516 Upstream Certificate CN Mismatch-fout oplossen

Inhoud

Inleiding

In dit document wordt beschreven hoe u een 516 Upstream Certificate CN Mismatch-fout kunt oplossen.

uitgeven

Wanneer de Umbrella Secure Web Gateway (SWG)-proxy is geconfigureerd om HTTPS-inspectie uit te voeren, kan een gebruiker een 516 Upstream Certificate CN Mismatch-foutpagina ontvangen wanneer hij naar een website bladert met behulp van een HTTPS-URL.

Deze fout wijst niet op een probleem met het kenmerk Common Name (CN) in het veld Onderwerp van het websitecertificaat. Het probleem heeft eerder betrekking op het DNS-naamattribuut in de extensie Subject Alternative Names (SAN) van een certificaat.

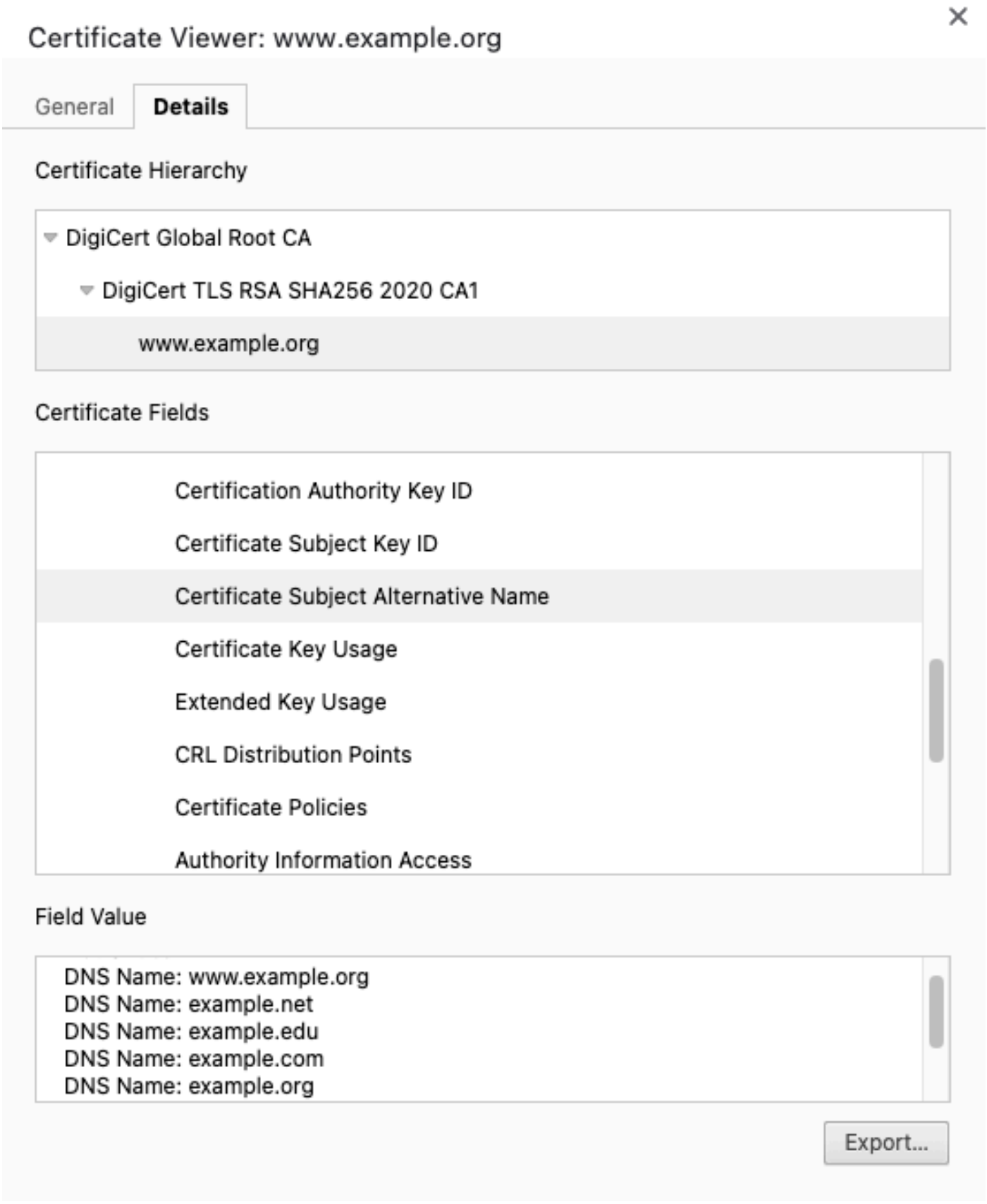
Als u na het bekijken van dit artikel de reden voor de 516-foutpagina niet kunt achterhalen, neemt u contact op met de technische ondersteuning van Umbrella en verstrekt u ons de informatie die is gespecificeerd in de sectie Certificaatidentiteitsfouten in dit document.

