# Configuration de l'option Ne pas décrypter SSE pour contourner le décryptage IPS et SWG

## Table des matières

## Problème

Le trafic HTTPS vers les destinations de catégorie Finance continue à présenter un certificat Cisco SSE au lieu du certificat du site Web d'origine, même après l'ajout de la catégorie Finance ou de domaines spécifiques à une liste DND (Do Not Decrypt) et l'application de la règle d'accès appropriée. Ce comportement est observé lors de l'accès à des sites via le client Zero Trust Access (TIA), ce qui a un impact particulier sur l'accès à des sites Web liés à la finance tels que https://onlinesbi.sbi.bank.in/ où une visibilité de bout en bout des certificats est requise.

Le comportement attendu est que lorsqu'un site ou une catégorie de contenu est ajouté à la liste DND, le certificat du site Web d'origine peut être présenté au navigateur au lieu du certificat Cisco SSE. Cependant, le certificat Cisco SSE continue d'être présenté, ce qui indique que le déchiffrement du trafic est toujours en cours malgré la configuration DND.

## Environnement

- Cisco Secure Service Edge (SSE)
- Connectivité TIA (Zero Trust Access Client)
- Déchiffrement IPS global activé
- IPS actif sur les stratégies d'accès
- Catégorie Finance configurée dans la liste Ne pas déchiffrer dans le profil de sécurité
- Règles d'accès appliquées avec les profils de sécurité correspondants

## Résolution

La résolution implique de comprendre que Cisco SSE effectue deux types de déchiffrement

distincts et de configurer les paramètres Ne pas déchiffrer appropriés pour les deux types de déchiffrement.

## Présentation des types de décodage SSE

Cisco SSE exécute deux processus de déchiffrement distincts :

- Déchiffrement SWG (Secure Web Gateway) - Déchiffrement de proxy Web
- Déchiffrement IPS - Déchiffrement du système de prévention des intrusions

Les entrées Ne pas déchiffrer configurées dans un profil de sécurité s'appliquent uniquement au déchiffrement SWG et n'empêchent pas le déchiffrement IPS. Lorsque le décryptage IPS global est activé et qu'IPS est actif sur n'importe quelle stratégie d'accès, le décryptage IPS se produit toujours, ce qui entraîne la présentation du certificat Cisco SSE au navigateur.

## Configuration Steps

Étape 1: Ajoutez des sites ou des catégories de contenu à la liste de non-décodage fournie par le système.

La liste de refus de déchiffrement fournie par le système est appliquée à tous les profils IPS. L'ajout d'un site ou d'une catégorie de contenu à cette liste fournie par le système entraîne la présentation du certificat du site Web d'origine, contournant ainsi le déchiffrement IPS.

Étape 2: Vérifiez qu'aucune modification de stratégie supplémentaire n'est requise.

Il n'est pas nécessaire de faire référence à la liste de non-déchiffrement fournie par le système dans les stratégies d'accès. La liste est automatiquement appliquée à tous les profils IPS.

## Test de validation

Ces méthodes de validation peuvent être utilisées pour confirmer la configuration appropriée :

Méthode 1 : Ajouter un domaine à la liste de non-déchiffrement fournie par le système

L'ajout du domaine spécifique à la liste de non-déchiffrement fournie par le système peut entraîner la présentation du certificat du site Web d'origine au lieu du certificat Cisco SSE.

Méthode 2 : Désactivation temporaire du décodage IPS global (pour test uniquement)

La désactivation temporaire du déchiffrement IPS global entraîne également l'affichage du certificat d'origine pour le site testé, confirmant que le déchiffrement IPS est la cause de la présentation du certificat Cisco SSE.

### Résultats attendus

Après une configuration correcte :

- Les sites ou catégories de contenu ajoutés à la liste de non-décodage fournie par le système présentent leurs certificats de site Web d'origine.
- Le décryptage SWG et IPS est ignoré pour les sites ou catégories spécifiés.
- Le navigateur affiche le certificat du site Web réel au lieu du certificat Cisco SSE.

## Motif

Le problème se produit parce que Cisco SSE effectue deux processus de déchiffrement distincts : Décryptage SWG et décryptage IPS. Ne pas décrypter les entrées configurées dans les profils de sécurité ne contournent que le décryptage SWG. Lorsque le décryptage IPS global est activé et qu'IPS est actif sur les stratégies d'accès, le décryptage IPS continue de se produire indépendamment, ce qui entraîne la présentation du certificat Cisco SSE au navigateur même lorsque les sites sont inclus dans les listes DND du profil de sécurité.

Pour contourner complètement les deux types de décryptage, des sites ou des catégories de contenu doivent être ajoutés à la liste de non-décryptage fournie par le système, qui s'applique à tous les profils IPS et empêche le décryptage SWG et IPS.

## Autres informations utiles

- Créer une liste de refus de déchiffrement efficace pour un accès sécurisé
- Dépannage et collecte des informations de base pour un accès sécurisé
- 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.