Resolución de Problemas SWG SAML Authentication Cookie Surrogate Problema para Acceso Seguro

Contenido

Problema

Los usuarios que acceden a las aplicaciones web a través de Cisco Secure Access experimentan errores de autenticación cuando las aplicaciones realizan redirecciones entre dominios o obtienen recursos de varios dominios relacionados. El problema se manifiesta como:

- Las aplicaciones web no se inicializan correctamente después de la autenticación SAML.
- Las solicitudes de recursos entre dominios (error CORS) que se bloquean según las reglas de denegación predeterminadas.
- Registros de actividad que muestran las solicitudes atribuidas a la identidad de la red o del túnel en lugar de la identidad del usuario autenticado.
- Errores de política CORS que aparecen en la consola del navegador para las solicitudes redirigidas.
- Aplicaciones que funcionan correctamente en máquinas físicas cuando se utiliza un sustituto IP, pero que fallan en entornos de escritorio virtual Citrix con un sustituto Cookie.

El problema ocurre específicamente cuando se utiliza la autenticación sustituta de cookies en entornos virtualizados, donde las solicitudes redirigidas pierden la asignación de usuario a cookie durante las capturas de recursos entre dominios.

Entorno

- Cisco Secure Access con autenticación SAML configurada
- Autenticación sustituta de cookies habilitada para entornos de escritorio virtual Citrix

- Autenticación IP sustituta utilizada para máquinas físicas
- Aplicaciones web que realizan redirecciones entre dominios (error CORS en los registros de la consola de la herramienta de desarrollador web)
- Entorno mixto con infraestructura de escritorios físicos y virtuales

Resolución

El problema se resuelve implementando el desvío de IP sustituto para los rangos de red afectados, lo que permite la atribución de la identidad de usuario adecuada incluso durante redirecciones entre dominios.

Paso 1: Vaya a IP Surrogate Configuration .

Acceda al panel de Cisco Secure Access y navegue hasta Connect > Users and Groups > Configuration Management > Advanced Settings > IP Surrogate.

Paso 2: Activar omisión de red interna

Agregue los rangos de red afectados a la configuración de omisión de la red interna. Esto permite al sistema mantener la atribución de identidad de usuario para las solicitudes que se originan en estas redes.

Paso 3: Probar acceso a aplicaciones

Después de implementar IP Surrogate, pruebe las aplicaciones afectadas para verificar que:

- Las solicitudes de recursos entre dominios se atribuyen correctamente a la identidad del usuario
- Las aplicaciones se inicializan correctamente sin errores CORS

- Los registros de actividad muestran la identidad del usuario en lugar de la identidad basada en la red o el túnel para todas las solicitudes

Paso 5: Supervisar informes de actividad

Utilice Monitor > Búsqueda de actividad para verificar que las solicitudes ahora se atribuyen correctamente a usuarios autenticados en lugar de mostrarse como una identidad basada en la red o el túnel.

Causa

Este comportamiento se espera debido a la naturaleza de la autenticación SAML combinada con Cookie Surrogate en entornos virtualizados. Cuando las aplicaciones web realizan redirecciones entre dominios o obtienen recursos de varios dominios relacionados, es posible que las solicitudes redirigidas no lleven la cookie sustituta de una manera que Cisco Secure Access pueda asociar de nuevo a la sesión de usuario autenticada.

La causa raíz se debe a lo siguiente:

- Cookie Surrogate depende de la propagación de cookies del navegador a través de redirecciones.
- Las políticas de seguridad entre dominios (CORS) pueden eliminar las cookies durante los escenarios de redireccionamiento 307/3007.
- Las medidas de seguridad del navegador evitan el uso compartido de cookies entre diferentes dominios.
- Los entornos de escritorio virtual gestionan la propagación de cookies de forma diferente que las máquinas físicas.

Una vez que se pierde la asignación de usuario a cookie, Secure Access no puede resolver la solicitud al usuario autenticado, lo que hace que la solicitud se atribuya únicamente a la red registrada/identidad diferente como origen y, posteriormente, se bloquee mediante reglas de denegación predeterminadas.

Contenido relacionado

- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).