

보안 액세스에서 SSL 인증서 및 핸드셰이크 오류 이해

목차

문제

인증서 및 TLS 오류로 인해 차단된 HTTP 트래픽을 이제 Dashboard Activity Search(대시보드 활동 검색)에서 볼 수 있습니다. 이 문서에서는 일반적인 오류 메시지의 목록과 각 오류에 대한 간단한 설명을 제공합니다.

환경

- Cisco Secure Access — 보안 웹 게이트웨이 SSL 검사

해결

업스트림 인증서가 만료됨

웹 사이트의 인증서가 만료 날짜를 경과했으므로 Cisco Secure Access에서 인증서를 신뢰하지 않습니다. 이 것은 웹사이트 소유자에게 수정하도록 되어 있으니, 해당 사이트의 웹마스터에게 연락하여 알려주십시오.

업스트림 인증서 자체 서명

웹 사이트는 신뢰할 수 있는 인증 기관에서 발급한 인증서가 아니라 직접 서명한 인증서를 제공함

니다. Cisco Secure Access는 독립적인 인증 기관이 없기 때문에 인증서가 정품인지 확인할 방법이 없습니다.

소규모 내부 사용자를 위한 리소스에서 자체 서명 인증서를 자주 볼 수 있습니다. IT 보안 어플라이언스의 관리 포털이 대표적인 예입니다. 자체 서명 인증서를 신뢰하도록 Cisco Secure Access를 설정할 수 없다는 점에 유의하십시오.

중간 인증서 누락

Cisco Secure Access는 필요한 모든 중간 인증서를 수집할 수 없으므로 루트로 다시 완전한 신뢰 체인을 구축할 수 없습니다.

이것이 중요한 이유이다: 웹 사이트의 인증서("리프")는 중간 인증서에 의해 서명되며, 이는 다시 다른 중간 인증서에 의해 서명될 수 있으며, 이를 통해 신뢰할 수 있는 루트까지 서명될 수 있습니다. 이 체인이 체크 아웃하려면 웹 사이트는 중간 인증서와 함께 자체 인증서를 보내야 합니다. 이러한 정보가 누락되면 유효성 검사가 중단되므로 사이트의 웹 마스터에게 알립니다.

한 가지 예외가 있습니다. 인증서에 "AIA(Authority Information Access)" 확장이 포함된 경우 Cisco Secure Access는 누락된 중간체를 자체적으로 가져오려고 시도할 수 있습니다. HTTPS 암호 해독 및 파일 검사가 모두 켜져 있을 때만 작동합니다.

업스트림 인증서에 주체 이름 누락

인증서에는 주체 이름(Distinguished Name) 또는 주체 대체 이름(Subject Alternative Name)이 포함되지 않습니다. 즉, 인증서가 속한 사용자를 명확하게 식별하는 것이 없습니다. 이 기능이 없으면 Cisco Secure Access에서 이를 검증할 수 없습니다. 이것은 웹사이트 소유자가 수정해야 할 사항입니다.

업스트림 인증서에 공통 이름 누락

인증서에는 CN(Common Name)이 없습니다. 이 필드는 일반적으로 사이트의 호스트 이름을 가지고 있으며 방문하는 사이트에 실제로 속한 인증서임을 확인하는 데 도움이 됩니다. 요즘에는 이 검사가 SAN(주체 대체 이름)에 따라 달라지며 CN이 레거시 필드로 간주되지만 이 필드가 없으면 오류가 발생할 수 있습니다. 웹 마스터에게 연락하여 문제를 해결하십시오.

업스트림 인증서를 신뢰할 수 없음

Cisco Secure Access는 일반적으로 인증서를 발급한 루트 CA를 인식하지 못하므로 이 인증서를 신뢰하지 않습니다.

