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).

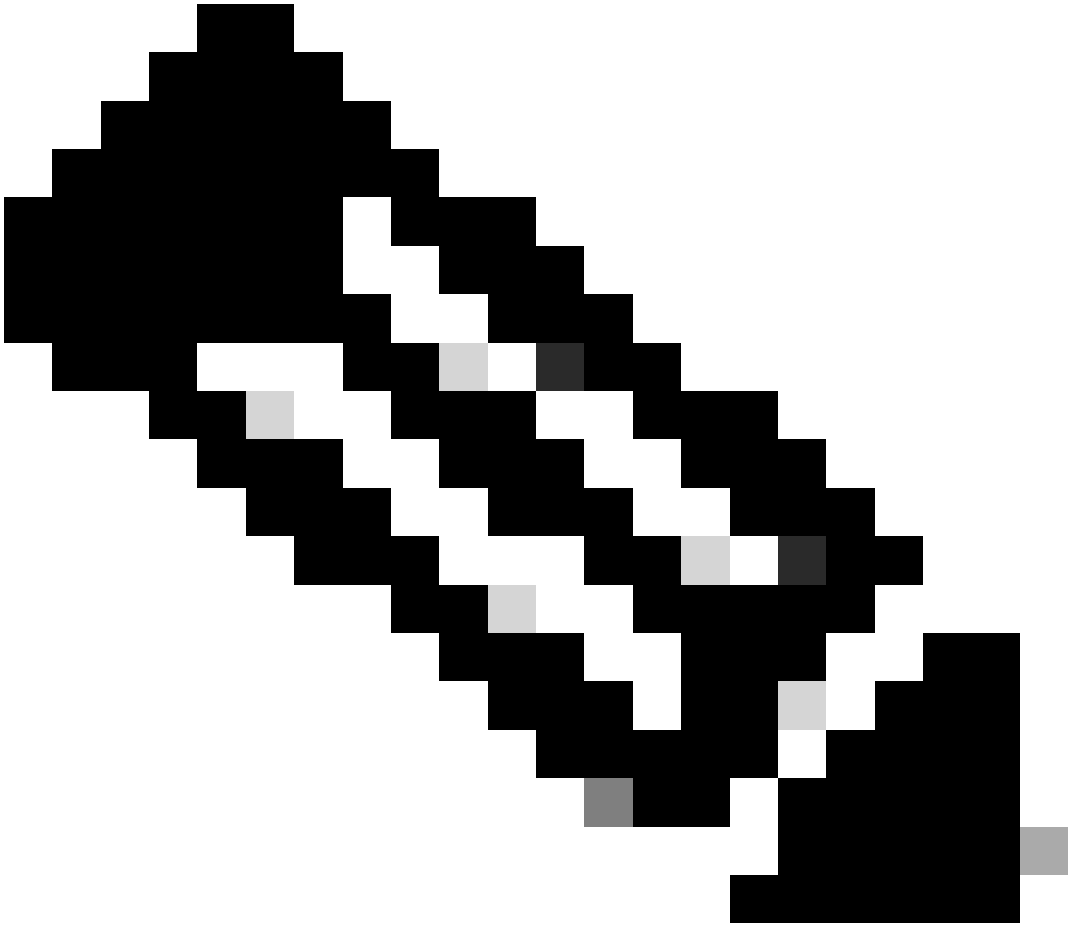
Components Used

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.

