

ZTA 브라우저 기반 프라이빗 리소스 TLS 핸드셰이크 실패

목차

문제

사용자는 Cisco Secure Access를 통해 브라우저 기반 프라이빗 리소스에 액세스할 수 없습니다.

연결을 시도할 때 다음과 같은 증상이 발생합니다.

- TCP 3방향 핸드셰이크가 성공적으로 완료되지만 클라이언트 Hello 이후 TLS 협상이 실패합니다.
- 공용 SSE 매핑된 URL(<https://example-orgid.ztna.sse.cisco.io>)에 대한 연결이 Cisco 인증에 도달하지만 HTTP 404 오류를 반환합니다.
- FQDN을 프라이빗 리소스 컨피그레이션에 추가한 후, 트래픽은 인증 프롬프트로 리디렉션되지만 인증 후에는 빈 페이지가 됩니다.
- HAR 파일은 HTTP 200 응답을 표시하지만 TLS 핸드셰이크가 완료되지 않습니다.
- 차단 이유는 다음과 같습니다. "개인 액세스: 디바이스에 대해 가져온 상태 데이터가 너무 오래되었습니다. 새로 고쳐야 합니다."

환경

- Cisco SSE(Secure Access)
- 보안 액세스 조직 ID: xxxx자
- 브라우저 기반 ZTNA(Zero Trust Network Access)
- 개인 리소스: example.net을 참조하십시오.
- 비교를 위한 작업 전용 리소스: abc.net을 참조하십시오.

- 와일드카드 인증서 컨피그레이션

해결

프라이빗 리소스가 작동하는 프라이빗 리소스와 동일한 인증서 컨피그레이션을 사용하도록 구성하여 문제를 해결했습니다.

다음 섹션에서 설명하는 단계를 수행했습니다.

1단계: 작업 구성 분석

오류가 발생한 전용 리소스(example.net)를 작업 중인 전용 리소스(abc.net)와 비교하여 컨피그레이션의 차이점을 확인합니다.

사용된 작업 리소스:

- Use a URL in your domain(도메인의 URL 사용) 옵션
- 기존 와일드카드 인증서/키 쌍에 대한 참조

2단계: 패킷 캡처 분석

Wireshark를 사용하여 패킷 캡처 분석을 수행하여 TLS 핸드셰이크 실패를 확인합니다.

- TCP 3-way 핸드셰이크가 성공적으로 완료되는지 확인합니다.
- Client Hello 후 TLS 협상이 실패하는지 확인합니다.
- 진단 아티팩트 수집: HAR 파일, DART 번들 및 패킷 캡처.

3단계: 인증서 확인

RAVPN 연결을 통해 애플리케이션에 액세스하여 인증서 표시를 확인합니다.

- 웹 사이트 example.net에서 와일드카드 인증서를 제공하고 있는지 확인합니다.
- 컨피그레이션 참조를 위해 인증서 세부 정보를 문서화합니다.

4단계: 프라이빗 리소스 구성

작업 중인 전용 리소스에서 사용하는 것과 동일한 컨피그레이션 접근 방식을 적용합니다.

- Use a URL in your domain(도메인에서 URL 사용) 옵션을 사용하도록 프라이빗 리소스를 구성합니다.
- 기존 와일드카드 인증서/키 쌍을 참조합니다.
- FQDN이 프라이빗 리소스 필드에 올바르게 구성되어 있는지 확인하십시오.

5단계: 검증

브라우저 기반 액세스를 테스트하여 컨피그레이션에서 문제를 해결하는지 확인합니다.

- TLS 핸드셰이크가 성공적으로 완료되었는지 확인합니다.
- 적절한 인증 흐름을 확인합니다.
- 인증 후 응용 프로그램 액세스 가능성을 확인합니다.

원인

근본 원인은 프라이빗 리소스 설정의 컨피그레이션 불일치입니다. 오류가 발생한 개인 리소스가 대상 응용 프로그램에서 제공하는 와일드카드 인증서를 제대로 참조하도록 구성되지 않았습니다. 프라이빗 리소스 구성이 애플리케이션 서버에서 사용하는 인증서 구성과 일치하지 않아 TLS 핸드셰이크가 실패했습니다. Use a URL in your domain(도메인에서 URL 사용) 옵션을 사용하도록 프라이빗 리소스를 구성하고 기존 와일드카드 인증서/키 쌍(작업 컨피그레이션과 일치)을 참조하여 TLS 협상을 성공적으로 완료할 수 있습니다.

관련 콘텐츠

- [보안 액세스를 위한 Cisco 참조 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.