Solucionar problemas de split-brain no failover do ASA

Contents

Introduction

Este documento descreve como solucionar problemas comuns de split-brain encontrados com o failover do Cisco Adaptive Security Appliance (ASA) ou pares de alta disponibilidade (HA) do Firepower Threat Defense (FTD).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento sobre como o ASA/FTD High Availability Pair (Failover) funciona - Sobre failover.

Componentes Utilizados

Este documento não está restrito a versões específicas de software ou hardware e se aplica a todas as implantações de ASA/FTD suportadas em 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

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

O que é Split-Brain?

Split-brain é um cenário em que as unidades de um ASA/FTD HA são incapazes de se detectar na rede e, portanto, ambas assumem a função ativa. Isso faz com que ambas as unidades tenham o mesmo endereço IP e endereço MAC da interface e pode causar inconsistências graves na rede, resultando em perda de serviços.

Para identificar se seu HA está em split-brain, execute o comando **show failover state** em ambas as unidades e verifique se ambas as caixas estão ativas.

Um exemplo de um cérebro dividido:

Unidade primária:

```
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==
```

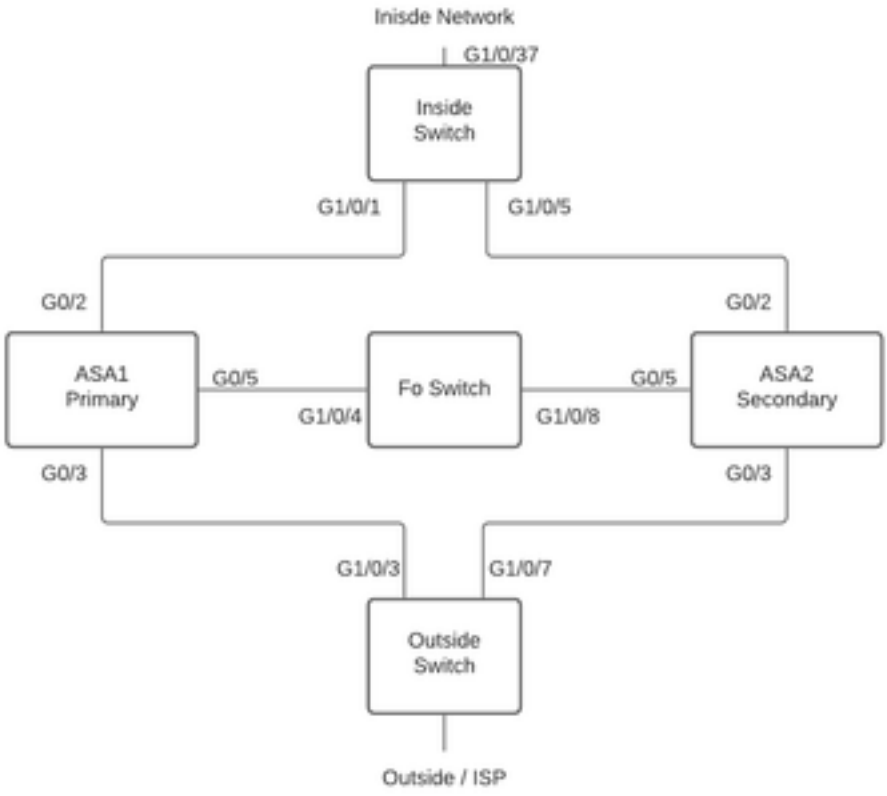
Unidade secundária:

```
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==
```

O split-brain (cérebro dividido) pode causar uma interrupção se o endereço MAC aprendido para os endereços IP ativos nos dispositivos conectados não forem todas as mesmas unidades. Por exemplo, considere a topologia de rede:



Topologia de laboratório

Os VMACs foram atribuídos à interface da seguinte forma, isso foi feito para tornar a **tabela de endereços mac** 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:** se os VMACs não estiverem configurados, o dispositivo Ativo sempre usará o MAC para a interface da unidade primária e o standby usará o MAC secundário.

