

Gestion des erreurs de certificat de déchiffrement SSL dans l'accès sécurisé

Table des matières

Problème

Les utilisateurs rencontrent des pages d'erreur liées aux certificats lorsque le déchiffrement SSL est activé dans Cisco Secure Access. Plusieurs demandes ont été reçues concernant trois types d'erreurs de certificat :

- Erreurs expirées du certificat du serveur d'origine
- Erreurs de non-concordance CN/SAN de certificat lorsque le nom commun ou les noms de remplacement de sujet répertoriés sur le certificat ne correspondent pas au domaine accédé
- Lien de liste de révocation de certificats (CRL) intégré dans le certificat du serveur d'origine, provoquant des problèmes de connectivité

Ces erreurs de certificat sont similaires aux avertissements normalement affichés dans les navigateurs Web. La question se pose de savoir si Cisco Secure Access peut gérer les erreurs liées aux certificats en affichant des pages d'avertissement (similaires aux navigateurs ou aux filtres de contenu), puis en autorisant l'accès après l'affichage de l'avertissement, ou en autorisant l'accès dans tous les cas. En outre, il est nécessaire de comprendre le comportement lorsque le déchiffrement SSL est désactivé et si le trafic transite, quels que soient les problèmes de certificat.

Environnement

- Accès sécurisé Cisco - Accès Internet (module d'itinérance, VA, DNS, SWG, PAC, IPS, certificats)
- Fonction de déchiffrement SSL activée
- Plusieurs domaines rencontrant des problèmes de validation de certificat
- Serveurs d'origine avec divers problèmes de certificat, notamment expiration et non-

Résolution

Limites de gestion des erreurs de certificat

La gestion des erreurs liées aux certificats n'est pas disponible dans Cisco Secure Access. Le produit ne prend pas en charge :

- Présentation de pages d'avertissement de type navigateur pour les problèmes de certificat
- Configuration du traitement des erreurs de certificat spécifiques au domaine
- Traitement personnalisé des erreurs en fonction des domaines de destination
- Pages d'avertissement de type filtre de contenu avec options de remplacement utilisateur

Solution d'exclusion de déchiffrement SSL

L'approche recommandée consiste à exclure les domaines problématiques du déchiffrement SSL à l'aide des paramètres de déchiffrement du profil de sécurité. Vous pouvez le configurer via :

Accédez à la section Profil de sécurité > Paramètres de décodage pour exclure des domaines spécifiques de l'inspection SSL.

Lorsque des domaines sont exclus du déchiffrement SSL, ce comportement se produit :

- Le trafic des domaines exclus contourne entièrement l'inspection SSL
- La validation du certificat n'est pas effectuée par Secure Access
- Les utilisateurs ne rencontrent pas les pages d'erreur de certificat générées par Secure Access
- Les erreurs de certificat d'origine sont peut-être toujours visibles dans le navigateur de l'utilisateur si les problèmes de certificat persistent

Comportement de décodage SSL désactivé

Lorsque le déchiffrement SSL est désactivé pour un domaine ou globalement, Cisco Secure Access transmet le trafic (transfert), quels que soient les problèmes de certificat. Le produit n'inspecte pas ou ne valide pas les certificats lorsque le déchiffrement n'est pas activé, ce qui permet à tout le trafic HTTPS de passer de manière transparente.

Motif

Les erreurs de certificat sont causées par des problèmes de validation de certificat légitimes sur les serveurs d'origine, y compris des certificats expirés, des incohérences CN/SAN et des problèmes de connectivité CRL. Cisco Secure Access procède à la validation des certificats dans le cadre de son processus de déchiffrement SSL. Lorsque ces échecs de validation se produisent, le produit génère des pages d'erreur pour empêcher les connexions potentiellement non sécurisées. Il s'agit du comportement de sécurité prévu de la fonctionnalité d'inspection SSL.

Autres informations utiles

- [Documentation de configuration du décodage Cisco Secure Access](#)
- [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.