

Habilitar canal/vídeo específico de YouTube y bloquear el resto de YouTube en SWA

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configuration Steps](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo permitir canales/videos específicos de YouTube y bloquear el resto de YouTube 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.

Configuration Steps

Siga estos pasos para permitir un canal de YouTube específico mientras el acceso a YouTube está bloqueado:

Paso 1. Cree categorías de URL externas y personalizadas para el canal que necesita conceder

acceso; en este ejemplo, esta categoría de URL se denomina "canal".

Paso 1.1. En GUI, vaya a Web Security Manager y elija Custom URL and External Categories.

Authentication

Identification Profiles

SaaS Policies

Web Policies

Decryption Policies

Routing Policies

Access Policies

Overall Bandwidth Limits

Data Transfer Policies

Cisco Data Security

Outbound Malware Scanning

External Data Loss Prevention

Web Traffic Tap Policies

SOCKS Policies

Custom Policy Elements

Custom and External URL Categories

: asegúrese de que la categoría de URL personalizada 'Canal' tenga una prioridad inferior a la categoría de URL personalizada 'YouTube'.

Custom and External URL Categories



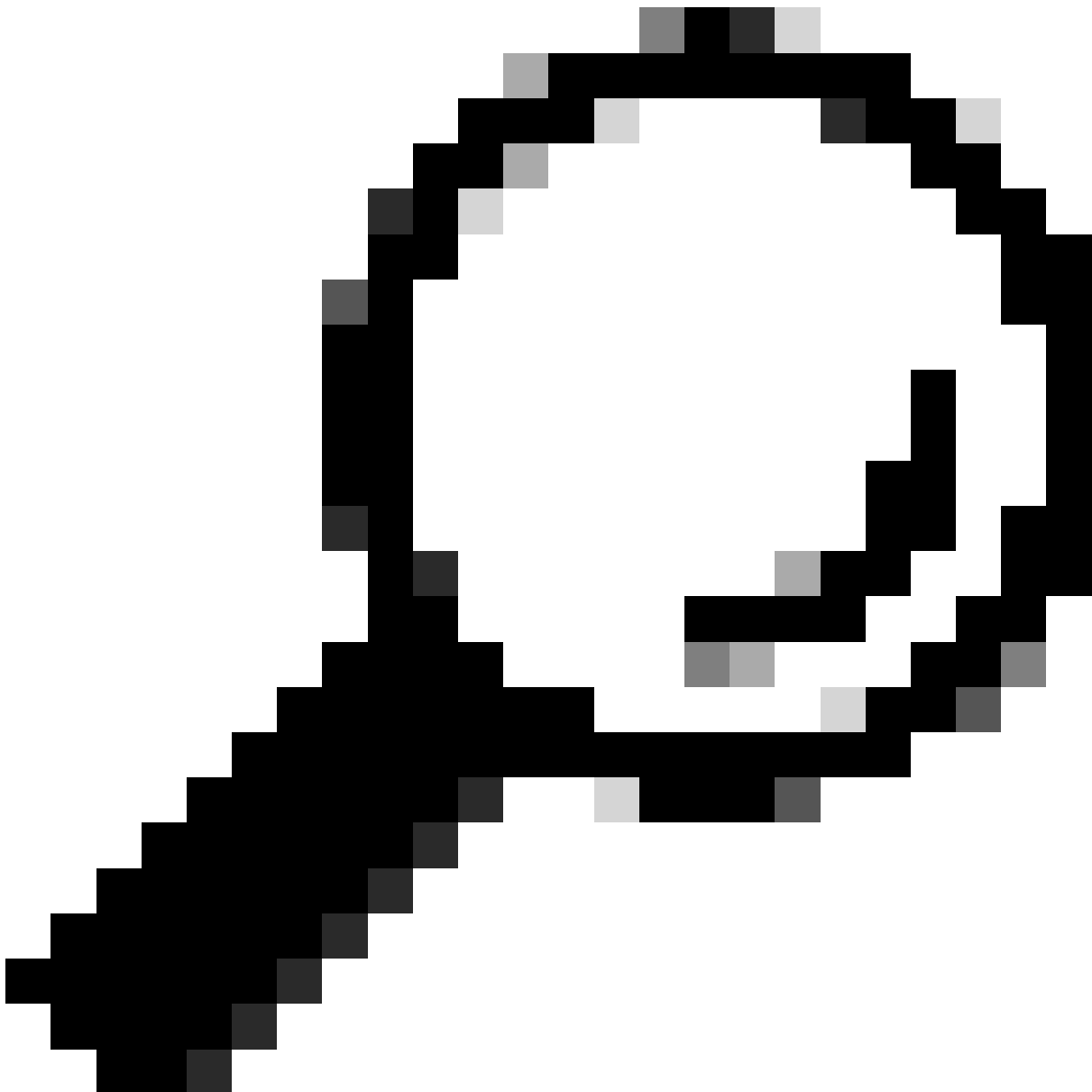
Categories List						
Add Category...						
Order	Category	Category Type	Comments	Last Updated	Feed Content	Delete
1	Channel	Custom (Local)		N/A	-	
2	YouTube	Custom (Local)	Block Access to YouTube	N/A	-	

