

# Permitir a Google reCAPTCHA cuando el acceso a los portales del motor de búsqueda está bloqueado

## Contenido

---

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuration Steps](#)

[Verificación](#)

[Troubleshoot](#)

[Referencias](#)

---

## Introducción

Este documento describe los pasos para permitir Google reCAPTCHA en Secure Web Appliance (SWA), cuando haya bloqueado el acceso a los portales del motor de búsqueda.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Secure Web Access y descifrado HTTPS.

Cisco recomienda que también tenga:

- SWA físico o virtual instalado.
- Licencia activada o instalada.
- El asistente de configuración ha finalizado.
- 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.

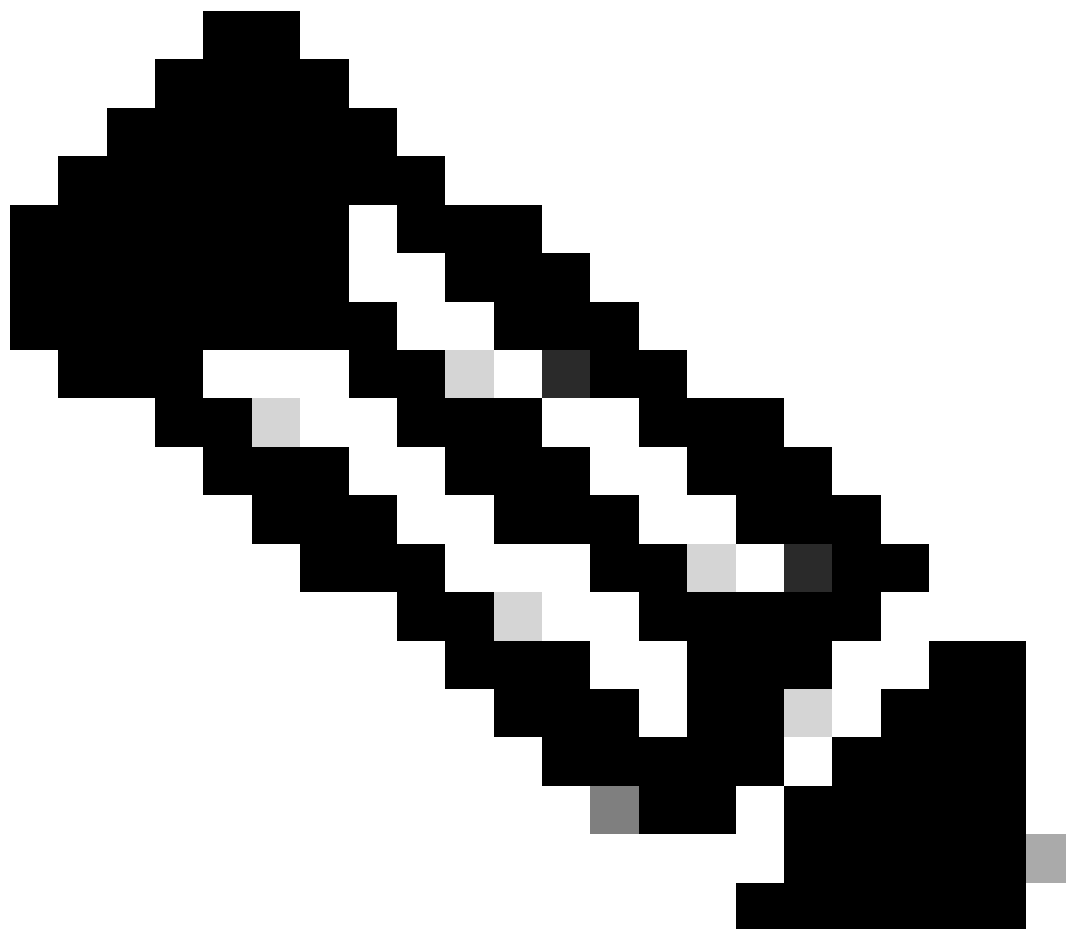
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en

funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Configuration Steps

**Paso 1.** En GUI, vaya a *Security Services* y seleccione *HTTPS Proxy*, enable *HTTPS decryption* (Activar descifrado HTTPS) si aún no está habilitado.

---



**Nota:** El descifrado HTTPS debe estar habilitado para esta configuración. Si no está habilitado, consulte el artículo al que se hace referencia al final de este documento.

---

**Paso 2.** Desde GUI, navegue hasta *Web Security Manager* y elija *Custom and External URL Categories*, cree dos categorías de URL

personalizadas, una para google.com y la otra para Google reCAPTCHA. Haga clic en Submit (Enviar).

