

# Permitir reCAPTCHA do Google quando o acesso aos portais do mecanismo de pesquisa for bloqueado

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configuration Steps](#)

[Verificar](#)

[Troubleshooting](#)

[Referências](#)

---

## Introdução

Este documento descreve as etapas para permitir que o Google reCAPTCHA no Secure Web Appliance (SWA), quando você tiver bloqueado o acesso aos portais do mecanismo de pesquisa.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Secure Web Access ecriptografia HTTPS.

A Cisco recomenda que você também tenha:

- SWA físico ou virtual instalado.
- Licença ativada ou instalada.
- O assistente de instalação foi concluído.
- Acesso administrativo à interface gráfica do usuário (GUI) do SWA.

### Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

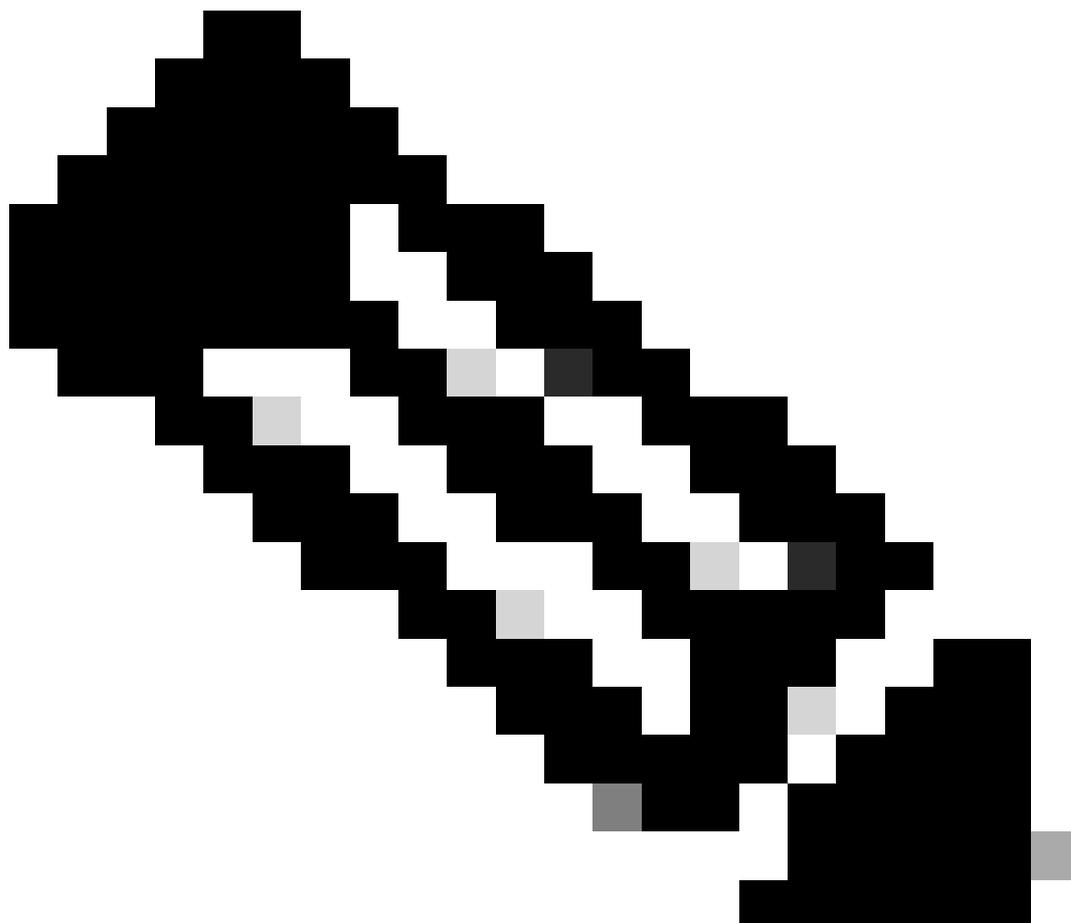
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto

potencial de qualquer comando.

## Configuration Steps

Etapa 1. Na GUI, navegue até Security Services e escolha HTTPS Proxy, habilitar descryptografia HTTPS se ainda não estiver habilitada.

