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.

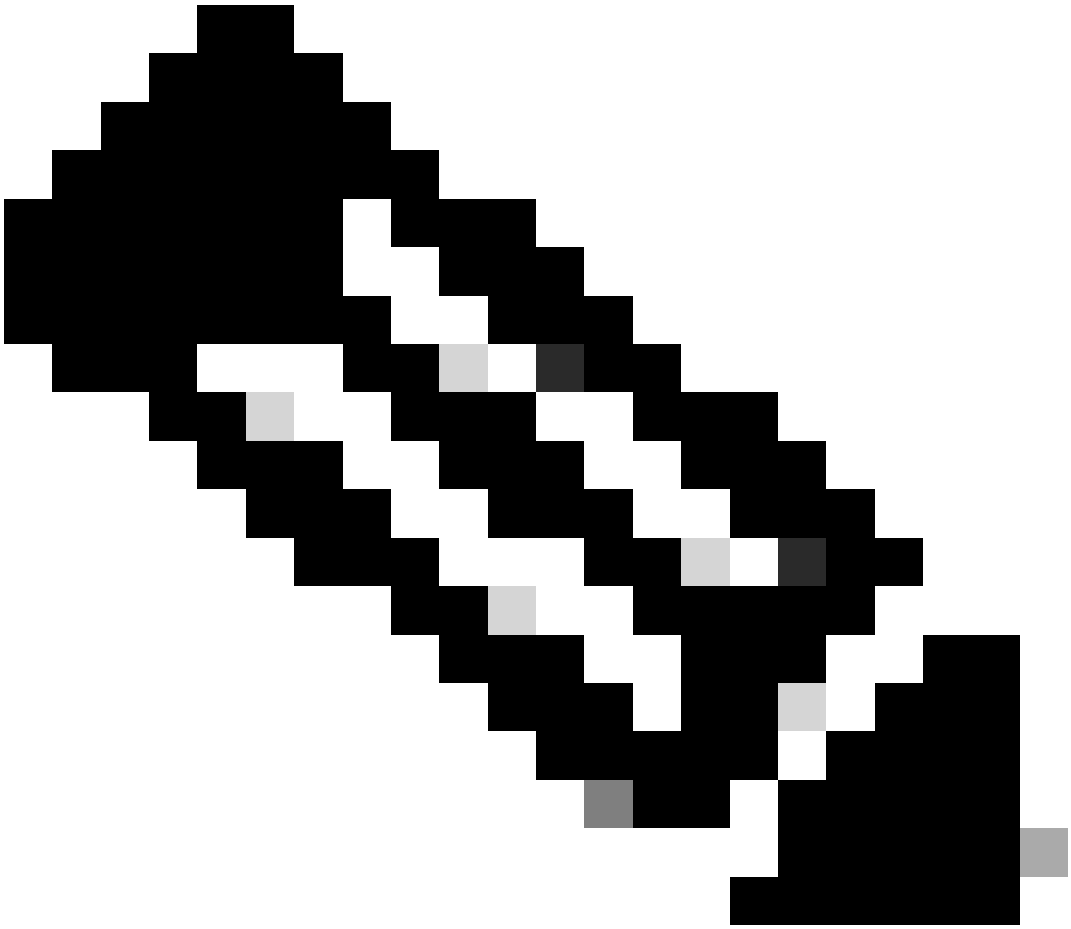
Composants utilisés

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.

