

Umbrella Secure Web Gateway에서 516개 오류 트러블슈팅

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[개요](#)

[516 오류 배경](#)

[Chrome 동작 변경](#)

[오류의 소스 확인](#)

[해결 방법](#)

[516 오류 및 이메일 시스템](#)

소개

이 문서에서는 Umbrella Secure Web Gateway에서 516개 오류가 증가하는 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 조건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Umbrella SWG(Secure Web Gateway)를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

HTTPS 검사를 통해 Umbrella SWG(Secure Web Gateway) 프록시를 검색하는 사용자는 2023년 10월 하반기부터 516개의 업스트림 인증서 CN 불일치 오류 페이지를 더 자주 받을 수 있습니다.

516 오류 페이지는 웹 사이트의 인증서가 클라이언트가 사이트에 액세스하는 데 사용하는 도메인 이름과 일치하지 않을 때 발생합니다.

오류 페이지의 증가는 HTTP(암호화되지 않은) 스키마를 사용하는 URL에 대한 Chrome 브라우저의 요청 처리가 변경되었기 [때문입니다](#). 이제 Chrome에서 먼저 HTTPS(암호화) 스키마로 리소스를

로드하려고 시도합니다. HTTPS 검사에 대해 [구성된 경우](#), SWG는 웹 사이트의 인증서를 검사하고 인증서가 허용되지 않는 경우 516과 같은 오류 코드를 표시하는 웹 페이지를 반환합니다.

이 문제를 해결하기 위해 고객은 516개의 오류가 발생하는 요청에 대해 HTTPS 검사를 우회하도록 웹 정책을 구성할 수 있습니다.

516 오류 배경

간단히 말해, HTTPS를 통해 웹 사이트에 액세스하는 데 사용된 도메인 이름이 서버의 디지털 인증서에 나타나지 않을 경우 Umbrella Secure Web Gateway는 516 오류 페이지를 반환합니다. Secure Web Gateway가 516 오류 페이지를 반환하는 이유에 대한 자세한 내용은 Umbrella Knowledge Base 문서 "516 Upstream Certificate CN Mismatch" 오류를 참조하십시오.

예를 들어 HTTP URL의 콘텐츠를 다음 형식으로 제공하는 사이트를 가정해 보십시오.

<http://www.example.com/path to content> 사용자가 동등한 HTTPS URL을 요청하지만 사이트에 SAN이 www.example.com과 일치하는 인증서가 없는 경우(SAN이 example.com과만 일치하는 경우), SWG의 HTTPS 검사 기능을 사용하는 웹 정책으로 Umbrella의 Secure Web Gateway에서 요청을 처리하는 경우 516 오류가 발생합니다.

Chrome 동작 변경

2023년 10월 하반기에 Google은 Chrome 브라우저를 위한 새로운 기능의 출시를 완료했습니다. 그 날짜 이후에는 HTTP URL에 대한 요청이 해당 URL의 HTTPS 버전을 사용하여 자동으로 생성됩니다. 예를 들어, 사용자가 <http://www.example.com>에 대한 요청을 하면 Chrome은 먼저 <https://www.example.com>을 사용하여 요청을 처리하려고 시도합니다.

Chrome이 HTTPS URL을 요청할 때 HTTPS 관련 오류를 수신하면 Chrome은 HTTP를 통해 동일한 콘텐츠를 로드하려고 시도합니다. HTTP URL에 대한 요청이 성공하면 Chrome은 아래 이미지에 따라 사이트가 안전하지 않음을 나타내는 텍스트와 사용자에게 계속 진행할 수 있는 옵션을 제공하는 링크가 포함된 중간 페이지를 표시합니다.



example.com doesn't support a secure connection with HTTPS

- **Attackers can see and change** information you send or receive from the site.
- **It's safest to visit this site later** if you're using a public network. There is less risk from a trusted network, like your home or work Wi-Fi.

You might also contact the site owner and suggest they upgrade to HTTPS. [Learn more about this warning](#)

Continue to site

Go back

이는 Chrome의 새로운 기능에서 나타나는 폴백 동작입니다.

