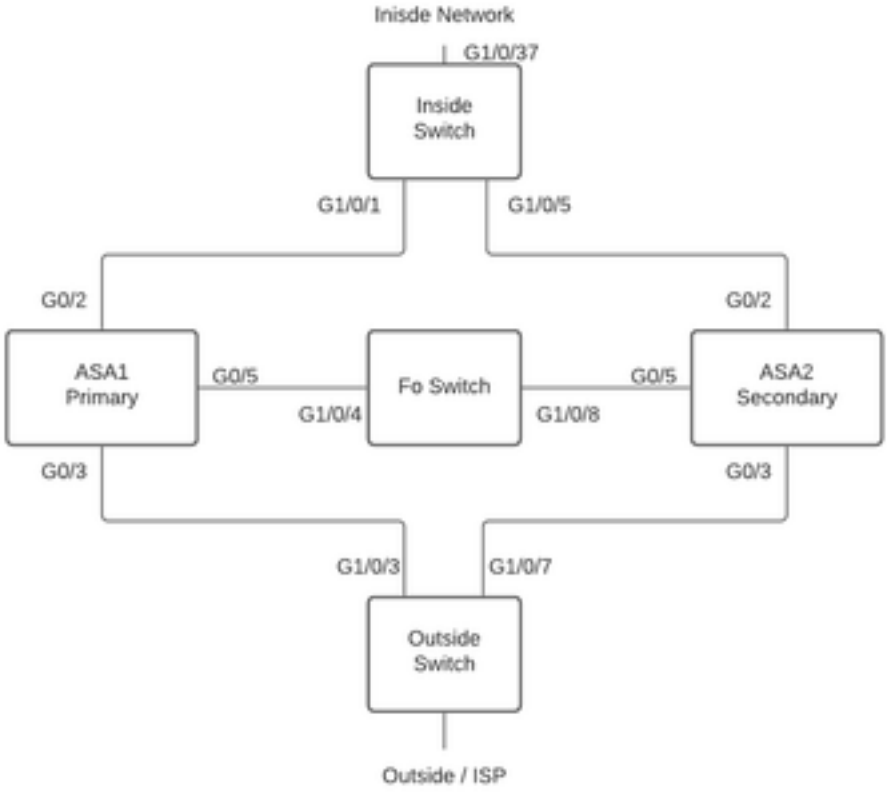
Secundaire eenheid:

```
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==
```

Splitsen-hersenen kunnen een stroomstoring veroorzaken als het MAC-adres dat is geleerd voor de actieve IP-adressen op de aangesloten apparaten niet alle dezelfde eenheden zijn. Denk bijvoorbeeld aan de netwerktopologie:



Lab Topologie

De VMAC's zijn als volgt aan de interface toegewezen, wat is gedaan om de **hoofdadrestabel** gemakkelijk te begrijpen:

```
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
```

Opmerking: Als VMAC's niet zijn ingesteld, neemt het actieve apparaat altijd de MAC voor de Primaire unit-interface en de standby neemt de secundaire MAC.

MAC-adrestabel op Switch bij een goede HA:

```
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
```

Indien de failover-koppeling niet werkt, blijft de actieve eenheid actief en blijft de stand-by standby

standby. Wanneer een unit geen drie opeenvolgende HELLO-berichten op de failover-link ontvangt, stuurt de unit LANTEST-berichten op elke gegevensinterface, inclusief de failover-link, om te bevestigen of de peer al dan niet reageert. De actie die de ASA onderneemt hangt af van de reactie van de andere eenheid.

De mogelijke acties zijn:

- Als de ASA een respons op de failover link ontvangt, dan is de failover niet defect.
- Als de ASA geen respons op de failover-link ontvangt, maar wel een respons op een data-interface ontvangt, dan is de eenheid geen failover. De failover-link is gemarkeerd als mislukt. U dient de failover-link zo snel mogelijk te herstellen omdat de unit niet kan uitvallen op standby terwijl de failover-link is uitgevallen.
- Als de ASA geen respons op een interface heeft ontvangen, dan worden de switches van de standby-unit in de actieve modus geclassificeerd en de andere unit als defect geclassificeerd. Dit zal leiden tot een Split-brain-scenario.

