Dépannage des problèmes d'accès au site Web SWG

Table des matières

Introduction

Informations générales

Erreur « Access Denied 403 » en raison du blocage en amont

Erreur « Access Denied 403 » en raison d'un problème Java

Cause première du problème : niveau élevé

- Quel est le problème lié à Java avec MPS ?
  - Résolution

Qu'est-ce que 502 Bad Gateway ?

Facteurs courants pour la passerelle 502 incorrecte

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

Introduction

Ce document décrit comment dépanner les problèmes d'accès au site Web vus avec le proxy de passerelle Web sécurisée Umbrella (SWG).

Informations générales

Supposons que le site www.xyz.com n'est pas accessible via le proxy SWG et que lorsque les utilisateurs essaient d'accéder directement à Internet (sans Umbrella SWG dans l'image), cela fonctionne correctement. Examinons les divers symptômes et les différents types de messages d'erreur signalés lorsque le site Web est inaccessible via SWG. Les plus courants sont 502 mauvaise passerelle, 502 ne pouvait pas relayer le message d'erreur en amont, certificat en amont révoqué, accès refusé 403 interdit, chiffrement en amont non concordant, site Web vient d'expirer après avoir tourné pendant un certain temps ou similaire.

Erreur « Access Denied 403 » en raison du blocage en amont

Le serveur Web ou le côté amont bloque ou limite nos plages IP de sortie proxy SWG. Par exemple, Akamai WAF a bloqué la liste de quelques plages IP de sortie SWG. Pour résoudre ce problème, la seule option est de contacter les administrateurs de sites Web et de leur demander de débloquer nos plages IP. Jusque-là, contourner SWG en utilisant la liste de gestion des domaines externes pour les déploiements de fichiers Anyconnect SWG et PAC. En bref, ce type

de problème n'est pas dû au proxy lui-même, mais plutôt à l'incompatibilité entre le proxy et les serveurs Web. Voici le lien pour faire référence à la base de connaissances spécifiquement pour l'erreur « Access Denied 403 » due au blocage de l'IP de sortie.

En outre, voici le lien qui couvre quelques raisons possibles pour lesquelles Akamai a bloqué les adresses IP répertoriées.

Erreur « Access Denied 403 » en raison d'un problème Java

Le site Web n'est pas accessible et affiche « Access Denied or 403 Forbidden - Umbrella cloud security gateway error » lorsque la demande est envoyée via le proxy SWG MPS avec le paramètre d'inspection de fichier activé. Mais si l'inspection des fichiers est désactivée, les sites Web se chargent correctement. Ou si nous mettons le site Web dans le décodage de contournement, les sites Web se chargent avec succès.

Cause première du problème : niveau élevé

Quel est le problème lié à Java avec MPS ?

Le site ou le serveur Web en question renvoie un avertissement TLS concernant une alerte SNI ou SSL au proxy après que le proxy a tenté de se connecter au serveur. En fait, cela se produit après l'envoi du Hello du client. Proxy MPS (qui est basé sur Java et en tant que tel) par conception, il traite toutes les alertes TLS avec "Nom non reconnu" dans le champ de description comme une erreur pendant l'analyse SNI et il termine la transaction. Plus de détails trouvés ici

Sachez qu'il ne s'agit pas d'un problème de proxy SWG ou MPS. Il s'agit d'une des incompatibilités avec SWG ou tout autre proxy en raison d'une mauvaise configuration côté serveur. Les navigateurs ignorent généralement cet avertissement, mais SWG ou un autre filtre de sécurité du contenu traite l'avertissement SSL comme une erreur irrécupérable et met fin à la session, ce qui entraîne 403 pages d'erreur interdites aux utilisateurs. Il peut également signaler une erreur 502 Bad Gateway, mais avec la plupart des exemples, nous avons vu une erreur 403 Forbidden, comme illustré dans cette image.

Comme MPS fonctionne au niveau de la couche application, il ne contrôle que très peu, voire pas du tout, la manière dont la couche TLS gère la transaction en fonction des alertes générées dans le protocole TLS. Il incombe au serveur de s'assurer que son terminal TLS/ses certificats sont configurés correctement. Veuillez consulter ce lien.