Cisco Secure Access SWG는 신뢰할 수 있는 루트 인증 기관의 내장형 목록을 신뢰할 수 있는 제공자로부터 소싱하여 최신 상태로 유지합니다. 사이트의 인증서가 해당 목록에 없는 CA로 다시 추적되면 검증이 실패합니다. Root CA가 신뢰할 수 있는 솔루션이라고 확인하는 경우 기술 지원에 문의하면 Cisco에서 확인할 수 있습니다.

인증서의 호스트 이름이 예상과 다릅니다.

요청한 주소가 인증서의 이름과 일치하지 않습니다. 해당 CN(Common Name)과 SAN(Subject Alternative Name)이 일치하지 않습니다. 인증서가 도달하려는 사이트에 속하지 않는 것으로 나타나므로 Cisco Secure Access는 이 요청에 대해 인증서를 신뢰하지 않습니다. 웹 마스터가 이 문제를 해결해야 합니다.

업스트림 인증서가 해지됨

이 인증서를 발급한 인증 기관이 인증서를 취소했습니다. 다시 말해, 더 이상 유효한 인증서로 간주되지 않습니다.

Cisco Secure Access는 인증서가 폐기되었는지 실시간으로 확인하는 OSCP(Online Certificate Status Protocol)를 사용하여 이를 확인합니다. 사이트 웹 마스터에게 알려 해당 웹 사이트를 대체할 수 있도록 합니다.

TLS 핸드셰이크 오류

지원되지 않는 업스트림 암호

웹 사이트에서 Cisco Secure Access SWG가 사용하는 암호 그룹을 지원하지 않으므로 TLS 핸드셰

이크를 완료할 수 없습니다. 이는 더 약한 암호만 제공하는 오래된 서버 또는 오래된 서버와 함께 나타나는 경향이 있습니다. 수정사항은 서버측에 있으니 웹마스터에게 전달하세요.

업스트림 TLS 버전 불일치

웹 사이트에서 Cisco Secure Access SWG가 지원하는 TLS 버전을 사용하고 있지 않으므로 핸드셰이크에 실패했습니다. 현재 Cisco Secure Access SWG 프록시는 클라이언트에서 들어오는 연결 및 대상 서버로 나가는 연결 모두에 대해 TLS 1.2 및 TLS 1.3에서 작동합니다.

1024비트 미만의 업스트림 DH 키

웹 사이트에서 Cisco Secure Access가 수락하기에 너무 약한(1024비트 미만) Diffie-Hellman 키를 사용하고 있으므로 핸드셰이크를 완료할 수 없습니다. 이는 서버측 한계이므로 웹마스터가 이를 강화할 필요가 있다.

해결 방법

Cisco Secure Access에서 컨피그레이션을 변경하여 이러한 문제를 해결할 수 있습니다.

이 작업은 서버와 인증서의 신뢰성을 신뢰하는 경우에만 수행해야 합니다.

"선택적 암호 해독 목록" 항목을 사용하여 암호 해독을 비활성화하거나, "외부 도메인" 항목을 사용하여 Cisco Secure Access의 트래픽을 완전히 우회할 수 있습니다. 암호 해독이 비활성화되면 Cisco Secure Access는 인증서 검증을 수행하지 않습니다.

대부분의 경우 트래픽이 Cisco Secure Access에서 우회될 때 브라우저가 여전히 오류 또는 경고를 표시합니다. 웹 브라우저는 유사한 인증서 검증을 수행합니다.

원인

Cisco Secure Access SSL 검사 프록시에서 TLS 핸드셰이크를 완료할 수 없습니다. 가장 일반적인

이유는 대상이 CSA 재서명된 인증서를 거부하는 인증서 피닝을 사용하기 때문입니다.

- 인증서 피닝: 클라이언트 하드 코드에는 인증서 지문이 필요합니다.
- 엔드포인트에서 CSA CA를 신뢰할 수 없음: 검사 CA 인증서가 트러스트된 루트 저장소에 배포되지 않았습니다.

관련 콘텐츠

- [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.