트러블슈팅 오류 "517 업스트림 인증서 취소 "

목차

소개

이 문서에서는 HTTPS URL을 찾을 때 "517 업스트림 인증서가 해지됨" 오류를 해결하는 방법에 대해 설명합니다.

문제

Umbrella SWG(Secure Web Gateway) 웹 프록시가 HTTPS 검사를 수행하도록 구성된 경우 사용자는 517 업스트림 인증서 취소 오류 페이지를 받을 수 있습니다. 이 오류는 요청된 웹 사이트가 TLS 협상에서 해당 인증서의 발급자 또는 유사한 기관에 따라 "취소됨" 상태의 디지털 인증서를 보냈음을 나타냅니다. 폐기된 인증서가 더 이상 유효하지 않습니다.

원인

Umbrella 클라이언트가 Umbrella Secure Web Gateway를 통해 HTTPS를 요청하면 SWG는 OCSP(Online Certificate Status Protocol)를 사용하여 인증서 폐기 검사를 수행합니다. OCSP는 인증서의 폐기 상태를 제공합니다. SWG는 Umbrella 클라이언트를 대신하여 OCSP에서 인증서 폐기 상태를 요청합니다.

SWG는 요청된 웹 서버 인증서의 인증서 폐기 상태 및 신뢰할 수 있는 루트 인증서 경로에서 발급하는 모든 중간 인증서를 결정합니다. 이러한 점검은 발행 이후 유효한 신뢰 체인이 유효하지 않게 된 것을 보장한다.

OCSP 해지 검사를 사용하는 디지털 인증서의 "Authority Information Access" X.509 확장에는 하나 이상의 "OCSP" 필드가 포함되어 있습니다. 필드는 인증서의 폐기 상태를 쿼리할 수 있는 OCSP "엔드포인트"(웹 서버)에 대한 HTTP URL을 포함합니다. SWG는 다음 중 하나를 나타내는 응답이 수신될 때까지 인증서의 각 OCSP URL에 요청을 합니다.

- 인증서가 유효(취소되지 않음)한 경우 SWG가 웹 요청의 진행을 허용할 때 또는
- SWG가 적절한 오류 페이지/메시지를 표시하고 웹 요청이 실패하는 경우 OCSP "certificate valid" 응답 이외의 다른 모든 응답(예: 인증서가 해지됨, 서버가 현재 시간에 응답할 수 없음, HTTP 오류 상태, 네트워크/전송 계층 시간 초과 등)

OCSP 응답은 일반적으로 캐시되며 향후 검사에 응답하는 데 사용됩니다. 캐싱 시간은 OCSP 응답에서 서버에 의해 설정됩니다.

직접 탐색 시 다른 동작

웹 클라이언트는 클라이언트에 따라 다양한 폐기 검사 메커니즘을 사용할 수 있습니다. 예를 들어 Google의 Chrome 브라우저는 기본적으로 OCSP 또는 표준 CRL 방법을 사용하지 않습니다. 대신 Chrome은 CRLet이라는 CRL의 전용 버전을 사용하는데, 이는 Secure Web Gateway에서 사용하지 않습니다. 따라서 Chrome은 인증서의 폐기 상태를 확인할 때 SWG와 동일한 결과를 생성하지 않을 수 있습니다.

그러나 CRLSet 설명서에는 "어떤 경우에는 기본 시스템 인증서 라이브러리가 크롬이 무엇을 하든지 항상 이러한 검사를 수행합니다"라고 명시되어 있습니다. 따라서 로컬 환경에 따라 OCSP 및/또는 CRL 검사는 브라우저 또는 운영 체제의 암호화 서비스 라이브러리(예: SChannel, Secure Transport 또는 NSS)에서 수행할 수 있습니다.

또한 OCSP 및 CRL 확인은 동일한 결과를 생성할 수 없다는 점에 유의하십시오.

브라우징 시 클라이언트에서 어떤 인증서 폐기 검사를 수행하는지 확인하려면 해당 브라우저 또는 운영 체제 공급업체의 설명서를 참조하십시오.

해결

유효한 인증서의 사용은 웹 서버 관리자의 책임입니다. 폐기된 인증서의 교정은 서버 관리자가 서버에서 수행해야 합니다. Cisco Umbrella는 이 프로세스를 지원할 수 없습니다.

Cisco Umbrella는 폐기된 인증서를 사용하는 웹 사이트에 액세스하는 것을 강력하게 권장합니다. 해결 방법은 사용자가 사이트에서 폐기된 인증서를 사용하는 이유를 완전히 이해하고 모든 위험을 완전히 수용하는 경우에만 사용할 수 있습니다.

오류를 방지하기 위해 사이트의 도메인 이름이 포함된 선택적 암호 해독 목록을 만들어 HTTPS 검사에서 해당 사이트를 제외할 수 있습니다. 선택적 암호 해독 목록은 사이트에 대한 액세스를 허용하는 웹 정책에 적용됩니다. 또는 SWG를 우회하여 트래픽을 사이트로 직접 전송하도록 사이트를 External Domains(외부 도메인) 목록에 추가할 수 있습니다.

추가 정보

서버의 인증서가 폐기되었는지 확인하려는 고객은 폐기 상태를 확인할 수 있도록 설계된 타사 툴을 사용할 수 있습니다. 특히 Qualys SSL Labs의 SSL Server Test 툴은 다른 인증서 유효성 정보를 제공하는 것 외에도 OCSP 및 CRL 검사를 모두 수행합니다. 이 툴은 다음 웹 사이트에서 이용할 수 있습니다.

- https://www.ssllabs.com/ssltest/analyze.html

Cisco Umbrella에서 지원 케이스를 열기 전에 이 툴을 사용하여 517 업스트림 인증서 취소 오류를 생성하는 사이트를 확인하는 것이 좋습니다.

다음 항목도 참고하십시오. https://support.umbrella.com/hc/en-us/articles/4406133198100-Certificate-and-TLS-Protocol-Errors

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.