Résoudre l'erreur de non-concordance CN du certificat en amont 516

Table des matières

Introduction

Problème

- Mécanique d'identité de certificat
- Erreurs d'identité de certificat

Résolution

- Le nom commun est déconseillé

Additional Information

Introduction

Ce document décrit comment résoudre une erreur 516 Upstream Certificate CN Mismatch.

Problème

Lorsque le proxy SWG (Umbrella Secure Web Gateway) est configuré pour effectuer l'inspection HTTPS, un utilisateur peut recevoir une page d'erreur 516 Upstream Certificate CN Mismatch lorsqu'il navigue vers un site Web à l'aide d'une URL HTTPS.

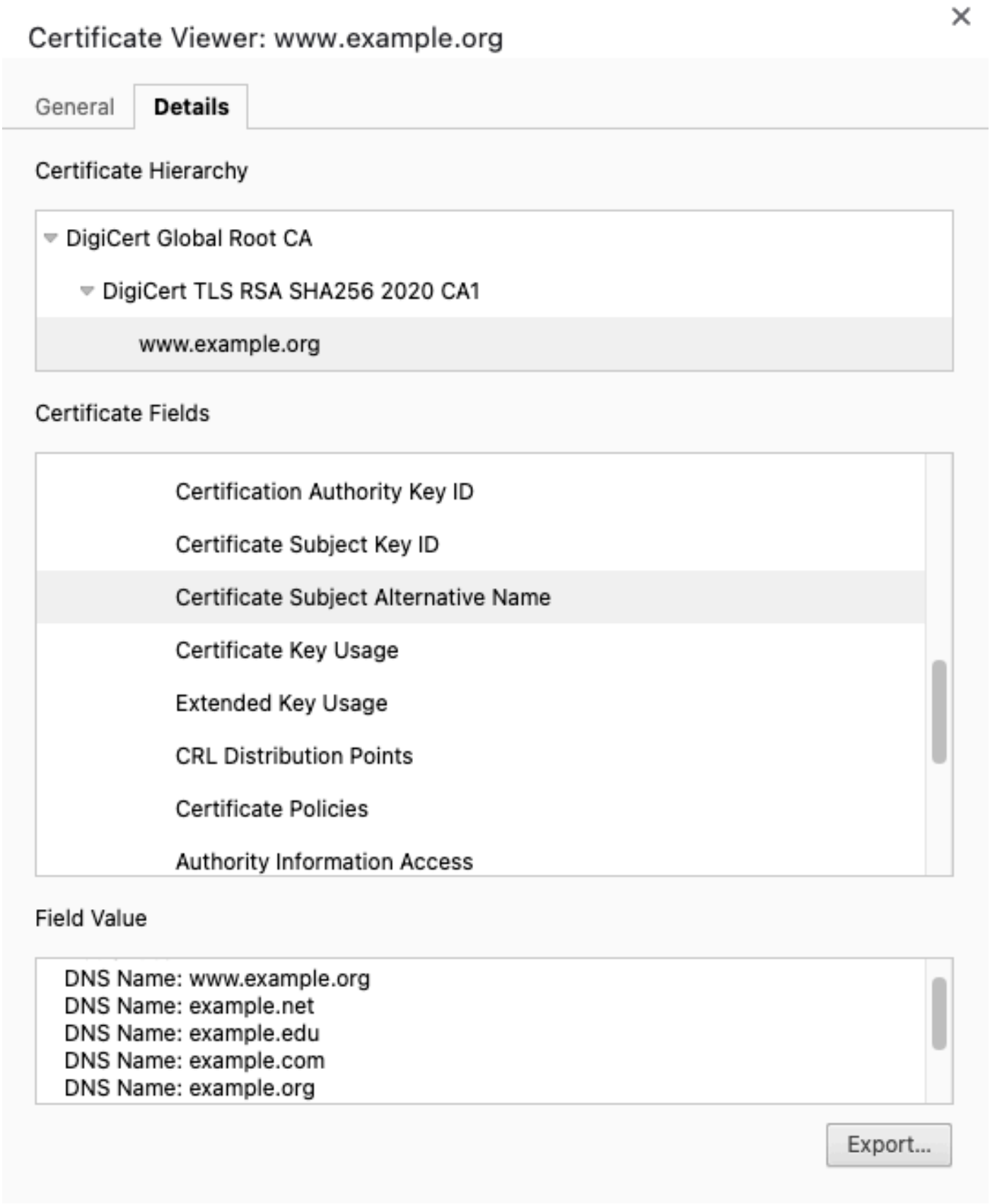
Cette erreur n'indique pas de problème avec l'attribut Common Name (CN) dans le champ Subject du certificat de site Web. Le problème se rapporte plutôt à l'attribut Nom DNS dans l'extension Sujet Autres noms (SAN) d'un certificat.

