

Autoriser Google reCAPTCHA lorsque l'accès aux portails des moteurs de recherche est bloqué

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configuration Steps](#)

[Vérifier](#)

[Dépannage](#)

[Références](#)

Introduction

Ce document décrit les étapes à suivre pour autoriser Google reCAPTCHA dans Secure Web Appliance (SWA), lorsque vous avez bloqué l'accès aux portails des moteurs de recherche.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Secure Web Access et déchiffrement HTTPS.

Cisco vous recommande également de disposer des éléments suivants :

- SWA physique ou virtuel installé.
- Licence activée ou installée.
- L'Assistant de configuration est terminé.
- Accès administratif à l'interface utilisateur graphique (GUI) de SWA.

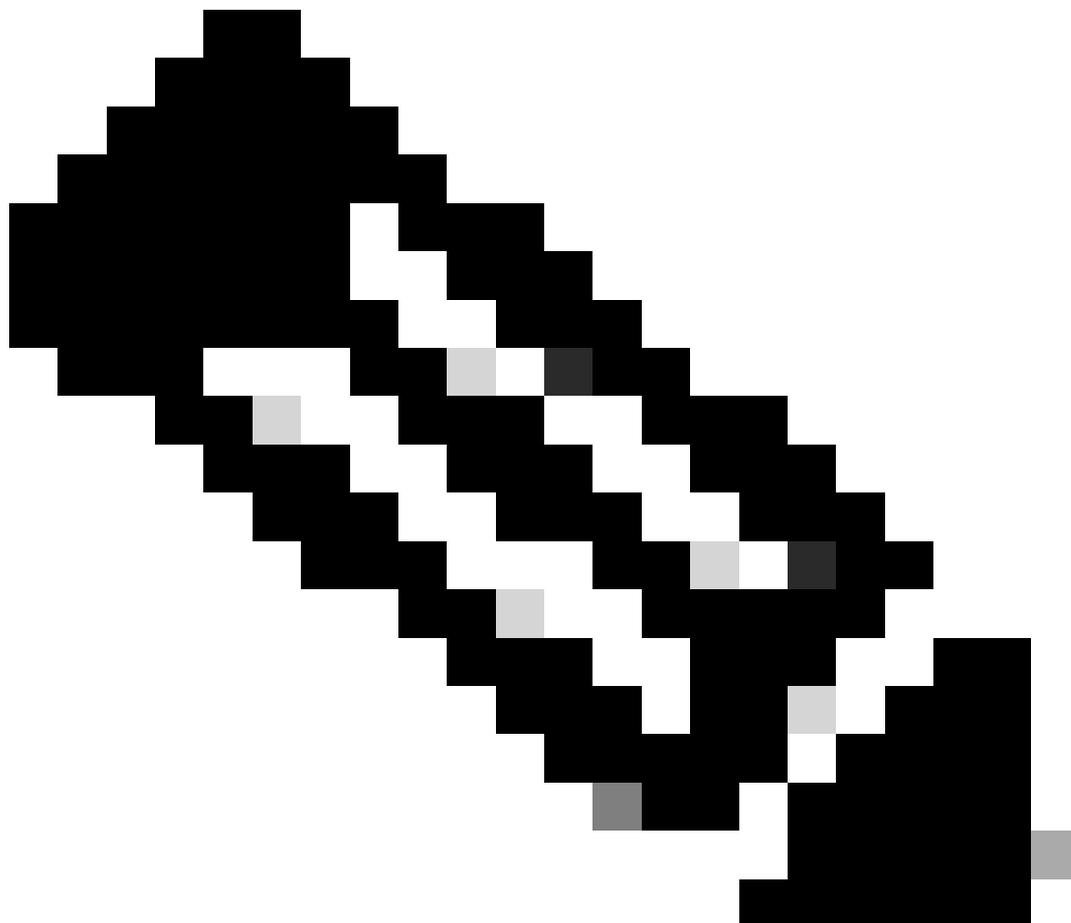
Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration Steps

Étape 1. Dans l'interface utilisateur graphique, accédez à Security Services et sélectionnez HTTPS Proxy, enable HTTPS decryption (activer le décodage HTTPS) si ce n'est pas déjà fait.