Certificaat Identiteitsmechanica

Bij het aanvragen van een HTTPS-URL stuurt een browser of andere webclient de domeinnaam in de URL naar de webserver via de extensie Server Name Indication (SNI) in het Hello-bericht van de client van de TLS-onderhandeling. De server gebruikt deze SNI-waarde om het servercertificaat te selecteren om terug te keren naar de client, omdat een server vaak meerdere websites host en verschillende certificaten kan hebben voor sommige of alle sites.

Wanneer het servercertificaat door de webclient wordt ontvangen, controleert de client of het certificaat het juiste certificaat is voor het verzoek door de aangevraagde domeinnaam te vergelijken met de domeinnaam (domeinnamen) in de DNS-naamkenmerken van de Subject

Alternative Names-extensie van het certificaat. Deze afbeelding toont deze SAN's in een servercertificaat.



16796247745556

Deze webserver retourneert dit certificaat als reactie op verzoeken met deze SNI-waarden en

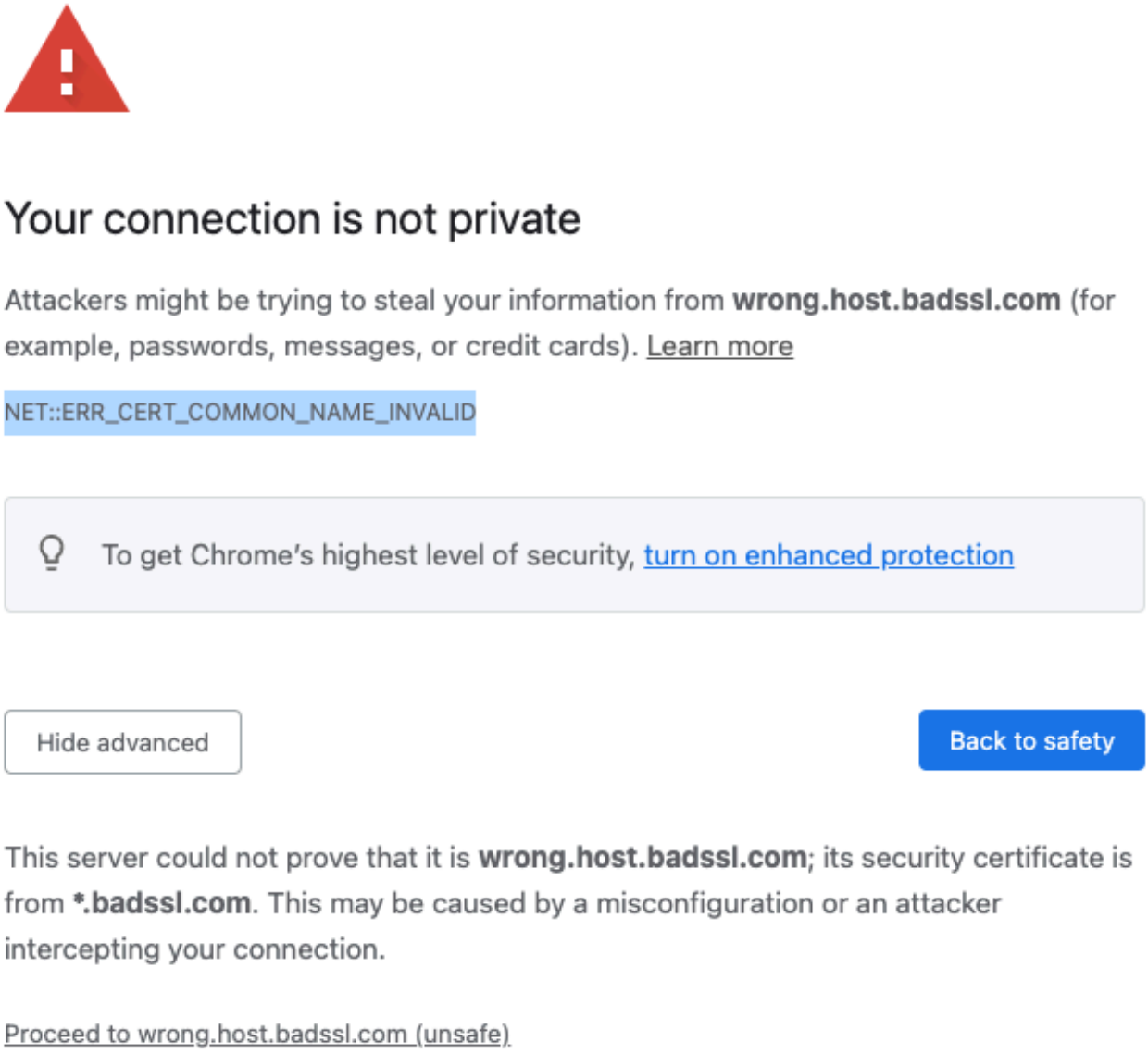
andere niet-zichtbare waarden in het deelvenster Veldwaarde:

