Consenti a Google reCAPTCHA quando l'accesso ai portali del motore di ricerca è bloccato

Sommario

Introduzione

In questo documento viene descritto come consentire a Google reCAPTCHA in Secure Web Appliance (SWA) di bloccare l'accesso ai portali del motore di ricerca.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Web Access e decrittografia HTTPS.

Cisco consiglia inoltre di:

- SWA fisico o virtuale installato.
- Licenza attivata o installata.
- Installazione guidata completata.
- Accesso amministrativo all'interfaccia grafica (GUI) SWA.

Componenti usati

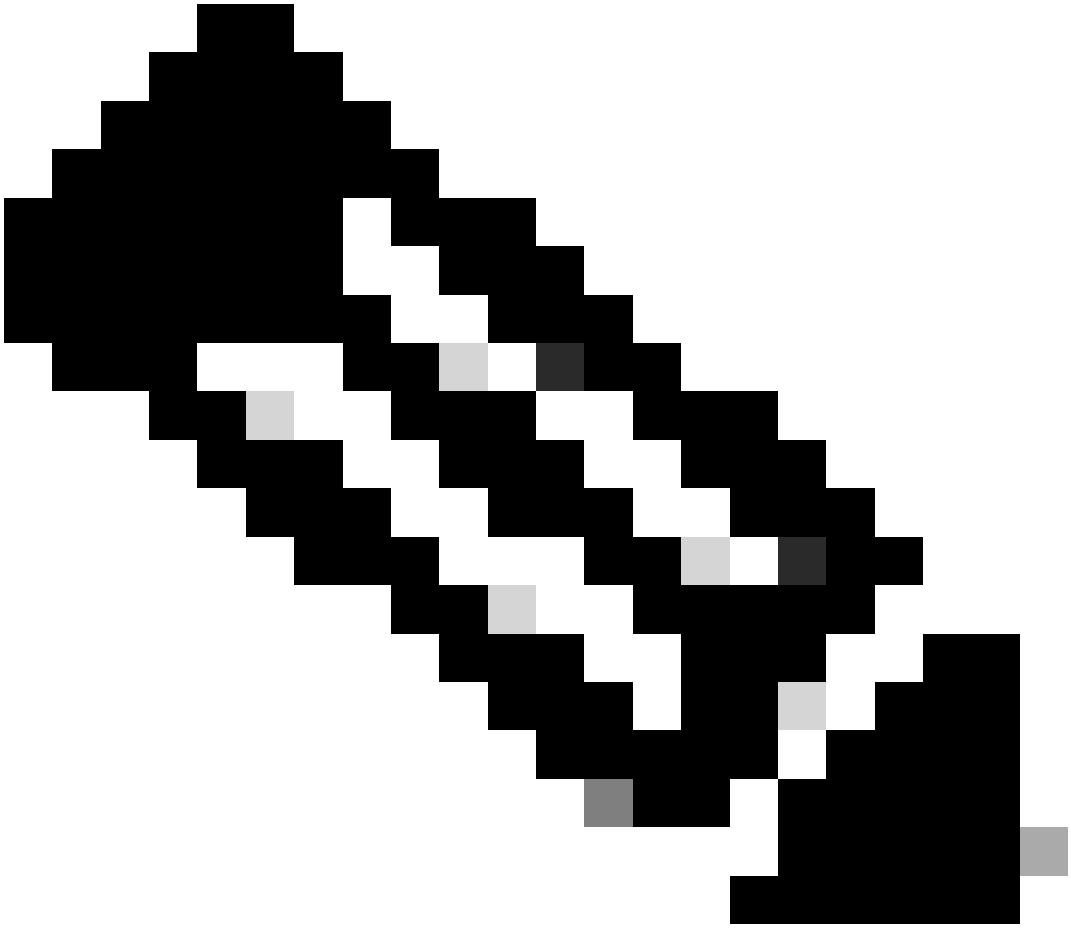
Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

