Dépannage des erreurs 516 sur Umbrella Secure Web Gateway

Table des matières

Introduction

Ce document décrit comment dépanner une augmentation de 516 erreurs sur Umbrella Secure Web Gateway.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur la passerelle Web sécurisée Umbrella (SWG).

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Aperçu

Les utilisateurs qui naviguent sur le proxy SWG (Umbrella Secure Web Gateway) avec l'inspection HTTPS peuvent recevoir plus fréquemment des pages d'erreur 516 Upstream Certificate CN Mismatch à partir de la deuxième moitié d'octobre 2023.

La page d'erreur 516 se produit lorsque le certificat d'un site Web ne correspond pas au nom de domaine utilisé par le client pour accéder au site.

L'augmentation des pages d'erreur est due à un changement dans la gestion du navigateur Chrome des demandes d'URL qui utilisent le schéma HTTP (non crypté). Chrome tente maintenant de charger la ressource avec le schéma HTTPS (chiffré) en premier. Lorsqu'il est configuré pour l'inspection HTTPS, SWG inspecte le certificat d'un site Web et retourne une page Web affichant un code d'erreur tel que 516 si le certificat n'est pas acceptable.

Pour contourner ce problème, les clients peuvent configurer leurs stratégies Web de manière à contourner l'inspection HTTPS pour les requêtes qui, sinon, entraînent 516 erreurs.

516 Erreur - Arrière-plan

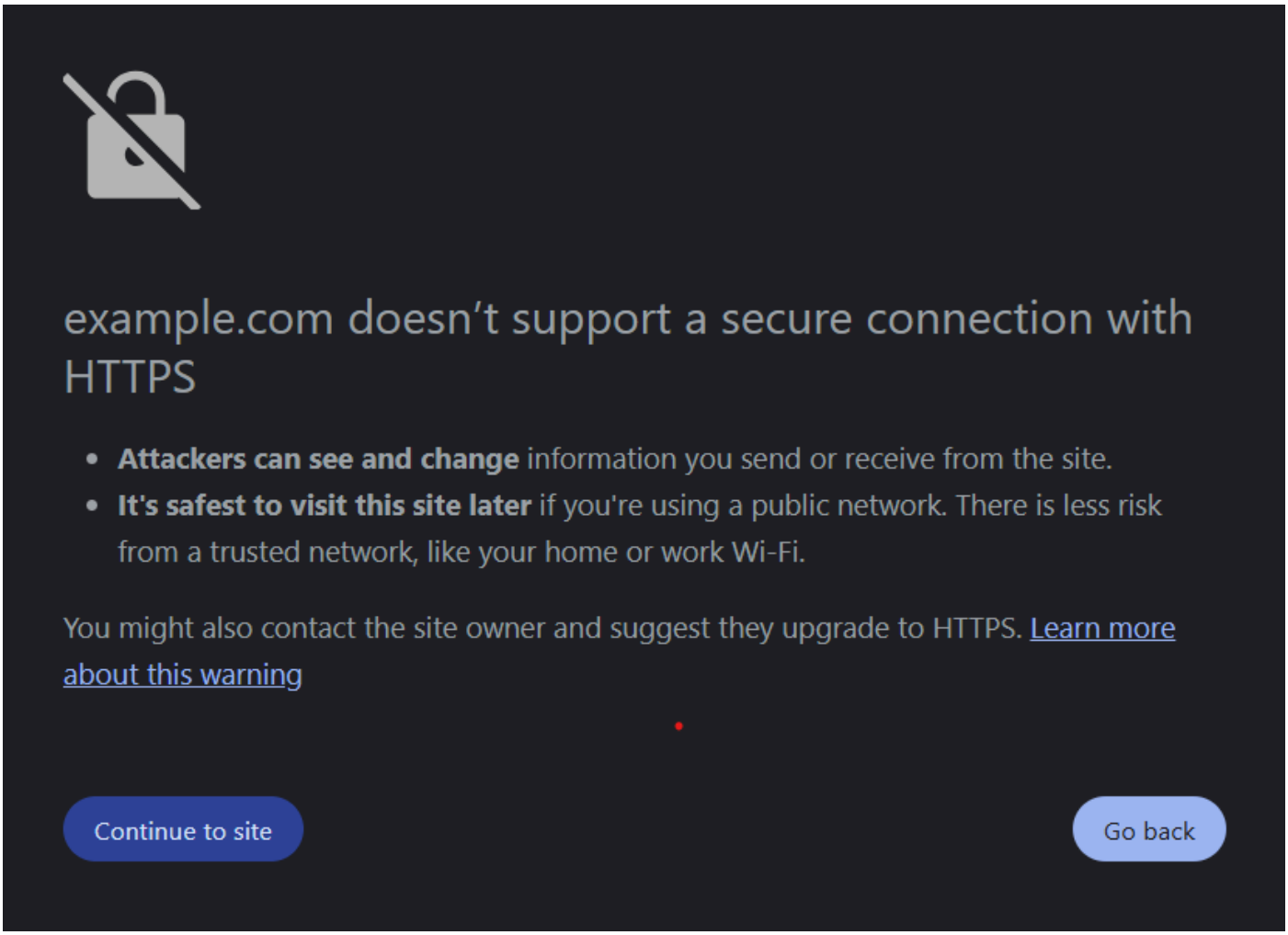
En bref, la passerelle Web Umbrella Secure renvoie une page d'erreur 516 lorsque le nom de domaine utilisé pour accéder à un site Web via HTTPS n'apparaît pas dans le certificat numérique du serveur. Pour plus d'informations sur la raison du renvoi d'une page d'erreur 516 par la passerelle Web sécurisée, consultez l'article de la base de connaissances Umbrella « 516 Upstream Certificate CN Mismatch » error.