그러나 HTTPS 검사를 사용하여 SWG를 통해 검색할 때 HTTPS 요청으로 사이트에서 "ERR_CERT_COMMON_NAME_INVALID"와 같은 HTTPS 관련 오류가 발생하면 SWG가 오류를 인터셉트하고 516 오류 페이지와 같은 SWG 오류 페이지를 Chrome으로 반환합니다. 이 SWG 콘텐츠는 Chrome의 HTTPS 관련 오류로 간주되지 않으므로 폴백 동작이 생성되지 않으며 이전 이미지의 페이지가 아닌 SWG 오류 페이지가 표시됩니다.

새로운 Chrome 동작에 대한 자세한 내용은 Chrome [블로그](#) 및 [기능](#)의 GitHub 리포지토리에서 [확인할 수 있습니다](#).

오류의 소스 확인

이제 Chrome은 HTTP URL을 HTTPS URL로 자동 승격하므로 516개의 오류를 생성하는 웹 사이트가 사용자에게 더 자주 표시됩니다.

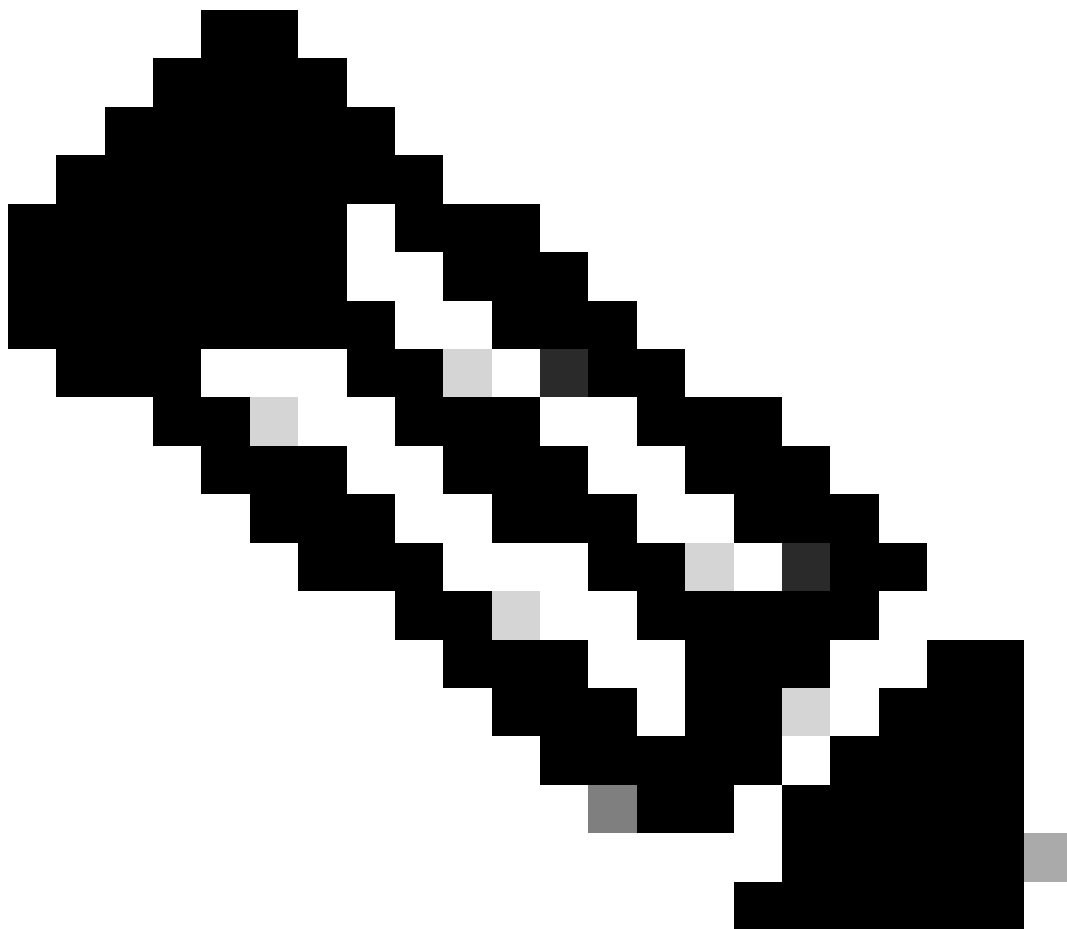
웹 사이트에서 516 응답과 같은 HTTPS 관련 오류가 발생하는지 확인하려면 Umbrella를 사용하지 않는 데스크톱 시스템에서 Chrome으로 사이트를 탐색합니다. HTTP 하이퍼링크를 클릭하는 대신 URL의 HTTPS 버전을 Chrome의 Omnibox(예: 주소 표시줄)에 직접 입력해야 합니다. 하이퍼링크가 SWG로 516 오류를 발생시킨 경우 SWG가 없는 Chrome에서 HTTPS URL을 수동으로 요청하면 "ERR_CERT_COMMON_NAME_INVALID" 오류 메시지가 나타날 수 있습니다. 이 오류 메시지는 문제가 웹 사이트에 액세스하는 데 사용된 도메인 이름에 대한 잘못된 인증서임을 확인합니다.