Tabela de endereços MAC no switch quando o HA está em bom 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
```

Se o link de failover falhar, a unidade ativa deve permanecer ativa e o standby permanece em espera. Quando uma unidade não recebe três mensagens HELLO consecutivas no link Failover, a unidade envia mensagens LANTEST em cada interface de dados, incluindo o link de failover, para validar se o peer está respondendo ou não. A ação tomada pelo ASA depende da resposta da outra unidade.

As ações possíveis são:

- Se o ASA receber uma resposta no link de failover, ele não realizará failover.
- Se o ASA não receber uma resposta no link de failover, mas receber uma resposta em uma interface de dados, a unidade não realizará failover. O link de failover está marcado como falha. Você deve restaurar o link de failover o mais rápido possível porque a unidade não pode fazer failover para standby enquanto o link de failover está inativo.
- Se o ASA não receber uma resposta em nenhuma interface, a unidade de standby alterna para o modo ativo e classifica a outra unidade como falha. Isso levará a um cenário de cérebro dividido.

Neste estágio, todas as interfaces de dados em ambos os Firewalls atuarão como se fossem a unidade ativa. Assim, as interfaces no firewall ativo e em standby usarão os mesmos endereços IP e MAC. Isso levará a uma tabela de endereços MAC inconsistente devido à entrada arp venenosa e, portanto, causará uma interrupção.

> **Note:** O link de failover é responsável pela comunicação desses dados entre o par de failover: estado da unidade (ativo/standby), mensagens de saudação, status do link da rede, troca de endereço MAC, replicação de configuração e sincronização.

Como se preparar proativamente contra problemas de failover

Para se preparar proativamente contra uma condição de cérebro dividido:

- Esteja na versão de ouro recomendada pela Cisco - Em certas condições, o split-brain também pode ser causado por problemas como vazamento de memória. Com as versões recomendadas pela Cisco, você reduz bastante a exposição a tais situações.
- Topologia de rede - Recomenda-se que as interfaces de dados e os links de failover tenham caminhos diferentes para diminuir a chance de todas as interfaces falharem ao mesmo tempo.
- Usar uma interface de canal de porta para a interface de failover - Se você tiver interfaces não utilizadas no firewall, emparelhe-as para formar um canal de porta e use-o como o link de failover, isso aumentará a confiabilidade do link e removerá um ponto de falha único (SPOF).