- www.example.org
- example.net
- example.edu
- example.com
- example.org

Merk op dat het SAN "example.com" niet overeenkomt met een SNI van "www.example.com". Een wildcard-SAN van "*.example.com" zou echter overeenkomen met een SNI van "www.example.com", of een andere domeinnaam met één label (een tekenreeks zonder "."-teken) dat aan example.com is toegevoegd, maar niet met meerdere labels. Bijvoorbeeld, "www.hr.example.com" wordt niet geëvenaard door "*.example.com" omdat "www.hr" bestaat uit twee labels: "www" en "hr". Een enkele joker kan alleen overeenkomen met een enkel label.

Fouten in certificaatidentiteit

Wanneer een webclient een servercertificaat ontvangt en geen van de DNS-namen van het SAN overeenkomt met de SNI van de domeinnaam in de aangevraagde URL, geeft de webclient doorgaans een fout weer aan de gebruiker. Deze afbeelding toont Chrome met een "NET::ERR_CERT_COMMON_NAME_INVALID" interstitiële pagina.



16794294817428

In het image werd de site "https://wrong.host.badssl.com" gevraagd die niet overeenkomt met een van de SAN's. Het certificaat bevat een wildcard SAN DNS-naam, "*.badssl.com" waarvan de wildcard alleen kan overeenkomen met een enkel label zoals "host". Bovendien heeft het certificaat geen SAN DNS-naam met de exacte waarde "wrong.host.badssl.com" of een wildcard-SAN van "*.host.badssl.com", zodat de gebruiker deze fout te zien krijgt.

Als u de reden voor een mismatch in de certificaatidentiteit wilt identificeren, controleert u de SAN DNS-namen van het certificaat met de functie voor het weergeven van certificaten in de browser en vergelijkt u deze met de domeinnaam in de aangevraagde URL. Als alternatief kan een tool zoals de Qualys SSL Server Test worden gebruikt om een identiteitsprobleem met een certificaat te diagnosticeren.

Als de oorzaak van de 516-fout niet kan worden vastgesteld nadat de informatie in deze sectie is

