Retos de identificación y aplicación de políticas por usuario en el gateway web seguro (SWG) para entornos de equipos compartidos con autenticación SAML y reenvío de tráfico basado en PAC

Contenido

Problema

En las implementaciones de Cisco Secure Web Gateway (SWG) que utilizan acceso seguro con autenticación SAML y reenvío de tráfico de sucursal a Internet o basado en PAC, solo el primer usuario que ha iniciado sesión en un equipo compartido se identifica correctamente para el tráfico web y la aplicación de políticas. Al cambiar de usuario, el tráfico web subsiguiente sigue atribuyéndose al usuario inicial, incluso cuando la opción Sustituto IP está desactivada y se utiliza un archivo PAC. Las consultas DNS reflejan el usuario activo correcto a través de Umbrella Virtual Appliance, pero los registros web y de firewall asignan de forma persistente la actividad al usuario anterior. La solicitud consiste en determinar si SWG admite la identificación por usuario y la aplicación de políticas en entornos de equipos compartidos y cómo garantizar la asignación correcta de usuarios.

Entorno

- Dispositivo virtual para la resolución de DNS.
- Autenticación SAML para la identidad del usuario.
- Mezcla de reenvío de tráfico con PAC y sin archivos PAC.
- Opción de sustituto IP activada, con subredes y hosts específicos omitidos para sustituto de cookie.
- Dispositivos in situ; sin terminales ni usuarios remotos.

Resolución

El problema se resolvió mediante la orientación sobre la configuración y la formación del usuario teniendo en cuenta los siguientes puntos:

- Utilice la identificación de sustituto de cookies con archivos PAC. El tráfico puede enrutarse dentro o fuera de un túnel de red.
- Utilice la identificación sustituta de cookies sin archivos PAC, pero el tráfico debe enrutarse

a través de un túnel de red.
- La política de acceso que desea aplicar como sustituto de las cookies debe tener habilitada la autenticación SAML en el perfil de seguridad.
- El tráfico sustituto de cookies es solo para tráfico basado en navegador. Se necesita una regla independiente para identificar el tráfico no cookie de la máquina (por ejemplo, equipos o tráfico Webex) con la identidad de origen como la red.
- El módulo SWG no debe estar en uso para que funcione el sustituto de cookies.
- Cuando el sustituto IP también está habilitado, debe agregar las direcciones IP privadas/subredes que pretenden utilizar sustituto de cookies en la lista de desvío (Usuarios y grupos - Administración de configuración - Configuración avanzada).
- La lista de omisión para el sustituto de cookies también coincide con prefijos más cortos. Por ejemplo, si agrega 10.10.10.0/24 into the bypass list, and you also have a defined network as 10.10.10.5/32, you must
- El sustituto de cookies permite al usuario cambiar de equipo sin tener que cerrar sesión para conservar varias identidades.

Gran parte de la solución de problemas ha sido la prueba de políticas y la búsqueda de actividades.

Causa

La causa principal de la identificación incorrecta de usuarios en entornos de equipos compartidos se debe principalmente a la formación de los usuarios.

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).