516 Fehler auf Umbrella Secure Web Gateway beheben

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie eine erhöhte Anzahl von 516 Fehlern bei Umbrella Secure Web Gateway beheben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Umbrella Secure Web Gateway (SWG).

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Überblick

Benutzer, die den Umbrella Secure Web Gateway (SWG)-Proxy mit HTTPS Inspection durchsuchen, können ab der zweiten Oktoberhälfte 2023 häufiger 516 Upstream Certificate CN Mismatch-Fehlerseiten erhalten.

Die Fehlerseite 516 tritt auf, wenn das Zertifikat einer Website nicht mit dem Domänennamen übereinstimmt, der vom Client für den Zugriff auf die Website verwendet wird.

Der Anstieg der Fehlerseiten ist auf eine Änderung in der Chrome-Browser-Behandlung von Anfragen für URLs, die das HTTP (unverschlüsselt) Schema verwenden. Chrome versucht nun, die Ressource mit dem HTTPS-Schema (verschlüsselt) zuerst zu laden. Bei der Konfiguration für HTTPS-Inspektion prüft die SWG das Zertifikat einer Website und gibt eine Webseite mit einem Fehlercode wie 516 zurück, wenn das Zertifikat nicht akzeptiert werden kann.

Um dieses Problem zu umgehen, können Kunden ihre Webrichtlinien so konfigurieren, dass HTTPS Inspection für Anfragen umgangen wird, die sonst zu 516 Fehlern führen.

516 Fehlerhintergrund

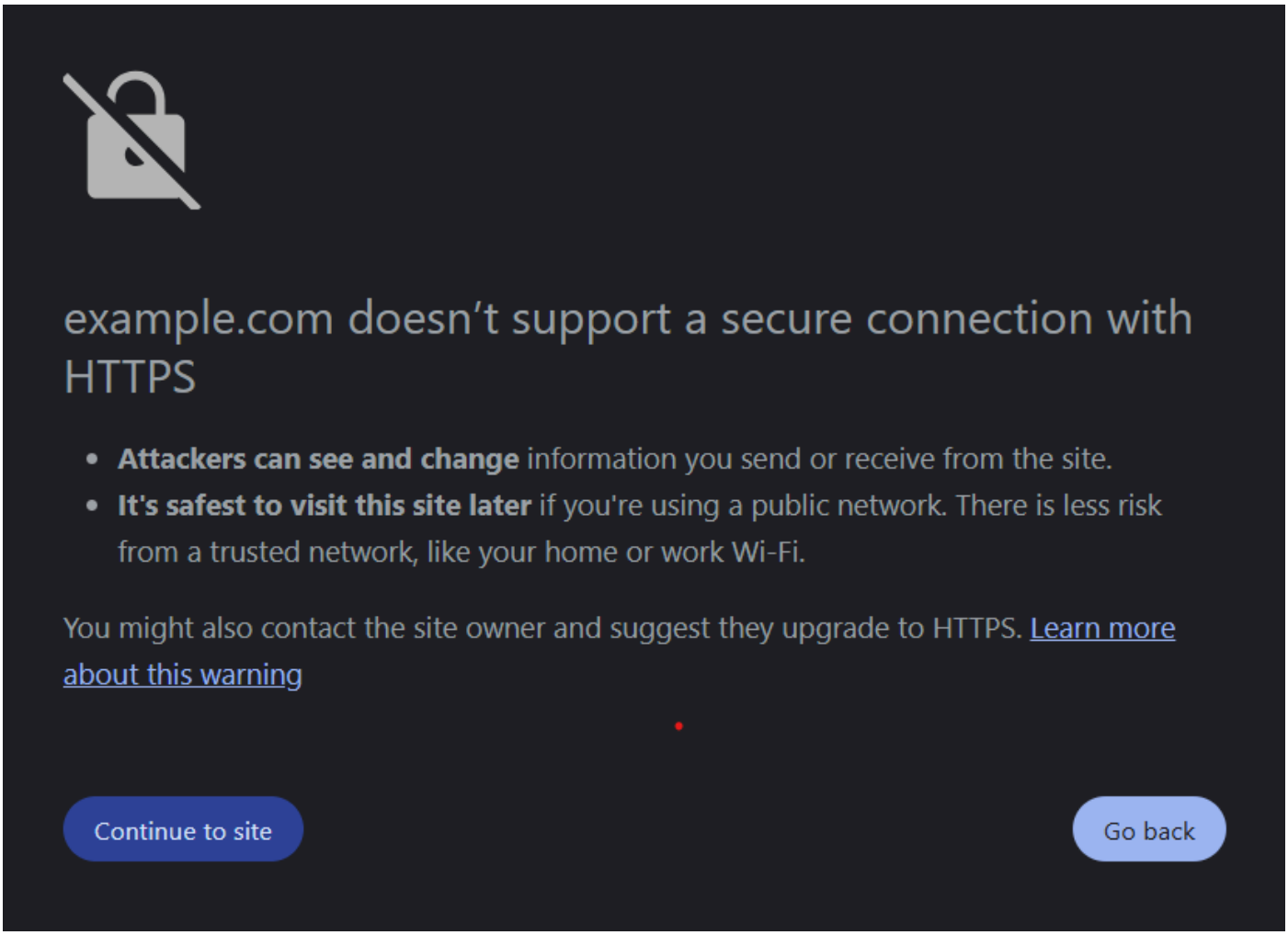
Kurz gesagt, das Umbrella Secure Web Gateway gibt eine 516-Fehlerseite zurück, wenn der Domänenname, der für den Zugriff auf eine Website über HTTPS verwendet wird, nicht im digitalen Zertifikat des Servers erscheint. Weitere Informationen, die den Grund dafür beschreiben, dass Secure Web Gateway eine Fehlerseite vom Typ 516 zurückgibt, finden Sie im Umbrella Knowledge Base-Artikel "516 Upstream Certificate CN Mismatch" (Fehler 516 Upstream-Zertifikat CN stimmt nicht überein).