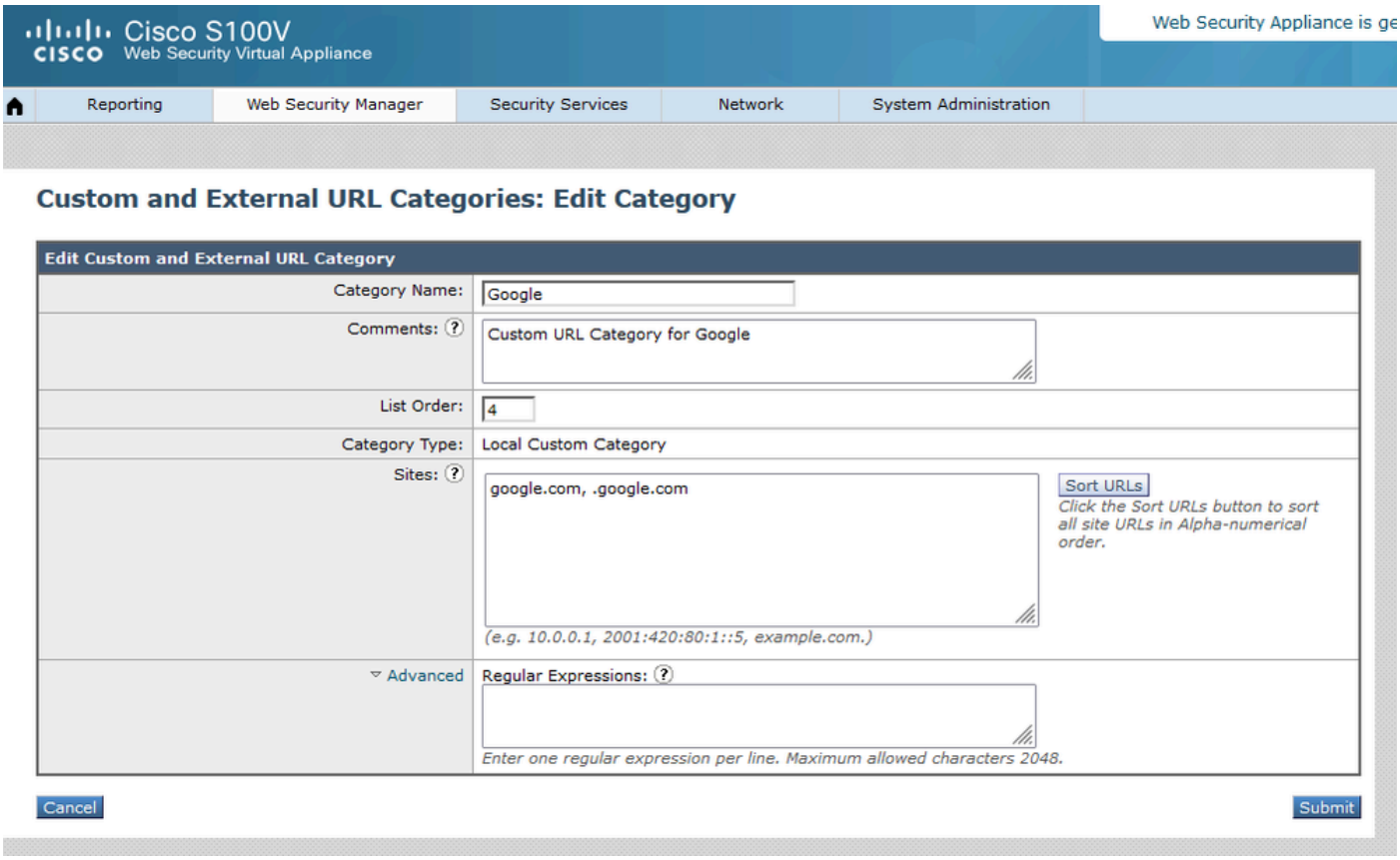
Configuration Steps

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.

