Dépannage de l'erreur " ; 517 Certificat en amont révoqué" ;

Table des matières

Introduction

Ce document décrit comment dépanner l'erreur "517 Certificat en amont révoqué" lors de la navigation vers une URL HTTPS.

Problème

Lorsque le proxy Web Umbrella Secure Web Gateway (SWG) est configuré pour effectuer l'inspection HTTPS, un utilisateur peut recevoir une page d'erreur 517 Upstream Certificate Revoked. Cette erreur indique que le site Web demandé a envoyé un certificat numérique dans la négociation TLS qui a un statut de « révoqué » selon l'émetteur de ce certificat, ou une autorité similaire. Un certificat révoqué n'est plus valide.

13351060307092

Motif

Lorsqu'un client Umbrella effectue une requête HTTPS via la passerelle Web sécurisée Umbrella, SWG effectue des vérifications de révocation de certificat à l'aide du protocole OCSP (Online Certificate Status Protocol). OCSP indique l'état de révocation d'un certificat. SWG effectue des demandes OCSP pour l'état de révocation de certificat au nom des clients Umbrella.

SWG détermine l'état de révocation du certificat du serveur Web demandé et de tous les certificats intermédiaires émettant dans le chemin d'accès à un certificat racine approuvé. Ces vérifications permettent de s'assurer qu'une chaîne de confiance valide n'est pas devenue non valide depuis son émission.

Dans un certificat numérique qui utilise le contrôle de révocation OCSP, l'extension X.509 "Authority Information Access" contient un ou plusieurs champs "OCSP". Un champ contient une URL HTTP pour un « point d'extrémité » OCSP (serveur Web) qui peut être interrogé sur l'état de révocation du certificat. SWG envoie des requêtes à chaque URL OCSP dans un certificat jusqu'à ce qu'une réponse soit reçue, indiquant l'une des options suivantes :

- le certificat est valide (non révoqué) et SWG autorise la demande Web à continuer, OU
- autre chose qu'une réponse OCSP « certificate valid » (par exemple, le certificat est révoqué, le serveur ne peut pas répondre à l'heure actuelle, un état d'erreur HTTP, un délai d'expiration de la couche réseau/transport, etc.) à laquelle SWG présente la page/le message d'erreur approprié et la requête Web échoue

Notez que les réponses OCSP sont généralement mises en cache et utilisées pour répondre à

des vérifications ultérieures. Le temps de mise en cache est défini par le serveur dans la réponse OCSP.

Comportement différent lors de la navigation directe

Les clients Web peuvent utiliser divers mécanismes de vérification de révocation, selon le client. Par exemple, le navigateur Chrome de Google n'utilise pas par défaut les méthodes OCSP ou CRL standard. Au lieu de cela, Chrome utilise une version propriétaire d'une CRL appelée CRLSet, que Secure Web Gateway n'utilise pas. Par conséquent, Chrome peut ne pas produire le même résultat que SWG lors de la vérification de l'état de révocation d'un certificat.

Notez cependant que, comme l'indique la documentation CRLSet, « dans certains cas, la bibliothèque de certificats système sous-jacente effectue toujours ces vérifications, peu importe ce que fait Chrome. » Ainsi, en fonction de votre environnement local, une vérification OCSP et/ou CRL peut être effectuée par votre navigateur ou par les bibliothèques de services cryptographiques du système d'exploitation, telles que SChannel, Secure Transport ou NSS.

Notez également que les contrôles OCSP et CRL ne sont pas garantis pour produire le même résultat.

Consultez la documentation du fournisseur de votre navigateur ou de votre système d'exploitation pour déterminer les contrôles de révocation de certificat effectués par vos clients lors de la navigation.

Résolution

L'utilisation de certificats valides est de la responsabilité de l'administrateur du serveur Web. La correction des certificats révoqués doit être effectuée sur le serveur par l'administrateur du serveur. Cisco Umbrella ne peut pas vous aider dans ce processus.

Cisco Umbrella déconseille vivement d'accéder à un site Web qui utilise un certificat révoqué. Les solutions de contournement ne peuvent être utilisées que si l'utilisateur comprend parfaitement pourquoi un site utilise un certificat révoqué et accepte pleinement les risques.

Pour éviter l'erreur, le site peut être exempté de l'inspection HTTPS en créant une liste de décodage sélectif qui inclut le nom de domaine du site. La liste de décodage sélectif serait appliquée à la stratégie Web qui autorise l'accès au site. Vous pouvez également ajouter le site à la liste Domaines externes pour envoyer le trafic directement au site, en contournant SWG.

Additional Information

Les clients souhaitant confirmer la révocation du certificat d'un serveur peuvent utiliser des outils tiers conçus pour vérifier l'état de révocation. Plus particulièrement, l'outil SSL Server Test de Qualys SSL Labs effectue des vérifications OCSP et CRL, en plus de fournir d'autres informations de validité de certificat. L'outil est disponible en ligne à l'adresse :

- https://www.ssllabs.com/ssltest/analyze.html

Nous vous recommandons d'utiliser cet outil pour vérifier le site qui produit une erreur 517 Upstream Certificate Revoked, avant d'ouvrir un dossier d'assistance avec Cisco Umbrella.

Voir également : https://support.umbrella.com/hc/en-us/articles/4406133198100-Certificate-and-TLS-Protocol-Errors

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.