Après avoir lu cet article, si vous ne pouvez pas identifier la raison de la page d'erreur 516, veuillez contacter le support technique d'Umbrella et nous fournir les informations spécifiées dans la section Erreurs d'identité de certificat dans ce document.

Mécanique d'identité de certificat

Lors de la demande d'une URL HTTPS, un navigateur ou un autre client Web envoie le nom de domaine dans l'URL au serveur Web via l'extension Server Name Indication (SNI) dans le message Hello du client de la négociation TLS. Le serveur utilise cette valeur SNI pour sélectionner le certificat de serveur à renvoyer au client, car un serveur héberge souvent plusieurs sites Web et peut avoir des certificats différents pour certains ou tous les sites.

Lorsque le certificat de serveur est reçu par le client Web, le client vérifie que le certificat est le bon pour la demande en comparant le nom de domaine demandé au(x) nom(s) de domaine dans les attributs DNS Name de l'extension Subject Alternative Names du certificat. Cette image présente ces réseaux SAN dans un certificat de serveur.



16796247745556

Ce serveur Web renvoie ce certificat en réponse à des requêtes contenant ces valeurs SNI, ainsi que d'autres valeurs non visibles dans le panneau Valeur du champ :

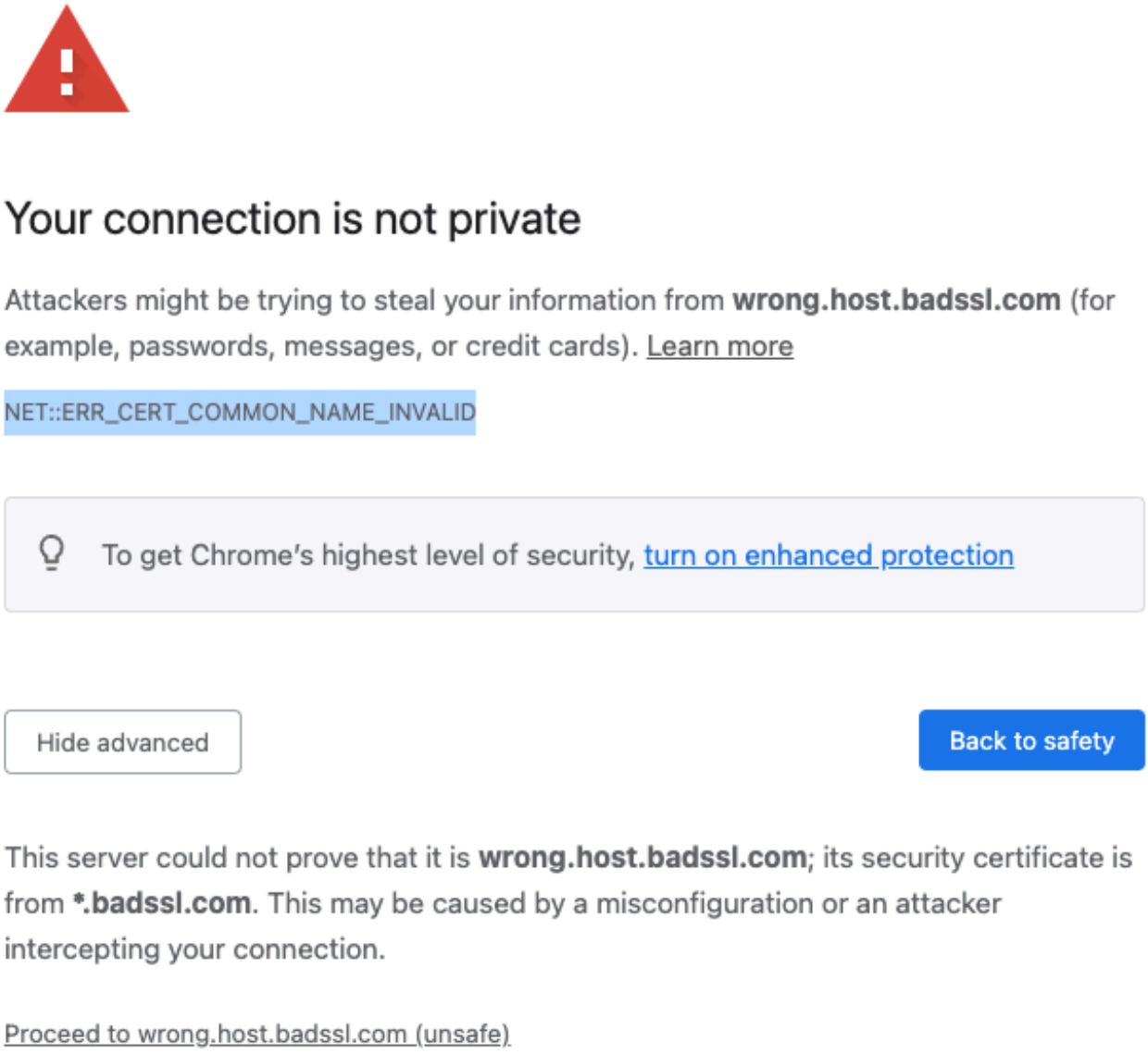
- www.example.org

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

Notez que le SAN « example.com » ne correspond pas à un SNI de « www.example.com ». Cependant, un SAN générique de "*.example.com" correspondrait à un SNI de "www.example.com", ou tout autre nom de domaine contenant une seule étiquette (une chaîne sans ".") préfixé à example.com, mais pas à plusieurs étiquettes. Par exemple, "www.hr.example.com" ne correspond pas à "*.exemple.com" car "www.hr" se compose de deux étiquettes : "www" et "hr". Un seul caractère générique ne peut correspondre qu'à une seule étiquette.