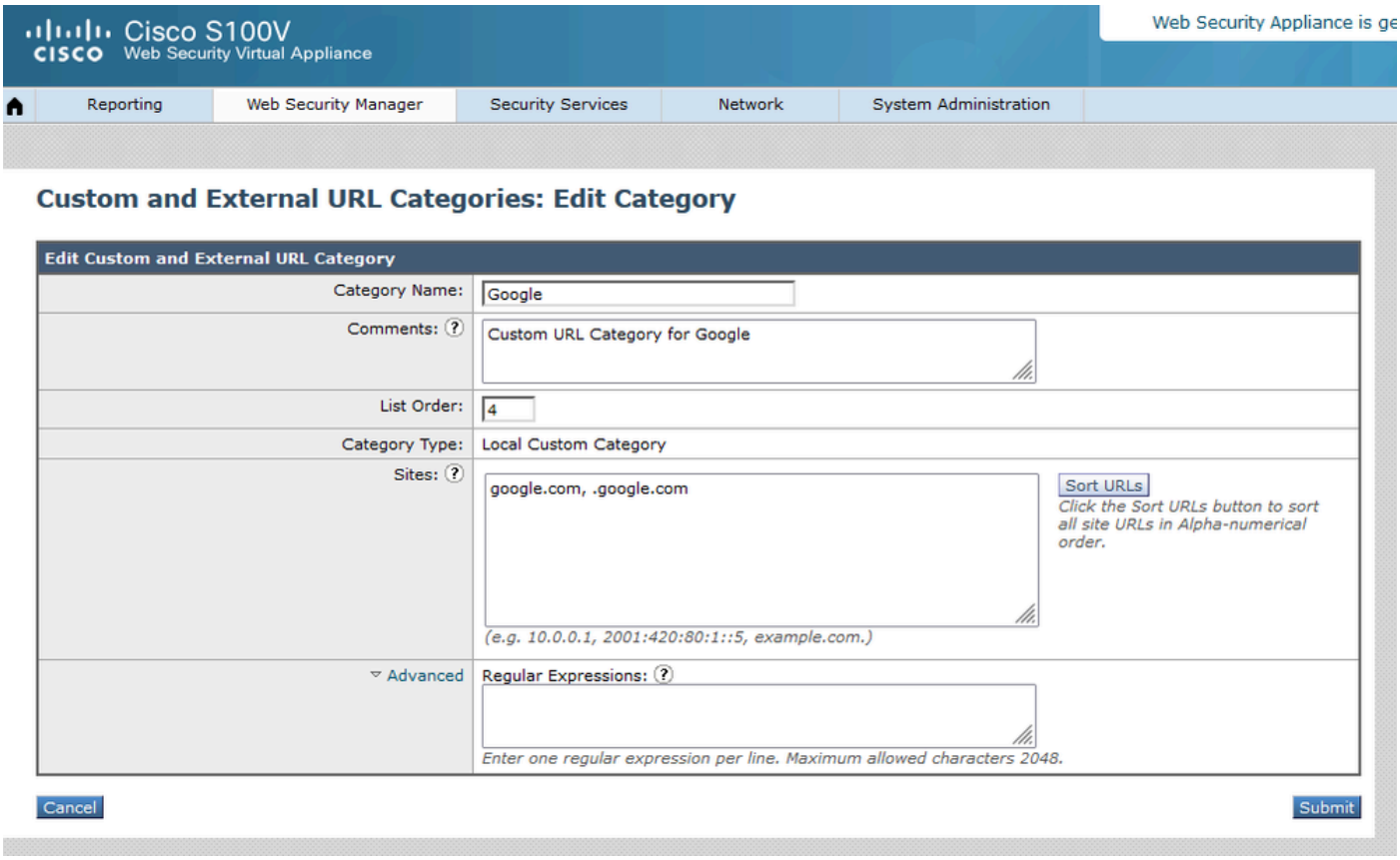
Procedura di configurazione

Passaggio 1. Dalla GUI, passare allaSecurity Services schermata e scegliere HTTPS Proxy, abilita decrittografia HTTPS se non è già abilitata.

