Resolver error de discrepancia CN de certificado ascendente 516

Contenido

Introducción

Este documento describe cómo resolver un error 516 Upstream Certificate CN Mismatch.

Problema

Cuando el proxy de Umbrella Secure Web Gateway (SWG) se configura para realizar la inspección de HTTPS, un usuario puede recibir una página de error 516 Upstream Certificate CN Mismatch al navegar a un sitio web usando una URL HTTPS.

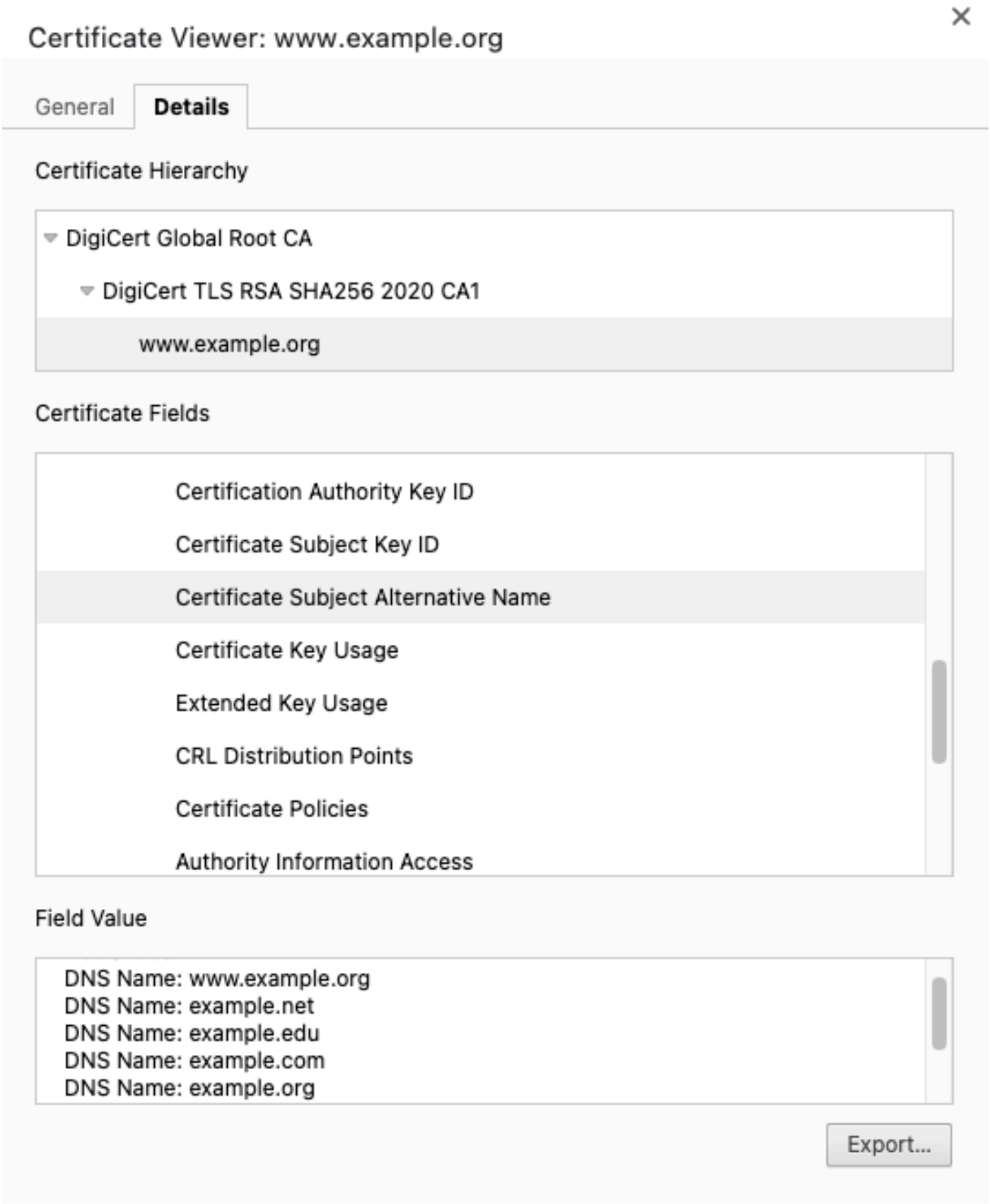
Este error no indica un problema con el atributo Common Name (CN) en el campo Subject (Asunto) del certificado del sitio web. Más bien, el problema pertenece al atributo Nombre DNS en la extensión de Nombres alternativos de sujeto (SAN) de un certificado.

