

Comprendre les erreurs de certificat SSL et de connexion dans Secure Access

Table des matières

Problème

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. Cet article fournit une liste des messages d'erreur courants ainsi qu'une brève explication de chacune des erreurs.

Environnement

- Cisco Secure Access : inspection SSL de la passerelle Web sécurisée

Résolution

Certificat en amont expiré

Le certificat du site Web a dépassé sa date d'expiration, donc Cisco Secure Access ne lui fait pas confiance. Celui-ci est sur le propriétaire du site à réparer, donc contactez le webmaster du site et faites-le savoir.

Certificat en amont auto-signé

Le site Web présente un certificat qu'il a lui-même signé, plutôt qu'un certificat émis par une

autorité de certification de confiance. Étant donné qu'aucune autorité indépendante ne se porte garante, Cisco Secure Access n'a aucun moyen de confirmer l'authenticité du certificat.

Vous voyez souvent des certificats auto-signés sur des ressources destinées à un petit public interne. Les portails d'administration sur les appliances de sécurité informatique en sont un exemple classique. Notez simplement que Cisco Secure Access ne peut pas être configuré pour faire confiance aux certificats auto-signés.

Certificat intermédiaire manquant

Cisco Secure Access n'a pas pu rassembler tous les certificats intermédiaires dont il a besoin. Il ne peut donc pas reconstruire la chaîne complète de confiance à la racine.

Voici pourquoi cela est important : le certificat d'un site web (le « leaf ») est signé par un certificat intermédiaire, qui peut à son tour être signé par un autre intermédiaire, et ainsi de suite jusqu'à une racine de confiance. Pour que cette chaîne puisse s'enregistrer, le site Web doit envoyer son ou ses certificats intermédiaires en même temps que les siens. Lorsque ceux-ci sont manquants, la validation s'arrête — donc faites savoir au webmaster du site.

Il y a une exception : si le certificat inclut l'extension « Authority Information Access » (AIA), Cisco Secure Access peut essayer de récupérer les intermédiaires manquants par lui-même. Gardez à l'esprit que cela ne fonctionne que lorsque le décodage HTTPS et l'inspection de fichier sont activés.

Nom de sujet manquant dans le certificat en amont

Le certificat n'inclut pas de nom de sujet (nom distinctif) ou de nom alternatif de sujet, ce qui signifie qu'il n'y a rien qui identifie clairement à qui le certificat appartient. Sans cela, Cisco Secure Access ne peut pas le valider. C'est quelque chose que le propriétaire du site doit corriger.

Nom commun manquant dans le certificat en amont

Le certificat n'a pas de nom commun (CN) : champ qui contenait traditionnellement le nom d'hôte du site et permettait de confirmer que le certificat appartient bien au site que vous visitez. De nos jours, cette vérification dépend vraiment du nom alternatif de l'objet (SAN), et CN est considéré

comme un champ hérité, mais son absence peut toujours déclencher cette erreur. Contactez le webmestre pour qu'il s'en occupe.

Certificat en amont non approuvé

Cisco Secure Access ne fait pas confiance à ce certificat, généralement parce qu'il ne reconnaît pas l'autorité de certification racine qui l'a émis.

Cisco Secure Access SWG conserve une liste intégrée d'autorités de certification racine de confiance, provenant d'un fournisseur réputé et tenue à jour. Si le certificat d'un site est retracé vers une autorité de certification qui ne figure pas dans cette liste, la validation échoue. Si vous êtes sûr que l'autorité de certification racine est fiable, contactez le support technique et nous pourrons y jeter un oeil.

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

L'adresse que vous avez demandée ne correspond pas au nom figurant sur le certificat, ni à son nom commun (CN), ni à aucun de ses autres noms d'objet (SAN). Puisque le certificat ne semble pas appartenir au site que vous atteignez, Cisco Secure Access ne lui fait pas confiance pour cette demande. Le webmaster doit régler ça.

Certificat en amont révoqué

L'autorité de certification qui a délivré ce certificat l'a depuis révoqué, c'est-à-dire qu'il n'est plus considéré comme valide.

Cisco Secure Access le confirme à l'aide du protocole OSCP (Online Certificate Status Protocol), qui vérifie en temps réel si un certificat a été révoqué. Informez le webmestre du site afin qu'il puisse le remplacer.

Erreurs de connexion TLS

Chiffrement en amont non pris en charge

La connexion TLS n'a pas pu être effectuée car le site Web ne prend en charge aucune des suites de chiffrement utilisées par Cisco Secure Access SWG. Cela a tendance à apparaître avec des serveurs plus anciens ou obsolètes qui n'offrent que des chiffrements plus faibles. Le correctif se trouve du côté du serveur, donc transmettez-le au webmaster.

Incompatibilité de version TLS en amont

La connexion a échoué car le site Web n'utilise pas une version TLS prise en charge par Cisco Secure Access SWG. Actuellement, le proxy SWG d'accès sécurisé Cisco fonctionne avec TLS 1.2 et TLS 1.3, à la fois pour les connexions provenant des clients et pour les connexions qu'il établit avec les serveurs de destination.

Clé DH en amont inférieure à 1 024 bits

La connexion n'a pas pu se terminer car le site Web utilise une clé Diffie-Hellman trop faible (moins de 1 024 bits) pour que Cisco Secure Access l'accepte. Il s'agit d'une limitation côté serveur, donc le webmaster doit la renforcer.

Solution De Contournement

Il est possible de contourner ces problèmes en modifiant la configuration dans Cisco Secure Access.

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 provenant de Cisco Secure Access. L'accès sécurisé Cisco 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 de Cisco Secure Access - les navigateurs Web effectuent une validation de certificat similaire.

Motif

Le proxy d'inspection SSL d'accès sécurisé Cisco n'a pas pu terminer la connexion TLS, généralement parce que la destination utilise l'épingle de certificat qui rejette le certificat résigné CSA.

- Épingle de certificat : code matériel client - empreinte cert attendue
- CSA CA non approuvé sur le terminal : certificat CA d'inspection non déployé vers le magasin racine approuvé

Autres informations utiles

- [Assistance technique de Cisco et téléchargements](#)

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.