Imagen- URL personalizado Categoría Order.png

Paso 3. Cree perfiles de identificación para los usuarios que tienen permiso para acceder al canal de YouTube.



Sugerencia: Puede establecer las categorías personalizadas en la política de acceso y descifrado. En este caso, no es necesario establecer un perfil de ID independiente.

Paso 3.1. Desde GUI, navegue hasta Web Security Manager y elija Identification Profiles.

Paso 3.2. Elija Agregar perfil de identificación.

Paso 3.3. Introduzca el nombre del perfil.

Paso 3.4. Elija los usuarios o defina los miembros por subred IP.

Paso 3.5. Haga clic en la sección Advanced y elija URL Categories.

Identification Profiles: Users Allowed To View Channel

The screenshot displays the configuration interface for an Identification Profile. It is divided into three main sections: Client / User Identification Profile Settings, User Identification Method, and Membership Definition.

- Client / User Identification Profile Settings:**
 - Enable Identification Profile**
 - Name:** Users Allowed To View Channel (e.g. my IT Profile)
 - Description:** Users Allowed to View Channel (Maximum allowed characters 256)
 - Insert Above:** 1 (Global Profile)
- User Identification Method:**
 - Identification and Authentication:** For additional options, define an authentication realm (see Network > Authentication) or enable ISE (see Network > Identity Services Engine).
- Membership Definition:**
 - Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.*
 - Define Members by Subnet:** 10.0.0.0/8 (examples: 10.1.1.0, 10.1.1.0/24, 10.1.1.1-10, 2001:420:80:1::5, 2000:db8::1-2000:db8::10)
 - Define Members by Protocol:** HTTP/HTTPS
 - Advanced:** Use the Advanced options to define or edit membership by proxy port, destination (URL Category), or User Agents. The following advanced membership criteria have been defined:
 - Proxy Ports:** None Selected
 - URL Categories:** None Selected
 - User Agents:** None Selected*The Advanced options may be protocol-specific. For instance, user agent strings are applicable only for HTTP and decrypted HTTPS. Similarly, URL Categories, including Custom URL Categories are not applicable for SOCKS transactions or transparent HTTPS (unless decrypted). When Advanced options that do not apply to a protocol are selected, no transactions in that protocol will match this Identity, regardless of the protocol selection above.*

Imagen- Crear perfil de ID

Paso 3.6. Agregue las dos categorías de URL que se crearon en el paso 1 y el paso 2 y haga clic en Finalizado.

Identity Profiles: Policy "Users Allowed To View Channel": Membership by URL Categories

Advanced Membership Definition: URL Category

Select any row below to use that URL Category as membership criteria. Leave all rows unselected if membership by URL Category is not desired.