Stellen Sie sich beispielsweise eine Website vor, die Inhalt von HTTP-URLs in folgender Form bereitstellt: http://www.example.com/path_to_content Wenn ein Benutzer die entsprechenden HTTPS-URLs anfordert, der Standort jedoch kein Zertifikat besitzt, dessen SANs mit www.example.com übereinstimmen (möglicherweise stimmt das SAN nur mit example.com überein), erhält der Benutzer einen 516-Fehler, wenn die Anforderung vom sicheren Web-Gateway von Umbrella mit einer Webrichtlinie verarbeitet wird, die die HTTPS-Überprüfungsfunktion von SWG verwendet.

Änderung des Chrome-Verhaltens

In der zweiten Hälfte des Monats Oktober 2023, Google abgeschlossen die Einführung einer neuen Funktion für den Chrome-Browser. Nach diesem Datum wird automatisch eine HTTP-URL über die HTTPS-Version dieser URL angefordert. Wenn ein Benutzer beispielsweise eine Anfrage für http://www.example.com stellt, versucht Chrome zunächst, die Anfrage mithilfe von https://www.example.com zu erfüllen.

Wenn Chrome bei der Anforderung der HTTPS-URL einen HTTPS-bezogenen Fehler empfängt, versucht Chrome dann, denselben Inhalt über HTTP zu laden. Wenn die Anfrage für die HTTP-URL erfolgreich ist, zeigt Chrome eine interstitielle Seite mit Text, der darauf hinweist, dass die Website nicht sicher ist, und einen Link, der dem Benutzer die Möglichkeit gibt, fortzufahren, gemäß dem Bild unten.



Dies ist das Fallback-Verhalten in Chrome neue Funktionalität.