Erreurs d'identité de certificat

Lorsqu'un client Web reçoit un certificat de serveur, si aucun des noms DNS du SAN ne correspond au SNI du nom de domaine dans l'URL demandée, le client Web affiche généralement une erreur à l'intention de l'utilisateur. Cette image montre Chrome affichant une page interstitielle "NET::ERR_CERT_COMMON_NAME_INVALID".



16794294817428

Dans l'image, le site demandé était "https://wrong.host.badssl.com" qui ne correspond à aucun des SAN. Le certificat contient un nom DNS SAN générique, « *.badssl.com », dont le caractère générique ne peut correspondre qu'à une seule étiquette, telle que « host ». En outre, le certificat ne possède pas de nom DNS SAN avec la valeur exacte « error.host.badssl.com » ou un SAN générique de « *.host.badssl.com », de sorte que l'utilisateur se voit présenter cette erreur.

Pour identifier la raison d'une non-correspondance d'identité de certificat, examinez les noms DNS SAN du certificat à l'aide de la fonction d'affichage de certificat du navigateur et comparez-les au nom de domaine dans l'URL demandée. Vous pouvez également utiliser un outil tel que le Qualys SSL Server Test pour diagnostiquer un problème d'identité de certificat.

Si la raison de l'erreur 516 ne peut pas être identifiée après avoir utilisé les informations de cette section, ou si les résolutions et solutions de contournement de la section suivante ne peuvent pas

