Authentification SSO Cisco Secure Access avec Duo IdP pour le trafic SWG du client d'itinérance

Table des matières

Problème

Lorsque vous essayez d'utiliser l'authentification SSO avec un IDp duo pour le trafic SWG (Secure Web Gateway) d'accès sécurisé provenant d'un client itinérant, les utilisateurs ne sont pas invités à utiliser l'authentification SSO duo et l'identité de l'utilisateur n'est pas renseignée dans le tableau de bord d'accès sécurisé. Bien que le trafic Web corresponde à la règle SWG prévue avec l'authentification activée et que le trafic soit décrypté, le flux d'authentification ne démarre pas pour le trafic client itinérant, ce qui empêche l'identification au niveau de l'utilisateur de l'activité Web.

Plus précisément, les comportements suivants ont été observés :

- La journalisation et l'activité SWG ont montré que le trafic correspondait à la règle SWG prévue et que le trafic de destination était déchiffré
- Les journaux et l'affichage de l'activité Accès sécurisé affichaient uniquement l'identité du PC et l'identité du réseau ; aucune demande d'authentification Duo/SAML, redirection SSO ou invite interactive n'a été observée
- Les entrées de politique ne contenaient que des informations sur l'itinérance et l'origine ; aucune identité d'utilisateur n'était présente avant la jonction AD
- Lorsque la machine virtuelle de test a été jointe à Active Directory lors du dépannage, l'identité de l'utilisateur est devenue visible dans la recherche d'activité d'accès sécurisé, mais l'invite interactive Duo/SAML ne s'est toujours pas produite

Environnement

- Accès sécurisé Cisco avec fonctionnalité SWG
- Client sécurisé version 5.1.13.17
- IDp duo configuré pour l'authentification SSO
- Abonnement à l'entreprise : Secure Access Essentials
- Réauthentifier l'intervalle proxy Web défini sur Quotidien

- Aucun fichier PAC ou VPN utilisé pendant les tests
- Environnement de test utilisant la configuration des ordinateurs itinérants

Résolution

Après une analyse et des tests complets, il a été déterminé que l'authentification SSO utilisant SAML n'est pas prise en charge pour le trafic client d'itinérance Secure Access en raison des limites de conception du produit. Les étapes de dépannage suivantes ont été effectuées pour confirmer cette limitation :

Étape 1: Dépannage en direct et reproduction des comportements

Le test a confirmé que la mise en correspondance de la stratégie SWG et le déchiffrement SSL s'étaient correctement déroulés, mais le flux d'authentification (redirection et défi SSO SAML/Duo interactifs) n'a pas été initié pour le trafic client d'itinérance.

Étape 2: Modifications des règles et de la source

La source de la règle SWG est passée du nom d'ordinateur itinérant à une identité d'utilisateur spécifique lors des tentatives de reprographie. Les services clients sécurisés ont été redémarrés et la propagation des politiques a été observée. Ces modifications n'ont pas résolu le problème du flux d'authentification.

Étape 3: Tests de jointure Active Directory

La machine virtuelle de test a été jointe à Active Directory pour déterminer l'effet sur la visibilité de l'identité des utilisateurs. Bien que cela ait rendu l'identité de l'utilisateur visible dans Secure Access Activity Search, l'invite interactive Duo/SAML ne s'est toujours pas produite, confirmant que le problème n'était pas lié à la seule visibilité de l'identité de l'utilisateur.

Étape 4: Analyse du bundle DART

Un faisceau DART a été collecté et analysé. L'analyse a confirmé l'application de la stratégie SWG, mais n'a montré aucune initiation de flux d'authentification pour le trafic client d'itinérance, ce qui permet de conclure que ce comportement est intentionnel.

Étape 5: Validation de la configuration Duo IdP

Des tests indépendants des métadonnées et de la configuration du protocole d'identification Duo ont été effectués et menés à bien, confirmant que la configuration Duo elle-même n'était pas la source du problème.

Étape 6: Validation interne

L'authentification SSO à l'aide de SAML n'est pas prise en charge pour le trafic client d'itinérance Secure Access comme limitation de conception du produit.

Conclusion: Aucune erreur de configuration n'a été détectée dans l'installation. L'absence d'invite SSO interactive a été attribuée à une limitation explicite du support produit plutôt qu'à un problème de configuration pouvant être résolu.

Motif

Le problème est causé par une limitation de conception de produit où l'authentification SSO à l'aide de SAML (y compris l'intégration de Duo IdP) n'est pas prise en charge pour le trafic client d'itinérance Secure Access. Il s'agit d'une limitation inhérente à l'architecture actuelle de la plate-forme Secure Access et elle n'est pas liée à des problèmes de configuration ou à des bogues logiciels.

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.