**Cisco S100V** Web Security Virtual Appliance Web Security Appliance is ge

Reporting Web Security Manager Security Services Network System Administration

### Custom and External URL Categories: Edit Category

**Edit Custom and External URL Category**

Category Name:	<input type="text" value="Google"/>
Comments: (?)	<input type="text" value="Custom URL Category for Google"/>
List Order:	<input type="text" value="4"/>
Category Type:	Local Custom Category
Sites: (?)	<input type="text" value="google.com, .google.com"/> <small>(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)</small>
Advanced	Regular Expressions: (?) <input type="text"/> <small>Enter one regular expression per line. Maximum allowed characters 2048.</small>

[Sort URLs](#)  
Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

Crear categoría de URL personalizada para Google

**Cisco S100V** Web Security Virtual Appliance Web Security Appliance is

Reporting Web Security Manager Security Services Network System Administration

### Custom and External URL Categories: Edit Category

**Edit Custom and External URL Category**

Category Name:	<input type="text" value="Captchaallow"/>
Comments: (?)	<input type="text" value="Custom URL Category for Google RECAPTCHA"/>
List Order:	<input type="text" value="5"/>
Category Type:	Local Custom Category
Sites: (?)	<input type="text"/> <small>(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)</small>
Advanced	Regular Expressions: (?) <input type="text" value="www\.google\.com/recaptcha/"/> <small>Enter one regular expression per line. Maximum allowed characters 2048.</small>

[Sort URLs](#)  
Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

Crear categoría de URL personalizada para Google

**Paso 3.** Desde GUI, vaya a **Web Security Manager** y elija **Decryption Policies**, cree una política de descifrado para descifrar google.com. Haga clic en **Ninguno seleccionado** junto a **Categorías de URL** y seleccione la categoría de URL personalizado de **Google**. Haga clic en Submit (Enviar).

### Decryption Policy: Add Group

**Policy Settings**

**Enable Policy**

Policy Name: (?)   
*(e.g. my IT policy)*

Description:   
*(Maximum allowed characters 256)*

Insert Above Policy:  ▼

Policy Expires:

Set Expiration for Policy

On Date:  MM/DD/YYYY

At Time:  :

**Policy Member Definition**

*Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.*

Identification Profiles and Users:  ▼

*If "All Identification Profiles" is selected, at least one Advanced membership option must also be selected. Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.*

Advanced

Use the Advanced options to define or edit membership by proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

**Proxy Ports:** None Selected

**Subnets:** None Selected

**Time Range:** No Time Range Definitions Available  
(see Web Security Manager > Defined Time Ranges)

**URL Categories:** Google

**User Agents:** None Selected

*Política de descifrado para descifrar Google*

**Paso 3.1.** Navegue hasta **Políticas de descifrado** y haga clic en **Monitor** en línea con la política **GoogleDecrypt**.

**Paso 3.2.** Seleccione **Decrypt** en línea con **Google Category** y haga clic en **Submit**.

### Decryption Policies: URL Filtering: GoogleDecrypt

**Custom and External URL Category Filtering**

*These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.*

Category	Category Type	Use Global Settings	Override Global Settings					Quota-Based	Time-Based
			Pass Through	Monitor	Decrypt	Drop (?)			
		Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)	
Google	Custom (Local)	—			✓		—	—	

*Seleccione Categoría de URL personalizada creada para que Google la descifre en la política de descifrado*

**Paso 4.** Desde GUI, navegue hasta **Web Security Manager** y elija **Access Policies**, cree una política de acceso para permitir Google reCAPTCHA y seleccione **captchallow** como **categorías de URL**.

### Access Policy: Add Group

**Policy Settings**

**Enable Policy**

Policy Name:  (e.g. my IT policy)

Description:  (Maximum allowed characters 256)

Insert Above Policy:  ▼

Policy Expires:  Set Expiration for Policy

On Date:  MM/DD/YYYY

At Time:  :

---

**Policy Member Definition**

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:  ▼

If "All Identification Profiles" is selected, at least one Advanced membership option must also be selected.

▼ **Advanced** Use the Advanced options to define or edit membership by protocol, proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

**Protocols:** None Selected

**Proxy Ports:** None Selected

**Subnets:** None Selected

**Time Range:** No Time Range Definitions Available  
(see Web Security Manager > Defined Time Ranges)

**URL Categories:** Captchaallow

**User Agents:** None Selected

Cancel
Submit

Política de acceso para permitir Google RECAPTCHA

**Paso 4.1.** Navegue hasta **Access Policies** y haga clic en **Monitor** en línea con la política **GoogleCaptchaAccessPolicy**. Seleccione **Allow** in line to **Captchallow** Category. **Enviar** y **registrar cambios**.

