Autenticación SSO de Cisco Secure Access con Duo IdP para tráfico SWG de clientes de roaming

Contenido

Problema

Cuando se intenta utilizar la autenticación SSO con un IdP Duo para el tráfico SWG (gateway web segura) de acceso seguro que se origina en un cliente de roaming, no se solicita a los usuarios la autenticación SSO Duo y la identidad del usuario no se rellena en el panel de acceso seguro. Aunque el tráfico web coincide con la regla SWG deseada con la autenticación habilitada y el tráfico se descifra, el flujo de autenticación no se inicia para el tráfico de cliente de roaming, lo que impide la identificación a nivel de usuario de la actividad web.

Específicamente, se observó el siguiente comportamiento:

- La actividad y el registro de SWG mostraron que el tráfico coincidía con la regla SWG prevista y que el tráfico de destino se descifraba
- Los registros y la vista de actividad de Secure Access mostraban solo la identidad del PC y la identidad de la red; no se observó ningún desafío de autenticación Duo/SAML, redirección de SSO o mensaje interactivo
- Las entradas de políticas solo mostraban información sobre itinerancia y origen; no había ninguna identidad de usuario antes de unirse a AD
- Cuando la máquina virtual de prueba se unió a Active Directory durante la resolución de problemas, la identidad del usuario se hizo visible en la búsqueda de actividad de acceso seguro, pero el mensaje interactivo de Duo/SAML no se produjo

Entorno

- Cisco Secure Access con funcionalidad SWG
- Secure Client versión 5.1.13.177
- IdP dúo configurado para autenticación SSO

- Suscripción a la organización: Secure Access Essentials
- Vuelva a autenticar el intervalo de proxy web establecido en Diario
- No hay ningún archivo PAC ni VPN en uso durante las pruebas
- Probar entorno con configuración de equipo móvil

Resolución

Tras un análisis y unas pruebas exhaustivos, se determinó que la autenticación de SSO mediante SAML no es compatible con el tráfico de clientes de roaming de Secure Access debido a las limitaciones de diseño del producto. Para confirmar esta limitación, se han llevado a cabo los siguientes pasos de solución de problemas:

Paso 1: Resolución de problemas en directo y reproducción del comportamiento

Las pruebas confirmaron que la coincidencia de la política SWG y el descifrado SSL se produjeron correctamente, pero el flujo de autenticación (redirección y desafío de SSO SAML/Duo interactivo) no se inició para el tráfico de clientes de roaming.

Paso 2: Modificaciones de reglas y orígenes

El origen de la regla SWG se cambió del nombre del equipo móvil a una identidad de usuario específica durante los intentos de réplica. Se reiniciaron los servicios de Secure Client y se observó la propagación de políticas. Estas modificaciones no resolvieron el problema del flujo de autenticación.

Paso 3: Prueba de unión a Active Directory

La máquina virtual de prueba se unió a Active Directory para determinar el efecto en la visibilidad de la identidad del usuario. Aunque esto hacía visible la identidad del usuario en la búsqueda de actividad de acceso seguro, el mensaje interactivo Duo/SAML no se produjo, lo que confirma que el problema no estaba relacionado únicamente con la visibilidad de la identidad del usuario.

Paso 4: Análisis del paquete DART

Se recopiló y analizó un paquete DART. El análisis confirmó la aplicación de la política SWG, pero no mostró ningún inicio de flujo de autenticación para el tráfico de cliente de roaming, lo que respalda la conclusión de que este comportamiento se basa en el diseño.

Paso 5: Validación de Configuración de Duo IdP

Se llevaron a cabo pruebas independientes de la configuración y metadatos del Duo IdP y se completaron con éxito, lo que confirmó que la configuración del Duo en sí no era el origen del problema.

Paso 6: Validación interna

La autenticación SSO mediante SAML no se admite para el tráfico de clientes de roaming de acceso seguro como limitación del diseño del producto.

Conclusión: No se ha encontrado ningún error de configuración en la configuración. La falta de mensajes de SSO interactivos se atribuyó a una limitación explícita del soporte del producto en lugar de a un problema de configuración solucionable.

Causa

El problema se debe a una limitación del diseño del producto en el que la autenticación SSO mediante SAML (incluida la integración Duo IdP) no se admite para el tráfico de cliente de roaming de acceso seguro. Se trata de una limitación inherente a la arquitectura actual de la plataforma Secure Access y no está relacionada con problemas de configuración o errores de software.

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).