Solución de problemas de errores 516 en Umbrella Secure Web Gateway

Contenido

Introducción

Este documento describe cómo resolver un aumento de 516 errores en Umbrella Secure Web Gateway.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Umbrella Secure Web Gateway (SWG).

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

Los usuarios que navegan a través del proxy de Umbrella Secure Web Gateway (SWG) con inspección HTTPS pueden recibir con más frecuencia páginas de error 516 Upstream Certificate CN Mismatch a partir de la segunda quincena de octubre de 2023.

La página de error 516 se produce cuando el certificado de un sitio web no coincide con el nombre de dominio utilizado por el cliente para acceder al sitio.

El aumento de las páginas de error se debe a un cambio en el navegador de Chrome la gestión de las solicitudes de URL que utilizan el esquema HTTP (sin cifrar). Chrome ahora intenta cargar el recurso con el esquema HTTPS (cifrado) primero. Cuando se configura para la inspección HTTPS, SWG inspecciona el certificado de un sitio web y devuelve una página web que muestra un código de error como 516 si el certificado no es aceptable.

Para solucionar este problema, los clientes pueden configurar sus políticas web para omitir la inspección HTTPS en las solicitudes que, de lo contrario, generarían 516 errores.

516 Fondo del error

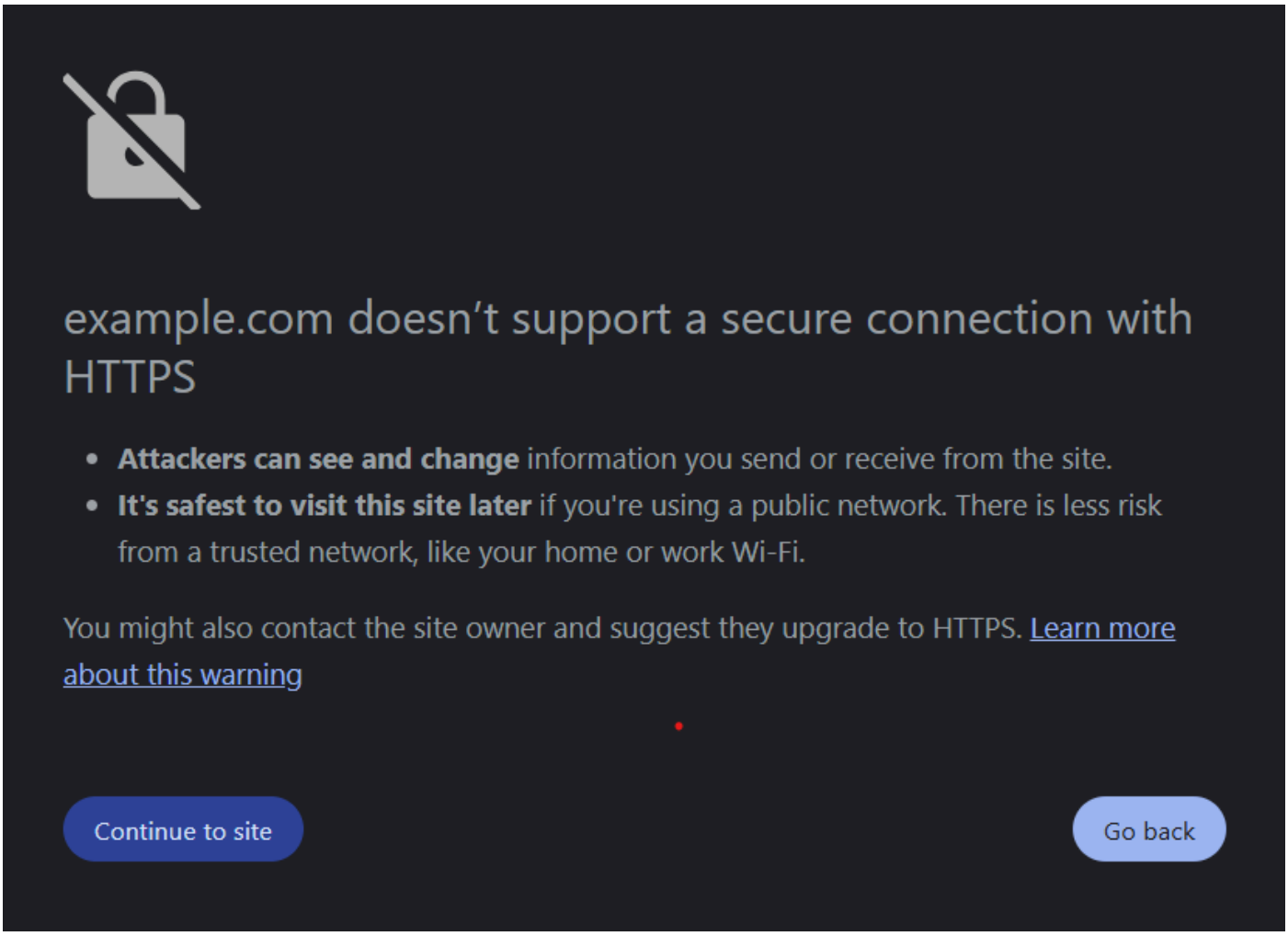
En resumen, Umbrella Secure Web Gateway devuelve una página de error 516 cuando el nombre de dominio utilizado para acceder a un sitio web a través de HTTPS no aparece en el certificado digital del servidor. Para obtener información adicional que describa el motivo por el que el gateway web seguro devuelve una página de error 516, consulte el artículo de la Base de conocimiento de Umbrella "516 Upstream Certificate CN Mismatch" error.