Después de revisar este artículo, si no puede identificar la razón de la página de error 516, comuníquese con el soporte técnico de Umbrella y proporciónenos la información especificada en la sección Errores de identidad de certificado en este documento.

Mecánica de identidad de certificados

Al solicitar una URL HTTPS, un navegador u otro cliente web envía el nombre de dominio en la URL al servidor web a través de la extensión Indicación de nombre de servidor (SNI) en el mensaje de saludo del cliente de la negociación TLS. El servidor utiliza este valor SNI para seleccionar el certificado de servidor que se devolverá al cliente, ya que un servidor suele alojar varios sitios web y puede tener certificados diferentes para algunos o todos los sitios.

Cuando el cliente web recibe el certificado de servidor, el cliente comprueba que el certificado es el correcto para la solicitud comparando el nombre de dominio solicitado con los nombres de dominio en los atributos Nombre DNS de la extensión Nombres alternativos de sujeto del certificado. Esta imagen muestra estas SAN en un certificado de servidor.



16796247745556

Este servidor web devuelve este certificado en respuesta a las solicitudes con estos valores SNI, así como otros valores no visibles en el panel Valor de campo:

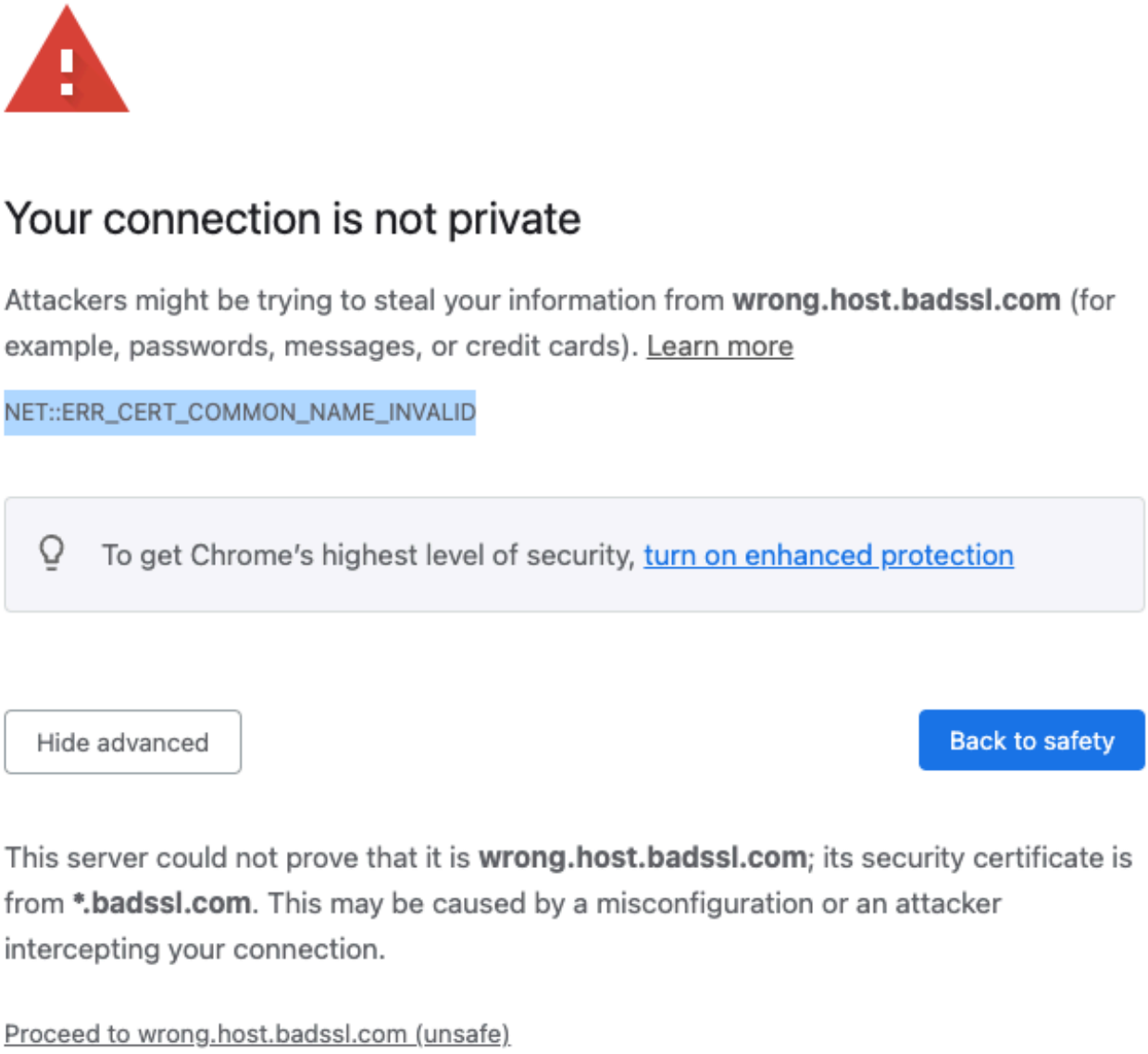
- www.example.org

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

