

보안 액세스에서 SSL 암호 해독 인증서 오류 처리

목차

문제

Cisco Secure Access에서 SSL 암호 해독이 활성화된 경우 사용자에게 인증서 관련 오류 페이지가 표시됩니다. 세 가지 특정 유형의 인증서 오류에 대해 여러 가지 문의가 접수되었습니다.

- 원본 서버 인증서 만료 오류
- 인증서에 나열된 일반 이름 또는 주체 대체 이름이 액세스한 도메인과 일치하지 않는 경우 인증서 CN/SAN 불일치 오류
- 원본 서버 인증서에 포함된 CRL(Certificate Revocation List) 링크로 인해 연결 문제가 발생했습니다.

이러한 인증서 오류는 일반적으로 웹 브라우저에 표시되는 경고와 비슷합니다. Cisco Secure Access에서 경고 페이지(브라우저 또는 콘텐츠 필터와 유사)를 표시한 다음 경고를 표시한 후 액세스를 허용하거나 모든 경우에 액세스를 허용하여 인증서 관련 오류를 처리할 수 있는지 여부가 문제입니다. 또한, SSL 해독이 비활성화될 때의 동작 및 인증서 문제와 상관없이 트래픽이 통과하는지 여부를 이해해야 합니다.

환경

- Cisco Secure Access - 인터넷 액세스(로밍 모듈, VA, DNS, SWG, PAC, IPS, 인증서)
- SSL 암호 해독 기능 활성화됨
- 여러 도메인에서 인증서 유효성 검사 문제가 발생했습니다.
- 만료 및 도메인 불일치를 비롯한 다양한 인증서 문제가 있는 오리진 서버

해결

인증서 오류 처리 제한

인증서 관련 오류 처리는 Cisco Secure Access에서 사용할 수 없습니다. 이 제품에서는 다음을 지원하지 않습니다.

- 인증서 문제에 대한 브라우저와 유사한 경고 페이지 제공
- 도메인별 인증서 오류 처리 컨피그레이션
- 대상 도메인을 기반으로 한 사용자 지정 오류 처리
- 사용자 재정의 옵션이 있는 콘텐츠 필터 스타일 경고 페이지

SSL 암호 해독 제외 해결 방법

권장 방법은 보안 프로파일 암호 해독 설정을 사용하여 SSL 암호 해독에서 문제가 있는 도메인을 제외하는 것입니다. 다음을 통해 구성할 수 있습니다.

SSL 검사에서 특정 도메인을 제외하려면 Security Profile(보안 프로파일) > Decryption Settings(해독 설정) 섹션으로 이동합니다.

도메인이 SSL 해독에서 제외되면 다음 동작이 발생합니다.

- 제외된 도메인에 대한 트래픽은 SSL 검사를 완전히 우회합니다
- 보안 액세스에서 인증서 유효성 검사를 수행하지 않음
- 보안 액세스로 생성된 인증서 오류 페이지가 사용자에게 표시되지 않음
- 인증서 문제가 지속되면 원래 인증서 오류가 사용자 브라우저에 계속 표시될 수 있습니다

SSL 암호 해독 사용 안 함 동작

도메인 또는 전역적으로 SSL 해독이 비활성화되면 Cisco Secure Access는 인증서 문제와 상관없이 트래픽을 전달(전달)합니다. 이 제품은 암호 해독이 활성화되지 않은 경우 인증서를 검사하거나 검증하지 않으므로 모든 HTTPS 트래픽이 투명하게 통과하도록 효과적으로 허용합니다.

원인

인증서 오류는 만료된 인증서, CN/SAN 불일치, CRL 연결 문제 등 원본 서버의 합법적인 인증서 검증 문제로 인해 발생합니다. Cisco Secure Access는 SSL 암호 해독 프로세스의 일부로 인증서 검증을 수행하며, 이러한 검증 실패가 발생하면 제품에서 잠재적으로 안전하지 않은 연결을 방지하는 오류 페이지를 생성합니다. 이는 SSL 검사 기능의 의도된 보안 동작입니다.

관련 콘텐츠

- [Cisco Secure Access Decryption 컨피그레이션 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.