

SWG 프록시에서 비표준 HTTPS 요청을 처리하는 방법 이해

목차

[소개](#)

[개요](#)

[일반적인 질문](#)

[SWG 프록시가 비표준 HTTPS 웹 요청을 처리할 수 있습니까?](#)

[HTTPS 검사를 사용하지 않도록 설정하거나 문제의 도메인을 선택적 암호 해독 목록에 추가할 수 있습니까?](#)

[솔루션](#)

소개

이 문서에서는 SWG 프록시가 비표준 HTTPS 요청을 처리하는 방법과 필요한 클라이언트 규정 준수에 대해 설명합니다.

개요

Umbrella는 TLS SNI 확장을 사용하여 대상 도메인을 검색하고 HTTPS 요청에 선택적 암호 해독 목록을 사용하여 암호 해독 또는 암호 해독 우회가 필요한지 여부를 결정합니다. 클라이언트는 관련 RFC에 정의된 TLS 표준을 준수해야 합니다. 대부분의 잘 알려진 브라우저는 이러한 표준을 준수하며 Umbrella는 이러한 표준을 지원합니다.

일반적인 질문

SWG 프록시가 비표준 HTTPS 웹 요청을 처리할 수 있습니까?

클라이언트가 기본 TLS 핸드셰이크를 수행하지 않으면 HTTPS 요청이 [실패합니다](#). 예를 들어 Client Hello 또는 Server Hello exchange가 없는 경우 요청을 완료할 수 없습니다.

HTTPS 검사를 사용하지 않도록 설정하거나 문제의 도메인을 선택적 암호 해독 목록에 추가할 수 있습니까?

아니요. 이러한 조치로 문제가 해결되지 않습니다.

솔루션

문제의 비표준 HTTPS 사이트에 대해 SWG 프록시를 완전히 우회해야 합니다.

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.