Comprendre les erreurs courantes de certificat et de protocole TLS

Table des matières

Introduction

Ce document décrit les erreurs courantes de certificat et de protocole TLS dans la recherche d'activité de tableau de bord Umbrella.

Aperçu

Le trafic HTTP bloqué en raison d'erreurs de certificat et TLS peut désormais être affiché dans la recherche d'activité du tableau de bord Umbrella. Cet article fournit une liste des messages d'erreur courants ainsi qu'une brève explication de chacune des erreurs.

Erreurs de certificat

Certificat en amont expiré

Un certificat présenté par le site Web a expiré. Contactez le webmestre du site pour signaler ce problème.

Certificat en amont auto-signé

Le certificat de serveur présenté par le site Web n'est pas signé par une autorité de certification, et par conséquent Umbrella ne peut pas déterminer si le certificat est fiable.

Les certificats auto-signés sont parfois utilisés lorsqu'un serveur héberge une ressource destinée à une audience restreinte. Par exemple, les portails Web pour les appareils de sécurité informatique utilisent souvent par défaut des certificats auto-signés. Umbrella ne peut pas être configuré pour faire confiance aux certificats auto-signés.

Certificat intermédiaire manquant

Umbrella n'a pas pu obtenir de certificats pour toutes les autorités intermédiaires et n'a donc pas pu valider l'ensemble de la chaîne de confiance.

Les certificats de serveur Web sont généralement émis/signés par le certificat intermédiaire d'une autorité de certification. Ces certificats intermédiaires peuvent également être délivrés par d'autres certificats intermédiaires. Le certificat du serveur Web (également appelé « certificat leaf ») et tout certificat intermédiaire forment une chaîne de retour vers un certificat racine. Le site Web doit regrouper le ou les certificats intermédiaires avec le certificat du serveur afin qu'Umbrella valide l'ensemble de la chaîne de confiance. Contactez le webmestre du site pour signaler ce problème.

Par ailleurs, si le certificat inclut l'extension « Authority Information Access », Umbrella tente de récupérer automatiquement les CA intermédiaires. Notez qu'Umbrella ne prend en charge l'extension AIA que lorsque le décodage HTTPS et l'inspection des fichiers sont activés.

Nom de sujet manquant dans le certificat en amont.

Le champ Objet du certificat ne contient pas de nom distinctif (DN) permettant d'identifier ce certificat. Il s'agit d'une exigence pour tous les certificats délivrés par une autorité de certification, et donc requis par Cisco Umbrella. Contactez le webmestre du site pour signaler ce problème.

Nom commun manquant dans le certificat en amont.

Le certificat présenté par le site Web n'a pas de nom commun. Le champ Nom commun (CN) est requis par Umbrella SWG. Contient le nom d'hôte du certificat, qui est requis pour valider que le certificat correspond à la ressource demandée par l'utilisateur (par ex. L'adresse saisie dans le navigateur). Contactez le webmestre du site pour signaler ce problème.

Certificat en amont non approuvé

Le certificat n'est pas approuvé par Cisco Umbrella. Cette erreur signifie généralement que Cisco ne fait pas confiance à l'autorité de certification racine qui a émis le certificat.

Umbrella SWG dispose d'une liste intégrée d'autorités de certification racine de confiance connues que nous mettons à jour à partir d'une source fiable. Si le certificat des sites Web n'est pas signé par une autorité de certification de cette liste, la validation du certificat échoue. Si vous pensez qu'il manque une autorité de certification racine à Umbrella, contactez le support technique.

Le nom d'hôte du certificat est différent de celui attendu

La ressource demandée par l'utilisateur (par ex. l'adresse saisie dans le navigateur) ne correspond pas au nom commun (CN) ou au nom alternatif de l'objet (SAN) du certificat. Par conséquent, Umbrella ne peut pas faire confiance au certificat pour cette demande. Contactez le webmestre du site pour signaler ce problème.

Certificat en amont révoqué

Le certificat fourni par le site Web a été révoqué par l'autorité de certification émettrice.

Umbrella effectue des contrôles OCSP (Online Certificate Status Protocol) pour déterminer si un certificat a été ultérieurement révoqué par une autorité de certification. Contactez le webmestre du site pour signaler ce problème.

Erreurs de connexion TLS

Chiffrement en amont non pris en charge

La connexion TLS n'a pas pu être terminée. Cela signifie généralement que le site Web ne prend en charge aucune des suites de chiffrement utilisées par Umbrella SWG. Cette erreur peut se produire avec des serveurs Web plus anciens ou obsolètes qui ne prennent en charge que des chiffrements TLS plus faibles. Contactez le webmestre du site pour signaler ce problème.

Incompatibilité de version TLS en amont

La connexion TLS n'a pas pu être effectuée car le site Web ne prend pas en charge la même version TLS que celle utilisée par Umbrella SWG. À l'heure actuelle, le proxy SWG Umbrella prend en charge TLS 1.2 et TLS 1.3 à la fois sur les connexions côté client à Umbrella SWG et également sur les connexions proxy SWG Umbrella aux serveurs Web de destination.

Clé DH en amont inférieure à 1 024 bits

La connexion TLS n'a pas pu être effectuée car le site Web utilise une clé Diffie-Hellman faible qui n'est pas prise en charge par Umbrella. Contactez le webmestre du site pour signaler ce problème.

Solution De Contournement

Il est possible de contourner ces problèmes en modifiant la configuration dans Cisco Umbrella. Cela ne doit être fait que si vous faites confiance à l'authenticité du serveur et du certificat.

Les solutions de contournement peuvent être appliquées à l'aide d'une entrée « Liste de décodage sélectif » pour désactiver le décodage ou d'une entrée « Domaines externes » pour contourner entièrement le trafic d'Umbrella. Umbrella n'effectue pas de validation de certificat lorsque le déchiffrement est désactivé. Sachez que dans la plupart des cas, le navigateur

présente toujours une erreur ou un avertissement lorsque le trafic est contourné à partir d'Umbrella - les navigateurs Web effectuent une validation de certificat similaire.

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.