2026年9月にASAまたはFTDを強化リリースにアップグレードした後のVPNロードバランシングクラスタ形成障害のトラブルシューティング

内容

- 問題
- 環境
- 解決方法
  - オプション1：アップグレードの完了（推奨）
  - オプション2：ヒットレスアップグレード方式（ASAのみ）
  - 確認手順
- 原因
- 関連コンテンツ

問題

Cisco ASAまたはFTDデバイスを、2026年9月の強化リリースの一部として公開されているバージョンのいずれかにアップグレードすると、VPNロードバランシング(VPN LB)クラスタの形成に失敗します。デバッグ出力に示されるように、デバイスで接続障害が繰り返し発生します。

```
device# debug vpnlb 125
debug vpnlb enabled at level 125
device# 5718045: Created peer[198.51.100.1]
5718012: Sent HELLO request to [198.51.100.1]
5718061: Inbound socket read fail: context=0.
7718036: Process timeout for req-type[13], exid[304], peer[198.51.100.1]
6718038: Slave processed 1 timeouts
5718028: Send OOS indicator failure to [198.51.100.1]
```

```
5718056: Deleted Master peer, IP 198.51.100.1
5718044: Deleted peer[198.51.100.1]
7718017: Got timeout for unknown peer[198.51.100.1] msg type[25]
```

クラスタ暗号化が無効になっている場合、VPN負荷分散クラスタは正常に形成されます。ただし、暗号化を再度有効にすると、クラスタの形成が失敗し、設定が完了してもIKEv1デバッグメッセージは表示されません。

この問題が影響するのは、クラスタ内のメンバ間の調整だけです。リモートアクセスVPNクライアントセッションはドロップされません。影響を受けるクラスタメンバは、アップグレードされるまでVPNロードバランシングに参加しません。

環境

- Cisco Secure Firewall ASAまたはFTD
- 強化版リリースの修正を含むASAまたはFTDソフトウェアのバージョン:2026年9月
- クラスタ暗号化を有効にしたVPNロードバランシング設定
- クラスタ通信用に構成されたIKEv1ポリシー

解決方法

この問題を解決するには、次の2つの検証済みオプションを使用できます。

オプション1：アップグレードの完了（推奨）

すべてのクラスタメンバーを同じASAまたはFTDソフトウェアバージョンにアップグレードします。すべてのメンバーが同じリリースを実行すると、クラスタは自動的に改革されます。

すべてのクラスタメンバがアップグレードされるまで、古いバージョンを実行しているメンバは、新しいバージョンを実行しているメンバと同期していません。

手順1：すべてのクラスタメンバーの現在のソフトウェアバージョンを確認します。

```
device# show version
```

ステップ2：残りのクラスタメンバーを同じASAまたはFTDソフトウェアバージョンにアップグレードします。

手順3：すべてのアップグレードが完了した後で、クラスタの構成を確認します。

```
device# show vpn load-balancing
```

オプション2：ヒットレスアップグレード方式（ASAのみ）

アップグレードプロセス中にすべてのメンバーのクラスターキーを一時的に削除し、すべてのデバイスのアップグレード後に再適用します。

ステップ1：すべてのクラスタメンバーからクラスタキーを削除します。

```
device(config)# vpn load-balancing
device(config-load-balancing)# no cluster key
```

手順2：すべてのクラスタメンバーを同じASAソフトウェアバージョンにアップグレードします。

ステップ3：アップグレード完了後にすべてのメンバーでクラスタキーを再適用します。

```
device(config)# vpn load-balancing
device(config-load-balancing)# cluster key your-cluster-key
```

重要：クラスタ暗号化だけを削除するだけでは不十分です。アップグレードプロセス中にクラスタキーを完全に削除する必要があります。

FMCによって管理されるFTDデバイスには暗号化が必須であるため、この回避策はFTDデバイス

には適用されません。

確認手順

いずれかのオプションを実装した後、クラスタが適切に動作することを確認します。

手順1：すべてのクラスタメンバーの現在のソフトウェアバージョンを確認します。

```
device# show version
```

手順2：すべてのアップグレードが完了した後でクラスタが形成されたことを確認します。

```
device# show vpn load-balancing
```

手順3：ピア接続を確認します。

```
device# debug vpnlb 125
```

ステップ4：暗号化が有効になっている場合は、IKEv1 SAが確立されていることを確認します。

```
device# show crypto ikev1 sa
```

「Cisco Bug ID CSCww64385」を確認してください。 この問題は、トポロジの可視性と再コンバージェンス時間に影響しますが、アップグレードされたデバイス上のアクティブなVPN接続やトラフィック転送には影響しません。

原因

この問題は、VPNロードバランシングクラスタのメンバ間通信に認証を追加するセキュリティ強

化機能が原因で発生します。拡張セキュリティプロトコルは以前のASAまたはFTDバージョンと互換性がないため、複数バージョンの導入でクラスタを形成できません。その結果、プロトコルの非互換性が発生し、次のような問題が発生します。

- アップグレードされたノードは認証済みv5プロトコルを適用
- アップグレード前のノードは非認証v4プロトコルを使用
- アップグレードされたメンバには、古いメンバが通信できない強化されたプロトコルが必要です
- すべてのメンバが同じプロトコルバージョンを使用するまで、クラスタの形成は失敗します

関連コンテンツ

- 『Cisco Bug ID CSCww64385』
- 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。