Comportement d'authentification SSO d'accès sécurisé pour le trafic Web hors navigateur

Table des matières

Problème

Lors de la mise en oeuvre de Cisco Secure Access (CSA) avec la connectivité IPsec, il était nécessaire de clarifier le comportement d'authentification SSO dans les profils de sécurité. Plus précisément, la question s'est posée de savoir quels types de trafic Internet sortant déclenchent l'authentification SSO lorsque les sites sont connectés via des tunnels IPsec.

La principale préoccupation était de savoir si l'authentification SSO s'applique uniquement à l'accès Web basé sur navigateur sur les ports TCP 80 et 443, ou si elle s'étend également aux applications et périphériques non basés sur navigateur, tels que les imprimantes ou les terminaux non Windows qui génèrent du trafic Web. Le comportement nécessitait une clarification concernant le moment où les invites d'authentification et les redirections vers les fournisseurs d'identité (IdP) se produiraient pour différents types de trafic Web provenant des sites connectés.

Environnement

- Déploiement de Cisco Secure Access (CSA)
- Connectivité du tunnel IPsec entre les sites et CSA
- Profils de sécurité configurés avec l'authentification SSO
- Environnement mixte avec divers périphériques, y compris des imprimantes et des terminaux non-Windows
- Inspection HTTPS activée
- Intégration SAML configurée

Résolution

Le comportement d'authentification SSO dans Cisco Secure Access est spécifiquement conçu pour cibler uniquement le trafic Web basé sur un navigateur. Le système exécute un processus d'inspection sophistiqué pour déterminer si les requêtes Web doivent être soumises à une authentification SSO.

Processus d'authentification SSO

Avant de rediriger une requête Web vers un fournisseur d'identité (IdP), Cisco Secure Access utilise l'inspection HTTPS pour déterminer si une requête provient d'un navigateur qui prend en charge les cookies. Ce processus d'inspection est le mécanisme clé qui différencie le trafic Web basé sur navigateur et le trafic Web non basé sur navigateur.

Classification du trafic

Trafic basé sur un navigateur (sujet à l'authentification SSO)

- Requêtes Web provenant de navigateurs qui prennent en charge les cookies
- Trafic HTTP/HTTPS sur les ports TCP 80 et 443 à partir des applications du navigateur
- Trafic qui réussit la détection de cookie/navigateur d'inspection HTTPS

Trafic hors navigateur (non soumis à l'authentification SSO)

- Trafic Web provenant d'imprimantes et d'autres périphériques réseau
- Applications qui ne prennent pas en charge les cookies ou qui ne sont pas identifiées comme des navigateurs
- Terminaux non Windows générant du trafic Web dont la détection du navigateur échoue

- Tout trafic Web qui ne passe pas la vérification du navigateur d'inspection HTTPS

Conditions requises pour l'authentification SSO

Pour que l'authentification SSO fonctionne correctement dans l'environnement, plusieurs conditions préalables doivent être remplies :

- La configuration SAML en cours doit être en place.
- Réseaux proxy avec XFF et/ou tunnels sans NAT (le substitut IP a besoin de visibilité sur les IP privées internes).
- L'inspection HTTPS doit être activée.
- Les sessions du navigateur doivent conserver les cookies (la suppression des cookies à la fin de la session ou la navigation incognito n'est pas recommandée).
- Adresses IP ne se chevauchant pas entre les emplacements, ou séparation de site appropriée si un chevauchement existe.

Motif

Le comportement est défini par conception dans Cisco Secure Access. Le mécanisme d'authentification SSO est spécifiquement conçu pour cibler des sessions utilisateur interactives via des navigateurs Web tout en permettant à des systèmes automatisés et à des dispositifs non interactifs d'accéder à des ressources Web sans interruption d'authentification. Cette conception empêche l'interruption des processus automatisés, des interfaces de gestion des périphériques et des applications qui ne peuvent pas gérer les redirections d'authentification ou les sessions basées sur des cookies.

Autres informations utiles

- Configurer les intégrations SAML - Activer les substituts IP pour SAML
- 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.