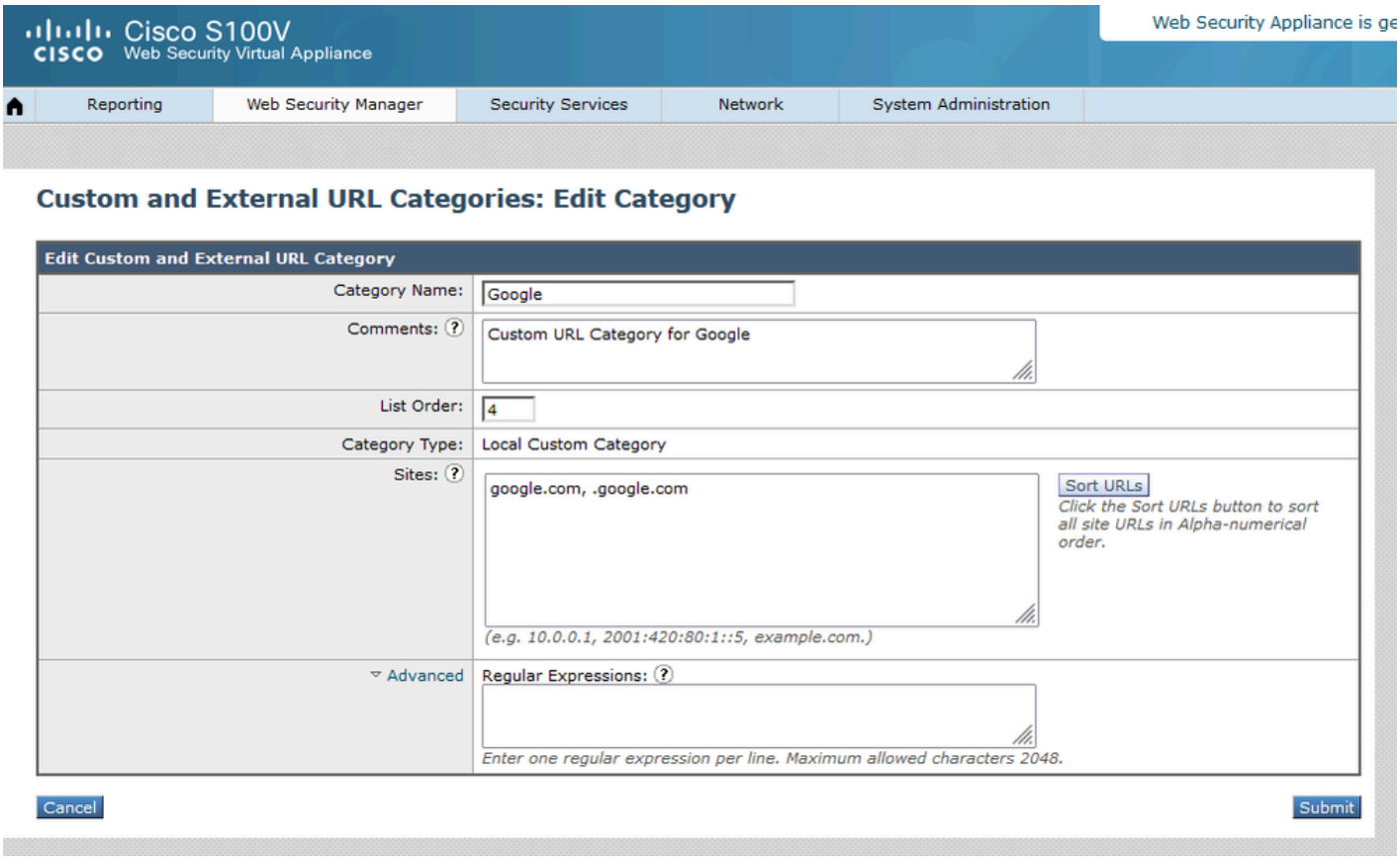
Configuration Steps

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

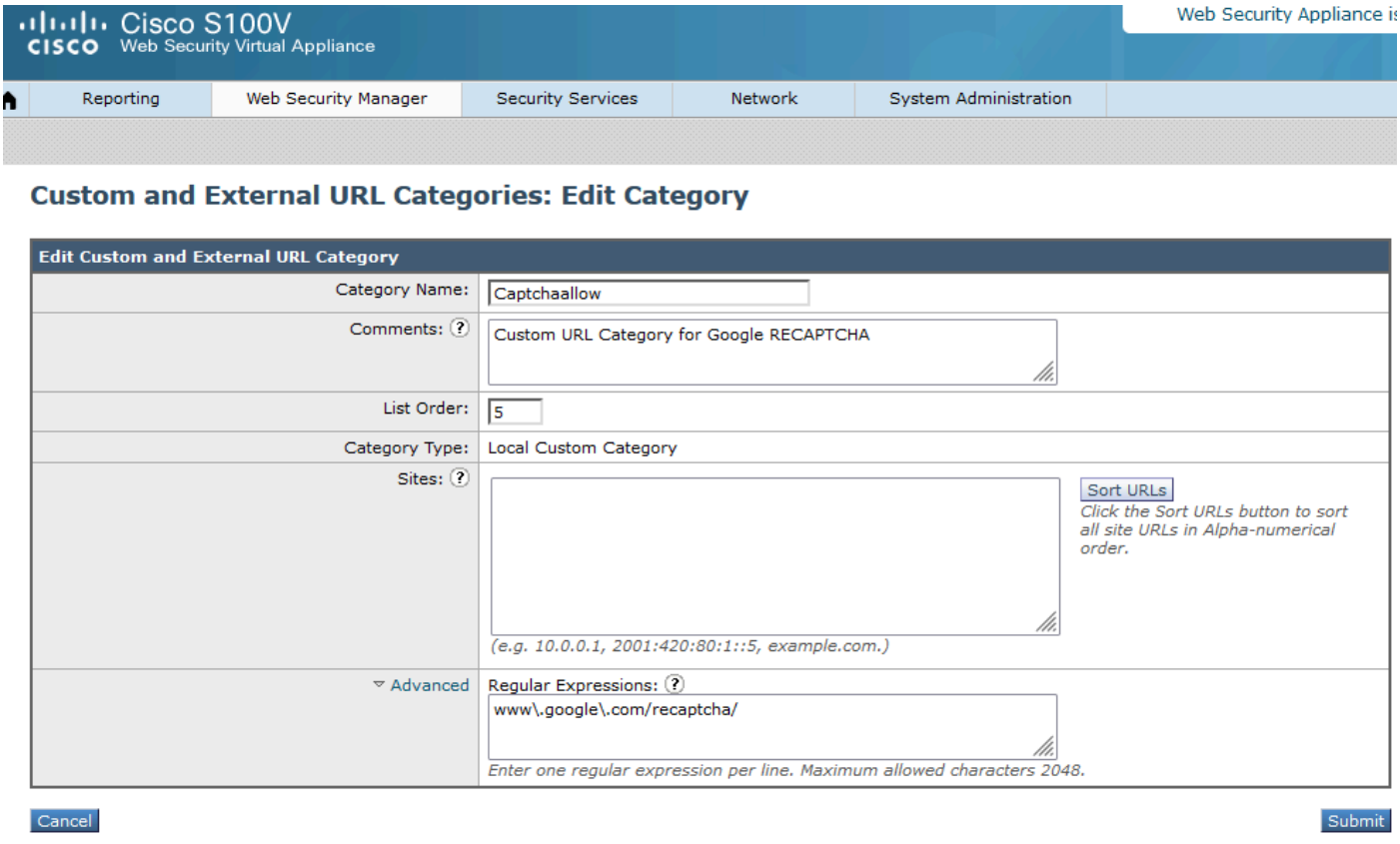


Note: HTTPS Decryption must be enabled for this configuration. If it is not enabled, please refer the referenced article given at the end of this document.

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**.