- Certifique-se de que a interface de failover não tenha muita latência - De acordo com o Guia de configuração do ASA "Para obter o melhor desempenho ao usar failover de longa distância, a latência do link de estado deve ser menor que 10 milissegundos e não mais que 250 milissegundos. Se a latência for superior a 10 milissegundos, alguma degradação do desempenho ocorrerá devido à retransmissão de mensagens de failover."
- Ajuste os valores do temporizador de sondagem/temporizador de espera de acordo com sua implantação - Não há um tamanho único para todos os métodos de temporizadores de failover. Em geral, um temporizador baixo pode causar failover desnecessário (especialmente se houver alguma latência) e um valor muito alto pode levar a um tempo maior para que

ocorra um failover. O que levará a failover notável. O valor do Temporizador de Espera deve ser 5x o valor do Temporizador de Votação.
- Configurando um endereço MAC virtual para interfaces - Em uma condição em que "a unidade secundária inicializa sem detectar a unidade primária, a unidade secundária se torna a unidade ativa e usa seus próprios endereços MAC porque não conhece os endereços MAC da unidade primária. Quando a unidade primária se torna disponível, a unidade secundária (ativa) altera os endereços MAC para os da unidade primária, o que pode causar uma interrupção no tráfego da rede. Da mesma forma, se você trocar a unidade primária por um novo hardware, um novo endereço MAC será usado." Os endereços MAC virtuais protegem contra essa interrupção, pois os endereços MAC ativos são conhecidos pela unidade secundária na inicialização e permanecem os mesmos no caso de novo hardware de unidade primária. Se você não configurar endereços MAC virtuais, talvez precise limpar as tabelas ARP em roteadores conectados para restaurar o fluxo de tráfego". Para obter mais detalhes, consulte Endereços MAC e Endereços IP em Failover.
- Enviar registros ASA/FTD para ambas as unidades para um servidor Syslog externo - Esta etapa é mais para a facilidade de manutenção dos problemas.

Motivos possíveis para o cérebro dividido

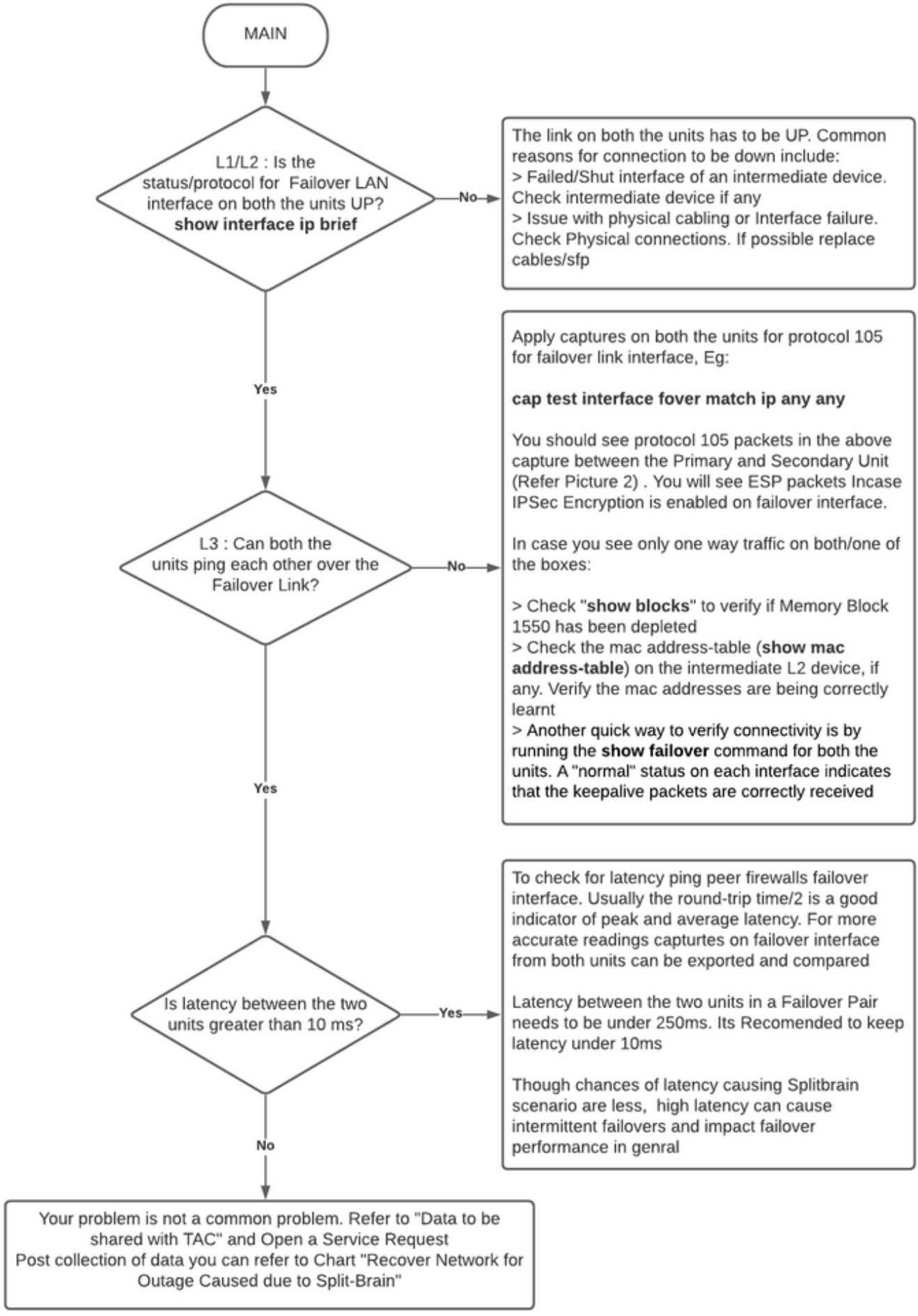
Como já foi mencionado, o split-brain ocorre quando a comunicação entre as interfaces de link de failover está inoperante (unidirecional ou bidirecional). Os motivos mais comuns são:

- Problemas de L1 - Cabo/SFP/Interface defeituosos
- Um problema em um dispositivo intermediário
- Falta de memória ou recursos da CPU no ASA/FTD **Observação:** o ASA/Lina Engine utiliza blocos de memória de 1550 bytes para armazenar pacotes para processamento. Se o número de blocos livres desse tamanho esgotar o ASA/FTD não conseguirá mais processar pacotes de failover. Execute os **blocos show** para verificar a depleção de blocos.

Procedimento para solução de problemas - fluxograma