Por ejemplo, piense en un sitio que ofrece contenido de URL HTTP con el siguiente formato: http://www.example.com/path_to_content. Si un usuario solicita las URL HTTPS equivalentes, pero el sitio no tiene un certificado cuyas SAN coincidan con www.example.com (quizá la SAN solo coincida con example.com), el usuario recibe un error 516 si la solicitud la gestiona el gateway web seguro de Umbrella con una política web que utilice la función de inspección HTTPS de SWG.

Cambio de comportamiento de Chrome

En la segunda mitad de octubre de 2023, Google completó el lanzamiento de una nueva función para el navegador Chrome. Después de esa fecha, se realiza automáticamente una solicitud de URL HTTP utilizando la versión HTTPS de esa URL. Por ejemplo, cuando un usuario realiza una solicitud para http://www.example.com, Chrome primero intenta satisfacer la solicitud mediante https://www.example.com.

Si Chrome recibe un error relacionado con HTTPS al solicitar la URL HTTPS, Chrome intenta cargar el mismo contenido a través de HTTP. Si la solicitud de la URL HTTP es exitosa, Chrome muestra una página intersticial con texto que indica que el sitio no es seguro y un enlace que da al usuario la opción de continuar, según la imagen a continuación.



Este es el comportamiento de repliegue en la nueva funcionalidad de Chrome.

Sin embargo, al navegar a través de SWG con la inspección HTTPS, si la solicitud HTTPS produce un error relacionado con HTTPS como "ERR_CERT_COMMON_NAME_INVALID" desde el sitio, SWG intercepta el error y devuelve una página de error SWG a Chrome como la página de error 516. Chrome no considera que este contenido de SWG sea un error relacionado con HTTPS, por lo que no produce el comportamiento de repliegue y se muestra la página de error de SWG, en lugar de la página de la imagen anterior.

Puede encontrar más información sobre el nuevo comportamiento de Chrome en el blog Chromium y en el repositorio GitHub de la función.

Determinación del Origen del Error

Ahora que Chrome promociona automáticamente las URL HTTP a las URL HTTPS, los sitios web que generan 516 errores son vistos con más frecuencia por los usuarios.

Para confirmar que un sitio web está causando un error relacionado con HTTPS, como la respuesta 516, navegue por el sitio con Chrome desde un sistema de escritorio que no utilice Umbrella. Asegúrese de introducir manualmente la versión HTTPS de la URL explícitamente en el Omnibox de Chrome (como la barra de direcciones) en lugar de hacer clic en un hipervínculo HTTP. Si un hipervínculo generó un error 516 con SWG, al solicitar manualmente la URL HTTPS en Chrome sin SWG se puede generar el mensaje de error

"ERR_CERT_COMMON_NAME_INVALID". Este mensaje de error confirma que el problema es un certificado incorrecto para el nombre de dominio utilizado para acceder al sitio web.

Alternativamente, utilice una herramienta en línea como el sitio Qualys SSL Server Test para diagnosticar el problema con el sitio web.