Prenons l'exemple d'un site qui fournit du contenu à partir d'URL HTTP sous la forme suivante : http://www.example.com/path_to_content. Si un utilisateur demande les URL HTTPS équivalentes, mais que le site n'a pas de certificat dont les SAN correspondent à www.example.com (peut-être que le SAN ne correspond qu'à example.com) alors l'utilisateur reçoit une erreur 516 si la demande est traitée par la passerelle Web sécurisée d'Umbrella avec une politique Web qui utilise la fonctionnalité d'inspection HTTPS de SWG.

Modification du comportement de Chrome

Dans la seconde moitié d'Octobre 2023, Google a terminé le déploiement d'une nouvelle fonctionnalité pour le navigateur Chrome. Après cette date, une demande d'URL HTTP est automatiquement effectuée à l'aide de la version HTTPS de cette URL. Par exemple, lorsqu'un utilisateur fait une demande pour http://www.example.com, Chrome tente d'abord de répondre à la demande en utilisant https://www.example.com.

Si Chrome reçoit une erreur liée à HTTPS lors de la demande de l'URL HTTPS, Chrome tente alors de charger le même contenu sur HTTP. Si la requête pour l'URL HTTP est réussie, Chrome affiche une page interstitielle avec du texte indiquant que le site n'est pas sécurisé et un lien qui donne à l'utilisateur la possibilité de continuer, selon l'image ci-dessous.



C'est le comportement de repli dans la nouvelle fonctionnalité de Chrome.

Cependant, lors de la navigation via SWG avec l'inspection HTTPS, si la requête HTTPS produit une erreur liée à HTTPS telle que "ERR_CERT_COMMON_NAME_INVALID" à partir du site, SWG intercepte l'erreur et renvoie une page d'erreur SWG à Chrome telle que la page d'erreur 516. Ce contenu SWG n'est pas considéré comme une erreur liée à HTTPS par Chrome, ne produit donc pas le comportement de secours, et la page d'erreur SWG est affichée, plutôt que la page dans l'image précédente.

Plus d'informations sur le nouveau comportement de Chrome peuvent être trouvées sur le blog de Chrome et le dépôt GitHub de la fonctionnalité.

Détermination de la source de l'erreur

Maintenant que Chrome promeut automatiquement les URL HTTP aux URL HTTPS, les sites Web qui génèrent 516 erreurs sont vus plus fréquemment par les utilisateurs.

Pour confirmer qu'un site Web provoque une erreur liée à HTTPS telle que la réponse 516, parcourez le site avec Chrome à partir d'un système de bureau n'utilisant pas Umbrella. Assurez-vous d'entrer manuellement la version HTTPS de l'URL explicitement dans Chrome's Omnibox (comme la barre d'adresse) plutôt que de cliquer sur un lien hypertexte HTTP. Si un lien hypertexte a produit une erreur 516 avec SWG, alors demander manuellement l'URL HTTPS dans Chrome sans SWG peut produire le message d'erreur "ERR_CERT_COMMON_NAME_INVALID."

Ce message d'erreur confirme que le problème provient d'un certificat incorrect pour le nom de domaine utilisé pour accéder au site Web.

Vous pouvez également utiliser un outil en ligne tel que le site Qualys SSL Server Test pour diagnostiquer le problème sur le site Web.