Remarque : le décodage HTTPS doit être activé pour cette configuration. S'il n'est pas activé, reportez-vous à l'article référencé fourni à la fin de ce document.

Étape 2. À partir de l'interface utilisateur graphique, accédez à **Web Security Manager** et sélectionnez **Custom and External URL Categories**, créez deux catégories d'URL personnalisées, l'une pour google.com et l'autre pour Google reCAPTCHA. Cliquez sur 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](#)

Créer une catégorie d'URL personnalisée pour 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](#)

Créer une catégorie d'URL personnalisée pour Google

Étape 3. Dans l'interface utilisateur graphique, accédez à **Web Security Manager** et choisissez **Decryption Policies**, créez une stratégie de décodage pour déchiffrer google.com. Cliquez sur **None Selected** en regard de **URL Categories** et sélectionnez **Google** custom URL category.

Cliquez sur 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

Politique de déchiffrement pour déchiffrer Google

Étape 3.1. Naviguez jusqu'à **Decryption Policies** et cliquez sur **Monitor** dans la ligne de la stratégie **GoogleDecrypt**.

Étape 3.2. Sélectionnez **Déchiffrer** dans la ligne de **catégorie Google** et cliquez sur **Envoyer**.

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"/> | | — | — |

Sélectionnez la catégorie d'URL personnalisée créée pour que Google la déchiffre dans la stratégie de déchiffrement

Étape 4. Dans l'interface graphique, accédez à **Web Security Manager** et choisissez **Access Policies**, créez une politique d'accès pour autoriser Google reCAPTCHA et sélectionnez **captchaallow** comme **catégories d'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:

User Agents: None Selected

Politique d'accès autorisant Google RECAPTCHA

Étape 4.1. Accédez à **Access Policies** et cliquez sur **Monitor** dans la ligne de la stratégie **GoogleCaptchaAccessPolicy**. Sélectionnez **Allow** in line to **Captchaallow** Category. **Envoyer** et **valider les modifications**.

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 (?) | Ove |
|--|----------------|---------------------|--------------------------|--------------------------|-------------------------------------|--------------------------|
| | | | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| <input checked="" type="checkbox"/> Captchaallow | Custom (Local) | - | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

Sélectionnez la catégorie d'URL personnalisée créée pour Google RECAPTCHA afin de l'autoriser dans la stratégie d'accès

Étape 5. Assurez-vous que **Search Engines and Portals in Predefined URL Category Filtering** est bloqué dans la stratégie d'accès globale :

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 checked="" type="radio"/> Regional Restricted Sites (Poland) | |
| <input checked="" type="radio"/> Religion | |
| <input checked="" type="radio"/> SaaS and B2B | |
| <input checked="" type="radio"/> Safe for Kids | |
| <input checked="" type="radio"/> Science and Technology | |
| <input checked="" type="radio"/> Search Engines and Portals | <input checked="" type="checkbox"/> |
| <input checked="" type="radio"/> Sex Education | |

Stratégie par défaut pour bloquer l'accès aux moteurs de recherche

Vérifier

Vous pouvez voir l'accès à Google reCAPTCHA fonctionne, mais l'accès au moteur de recherche (Google) est toujours refusé, après avoir activé le déchiffrement HTTPS et permettre l'accès à Google reCAPTCHA dans la politique d'accès :



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

Le site Google est bloqué

1675880581.157 0 10.106.40.203 TCP_DENIED/403 0 GET "<https://google.com/favicon.ico>" - NONE/- - BLOCK_WEBCAT_12-DefaultGroup-DefaultC

Dépannage

Si l'accès à Google reCAPTCHA est bloqué, vous pouvez vérifier les journaux d'accès dans l'interface de ligne de commande SWA. Si vous voyez l'URL Google et non l'URL Google reCAPTCHA, il se peut que le déchiffrement ne soit pas activé :

1675757652.291 2 192.168.100.79 TCP_DENIED/403 0 CONNECT tunnel://www.google.com:443/ - NONE/- - BLOCK_WEBCAT_12-DefaultGroup-F

Références

- [Guide de l'utilisateur d'AsyncOS 14.5 pour Cisco Secure Web Appliance - GD \(General Deployment\) - Connect, Install, and Configure \[Cisco Secure Web Appliance\] - Cisco](#)
- [Utilisation du certificat WSA pour le décodage HTTPS](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.