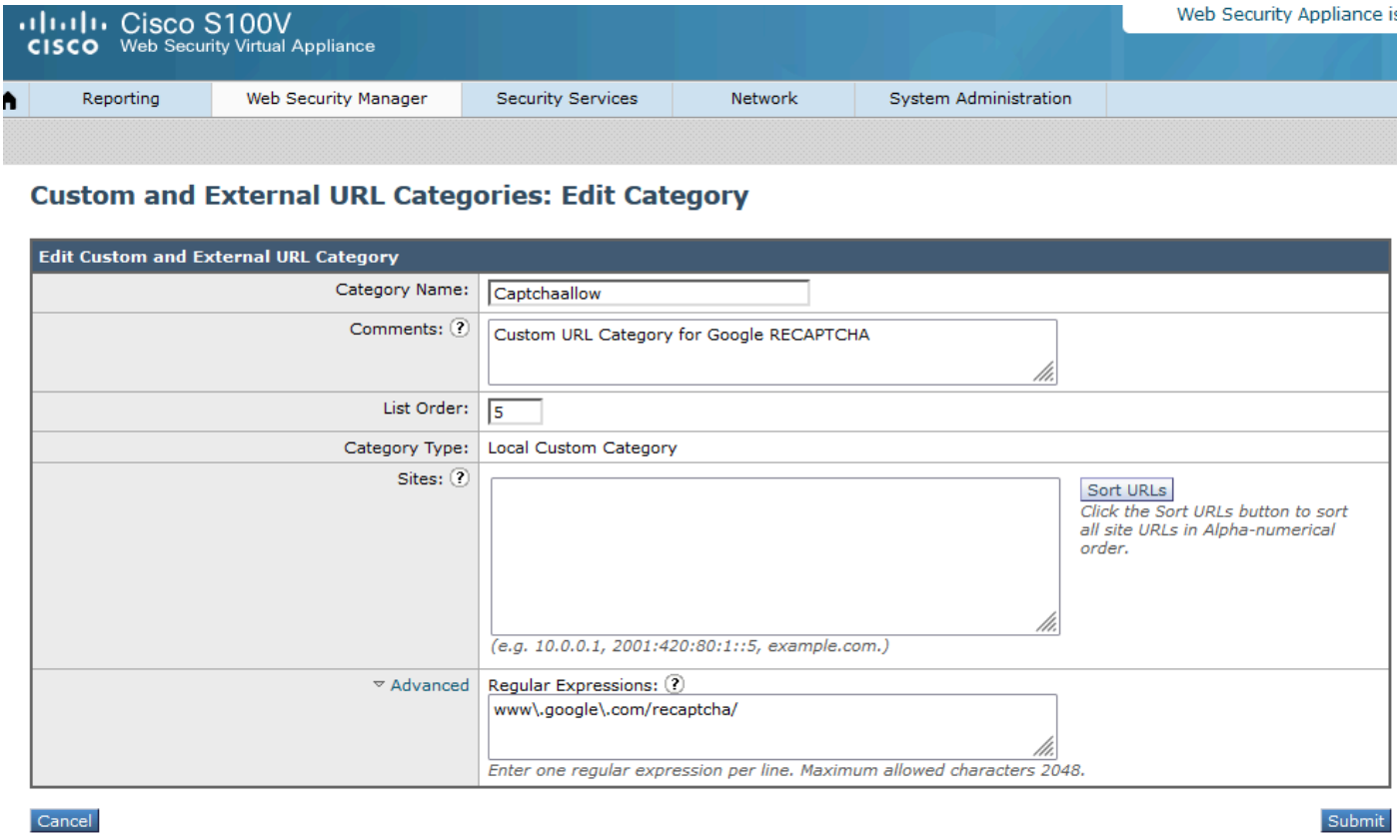


Remarque : le décodage HTTPS doit être activé pour cette configuration. S'il n'est pas activé, reportez-vous à l'article référencé fourni à la fin de ce document.

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.



