

Google reCAPTCHA toestaan wanneer toegang tot zoekmachineportals is geblokkeerd

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configuratiestappen](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Referenties](#)

Inleiding

In dit document worden de stappen beschreven om Google reCAPTCHA in Secure Web Appliance (SWA) toe te staan wanneer u de toegang tot Search Engine Portals hebt geblokkeerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Web Access en HTTPS-decryptie.

Cisco raadt u ook aan het volgende te hebben:

- Fysieke of virtuele SWA geïnstalleerd.
- Licentie geactiveerd of geïnstalleerd.
- De setup-wizard is voltooid.
- Administratieve toegang tot de grafische gebruikersinterface van de SWA (GUI).

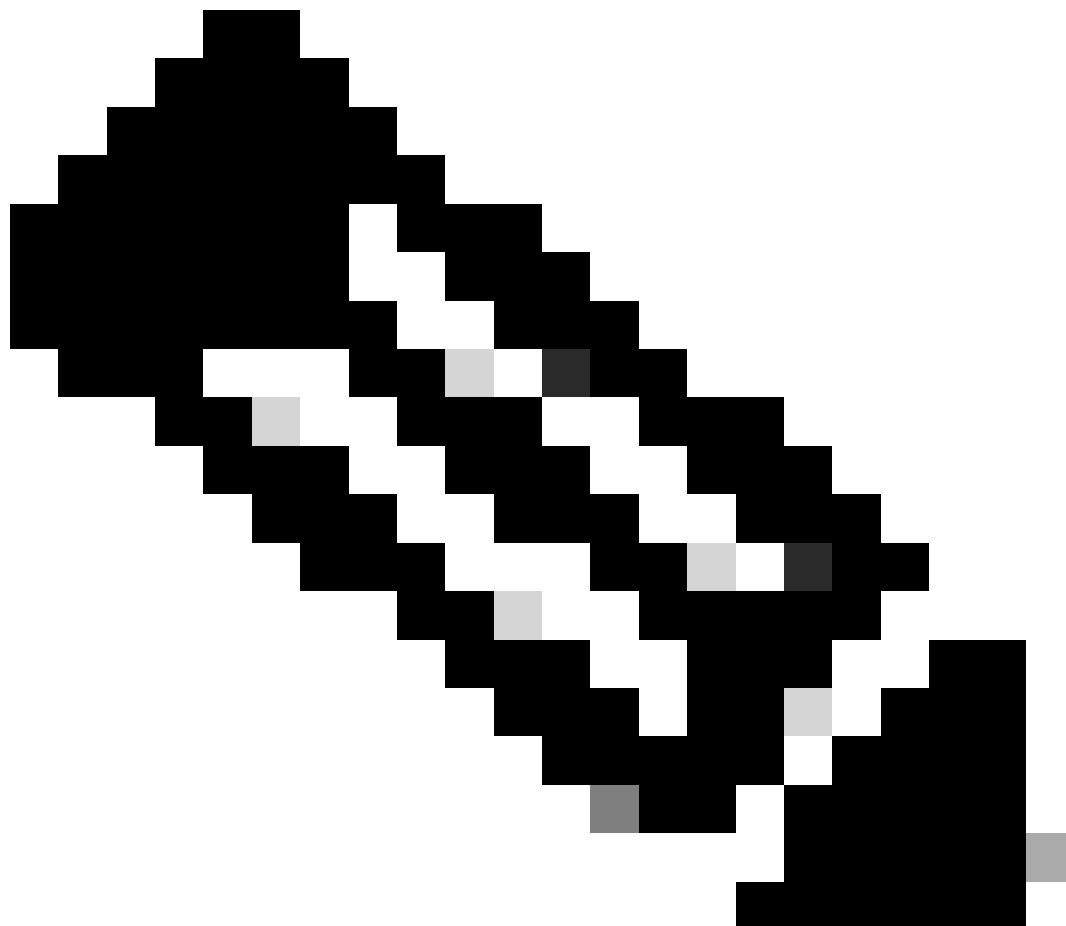
Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configuratiestappen

Stap 1. Van GUI navigeer aan Security Services en kies HTTPS Proxy, HTTPS-decryptie inschakelen als dit nog niet is ingeschakeld.



Opmerking: HTTPS-decryptie moet zijn ingeschakeld voor deze configuratie. Als het niet is ingeschakeld, raadpleegt u het artikel waarnaar verwezen wordt aan het eind van dit document.

Stap 2. Van GUI navigeer aan Web Security Manager en kies **Aangepaste en Externe URL Categorieën**, maak twee aangepaste URL categorieën, één voor google.com en andere voor Google reCAPTCHA. Klik op **Verzenden**.

