

516 업스트림 인증서 CN 불일치 오류 해결

목차

[소개](#)

[문제](#)

[인증서 ID 역학](#)

[인증서 ID 오류](#)

[해결](#)

[공용 이름은 사용되지 않습니다.](#)

[추가 정보](#)

소개

이 문서에서는 516 업스트림 인증서 CN 불일치 오류를 해결하는 방법에 대해 설명합니다.

문제

Umbrella SWG(Secure Web Gateway) 프록시가 HTTPS 검사를 수행하도록 구성된 경우 사용자는 HTTPS URL을 사용하여 웹 사이트를 탐색할 때 516 업스트림 인증서 CN 불일치 오류 페이지를 받을 수 있습니다.

이 오류는 웹 사이트 인증서의 Subject(주체) 필드에 있는 CN(Common Name) 특성에 문제가 있음을 나타내지 않습니다. 대신, 이 문제는 인증서의 SAN(Subject Alternative Names) 확장에 있는 DNS Name 특성과 관련이 있습니다.

이 문서를 검토한 후 516 오류 페이지의 이유를 확인할 수 없는 경우 Umbrella 기술 지원에 문의하고 이 문서의 Certificate Identity Errors 섹션에 지정된 정보를 제공하십시오.

인증서 ID 역학

HTTPS URL을 요청할 때 브라우저나 다른 웹 클라이언트가 TLS 협상의 Client Hello 메시지에 있는 SNI([Server Name Indication](#)) 확장 프로그램을 통해 URL의 도메인 이름을 웹 서버에 보냅니다. 서버는 종종 여러 웹 사이트를 호스팅하고 일부 또는 모든 사이트에 대해 서로 다른 인증서를 가질 수 있으므로 이 SNI 값을 사용하여 클라이언트로 반환할 서버 인증서를 선택합니다.

웹 클라이언트에서 서버 인증서를 수신하면 클라이언트는 요청된 도메인 이름을 인증서의 주체 대체 이름 확장명의 DNS 이름 특성에 있는 도메인 이름과 비교하여 인증서가 요청에 대한 올바른 이름인지 확인합니다. 이 그림에서는 서버 인증서의 이러한 SAN을 보여 줍니다.



Certificate Viewer: www.example.org

General

Details

Certificate Hierarchy

▼ DigiCert Global Root CA

▼ DigiCert TLS RSA SHA256 2020 CA1

www.example.org

Certificate Fields

Certification Authority Key ID

Certificate Subject Key ID

Certificate Subject Alternative Name

Certificate Key Usage

Extended Key Usage

CRL Distribution Points

Certificate Policies

Authority Information Access

Field Value

DNS Name: www.example.org

DNS Name: example.net

DNS Name: example.edu

DNS Name: example.com

DNS Name: example.org

Export...

16796247745556

이 웹 서버는 다음 SNI 값을 사용하는 요청과 필드 값 패널에 표시되지 않는 다른 요청에 대한 응답으로 이 인증서를 반환합니다.

- www.example.org

- example.net을 참조하십시오.
- example.edu
- example.com
- example.org

SAN "example.com"은 "www.example.com"의 SNI와 일치하지 [않습니다](#). 그러나 "*.example.com"의 와일드카드 SAN은 "www.example.com"의 SNI 또는 단일 레이블("이 없는 문자열)을 포함하는 다른 도메인 이름과 일치합니다. example.com 앞에 문자가 추가되었지만 여러 레이블은 추가되지 않았습니다. 예를 들어 "[www](#).hr"은 두 개의 레이블로 구성되어 있으므로 "www.hr.example.com"은 "*.example.com"과 일치하지 않습니다. "www" 및 "hr". 단일 와일드카드는 단일 레이블에만 일치할 수 있습니다.

인증서 ID 오류

웹 클라이언트가 서버 인증서를 받을 때 요청된 URL의 도메인 이름에서 SNI와 일치하는 SAN의 DNS 이름이 없으면 일반적으로 웹 클라이언트는 사용자에게 오류를 표시합니다. 이 그림에서는 "NET::ERR_CERT_COMMON_NAME_INVALID" 인터스티셜 페이지를 표시하는 Chrome을 보여줍니다.