Wenn die HTTPS-Anforderung jedoch beim Surfen über SWG mit HTTPS-Inspektion einen HTTPS-bezogenen Fehler wie "ERR_CERT_COMMON_NAME_INVALID" von der Website verursacht, fängt SWG den Fehler ab und gibt eine SWG-Fehlerseite an Chrome zurück, z. B. die 516-Fehlerseite. Dieser SWG-Inhalt wird von Chrome nicht als ein HTTPS-bezogener Fehler angesehen, daher erzeugt er nicht das Fallback-Verhalten, und die SWG-Fehlerseite wird angezeigt, und nicht die Seite im vorherigen Bild.

Weitere Informationen zum neuen Chrome-Verhalten finden Sie im Chromium-Blog und im GitHub-Repository der Funktion.

Ermitteln der Fehlerquelle

Nachdem Chrome HTTP-URLs automatisch zu HTTPS-URLs hochstuft, werden Websites, die 516 Fehler verursachen, häufiger von Benutzern angezeigt.

Um zu bestätigen, dass eine Website verursacht einen HTTPS-bezogenen Fehler wie die 516 Antwort, durchsuchen Sie die Website mit Chrome von einem Desktop-System nicht mit Umbrella. Achten Sie darauf, die HTTPS-Version der URL manuell explizit in Chrome Omnibox (wie die Adressleiste) statt auf einen HTTP-Hyperlink. Wenn ein Hyperlink einen 516-Fehler mit SWG verursacht hat, kann die manuelle Anforderung der HTTPS-URL in Chrome ohne SWG die Fehlermeldung "ERR_CERT_COMMON_NAME_INVALID" erzeugen. Diese Fehlermeldung

bestätigt, dass das Problem ein falsches Zertifikat für den Domänennamen ist, der für den Zugriff auf die Website verwendet wird.

Alternativ können Sie ein Online-Tool wie die Qualys SSL Server Test-Website verwenden, um das Problem mit der Website zu diagnostizieren.