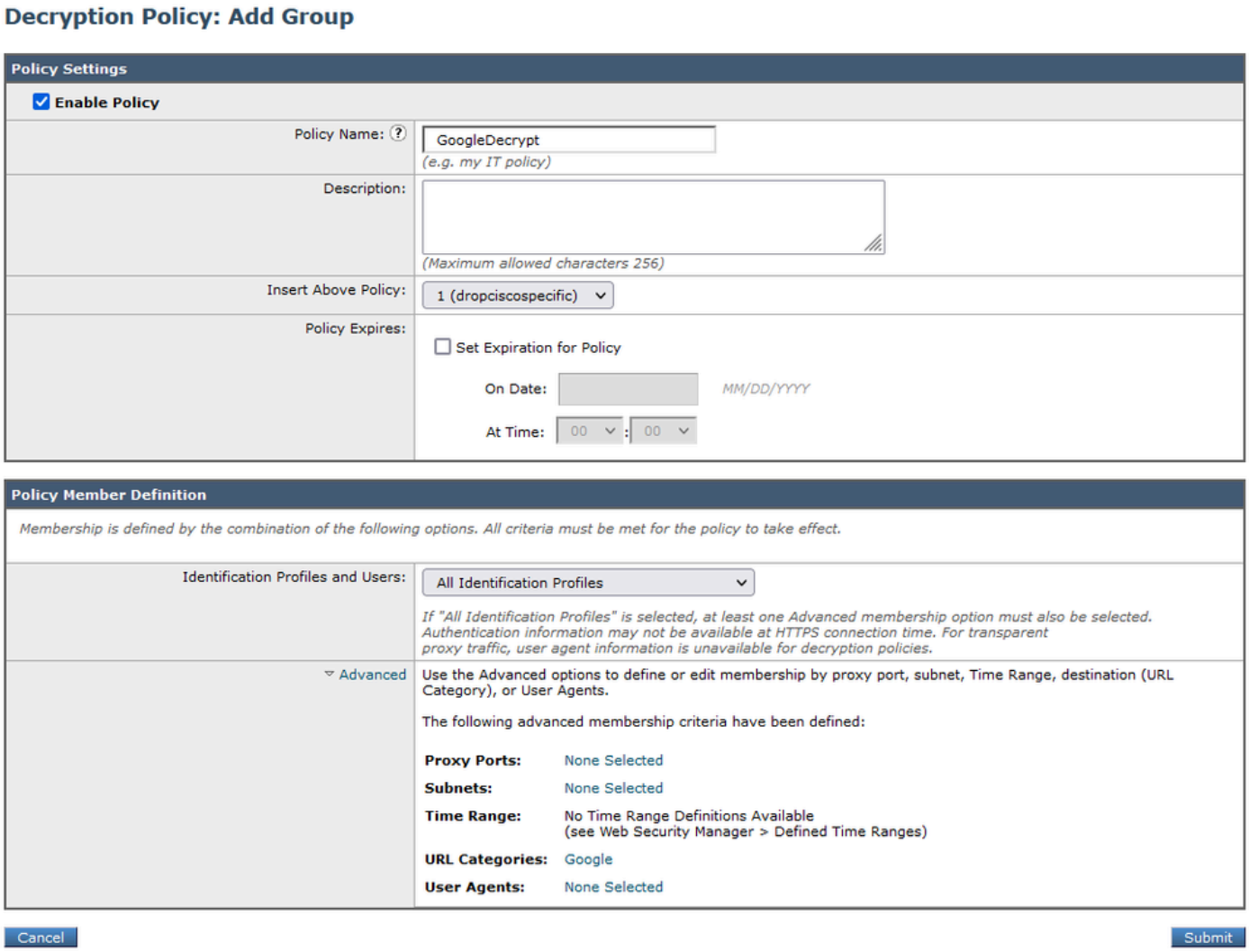
Créer une catégorie d'URL personnalisée pour Google



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.

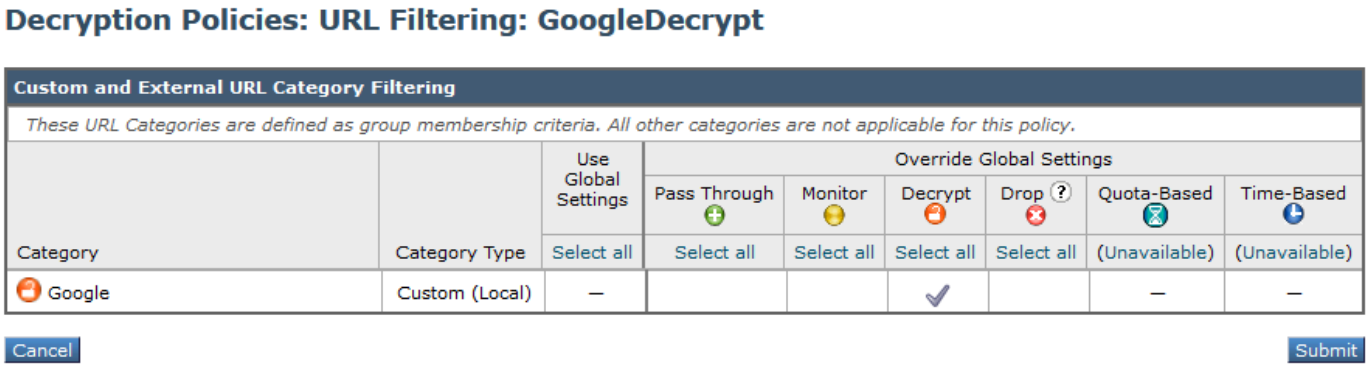
Cliquez sur Submit.