Pour réduire ou résoudre le problème, il peut être facilement signalé à partir du TP SSL.

15152060146964

Lorsque l'accès au site Web se fait sans proxy SWG au milieu ou que l'inspection HTTPS du SWG est contournée, le site Web fonctionne car le navigateur ignore l'alerte de nom non reconnu SNI et continue à communiquer avec le serveur Web.

Au moment de la rédaction de cet article, la solution de contournement recommandée est la meilleure atténuation que nous puissions vous suggérer. Dans un avenir proche, avec la nouvelle architecture de proxy, nous serons en mesure de traiter ces problèmes plus facilement.

Résolution

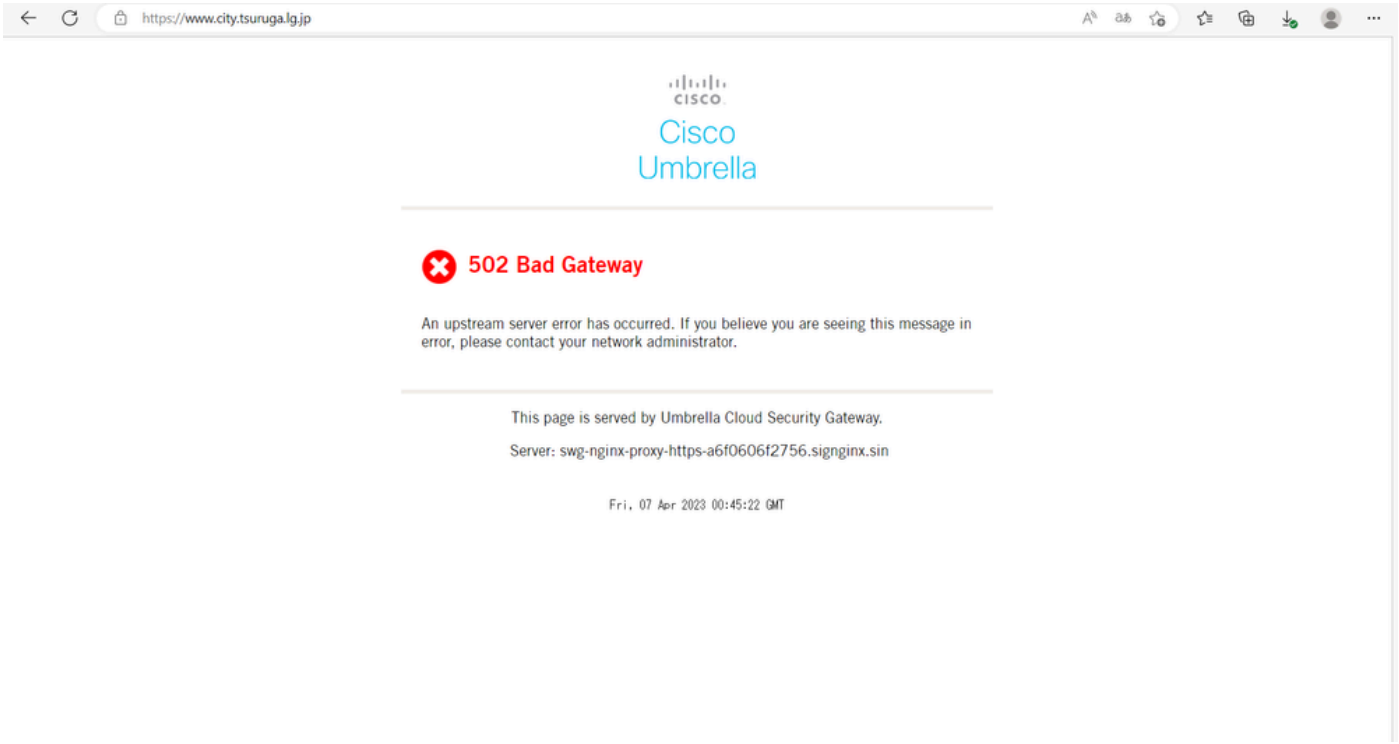
1. Désactivez le déchiffrement pour les domaines affectés - OU
2. Ajoutez le domaine à une liste de destinations et associez une règle d'autorisation (si vous approuvez le site)

Qu'est-ce que 502 Bad Gateway ?