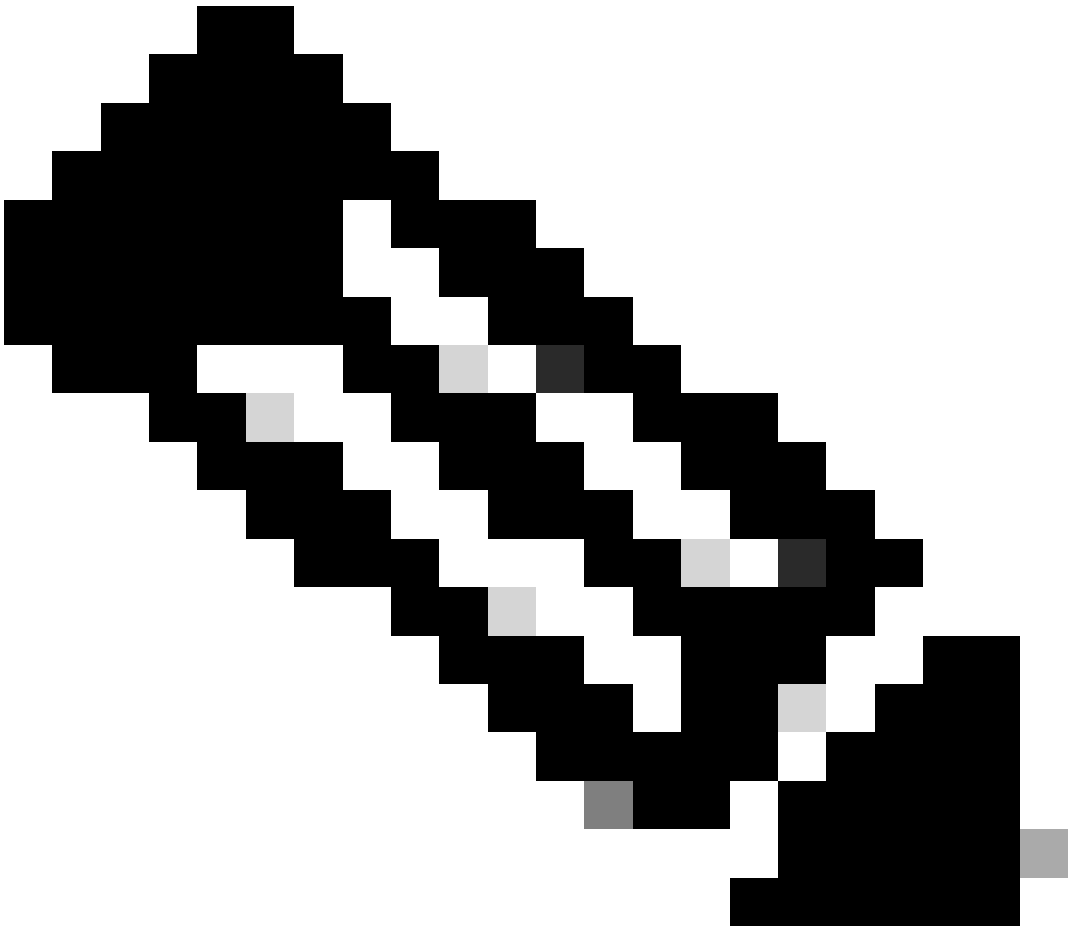
Solution De Contournement

Les administrateurs parapluie peuvent contourner le problème avec l'une des options suivantes :

1. Créez une liste de destinations spécifiquement pour ces sites et ajoutez la liste à une stratégie Web sans inspection HTTPS.

2. Créez une liste de décodage sélectif des sites qui produisent 516 pages d'erreur et ajoutez la liste de décodage sélectif à toutes les politiques Web pertinentes

---



Remarque : Des facteurs tels que les redirections HTTP ou les systèmes de sécurité de la messagerie électronique qui substituent les URL HTTPS de leur service aux URL HTTP d'origine peuvent masquer le nom de domaine requis. L'identification du nom de domaine