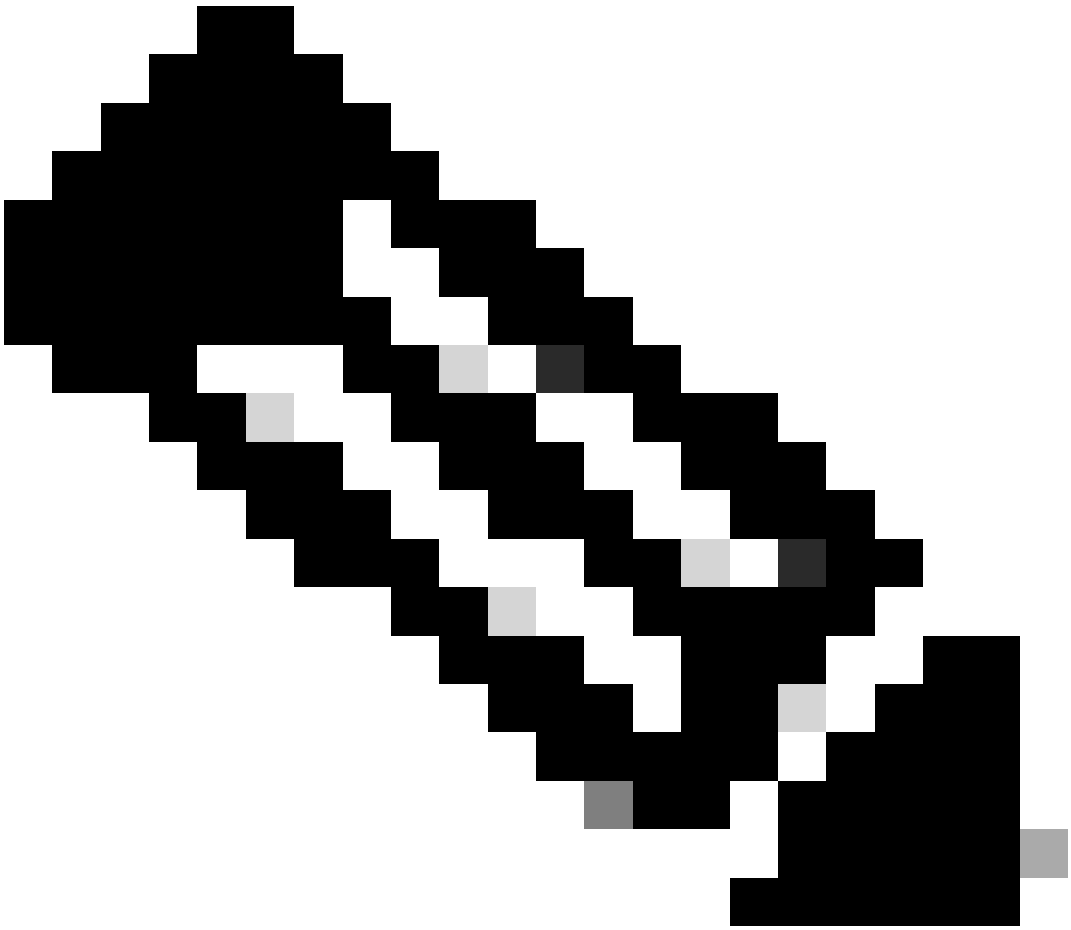
Soluciones alternativas

Los administradores generales pueden solucionar el problema con una de estas opciones:

1. Cree una lista de destino específica para estos sitios y agregue la lista a una política web sin inspección HTTPS.

2. Cree una Lista de Descifrado Selectivo de sitios que produzcan 516 páginas de error y agregue la Lista de Descifrado Selectivo a todas las políticas Web relevantes

---



Nota: Factores como los redireccionamientos HTTP o los sistemas de seguridad de correo electrónico que sustituyen las URL HTTPS de sus servicios por las URL HTTP originales pueden ocultar el nombre de dominio necesario. Identificar el nombre de

