# CRYPTO_INTERNAL_ERROR pendant les téléchargements sécurisés de Google Drive

## Table des matières

## Problème

Les fichiers cryptés Google Sheets ne peuvent pas s'ouvrir lorsqu'ils sont accessibles via Cisco Secure Access avec le déchiffrement du trafic activé. Les utilisateurs rencontrent une erreur CRYPTO_INTERNAL_ERROR pendant les téléchargements sécurisés de Google Drive. Ce problème se produit spécifiquement lorsque l'inspection Secure Web Gateway (SWG) est active, car les en-têtes Range sont ignorés lors du processus de déchiffrement et d'inspection, ce qui entraîne une interférence avec le mécanisme de téléchargement sécurisé de Google.

Le problème affecte les environnements utilisant l'implémentation RAVPN+ZTA et affecte l'accès aux Google Sheets cryptés pour les grandes populations d'utilisateurs.

## Environnement

- Technologie : Accès sécurisé Cisco (assistance pour les solutions)
- Sous-technologie : Accès sécurisé
- Mise en oeuvre : RAVPN+ZTA (accès à distance VPN + accès sans confiance)
- Composant affecté : Profil ZTA
- Domaines affectés : clients6.google.com et autres domaines liés à Google Drive

## Résolution

La résolution implique la mise en oeuvre de solutions de contournement temporaires tout en

surveillant les correctifs permanents côté fournisseur.

Les approches décrites dans les sections suivantes ont été validées pour restaurer l'accès aux Google Sheets chiffrés.

## Options de contournement temporaire

Option 1: Désactiver le décodage du trafic

Désactivez complètement le déchiffrement du trafic pour les groupes d'utilisateurs ou les stratégies affectés. Cela restaure l'accès à Google Sheets, mais supprime toutes les fonctionnalités d'inspection de sécurité basées sur le décryptage.

Option 2: Exclure les domaines Google Drive du déchiffrement

Ajoutez des domaines liés à Google Drive à la liste de non-déchiffrement dans la configuration de stratégie d'accès sécurisé :

- clients6.google.com
- Autres domaines liés à Google Drive identifiés dans l'analyse du trafic

Cette approche maintient le déchiffrement pour le reste du trafic tout en permettant aux feuilles Google de fonctionner normalement. Cependant, cette solution de contournement a l'avantage de désactiver la fonctionnalité de blocage de chargement de Google Drive CASB pour les domaines exclus.

## Analyse technique et surveillance

L'analyse Cisco a confirmé que l'inspection Secure Web Gateway ignore les en-têtes Range pour permettre une analyse de sécurité complète du contenu des fichiers. Ce comportement interfère avec le processus de téléchargement sécurisé de Google Drive, qui repose sur les en-têtes

Range pour un flux de décryptage approprié.

Google a reconnu le problème et a identifié que le comportement du proxy (y compris Cisco Umbrella/proxy réseau) interfère avec les demandes de téléchargement sécurisé de Google Drive en supprimant ou en réécrivant les en-têtes Range. Cela force un téléchargement de fichier complet qui rompt le mécanisme de déchiffrement de Google. Google développe une solution côté client, bien qu'aucune heure d'arrivée estimée n'ait été fournie.

### Considérations relatives à la mise en œuvre

Les entreprises qui mettent en oeuvre des solutions de contournement doivent tenir compte des implications en matière de sécurité :

- Évaluer le risque d'exclusion des domaines Google Drive de l'inspection de déchiffrement.
- Examiner les politiques CASB qui peuvent être affectées par les exclusions de domaine.
- Documenter la nature temporaire de la solution de contournement pour les révisions futures des stratégies.
- Surveillez les mises à jour de Google concernant le développement de correctifs côté client.

## Motif

La cause principale est un problème de compatibilité entre le comportement d'inspection de Cisco Secure Access SWG et le mécanisme de téléchargement sécurisé de Google Drive.

Plus précisément :

L'inspection de la passerelle Web sécurisée Cisco ignore les en-têtes Range lors du processus de déchiffrement et d'analyse de sécurité pour garantir une analyse complète des fichiers. Cependant, l'accès aux fichiers cryptés Google Drive dépend des en-têtes Range pour gérer correctement le flux de décryptage pour des téléchargements sécurisés. Lorsque ces en-têtes sont supprimés ou modifiés pendant le processus d'inspection du proxy, le déchiffrement côté client de Google échoue, ce qui entraîne l'erreur CRYPTO_INTERNAL_ERROR.

Cela représente une incompatibilité fondamentale entre les exigences d'inspection de sécurité

(analyse complète des fichiers) et le mécanisme de livraison de fichiers cryptés de Google (téléchargements sécurisés basés sur la plage).

## 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.