

セキュアファイアウォールFTD高可用性同期インターフェイスチェックの失敗

内容

お問い合わせ内容

ハイアベイラビリティ(HA)ペアのFTDは、常に障害状態で表示されていました。ユニット間のIP接続が成功したにもかかわらず、HAペア間で設定の同期が完了しませんでした。この導入は、まだ実稼働していないCisco Secure Firewall Threat Defenseソフトウェアを実行する新しい実装でした。

この問題は、プライマリユニットを最終的な場所に移動し、最初にHAペアを解除せずに管理IPアドレスを変更した後に発生しました。HAプロセスが、モニタ対象のデータインターフェイスで失敗したインターフェイスチェックを検出しました。これにより、HA状態評価ロジックがトリガーされ、プライマリユニットが失敗ロールに配置されました。

環境

- FMCで管理されるセキュアファイアウォールFTD HA
- 移行アクティビティの新規導入 (まだ実稼働環境に導入されていない)

解決策

この問題を解決するには、誤った障害の検出を防ぐために、選択したデータインターフェイスをHAインターフェイスモニタリング設定から削除する必要がありました。

実施されたトラブルシューティング手順

1: トラブルシューティングデータにより、監視対象のデータインターフェイスでHAインターフェイスチェックの障害が確認されましたが、HAピア接続 (ハートビートおよびping) は機能し続けました。

<#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: HA状態の遷移が、管理プレーンの接続の問題ではなく、インターフェイスの監視結果に基づいて発生していることを確認しました。

<#root>

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


原因

プライマリFTDは、監視対象のデータインターフェイスでのハイアベイラビリティインターフェイスヘルスチェックの障害により、障害が発生したとマークされ、その結果、ピアでは動作しているインターフェイスの数が増え、アクティブのままになっています。この動作はFTD High Availabilityで設計されており、Cisco Secure Firewall HAのガイドラインに記載されています。HAプロセスが、モニタ対象のデータインターフェイスで失敗したインターフェイスチェックを検出しました。これにより、HA状態評価ロジックがトリガーされ、プライマリユニットが失敗ロールに配置されました。

関連コンテンツ

- [Cisco Secure Firewall Device Managerコンフィギュレーションガイド - ハイアベイラビリティ \(フェールオーバー\)](#)
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。