Bloquear el acceso a las cuentas de consumo de Google en el SWA

Contenido

Introducción

En este documento se describe el proceso de bloqueo del acceso a Google Workspace o a las cuentas de usuario de Google en Secure Web Appliance (SWA).

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- Acceso a la interfaz gráfica de usuario (GUI) de SWA
- Acceso administrativo al SWA.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

<table>
<tr>
<td>Paso 1.Crear una categoría de URL personalizado para los sitios de Google.</td>
<td>Paso 1.1. Desde la GUI, navegue hasta Web Security Manager y elija Custom y External URL Categories.

Paso 1.2. Haga clic en Agregar categoría para crear una nueva Categoría de URL personalizado.

Paso 1.3. Introduzca Name para la nueva categoría.

Paso 1.4. Defina estas URL en la sección Sitios:

<code>.google.com</code>

Paso 1.5. Ejecute los cambios.

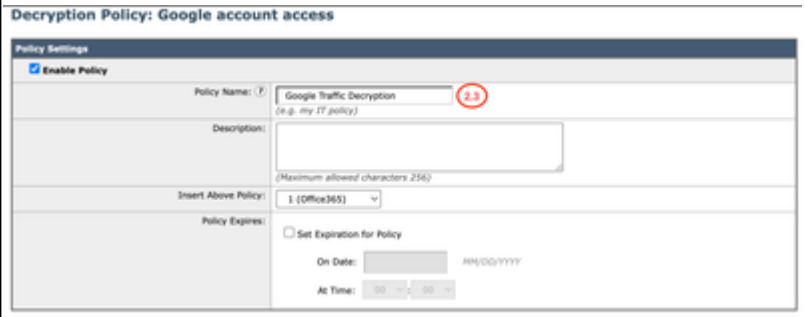
 

Imagen - Categoría de URL personalizado

Consejo: Para obtener más información sobre cómo configurar categorías de URL personalizadas, visite: Configure categorías de URL personalizadas en el dispositivo web seguro.</td>
</tr>
<tr>
<td>Paso 2.Descifrar el tráfico.</td>
<td>Paso 2.1. Desde la GUI, navegue hastaAdministrador de seguridad web y elijaPolíticas de descifrado.</td>
</tr>
</table>

Paso 2.2. Haga clic en Add Policy.

Paso 2.3. EnterName para la nueva política.



Paso 2.4. Seleccione el perfil de identificación al que necesita aplicar esta política.

Consejo: Si ha omitido las Autenticaciones para URL de Microsoft y está configurando esta directiva para Todos los usuarios, elija: Todos los perfiles de identificación > Todos los usuarios.

Paso 2.5. En la sección Definición de miembro de política, haga clic en los enlaces URL Categorías para agregar la categoría de URL personalizado.

Paso 2.6.Seleccione la categoría de URL que se creó en el Paso 1.

Paso 2.7.Haga clic en Enviar.

