ASA에서 FTD로 방화벽 마이그레이션 후 ISE(Identity Services Engine) 3.3 상태 검증 실패

목차

문제

보고된 문제는 "알 수 없음" 상태 규정 준수 상태에 남아 있는 끝점으로 나타날 수 있습니다. 또한 사용자에게 상태 프로비저닝 포털을 표시할 수 없습니다.

일부 시나리오에서 고객은 ASA에서 FTD로 마이그레이션한 후 동일한 컨피그레이션을 재사용한다고 보고했습니다. 그러나 FTD가 올바르게 작동하려면 Posture VPN에 대한 추가 및 특정 설정이 필요합니다.

환경

- Cisco ISE(Identity Services Engine) 버전 3.3
- 두 개의 노드가 있는 ISE 구축
- Cisco Secure Client 버전 5.1.7.80
- FTD(firepower Threat Defense) 버전 7.4.1.1
- VPN을 통해 연결되는 엔드포인트
- 보안 상태 검증에 필요한 관련 IP 주소: 72.163.1.80(enroll.cisco.com)

해결

이 단계에서는 FTD로 마이그레이션한 후 ISE 보안 상태 검증 문제를 식별, 진단 및 해결하기 위한 워크플로에 대해 자세히 설명합니다. 각 단계는 환경에서 관찰된 로그 및 컨피그레이션 지표를 직접 참조하여 명확성을 위해 설명합니다.

1단계: 프로브 확인을 위한 DART 번들 수집

VPN 연결을 시도하는 엔드포인트의 상태 상태에 오류 또는 중단된 상태가 있는지 확인합니다. ISE 상태 에이전트 로그(ISPosture.txt)에서 잘못된 서버 서버 서버 또는 다시 연결할 수 없는 상태를 나타내는 오류 메시지를 검토합니다.

문제를 나타내는 로그 발췌 예:

2026/01/05 15:38:26 [경고] csc_iseagent 함수: 대상::parsePostureStatusResponse 스레드 ID: 0x32D0 파일: Target.cpp 줄: 370 수준: 경고 헤드엔드가 비어 있습니다. 콘텐츠가 'X-ISE-PDP' 형식이 아닐 수 있습니다.

2026/01/05 15:38:26 [정보] csc_iseagent 함수: 대상::프로브 스레드 ID: 0x32D0 파일: 대상.cpp 줄:

212 수준: 리디렉션 대상 192.168.1.254의 디버그 상태가 5 <잘못된 서버.> 입니다.

2026/01/05 15:38:28 [정보] csc_iseagent 함수: SwiftHttpRunner::http_discovery_callback 스레드 ID: 0x1AD8 파일: SwiftHttpRunner.cpp 줄: 519 수준
: info Time out for Redirection target enroll.cisco.com.

2026/01/05 15:38:28 [정보] csc_iseagent 함수: SwiftHttpRunner::http_discovery_callback 스레드 ID: 0x1AD8 파일: SwiftHttpRunner.cpp 줄: 580 수준: 정보 다음 라운드 타이머를 사용하도록 설정합니다.

2026/01/05 15:38:28 [정보] csc_iseagent 함수: GetCurrentUserName 스레드 ID: 0x1AD8 파일: ImpersonateUser.cpp 줄: 60 수준: 정보 현재 로그인한 사용자의 사용자 이름은 basheer.mohamed입니다.

2026/01/05 15:38:29 [정보] csc_iseagent 함수: hs_transport_winhttp_get 스레드 ID: 0x698C 파일: hs_transport_winhttp.c 라인: 4912 수준: debug 요청이 시간 초과되었습니다.

2026/01/05 15:38:29 [정보] csc_iseagent 함수: 대상::probeDiscoveryUrl 스레드 ID: 0x698C 파일: Target.cpp 줄: 269 수준: debug GET request to URL (http://enroll.cisco.com/auth/discovery?architecture=9), returned status -1 <Operation Failed.>.

2026/01/05 15:38:29 [정보] csc_iseagent 함수: 대상::프로브 스레드 ID: 0x698C 파일: 대상.cpp 줄: 212 수준: 리디렉션 대상 enroll.cisco.com의 디버그 상태가 6 <연결 불가.> 입니다.

이 경우 enroll.cisco.com에 연결할 수 없으므로 검색 프로세스가 실패합니다.

2단계: ISE 권한 부여 프로파일 및 라이브 로그 확인

RADIUS LiveLog가 끝점에 올바르게 푸시되었는지 확인하십시오. 상태 검증을 위해 액세스 수락 및 URL 리디렉션 매개 변수를 포함해야 합니다.

예:

액세스 유형 = ACCESS_ACCEPT

cisco av 쌍 = url redirect acl=redirect

cisco av 쌍 = url-redirect=https://ip:port/portal/gateway?sessionId=SessionIdValue&portal=4cb1f740-e371-11e6-92ce-005056873bd0&action=cpp

이 특정 예에서는 리디렉션이 예상대로 작동하지만 게이트웨이가 잘못된 서버로 보고되어 검색 프로세스가 실패합니다. 엔드포인트가 검색을 위해 VPN 게이트웨이에 의존하지 않기 때문에 VPN 통합 시나리오에서 이 동작을 예상할 수 있습니다. 대신
the endpoint attempts to reach the ISE node using enroll.cisco.com.

3단계. FTD에서 ACL 설정 확인

스플릿 터널에 대해 구성된 ACL은 물론 리디렉션 ACL에서 enroll.cisco.com이 명시적으로 허용되

는지 확인합니다.

두 ACL을 모두 확인하려면 FMC에서 Object(개체) > Object Management(개체 관리) > Access List(액세스 목록) > Extended(확장)로 이동할 수 있습니다.

스플릿 터널이 VPN에 구성되어 있는지 확인하려면 Devices(디바이스) > VPN > Remote Access(원격 액세스) > Choose the VPN and Connection Profile settings(VPN 및 연결 프로파일 설정) > Edit Group Policy(그룹 정책 수정) > Split Tunnel(스플릿 터널)로 이동합니다.

참고: VPN 정책에 스플릿 터널이 구성되지 않은 경우 이 검증이 필요하지 않으므로 이 시나리오에서는 스플릿 터널 ACL이 필요하지 않습니다.

원인

문제의 근본 원인은 FTD(Firepower Threat Defense)로 마이그레이션한 후 네트워크 정책에 필요한 검색 IP 주소(72.163.1.80, enroll.cisco.com)가 없기 때문입니다.

이 IP가 없으면 Cisco Secure Client가 VPN을 통해 연결할 때 ISE 정책 서비스 노드를 검색할 수 없으므로 포스처 상태가 보류 중 상태로 유지됩니다. 또한 엔드포인트에서 비활성화된 위치 서비스가 완료되지 않은 포스처 검증의 원인이 되었습니다.

관련 콘텐츠

- Cisco 지원

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.