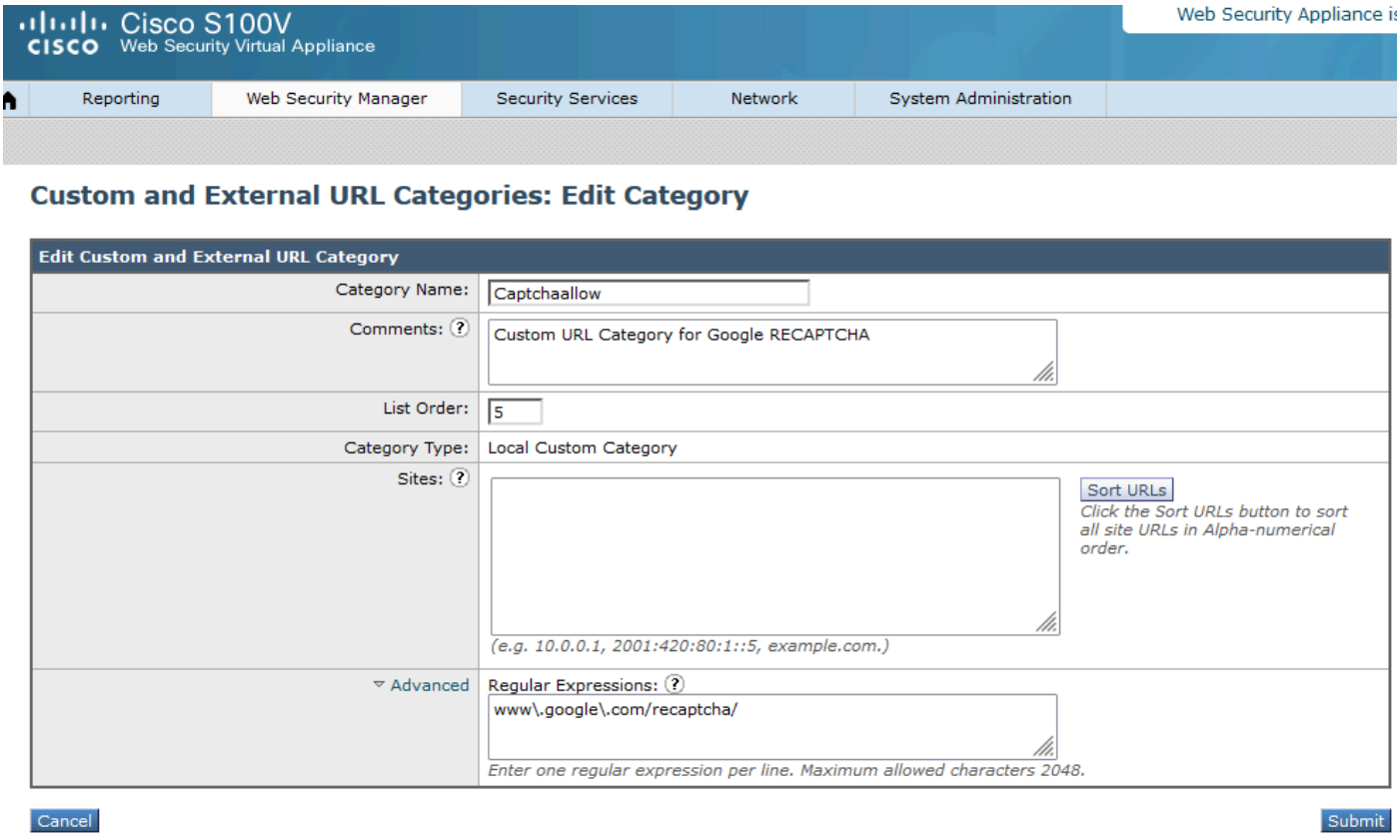


Nota: per questa configurazione è necessario abilitare la decrittografia HTTPS. In caso contrario, fare riferimento all'articolo di riferimento alla fine di questo documento.

Passaggio 2. Dalla GUI, selezionare **Web Security Manager** e scegliere **Custom and External URL Categories**, quindi creare due categorie di URL personalizzate, una per google.com e l'altra per Google reCAPTCHA. Fare clic su **Invia**.



