

阻止访问搜索引擎门户时允许Google reCAPTCHA

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置步骤](#)

[验证](#)

[故障排除](#)

[参考](#)

简介

本文档介绍阻止对搜索引擎门户的访问时，在安全Web设备(SWA)中允许Google reCAPTCHA的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全Web访问和HTTPS解密。

Cisco建议您还应具备：

- 已安装物理或虚拟SWA。
- 许可证已激活或已安装。
- 安装向导已完成。
- 对SWA图形用户界面(GUI)的管理权限。

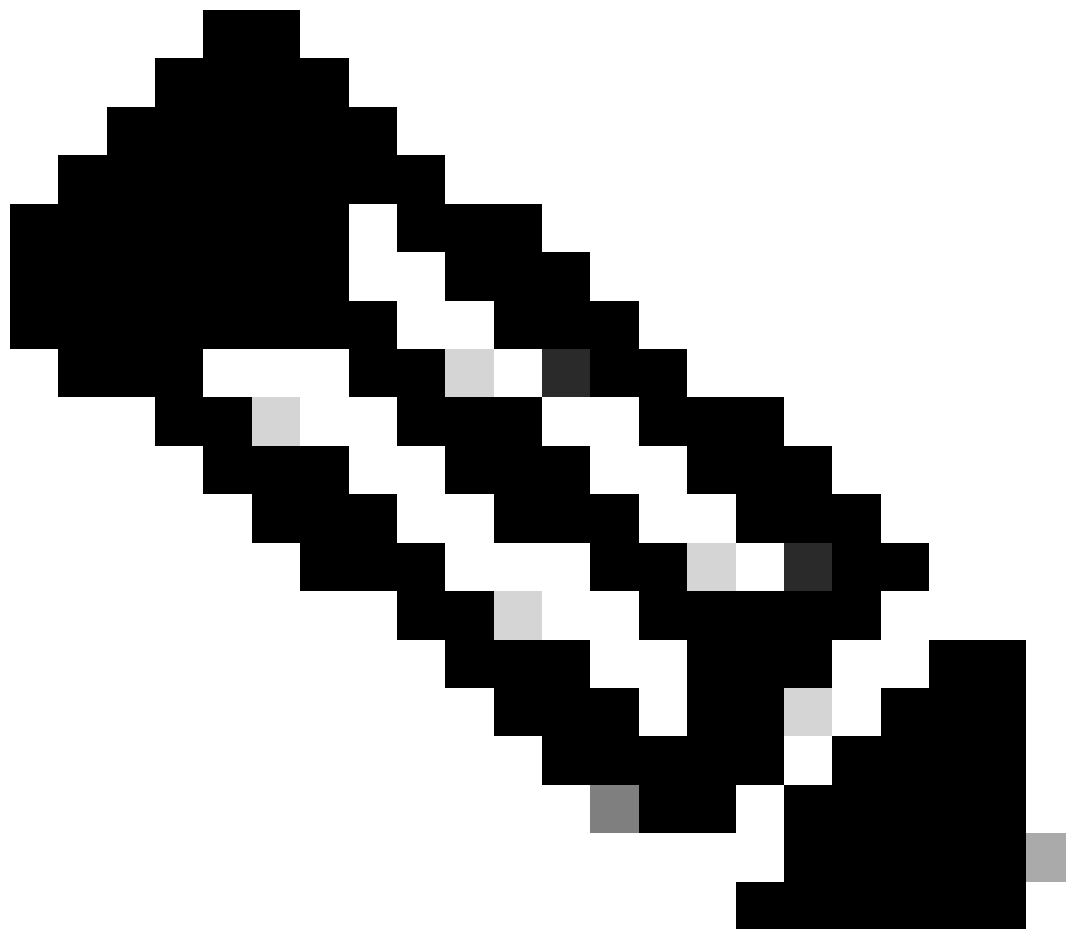
使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置步骤

步骤1:从GUI中，导航至Security Services并选择HTTPS Proxy, enable HTTPS decryption（如果尚未启用）。



注意：必须为此配置启用HTTPS解密。如果未启用，请参阅本文档末尾提供的引用文章。

第二步：在GUI中，导航到网络安全管理器并选择自定义和外部URL类别，创建两个自定义URL类别，一个用于google.com，另一个用于Google reCAPTCHA。单击“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; border: 1px solid #ccc; padding: 2px;"> 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>

为Google创建自定义URL类别

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; border: 1px solid #ccc; padding: 2px;"> 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>

为Google创建自定义URL类别

第三步：从GUI中，导航到网络安全管理器，然后选择解密策略，创建解密策略以解密google.com。单击URL Categories旁边的None Selected，然后选择Google自定义URL类别。单击“Submit”。

Decryption Policy: Add Group

Policy Settings

Enable Policy

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

Description:

Insert Above Policy: 1 (dropciscospecific) ▼

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: 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

解密Google的解密策略

步骤 3.1 导航到解密策略，然后点击Google解密策略行中的监控。

步骤 3.2 选择Google Category行中的Decrypt，然后单击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	
Google	Custom (Local)	—	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)

Cancel

Submit

选择Created Custom URL Category for Google以在解密策略中对其进行解密

第四步：在GUI中，导航到网络安全管理器并选择访问策略，创建访问策略以允许Google reCAPTCHA并选择captchaallow作为URL类别。

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

允许Google RECAPTCHA的访问策略

步骤 4.1 导航到访问策略，然后单击GoogleCaptchaAccessPolicy策略行中的监控。在Captchaallow Category行中选择Allow。提交和提交更改。

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

选择Created Custom URL Category for Google RECAPTCHA以在访问策略中允许它

第五步：确保已阻止全局访问策略中的预定义URL类别过滤中的搜索引擎和门户：

Access Policies: URL Filtering: Global Policy

Custom and External URL Category Filtering

No Custom Categories are included for this Policy.

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
<input type="radio"/> Regional Restricted Sites (Poland)	Select all
<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	

阻止访问搜索引擎的默认策略

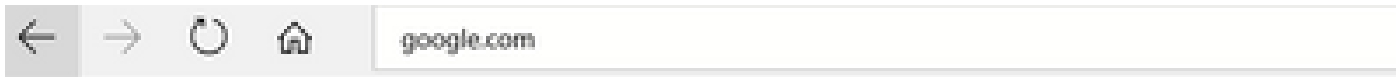
验证

您可以看到对Google reCAPTCHA的访问有效，但在启用HTTPS解密并在访问策略中允许对Google reCAPTCHA的访问后，搜索引擎(Google)访问仍然被拒绝：



Google CAPTCHA的工作原理

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

Google站点被阻止

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

故障排除

如果对Google reCAPTCHA的访问被阻止，您可以在SWA CLI中检查访问日志。如果看到Google URL而不是Google reCAPTCHA URL，则可能是解密未启用：

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

参考

- [思科安全网络设备AsyncOS 14.5用户指南- GD \(通用部署\)-连接、安装和配置\[思科安全网络设备\]-思科](#)
- [HTTPS解密的WSA证书用法](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。