

Problemen oplossen met de vorming van een VPN-taakverdelingscluster na ASA- of FTD-upgrade naar Hardening-release september 2026

Inhoud

[uitgifte](#)

[milieu](#)

[resolutie](#)

[Optie 1: Volledige upgrade \(aanbevolen\)](#)

[Optie 2: Hitless Upgrade-methode \(alleen ASA\)](#)

[Verificatiestappen](#)

[Oorzaak](#)

[Gerelateerde inhoud](#)

- [uitgifte](#)
 - [milieu](#)
 - [resolutie](#)
 - [Optie 1: Volledige upgrade \(aanbevolen\)](#)
 - [Optie 2: Hitless Upgrade-methode \(alleen ASA\)](#)
 - [Verificatiestappen](#)
 - [Oorzaak](#)
 - [Gerelateerde inhoud](#)
-

uitgifte

Na het upgraden van Cisco ASA- of FTD-apparaten naar een van de versies die zijn gepubliceerd als onderdeel van de [Hardening Release september 2026](#), ontstaan er geen VPN Load Balancing (VPN LB)-clusters. De apparaten ondervinden herhaaldelijk verbindingfouten, zoals wordt weergegeven in de debug-uitgang:

```
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]
```

Wanneer clustercodering is uitgeschakeld, wordt het VPN-cluster voor taakverdeling met succes gevormd. Als u de codering echter opnieuw inschakelt, mislukt de clustervorming en worden er geen IKEv1-foutopsporingsberichten weergegeven, hoewel de configuratie is voltooid.

Dit probleem heeft alleen invloed op de coördinatie tussen de leden binnen het cluster; VPN-clientsessies met externe toegang worden niet gedropt. Het betreffende clusterlid neemt niet deel aan VPN Load Balancing totdat het is geüpgraded.

milieu

- Cisco Secure Firewall ASA of FTD
- ASA- of FTD-softwareversie met fix voor [Hardening Release: september 2026](#)
- VPN-configuratie voor taakverdeling met clustercodering ingeschakeld
- IKEv1-beleid geconfigureerd voor clustercommunicatie

resolutie

Er zijn twee gevalideerde opties beschikbaar om dit probleem op te lossen:

Optie 1: Volledige upgrade (aanbevolen)

Upgrade alle clusterleden naar dezelfde ASA- of FTD-softwareversie. Het cluster wordt automatisch hervormd zodra alle leden dezelfde release uitvoeren.

Totdat alle clusterleden zijn geüpgraded, blijven leden met oudere versies niet gesynchroniseerd

met leden met nieuwere versies.

Stap 1: Controleer de huidige softwareversies op alle clusterleden:

```
device# show version
```

Stap 2: Upgrade resterende clusterleden naar dezelfde ASA- of FTD-softwareversie.

Stap 3: Controleer de clustervorming nadat alle upgrades zijn voltooid:

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

Optie 2: Hitless Upgrade-methode (alleen ASA)

Verwijder de clustersleutel tijdelijk van alle leden tijdens het upgradeproces en pas deze opnieuw toe nadat alle apparaten zijn bijgewerkt.

Stap 1: Verwijder de clustersleutel van alle clusterleden:

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

Stap 2: Upgrade alle clusterleden naar dezelfde ASA-softwareversie.

Stap 3: Pas de clustersleutel opnieuw toe op alle leden nadat de upgrade is voltooid:

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

Belangrijk: clustercodering alleen verwijderen is niet voldoende - de clustersleutel moet tijdens het upgradeproces volledig worden verwijderd.

Deze tijdelijke oplossing is niet van toepassing op FTD-apparaten omdat codering verplicht is voor FTD-apparaten die door FMC worden beheerd.

Verificatiestappen

Controleer na het implementeren van een van beide opties of de clusterbewerking correct is.

Stap 1: Controleer de huidige softwareversies op alle clusterleden:

```
device# show version
```

Stap 2: Controleer of het cluster is gevormd nadat alle upgrades zijn voltooid:

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

Stap 3: Verifieer de peer-connectiviteit:

```
device# debug vpn1b 125
```

Stap 4: Bevestig dat de IKEv1 SA's zijn ingesteld als de codering is ingeschakeld:

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

Denk hierbij aan de Cisco bug ID [CSCww64385](#). Dit probleem heeft invloed op de zichtbaarheid van de topologie en de tijd voor het opnieuw convergeren, maar heeft geen invloed op actieve VPN-verbindingen of het doorsturen van verkeer op geüpgradede apparaten.

Oorzaak

Dit probleem wordt veroorzaakt door een verbetering van de beveiliging die authenticatie toevoegt aan de communicatie tussen de leden van het VPN Load Balancing-cluster. Het verbeterde beveiligingsprotocol is niet compatibel met eerdere ASA- of FTD-versies, waardoor clustervorming bij implementaties met gemengde versies wordt voorkomen. Dit resulteert in een protocol incompatibiliteit waarbij:

- Geüpgradede knooppunten dwingen geverifieerd v5-protocol af
- Knooppunten vóór de upgrade gebruiken niet-geverifieerd v4-protocol
- De geüpgradede leden hebben het geharde protocol nodig waarmee oudere leden niet kunnen communiceren
- Clustervorming mislukt totdat alle leden dezelfde protocolversie gebruiken

Gerelateerde inhoud

- 'Cisco bug ID [CSCww64385](#)'
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.