보안 클라이언트 Umbrella 모듈 디바이스 등록 중 SSL/TLS 신뢰 실패

목차

문제

Umbrella 모듈로 Cisco Secure Client를 롤아웃하는 동안 디바이스가 대시보드와의 동기화를 중지하고 "비활성"으로 보고되었습니다. 영향을 받는 클라이언트에서 devices.api.sse.cisco.com에 등록을 시도할 때 SSL/TLS 트러스트 오류가 발생하여 디바이스 등록 및 보호 커버리지가 올바르게 이루어지지 않았습니다.

UI에서 다음 상태 메시지와 함께 Umbrella가 비활성 상태로 표시됩니다.

- Umbrella가 비활성 상태입니다.
- 현재 보안 웹 게이트웨이로 보호되어 있지 않습니다.
- 보안 웹 게이트웨이가 라이센스가 없거나 비활성화되어 있습니다.

진단 결과, 등록 중에 Secure Client 로그에 다음과 같은 오류 메시지가 나타나는 일관된 SSL/TLS Trust Failure가 발견되었습니다.

```
[ERROR] < 10> Device Registration: Registration failed against https://devices.api.sse.cisco.com/deploy
```

환경

- 2,000개 이상의 엔드포인트에 Umbrella 모듈을 구축한 Cisco Secure Client
- 경로 정책을 사용하는 SD-WAN 인프라
- 기존 Umbrella 터널

- Cisco 설명서당 필요한 모든 대상을 허용하는 네트워크 구성
- 경계에 있는 Cisco 대상에 대해 활성화된 SSL 암호 해독 없음

해결

이 해결책에는 디바이스 등록 트래픽이 레거시 Umbrella 터널을 통해 잘못 전달되도록 한 라우팅 컨피그레이션 문제를 식별하고 수정하는 작업이 포함되었습니다.

근본 원인 식별

패킷 캡처 데이터를 분석한 결과, API 연결을 위해 제공된 TLS 인증서가 예상 Cisco Secure Access/Let's Encrypt 인증서가 아닌 Cisco Umbrella 인증서인 것으로 나타났습니다. devices.api.sse.cisco.com의 IP 주소를 식별합니다.

추가 조사를 통해 146.112.0.0/16 서브넷과 일치하는 SD-WAN 경로 정책이 확인되었으며, 이로 인해 devices.api.sse.cisco.com으로 가는 트래픽이 의도한 대상 대신 레거시 Umbrella 터널로 라우팅되었습니다.

구성 변경

이 문제를 해결하기 위해 다음 단계를 수행했습니다.

- 1단계: 문제가 있는 고정 경로를 제거합니다. 레거시 Umbrella 터널에 146.112.0.0/16을 가리키는 고정 경로가 SD-WAN 컨피그레이션에서 제거되었습니다.
- 2단계: 연결을 확인합니다. 고정 경로를 제거한 후 영향을 받는 클라이언트가 devices.api.sse.cisco.com에 성공적으로 연결 및 등록할 수 있는지 테스트했습니다.

확인

devices.api.sse.cisco.com에 대한 예상 인증서 체인은 다음과 같이 표시되어야 합니다.

```
openssl s_client -connect devices.api.sse.cisco.com:443
CONNECTED(00000003)
depth=2 C = US, O = Internet Security Research Group, CN = ISRG Root X1
verify return:1
depth=1 C = US, O = Let's Encrypt, CN = R13
verify return:1
depth=0 CN = api.sse.cisco.com
verify return:1
---
Certificate chain
 0 s:CN = api.sse.cisco.com
   i:C = US, O = Let's Encrypt, CN = R13
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Mar  5 14:13:56 2026 GMT; NotAfter: Jun  3 14:13:55 2026 GMT
 1 s:C = US, O = Let's Encrypt, CN = R13
   i:C = US, O = Internet Security Research Group, CN = ISRG Root X1
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Mar 13 00:00:00 2024 GMT; NotAfter: Mar 12 23:59:59 2027 GMT
```

컨피그레이션 변경을 구현한 후 영향을 받는 클라이언트가 성공적으로 연결 및 등록되고 구축이 성공적으로 완료되었습니다.

원인

근본 원인은 146.112.0.0/16 서브넷과 일치하는 SD-WAN 경로 정책으로 인해 devices.api.sse.cisco.com(146.112.59.104)으로 향하는 디바이스 등록 트래픽이 레거시 Umbrella 터널을 통해 잘못 라우팅되었습니다. 이로 인해 잘못된 TLS 인증서(예상 Cisco Secure Access/Let's Encrypt 인증서 대신 Cisco Umbrella 인증서)가 표시되었으며, 이는 디바이스 등록 프로세스 중 SSL/TLS 트러스트 실패로 이어집니다.

관련 콘텐츠

- Cisco Secure Client 네트워크 요구 사항 설명서
- 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.