Bloqueo del modo Google AI en el dispositivo web seguro

Contenido

Introducción

Este documento describe los pasos necesarios que se deben realizar para que el Dispositivo web seguro esté configurado para bloquear las solicitudes HTTPS al Modo Google AI.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- administración SWA
- Protocolos básicos de red y proxy
- Proceso de descifrado de SWA
- Expresiones normales

Cisco recomienda tener instaladas estas herramientas:

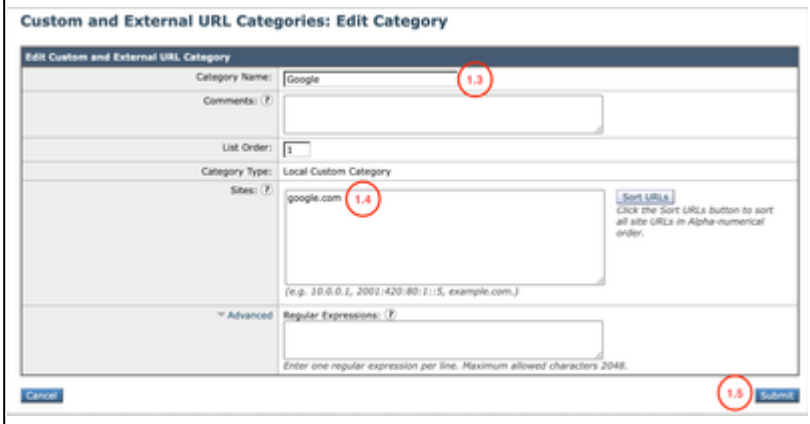
- SWA físico o virtual
- Acceso administrativo a la interfaz gráfica de usuario (GUI) de SWA

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.

Pasos de configuración

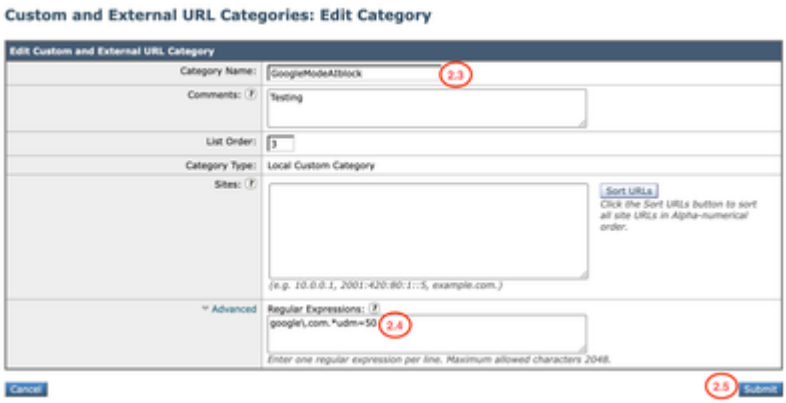
Paso 1. Crear una categoría de URL personalizado para el sitio web de Google.	Paso 1.1. Desde la GUI, navegue hasta Web Security Manager y elija Custom and External URL Categories. Paso 1.2. Haga clic en Agregar categoría para crear una nueva categoría de URL personalizada. Paso 1.3. Introduzca Name para la nueva categoría. Paso 1.4. Defina estas URL en la sección Sitios: `google.com` Paso 1.5. Envíe los cambios. 
Paso 2.Crear una categoría de URL personalizado para el modo Google AI.	Paso 2.1. Desde la GUI, navegue hasta Web Security Manager y elija Custom and External URL Categories. Paso 2.2. Haga clic en Agregar categoría para crear una nueva categoría de URL personalizada. Paso 2.3. Introduzca Name para la nueva categoría.