In deze fase zullen alle data interfaces op beide firewalls werken alsof ze de actieve eenheid zijn. Dus, interfaces op de actieve en standby firewall zullen het zelfde IP en MAC adres gebruiken. Dit zal leiden tot een inconsistente MAC-adrestabel door vergiftige arp-ingang en zal daarom een defect veroorzaken.

> **Opmerking:** Failover Link is verantwoordelijk voor de communicatie van deze gegevens tussen het Failover-paar: Unit State (active/stand-by), Hello berichten, Network Link-status, MAC-adresuitwisseling, Config-replicatie en sync.

Proactief voorbereiden op failover-problemen

Proactief voorbereiden op een splitter-hersenaandoening:

- Wees op de door Cisco aanbevolen gouden release - Onder bepaalde omstandigheden kan splitsen-brein ook worden veroorzaakt door problemen zoals een lek in het geheugen. Door op Cisco Aanbevolen releases te zijn te zijn, beperkt u uw blootstelling aan dergelijke situaties aanzienlijk.
- Netwerktopologie - Het wordt aanbevolen dat de Data Interfaces en de Failover links verschillende paden hebben om de kans op alle interfaces tegelijk te verminderen.
- Gebruik een poort-kanaalinterface voor de failover-interface - Als u ongebruikte interfaces op uw firewall hebt, koppelt u deze aan om een poortkanaal te vormen en het als de Failover Link te gebruiken, zal dit de betrouwbaarheid van de link vergroten en een Single Point of Failover (SPOF) verwijderen.
- Zorg ervoor dat de failover-interface niet te veel latentie heeft - Zoals in de ASA Config Guide "Voor optimale prestaties bij gebruik van lange-afstand-failover, moet de latentie voor de staatslink minder dan 10 milliseconden en niet meer dan 250 milliseconden zijn. Als de latentie meer dan 10 milliseconden is, komt enige prestatie-degradatie voor door hertransmissie van failover-berichten."
- Stel de waarden van de Timer/van de Hold Timer in zoals per uw plaatsing - er is geen één groote pasklare benadering van de a-overnamemeerders. In het algemeen, kan een timer laag een onnodige failover veroorzaken (vooral als er wat vertraging is) en kan een te hoge waarde tot verhoogde tijd voor een failover leiden om te voorkomen. Dat zal leiden tot

aanzienlijke mislukkingen. De waarde van de timer vasthouden moet 5x pooltimer zijn.
- Het configureren van een virtueel MAC-adres voor interfaces - Onder een voorwaarde waarbij "de secundaire unit start zonder de primaire unit te detecteren, wordt de secundaire eenheid de actieve eenheid en gebruikt de eigen MAC-adressen omdat de eenheid de primaire MAC-adressen niet kent. Wanneer de primaire eenheid beschikbaar wordt, verandert de secundaire (actieve) eenheid de MAC adressen aan die van de primaire eenheid, die een verstoring in uw netwerkverkeer kan veroorzaken. Op dezelfde manier wordt, als u de primaire eenheid met nieuwe hardware verruilt, een nieuw MAC-adres gebruikt." Virtuele MAC-adressen beschermen tegen deze verstoring, omdat de actieve MAC-adressen bekend zijn bij de secundaire eenheid bij opstarten, en hetzelfde blijven in het geval van nieuwe primaire unit-hardware. Als u geen virtuele MAC-adressen instelt, moet u misschien de ARP-tabellen op aangesloten routers wissen om de verkeersstroom te herstellen." Raadpleeg voor meer informatie - MAC-adressen en IP-adressen bij failover.
- ASA/FTD Logs voor beide eenheden naar een externe Syrische server sturen - Deze stap is meer voor de bruikbaarheid van problemen.

