Dépannage des problèmes d'accès au site Web Secure Web Gateway SWG

Table des matières

Introduction

Ce document décrit la méthodologie structurée pour diagnostiquer les problèmes d'accès aux sites Web lorsqu'ils sont routés via un proxy basé sur le cloud (Secure Web Gateway/SWG), mais pas lors de l'utilisation de l'accès direct à Internet (DIA).

- Portée : S'applique à Cisco Umbrella SIG et à Cisco Secure Access.

Conditions préalables et mises en garde importantes

- Vérifiez que tous les dépannages sont effectués sur des problèmes reproductibles.
- Collectez un fichier HAR (HTTP Archive) et une capture de paquets (PCAP) simultanée pour fournir des données précises à des fins d'analyse.
- Les modifications apportées aux politiques de proxy (par exemple, contournement du décodage ou de l'inspection) peuvent avoir une incidence sur la position de sécurité ; ne s'applique qu'au dépannage ou comme recommandé.

Identifier les erreurs de niveau proxy

Les indicateurs d'interférence proxy courants sont les suivants :

- 502 Passerelle incorrecte
- 515 Certificat en amont non approuvé
- 517 Certificat en amont révoqué
- 403 Interdit
- Certificats révoqués
- Discordances de la suite de chiffrements
- Délais de connexion au site Web

Méthodologie de dépannage

Étape 1: Confirmer que le trafic traverse le proxy

- Collecte de données : Générez un fichier HAR et PCAP lorsque le problème se produit.
- Analyse des en-têtes : Inspectez l'en-tête Via dans les réponses HTTP. La présence de `s_proxy` (proxy Nginx) ou de `m_proxy` (service proxy modulaire/MPS) confirme que le trafic est mis en proxy.
- Flux TCP : Dans Wireshark, suivez le flux TCP pour vous assurer que la connexion est à l'adresse IP du proxy et non à l'adresse IP de destination.

Étape 2: Vérifier l'état de décodage TLS

- Inspection du navigateur : Cliquez sur l'icône de verrouillage dans la barre d'adresse du navigateur. Si le certificat racine d'accès sécurisé Cisco apparaît dans la chaîne de certificats, l'inspection HTTPS est active.
- Validation : Référencez les en-têtes Via dans les fichiers HAR/PCAP.
- Commande OpenSSL : Pour inspecter les chaînes de certificats :
  `openssl s_client -connect www.example.com:443 -showcerts`
  Cette commande vérifie la chaîne de certificats présentée par le serveur. Exécutez-le à partir d'une machine qui traverse le proxy pour une validation directe.

Étape 3: Isolement et processus d'élimination

1. Phase A - Test de l'inspection HTTPS (couche Nginx) :
   - Ajoutez le domaine problématique à la liste SWG « Do Not Decrypt ».
   - Laissez l'inspection des fichiers activée.
   - Si le problème est résolu : La cause principale est probablement l'inspection SSL/TLS de Nginx. Analysez le PCAP pour détecter les incohérences de chiffrement ou les problèmes SNI. Utilisez `curl` avec et sans proxy pour comparer le comportement.
   - Si le problème persiste : Passez à la phase B.
2. Phase B - Inspection des fichiers de test (couche d'analyse) :
   - Désactivez l'inspection des fichiers pour le trafic spécifique.
   - Si le problème est résolu : La cause principale se trouve dans le moteur d'analyse de fichiers. Examinez les protocoles PCAP et HAR, effectuez une reproduction en TP et déterminez si un fichier ou une signature d'analyse spécifique déclenche le problème.
   - Si le problème n'est pas résolu : contactez le support technique pour obtenir des journaux et des résultats complets.

Problèmes courants et codes d'erreur

515 Certificat en amont non approuvé

Cette erreur se produit lorsque le proxy SWG ne peut pas valider le certificat du serveur de destination. Les causes incluent des chaînes de certificats expirées, auto-signées ou incomplètes.

- Inspection HTTPS ACTIVÉE + Inspection de fichier ACTIVÉE : Travaux de site Web ; aucune erreur de certificat.
- Inspection HTTPS ACTIVÉE + Inspection des fichiers DÉSACTIVÉE : Erreur 515 observée, rapport d'utilisateur correspondant.
- HTTPS Inspection OFF + File Inspection OFF (domaine sur la liste Ne pas déchiffrer) : Aucun problème observé.

Détails techniques : Le proxy Nginx peut échouer si le serveur en amont s'appuie sur l'accès aux informations d'autorité (AIA) pour rechercher les certificats intermédiaires manquants, car Nginx ne gère pas AIA aussi élégamment que le service proxy d'analyse de fichiers. Les incohérences entre les interfaces SNI et SAN lors de la connexion TLS peuvent également déclencher des défaillances.