<table>
<tr>
<td></td>
<td>Paso 2.4. Defina estas URL en la sección Expresiones Regulares:

<code>google\.com.*udm=50</code>

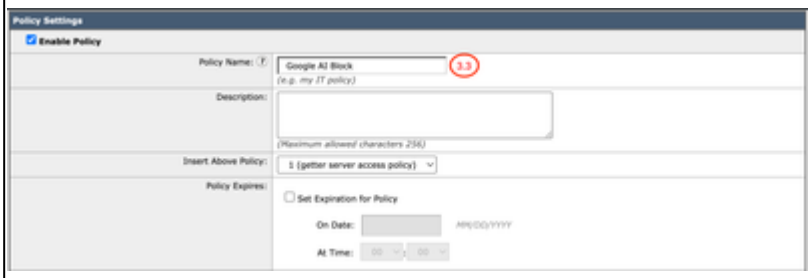
Paso 2.5. Envíe los cambios.

Consejo: Para obtener más información sobre cómo configurar categorías de URL personalizadas, visite: Configure Custom URL Categories in Secure Web Appliance - Cisco

 
</td>
</tr>
<tr>
<td>Paso 3. Descifrar el tráfico para Google.</td>
<td>Paso 3.1. Desde la GUI, navegue hasta Web Security Manager y elija Políticas de descifrado

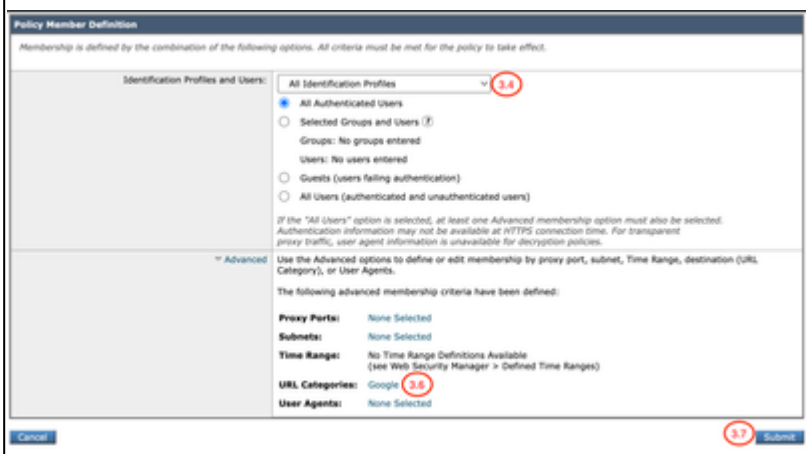
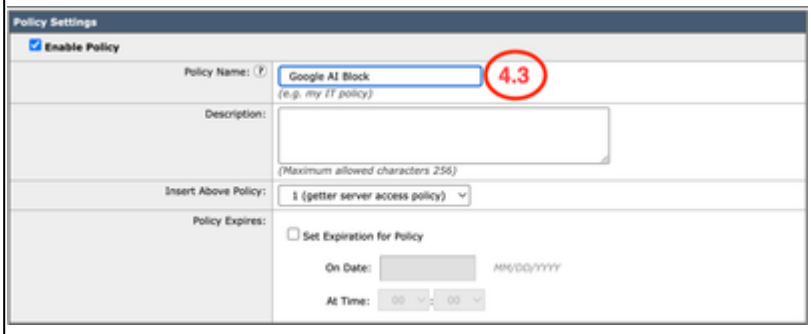
Paso 3.2. Haga clic en Agregar directiva.

Paso 3.3. Introduzca Name para la nueva política.

Paso 3.4. (Opcional) Seleccione el perfil de identificación al que necesita aplicar esta política.

