Dépannage de l'authentification SAML basée sur navigateur Secure Access affichant un écran blanc vierge avec EntraID

Table des matières

Problème

Lors de la configuration de Cisco Secure Access pour forcer l'authentification SAML basée sur navigateur sur les périphériques sans Cisco Secure Client installé, le processus d'authentification redirige vers un écran blanc vide au lieu d'afficher la page d'authentification EntraID. Ce problème se produit spécifiquement dans les navigateurs Microsoft Edge normal (non-InPrivate) et Google Chrome. L'authentification fonctionne correctement lorsque vous utilisez le mode InPrivate Edge. Le décodage et l'authentification SSO sont activés pour le profil d'authentification SAML.

La structure de stratégie configurée inclut :

- Autoriser la stratégie pour les utilisateurs post-authentification. (source : tout utilisateur, destination : tous les modèles)
- Autoriser la stratégie d'authentification SAML avec le profil d'authentification SAML. (source : Adresse IP du point d’extrémité, destination : 0.0.0.0 (TCP 80 443)
- Autoriser la stratégie d'assistance d'authentification SAML avec le profil d'authentification SAML. (source : Adresse IP du point d’extrémité, destination : tous les modèles)
- Bloquer la stratégie. (source : Adresse IP du point d’extrémité, destination : tous les modèles)

Environnement

- Cisco Secure Access (module d'accès à Internet)
- EntraID en tant que fournisseur d'identités (IdP)

- Authentification SAML basée sur navigateur pour les périphériques sans Cisco Secure Client
- Profil d'authentification SAML avec décodage et authentification SSO activés
- Navigateurs Microsoft Edge et Google Chrome

Résolution

Le problème est résolu en ajoutant des domaines EntraID spécifiques à la liste d'exclusion de déchiffrement dans la configuration du profil d'authentification SAML. Cela empêche le processus de déchiffrement SSL/TLS d'interférer avec le flux d'authentification EntraID.

Étape 1: Ajouter des domaines EntraID à la liste d'exclusion de déchiffrement

Configurez ces quatre domaines EntraID dans la liste d'exclusion de déchiffrement pour le profil d'authentification SAML :

```
login.live.com
login.microsoftonline.com
msauth.net
msftauth.net
```

Étape 2: Appliquer la configuration aux stratégies SAML

Assurez-vous que les paramètres d'exclusion de déchiffrement sont appliqués aux deux éléments :

- Autoriser la stratégie d'authentification SAML. (source : Adresse IP du point d’extrémité, destination : 0.0.0.0 (TCP 80 443)
- Autoriser la stratégie d'assistance d'authentification SAML. (source : Adresse IP du point d’extrémité, destination : tous les modèles)

Étape 3: Vérifier la résolution

Après avoir appliqué la configuration d'exclusion de déchiffrement, testez le flux d'authentification :

- Microsoft Edge (mode normal) : Redirection vers la page d'authentification EntraID réussie.
- Google Chrome: Redirection vers la page d'authentification EntraID réussie.
- Les deux navigateurs peuvent afficher de manière cohérente l'écran de saisie de l'authentification EntraID.

Motif

L'écran blanc vide se produit parce que le processus de déchiffrement SSL/TLS dans Cisco Secure Access interfère avec le flux d'authentification EntraID lorsque le déchiffrement est activé pour le profil d'authentification SAML. Le processus de déchiffrement interrompt la communication sécurisée entre le navigateur et les serveurs d'authentification EntraID, empêchant ainsi le chargement correct de la page d'authentification. Le mode InPrivate fonctionne car il gère les sessions SSL/TLS différemment, en contournant les interférences de déchiffrement. L'ajout des domaines EntraID à la liste d'exclusion de déchiffrement permet au trafic d'authentification de passer sans déchiffrement, préservant ainsi l'intégrité du flux d'authentification sécurisé.

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.