Fehlerbehebung bei Cluster-Formationsfehlern mit VPN-Lastenausgleich nach ASA- oder FTD-Upgrade auf die Härtungsversion September 2026

Inhalt

- Problem
- Umwelt
- Auflösung
  - Option 1: Vollständiges Upgrade (empfohlen)
  - Option 2: Upgrade-Methode bei laufendem Betrieb (nur ASA)
  - Verifizierungsschritte
- Ursache
- Verwandte Inhalte

Problem

Nach dem Upgrade von Cisco ASA- oder FTD-Geräten auf eine der Versionen, die im Härtungsbericht vom September 2026 veröffentlicht wurden, bilden sich keine VPN Load Balancing (VPN LB)-Cluster mehr. Bei den Geräten treten wiederholt Verbindungsfehler auf, wie in der Debug-Ausgabe gezeigt:

```
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]
```

Wenn die Clusterverschlüsselung deaktiviert ist, wird der VPN-Lastenausgleichs-Cluster erfolgreich erstellt. Die erneute Aktivierung der Verschlüsselung führt jedoch zu einem Fehler bei der Clusterbildung, und trotz abgeschlossener Konfiguration werden keine IKEv1-Debugmeldungen angezeigt.

Dieses Problem betrifft nur die Koordinierung zwischen den Mitgliedern innerhalb des Clusters. VPN-Clientsitzungen mit Remotezugriff werden nicht verworfen. Das betroffene Clustermitglied nimmt erst am VPN-Lastenausgleich teil, wenn ein Upgrade durchgeführt wurde.

Umwelt

- Cisco Secure Firewall ASA oder FTD
- ASA- oder FTD-Softwareversion mit Fix für Härtungsfreigabe: September 2026
- Konfiguration für VPN-Lastenausgleich mit aktivierter Cluster-Verschlüsselung
- IKEv1-Richtlinien für die Cluster-Kommunikation konfiguriert

Auflösung

Zur Behebung dieses Problems stehen zwei validierte Optionen zur Verfügung:

Option 1: Vollständiges Upgrade (empfohlen)

Aktualisieren Sie alle Cluster-Mitglieder auf dieselbe ASA- oder FTD-Softwareversion. Der Cluster wird automatisch reformiert, sobald alle Mitglieder dieselbe Version ausführen.

Bis zum Upgrade aller Cluster-Mitglieder bleiben Mitglieder mit älteren Versionen nicht mit den Mitgliedern mit neueren Versionen synchronisiert.

Schritt 1: Überprüfen Sie die aktuellen Softwareversionen aller Cluster-Elemente:

```
device# show version
```

Phase 2: Aktualisieren Sie die verbleibenden Cluster-Mitglieder auf dieselbe ASA- oder FTD-Softwareversion.

Schritt 3: Überprüfen Sie die Clusterbildung nach Abschluss aller Upgrades:

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

Option 2: Upgrade-Methode bei laufendem Betrieb (nur ASA)

Entfernen Sie während des Upgradevorgangs vorübergehend den Clusterschlüssel für alle Mitglieder, und wenden Sie ihn nach dem Upgrade aller Geräte erneut an.

Schritt 1: Entfernen Sie den Clusterschlüssel von allen Clustermitgliedern:

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

Phase 2: Aktualisieren Sie alle Cluster-Mitglieder auf dieselbe ASA-Softwareversion.

Schritt 3: Clusterschlüssel nach Abschluss des Upgrades erneut auf alle Mitglieder anwenden:

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

Wichtig: Die Cluster-Verschlüsselung allein zu entfernen, reicht nicht aus - der Cluster-Schlüssel

muss während des Upgrade-Vorgangs vollständig entfernt werden.

Diese Problemumgehung gilt nicht für FTD-Geräte, da die Verschlüsselung für von FMC verwaltete FTD-Geräte obligatorisch ist.

Verifizierungsschritte

Überprüfen Sie nach dem Implementieren einer der beiden Optionen den ordnungsgemäßen Clusterbetrieb.

Schritt 1: Überprüfen Sie die aktuellen Softwareversionen aller Cluster-Elemente:

```
device# show version
```

Phase 2: Stellen Sie sicher, dass sich der Cluster gebildet hat, nachdem alle Upgrades abgeschlossen sind:

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

Schritt 3: Überprüfen der Peer-Verbindung:

```
device# debug vpnlb 125
```

Schritt 4: Bestätigen Sie, dass die IKEv1-SAs eingerichtet sind, wenn die Verschlüsselung aktiviert ist:

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

Beachten Sie die Bug-ID "Cisco CSCww64385". Dieses Problem beeinflusst die Transparenz der Topologie und die Zeit für die erneute Konvergenz, jedoch nicht die aktiven VPN-Verbindungen oder die Datenweiterleitung auf aktualisierten Geräten.

Ursache

Dieses Problem wird durch eine Verbesserung der Sicherheitsabsicherung verursacht, die die Kommunikation zwischen den Mitgliedern des VPN-Lastenausgleichs-Clusters um Authentifizierung erweitert. Das erweiterte Sicherheitsprotokoll ist nicht mit früheren ASA- oder FTD-Versionen kompatibel und verhindert die Clusterbildung in Bereitstellungen mit gemischten Versionen. Dies führt zu einer Protokollinkompatibilität, bei der:

- Aktualisierte Knoten setzen authentifiziertes v5-Protokoll durch
- Pre-Upgrade-Knoten verwenden nicht authentifiziertes v4-Protokoll
- Die aktualisierten Mitglieder erfordern ein robustes Protokoll, mit dem ältere Mitglieder nicht kommunizieren können.
- Cluster-Erstellung schlägt fehl, bis alle Mitglieder dieselbe Protokollversion verwenden

Verwandte Inhalte

- 'Cisco Bug-ID CSCww64385'
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.