일반 인증서 및 TLS 프로토콜 오류 이해

목차

소개

이 문서에서는 Umbrella Dashboard Activity Search의 일반 인증서 및 TLS 프로토콜 오류에 대해 설명합니다.

개요

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

인증서 오류

업스트림 인증서가 만료됨

웹 사이트에서 제공한 인증서가 만료되었습니다. 이 문제를 보고하려면 사이트의 웹 마스터에게 문의하십시오.

업스트림 인증서 자체 서명

웹 사이트에서 제공하는 서버 인증서는 인증 기관에서 서명하지 않았으므로 Umbrella에서 인증서

를 신뢰할 수 있는지 확인할 수 없습니다.

자체 서명 인증서는 서버가 제한된 대상을 위한 리소스를 호스트할 때 사용되는 경우가 있습니다. 예를 들어 IT 보안 어플라이언스의 웹 포털은 자체 서명 인증서를 사용하는 것이 기본값입니다. 자체 서명 인증서를 신뢰하도록 Umbrella를 구성할 수 없습니다.

중간 인증서 누락

Umbrella가 모든 중간 기관의 인증서를 가져올 수 없으므로 전체 신뢰 체인을 확인할 수 없습니다.

웹 서버 인증서는 일반적으로 인증 기관의 중간 인증서에 발급/서명됩니다. 이러한 중간 인증서는 다른 중간 인증서에서도 발급할 수 있습니다. 웹 서버 인증서("리프 인증서")와 중간 인증서는 다시 루트 인증서로 체인을 형성합니다. Umbrella가 전체 신뢰 체인을 검증하려면 웹 사이트에서 중간 인증서를 서버 인증서와 번들로 묶어야 합니다. 이 문제를 보고하려면 사이트의 웹 마스터에게 문의하십시오.

또는 인증서에 "Authority Information Access(권한 정보 액세스)" 확장이 포함된 경우 Umbrella는 자동으로 중간 CA를 가져오려고 시도합니다. Umbrella는 HTTPS 암호 해독 및 파일 검사가 활성화된 경우에만 AIA 확장을 지원합니다.

업스트림 인증서에 주체 이름이 없습니다.

인증서의 Subject(주체) 필드에 이 인증서를 식별하는 DN(Distinguished Name)이 없습니다. 이는 Certificate Authority에서 발급한 모든 인증서에 대한 요구 사항이므로 Cisco Umbrella에서 요구합니다. 이 문제를 보고하려면 사이트의 웹 마스터에게 문의하십시오.

업스트림 인증서에 공통 이름이 없습니다.

웹 사이트에서 제공하는 인증서에 Common Name이 없습니다. Umbrella SWG에 CN(Common Name) 필드가 필요합니다. 여기에는 인증서가 사용자가 요청한 리소스와 일치하는지 검증하는 데 필요한 인증서 호스트 이름이 포함됩니다(예: 브라우저에 입력한 주소). 이 문제를 보고하려면 사이트의 웹 마스터에게 문의하십시오.

업스트림 인증서를 신뢰할 수 없음

Cisco Umbrella에서 인증서를 신뢰하지 않습니다. 이 오류는 일반적으로 Cisco가 인증서를 발급한 루트 CA를 신뢰하지 않음을 의미합니다.

Umbrella SWG에는 신뢰할 수 있는 알려진 루트 인증 기관의 기본 목록이 있으며, 이 목록은 신뢰할 수 있는 소스에서 업데이트됩니다. 웹 사이트의 인증서가 이 목록의 CA에 의해 서명되지 않은 경우 인증서 검증이 실패합니다. Umbrella에 신뢰할 수 있는 루트 CA가 없다고 생각되면 기술 지원에 문의하십시오.

인증서의 호스트 이름이 예상과 다릅니다.

사용자가 요청한 리소스(예: 브라우저에 입력한 주소가 인증서의 CN(Common Name) 또는 SAN(Subject Alternative Name)과 일치하지 않으므로 Umbrella가 이 요청에 대해 인증서를 신뢰할

수 없습니다. 이 문제를 보고하려면 사이트의 웹 마스터에게 문의하십시오.

업스트림 인증서가 해지됨

웹 사이트에서 제공한 인증서가 발급 인증 기관에 의해 해지되었습니다.

Umbrella는 OCSP(Online Certificate Status Protocol) 검사를 수행하여 인증서가 나중에 CA에 의해 폐기되었는지 확인합니다. 이 문제를 보고하려면 사이트의 웹 마스터에게 문의하십시오.

TLS 핸드셰이크 오류

지원되지 않는 업스트림 암호

TLS 핸드셰이크를 완료할 수 없습니다. 이는 일반적으로 웹 사이트가 Umbrella SWG에서 사용하는 Cipher Suites의 목록을 지원하지 않음을 의미합니다. 이 오류는 더 약한 TLS 암호만 지원하는 오래된 또는 오래된 웹 서버에서 발생할 수 있습니다. 이 문제를 보고하려면 사이트의 웹 마스터에게 문의하십시오.

업스트림 TLS 버전 불일치

웹 사이트에서 Umbrella SWG가 사용하는 것과 동일한 TLS 버전을 지원하지 않으므로 TLS 핸드셰이크를 완료할 수 없습니다. 현재 Umbrella SWG Proxy는 Umbrella SWG에 대한 클라이언트 측 연결과 Umbrella SWG 프록시 연결에서 대상 웹 서버로의 TLS 1.2 및 TLS 1.3을 모두 지원합니다.

1024비트 미만의 업스트림 DH 키

웹 사이트에서 Umbrella에서 지원하지 않는 약한 Diffie-Hellman 키를 사용하므로 TLS 핸드셰이크를 완료할 수 없습니다. 이 문제를 보고하려면 사이트의 웹 마스터에게 문의하십시오.

해결 방법

Cisco Umbrella에서 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 Umbrella에서 트래픽을 완전히 우회할 수 있습니다. 암호 해독이 비활성화되면 Umbrella는 인증서 검증을 수행하지 않습니다. 대부분의 경우 트래픽이 Umbrella에서 우회될 때 브라우저가 여전히 오류 또는 경고를 나타낸다는 점에 유의하십시오. 웹 브라우저는 유사한 인증서 검증을 수행합니다.

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.