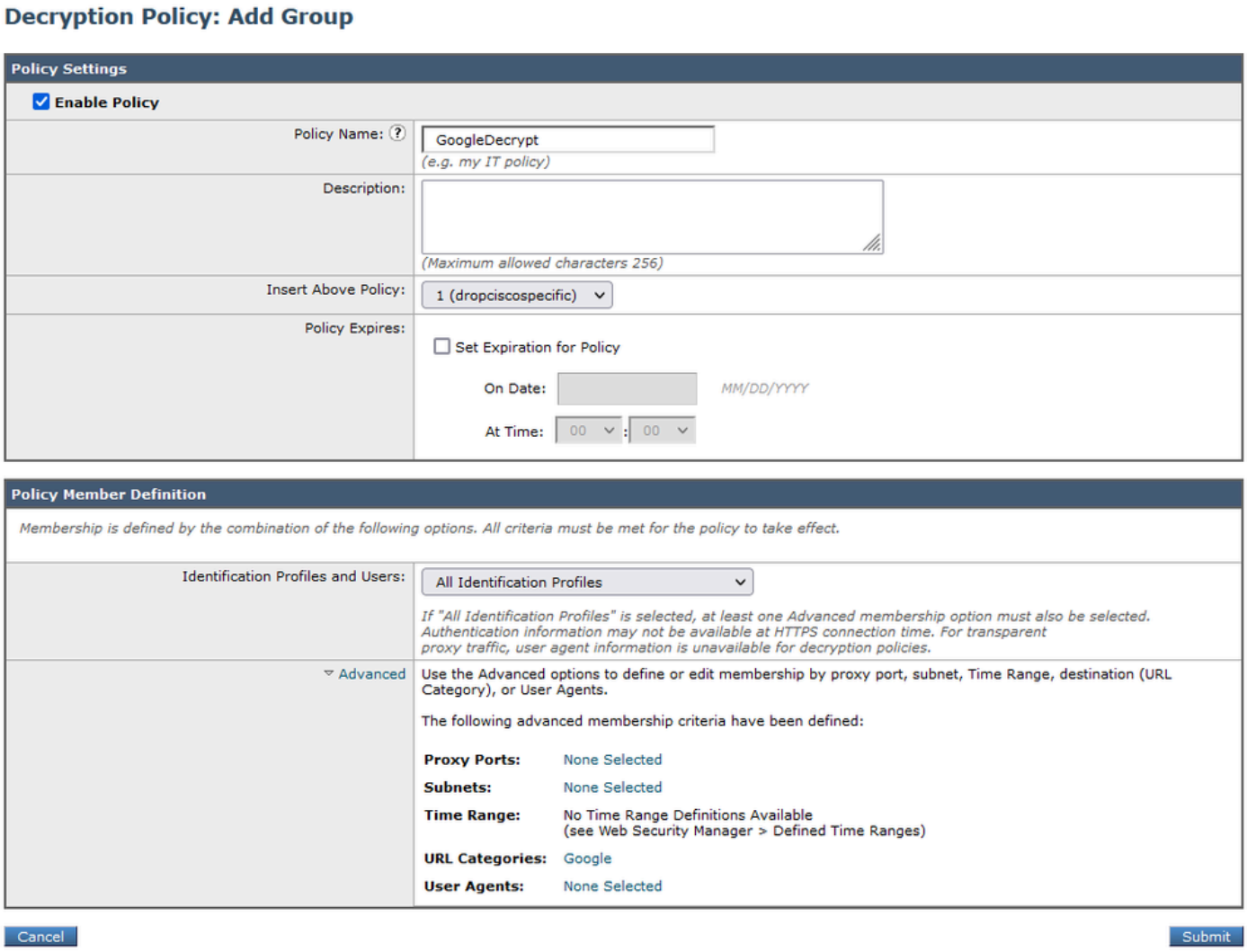
Create Custom URL Category for Google



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 to Decrypt Google