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 <small>(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)</small>
Sort URLs	Click the Sort URLs button to sort all site URLs in Alpha-numerical order.
Advanced	Regular Expressions: (?) <small>Enter one regular expression per line. Maximum allowed characters 2048.</small>

Cancel Submit

Aangepaste URL-categorie maken voor Google

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: (?)	 <small>(e.g. 10.0.0.1, 2001:420:80:1::5, example.com.)</small>
Sort URLs	Click the Sort URLs button to sort all site URLs in Alpha-numerical order.
Advanced	Regular Expressions: (?) www\.google\.com/recaptcha/ <small>Enter one regular expression per line. Maximum allowed characters 2048.</small>

Cancel Submit

Aangepaste URL-categorie maken voor Google

Stap 3. Van GUI navigeer aan de **Manager van de Veiligheid van het Web** en kies **het Beleid van de Decryptie**, creer decryptiebeleid om google.com te decrypteren. Klik op **Geen geselecteerd** naast de **URL-categorieën** en selecteer de **aangepaste Google-URL-categorie**. Klik op

Verzenden.

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: 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. 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

Het beleid van de decryptie om Google te decrypteren

Stap 3.1. Navigeer naar **decryptie beleid** en klik op **Monitor** in lijn met het **GoogleDecrypt** beleid.

Stap 3.2. Selecteer **Decrypt** in de lijn naar **Google Category** en klik op **Indienen**.

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"/>		—	—

Selecteer *Aangepaste URL-categorie voor Google* om deze te decrypteren in het decryptie beleid

Stap 4. Van GUI navigeer aan **Web Security Manager** en kies **Toegangsbeleid**, creëer Toegangsbeleid om Google reCAPTCHA toe te staan en selecteer **captchaallow** als **URL Categorieën**.

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

Toegangsbeleid om Google RECAPTCHA toe te staan

Stap 4.1. Navigeer naar **Toegangsbeleid** en klik op **Monitor** in lijn met het **GoogleCaptchaAccessPolicy**-beleid. Selecteer **Toestaan** in regel om **CaptureFlow** Category te selecteren. **Veranderingen verzenden en doorvoeren**

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

Selecteer Aangepaste URL-categorie voor Google RECAPTCHA om deze in het toegangsbeleid toe te staan

Stap 5. Zorg ervoor dat **zoekmachines en portals** in **vooraf gedefinieerde URL-categoriefiltering** worden geblokkeerd in het algemene toegangsbeleid:

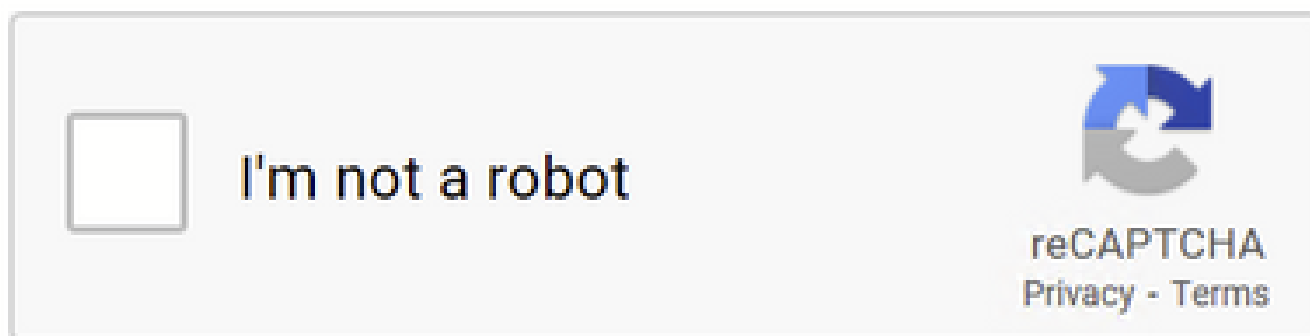
Access Policies: URL Filtering: Global Policy

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 checked="" type="checkbox"/>
<input type="radio"/> Sex Education	

Standaardbeleid om de toegang tot zoekmachines te blokkeren

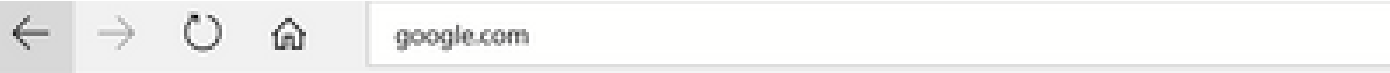
Verifiëren

U kunt toegang tot Google reCAPTCHA werken zien, maar toegang tot zoekmachine (Google) wordt nog steeds geweigerd, nadat u HTTPS-decryptie inschakelt en de toegang tot Google reCAPTCHA in het toegangsbeleid toestaat:



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

Google Site is geblokkeerd

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

Problemen oplossen

Als de toegang tot de Google reCAPTCHA wordt geblokkeerd, kunt u de toegangslogboeken in de SWA CLI controleren. Als u Google URL ziet en niet de Google reCAPTCHA URL, kan het zijn dat decryptie niet is ingeschakeld:

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

Referenties

- [Gebruikershandleiding voor AsyncOS 14.5 voor Cisco Secure Web Applicatie - GD \(Algemene implementatie\) - Verbinden, installeren en configureren \[Cisco Secure Web Applicatie\] - Cisco](#)
- [Gebruik van WSA-certificaat voor HTTPS-decryptie](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.