Une erreur 502 Bad Gateway Error signifie que le serveur agissait en tant que passerelle ou proxy et a reçu une réponse non valide du serveur en amont. Lorsque l'utilisateur tente d'accéder au site Web via le proxy SWG, deux flux de communication se produisent.

a) Client —> Connexion proxy (en aval)
b) Proxy—> Fin de la connexion au serveur Web (en amont)

502 Une erreur de passerelle incorrecte se produit entre le proxy SWG (MPS, Nginx) et la connexion du serveur final.



15026978020884

Facteurs courants pour la passerelle 502 incorrecte

1. Suites de chiffrement SWG non prises en charge

2. Demande d'authentification de certificat client

3. En-têtes ajoutés ou supprimés par le proxy SWG

Suites de chiffrement SWG non prises en charge

Supposons qu'un serveur Web signale des suites de chiffrement SWG non prises en charge lors de la négociation TLS. Veuillez noter que le proxy SWG MPS (Modular Proxy Service) ne prend pas en charge la suite de chiffrement TLS_CHACHA20_POLY1305_SHA256. Sachez qu'il existe un article distinct pour couvrir les suites de chiffrement et TLS pris en charge par SWG. Nous pouvons facilement identifier ce problème en examinant les paquets capturés lors de l'échange de suites de chiffrement dans hello client et hello serveur. Comme étape de dépannage, utilisez la commande CURL pour imposer l'utilisation de chiffrements spécifiques afin de réduire le problème et de confirmer qu'il est dû à des suites de chiffrements, comme illustré dans les exemples 1 et 2.

Exemple de commandes Curl :

<#root>

```
curl -vvv "" --ciphers TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 >> /dev/null
curl -vvv "" --ciphers ECDHE-RSA-AES256-GCM-SHA384 >> /dev/null
```

Testing website With Proxy:

```
 - curl -x  proxy.sig.umbrella.com:80 -v  xyz.com:80
```

```
curl -x swg-url-proxy-https.sigproxy.qq.opendns.com:443 -vvv -k "https://www.cnn.com" >> null
```

Testing website without Proxy

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

Mac/Linux:

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

Windows:

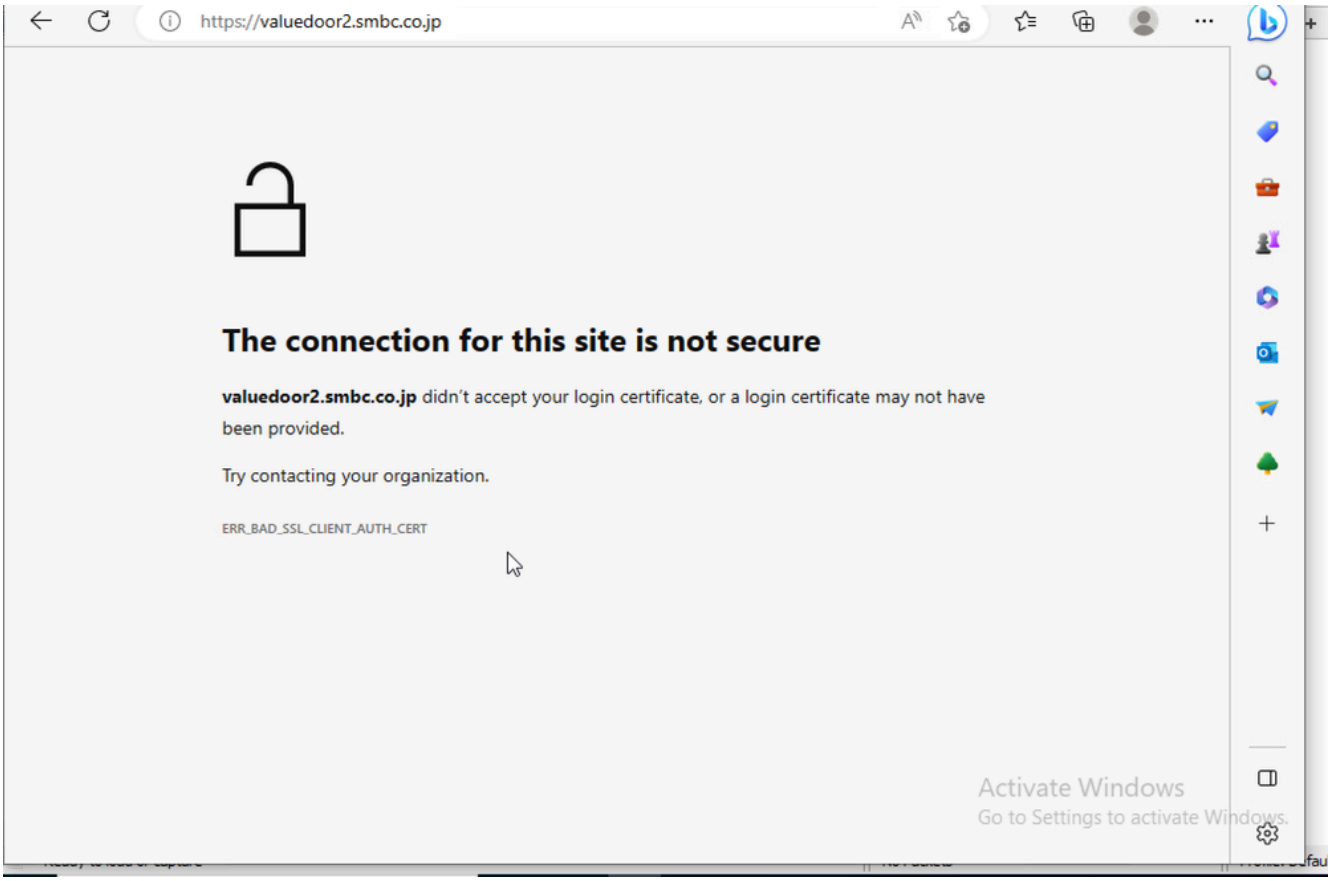
```
 - curl -vvv -o null -k -L www.cnn.com
```

