在阻止訪問搜尋引擎門戶時允許Google reCAPTCHA

目錄

簡介

本文檔介紹在阻止對搜尋引擎門戶的訪問時，允許在安全網路裝置(SWA)中使用Google reCAPTCHA的步驟。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco Secure Web Access和HTTPS解密。

思科建議您：

- 已安裝物理或虛擬SWA。
- 許可證已啟用或已安裝。
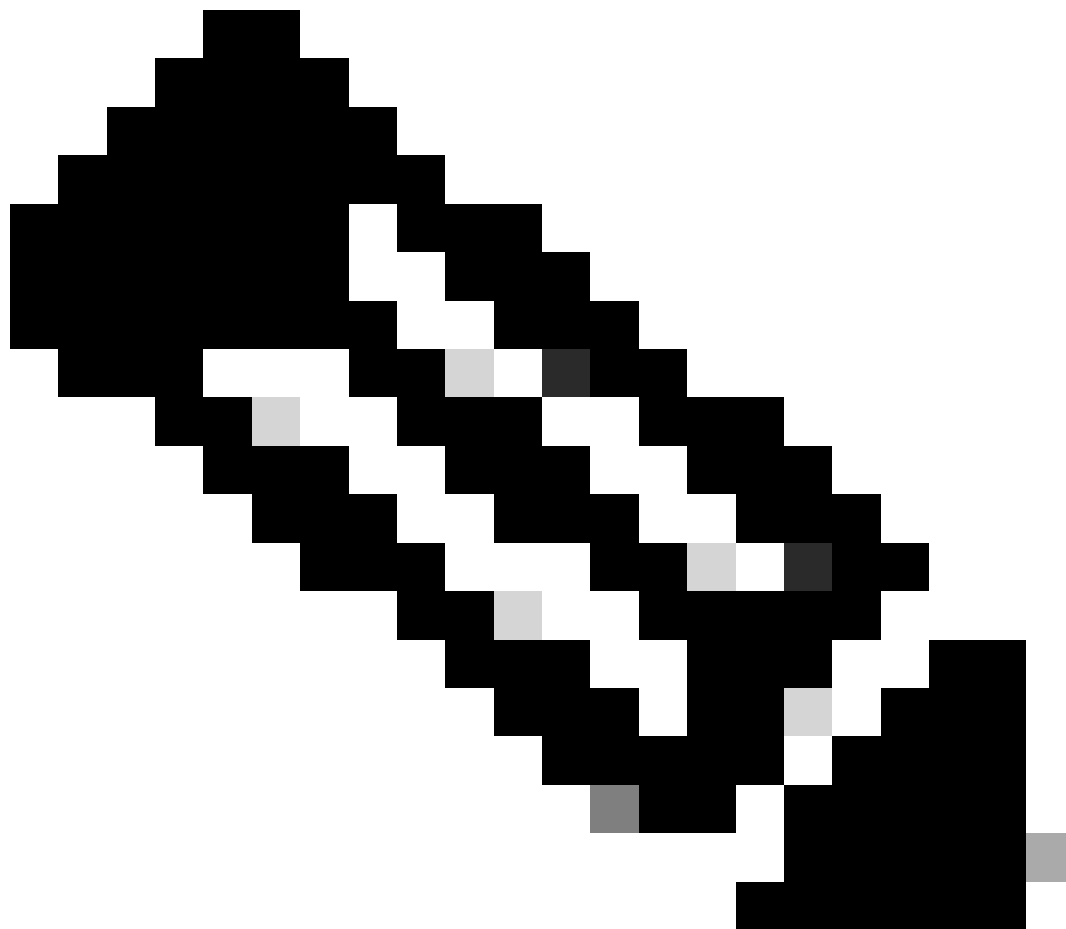- 安裝精靈已完成。
- 對SWA圖形使用者介面(GUI)的管理訪問。

採用元件

本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定步驟

步驟 1.如果尚未啟用HTTPS解密，請從GUI導航到 Security Services**並選擇**HTTPS Proxy,。

注意：必須為此配置啟用HTTPS解密。如果未啟用，請參閱本文檔末尾提供的參考文章。

步驟 2.從GUI導航到網路安全管理器，然後選擇**自定義和外部URL**類別，建立兩個自定義URL類別，一個用於google.com，另一個用於Google reCAPTCHA。按一下**Submit**。

Custom and External URL Categories: Edit Category

Edit Custom and External URL Category

Category Name:	Google
Comments: ?	Custom URL Category for Google
List Order:	4
Category Type:	Local Custom Category
Sites: ?	google.com, .google.com

Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)

▽ Advanced Regular Expressions: ?

Enter one regular expression per line. Maximum allowed characters 2048.

Cancel   Submit

為*Google*建立自定義*URL*類別

Custom and External URL Categories: Edit Category

Edit Custom and External URL Category

Category Name:	Captchaallow
Comments: ?	Custom URL Category for Google RECAPTCHA
List Order:	5
Category Type:	Local Custom Category
Sites: ?	

Click the Sort URLs button to sort all site URLs in Alpha-numerical order.

(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)

▽ Advanced Regular Expressions: ?
www\.google\.com/recaptcha/

Enter one regular expression per line. Maximum allowed characters 2048.