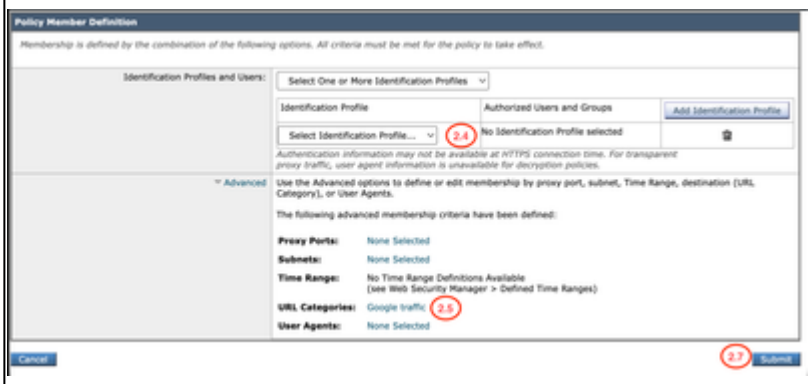
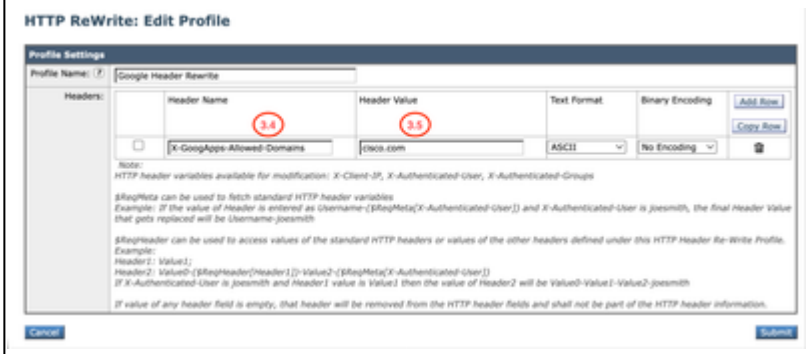
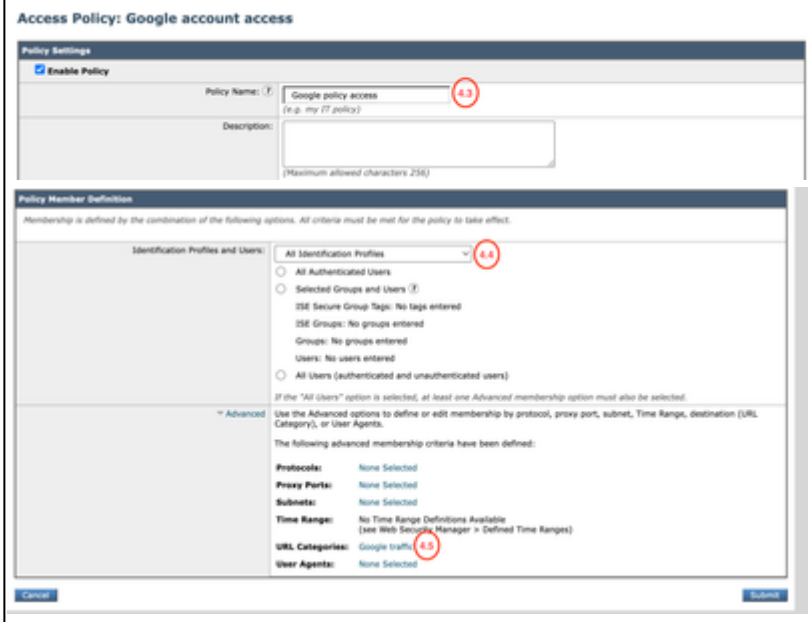
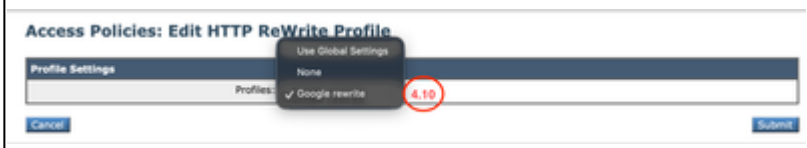


Imagen - Configurar política de descifrado

Paso 2.8. Página InDecryption Policies, haga clic en el enlace fromURL Filtering para la nueva política.

	Imagen - Editar acción de filtrado de URL Paso 2.9. Elegir descifrar como la acción para categoría de URL personalizado. Paso 2.10.Haga clic en Enviar.  Imagen - Descifrar la categoría de URL personalizado
Paso 3.Crear perfil de reescritura de HTTP.	Paso 3.1.En la GUI, navegue hastaAdministrador de seguridad web y elijaPerfiles de reescritura HTTP. Paso 3.2. Haga clic en Agregar perfil. Paso 3.3. EnterName para el nuevo perfil. Paso 3.4. Utilice X-GoogApps-Allowed-Domains para el firstHeader Name. Paso 3.5. Para la configuración Restrict-Access-To-Tenants, utilice un valor de dominio de la lista de arrendatarios permitidos, que debe ser una lista separada por comas de los arrendatarios a los que los usuarios pueden acceder. Paso 3.9.Haga clic en Enviar.  Imagen - Agregar perfil de reescritura HTTP