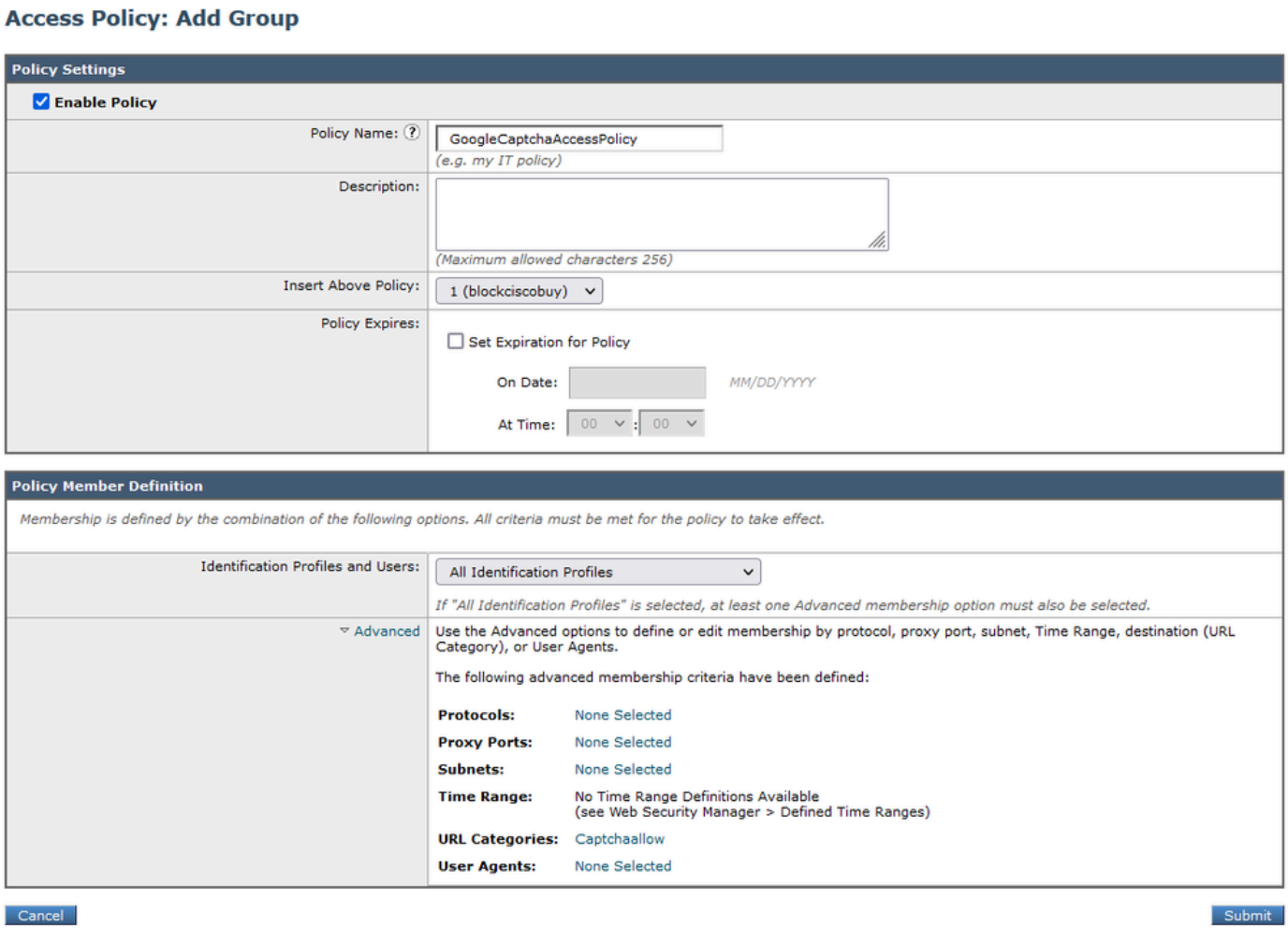
Step 3.1. Navigate to **Decryption Policies** and click **Monitor** in line to the **GoogleDecrypt** policy**.**