517 Certificat en amont révoqué

L'erreur 517 signifie que la vérification CRL ou OCSP du proxy SWG a détecté que le certificat du serveur en amont a été révoqué.

- Dépannage : Utilisez des outils externes tels que SSL Labs ou OpenSSL pour confirmer l'état de révocation.
- Documentation:
  - Erreur de dépannage Cisco 517 - Certificat en amont révoqué
  - Comprendre les erreurs courantes de certificat et de protocole

Options de gestion des erreurs de certificat

Cisco Secure Access introduira une nouvelle fonctionnalité appelée « Options de traitement des erreurs de certificat » pour le contournement granulaire des erreurs sans désactiver entièrement le déchiffrement. Les domaines qui déclenchent des erreurs de certificat en raison de l'inspection peuvent être gérés à l'aide de cette fonctionnalité au lieu de listes « Ne pas déchiffrer » générales. Cette fonctionnalité existe dans Umbrella SIG à partir d'aujourd'hui. Détails des demandes de

fonctionnalités pour CSA.

502 Passerelle incorrecte

L'erreur 502 indique que le proxy SWG a reçu une réponse non valide du serveur en amont alors qu'il agissait en tant qu'intermédiaire.

- En aval : Client vers proxy SWG
- En amont : Proxy SWG vers serveur de destination

L'erreur est toujours dans la connexion en amont, en raison d'erreurs de protocole, de réinitialisations TCP ou d'en-têtes mal formés.

502 causes courantes

- Suites de chiffrement SWG non prises en charge
- Demande d'authentification de certificat client
- En-têtes ajoutés par le proxy SWG

Suites de chiffrement non prises en charge

Motif: Le serveur nécessite un chiffrement non pris en charge par SWG (par exemple, TLS_CHACHA20_POLY1305_SHA256).
Résolution : Ajoutez le domaine à la liste de décodage sélectif.

Commandes de test :
Avec Proxy :

```
curl -x proxy.sig.umbrella.com:80 -v xyz.com:80
curl -x swg-url-proxy-https.sigproxy.qq.opendns.com:443 -vv -k "https://www.cnn.com" >> null
```

Sans proxy :

```
curl -v www.xyz.com:80
```

Mac/Linux :

```
curl -vv -o /dev/null -k -L www.cnn.com
```

Fenêtres:

```
curl -vv -o null -k -L www.cnn.com
```

Demande d'authentification de certificat client

Motif: Le serveur en amont nécessite des certificats côté client, que SWG ne prend pas en charge.

Résolution : Contourner le domaine du proxy à l'aide de la liste de gestion Domaines externes (Umbrella SIG) ou Contourner le proxy sécurisé (Cisco Secure Access). Contourner l'inspection HTTPS seule est insuffisant.

En-têtes ajoutés par proxy

Motif: Certains serveurs rejettent les requêtes avec l'en-tête X-Forwarded-For (XFF) ajouté par SWG lorsque l'inspection HTTPS est activée.
Résolution : Comparer le comportement avec/sans HTTPS et l'inspection des fichiers. Si l'erreur se produit uniquement lorsque XFF est présent, le serveur Web est probablement mal configuré.

Exemple :
`curl https://www.xyz.com -k –header 'X-Forwarded-For : 1.1.1.1' -o /dev/null -w "Code d'état : %{http_code}" -s`
Code d'état : 502
`curl https://www.xyz.com -k -o /dev/null -w "Code d'état : %{http_code}" -s`
Code d'état : 200

L'en-tête XFF est ajouté pour la géolocalisation. Si le serveur ne peut pas le traiter, une erreur 502 se produit.

Pua potentiellement indésirable ou fichiers corrompus

Si SWG ne peut pas analyser un fichier à l'aide de l'inspection de fichier (par exemple, les fichiers protégés, demandés par la plage ou corrompus), il bloque le téléchargement et les rapports - Bloqué - Application potentiellement indésirable (fichier protégé)

- Dépannage : Capturez un HAR pendant l'événement de blocage. Utilisez l'option Remplacer la sécurité comme solution de contournement temporaire. Si le fichier est corrompu ou malveillant, il doit être corrigé à la source.

Catégories et blocs de réputation potentiellement dangereux

- Utilisez Talos pour vérifier la réputation Web (WBRS). Si un domaine est mal classé, envoyez une demande COG Jira à Talos pour examen. Talos catégorisé comme sûr ou

favorable, mais toujours SWG bloc alors nous avons besoin de vérifier à partir du service Beaker de SWG.

Accès refusé par Akamai pour les adresses IP de sortie SWG

- SWG utilise des adresses IP de sortie partagées. Si les services de réputation IP (par exemple, Brightcloud) les bloquent, l'accès à certains sites peut être refusé.

Problèmes connus : Le robot de connexion et la vidéo de Youtube sont indisponibles

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.