Mogelijke redenen voor Split-Brain

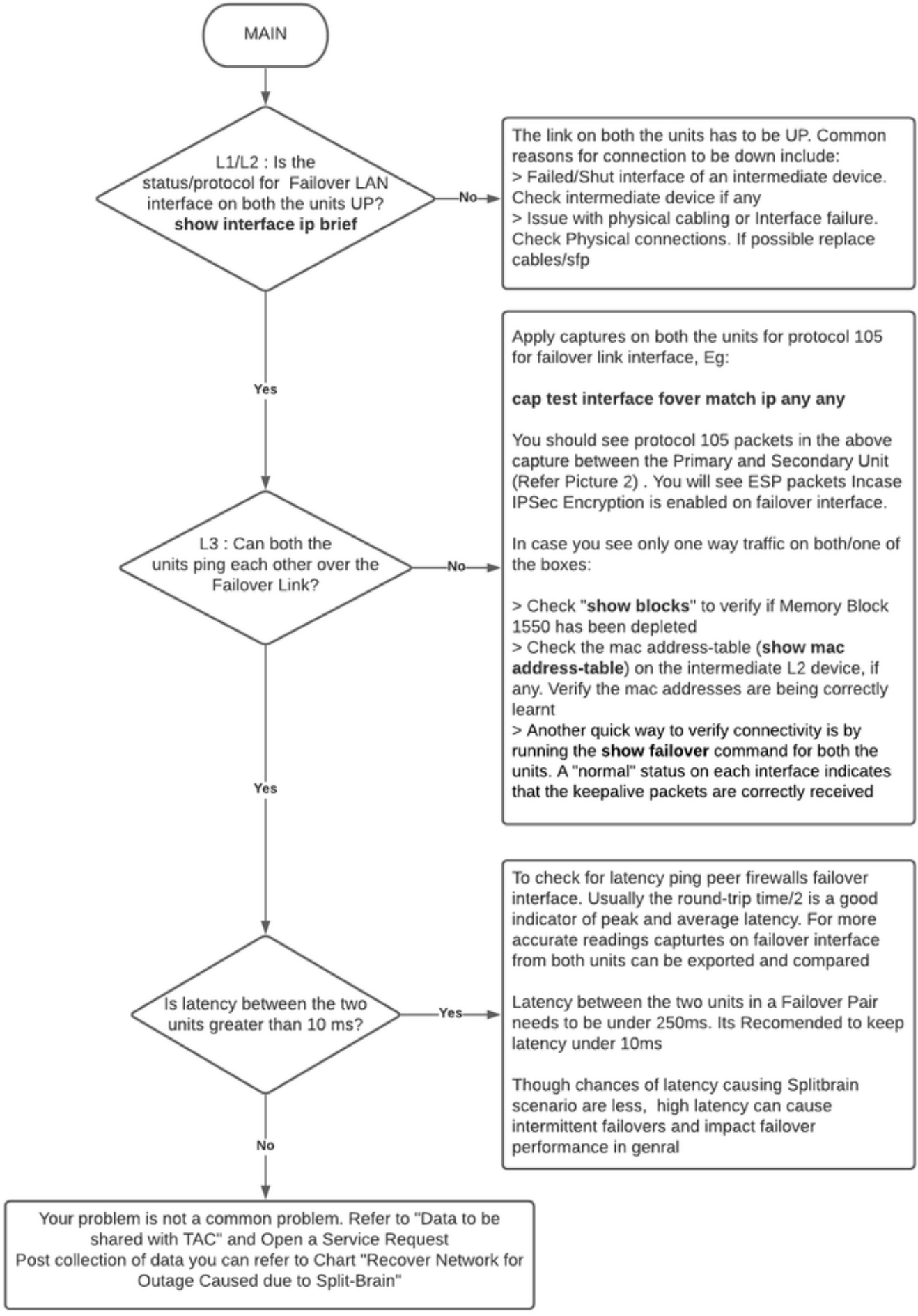
Zoals reeds vermeld, splitsen-brein komt voor wanneer de communicatie tussen de failliet Link interfaces is neergeslagen (unidirectioneel of bidirectioneel). De meest voorkomende redenen zijn:

- L1-problemen - defecte kabel/SFP/interface
- Een probleem met betrekking tot een tusseninstrument
- Gebrek aan geheugen of CPU-bronnen op ASA/FTD **Opmerking:** De ASA/LAN Engine gebruikt 1550 bytes geheugenblokken om pakketten op te slaan voor verwerking. Als het aantal gratis blokken van deze grootte uitgeput is, zal de ASA/FTD niet langer in staat zijn om failover-pakketten te verwerken. Draai de **showblokken** om te controleren op blokkdepletie.

Procedure voor probleemoplossing - stroomschema

Om een oplossing te vinden en een z.g.-breinscenario op te lossen, gebruikt u dit stroomschema, start in het vak met de markering **Main**. Er zijn een aantal problemen die wellicht niet kunnen worden opgelost. In deze gevallen worden de koppelingen geleverd aan Cisco Technical Support. U moet een geldig servicecontract hebben afgesloten om een serviceaanvraag te openen.

> **Opmerking:** Bij FTD-implementaties moeten de stappen in deze grafiek worden gevolgd van "**systeemondersteuning van diagnostiek-cli**".



Flow Chart voor probleemoplossing

Noodherstel na splitter-brein

Om uw netwerk van een gespleten brein terug te krijgen moet u ervoor zorgen dat het verkeer slechts één van de twee firewalls raakt, dat wil zeggen, de MAC adressen die voor de actieve IP's zijn geleerd moeten allen op één eenheid richten. Hiervoor kunt u failover op de unit uitschakelen of het netwerk volledig afsluiten.

1. Uitschakelen van failover op het apparaat dat geen verkeer doorgeeft: Op ASA Platform, via CLI, navigeer naar de configuratie terminal en voer **geen failover** opdracht in.Op het FTD Platform, over Clish modus, voer **de configuratie hoge beschikbaarheid schorsopdracht in**.
2. Voor ASA, sluit de data interfaces. Voor FTD, sluit de interfaces op het aangesloten apparaat. In plaats hiervan kunt u ook de interfaces fysiek uitschakelen. U kunt ook het apparaat uitzetten, maar dit beperkt u tot het beheer van het apparaat. Raadpleeg uw machine-configuratie gids op de stappen om dit te doen.

   N.B.: Als u problemen met de connectiviteit opmerkt zelfs nadat u de bovengenoemde stap(en) hebt uitgevoerd, is het waarschijnlijk dat de aangesloten apparatuur(apparaten) vaste arp-items hebben. Controleer de arp-ingangen op stroomopwaarts en stroomafwaarts gerichte apparatuur. Om het probleem te repareren kunt u deze doorspoelen of de werkende ASA/FTD dwingen om een pakket garp voor de interface-IP te verzenden dat het probleem heeft. Om dit te doen, voer opdracht in om modus (voor FTD in System ondersteunt diagnostiek-cli) in te schakelen - **debug menu ipad 6 <interface ip-adres>**.

   Voorzichtig: Als u een ondersteuningsticket met TAC opent voor problemen met betrekking tot Split-hersenen, deelt u de informatie onder sectie **Data** die **moet worden verzameld voor TAC-serviceaanvraag** in dit document.

Gegevens die met TAC moeten worden gedeeld

Geef de vermelde gegevens door voor het geval u een TAC-serviceaanvraag moet openen.

1. Topologisch diagram dat ASA/FTD-HA en zijn fysieke verbindingen met naburige apparaten (inclusief failover-interfaces) toont.
2. Uitvoer voor **show tech-support** bij ASA of bestand voor probleemoplossing op platforms die FTD uitvoeren.
3. Syslogs samen met tijdzegels voor +/- 5 minuten toen de kwestie optrad.
4. FXOS-bestanden voor probleemoplossing, als de hardware een FPR-apparaat is.

Raadpleeg de procedures voor het genereren van problemen bij het genereren van bestanden voor FTD of FXOS. Open een TAC-SR.