Erreur Secure Access 502 Pour Les Sites Bancaires Après Authentification

Table des matières

Problème

Les utilisateurs ont signalé avoir reçu un code d'erreur HTTP 502 Bad Gateway après s'être authentifiés auprès de FCBanking. Le processus d'authentification s'est terminé avec succès, ce qui a permis aux utilisateurs d'entrer leurs identifiants de connexion. Cependant, le navigateur a affiché une erreur 502 bad gateway immédiatement après l'authentification.

Le domaine pour FCBanking et sa catégorie pertinente ont été exemptés du déchiffrement SSL et IPS et ce changement de configuration n'a pas résolu l'erreur HTTP 502. Le problème s'est produit par intermittence et n'a été résolu qu'après avoir contourné l'accès sécurisé pour le domaine FCBanking. L'analyse du fichier HAR a révélé 502 erreurs sur la destination de « my.fcbanking.com », et les journaux de recherche d'activité n'ont pas montré les 502 erreurs qui ont été capturées dans le fichier HAR, indiquant que ces erreurs se produisaient au niveau d'un périphérique intermédiaire.

Environnement

- Accès sécurisé Cisco - Accès Internet (module d'itinérance, VA, DNS, SWG, PAC, IPS, certificats)
- Topologie du réseau : PC utilisateur > Commutateur > Routeur SD-WAN Catalyst > Internet local ou tunnel CSA
- Catalyst SD-WAN Edge configuré avec une règle de stratégie d'application pour envoyer tout le trafic sur les ports 80 et 443 via l'accès Internet direct (DIA) en contournant le groupe de tunnels réseau (NTG)
- Cisco Secure Client s'appuyant sur une liste de contournement pour déterminer le routage du trafic vers Secure Access
- Domaine bancaire : fcbanking.com et sous-domaines associés (my.fcbanking.com,

treasury.fcbanking.com)

Résolution

La résolution principale implique l'ajout du domaine bancaire pour contourner entièrement l'accès sécurisé, permettant au trafic de circuler directement vers Internet tout en maintenant la sécurité de la couche DNS.

Étape 1: Ajouter un domaine principal à la liste de contournement

- Ajoutez fcbanking.com à la liste bypass proxy only dans la configuration Secure Access. Cela garantit que le trafic Web contourne le proxy d'accès sécurisé tandis que la sécurité de la couche DNS reste appliquée et consignée dans la recherche d'activité.

Étape 2: Identifier et ajouter des alias de domaine

- Les sites bancaires utilisent souvent plusieurs alias qui doivent également être ajoutés à la liste de contournement. Utilisez Cache Check pour identifier tous les alias du domaine bancaire.
- Pour fcbanking.com, ces alias ont été identifiés et ajoutés à la liste de contournement :
  - treasury.fcbanking.com (alias : treasuryvanity.jackhenry.com)
  - my.fcbanking.com (alias : banno-online.jackhenry.bank)
  - treasuryvanity.jackhenry.com
  - banno-online.jackhenry.bank

Étape 3: Résolution alternative utilisant des adresses IP

- Comme alternative au contournement basé sur le domaine, les adresses IP résolues des sites bancaires peuvent être ajoutées à la liste de contournement. Le client sécurisé Cisco traduit les noms de domaine complets de la liste de contournement en adresses IP et achemine le trafic Web directement vers Internet.

Étape 4: Activer la consignation de débogage pour le dépannage

- Pour capturer des journaux détaillés en vue d'une analyse plus approfondie, activez la

journalisation de débogage maximale :

- Créez un fichier nommé « SWGConfigOverride.json » avec le contenu suivant :

```
{"logLevel": "1"}
```

Placez le fichier SWGConfigOverride.json dans le dossier SWG :

```
C:\ProgramData\Cisco\Cisco Secure Client\Umbrella\SWG\
```

Redémarrez le service SWG ou Umbrella ou redémarrez le système pour appliquer la configuration de journalisation du débogage.



Remarque : La journalisation du débogage n'affecte pas les performances du système, mais peut augmenter la taille du fichier journal. Supprimez le fichier SWGConfigOverride.json après avoir obtenu le bundle DART pour revenir à des niveaux de journalisation normaux.

Étape 5: Vérification

- Après la mise en oeuvre de la configuration de contournement, les utilisateurs n'ont signalé aucune autre erreur 502 lors de l'accès au site bancaire. Le trafic DNS continue d'être connecté à la recherche d'activité tandis que le trafic Web circule directement sur Internet.

Motif

Les sites bancaires mettent généralement en oeuvre des mesures de sécurité qui détectent et bloquent le trafic provenant de serveurs proxy ou de plages d'adresses IP partagées. Cisco Secure Access utilise des plages IP partagées (151.186.144.0/20 et 151.186.176.0/20) pour le trafic proxy, que les sites bancaires peuvent détecter et supprimer silencieusement ou auquel ils peuvent répondre par des erreurs HTTP 502.

Lorsque des domaines sont placés dans la liste de non-déchiffrement, l'adresse IP source semble toujours provenir de la plage d'adresses IP partagées d'accès sécurisé, ce qui déclenche les mécanismes de sécurité du site bancaire. En outre, l'inspection IPS sur le trafic bancaire et les

alias de domaine qui ne sont pas correctement exemptés peuvent contribuer à des échecs de connexion. La nature intermittente de ce problème et les erreurs 502 apparaissant dans les fichiers HAR mais pas dans les journaux de recherche d'activité indiquent que les erreurs ont été générées par le traitement intermédiaire par proxy plutôt que par les serveurs bancaires de destination.

Autres informations utiles

- Dépannage des problèmes d'accès au site Web SWG
- Désactiver le protocole QUIC pour assurer une inspection correcte du trafic Web
- Documentation des plages IP 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.