Step 3.2. Select **Decrypt** in line to **Google Category** and Click **Submit.**



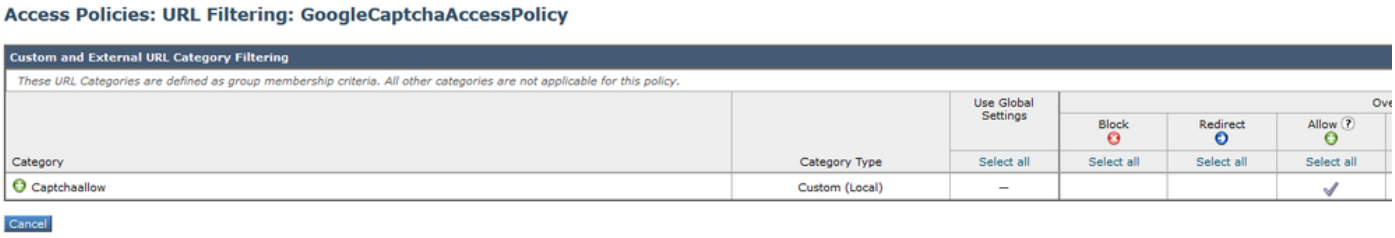
Select Created Custom URL Category for Google to Decrypt it in the Decryption Policy

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**.