Your connection is not private

Attackers might be trying to steal your information from **wrong.host.badssl.com** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_COMMON_NAME_INVALID



To get Chrome's highest level of security, [turn on enhanced protection](#)

Hide advanced

Back to safety

This server could not prove that it is **wrong.host.badssl.com**; its security certificate is from ***.badssl.com**. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to wrong.host.badssl.com \(unsafe\)](#)

16794294817428

이미지에서 요청한 사이트는 SAN과 일치하지 않는 "https://wrong.host.badssl.com"입니다. 인증서에는 와일드카드 SAN DNS 이름 "*.badssl.com"이 포함되어 있으며, 와일드카드는 "host"와 같은 단일 레이블에만 일치할 수 있습니다. 또한 인증서에는 정확한 값이 "wrong.host.badssl.com"인 SAN DNS 이름 또는 "*.host.badssl.com"인 와일드카드 SAN이 없으므로 사용자에게 이 오류가 표시됩니다.

인증서 ID가 일치하지 않는 이유를 식별하려면 브라우저의 인증서 보기 기능을 사용하여 인증서의 SAN DNS 이름을 검사하고 요청된 URL의 도메인 이름과 비교합니다. 또는 [Qualys SSL Server Test](#)와 같은 [도구](#)를 사용하여 인증서 ID 문제를 진단할 수 있습니다.

이 섹션의 정보를 채운 후 516 오류의 이유를 확인할 수 없거나 다음 섹션의 해결 방법 및 해결 방법을 사용할 수 없는 경우 Umbrella 기술 지원 케이스를 [열고 다음](#)을 제공하십시오.

1. 캡처한 스크린샷

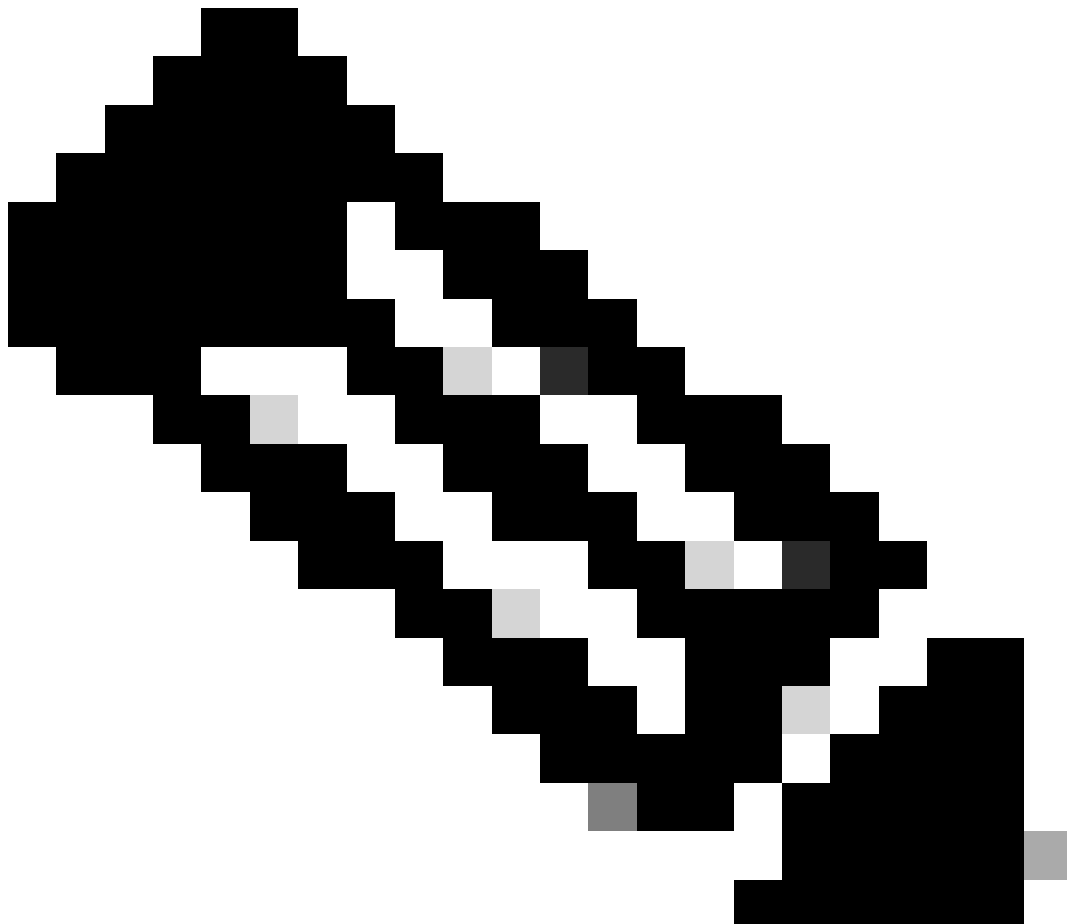
- 요청된 URL을 표시하는 브라우저의 주소 표시줄
- 전체 516 오류 페이지(다음 섹션의 이미지 참조)