Paso 4.Crear directiva de acceso.	Paso 4.1. Desde la GUI, navegue hastaAdministrador de seguridad web y elijaPolíticas de acceso. Paso 4.2. Haga clic en Add Policy. Paso 4.3. EnterName para la nueva política. Paso 4.4. (Opcional) Seleccione el perfil de identificación al que necesita aplicar esta política. Paso 4.5.Desde la sección Definición de miembro de política, haga clic en los enlaces URL Categorías para agregar la categoría de URL personalizado. Paso 4.6.Seleccione la categoría de URL que se creó en el Paso 1. Paso 4.7. Haga clic en Enviar.  Imagen - Crear política de acceso Paso 4.8.En la página Políticas de acceso, asegúrese de que la acción del filtrado de URL está establecida en Monitor. Paso 4.9.Haga clic en el enlace en HTTP ReWrite Profile para agregar el HTTP Header Profile a esta política.  Imagen - Propiedades de directiva de acceso

	Paso 4.10. Elija los Perfiles de Reescritura HTTP, creados en el Paso [3].  Imagen - Agregar perfil de reescritura HTTP Paso 4.11. Haga clic en Enviar. Paso 4.12. CommitChanges.

Informes y registros

Registros

Puede agregar campos personalizados a los registros de acceso o a los registros de W3C para ver el nombre del perfil de reescritura del encabezado HTTP.

Especificador de formato en registros de acceso	Campo Log (Registro) en Registros W3C	Descripción
%]	x-http-rewrite-profile-name	Nombre del perfil de reescritura del encabezado HTTP.

Puede generar un informe de seguimiento web para ver los informes del tráfico por el nombre de la directiva de acceso.

Siga estos pasos para generar los informes:

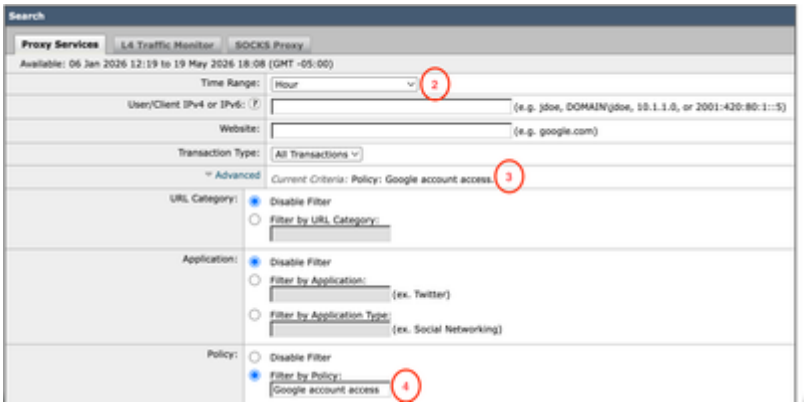
Paso 1. En la GUI, seleccioneInformes y elijaSeguimiento web.

Paso 2. Seleccione el rango de tiempo deseado.

Paso 3. Haga clic en el enlace Avanzado para buscar transacciones utilizando criterios avanzados.

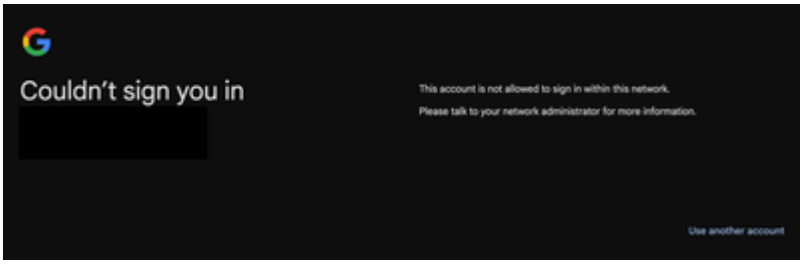
Paso 4. En la sección Política, seleccione Filtrar por Política y escriba el nombre de la Política de Acceso que se creó anteriormente.

Paso 5. Pulse Buscar para revisar el informe.



Verificación

Una vez finalizada la configuración de restricción de dominio de Google, el usuario sólo podrá acceder a las cuentas que se encuentren en el dominio configurado en el perfil Header Rewrite del paso 3. Si el usuario intenta acceder a una cuenta en un dominio diferente o, en otra cuenta personal de Google, el acceso se restringe con este aviso:



Información Relacionada

[Definición de categorías de URL personalizadas en WSA]

[Guía del usuario de AsyncOS 15.2 para Cisco Secure Web Appliance]

[Configurar certificado de descifrado en dispositivo web seguro]

[Reescritura del encabezado HTTP de WSA]

[Bloquear el acceso a cuentas de consumidores (Documentación de Google)]

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).