Dépannage de l'identité SAML non appliquée au trafic de la passerelle Web sécurisée

Table des matières

Introduction

Ce document décrit comment dépanner les identités SAML qui ne sont pas appliquées au trafic de passerelle Web de sécurité.

Identité SAML non appliquée pour le trafic web ANY

Si l'identité SAML n'est pas appliquée pour TOUT trafic Web, veuillez consulter la documentation Umbrella pour vous assurer que la configuration a été correctement effectuée. Ces éléments de configuration doivent être terminés.

- Paramètres du fournisseur d'identité configurés et testés dans 'Déploiements > Configuration SAML'
- Liste des utilisateurs/groupes provisionnés dans 'Déploiements > Utilisateurs et groupes Web'
- SAML doit être activé dans la stratégie appropriée* dans 'Stratégies > Stratégies Web'.
- Le décodage HTTPS doit être activé dans la stratégie appropriée dans 'Stratégies > Stratégies Web'

Activation de SAML dans les stratégies Web

Le décodage SAML et HTTPS doit être activé dans la stratégie qui s'applique à l'identité de réseau ou de tunnel concernée. Ces fonctionnalités s'appliquent avant qu'un utilisateur ait été identifié, de sorte que la stratégie importante est celle appliquée à la « méthode de connexion ».

Les stratégies SAML doivent être classées comme suit :

1. PRIORITE SUPERIEURE - La politique s'applique aux utilisateurs/groupes. Cette stratégie détermine les paramètres de contenu/sécurité pour les utilisateurs authentifiés.

2. Priorité INFÉRIEURE - La politique s'applique au réseau/tunnel. SAML est activé pour cette stratégie et déclenche l'authentification initiale.

Identité SAML non appliquée pour le trafic Web spécifique

Substituts IP (comportement par défaut)

Pour améliorer la cohérence de l'identification des utilisateurs, nous vous recommandons d'activer la nouvelle fonctionnalité IP Surrogates. Cette fonctionnalité est activée automatiquement pour tous les nouveaux clients Umbrella SAML, mais doit être activée manuellement pour les clients Umbrella existants.

Les substituts IP utilisent un cache d'informations IP interne > Username, ce qui signifie que l'identification SAML peut être appliquée à tous les types de requêtes : même le trafic hors navigateur Web, le trafic qui ne prend pas en charge les cookies et le trafic non soumis au décodage SSL.

Les substituts IP peuvent améliorer considérablement la cohérence de l'identification des utilisateurs et réduire la charge administrative.

Veuillez noter que les substituts IP ont ces exigences :

- La visibilité IP interne doit être fournie à l'aide d'un tunnel de réseau parapluie ou d'un déploiement de chaîne proxy et d'en-têtes X-Forwarded-For. Cela ne fonctionne pas avec le fichier PAC hébergé d'Umbrella
- Les substituts IP ne peuvent pas être utilisés dans des scénarios d'adresses IP partagées (serveurs Terminal Server, commutation rapide d'utilisateurs)
- Les cookies doivent être activés dans le navigateur. Les cookies sont toujours requis pour l'étape d'authentification initiale.

Substituts de cookie (Substituts IP désactivés)

Lorsque IP Surrogates est désactivé, l'identité de l'utilisateur est uniquement appliquée aux requêtes des navigateurs Web pris en charge et le navigateur Web DOIT prendre en charge les cookies. SWG exige que le navigateur prenne en charge les cookies pour chaque demande afin de suivre la session des utilisateurs dans un cookie. Malheureusement, cela signifie qu'il n'est pas prévu que chaque demande Web soit associée à un utilisateur dans ce mode.

SAML n'est pas appliqué dans ces circonstances et la stratégie par défaut attribuée à l'identité réseau/tunnel est utilisée à la place :

- Trafic de navigateur non Web
- Navigateurs Web avec cookies désactivés ou Configuration de sécurité renforcée d'IE
- Contrôles OCSP/de révocation de certificat qui ne prennent pas en charge les cookies
- Requêtes Web individuelles qui ne prennent pas en charge les cookies. Dans certains cas, les cookies sont bloqués pour les requêtes individuelles en raison de la stratégie de sécurité du contenu du site Web. Cette restriction s'applique à de nombreux réseaux de diffusion de

contenu populaires.
- Lorsque le domaine/la catégorie cible a été contourné de SAML à l'aide d'une liste de contournement SAML
- Lorsque le domaine/la catégorie cible a été contourné(e) du décodage HTTPS à l'aide d'une liste de décodage sélectif Umbrella.

En raison de ces restrictions, il est important de configurer un niveau d'accès minimal approprié dans la politique de réseau/tunnel appropriée. La stratégie par défaut doit autoriser les applications/domaines/catégories stratégiques et les réseaux de diffusion de contenu.

Vous pouvez également utiliser le système IP Surrogates pour améliorer la compatibilité.

Contournement SAML

Dans de rares cas, des exceptions sont nécessaires. Cela est nécessaire lorsque SWG soumet une demande d'authentification SAML, mais que l'application ou le site Web ne peut pas la prendre en charge. Cela se produit lorsque :

- Une application non-navigateur utilise un agent utilisateur qui ressemble à un navigateur Web
- Un script ne peut pas gérer les redirections HTTP effectuées par nos tests de cookies
- La première requête d'une session de navigation est une requête POST (par ex. URL d'authentification unique) qui ne peut pas être redirigée correctement pour SAML

La liste de contournement SAML est la meilleure façon d'exclure un domaine de l'authentification tout en maintenant la sécurité (inspection de fichier).

- L'exception de liste de contournement SAML doit être appliquée à la stratégie correcte affectant le réseau/tunnel utilisé pour la connexion
- La liste de contournement SAML n'autorise pas automatiquement le trafic. Le ou les domaines doivent toujours être autorisés par catégorie ou par liste de destination dans la stratégie concernée.

Contournement SAML - Considérations

Lors de l'ajout d'exclusions pour les sites populaires et les « pages d'accueil », il est important de tenir compte de l'impact sur la LMEA. SAML fonctionne mieux lorsque la première requête d'une session de navigation est une requête GET vers une page HTML. Par exemple : http://www.myhomepage.tld. Cette demande est redirigée pour l'authentification SAML et les demandes suivantes prennent la même identité à l'aide de substituts IP ou de cookies.

Le contournement des pages d'accueil de SAML peut déclencher un problème lorsque la première requête vue par le système SAML concerne le contenu d'arrière-plan. Par exemple, http://homepage-content.tld/script.js. Il s'agit d'un problème car la redirection SAML vers une page de connexion SAML n'est pas possible lorsque le navigateur charge du contenu incorporé (comme les fichiers JS). Cela signifie que la page semble s'afficher ou fonctionner de manière incorrecte jusqu'à ce que l'utilisateur se rende sur un autre site pour déclencher la connexion.

Lorsque vous consultez des sites et des pages d'accueil populaires, tenez compte des choix suivants :

- N'excluez pas les pages d'accueil et les sites populaires du déchiffrement SAML ou HTTPS, sauf si nécessaire
- Si une page d'accueil est exclue, tous les domaines utilisés par ce site (y compris le contenu d'arrière-plan) doivent être exclus pour éviter les incompatibilités SAML

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.