ASA 또는 FTD 업그레이드 후 발생한 VPN 부하 균형 클러스터 형성 실패 문제를 해결하여 릴리스 강화 2026년 9월

목차

- 문제
- 환경
- 해결
  - 옵션 1: 업그레이드 완료(권장)
  - 옵션 2: 히트리스 업그레이드 방법(ASA 전용)
  - 확인 단계
- 원인
- 관련 콘텐츠

문제

Cisco ASA 또는 FTD 디바이스를 2026년 9월 Hardening Release의 일부로 게시된 버전 중 하나로 업그레이드한 후, VPN LB(VPN Load Balancing) 클러스터가 생성되지 않습니다. 디버그 출력에 표시된 것처럼 디바이스에서 연결 실패가 반복됩니다.

```
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]
```

클러스터 암호화가 비활성화되면 VPN 로드 밸런싱 클러스터가 성공적으로 형성됩니다. 그러나 암호화를 다시 활성화하면 클러스터 형성이 실패하고 컨피그레이션이 완료되어도 IKEv1 디버그 메시지가 표시되지 않습니다.

이 문제는 클러스터 내의 멤버 간 조정에만 영향을 미칩니다. 원격 액세스 VPN 클라이언트 세션은 삭제되지 않습니다. 영향을 받는 클러스터 멤버는 업그레이드될 때까지 VPN 부하 균형에 참여하지 않습니다.

환경

- Cisco Secure Firewall ASA 또는 FTD
- Hardening Release용 픽스가 포함된 ASA 또는 FTD 소프트웨어 버전: 2026년 9월
- 클러스터 암호화가 활성화된 VPN 로드 밸런싱 컨피그레이션
- 클러스터 통신에 대해 구성된 IKEv1 정책

해결

이 문제를 해결하기 위해 두 가지 검증된 옵션을 사용할 수 있습니다.

옵션 1: 업그레이드 완료(권장)

모든 클러스터 멤버를 동일한 ASA 또는 FTD 소프트웨어 버전으로 업그레이드합니다. 모든 멤버가 동일한 릴리스를 실행하면 클러스터가 자동으로 개혁됩니다.

모든 클러스터 멤버가 업그레이드될 때까지 이전 버전을 실행 중인 멤버는 최신 버전을 실행 중인 멤버와 동기화되지 않습니다.

1단계: 모든 클러스터 멤버의 현재 소프트웨어 버전 확인:

```
device# show version
```

2단계: 나머지 클러스터 멤버를 동일한 ASA 또는 FTD 소프트웨어 버전으로 업그레이드합니다.

3단계: 모든 업그레이드가 완료된 후 클러스터 형성 확인:

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

옵션 2: 히트리스 업그레이드 방법(ASA 전용)

업그레이드 프로세스 중에 모든 멤버의 클러스터 키를 일시적으로 제거한 다음 모든 디바이스가 업그레이드된 후 다시 적용합니다.

1단계: 모든 클러스터 멤버에서 클러스터 키를 제거합니다.

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

2단계: 모든 클러스터 멤버를 동일한 ASA 소프트웨어 버전으로 업그레이드합니다.

3단계: 업그레이드 완료 후 모든 멤버에 클러스터 키를 다시 적용합니다.

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

중요: 클러스터 암호화만 제거하는 것만으로는 충분하지 않습니다. 업그레이드 프로세스 중에 클러스터 키를 완전히 제거해야 합니다.

FMC에서 관리하는 FTD 디바이스에는 암호화가 필수이므로 이 해결 방법은 FTD 디바이스에는 적용되지 않습니다.

확인 단계

두 옵션 중 하나를 구현한 후 적절한 클러스터 작동을 확인합니다.

1단계: 모든 클러스터 멤버의 현재 소프트웨어 버전을 확인합니다.

```
device# show version
```

2단계: 모든 업그레이드가 완료된 후 클러스터가 구성되었는지 확인합니다.

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

3단계: 피어 연결 확인:

```
device# debug vpnlb 125
```

4단계: 암호화가 활성화된 경우 IKEv1 SA가 설정되었는지 확인합니다.

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

'Cisco 버그 ID CSCww64385'에 유의하십시오. 이 문제는 토폴로지 가시성 및 재통합 시간에 영향을 미치지만, 업그레이드된 디바이스의 활성 VPN 연결 또는 트래픽 포워딩에는 영향을 미치지 않습니다.

원인

이 문제는 VPN 부하 균형 클러스터 구성원 간 통신에 인증을 추가하는 보안 강화 기능 향상으로 인해 발생합니다. 향상된 보안 프로토콜은 이전 ASA 또는 FTD 버전과 호환되지 않으므로 혼합 버전 구축에서 클러스터를 구성할 수 없습니다. 이렇게 하면 다음과 같은 프로토콜 비호환성이 발생합니다.

- 업그레이드된 노드에서 인증된 v5 프로토콜 적용
- 업그레이드 전 노드에서 인증되지 않은 v4 프로토콜 사용
- 업그레이드된 멤버에는 이전 멤버와 통신할 수 없는 강화된 프로토콜이 필요합니다
- 모든 멤버가 동일한 프로토콜 버전을 사용할 때까지 클러스터 형성이 실패합니다

관련 콘텐츠

- 'Cisco 버그 ID CSCww64385'
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.