Troubleshoot Split-Brain Issues on ASA Failover

Contents

Introduction

This document describes how to troubleshoot common split-brain problems encountered with Cisco Adaptive Security Appliance (ASA) Failover or Firepower Threat Defence (FTD) High Availability (HA) Pairs.

Prerequisites

Requirements

Cisco recommends that you have knowledge about how ASA/FTD High Availability Pair (Failover) works - About Failover.

Components Used

This document is not restricted to specific software or hardware versions and applies to all supported ASA/FTD deployments in 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. If your network is live, ensure that you understand the potential impact of any command.

Conventions

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

What is Split-Brain?

Split-brain is a scenario in which the units of an ASA/FTD HA are unable to detect each other on the network and hence both take the active role. This causes both the units to have the same interface IP Address and MAC Address and may cause severe inconsistencies in your network resulting in loss of services.

To identify if your HA is in split-brain, run the command **show failover state** on both the units and check if both boxes are active.

An example of a Split-brain:

Primary Unit:

```
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==
```

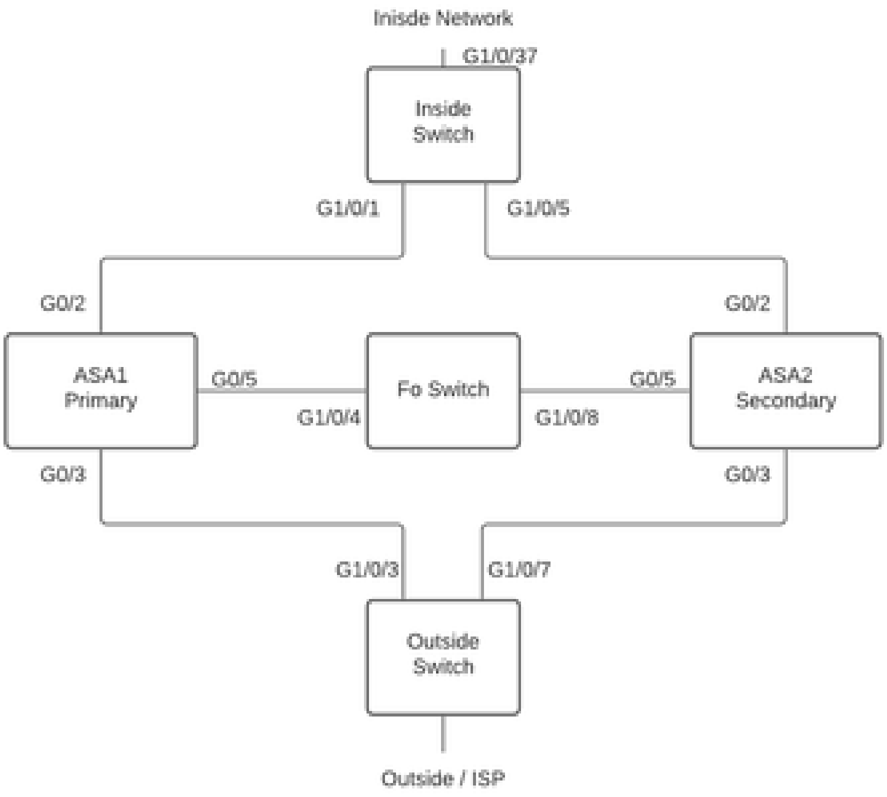
Secondary unit:

```
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==
```

Split-brain may cause an outage if the MAC address learnt for the Active IP Addresses on the connected devices are not all of the same units. For example, consider the network topology:



Lab Topology

VMAC’s have been assigned to the interface as follows, this has been done to make the **mac address-table** easy to understand:

```
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
```

> **Note:** If VMAC’s are not configured the Active device always take the MAC for the Primary unit interface and standby takes the Secondary MAC.

MAC Address Table on Switch when HA is healthy:

```
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
```

Should the Failover link fail, the active unit shall stay active and the standby remains standby.

When a unit does not receive three consecutive HELLO messages on the Failover link, the unit sends LANTEST messages on each data interface, including the failover link, to validate whether or not the peer is responsive. The action that the ASA takes depends on the response from the other unit.

Possible actions are:

- If the ASA receives a response on the failover link, then it does not failover.
- If the ASA does not receive a response on the failover link, but it does receive a response on a data interface, then the unit does not failover. The failover link is marked as failed. You should restore the failover link as soon as possible because the unit cannot failover to standby while the failover link is down.
- If the ASA does not receive a response on any interface, then the standby unit switches to active mode and classifies the other unit as failed. This will lead to a Split-brain scenario.