---



**Observação:** a descryptografia HTTPS deve ser habilitada para esta configuração. Se não estiver habilitado, consulte o artigo mencionado no final deste documento.

---

Etapa 2. Na GUI, navegue até Web Security Manager e escolha Custom and External URL Categories, crie duas categorias de URL personalizadas, uma para google.com e outra para o Google reCAPTCHA. Clique em Submit.

### 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"/> <div style="float: right; text-align: right;"> <a href="#">Sort URLs</a>  <small>Click the Sort URLs button to sort all site URLs in Alpha-numerical order.</small> </div> <p><small>(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)</small></p>
Advanced	Regular Expressions: (?) <input type="text"/> <small>Enter one regular expression per line. Maximum allowed characters 2048.</small>

[Cancel](#)

[Submit](#)

Criar categoria de URL personalizada para o Google

### 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"/> <div style="float: right; text-align: right;"> <a href="#">Sort URLs</a>  <small>Click the Sort URLs button to sort all site URLs in Alpha-numerical order.</small> </div> <p><small>(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)</small></p>
Advanced	Regular Expressions: (?) <input type="text" value="www\.google\.com/recaptcha/"/> <small>Enter one regular expression per line. Maximum allowed characters 2048.</small>

[Cancel](#)

[Submit](#)

Criar categoria de URL personalizada para o Google

**Etapla 3.** Na GUI, navegue até **Web Security Manager** e escolha **Decryption Policies**, crie a política de descriptografia para descriptografar google.com. Clique em **Nenhum selecionado** ao lado de **Categorias de URL** e selecione **Google** categoria de URL personalizada. Clique em

Submit.

## 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:   
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 descryptografia para descryptografar o Google

**Etapa 3.1.** Navegue até **Decryption Policies** e clique em **Monitor** de acordo com a **políticaGoogleDecrypt**.

**Etapa 3.2.** Selecione **Decrypt** na linha para **Google Category** e clique em **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					
			Pass Through	Monitor	Decrypt	Drop	Quota-Based	Time-Based
		Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
Google	Custom (Local)	—			<input checked="" type="checkbox"/>		—	—

Selecione a categoria de URL personalizada criada para o Google para descryptografá-la na política de descryptografia

**Etapa 4.** Na GUI, navegue para **Web Security Manager** e escolha **Access Policies**, crie Access policy para permitir que o Google reCAPTCHA e selecione **captchaallow** como **URL Categories**.

## 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 acesso para permitir o Google RECAPTCHA

**Etapa 4.1.** Navegue para **Access Policies** e clique em **Monitor** de acordo com a política do **GoogleCaptchaAccessPolicy**. Selecione **Permitir** na linha para **Captchaallow** Categoria. **Enviar** e **confirmar alterações**.

### 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	Over		
			Block	Redirect	Allow
Captchaallow	Custom (Local)	—	Select all	Select all	Select all

Cancel

Selecione a categoria de URL personalizada criada para o Google RECAPTCHA para permitir na política de acesso

**Etapa 5.** Certifique-se de que os **mecanismos de pesquisa e portais** em **Filtragem de categoria de URL predefinida** estejam bloqueados na política de acesso 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	Block ⊘ 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 type="radio"/> Sex Education	

Política padrão para bloquear o acesso a mecanismos de pesquisa

### Verificar

Você pode ver o acesso ao Google reCAPTCHA funciona, mas o acesso ao mecanismo de pesquisa (Google) ainda é negado, depois que você habilita a descryptografia HTTPS e permite o acesso ao Google reCAPTCHA na política de acesso:



Google CAPTCHA Works

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

*O site do 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

### Troubleshooting

Se o acesso ao Google reCAPTCHA estiver bloqueado, você poderá verificar os logs de acesso na CLI SWA. Se você vir o URL do Google e não o URL reCAPTCHA do Google, pode ser que acriptografia não esteja ativada:

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

### Referências

- [Manual do usuário do AsyncOS 14.5 para Cisco Secure Web Appliance - GD \(General Deployment\) - Conectar, Instalar e Configurar \[Cisco Secure Web Appliance\] - Cisco](#)
- [Uso do certificado WSA paracriptografia HTTPS](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.