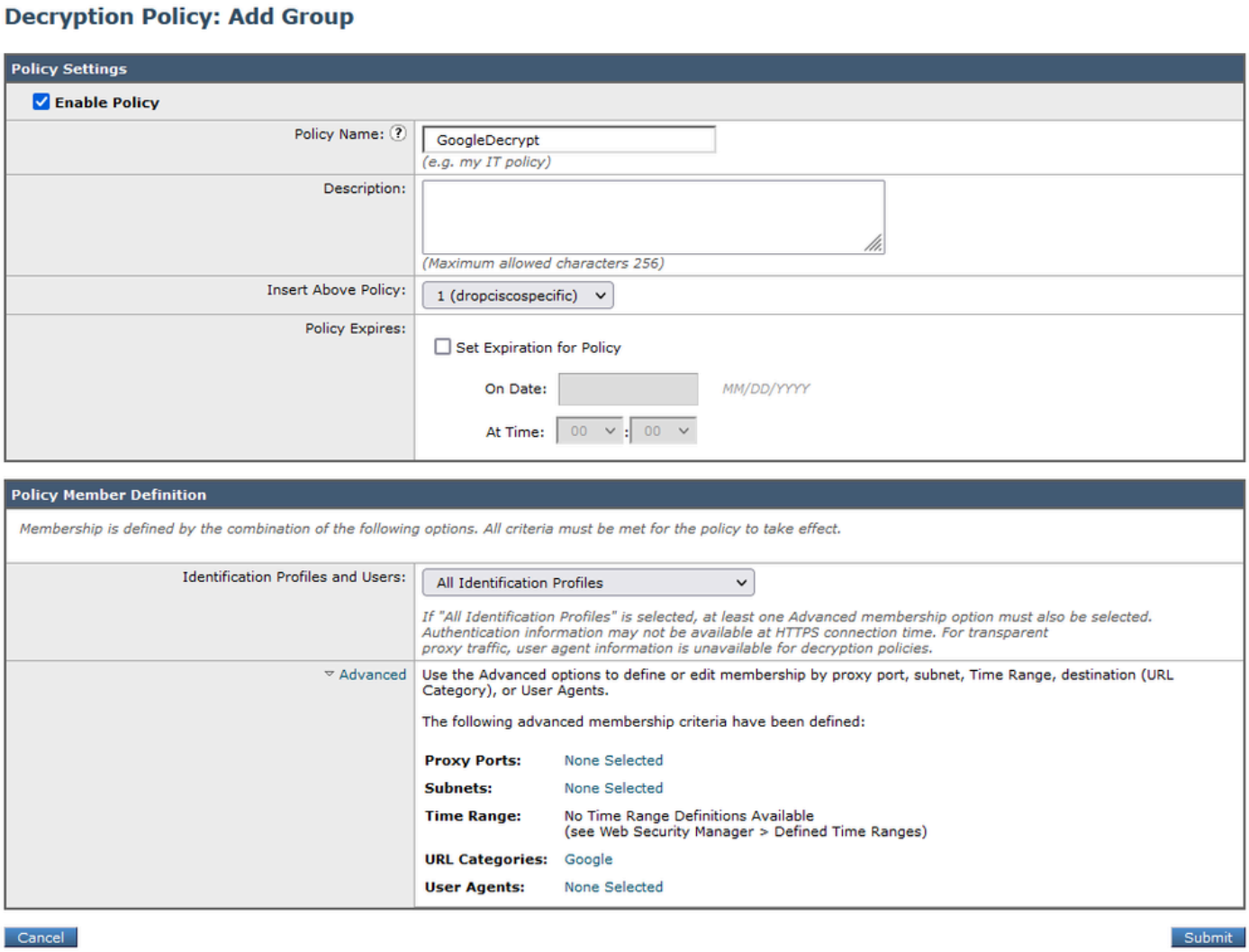
Crea categoria URL personalizzata per Google



Crea categoria URL personalizzata per Google

Passaggio 3. Dalla GUI, passare a **Web Security Manager** e scegliere **Criteri di decrittografia**, quindi creare i criteri di decrittografia per decrittografare google.com. Fare clic su **None Selected** (Nessuno) accanto a **URL Categories** (Categorie URL), quindi selezionare **Google**

