Secure Firewall FTD High Availability Sync Interface Check Failure

Contents

Issue

The FTD in a High Availability (HA) pair was consistently showing in a **Failed** state. Configuration synchronization was not completing between the HA peers, despite successful IP connectivity between the units. The deployment was a new implementation running Cisco Secure Firewall Threat Defense software, not yet in production.

The issue appeared after the Primary unit was moved to its final location and its management IP address was changed without first breaking the HA pair. The HA process detected failed interface checks on monitored data interfaces, which triggered the HA state evaluation logic to place the Primary unit into a Failed role.

Environment

- Secure Firewall FTD HA managed by FMC
- New deployment of a migration activity, not yet in production

Resolution

The resolution involved removing selected data interfaces from the HA interface monitoring configuration to prevent false failure detection.

Troubleshooting Steps Performed

1: The troubleshooting data confirmed HA interface check failures on the monitored data interfaces, while HA peer connectivity (heartbeat and ping) remained functional.

<#root>

```
device# show failover
Failover On
Failover unit Primary
Failover LAN Interface: FailOver Ethernet1/8 (up)
Reconnect timeout 0:00:00
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 5 of 776 maximum
MAC Address Move Notification Interval not set
failover replication http
Version: Ours 9.20(2)121, Mate 9.20(2)121
Serial Number: Ours SERIAL#, Mate SERIAL#
Last Failover at: 17:14:25 UTC Mar 16 2026


This host: Primary - Failed

        Active time: 0 (sec)
        slot 0: FPR-1120 hw/sw rev (2.0/9.20(2)121) status (Up Sys)


Interface To-DC1-ACC (0.0.0.0): No Link (Waiting)
          Interface To-DC1-WAN (0.0.0.0): No Link (Waiting)


          Interface management (203.0.113.131/fe80::a610:b6ff:fe3d:e101): Normal (Monitored)
        slot 1: snort rev (1.0)  status (up)
        slot 2: diskstatus rev (1.0)  status (up)
    Other host: Secondary - Active
        Active time: 184688 (sec)


Interface To-DC1-ACC (0.0.0.0): No Link (Waiting)


          Interface To-DC1-WAN (10.230.2.2): Normal (Waiting)
          Interface management (203.0.113.130/fe80::6ae5:9eff:fee6:d681): Normal (Monitored)
        slot 1: snort rev (1.0)  status (up)
        slot 2: diskstatus rev (1.0)  status (up)
```

2: Confirmed that HA state transitions were occurring based on interface monitoring results, not management-plane connectivity issues.

<#root>

```
device# show failover history
17:16:51 UTC Mar 16 2026
Standby Ready

Failed                    Interface check



This host:2
                                                    single_vf: To-DC1-ACC
```

```
single_vf: To-DC1-WAN

Other host:1
single_vf: To-DC1-ACC
```

Configuration Changes

1: The HA configuration was updated to exclude the affected data interfaces from interface health monitoring, preventing false failure detection.

2: After the configuration changes, the Primary FTD successfully transitioned to **Standby Ready** status, confirming proper HA synchronization and state stability.

3: HA failover testing was successfully completed with expected results, validating the stability of the HA configuration after the changes.

Expected Behavior Clarifications

These behaviors observed during troubleshooting are expected and by design:

- Duplicate hostnames on FTD peers: Both units displaying the same hostname is expected behavior in FTD HA, as the Active unit hostname is presented system-wide (tracked under enhancement request CSCwe31354)
- IP address ownership: Only the Active FTD displays active IP addresses on data interfaces, which is expected behavior by design to prevent split-brain conditions. If no interface standby IP addresses are configured, the Standby Ready FTD appears as having no IP addresses configured on its interfaces.

Cause

The Primary FTD was marked as Failed due to High Availability interface health check failures on monitored data interfaces, causing the peer with more operational interfaces to remain Active. This behavior is by design in FTD High Availability and is documented in Cisco Secure Firewall HA guidelines. The HA process detected failed interface checks on monitored data interfaces, which triggered the HA state evaluation logic to place the Primary unit into a Failed role.

Related Content

- Cisco Secure Firewall Device Manager Configuration Guide – High Availability (Failover)
- Cisco Technical Support & Downloads