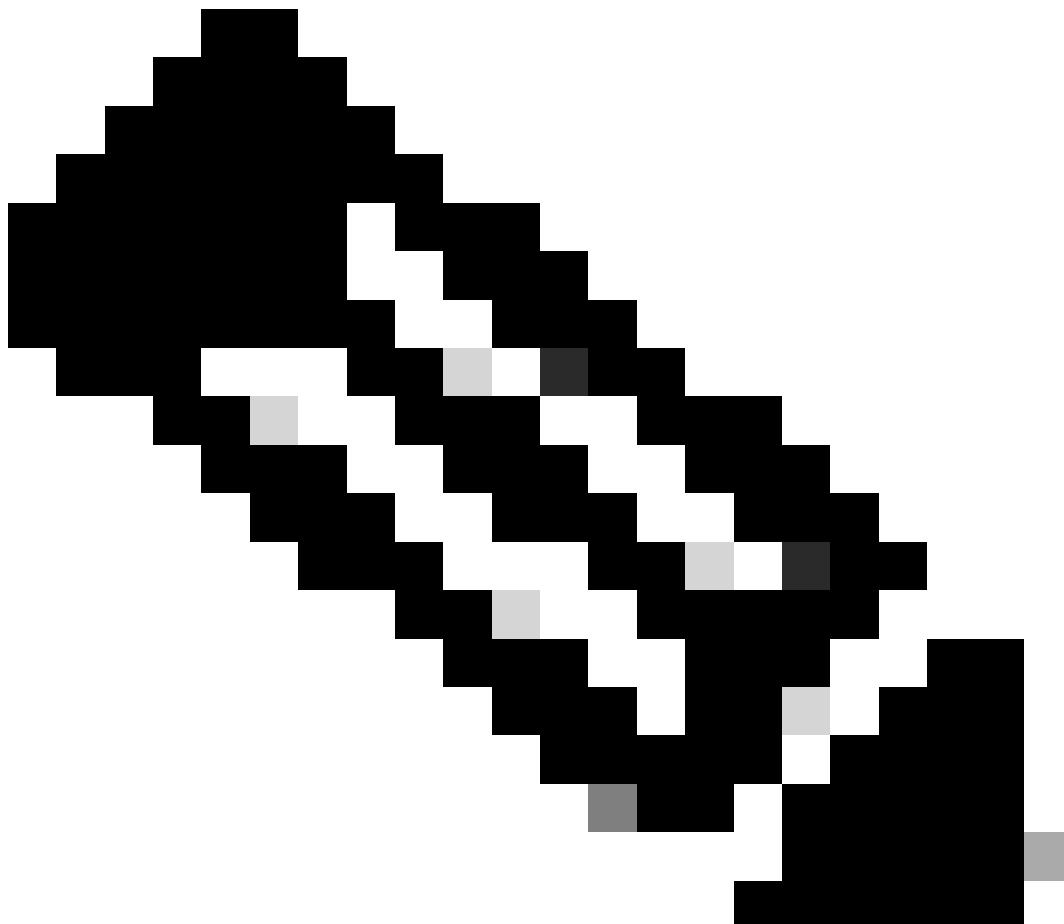
Custom and External URL Categories		
Category	Category Type	
Channel	Custom (Local)	<input type="checkbox"/>
YouTube	Custom (Local)	<input type="checkbox"/>

Add
Select all
✓
✓

Imagen- Agregar categorías de URL

Paso 3.7. Enviar cambios.

Paso 4. Cree una política de descifrado para descifrar el tráfico de YouTube. En este ejemplo, el nombre de la política es Descifrar Youtube.



Nota: Si no descifra el tráfico de YouTube, SWA no podrá determinar la dirección del

canal en la implementación de Transparente.

Paso 4.1. Desde GUI, navegue hasta Web Security Manager y elija Políticas de descifrado.

Paso 4.2. Elija Add Políticas e ingrese el nombre de la política.

Paso 4.3. Elija el perfil de identificación que creó en el paso 3.

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:

Identification Profile	Authorized Users and Groups	Add Identification Profile
<input type="text" value="Users Allowed To View Channel"/>	No authentication required	<input type="button" value="Add Identification Profile"/>

Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.

Define additional group membership criteria.

Imagen- Crear política de descifrado

Paso 4.4. Envíe los cambios.

Paso 4.5. En la página Políticas de descifrado, haga clic en Monitor en la sección Filtrado de URL.

Decryption Policies

Policies						
Add Policy...						
Order	Group	URL Filtering	Web Reputation	Default Action	Clone Policy	Delete
1	Decrypt Youtube Identification Profile: Users Allowed To View Channel All identified users	Monitor: 2	(global policy)	(global policy)		
Global Policy Identification Profile: All		Monitor: 107	Enabled	Decrypt		
Edit Policy Order...						

Imagen: haga clic en Filtrado de URL

Paso 4.6. Elija Decrypt para ambas categorías de URL y Submit.