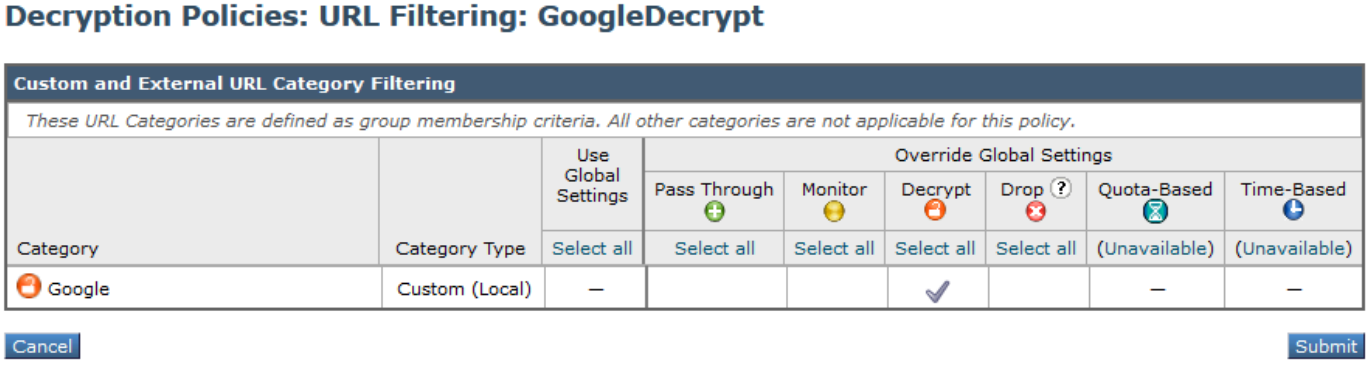
custom URL category (Categoria URL personalizzata Google). Fare clic su **Invia.**



Criterio di decrittografia per decrittografare Google

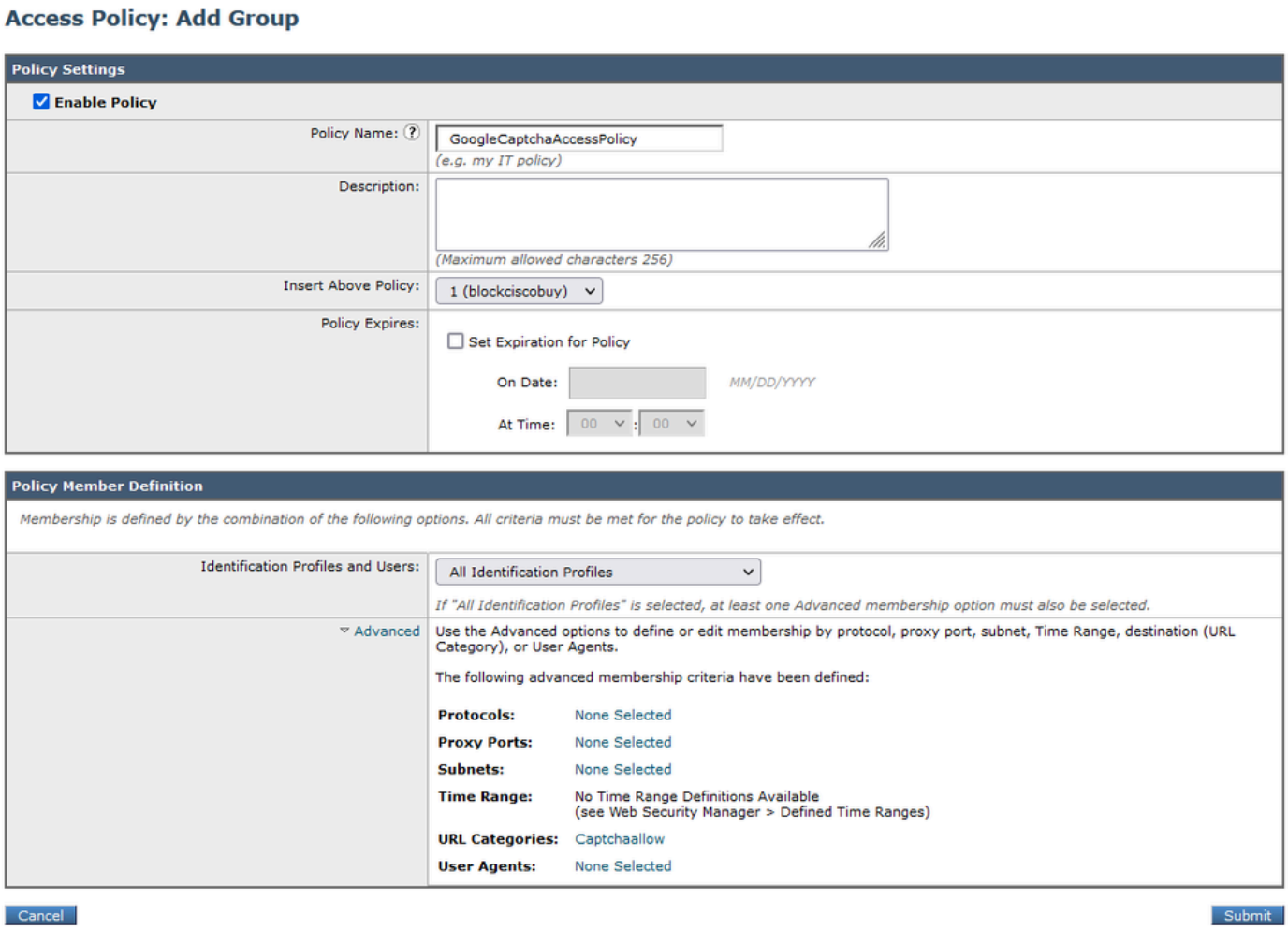
Passaggio 3.1. Passare a **Criteri di decrittografia** e fare clic su **Monitor** in linea con il criterio **GoogleDecrypt.**