Politique de déchiffrement pour déchiffrer Google

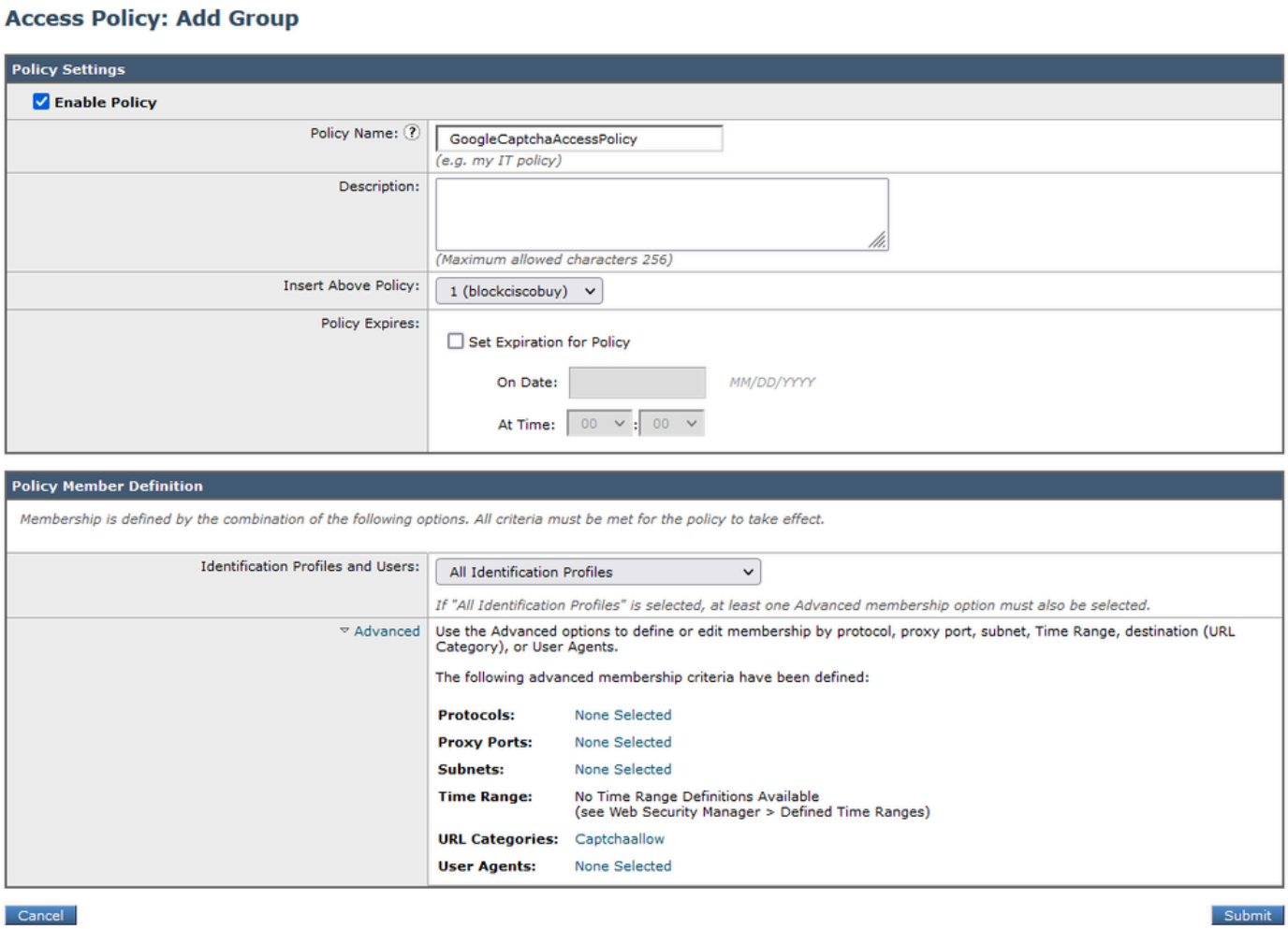
Étape 3.1. Naviguez jusqu'à **Decryption Policies** et cliquez sur **Monitor** dans la ligne de la stratégie **GoogleDecrypt**.