---

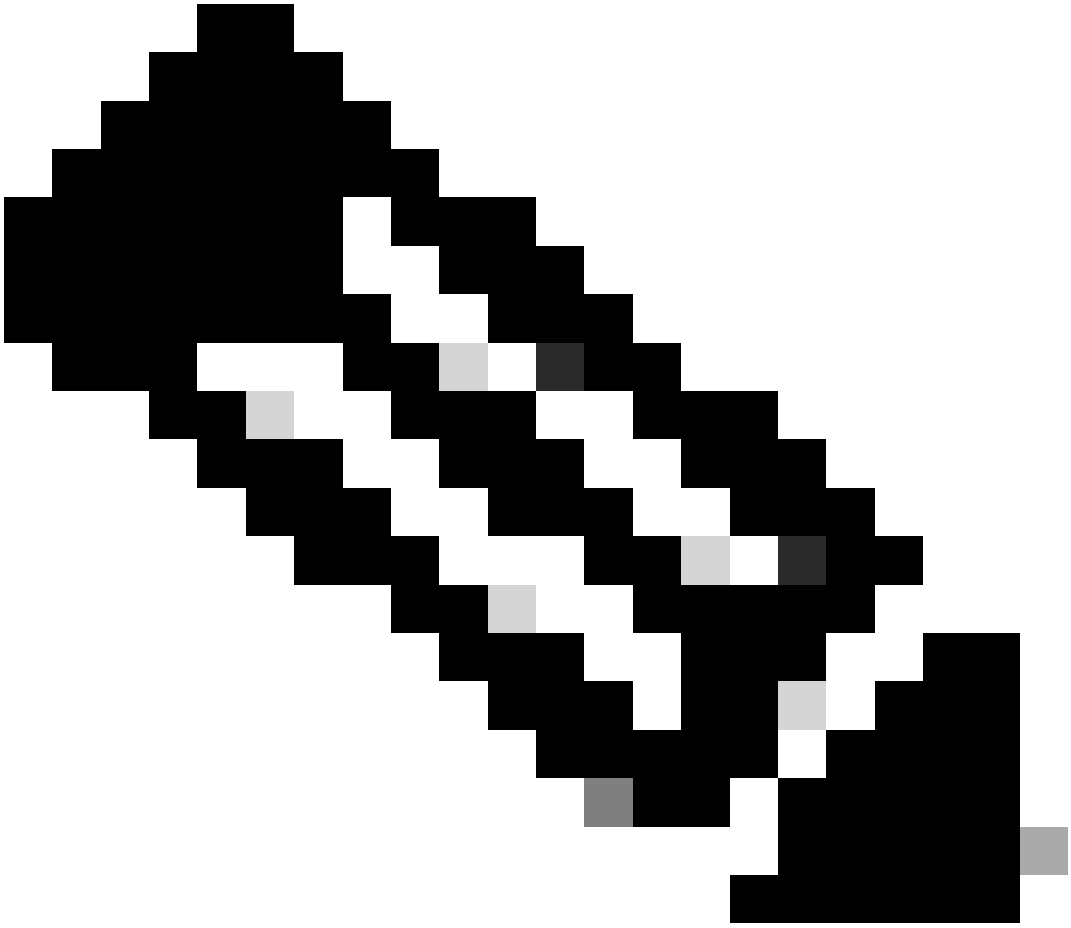
dominio correcto para una lista de destino o una lista de descifrado selectivo puede requerir investigación, incluido el uso de herramientas específicas (curl, Chrome Developer Tools, un registro del proveedor de seguridad de correo electrónico, etc.).

516 Errores y sistemas de correo electrónico

Un aumento en la frecuencia de error de 516 puede ser el resultado de sistemas de correo electrónico que muestran correos electrónicos en formato HTML y permiten hipervínculos en los correos electrónicos. Al redactar un correo electrónico, si el remitente escribe o pega un nombre de dominio en el cuerpo del correo electrónico, muchos sistemas de correo electrónico promocionan automáticamente un nombre de dominio de texto sin formato a un hipervínculo. Normalmente, cuando se crea el enlace, el esquema es HTTP en lugar de HTTPS.

Por ejemplo, si escribe la cadena `example.com` en un mensaje de correo electrónico, puede recibir un mensaje de correo electrónico con el código HTML `<a href="http://www.example.com">`, que se muestra como hipervínculo www.example.com.

Si un destinatario de dicho correo electrónico hace clic en ese hipervínculo HTTP, la solicitud utiliza inicialmente HTTPS si el clic se abre en Chrome, o si Chrome ya se está utilizando para ver el correo electrónico.



Nota: Otros navegadores también pueden promocionar HTTP a HTTPS.

Además, un hipervínculo en un correo electrónico que usa intencionadamente el esquema HTTP se maneja de manera similar.

Algunos servicios comunes en la nube envían mensajes de correo electrónico de sus proveedores de servicios de correo electrónico transaccionales externos con hipervínculos HTTP en lugar de hipervínculos HTTPS. El sitio HTTPS que Chrome intenta cargar automáticamente puede responder con un error de certificado al nombre de dominio en el enlace de correo electrónico como en [este ejemplo de Segrid.]

Cuando estos correos electrónicos tienen listas de destinatarios grandes, muchos usuarios cuyos clics (o solicitudes) se envían a través de SWG pueden informar de errores como el error 516. Póngase en contacto con su proveedor de servicios de correo electrónico o con la organización que envió el correo electrónico para que se corrija el error del certificado.

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).