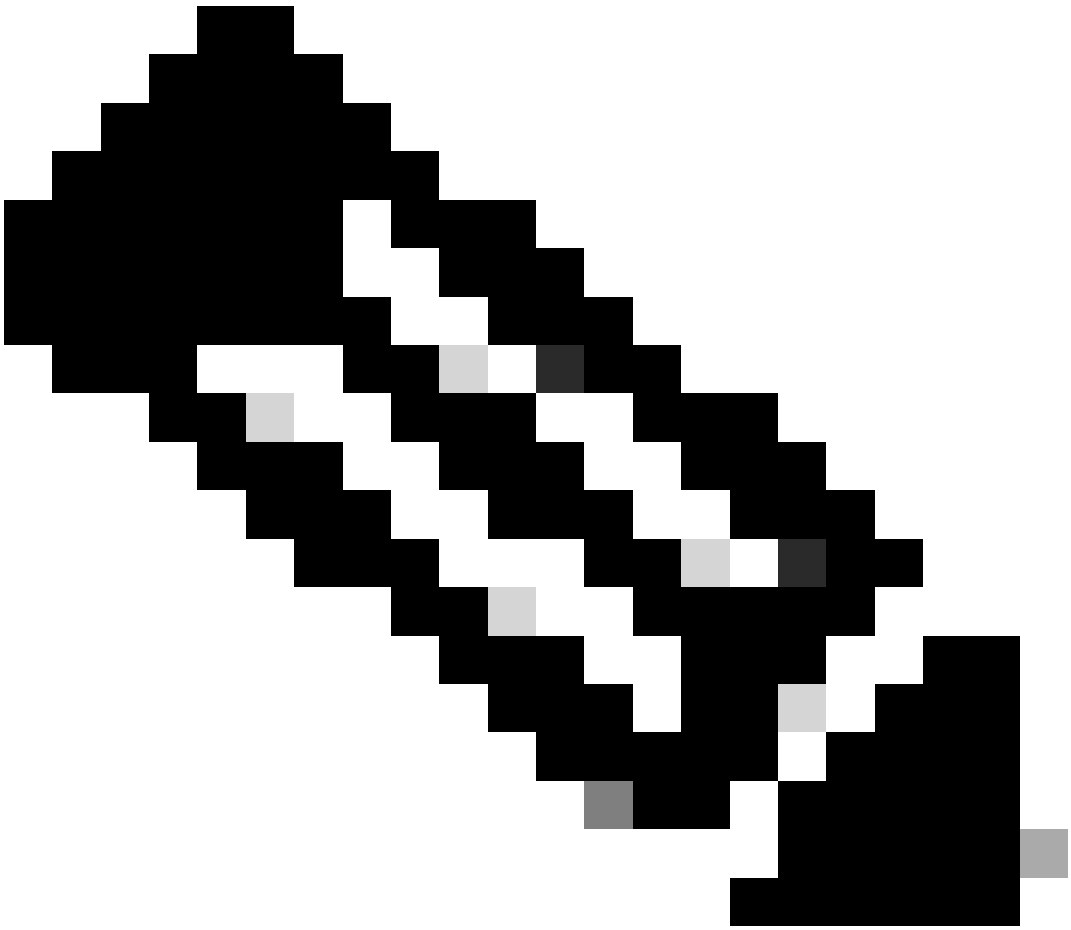
Problemumgehungen

Umbrella-Administratoren können das Problem mit einer der folgenden Optionen umgehen:

1. Erstellen Sie eine Zielliste speziell für diese Websites und fügen Sie die Liste einer Webrichtlinie ohne HTTPS-Überprüfung hinzu.

2. Erstellen Sie eine selektive Entschlüsselungsliste von Websites, die 516 Fehlerseiten erzeugen, und fügen Sie die selektive Entschlüsselungsliste allen relevanten Webrichtlinien hinzu

---



Anmerkung: Faktoren wie HTTP-Umleitungen oder E-Mail-Sicherheitssysteme, die die HTTPS-URLs des Dienstes durch die ursprünglichen HTTP-URLs ersetzen, können den erforderlichen Domänennamen verdecken. Die Identifizierung des richtigen