Tenga en cuenta que el archivo SAN "example.com" no coincide con un SNI de "www.example.com". Sin embargo, una SAN comodín de "*.example.com" coincidiría con un SNI de "www.example.com" o cualquier otro nombre de dominio que contenga una sola etiqueta (una cadena sin ".") delante de example.com, pero no de varias etiquetas. Por ejemplo, "www.hr.example.com" no coincide con "*.example.com" porque "www.hr" consta de dos etiquetas: "www" y "hr". Un solo comodín solo puede coincidir con una sola etiqueta.

Errores de identidad del certificado

Cuando un cliente web recibe un certificado de servidor, si ninguno de los nombres DNS de la SAN coincide con el SNI del nombre de dominio en la URL solicitada, el cliente web normalmente muestra un error al usuario. Esta imagen muestra Chrome mostrando una página intersticial "NET::ERR_CERT_COMMON_NAME_INVALID".



16794294817428

En la imagen, el sitio solicitado era "https://wrong.host.badssl.com", que no coincide con ninguna de las redes SAN. El certificado contiene un nombre DNS de SAN comodín, "*.badssl.com", cuyo comodín solo puede coincidir con una sola etiqueta como "host". Además, el certificado no tiene un nombre DNS de SAN con el valor exacto "wrong.host.badssl.com" o un comodín SAN de "*.host.badssl.com", por lo que se presenta este error al usuario.

Para identificar el motivo de una discordancia de identidad de certificado, inspeccione los nombres DNS de SAN del certificado mediante la función de visualización de certificados del navegador y compárelos con el nombre de dominio de la URL solicitada. Alternativamente, una herramienta como la prueba de servidor SSL de Qualys se puede utilizar para diagnosticar un problema de identidad de certificado.

Si la razón del error 516 no se puede identificar después de emplear la información de esta

