Dépannage du problème de substitution de cookie d'authentification SWG SAML pour un accès sécurisé

Table des matières

Problème

Les utilisateurs accédant aux applications Web via Cisco Secure Access connaissent des échecs d'authentification lorsque les applications effectuent des redirections entre domaines ou récupèrent des ressources à partir de plusieurs domaines associés. Le problème se manifeste comme suit :

- Échec de l'initialisation des applications Web après l'authentification SAML.
- Les demandes de ressources inter-domaines (erreur CORS) étant bloquées par les règles de refus par défaut.
- Journaux d'activité affichant les demandes attribuées à l'identité du réseau ou du tunnel au lieu de l'identité utilisateur authentifiée.
- Erreurs de stratégie CORS apparaissant dans la console du navigateur pour les demandes redirigées.
- Applications fonctionnant correctement sur les machines physiques lors de l'utilisation de substituts IP mais échouant sur les environnements de postes de travail virtuels Citrix utilisant le substitut Cookie.

Le problème se produit spécifiquement lorsque l'authentification de substitution de cookie est utilisée dans des environnements virtualisés, où les requêtes redirigées perdent le mappage utilisateur-cookie lors des extractions de ressources entre domaines.

Environnement

- Accès sécurisé Cisco avec authentification SAML configurée
- Authentification par substitution de cookie activée pour les environnements de postes de travail virtuels Citrix
- Authentification IP de substitution utilisée pour les machines physiques
- Applications Web qui effectuent des redirections entre domaines (erreur CORS dans les journaux de la console de l'outil de développement Web)
- Environnement mixte avec infrastructure de postes de travail physiques et virtuels

Résolution

Le problème est résolu par la mise en oeuvre du contournement IP Surrogate pour les plages réseau affectées, permettant une attribution correcte de l'identité de l'utilisateur même lors des redirections interdomaines.

Étape 1: Accédez à IP Surrogate Configuration

Accédez au tableau de bord Cisco Secure Access et naviguez jusqu'à Connect > Users and Groups > Configuration Management > Advanced Settings > IP Surrogate.

Étape 2: Activer le contournement réseau interne

Ajoutez les plages réseau affectées à la configuration de contournement du réseau interne. Cela permet au système de maintenir l'attribution d'identité d'utilisateur pour les demandes provenant de ces réseaux.

Étape 3: Tester l'accès aux applications

Après avoir mis en oeuvre la substitution IP, testez les applications concernées pour vérifier que :

- Les demandes de ressources interdomaines sont correctement attribuées à l'identité de l'utilisateur
- Initialisation réussie des applications sans erreurs CORS
- Les journaux d'activité affichent l'identité utilisateur au lieu de l'identité réseau ou tunnel pour toutes les requêtes

Étape 5: Surveiller les rapports d'activité

Utilisez Monitor > Activity Search pour vérifier que les demandes sont maintenant correctement attribuées aux utilisateurs authentifiés plutôt que d'afficher comme identité réseau ou basée sur un tunnel.

Motif

Ce comportement est attendu en raison de la nature de l'authentification SAML combinée à Cookie Surrogate dans les environnements virtualisés. Lorsque des applications Web effectuent des redirections entre domaines ou récupèrent des ressources à partir de plusieurs domaines associés, les requêtes redirigées ne transportent peut-être pas le cookie de substitution d'une manière que Cisco Secure Access peut associer de nouveau à la session utilisateur authentifiée.

La cause principale est la suivante :

- Cookie Surrogate repose sur la propagation des cookies du navigateur à travers les redirections.
- Les stratégies de sécurité interdomaines (CORS) peuvent supprimer les cookies pendant les scénarios 307/redirection.
- Les mesures de sécurité du navigateur empêchent le partage de cookies entre différents domaines.
- Les environnements de bureau virtuel gèrent la propagation des cookies différemment des machines physiques.

Une fois le mappage utilisateur-cookie perdu, Secure Access ne peut pas résoudre la demande vers l'utilisateur authentifié, ce qui entraîne l'attribution de la demande uniquement au réseau enregistré/à une identité différente en tant que source et son blocage par les règles de refus par

défaut.

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.