Troubleshoot VPN Load Balancing Cluster Formation Failure after ASA or FTD Upgrade to Hardening Release September 2026

Contents

- Issue
- Environment
- Resolution
  - Option 1: Complete Upgrade (Recommended)
  - Option 2: Hitless Upgrade Method (ASA-only)
  - Verification Steps
- Cause
- Related Content

Issue

After upgrading Cisco ASA or FTD devices to one of the versions published as part of the Hardening Release September 2026, VPN Load Balancing (VPN LB) clusters fail to form. The devices experience repeated connection failures, as shown in the debug output:

```
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]
```

When cluster encryption is disabled, the VPN Load Balancing cluster forms successfully. However, re-enabling encryption causes cluster formation to fail, and no IKEv1 debug messages are displayed despite the configuration being complete.

This issue affects only inter-member coordination within the cluster; remote-access VPN client sessions are not dropped. The affected cluster member does not participate in VPN Load Balancing until it is upgraded.

Environment

- Cisco Secure Firewall ASA or FTD
- ASA or FTD Software version containing fix for Hardening Release: September 2026
- VPN Load Balancing configuration with cluster encryption enabled
- IKEv1 policies configured for cluster communication

Resolution

Two validated options are available to resolve this issue:

Option 1: Complete Upgrade (Recommended)

Upgrade all cluster members to the same ASA or FTD software version. The cluster automatically reforms once all members are running the same release.

Until all cluster members are upgraded, members running older versions remain out of sync with those running newer versions.

Step 1: Verify current software versions on all cluster members:

```
device# show version
```

Step 2: Upgrade remaining cluster members to the same ASA or FTD software version.

Step 3: Verify cluster formation after all upgrades are complete:

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

Option 2: Hitless Upgrade Method (ASA-only)

Temporarily remove the cluster key on all members during the upgrade process, then reapply it after all devices are upgraded.

Step 1: Remove the cluster key from all cluster members:

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

Step 2: Upgrade all cluster members to the same ASA software version.

Step 3: Reapply the cluster key on all members after upgrade completion:

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

Important: Simply removing cluster encryption alone is not sufficient - **the cluster key must be completely removed during the upgrade process.**

This workaround does not apply to FTD devices because encryption is mandatory for FTD devices managed by FMC.

Verification Steps

After implementing either option, verify proper cluster operation.

Step 1: Verify the current software versions on all cluster members:

```
device# show version
```

Step 2: Verify that the cluster has formed after all upgrades are complete:

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

Step 3: Verify peer connectivity:

```
device# debug vpnlb 125
```

Step 4: Confirm that the IKEv1 SAs are established, if encryption is enabled:

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

Be aware of 'Cisco bug ID CSCww64385'. This issue affects topology visibility and re-convergence time but does not affect active VPN connections or traffic forwarding on upgraded devices.

Cause

This issue is caused by a security hardening enhancement that adds authentication to VPN Load Balancing cluster inter-member communication. The enhanced security protocol is incompatible with earlier ASA or FTD versions, preventing cluster formation in mixed-version deployments. This results in a protocol incompatibility in which:

- Upgraded nodes enforce authenticated v5 protocol
- Pre-upgrade nodes use unauthenticated v4 protocol
- The upgraded members require the hardened protocol that older members cannot communicate with
- Cluster formation fails until all members use the same protocol version

Related Content

- 'Cisco bug ID CSCww64385'
- Cisco Technical Support & Downloads