### Access Policies: URL Filtering: GoogleCaptchaAccessPolicy

Custom and External URL Category Filtering					
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.					
Category	Category Type	Use Global Settings	Block	Redirect	Allow (?)
		Select all	Select all	Select all	Select all
Captchaallow	Custom (Local)	-			
					Ove

Cancel

Seleccione **Created Custom URL Category** for Google RECAPTCHA to Allow it in the Access Policy

**Paso 5.** Asegúrese de que **Motores de búsqueda y portales** en **Filtrado de categoría de URL predefinido** esté bloqueado en la política de acceso global:

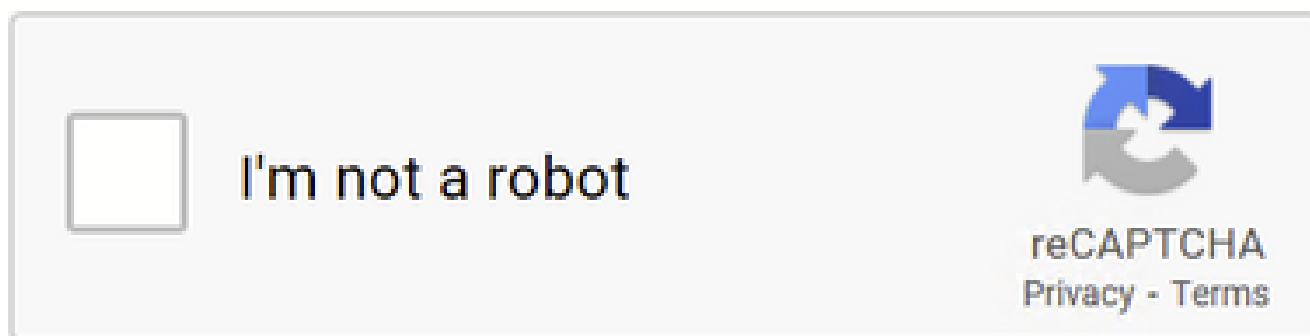
## Access Policies: URL Filtering: Global Policy

Custom and External URL Category Filtering	
No Custom Categories are included for this Policy.	
<input type="button" value="Select Custom Categories..."/>	
Predefined URL Category Filtering	
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.	
Category	<input type="checkbox"/> Block <input type="checkbox"/> Select all
<input type="radio"/> Regional Restricted Sites (Poland)	
<input type="radio"/> Religion	
<input type="radio"/> SaaS and B2B	
<input type="radio"/> Safe for Kids	
<input type="radio"/> Science and Technology	
<input checked="" type="radio"/> Search Engines and Portals	<input checked="" type="checkbox"/>
<input type="radio"/> Sex Education	

Política predeterminada para bloquear el acceso a los motores de búsqueda

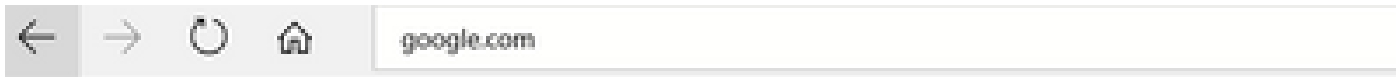
## Verificación

Puede ver el acceso a Google reCAPTCHA funciona, pero el acceso al motor de búsqueda (Google) sigue siendo denegado, después de activar el descifrado HTTPS y permitir el acceso a Google reCAPTCHA en la política de acceso:



Google CAPTCHA funciona

1675880489.667 279 10.106.40.203 TCP\_MISS\_SSL/200 23910 GET <https://www.google.com:443/recaptcha/api2/anchor?ar=1&k=6LdN4qUZAAAAA>



## This Page Cannot Be Displayed

Based on your organization's access policies, access to this web site ( <http://google.com/> ) has been blocked because the web category "Search Engines and Portals" is not allowed.

If you have questions, please contact your organization's network administrator and provide the codes shown below.

Date: Wed, 08 Feb 2023 18:23:01 GMT

Username:

Source IP: 10.106.40.203

URL: GET <http://google.com/>

Category: Search Engines and Portals

Reason: BLOCK-WEBCAT

Notification: WEBCAT

*El sitio de Google está bloqueado*

1675880581.157 0 10.106.40.203 TCP\_DENIED/403 0 GET "<https://google.com/favicon.ico>" - NONE/- - BLOCK\_WEBCAT\_12-DefaultGroup-DefaultC

### Troubleshoot

Si el acceso a Google reCAPTCHA está bloqueado, puede comprobar los registros de acceso en la CLI de SWA. Si ve la URL de Google y no la URL de Google reCAPTCHA, puede ser que el descifrado no esté habilitado:

1675757652.291 2 192.168.100.79 TCP\_DENIED/403 0 CONNECT tunnel://[www.google.com:443/](http://www.google.com:443/) - NONE/- - BLOCK\_WEBCAT\_12-DefaultGroup-F

### Referencias

- [Guía del usuario de AsyncOS 14.5 para Cisco Secure Web Appliance - GD \(implementación general\) - Conexión, instalación y configuración \[Cisco Secure Web Appliance\] - Cisco](#)
- [Uso de certificados WSA para descifrado HTTPS](#)

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).