在ASA或FTD升级到强化版本2026年9月后，排除VPN负载平衡集群形成故障

目录

- 问题
- 环境
- 分辨率
  - 选项 1：完成升级（推荐）
  - 选项 2：无中断升级方法（仅限ASA）
  - 验证步骤
- 原因
- 相关内容

问题

将Cisco ASA或FTD设备升级到Hardening Release 2026中发布的一个版本后，无法形成VPN负载平衡(VPN LB)集群。设备反复出现连接故障，如调试输出所示：

```
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]
```

当禁用集群加密时，VPN负载平衡集群成功形成。但是，重新启用加密会导致集群形成失败，并且即使配置已完成，也不会显示IKEv1调试消息。

这个问题只影响组群内的成员间协调；不会丢弃远程访问VPN客户端会话。在升级之前，受影响的集群成员不会参与VPN负载均衡。

环境

- 思科安全防火墙ASA或FTD
- ASA或FTD软件版本，包含针对强化版本的修复程序：2026年9月
- 启用了集群加密的VPN负载均衡配置
- 为集群通信配置的IKEv1策略

分辨率

有两个经过验证的选项可用于解决此问题：

选项 1：完成升级（推荐）

将所有集群成员升级到相同的ASA或FTD软件版本。所有成员运行同一版本后，集群将自动进行改革。

在升级所有集群成员之前，运行旧版本的成员与运行新版本的成员保持不同步。

步骤 1：验证所有集群成员上的当前软件版本：

```
device# show version
```

步骤 2：将剩余集群成员升级到相同的ASA或FTD软件版本。

步骤 3：完成所有升级后验证集群的形成：

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

选项 2：无中断升级方法（仅限ASA）

在升级过程中暂时删除所有成员上的集群密钥，然后在升级所有设备后重新应用该密钥。

步骤 1：从所有集群成员中删除集群密钥：

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

步骤 2：将所有集群成员升级到相同的ASA软件版本。

步骤 3：升级完成后，在所有成员上重新应用群集密钥：

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

重要信息：仅删除群集加密是不够的 — 在升级过程中必须完全删除群集密钥。

此解决方法不适用于FTD设备，因为加密对于FMC管理的FTD设备是必需的。

验证步骤

在实施任一选项后，验证集群操作是否正确。

步骤 1：验证所有集群成员上的当前软件版本：

```
device# show version
```

步骤 2：验证所有升级完成后已形成集群：

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

步骤 3：验证对等连接：

```
device# debug vpnlb 125
```

步骤 4：如果加密已启用，请确认已建立IKEv1 SA:

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

请注意“Cisco bug ID CSCww64385”(Cisco bug ID CSCww64385)。 此问题会影响拓扑可见性和重新收敛时间，但不会影响已升级设备上的活动VPN连接或流量转发。

原因

此问题是由安全强化增强引起的，该增强将身份验证添加到VPN负载平衡集群成员间通信。增强的安全协议与早期的ASA或FTD版本不兼容，从而阻止在混合版本部署中形成集群。这会导致协议不兼容，其中：

- 升级的节点实施经过身份验证的v5协议
- 预升级节点使用未经身份验证的v4协议
- 已升级的成员需要老成员无法与之通信的强化协议
- 集群建立失败，直到所有成员使用相同的协议版本

相关内容

- 'Cisco Bug ID CSCww64385'
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。