Comportamiento de autenticación SSO de acceso seguro para tráfico web que no es del navegador

Contenido

Problema

Al implementar Cisco Secure Access (CSA) con conectividad IPsec, era necesario aclarar el comportamiento de autenticación de SSO en los perfiles de seguridad. Específicamente, surgió la pregunta sobre qué tipos de tráfico de Internet saliente activan la autenticación SSO cuando los sitios se conectan a través de túneles IPsec.

La principal preocupación era comprender si la autenticación SSO se aplica solamente al acceso web basado en navegador a través de los puertos TCP 80 y 443, o si también se extiende a aplicaciones y dispositivos que no son navegadores, como impresoras o terminales que no son de Windows que generan tráfico web. El comportamiento necesitaba una aclaración con respecto a cuándo se producirían los avisos de autenticación y las redirecciones a los proveedores de identidad (IdP) para los diferentes tipos de tráfico web que se originan en los sitios conectados.

Entorno

- Implementación de Cisco Secure Access (CSA)
- Conectividad de túnel IPsec entre sitios y CSA
- Perfiles de seguridad configurados con autenticación SSO
- Entorno mixto con varios dispositivos, incluidas impresoras y terminales que no son de Windows
- Inspección HTTPS habilitada
- Integración de SAML configurada

Resolución

El comportamiento de autenticación de SSO en Cisco Secure Access está diseñado específicamente para dirigirse únicamente al tráfico web basado en navegador. El sistema realiza un proceso de inspección sofisticado para determinar si las solicitudes web deben estar sujetas a la autenticación SSO.

Proceso de autenticación de SSO

Antes de redirigir una solicitud web a un proveedor de identidad (IdP), Cisco Secure Access utiliza la inspección HTTPS para determinar si una solicitud se origina en un navegador que admite cookies. Este proceso de inspección es el mecanismo clave que diferencia entre el tráfico web basado en navegador y el que no lo es.

Clasificación del tráfico

Tráfico basado en navegador (sujeto a autenticación SSO)

- Solicitudes web originadas en navegadores que admiten cookies
- Tráfico HTTP/HTTPS en los puertos TCP 80 y 443 desde las aplicaciones del navegador
- Tráfico que pasa la detección de la cookie/navegador de inspección HTTPS

Tráfico que no es del navegador (no sujeto a autenticación SSO)

- Tráfico web desde impresoras y otros dispositivos de red
- Aplicaciones que no admiten cookies o que no se identifican como navegadores
- Terminales que no son de Windows y generan tráfico web que no supera la detección del explorador

- Cualquier tráfico web que no pase la verificación del navegador de inspección HTTPS

Prerrequisitos de la Autenticación SSO

Para que la autenticación de SSO funcione correctamente en el entorno, se deben cumplir varios requisitos previos:

- La configuración SAML en funcionamiento debe estar en su lugar.
- Redes proxy con XFF y/o túneles sin NAT (el sustituto de IP necesita visibilidad para las IP privadas internas).
- La inspección HTTPS debe estar habilitada.
- Las sesiones del navegador deben mantener cookies (no se recomienda eliminar las cookies al final de la sesión o la navegación de incógnito).
- Direcciones IP no superpuestas entre ubicaciones o separación de sitios adecuada si existe superposición.

Causa

El comportamiento se basa en el diseño de Cisco Secure Access. El mecanismo de autenticación SSO está diseñado específicamente para dirigirse a sesiones de usuario interactivas a través de navegadores web, al tiempo que permite que los sistemas automatizados y los dispositivos no interactivos accedan a los recursos web sin interrupción de la autenticación. Este diseño evita la interrupción de los procesos automatizados, las interfaces de administración de dispositivos y las aplicaciones que no pueden gestionar las redirecciones de autenticación o las sesiones basadas en cookies.

Contenido relacionado

- Configurar integraciones SAML - Habilitar sustitutos IP para SAML
- 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).