Para solucionar problemas e resolver um cenário de cérebro dividido, use este fluxograma e comece na caixa marcada como **Main**. Há alguns problemas que podem não ser resolvidos aqui. Nesses casos, são fornecidos links para o Suporte Técnico da Cisco. Para abrir uma solicitação de serviço, você deve ter um contrato de serviço válido.

> **Observação:** em implantações FTD, as etapas neste gráfico devem ser seguidas de "**system support diagnostics-cli**".



Troubleshooting de Fluxograma

Recuperação de emergência de split-brain

Para recuperar sua rede de um cérebro dividido, você precisa garantir que o tráfego atinja apenas um dos dois firewalls, ou seja, os endereços MAC aprendidos para os IPs ativos devem apontar para uma única unidade. Para fazer isso, você pode desativar o failover na unidade ou cortá-lo totalmente da rede.

1. Desabilitar failover na unidade que não está passando tráfego: Na plataforma ASA, na CLI, navegue até o terminal de configuração e insira o comando **no failover**.Na plataforma FTD, no modo de Certificação, insira o comando **configure high-available suspendure**.
2. Para o ASA, feche as interfaces de dados. Para o FTD, feche as interfaces no dispositivo conectado. Como alternativa, você também pode desconectar fisicamente as interfaces. Além disso, você pode desligar o dispositivo, mas isso o limitará de gerenciar o dispositivo. Consulte o guia de configuração do dispositivo para saber como fazer isso.

   Nota: Se você notar problemas de conectividade mesmo depois de executar as etapas mencionadas, é provável que os dispositivos conectados tenham entradas arp antigas. Verifique as entradas arp em dispositivos upstream e downstream. Para corrigir o problema, você pode descarregá-los ou forçar o ASA/FTD em funcionamento a enviar um pacote garp para o IP da interface que tem o problema. Para fazer isso, execute o comando no modo de ativação (para FTD no sistema suporta diagnósticos-cli) - **debug menu ipaddrutl 6 <interface ip address>**.

   Caution: Caso você abra um tíquete de suporte com TAC para problemas relacionados à divisão do cérebro, compartilhe as informações mencionadas na seção **Dados a serem coletados para a solicitação de serviço do TAC** neste documento.

Dados a serem compartilhados com o TAC

Compartilhe os dados mencionados caso precise abrir uma solicitação de serviço do TAC.

1. Diagrama de topologia que mostra o ASA/FTD-HA e suas conexões físicas com dispositivos vizinhos (incluindo interfaces de failover).
2. Saída para **show tech-support** no ASA ou Troubleshooting File em Plataformas que executam FTD.
3. Syslogs junto com timestamps por +/- 5 minutos quando o problema ocorreu.
4. Arquivos de solução de problemas do FXOS, se o hardware for um dispositivo FPR.

Para gerar arquivos de solução de problemas para FTD ou FXOS, consulte Procedimentos de solução de problemas do Firepower. Abra um TAC SR.