---

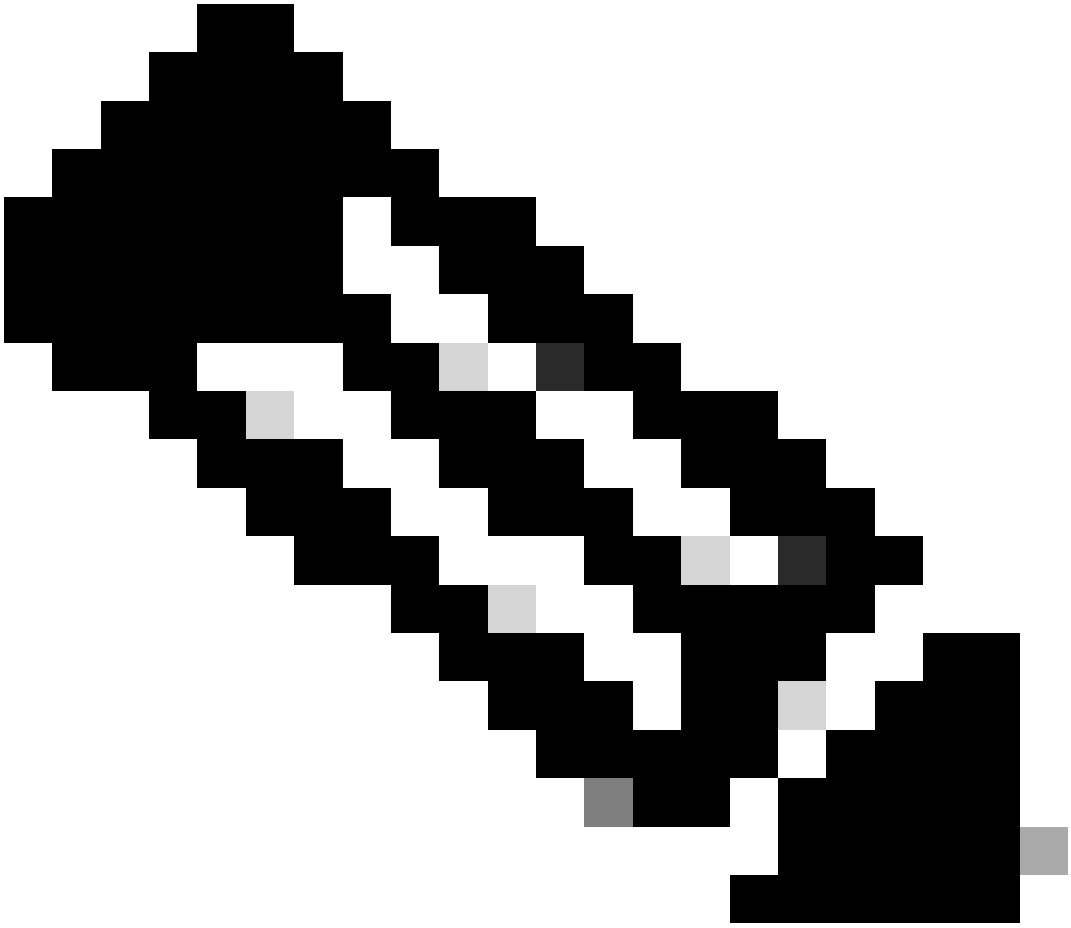
Domänennamens für eine Zielliste oder eine selektive Entschlüsselungsliste kann eine Untersuchung erfordern, einschließlich der Verwendung bestimmter Tools (curl, Chrome Developer Tools, ein E-Mail-Security-Herstellerprotokoll usw.).

516 Fehler und E-Mail-Systeme

E-Mail-Systeme, die E-Mails im HTML-Format anzeigen und Hyperlinks in den E-Mails zulassen, können die Fehlerquote um 516 erhöhen. Wenn der Absender beim Verfassen einer E-Mail einen Domänennamen eingibt oder in den E-Mail-Text einfügt, wird von vielen E-Mail-Systemen automatisch ein Nur-Text-Domänenname zu einem Hyperlink hochgestuft. Wenn der Link erstellt wird, lautet das Schema in der Regel HTTP statt HTTPS.

Wenn Sie beispielsweise die Zeichenfolge `example.com` in eine E-Mail eingeben, wird möglicherweise eine E-Mail mit dem HTML-Code <`a href="http://www.example.com">` angezeigt, der als Hyperlink www.example.com.

Wenn ein Empfänger einer solchen E-Mail auf diesen HTTP-Hyperlink klickt, verwendet die Anforderung zunächst HTTPS, wenn der Klick Chrome öffnet, oder wenn Chrome bereits zum Anzeigen der E-Mail verwendet wird.



Anmerkung: Andere Browser können auch HTTP zu HTTPS hochstufen.

Ein Hyperlink in einer E-Mail, der absichtlich das HTTP-Schema verwendet, wird ähnlich behandelt.

Einige gängige Cloud-Services senden E-Mails von externen Anbietern transaktionaler E-Mail-Services mit HTTP- statt HTTPS-Hyperlinks. Die HTTPS-Site, die Chrome automatisch zu laden versucht, kann mit einem Zertifikatfehler auf den Domänennamen im E-Mail-Link reagieren, wie in diesem Beispiel aus Seegrid.

Wenn diese E-Mails umfangreiche Empfängerlisten enthalten, können viele Benutzer, deren Klicks (oder Anfragen) über die SWG gesendet werden, Fehler wie den 516-Fehler melden. Wenden Sie sich an Ihren E-Mail-Dienstanbieter oder die Organisation, die die E-Mail gesendet hat, um den Zertifikatfehler beheben zu lassen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.