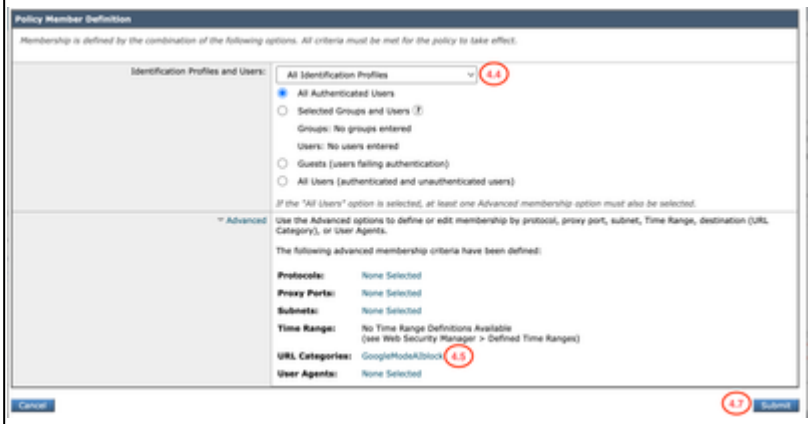
Paso 3.5. En la sección Definición de miembro de política, haga clic en los enlaces Categorías de URL para agregar la categoría de URL personalizado.</td>
</tr>
</table>

	Paso 3.6. Seleccione la categoría de URL que se creó en el Paso 1. Paso 3.7. Haga clic en Enviar.  Paso 3.8. En la página Políticas de descifrado, haga clic en el enlace de Filtrado de URL para la nueva política. Paso 3.9. Elija Decrypt como la acción para Custom URL Category. Paso 3.10. Haga clic en Enviar. 
Paso 4. Bloquear el tráfico de Google AI Mode.	Paso 4.1. Desde la GUI, navegue hasta Web Security Manager y elija Access Policies. Paso 4.2. Haga clic en Agregar directiva. Paso 4.3. Introduzca Name para la nueva política.  Paso 4.4. (Opcional) Seleccione el perfil de identificación al que necesita aplicar esta política.

Paso 4.5. En la sección Definición de miembro de política, haga clic en los enlaces Categorías de URL para agregar la categoría de URL personalizado.

Paso 4.6. Seleccione la categoría de URL que se creó en el Paso 2.

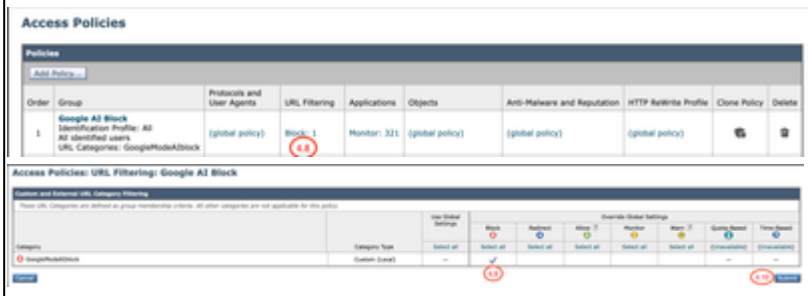
Paso 4.7. Haga clic en Enviar.



Paso 4.8. En la página Access Policies, haga clic en el enlace de URL Filtering para la nueva política.

Paso 4.9. Elija Block como la acción para Custom URL Category.

Paso 4.10. Haga clic en Enviar.



Paso 4.11. Realice los cambios.

Verificación

Cuando se completan los ajustes de configuración, el tráfico de Google AI se procesa en los registros de acceso como Block (Bloquear), ya que la categoría personalizada que creamos para Google AI Block lo detecta.

<#root>

```
1779219170.427 101 10.184.103.26
```

TCP_DENIED_SSL/403

```
 0 GET https://www.google.com:443/search?q=cisco+live+&sca_esv=afc85aa92f7b31d4&source=hp&ei=2roMatavIo
```

BLOCK_CUSTOMCAT_12-Google_AI_Block

```
-ciscotest-NONE-NONE-NONE-NONE-NONE <"C_Goo0",4.7,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,"IW_srch"
```

Una solicitud de consulta de búsqueda a través del modo Google AI se bloquea y muestra esta notificación de usuario final.

El resto del tráfico de Google sigue estando permitido.

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]

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).