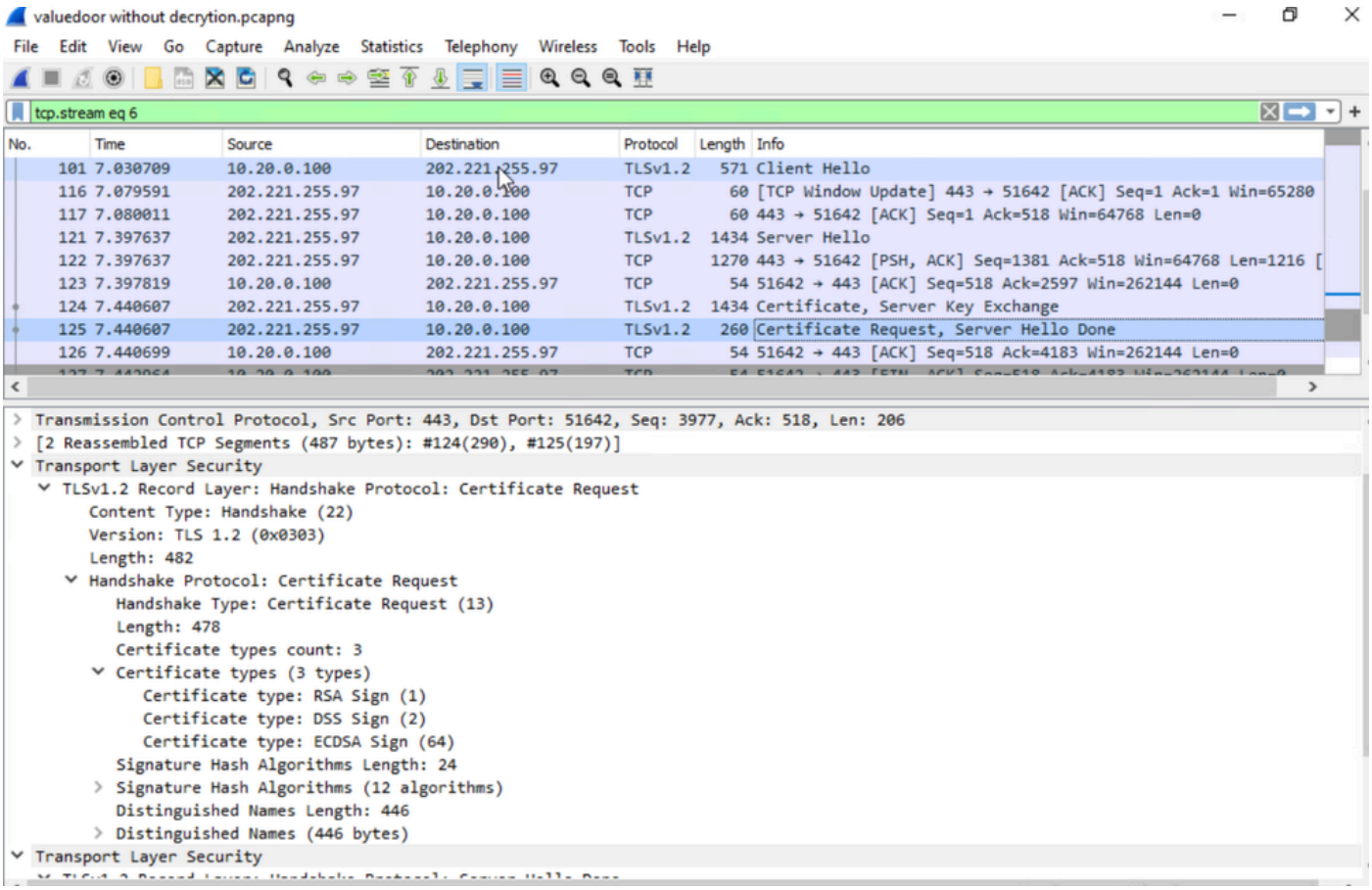
Résolution

Pour résoudre le problème, ignorez l'inspection du site Web problématique à l'aide de la liste de décodage sélective.

Demande d'authentification de certificat client

Lors de la connexion TLS entre le proxy SWG et le serveur Web en amont, le serveur Web en amont attend l'authentification du certificat client. Comme l'authentification de certificat client n'est pas prise en charge, nous devons contourner ces domaines à partir du proxy à l'aide de la liste de gestion des domaines externes, et contourner simplement l'inspection https n'est pas suffisant. Exemple : https://valuedoor2.smbc.co.jp.

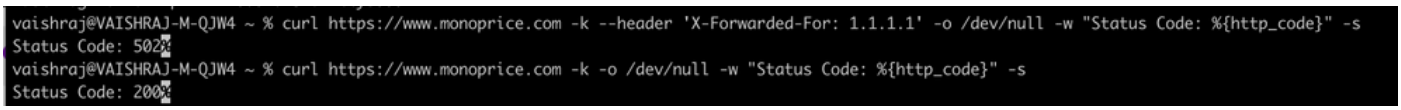




15027192992276

En-têtes ajoutés par proxy

Le serveur Web signale une erreur 502 de passerelle incorrecte en raison de l'en-tête X-Forward-For (XFF) ajouté par le proxy SWG lorsque l'inspection https est activée. Nous pouvons facilement réduire la plupart des problèmes de mauvaise passerelle 502 en commençant par dépanner le problème avec ou sans inspection https, et avec ou sans inspection de fichier pour éliminer le problème d'analyse de fichier avec le proxy MPS.



15123666760340

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

Nous utilisons l'en-tête XFF lorsque l'inspection HTTPS est activée, de sorte que le serveur en amont puisse fournir un contenu de géolocalisation optimal basé sur l'adresse IP du client (qui fournit l'emplacement physique de l'utilisateur).

Lorsque l'inspection HTTPS n'est pas activée, cet en-tête n'est pas ajouté par le proxy et il n'y a donc pas d'erreur 502 Bad Gateway. Ce n'est pas un problème de proxy SWG . Cette erreur est due au serveur Web en amont qui est mal configuré pour ne pas prendre en charge l'en-tête XFF standard.

Résolution

Pour résoudre le problème, ignorez l'inspection HTTPS pour des domaines spécifiques à l'aide de listes de déchiffrement sélectives.

- 517 Certificat en amont révoqué
- Erreurs de certificat et de protocole TLS
- Sélection manuelle du contrôleur de domaine SWG pour les tests internes

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.