Passaggio 3.2. Selezionare **Decrypt** in line to **Google Category** e fare clic su **Submit (Invia).**



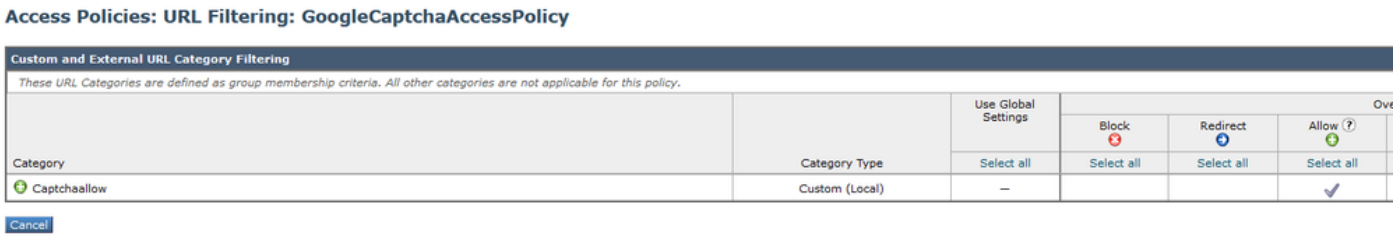
Selezionare la categoria URL personalizzato creato per Google per decrittografarlo nei criteri di decrittografia

Passaggio 4. Dalla GUI, selezionare **Web Security Manager**, quindi **Access Policies**, creare i criteri di accesso per consentire a Google reCAPTCHA e selezionare **captchaallow** come **categorie URL**.