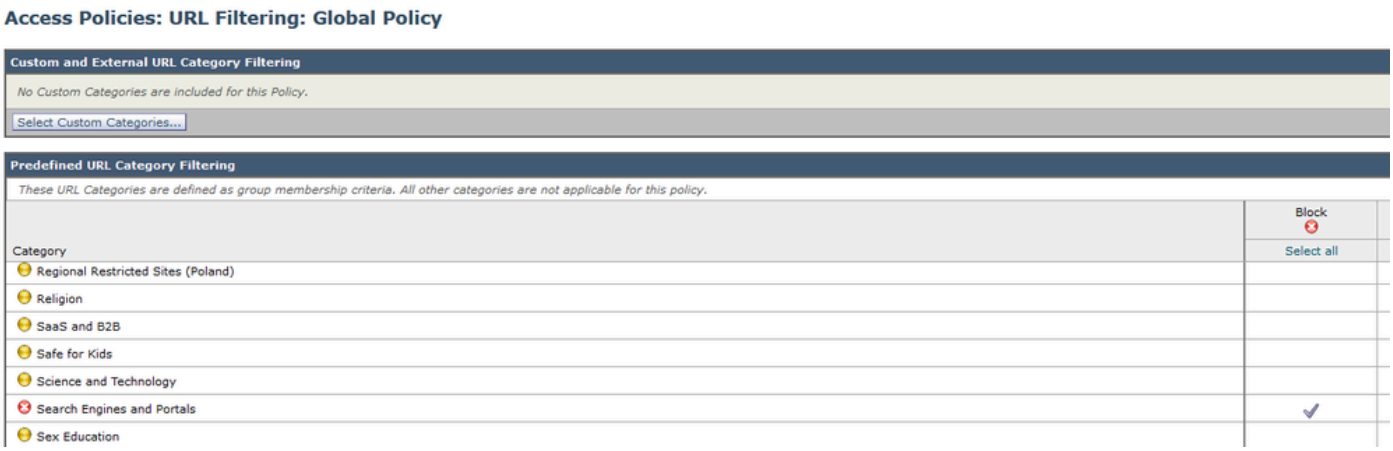
Access Policy to Allow Google RECAPTCHA

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



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:



Default Policy to Block the Access to Search Engines

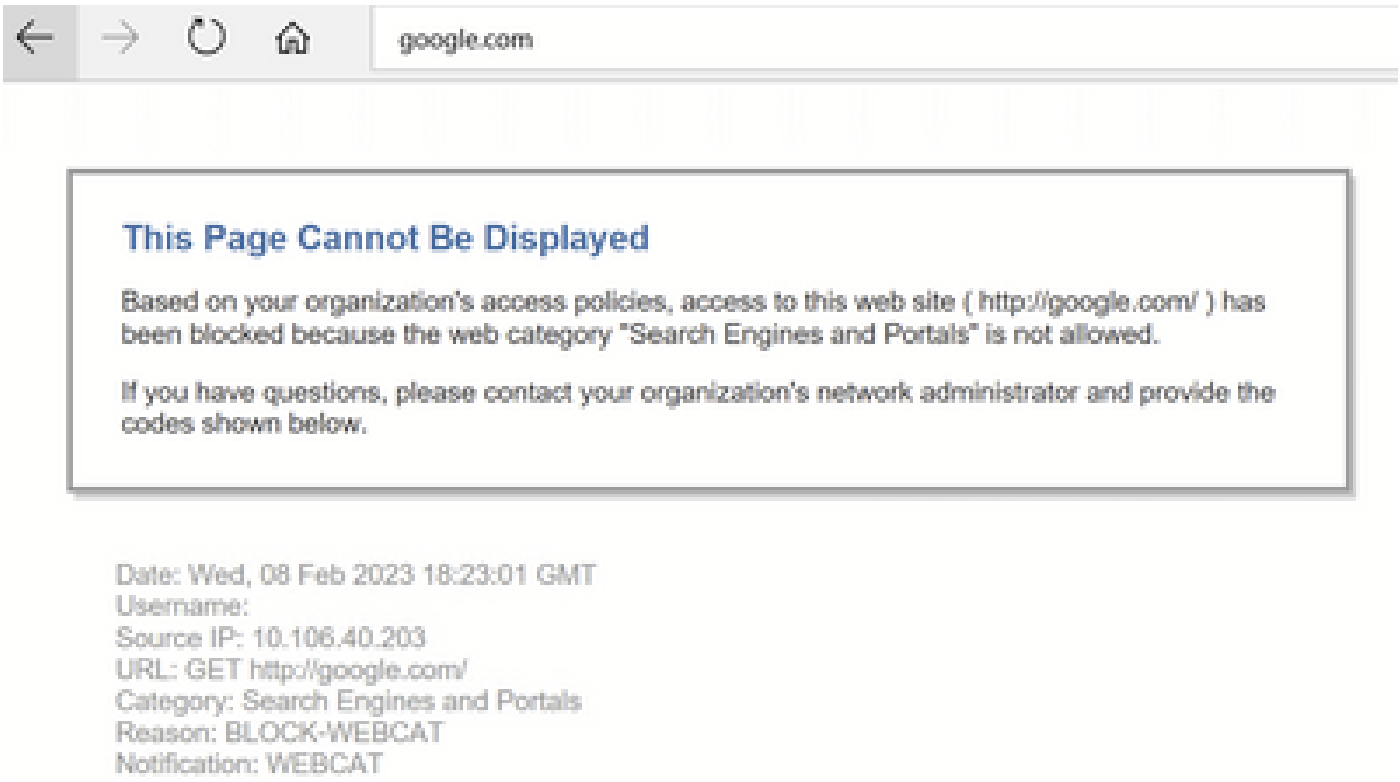
Verify

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
```



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_
```

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