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



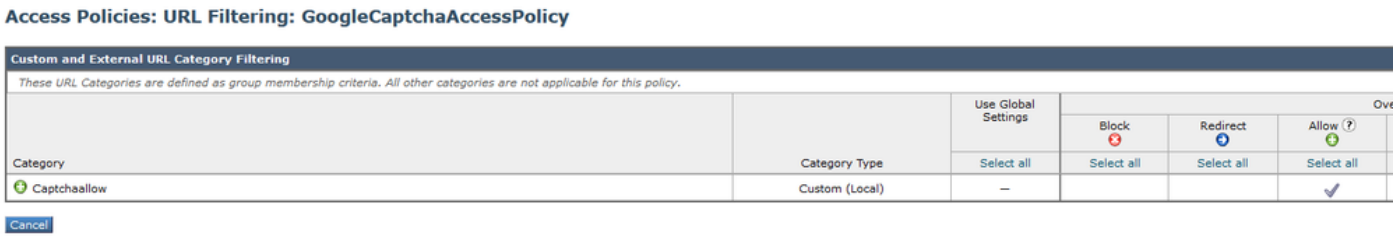
Sélectionnez la catégorie d'URL personnalisée créée pour que Google la déchiffre dans la stratégie de déchiffrement

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**.



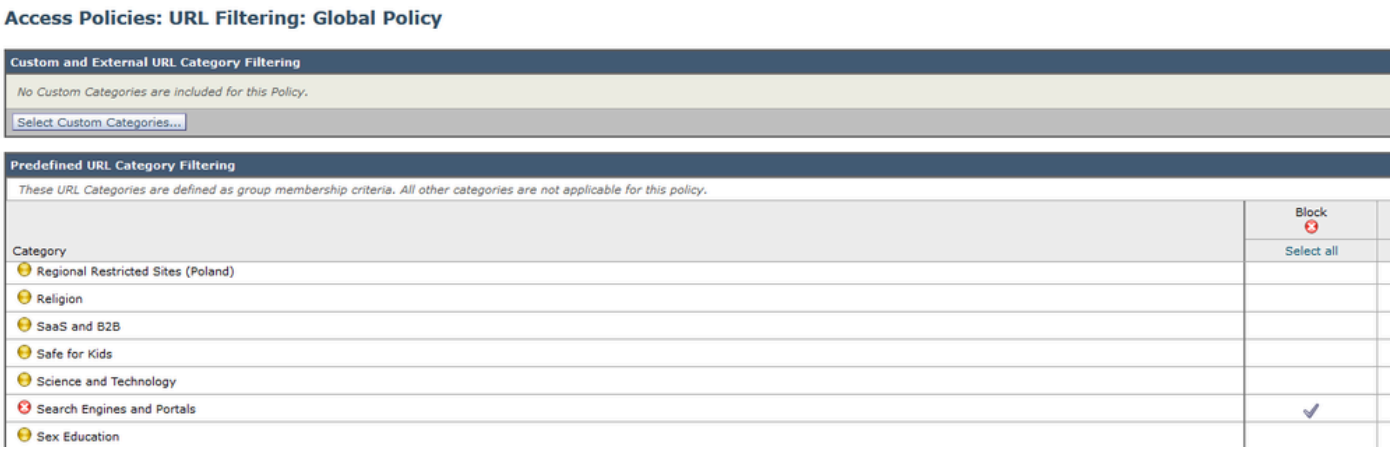
Politique d'accès autorisant Google RECAPTCHA

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



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

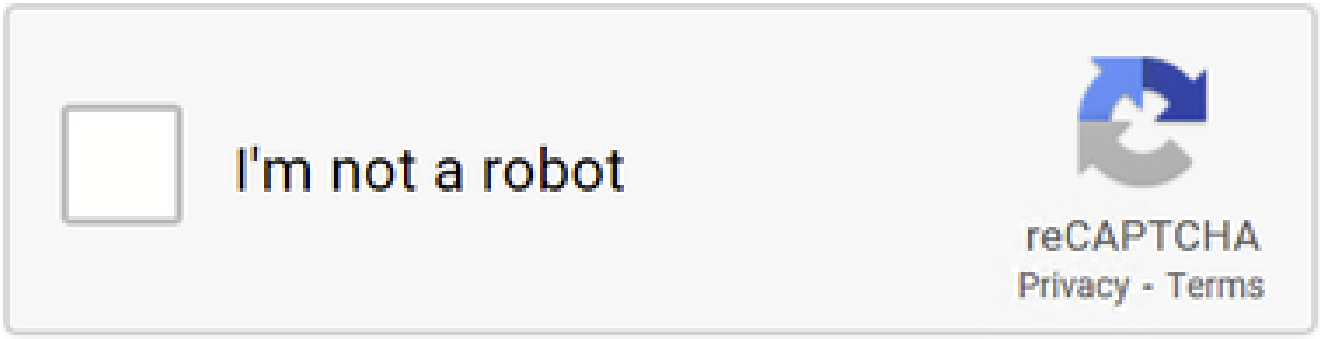
Étape 5. Assurez-vous que **Search Engines and Portals** in **Predefined URL Category Filtering** est bloqué dans la stratégie d'accès globale :