2. 주소 표시줄에서 복사한 URL의 텍스트

해결

이 문제를 해결하려면 인증서의 SAN DNS 이름 중 하나와 일치하는 도메인 이름을 사용하여 서버에 액세스합니다. 이렇게 하려면 웹 사이트의 관리자가 해당 영역의 DNS에 일치하는 도메인 이름을 추가해야 합니다. 또는 관리자는 SAN DNS 이름 중 하나에 URL의 도메인 이름을 포함하도록 인증서를 다시 발급할 수 있습니다.

이를 해결하려면 URL의 도메인 이름을 보안 웹 게이트웨이 프록시의 [선택적 암호 해독 목록](#) 또는 지능형 프록시의 [대상 목록](#)에 추가할 수 있습니다. 적절한 웹 정책 규칙 집합 설정(보안 웹 게이트웨이) 또는 DNS 정책 허용 목록(지능형 프록시)에 목록을 적용합니다. 이렇게 하면 웹 사이트에 대한 요청이 프록시에 의해 암호 해독되지 않으므로 프록시에서 516 오류 페이지를 표시할 수 없습니다.



하나의 프록시 기술만 사용할 수 있습니다. Secure Web Gateway에 대한 구독이 있는 조직은 SWG를 사용하고 Intelligent Proxy를 사용하지 않는 것이 좋습니다.

공용 이름은 사용되지 않습니다.

원래 웹 클라이언트가 요청된 URL의 도메인 이름을 인증서의 Subject(주체) 필드에 있는 CN(Common Name) 특성과 일치시켰습니다. 이 메커니즘은 최신 웹 클라이언트에서 더 이상 사용되지 않습니다. 이제 도메인이 주체 대체 이름 확장의 DNS 이름에 대해 확인됩니다. 그러나 오류 메시지의 텍스트는 종종 Chrome의 "NET::ERR_CERT_COMMON_NAME_INVALID"와 같이 더 이상 사용되지 않는 메커니즘을 계속 참조합니다.

마찬가지로, SWG 프록시가 웹 서버에서 URL을 요청하고 SAN DNS Name 불일치가 발생하는 경우 Umbrella SWG는 이 텍스트와 함께 516 오류 페이지를 표시합니다.



516 Upstream Certificate CN Mismatch

The SSL security certificate presented by this site was issued for a different site's address. This happens when the common name of the SSL Certificate doesn't exactly match the name displayed in the address bar. Certificate doesn't exactly match the name displayed in the address bar and can indicate that attackers might be trying to steal your information (for example, passwords, messages, or credit cards). If you continue seeing this error, please contact your Administrator.

This page is served by Umbrella Cloud Security Gateway. Server: mps-d05f188a1162.sigenv1.cdg1

Thu, 22 Jul 2021 14:09:45 GMT

16794325789332

Cisco Umbrella는 현재 동작을 더 잘 반영하기 위해 향후 이 텍스트를 업데이트할 계획입니다.

추가 정보

RFC 5280 참조: Internet X.509 CRL(Public Key Infrastructure Certificate and Certificate

Revocation List) Profile, Section [4.1.2.6](#) for information on certificate Subject, Section [4.2.1.6](#) for information on Subject Alternative Name.

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.