Decryption Policies: URL Filtering: Decrypt Youtube

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					
			Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
		Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Channel	Custom (Local)	—			<input checked="" type="checkbox"/>		—	—
YouTube	Custom (Local)	—			<input checked="" type="checkbox"/>		—	—

Cancel Submit

Imagen: elija Descifrar

Paso 5. Cree una política de acceso para configurar el acceso al canal de YouTube. En este ejemplo, el nombre de la política es Allow YouTube.

Paso 5.1. Desde GUI, navegue hasta Web Security Manager y elija Access Policies.

Paso 5.2. Haga clic en Add Policy e ingrese el nombre de la política.

Paso 5.3. Elija el perfil de identificación que creó en el paso 3.

Access Policy: Add Group

Policy Settings

Enable Policy

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

Description:
(Maximum allowed characters 256)

Insert Above Policy: 1 (Global 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: Select One or More Identification Profiles

Identification Profile	Authorized Users and Groups	
Users Allowed To View Channel	No authentication required	<input type="button" value="Add Identification Profile"/>

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: HTTP/HTTPS/FTP over HTTP in Identification Profile Users Allowed To View Channel

Proxy Ports: None Selected

Subnets: None Selected

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

URL Categories: URL Categories Channel, YouTube in Identification Profile Users Allowed To View Channel

User Agents: None Selected

Imagen- Crear política de acceso

Paso 5.4. Enviar cambios.

Paso 5.5. En la página Access Policies, haga clic en Monitor en la sección URL Filtering.

Access Policies

Policies									
<input type="button" value="Add Policy..."/>									
Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects	Anti-Malware and Reputation	HTTP ReWrite Profile	Clone Policy	Delete
1	Allow YouTube Identification Profile: Users Allowed To View Channel All identified users	(global policy)	Monitor: 2	(global policy)	(global policy)	(global policy)	(global policy)		
	Global Policy Identification Profile: All	No blocked items	Monitor: 107	Monitor: 342	No blocked items	Web Reputation: Enabled Secure Endpoint: Enabled Anti-Malware Scanning: Enabled	None		

Imagen- Configurar política de acceso

Paso 5.6. Elija Allow para la categoría Channel.

Paso 5.7. Elija Block para la categoría YouTube.

Access Policies: URL Filtering: Allow YouTube

Custom and External URL Category Filtering		Use Global Settings		Override Global Settings												
Category	Category Type	Select all	Block	Select all	Redirect	Select all	Allow ?	Select all	Monitor	Select all	Warn ?	Select all	Quota-Based	(Unavailable)	Time-Based	(Unavailable)
Channel	Custom (Local)	--											--	--	--	--
YouTube	Custom (Local)	--		✓				✓					--	--	--	--

Acción de categoría de conjunto de imágenes

Paso 5.8. En la misma página, desplácese hasta Excepciones al bloqueo de contenido incrustado/referido y Habilitar excepciones de referencia.

Paso 5.9. Elija Todo el contenido incrustado/referido.

Exceptions to Blocking for Embedded/Referred Content

A web site may embed or refer to content that is categorized as a different category, or that is considered an application. For example, a News web site could contain content categorized as Streaming Video, and that is identified as being the application Youtube. By default, embedded content is blocked or monitored based on the action selected for its own category / application, regardless of what web site it is embedded in. Use this table to set exceptions (e.g., to permit all content referred from News web sites, or from a custom category representing your intranet).

Enable Referrer Exceptions

Set Exception for Content Referred by These Categories:

Set Exception for This Referred Content:

Imagen- Habilitar el remitente

Paso 5.10. En Set Exception for Content Referred by These Categories, elija la categoría de URL personalizada de **YouTube**.

Exceptions to Blocking for Embedded/Referred Content

A web site may embed or refer to content that is categorized as a different category, or that is considered an application. For example, a News web site could contain content categorized as Streaming Video, and that is identified as being the application Youtube. By default, embedded content is blocked or monitored based on the action selected for its own category / application, regardless of what web site it is embedded in. Use this table to set exceptions (e.g., to permit all content referred from News web sites, or from a custom category representing your intranet).