---

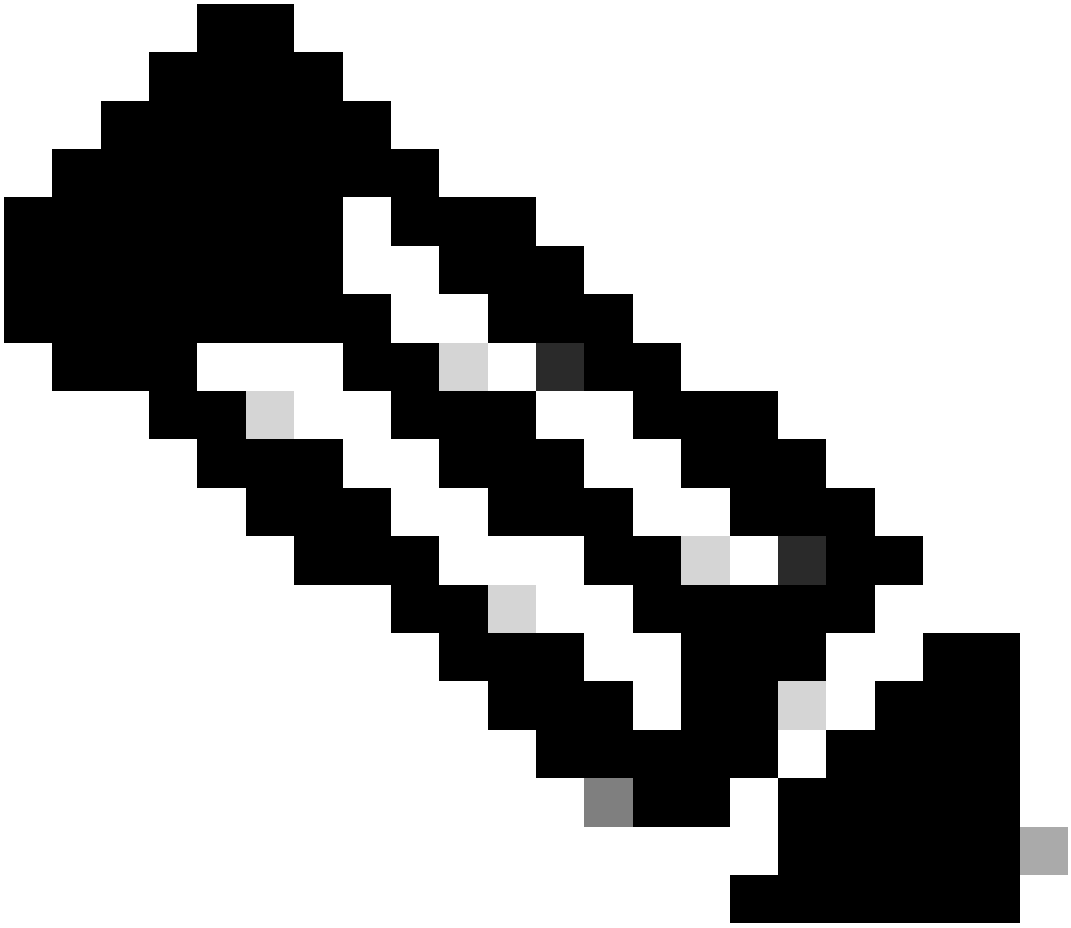
correct pour une liste de destination ou une liste de décodage sélectif peut nécessiter une enquête, y compris l'utilisation d'outils spécifiques (curl, Chrome Developer Tools, un journal d'un fournisseur de sécurité de messagerie électronique, et ainsi de suite).

516 Erreurs et systèmes de messagerie

Une augmentation de la fréquence d'erreur 516 peut résulter de systèmes de messagerie qui affichent des e-mails au format HTML et autorisent l'utilisation de liens hypertexte dans les e-mails. Lors de la composition d'un e-mail, si l'expéditeur saisit ou colle un nom de domaine dans le corps de l'e-mail, de nombreux systèmes de messagerie promeuvent automatiquement un nom de domaine en texte clair en lien hypertexte. Généralement, lorsque la liaison est créée, le modèle est HTTP plutôt que HTTPS.

Par exemple, la saisie de la chaîne `example.com` dans un e-mail peut générer un e-mail contenant le code HTML `<a href="http://www.example.com">` qui s'affiche sous la forme du lien hypertexte www.example.com.

Si un destinataire d'un tel e-mail clique sur ce lien hypertexte HTTP, la requête utilise initialement HTTPS si le clic ouvre Chrome, ou si Chrome est déjà utilisé pour afficher l'e-mail.



Remarque : D'autres navigateurs peuvent également promouvoir HTTP en HTTPS.

En outre, un lien hypertexte dans un e-mail qui utilise intentionnellement le schéma HTTP est géré de la même manière.

Certains services cloud courants envoient des e-mails provenant de fournisseurs de services de messagerie transactionnelle tiers avec des liens hypertexte HTTP plutôt que des liens hypertexte HTTPS. Le site HTTPS que Chrome tente automatiquement de charger peut répondre avec une erreur de certificat au nom de domaine dans le lien d'e-mail comme dans cet exemple de Seegrid.

Lorsque ces e-mails comportent de grandes listes de destinataires, de nombreux utilisateurs dont les clics (ou requêtes) sont envoyés via SWG peuvent signaler des erreurs telles que l'erreur 516. Veuillez contacter votre fournisseur de service de messagerie ou l'organisation qui a envoyé l'e-mail pour que l'erreur de certificat soit corrigée.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.