또는 [Qualys SSL Server Test](#) 사이트와 같은 온라인 툴을 사용하여 웹 사이트의 문제를 진단할 수 있습니다.

해결 방법

Umbrella 관리자는 다음 옵션 중 하나를 사용하여 문제를 해결할 수 있습니다.

1. 이러한 [사이트](#)에 대한 [대상](#) 목록을 만들고 HTTPS 검사 없이 [웹](#) 정책에 [추가합니다](#).
 2. 516개의 오류 페이지를 생성하는 사이트의 선택적 암호 해독 목록을 만들고 선택적 암호 해독 목록을 모든 관련 웹 정책에 추가합니다
-



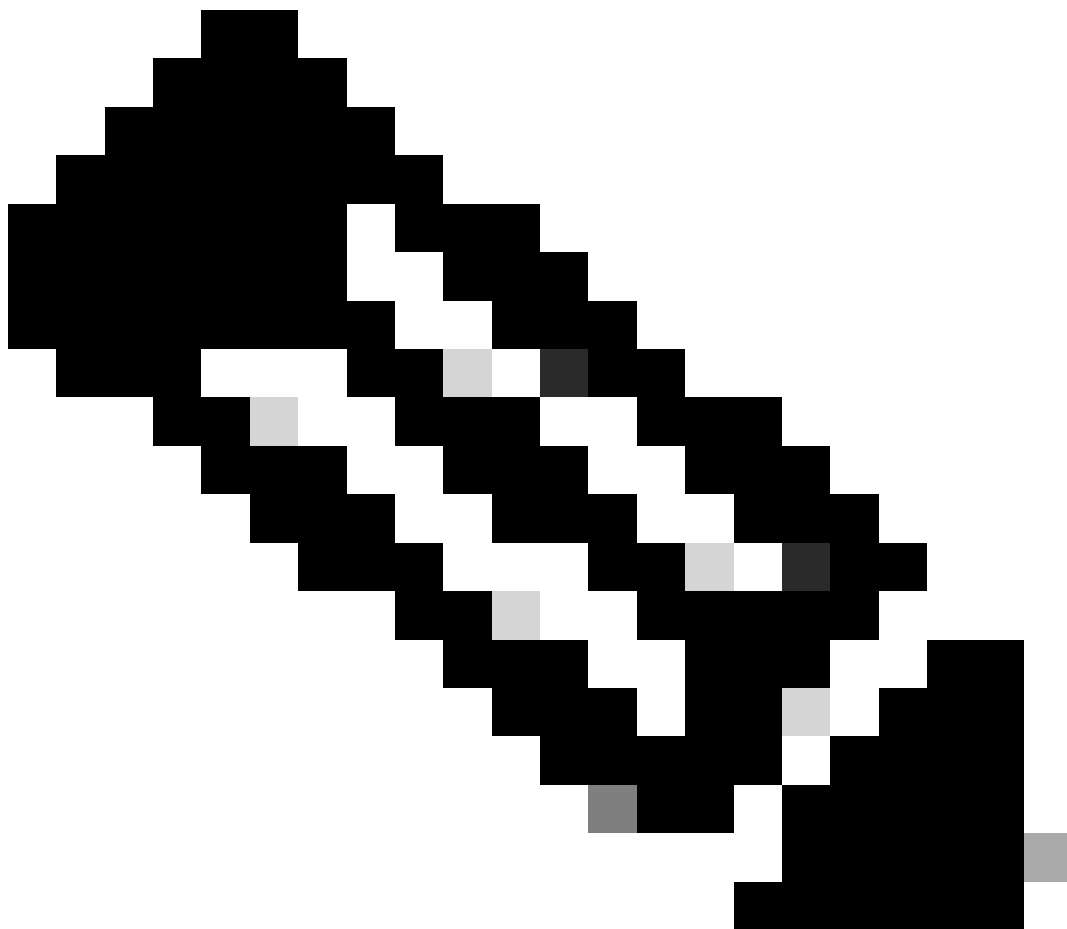
참고: 서비스의 HTTPS URL을 원래 HTTP URL로 대체하는 HTTP 리디렉션 또는 이메일 보안 시스템과 같은 요소는 필요한 도메인 이름을 모호하게 할 수 있습니다. 대상 목록 또는 선택적 암호 해독 목록의 올바른 도메인 이름을 식별하려면 특정 도구(curl, Chrome Developer Tools, 이메일 보안 벤더의 로그 등)를 사용하는 등 조사가 필요할 수 있습니다.