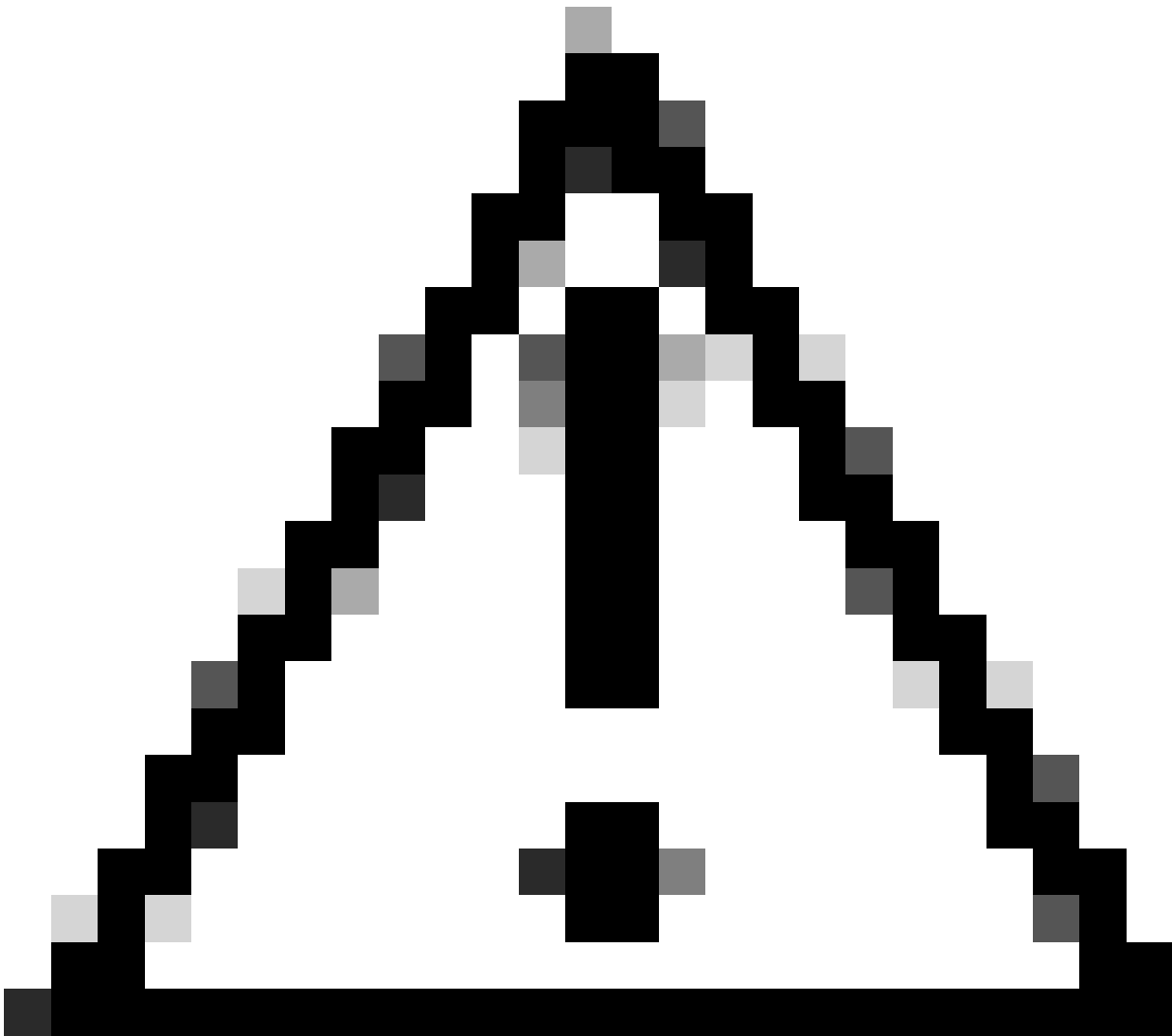
Enable Referrer Exceptions

Set Exception for Content Referred by These Categories:

Set Exception for This Referred Content:

Imagen- Configurar contenido incrustado

Paso 5.11. **Enviar** y **registrar** cambios.



Precaución: si los usuarios acceden primero al canal, podrán navegar hasta todos los vídeos de YouTube.

Información Relacionada

- [Guía del usuario de AsyncOS 15.0 para Cisco Secure Web Appliance - GD\(General Deployment\) - Resolución de problemas \[Cisco Secure Web Appliance\] - Cisco](#)
- [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).