Troubleshooting de la Identidad SAML que No se Aplica para el Tráfico de Gateway Web Segura

Contenido

Introducción

Identidad SAML no aplicada para CUALQUIER tráfico web

- Habilitación de SAML en Políticas Web

Identidad SAML no aplicada para tráfico web específico

- Sustitutos IP (comportamiento predeterminado)
- Sustitutos de cookies (sustitutos de IP desactivados)
- Omisión de SAML
- Omisión de SAML - Consideraciones

Introducción

Este documento describe cómo resolver problemas de identidades SAML que no se aplican al Tráfico de Gateway Web de Secture.

Identidad SAML no aplicada para CUALQUIER tráfico web

Si la identidad SAML no se aplica para CUALQUIER tráfico web, consulte la documentación de Umbrella para asegurarse de que la configuración se ha completado correctamente. Estos elementos de configuración deben completarse.

- Valores de IdP configurados y probados en 'Implementaciones > Configuración SAML'
- Lista de usuarios/grupos aprovisionados en 'Implementaciones > Usuarios y grupos web'
- SAML debe estar habilitado en la política correspondiente* en 'Políticas > Políticas web'.
- El descifrado HTTPS debe estar habilitado en la política correspondiente en 'Políticas > Políticas web'

Habilitación de SAML en Políticas Web

El descifrado SAML y HTTPS debe estar habilitado en la política que se aplica a la identidad de red o túnel relevante. Estas funciones se aplican antes de que se haya identificado al usuario, por lo que la política importante es la que se aplica al "método de conexión".

Las políticas SAML deben ordenarse de la siguiente manera:

1. MÁS ALTA prioridad: la política se aplica a usuarios/grupos. Esta directiva decide el contenido y la configuración de seguridad de los usuarios autenticados.

2. Prioridad más baja: la política se aplica a la red/túnel. Esta política tiene habilitado SAML y activa la autenticación inicial.

Identidad SAML no aplicada para tráfico web específico

Sustitutos IP (comportamiento predeterminado)

Para mejorar la uniformidad de la identificación del usuario, se recomienda habilitar la nueva función Sustitutos IP. Esta función se activa automáticamente para todos los clientes nuevos de Umbrella SAML, pero debe activarse manualmente para los clientes existentes de Umbrella.

Los sustitutos IP utilizan una memoria caché de la información Internal IP > Username, lo que significa que la identificación SAML se puede aplicar a todos los tipos de solicitudes: incluso el tráfico que no es de navegador web, el tráfico que no admite cookies y el tráfico que no está sujeto al descifrado SSL.

Los sustitutos de IP pueden mejorar considerablemente la coherencia de la identificación de usuarios y reducir la carga administrativa.

Tenga en cuenta que los sustitutos IP tienen estos requisitos:

- La visibilidad de IP interna debe proporcionarse mediante una implementación de túnel de red de paraguas o de cadena de proxy y encabezados X-Forwarded-For. Esto no funciona con el archivo PAC alojado de Umbrella
- Los sustitutos IP no se pueden utilizar en escenarios de direcciones IP compartidas (Terminal Servers, Fast User Switching)
- Las cookies deben estar habilitadas en el navegador. Las cookies siguen siendo necesarias para el paso de autenticación inicial.

Sustitutos de cookies (sustitutos de IP desactivados)

Con las sustituciones IP desactivadas, la identidad del usuario solo se aplica a las solicitudes de los navegadores web compatibles y el navegador web DEBE admitir cookies. SWG requiere que el navegador admita cookies para cada solicitud con el fin de realizar un seguimiento de la sesión de los usuarios en una cookie. Desafortunadamente, esto significa que no se espera que cada solicitud web se asocie con un usuario en este modo.

SAML no se aplica en estas circunstancias y en su lugar se utiliza la política predeterminada asignada a la identidad de red/túnel:

- Tráfico de navegador no Web
- Navegadores web con cookies desactivadas o Configuración de seguridad mejorada de IE
- Comprobaciones de OCSP/revocación de certificados que no admiten cookies
- Solicitudes web individuales que no admiten cookies. En algunos casos, las cookies se bloquean para solicitudes individuales debido a la Política de seguridad de contenidos del sitio web. Esta restricción se aplica a muchas redes populares de distribución de contenido.
- Cuando el dominio/categoría de destino se ha omitido de SAML mediante una lista de

omisión de SAML
- Cuando el dominio/categoría de destino se ha omitido del descifrado HTTPS mediante una lista de descifrado selectivo de Umbrella.

Debido a estas restricciones, es importante configurar un nivel mínimo de acceso adecuado en la política de red/túnel correspondiente. La política predeterminada debe permitir las aplicaciones/dominios/categorías fundamentales para la empresa y las redes de distribución de contenido.

También puede utilizar el sistema IP Surrogates para mejorar la compatibilidad.

Omisión de SAML

En raras ocasiones se requieren excepciones. Esto es necesario cuando SWG envía una solicitud de autenticación SAML pero la aplicación o el sitio web no pueden admitirla. Esto sucede cuando:

- Una aplicación que no es de navegador utiliza un agente de usuario que se parece a un navegador web
- Una secuencia de comandos no puede manejar las redirecciones HTTP realizadas por nuestras pruebas de cookie
- La primera solicitud en una sesión de navegación es una solicitud POST (por ejemplo, URL de inicio de sesión único) que no se puede redirigir correctamente para SAML

La lista de omisión de SAML es la mejor manera de excluir un dominio de la autenticación mientras se mantiene la seguridad (inspección de archivos).

- La excepción de la lista de omisión de SAML debe aplicarse a la política correcta que afecta a la red/túnel utilizado para la conexión
- La lista de omisión de SAML no permite automáticamente el tráfico. Los dominios deben seguir estando permitidos por categorías o listas de destinos en la política pertinente.

Omisión de SAML - Consideraciones

Al añadir exclusiones para sitios populares y "páginas de inicio", es importante tener en cuenta el impacto en SAML. SAML funciona mejor cuando la primera solicitud de una sesión de exploración es una solicitud GET a una página HTML. Por ejemplo: http://www.myhomepage.tld. Esta solicitud se redirige para la autenticación SAML y las solicitudes subsiguientes asumen la misma identidad mediante sustitutos IP o cookies.

Omitir las páginas de inicio de SAML puede desencadenar un problema en el que la primera solicitud vista por el sistema SAML es para el contenido de fondo. Por ejemplo, http://homepage-content.tld/script.js. Esto es un problema porque el redireccionamiento de SAML a una página de inicio de sesión de SAML no es posible cuando el navegador está cargando contenido incrustado (como archivos JS). Esto significa que parece que la página se representa o funciona incorrectamente hasta que el usuario va a un sitio diferente para iniciar el inicio de sesión.

Al considerar sitios y páginas de inicio populares, tenga en cuenta estas opciones:

- No excluya páginas de inicio y sitios populares del descifrado SAML o HTTPS a menos que sea necesario
- Si excluye una página de inicio, todos los dominios utilizados por ese sitio (incluido el contenido de fondo) deben excluirse para evitar incompatibilidades SAML

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).