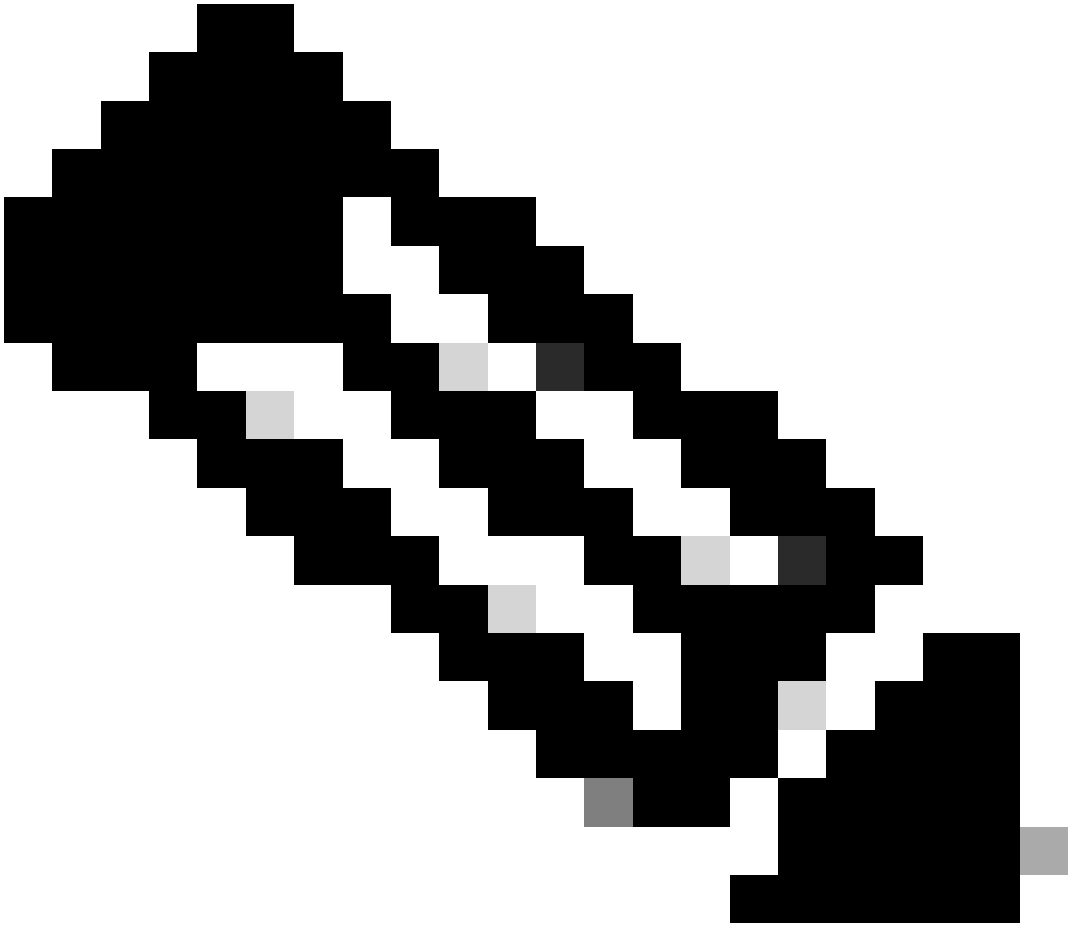
être utilisées, veuillez ouvrir un dossier avec l'assistance technique Umbrella et fournir :

1. une capture d'écran qui capture
    - la barre d'adresse du navigateur affichant l'URL demandée
    - toute la page d'erreur 516 (voir image dans la section suivante)
2. Texte de l'URL copié à partir de la barre d'adresse

Résolution

Pour résoudre ce problème, accédez au serveur avec un nom de domaine qui correspond à l'un des noms DNS SAN dans le certificat. Cela peut nécessiter que l'administrateur du site Web ajoute un nom de domaine correspondant dans le DNS de la zone. L'administrateur peut également réémettre le certificat pour inclure le nom de domaine de l'URL dans l'un des noms DNS SAN.

Pour contourner ce problème, le nom de domaine de l'URL peut être ajouté à une liste de décodage sélectif pour le proxy de passerelle Web sécurisée ou à une liste de destination dans le proxy intelligent. Appliquez la liste au paramètre de jeu de règles de stratégie Web approprié (passerelle Web sécurisée) ou à la liste verte de stratégie DNS (proxy intelligent). Cela empêche la requête au site Web d'être décryptée par le proxy, ce qui empêche le proxy d'afficher une page d'erreur 516.



Remarque : L'utilisation du proxy Secure Web Gateway et du proxy intelligent n'est pas prise en charge. Une seule technologie de proxy peut être utilisée par entreprise. Il est recommandé que les organisations disposant d'abonnements pour Secure Web Gateway utilisent SWG et non Intelligent Proxy.

Le nom commun est déconseillé

Les clients Web ont à l'origine fait correspondre le nom de domaine dans l'URL demandée à l'attribut Common Name (CN) dans le champ Subject du certificat. Ce mécanisme a été déconseillé dans les clients Web modernes ; sont maintenant comparés aux noms DNS de l'extension Subject Alternative Name. Cependant, le texte des messages d'erreur continuent souvent de faire référence au mécanisme déconseillé, comme "NET::ERR_CERT_COMMON_NAME_INVALID" dans Chrome.

De même, Umbrella SWG affiche une page d'erreur 516 avec ce texte lorsque le proxy SWG demande une URL à partir d'un serveur Web et qu'une non-correspondance de nom DNS SAN se produit :

16794325789332

Cisco Umbrella prévoit de mettre à jour ce texte à une date ultérieure afin de mieux refléter le comportement actuel.

Additional Information

Voir RFC 5280 : Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Section 4.1.2.6 pour des informations sur le sujet du certificat et Section 4.2.1.6 pour des informations sur le nom alternatif du sujet.

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.