

Allow Google reCAPTCHA when Access to Search Engine Portals Is Blocked

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configuration Steps](#)

[Verify](#)

[Troubleshoot](#)

[References](#)

Introduction

This document describes the steps to allow Google reCAPTCHA in Secure Web Appliance (SWA), when you have blocked the access to Search Engine Portals.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Web Access and HTTPS decryption.

Cisco recommends that you also have:

- Physical or Virtual SWA Installed.
- License activated or installed.
- The setup wizard is completed.
- Administrative Access to the SWA Graphical User Interface (GUI).

Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configuration Steps

Step 1. From GUI navigate to Security Services and choose HTTPS Proxy, enable HTTPS decryption if it is not already enabled.



Note: HTTPS Decryption must be enabled for this configuration. If it is not enabled, please refer the referenced article given at the end of this document.

Step 2. From GUI navigate to **Web Security Manager** and choose **Custom and External URL Categories**, create two custom URL categories, one for google.com and the other for Google reCAPTCHA. Click **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;"> Sort URLs Click the Sort URLs button to sort all site URLs in Alpha-numerical order. </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](#)

Create Custom URL Category for 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;"> Sort URLs Click the Sort URLs button to sort all site URLs in Alpha-numerical order. </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](#)

Create Custom URL Category for Google

Step 3. From GUI navigate to **Web Security Manager** and choose **Decryption Policies**, create decryption policy to decrypt google.com. Click **None Selected** next to the **URL Categories** and select **Google** custom

URL category. Click **Submit**.

Decryption Policy: Add Group

Policy Settings

Enable Policy

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

Description:
(Maximum allowed characters 256)

Insert Above Policy: 1 (dropciscospecific) ▾

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: All Identification Profiles ▾

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

Cancel
Submit

Decryption Policy to Decrypt Google

Step 3.1. Navigate to **Decryption Policies** and click **Monitor** in line to the **GoogleDecrypt** policy.

Step 3.2. Select **Decrypt** in line to **Google Category** and Click **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)	—			✓		—	—

Cancel
Submit

Select Created Custom URL Category for Google to Decrypt it in the Decryption Policy

Step 4. From GUI navigate to **Web Security Manager** and choose **Access Policies**, create Access policy to allow Google reCAPTCHA and select **captchaallow** as **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

Access Policy to Allow Google RECAPTCHA

Step 4.1. Navigate to **Access Policies** and click **Monitor** in line to the **GoogleCaptchaAccessPolicy** policy. Select **Allow** in line to **Captchaallow** Category. **Submit** and **Commit Changes**.

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

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

Step 5. Make sure that **Search Engines and Portals** in **Predefined URL Category Filtering** is blocked in the global access policy:

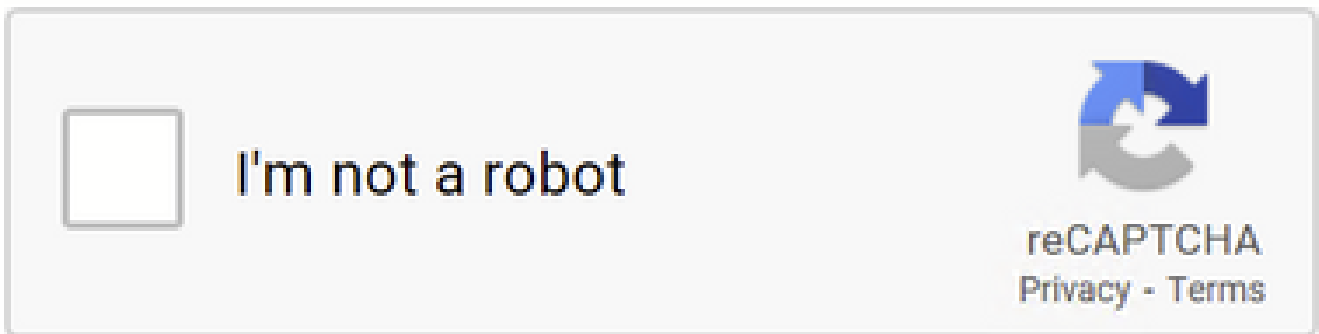
Access Policies: URL Filtering: Global Policy

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	

Default Policy to Block the Access to Search Engines

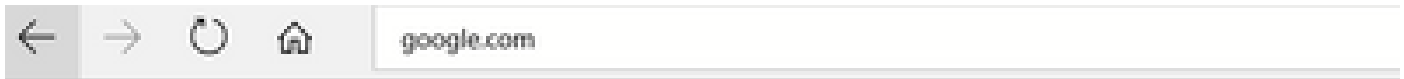
Verify

You can see access to Google reCAPTCHA works, but search engine (Google) access is still denied, after you enable HTTPS decryption and allow the access to Google reCAPTCHA in the access policy:



Google CAPTCHA Works

1675880489.667 279 10.106.40.203 TCP_MISS_SSL/200 23910 GET <https://www.google.com:443/recaptcha/api2/a>



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

Google Site is Blocked

```
1675880581.157 0 10.106.40.203 TCP_DENIED/403 0 GET "https://google.com/favicon.ico" - NONE/- - BLOCK_W
```

Troubleshoot

If the access to the Google reCAPTCHA is blocked, you can check the access logs in the SWA CLI. If you see Google URL and not the Google reCAPTCHA URL, it can be that decryption is not enabled:

```
1675757652.291 2 192.168.100.79 TCP_DENIED/403 0 CONNECT tunnel://www.google.com:443/ - NONE/- - BLOCK_L
```

References

- [User Guide for AsyncOS 14.5 for Cisco Secure Web Appliance - GD \(General Deployment\) - Connect, Install, and Configure \[Cisco Secure Web Appliance\] - Cisco](#)
- [WSA Certificate Usage for HTTPS Decryption](#)