Cancel   Submit

為*Google*建立自定義*URL*類別

步驟 3.在GUI中，導航到**網路安全管理器**並選擇**解密策略**，建立解密策略以解密google.com。按一下**URL Categories** 旁邊的**None Selected**，然後選擇**Google** 自定義URL類別。點選**提交**。

Decryption Policy: Add Group

Policy Settings

☑ **Enable Policy**

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

Description: |
(Maximum allowed characters 256)

Insert Above Policy: | 1 (dropciscospecific) ▾

Policy Expires: | ☐ Set Expiration for Policy

On Date: | | MM/DD/YYYY

At Time: | 00 ▾ : 00 ▾

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

步驟 3.1.導航到**解密策略**，然後點選**GoogleDecrypt**策略行中的**監控**。

步驟 3.2.選擇**Google Category**行中的**Decrypt**，然後按一下**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	Pass Through ➕	Monitor 🟡	Decrypt 🔴	Drop ? ❌	Quota-Based ⏳	Time-Based 🕐
				Override Global Settings				
		Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)
🔴 Google	Custom (Local)	—			✓		—	—

Cancel | Submit

選擇已建立的自定義*URL*類別，以便*Google*在解密策略中對它進行解密

步驟 4.從GUI導航到**網路安全管理器**，然後選擇**訪問策略**，建立允許Google reCAPTCHA的訪問策略，然後選擇**captchaallow**作為
URL類別。

Access Policy: Add Group

Policy Settings	
☑ **Enable Policy**	
Policy Name: ⑦	GoogleCaptchaAccessPolicy
	(e.g. my IT policy)
Description:	
	(Maximum allowed characters 256)
Insert Above Policy:	1 (blockciscobuy) ∨
Policy Expires:	☐ Set Expiration for Policy
	On Date: _____ *MM/DD/YYYY*
	At Time: 00 ∨ : 00 ∨

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.
▽ 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

允許*Google RECAPTCHA*的訪問策略

步驟 4.1.導航到訪問策略，然後點選**GoogleCaptchAccessPolicy**策略行中的**監控**。選擇**Captchaallow 類別**旁的**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.			Use Global Settings			Ove
				Block ⊗	Redirect ⊕	Allow ⑦ ⊕
Category		Category Type	Select all	Select all	Select all	Select all
⊕ Captchaallow		Custom (Local)	—			✓

Cancel

為*Google RECAPTCHA*選擇*Created Custom URL Category*以在訪問策略中允許它

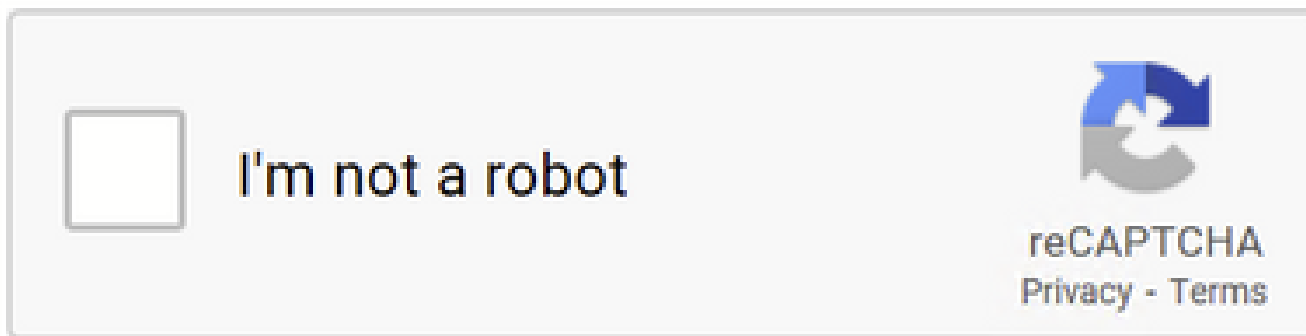**步驟 5.**確保已在全局訪問策略中阻止了**Predefined URL Category Filtering**中的**搜尋引擎和門戶**：

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		Block ⊗
These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.		
Category		Select all
🟡 Regional Restricted Sites (Poland)		
🟡 Religion		
🟡 SaaS and B2B		
🟡 Safe for Kids		
🟡 Science and Technology		
⊗ Search Engines and Portals		✓
🟡 Sex Education		

阻止搜尋引擎訪問的預設策略

驗證

您可以看到對Google reCAPTCHA的訪問起作用，但是在啟用HTTPS解密並在訪問策略中允許對Google reCAPTCHA的訪問後，搜尋引擎(Google)訪問仍然被拒絕：

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=6LdN4qUZAAAAAF

*Google*站點被阻止

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

疑難排解

如果對Google reCAPTCHA的訪問被阻止，您可以在SWA CLI中檢查訪問日誌。如果您看到Google URL而非Google reCAPTCHA URL，則可能是因為未啟用解密：

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

參考資料

- Cisco Secure Web Appliance的AsyncOS 14.5使用手冊- GD（常規部署）-連線、安裝和配置[Cisco Secure Web Appliance] - 思科

- 用於HTTPS解密的WSA證書使用情況

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。