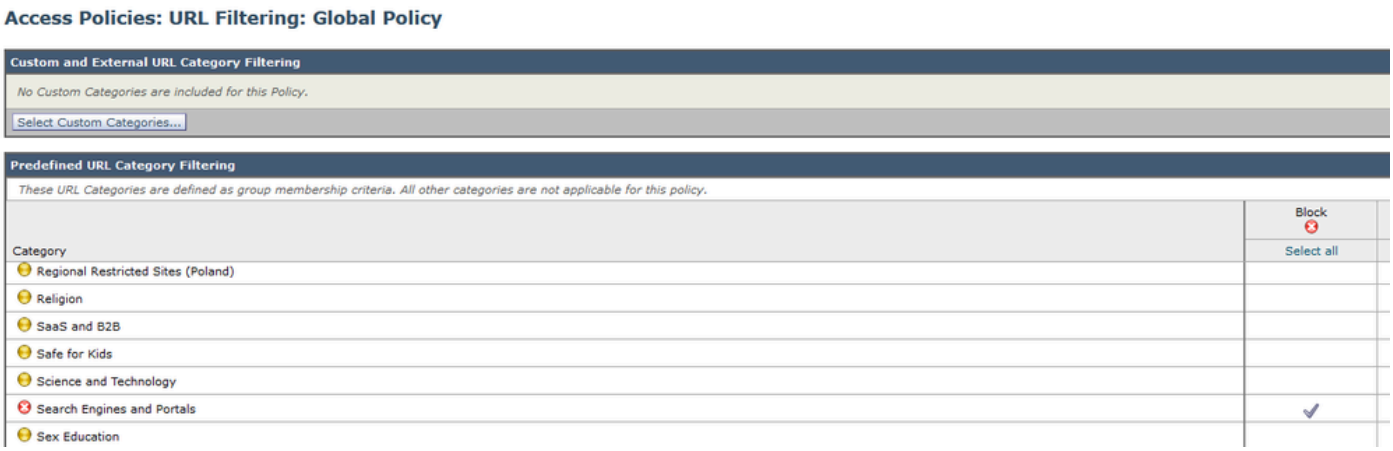
Criteri di accesso per consentire a Google RECAPTCHA

Passaggio 4.1. Passare a Criteri di accesso e fare clic su **Monitoraggio** in linea con il criterio **GoogleCaptchAccessPolicy. Selezionare Allow** in line to **Captchaallow** Category (Consenti in linea alla categoria Captchaallow)**. Invia** e **conferma modifiche.**



Selezionare la categoria URL personalizzato creato per Google RECAPTCHA per consentirlo nei criteri di accesso

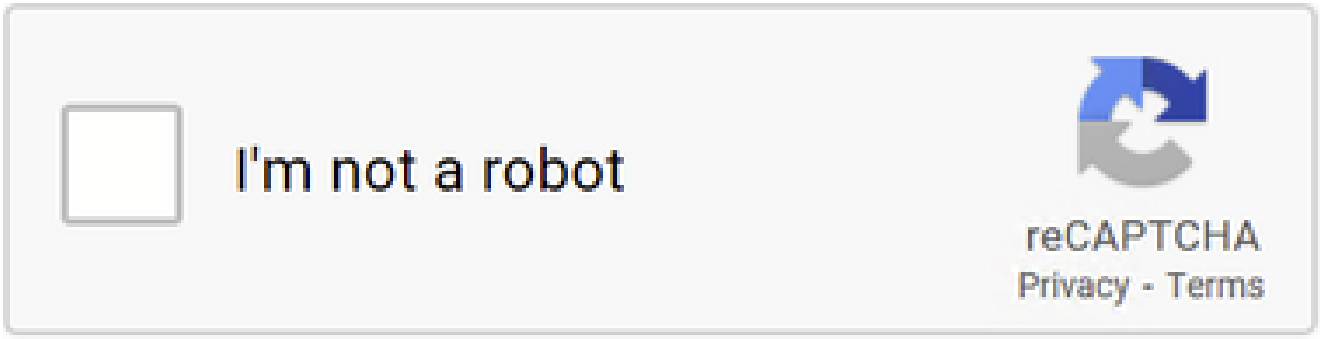
Passaggio 5. Verificare che i **motori di ricerca e i portali** in **Filtro categoria URL predefinito** siano bloccati nei criteri di accesso globale:



Criterio predefinito per bloccare l'accesso ai motori di ricerca

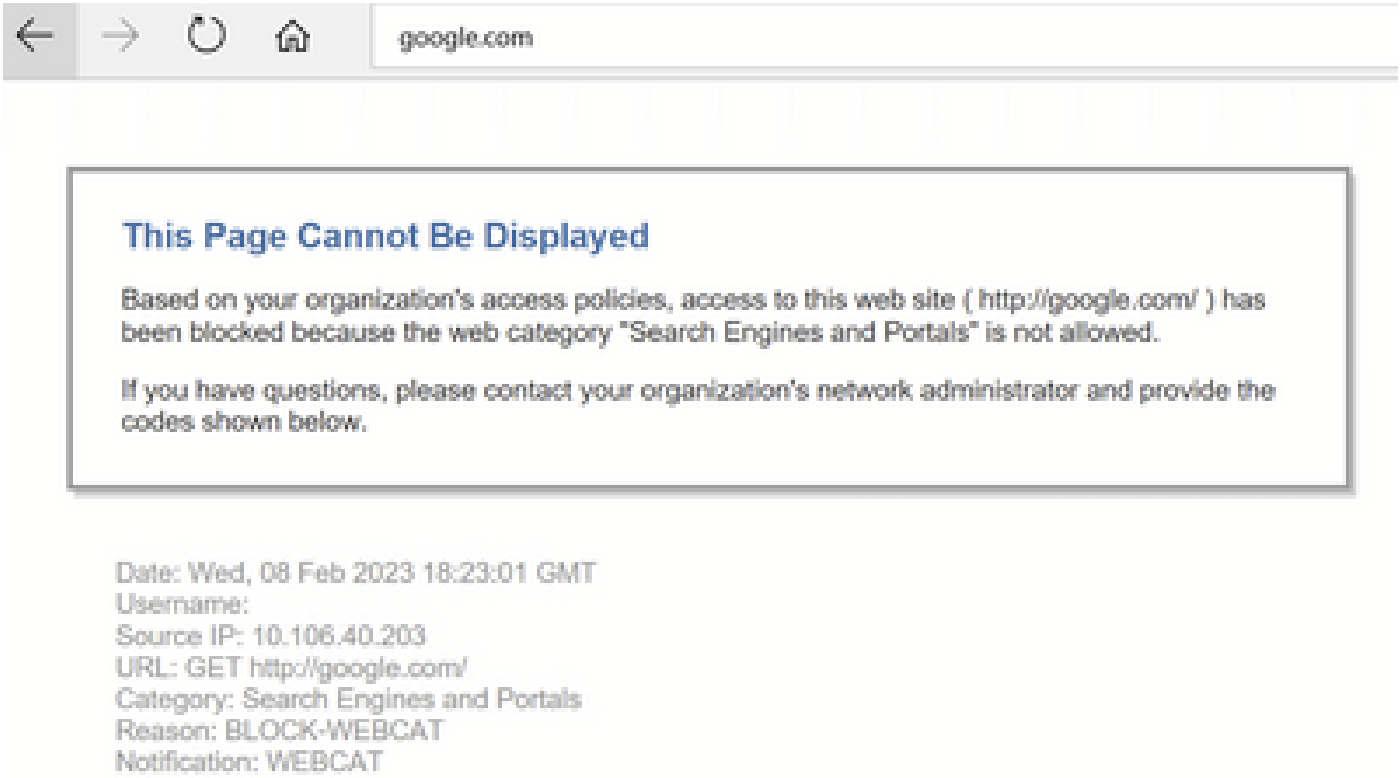
Verifica

È possibile vedere l'accesso a Google reCAPTCHA funziona, ma l'accesso al motore di ricerca (Google) è ancora negato, dopo aver abilitato la decrittografia HTTPS e consentito l'accesso a Google reCAPTCHA nei criteri di accesso:



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



Sito Google bloccato

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

Risoluzione dei problemi

Se l'accesso a Google reCAPTCHA è bloccato, è possibile controllare i log degli accessi nella CLI SWA. Se vedi Google URL e non l'URL di Google reCAPTCHA, è possibile che la decrittografia non sia abilitata:

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

Riferimenti

- Guida per l'utente di AsyncOS 14.5 for Cisco Secure Web Appliance - GD (General Deployment) - Connessione, installazione e configurazione [Cisco Secure Web Appliance] - Cisco
- Utilizzo certificato WSA per decrittografia HTTPS

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).