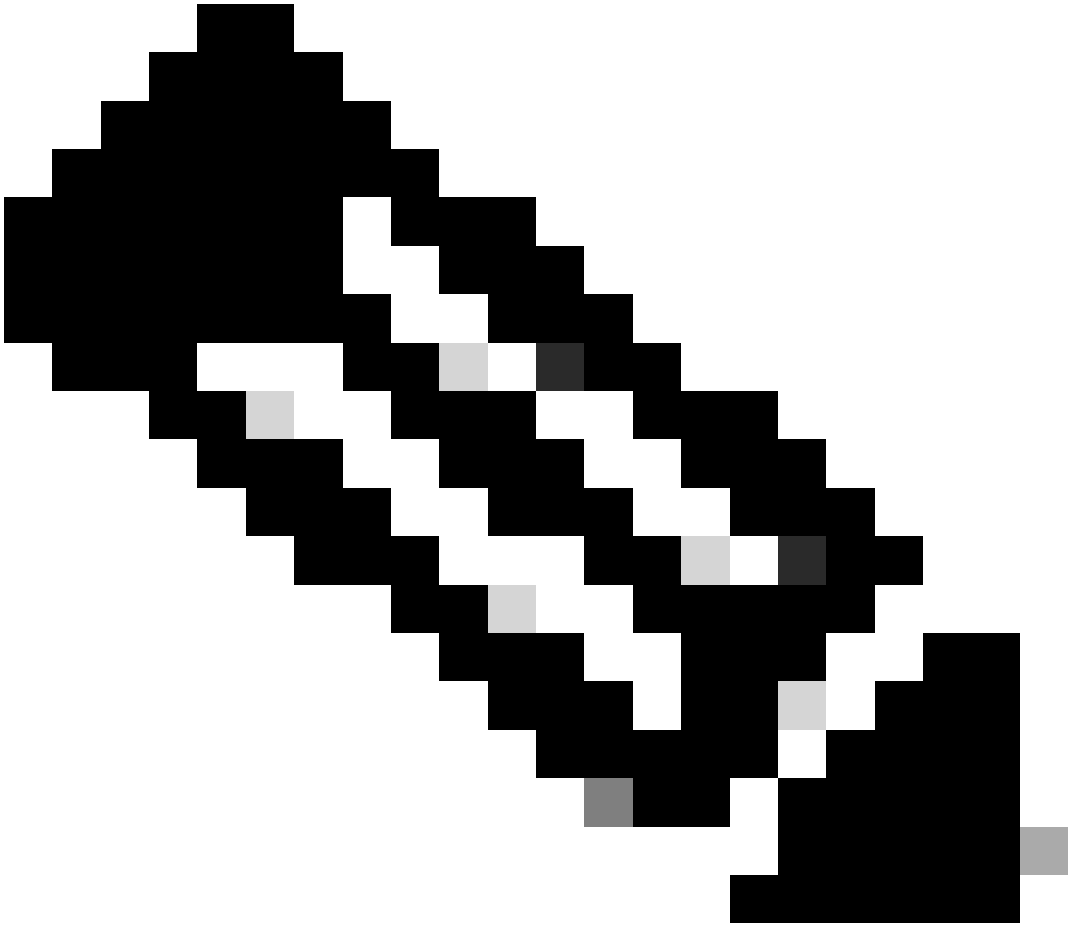
gebruikt, of als de oplossingen en oplossingen in de volgende sectie niet kunnen worden gebruikt, opent u een zaak met technische ondersteuning van Umbrella en verstrekt u:

1. Een screenshot die
    - de adresbalk van de browser met de gevraagde URL
    - De gehele 516-foutpagina (zie afbeelding in de volgende sectie)
2. de tekst van de URL die is gekopieerd van de adresbalk

resolutie

Om dit probleem op te lossen, opent u de server met een domeinnaam die overeenkomt met een van de SAN DNS-namen in het certificaat. Dit kan vereisen dat de beheerder van de website een overeenkomende domeinnaam toevoegt aan de DNS voor de zone. Als alternatief kan de beheerder het certificaat opnieuw uitgeven om de domeinnaam van de URL op te nemen in een van de SAN DNS-namen.

Als tijdelijke oplossing kan de domeinnaam van de URL worden toegevoegd aan een selectieve decoderingslijst voor de proxy voor de beveiligde webgateway of aan een bestemmingslijst in de intelligente proxy. Pas de lijst toe op de juiste instelling voor webbeleidsregels (Secure Web Gateway) of de lijst met toegestane DNS-beleidsregels (Intelligente proxy). Dit voorkomt dat het verzoek naar de website wordt ontsleuteld door de proxy, waardoor de proxy geen 516-foutpagina kan weergeven.



Opmerking: het gebruik van zowel de Secure Web Gateway-proxy als de Intelligent Proxy wordt niet ondersteund. Per organisatie kan slechts één proxy-technologie worden ingezet. Het wordt aanbevolen dat organisaties die een abonnement hebben op Secure Web Gateway SWG gebruiken en geen gebruik maken van Intelligent Proxy.

De algemene naam is afgekeurd

Webclients hebben de domeinnaam in de aangevraagde URL oorspronkelijk gekoppeld aan het kenmerk Common Name (CN) in het veld Onderwerp van het certificaat. Dit mechanisme is afgekeurd in moderne webclients; domeinen worden nu vergeleken met de DNS-namen van de Subject Alternative Name-extensie. Tekst van foutmeldingen blijft echter vaak verwijzen naar het afgekeurde mechanisme, zoals "NET:: ERR_CERT_COMMON_NAME_INVALID" in Chrome.

Op dezelfde manier geeft Umbrella SWG een 516-foutpagina met deze tekst weer wanneer de SWG-proxy een URL van een webserver aanvraagt en er een SAN DNS-naammismatch optreedt:

16794325789332

Cisco Umbrella is van plan om deze tekst op een toekomstige datum bij te werken om het huidige gedrag beter weer te geven.

Aanvullende informatie

Zie RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Section 4.1.2.6 voor informatie over het onderwerp van het certificaat en Section 4.2.1.6 voor informatie over de alternatieve naam van het onderwerp.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.