Contenu

Question

Pourquoi est-ce que des utilisateurs sont incités pour l'authentification quand SaaS avec le fournisseur d'identité a initié des écoulements et NTLM ?

Environnement

- Appliance de sécurité Web de Cisco (WSA) exécutant des versions 7.0 ou ultérieures d'AsyncOS
- NTLM utilisé pour l'authentification transparente
- Contrôle d'accès de SaaS configuré utilisant l'écoulement initié parfournisseur
- SaaS SSO configuré

J'ai le contrôle d'accès de SaaS configuré avec mon application externe, utilisant l'écoulement et le SAML fournisseur-initiés par identité pour l'ouverture de session simple. J'emploie également NTLM pour authentifier d'une manière transparente mes utilisateurs. Est-ce que cependant, comment je peux les empêcher de voir cette demande ?

Symptômes

- Quand les utilisateurs cliquent sur en fonction leur signet pour l'URL de SaaS SSO, ils voient parfois les demandes d'authentification.
- Accédez à fonctionne bien si l'accès utilisateur un autre site Web externe et puis clique sur le signet URL de SaaS SSO.

Ce problème se pose quand/parce que la première demande que le WSA voit du client est à l'URL de l'offre spéciale SSO, qui est servi directement du WSA.

Le contenu qui est servi directement du WSA - tel que des pages EUN ou des fichiers PAC - est normalement exempt de l'authentification. Tandis que la caractéristique de SaaS peut accéder aux substituts d'authentification mis à jour par le proxy, elle ne peut elle-même authentification de demande suivre aucune méthode sans compter que l'authentification forme forme (NTLM ou LDAP). Ainsi le comportement observé est par conception mais n'est pas une solution optimale.

Le défaut CSCzv55859 est classé pour dépister ce problème et pour fournir un meilleur mécanisme pour aborder cette question.

Il y a deux contournements disponibles.

Contournement 1

1. Le premier est d'utiliser un écoulement Fournisseur-initié par service dans la configuration de SaaS. Dans un écoulement Fournisseur de services-initié, les débuts d'utilisateur par le furetage à l'application de SaaS de cible, qui sort alors la réorientation par l'URL SSO. Puisque ce premier trafic passe par le proxy, l'utilisateur obtiendra authentifié correctement utilisant NTLM. Ce contournement fonctionne seulement si les supports d'application de cible Fournisseur de services-initiaient des écoulements.
2. Créez un nouvel URL SSO dans la stratégie WSA, forçant l'authentification et puis réorientant le client au « vrai » URL SSO.

Contournement 2

1. Décidez d'un nouvel URL SSO. Cet URL sera accédé à jamais réellement par le proxy ; il agira simplement en tant que point pour initier le processus d'ouverture de session.

   Par exemple, si l'URL du courant SSO est « **wsa.mycompany.com/SSOURL/WebEx** », vous pouvez utiliser « **wsa.example.com/SSOURL/WebEx** ».L'importante considération veille que la partie d'adresse Internet que vous utilisez proxied par le WSA.

   Quand le WSA est déployé comme proxy explicite, l'adresse Internet peut être juste au sujet de n'importe quoi.Si le WSA est déployé comme proxy transparent, alors l'adresse Internet devra être une vraie adresse Internet qui la résout à une adresse IP externe.

2. Créez une catégorie URL de coutume (**GUI > gestionnaire de sécurité Web > des catégories faites sur commande URL**) qui apparie le nouvel URL.You devra créer une catégorie faite sur commande URL pour chaque application de SaaS que vous devez s'appliquer le contournement à.
   Employez la correspondance d'expression régulière pour apparier sur l'URL complet.

3. Allez accéder à des stratégies (**GUI > gestionnaire de sécurité Web > stratégies d'Access**) et sous la colonne de Filtrage URL pour une stratégie d'accès que la requête du client appariera. Ceci peut être une stratégie globale ou une stratégie différente plus tôt dans la table.
   Incluez la nouvelle catégorie URL de coutume dans cette stratégie d'accès, et placez son action **de réorienter**. La cible de la redirection devrait être le « vrai » URL SSO.

4. Soumettez et commettez les modifications pour appliquer la nouvelle configuration.

Les utilisateurs devraient maintenant employer le nouvel URL SSO pour accéder à l'application. Puisque l'accès à cet URL est traité par le proxy, l'authentification NTLM sera appelée et l'utilisateur soit toujours sera connecté d'une manière transparente, évitant l'authentification incite.