Resolución de problemas de autenticación SAML basada en explorador de acceso seguro que muestra una pantalla blanca en blanco con EntraID

Contenido

Problema

Al configurar Cisco Secure Access para forzar la autenticación SAML basada en navegador en dispositivos sin Cisco Secure Client instalado, el proceso de autenticación se redirige a una pantalla blanca en blanco en lugar de mostrar la página de autenticación EntraID. Este problema ocurre específicamente en el modo normal de Microsoft Edge (no InPrivate) y los navegadores de Google Chrome. La autenticación funciona correctamente cuando se utiliza el modo Edge InPrivate. El perfil de autenticación SAML tiene activadas tanto la autenticación de descifrado como la de SSO.

La estructura de políticas configurada incluye:

- Permitir directiva para usuarios posteriores a la autenticación. (fuente: cualquier usuario, destino: cualquiera)
- Permitir directiva de autenticación SAML con perfil de autenticación SAML. (fuente: IP de terminal, destino: 0.0.0.0 (TCP 80.443)
- Permitir la política auxiliar de autenticación SAML con el perfil de autenticación SAML. (fuente: IP de terminal, destino: cualquiera)
- Bloquear directiva. (fuente: IP de terminal, destino: cualquiera)

Entorno

- Cisco Secure Access (módulo de acceso a Internet)

- EntraID como proveedor de identidad (IdP)
- Autenticación SAML basada en navegador para dispositivos sin Cisco Secure Client
- Perfil de autenticación SAML con el descifrado y la autenticación SSO habilitados
- Navegadores Microsoft Edge y Google Chrome

Resolución

El problema se resuelve agregando dominios específicos relacionados con EntraID a la lista de exclusión de descifrado en la configuración del perfil de autenticación SAML. Esto evita que el proceso de descifrado SSL/TLS interfiera con el flujo de autenticación EntraID.

Paso 1: Agregar dominios EntraID a la lista de exclusión de descifrado

Configure estos cuatro dominios EntraID en la lista de exclusión de descifrado para el perfil de autenticación SAML:

```
login.live.com
login.microsoftonline.com
msauth.net
msftauth.net
```

Paso 2: Aplicar configuración a políticas SAML

Asegúrese de que la configuración de exclusión de descifrado se aplique a:

- La directiva Permitir autenticación SAML. (fuente: IP de terminal, destino: 0.0.0.0 (TCP 80.443)
- La política del ayudante de autenticación de SAML. (fuente: IP de terminal, destino: cualquiera)

Paso 3: Verificar resolución

Después de aplicar la configuración de exclusión de descifrado, pruebe el flujo de autenticación:

- Microsoft Edge (modo normal): Se puede redirigir correctamente a la página de autenticación EntraID.
- Google Chrome: Se puede redirigir correctamente a la página de autenticación EntraID.
- Ambos exploradores pueden mostrar de forma coherente la pantalla de entrada de autenticación EntraID.

Causa

La pantalla blanca en blanco se produce porque el proceso de descifrado SSL/TLS en Cisco Secure Access interfiere con el flujo de autenticación EntraID cuando el descifrado está habilitado para el perfil de autenticación SAML. El proceso de descifrado interrumpe la comunicación segura entre el explorador y los servidores de autenticación EntraID, lo que impide que la página de autenticación se cargue correctamente. El modo InPrivate funciona porque gestiona las sesiones SSL/TLS de forma diferente, evitando la interferencia de descifrado. Agregar los dominios EntraID a la lista de exclusión de descifrado permite que el tráfico de autenticación pase sin descifrado, manteniendo la integridad del flujo de autenticación segura.

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).