Los usuarios indicaron para la autenticación cuando SaaS con el proveedor de la identidad inició los flujos y el NTLM

Contenido

[Pregunta](#)
[Entorno](#)
[Síntomas](#)
[Workaround 1](#)
[Workaround 2](#)

Pregunta

¿Por qué indican a los usuarios para la autenticación cuando SaaS con el proveedor de la identidad inició los flujos y el NTLM?

Entorno

- Versiones 7.0 de AsyncOS del dispositivo de seguridad de la red de Cisco que se ejecutan (WSA) o más adelante
- NTLM usado para la autenticación transparente
- Control de acceso de SaaS configurado usando el flujo iniciado identidad-proveedor
- SaaS SSO configurado

Tengo control de acceso de SaaS configurado con mi aplicación externa, usando el flujo proveedor-iniciado identidad y SAML para solo muestra-en. También estoy utilizando el NTLM transparente para autenticar a mis usuarios. ¿Sin embargo, cómo puedo evitar que vean este prompt?

Síntomas

- Cuando los usuarios hacen clic en su dirección de la Internet para el SaaS SSO URL, ven a veces los prompts de la autenticación.
- Acceda los trabajos muy bien si los usuarios acceden otro sitio Web externo y después hacen clic el marcador de SaaS SSO URL.

Este problema ocurre cuando/porque la primera petición que el WSA ve del cliente está al SSO especial URL, que se sirve directamente del WSA.

El contenido que se sirve directamente del WSA - tal como páginas EUN o archivos PAC - está

normalmente exento de la autenticación. Mientras que la característica de SaaS puede acceder a los sustitutos de la autenticación mantenidos por el proxy, no puede sí mismo autenticación de la petición usando ningún método además de la autenticación forma-basada (NTLM o LDAP). La conducta observada es tan por el diseño pero no es una solución óptima.

El defecto CSCzv55859 se clasifía para seguir este problema y para proporcionar un mejor mecanismo para abordar este problema.

Hay dos soluciones alternativas disponibles.

Workaround 1

1. El primer es utilizar un flujo Proveedor-iniciado servicio en la configuración de SaaS. En un flujo SP-iniciado, el usuario comienza hojeando a la aplicación de SaaS de la blanco, que entonces publica la reorientación con el SSO URL.
   Porque este tráfico inicial pasa con el proxy, el usuario conseguirá autenticado correctamente usando el NTLM. Esta solución alternativa trabaja solamente si los soportes de aplicaciones de la blanco SP-iniciaron los flujos.
2. Cree un nuevo SSO URL en la directiva WSA, forzando la autenticación y después reorientando al cliente al SSO “real” URL.

Workaround 2

1. Decida sobre un nuevo SSO URL. Este URL será accedido nunca realmente por el proxy; actuará simplemente como punta para iniciar muestra-en el proceso.

   Por ejemplo, si el SSO actual URL es “**wsa.mycompany.com/SSOURL/WebEx**”, usted puede utilizar “**wsa.example.com/SSOURL/WebEx**”.La consideración importante se está aseegurando la porción del nombre de host que usted utiliza proxied con el WSA.

   Cuando el WSA se despliega como proxy explícito, el nombre de host puede estar apenas sobre cualquier cosa.Si el WSA se despliega como proxy transparente, después el nombre de host necesitará ser un nombre de host real que resuelve a un IP Address externo.

2. Cree una categoría de la aduana URL (**GUI > administrador de seguridad de la red > las categorías de encargo URL**) que haga juego el nuevo URL.You necesite crear una categoría de encargo URL para cada aplicación de SaaS que usted necesita aplicar la solución alternativa a.
   Utilice la coincidencia de la expresión normal para hacer juego en el URL lleno.

3. Vaya a las políticas de acceso (**GUI > administrador de seguridad > las políticas de acceso de la red**) y bajo la columna del Filtrado de URL para una política de acceso que la petición de usuario haga juego. Ésta puede ser la política global u otra directiva anterior en la tabla. Incluya la nueva categoría de la aduana URL en esta política de acceso, y fije su acción **para reorientar**. La blanco del cambio de dirección debe ser el SSO “real” URL.

4. Someta y confíe los cambios para aplicar la nueva configuración.

Los usuarios deben ahora utilizar el nuevo SSO URL para acceder la aplicación. Porque el acceso a este URL es procesado por el proxy, la autenticación NTLM será invocada y el usuario esté siempre será ingresado transparente, evitando la autenticación indica.