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

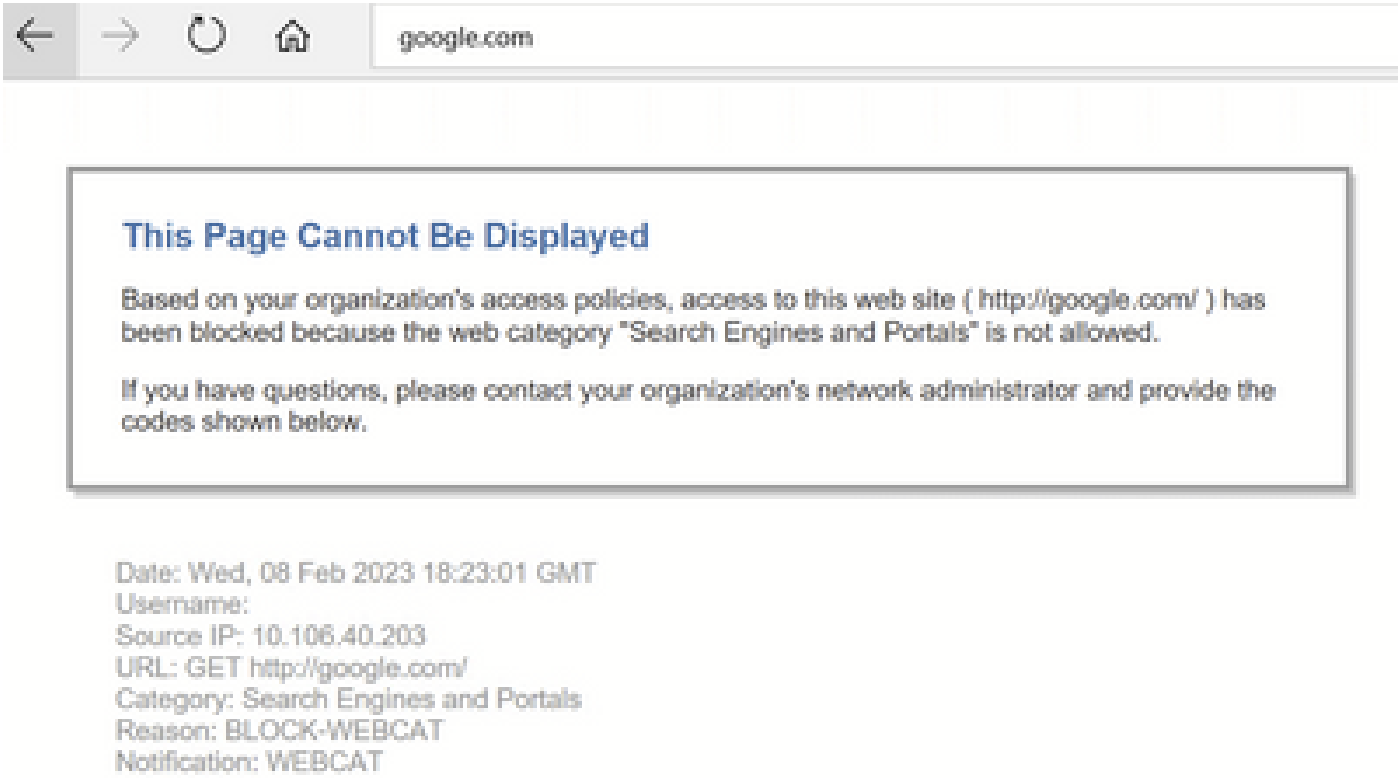
Vérifier

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=6LdN4qUZAAAAAF



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-DefaultG

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-Fi

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.

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.