516 오류 및 이메일 시스템

516 오류 빈도의 증가는 이메일을 HTML 형식으로 표시하고 이메일의 하이퍼링크를 허용하는 이메일 시스템에서 발생할 수 있습니다. 이메일을 작성할 때 발신자가 도메인 이름을 입력하거나 이메일 본문에 붙여넣으면 많은 이메일 시스템에서 자동으로 일반 텍스트 도메인 이름을 하이퍼링크로 승격합니다. 일반적으로 링크가 생성되면 스키마는 HTTPS가 아닌 HTTP입니다.

예를 들어, 이메일에 `example.com` 문자열을 입력하면 HTML 코드 `<a href="http://www.example.com">`가 포함된 이메일이 나타날 수 있습니다. 이 코드는 하이퍼링크 `www.example.com`으로 표시됩니다.

이러한 이메일의 수신자가 해당 HTTP 하이퍼링크를 클릭하는 경우, 클릭이 Chrome을 열거나 Chrome이 이미 이메일을 보는 데 사용되고 있는 경우 요청이 처음에 HTTPS를 사용합니다.



참고: 다른 브라우저에서는 HTTP를 HTTPS로 승격할 수도 있습니다.

또한 HTTP 체계를 의도적으로 사용하는 이메일의 하이퍼링크도 비슷하게 처리됩니다.

일부 일반적인 클라우드 서비스는 서드파티 트랜잭션 이메일 서비스 공급자로부터 HTTPS 하이퍼

링크가 아닌 HTTP 하이퍼링크를 사용하여 이메일을 전송합니다. Chrome이 자동으로 로드하려고 하는 HTTPS 사이트는 Seegrid의 [이 예](#)와 같이 이메일 링크의 도메인 이름에 인증서 오류 [로](#) 응답할 수 [있습니다](#).

이러한 이메일에 수신자 목록이 큰 경우 SWG를 통해 클릭(또는 요청)을 보낸 많은 사용자가 516 오류와 같은 오류를 보고할 수 있습니다. 인증서 오류를 해결하려면 전자 메일 서비스 공급자 또는 전자 메일을 보낸 조직에 문의하십시오.

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.