At this stage, all data interfaces on both the Firewalls will act like they are the active unit. So, interfaces on the active and standby firewall will use the same IP and MAC address. This will lead to an inconsistent MAC address-table due to poison arp entry and hence cause an outage.

> **Note:** Failover Link is responsible for the communication of this data between the Failover Pair: Unit State (active/standby), Hello messages, Network Link status, MAC Address exchange, Config Replication and Sync.

How to Proactively Prepare Against Failover Issues

To proactively prepare against a Split-brain condition:

- Be on the Cisco Recommended Golden Release - Under certain conditions, split-brain can also be caused due to issues like a memory leak. By being on Cisco Recommended releases you greatly reduce your exposure to such situations.
- Network Topology - It is recommended that the Data Interfaces and the Failover Links have different paths to decrease the chance of all interfaces failing at the same time.
- Use a port-channel interface for the Failover interface - If you have unused interfaces on your firewall, pair them to form a port-channel and use it as the Failover Link, this will increase link reliability and remove a Single Point of Failure (SPOF).
- Ensure Failover interface doesn't have too much latency - As per the ASA Config Guide "For optimum performance when using long distance failover, the latency for the state link should be less than 10 milliseconds and no more than 250 milliseconds. If latency is more than 10 milliseconds, some performance degradation occurs due to retransmission of failover messages."
- Adjust Poll Timer/Hold Timer values as per your deployment - There is no one size fits all approach to failover Timers. In general, to low a timer can cause unnecessary Failovers (especially if there is some latency) and too high a value can lead to increased time for a failover to occur. Which will lead to noticeable Failovers. Hold Timer value must be 5x Poll Timer value.
- Configuring a Virtual MAC Address for interfaces - Under a condition where "the secondary unit boots without detecting the primary unit, then the secondary unit becomes the active unit and uses its own MAC addresses because it does not know the primary unit MAC addresses.

When the primary unit becomes available, the secondary (active) unit changes the MAC addresses to those of the primary unit, which can cause an interruption in your network traffic. Similarly, if you swap out the primary unit with new hardware, a new MAC address is used." Virtual MAC addresses guard against this disruption, because the active MAC addresses are known to the secondary unit at startup, and remain the same in the case of new primary unit hardware. If you do not configure virtual MAC addresses, you might need to clear the ARP tables on connected routers to restore traffic flow". For more details Refer - MAC Addresses and IP Addresses in Failover.

- Send ASA/FTD Logs for both the units to an external Syslog server - This step is more for the serviceability of issues.

Possible Reasons for Split-Brain

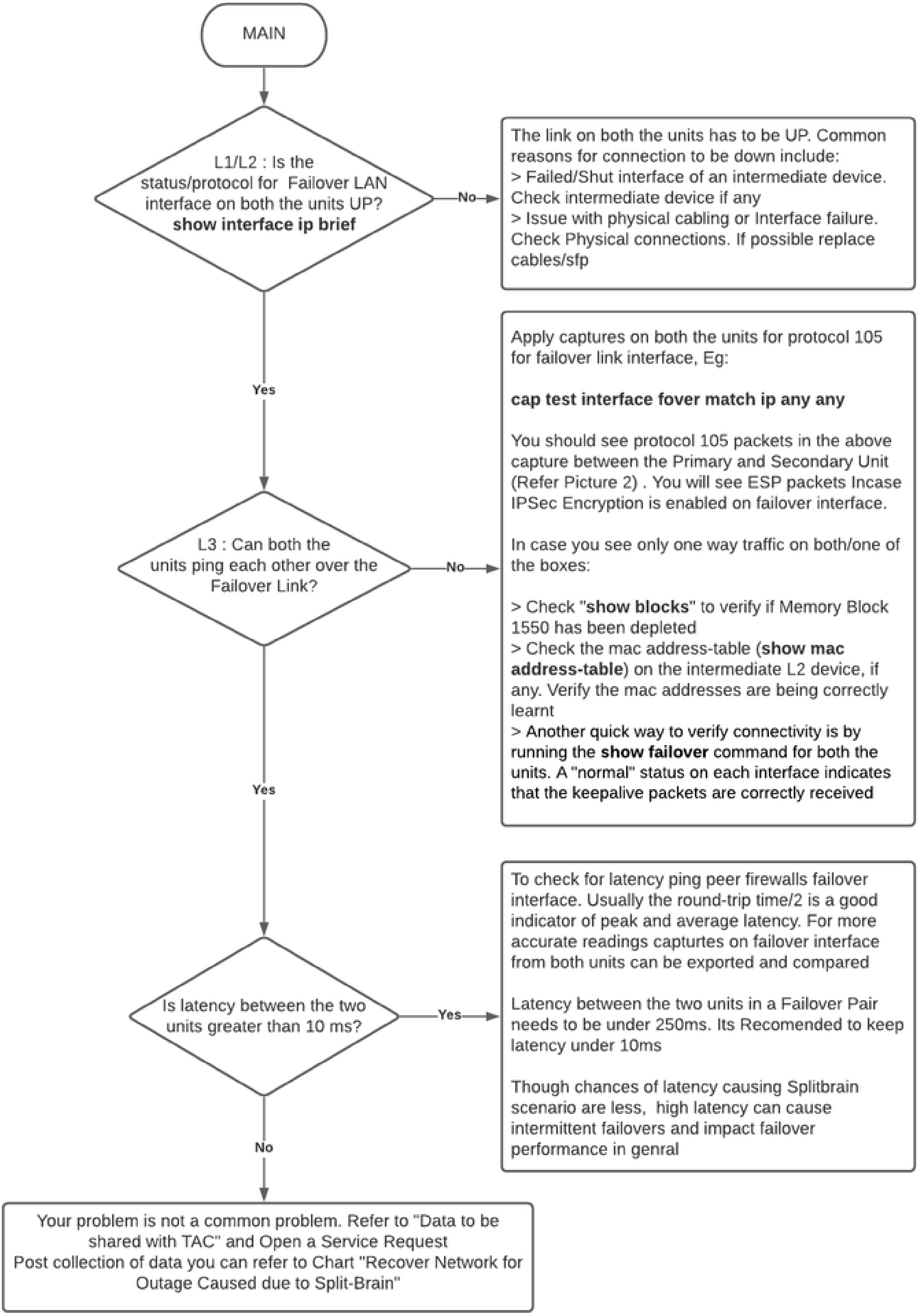
As already mentioned, split-brain occurs when the communication between the failover Link interfaces is down (unidirectionally or bidirectionally). The most common reasons are:

- L1 Issues – Faulty Cable/SFP/Interface
- An issue on an intermediate device
- Lack of Memory or CPU Resources on ASA/FTD **Note:** The ASA/Lina Engine utilize1550 byte memory blocks to store packets for processing. If the no of free blocks of this size depletes the ASA/FTD will no longer be able to process failover packets. Run the **show blocks** to check for block depletion.

Procedure to Troubleshoot - Flowchart

In order to troubleshoot and resolve a split-brain Scenario, use this flowchart, start at the box marked **Main**. There are some problems that might not be resolvable here. In these cases, links are provided to Cisco Technical Support. In order to open a service request, you must have a valid service contract.

> **Note:** In FTD Deployments, the steps in this chart must be followed from “**system support diagnostics-cli**”.



L1/L2 : Is the status/protocol for Failover LAN interface on both the units UP? **show interface ip brief**

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

L3 : Can both the units ping each other over the Failover Link?

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

Is latency between the two units greater than 10 ms?

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

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"

Troubleshooting Flow Chart

Emergency Recovery from Split-Brain

To recover your network from a split-brain you need to ensure that traffic hits only one of the two firewalls, that is, the MAC addresses learnt for the Active IPs should all point to a single unit. To do this, you can disable failover on the unit or cut it off the network entirely.

1. Disable Failover on the unit not passing traffic: On ASA Platform, over CLI, navigate to the configuration terminal and enter **no failover** command.On FTD Platform, over Clish mode, enter **configure high-availability suspend** command.
2. For ASA, shut the data interfaces. For FTD, shut the interfaces on the connected device. Alternatively, you can also physically disconnect the interfaces. Also, you can power off the device, but this will limit you from managing the device. Refer to your device config guide on the steps to do this.

   Note: If you notice connectivity issues even after you perform the mentioned step(s), it's likely that the connected device(s) have stale arp entries. Check arp entries on upstream and downstream devices. To fix the issue you may either flush these or force the working ASA/FTD to send a garp packet for the interface IP that has the issue. To do this, run command in enable mode (for FTD in System supports diagnostics-cli) - **debug menu ipaddrutl 6 <interface ip address>**.

   Caution: In case you open a support ticket with TAC for Split-brain related issues, please share the information mentioned under section **Data to be Collected for TAC Service Request** in this document.

Data to be Shared with TAC

Please share mentioned data in case you need to open a TAC Service Request.

1. Topology diagram that shows ASA/FTD-HA and its physical connections with neighbouring devices (Including Failover Interfaces).
2. Output for **show tech-support** on ASA or Troubleshooting File on Platforms running FTD.
3. Syslogs along with timestamps for +/- 5 minutes when the issue occurred.
4. FXOS Troubleshooting files, if the hardware is an FPR appliance.

To generate Troubleshooting Files for FTD or FXOS, please refer to Firepower Troubleshoot File Generation Procedures. Open a TAC SR.