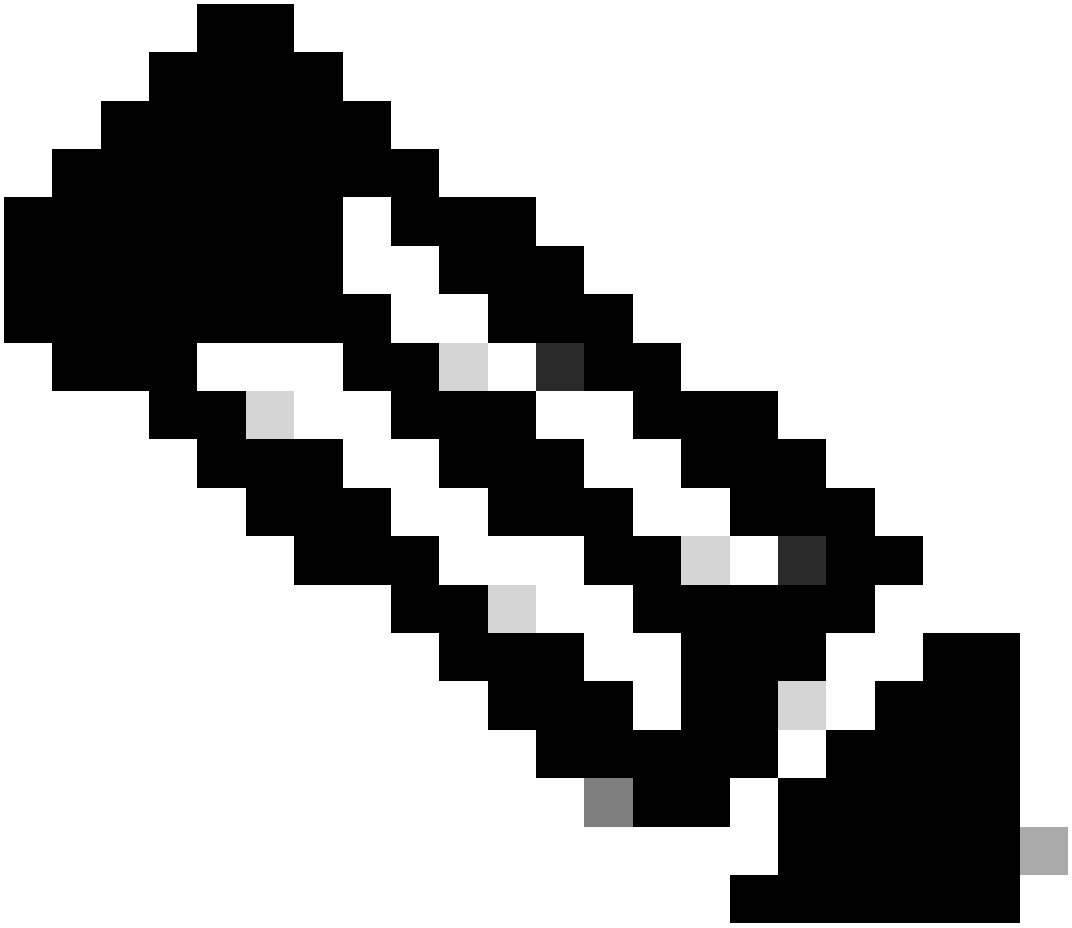
sección, o si no se pueden emplear las resoluciones y soluciones alternativas de la siguiente sección, abra un caso con el soporte técnico de Umbrella y proporcione:

1. una captura de pantalla que captura
    - la barra de direcciones del navegador que muestra la URL solicitada
    - la página de error 516 completa (consulte la imagen en la siguiente sección)
2. el texto de la URL copiada de la barra de direcciones

Resolución

Para resolver este problema, acceda al servidor con un nombre de dominio que coincida con uno de los nombres DNS de SAN del certificado. Esto puede requerir que el administrador del sitio web agregue un nombre de dominio coincidente al DNS de la zona. Como alternativa, el administrador puede volver a emitir el certificado para incluir el nombre de dominio de la URL en uno de los nombres DNS de SAN.

Como solución temporal, el nombre de dominio de la URL se puede agregar a una lista de descifrado selectivo para el proxy de gateway web seguro o a una lista de destino en el proxy inteligente. Aplique la lista a la configuración del conjunto de reglas de la directiva Web correspondiente (gateway Web seguro) o a la lista de permitidos de la directiva DNS (proxy inteligente). Esto evita que la solicitud al sitio web sea descifrada por el proxy, lo que evita que el proxy muestre una página de error 516.



Nota: No se admite el uso del proxy de gateway web seguro y del proxy inteligente. Solo se puede emplear una tecnología proxy por organización. Se recomienda que las organizaciones que tengan suscripciones a Secure Web Gateway utilicen SWG y no Intelligent Proxy.

El nombre común está obsoleto

Los clientes web coincidieron originalmente con el nombre de dominio de la dirección URL solicitada en el atributo Common Name (CN) del campo Subject del certificado. Este mecanismo ha quedado obsoleto en los clientes web modernos; Ahora los dominios se comparan con los Nombres DNS de la extensión Nombre Alternativo del Sujeto. Sin embargo, el texto de los mensajes de error suele seguir haciendo referencia al mecanismo desaprobado, como "NET::ERR_CERT_COMMON_NAME_INVALID" en Chrome.

Del mismo modo, Umbrella SWG muestra una página de error 516 con este texto cuando el proxy SWG solicita una URL de un servidor web y se produce una discordancia de nombre DNS de SAN:

16794325789332

Cisco Umbrella tiene previsto actualizar este texto en una fecha futura para reflejar mejor el comportamiento actual.

Additional Information

Consulte RFC 5280: Perfil de Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL), Sección 4.1.2.6 para obtener información sobre el asunto del certificado, y Sección 4.2.1.6 para obtener información sobre el nombre alternativo del sujeto.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).