Google reCAPTCHA toestaan wanneer toegang tot zoekmachineportals is geblokkeerd

Inhoud

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).

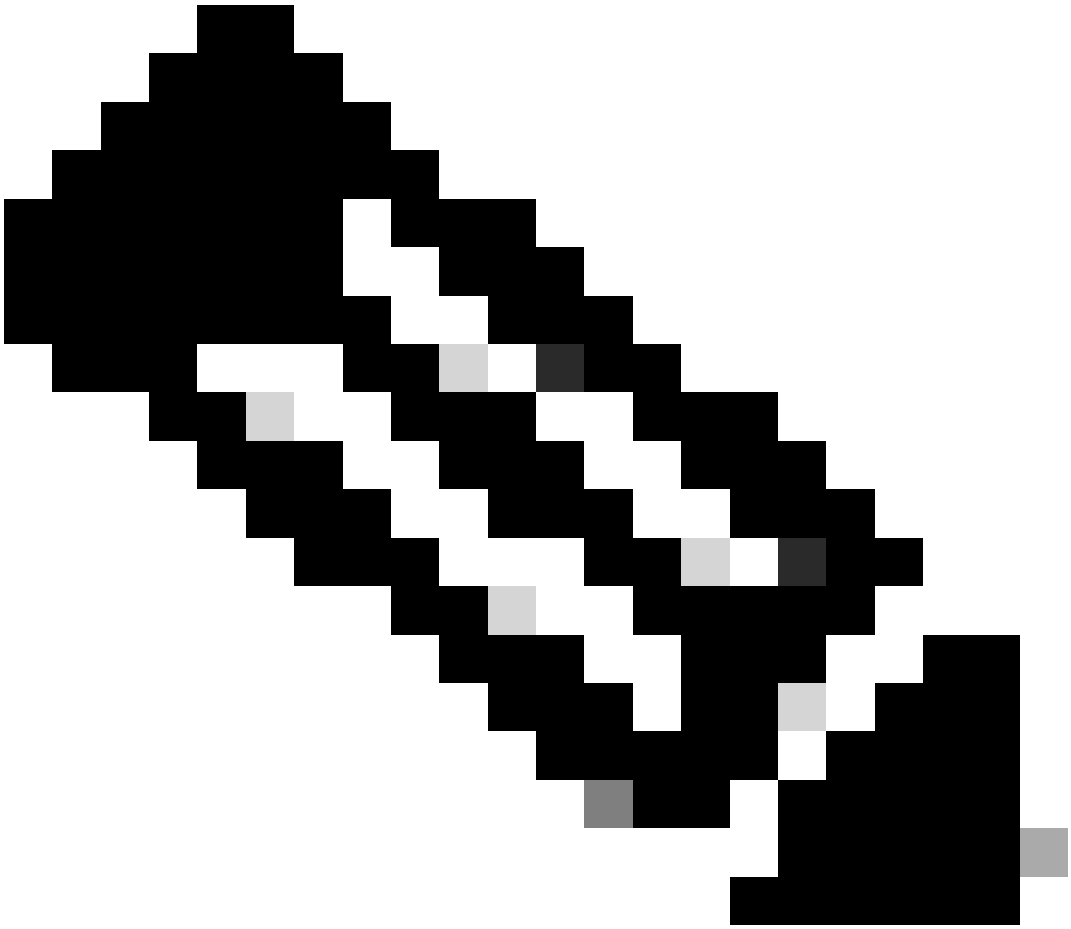
Gebruikte componenten

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.

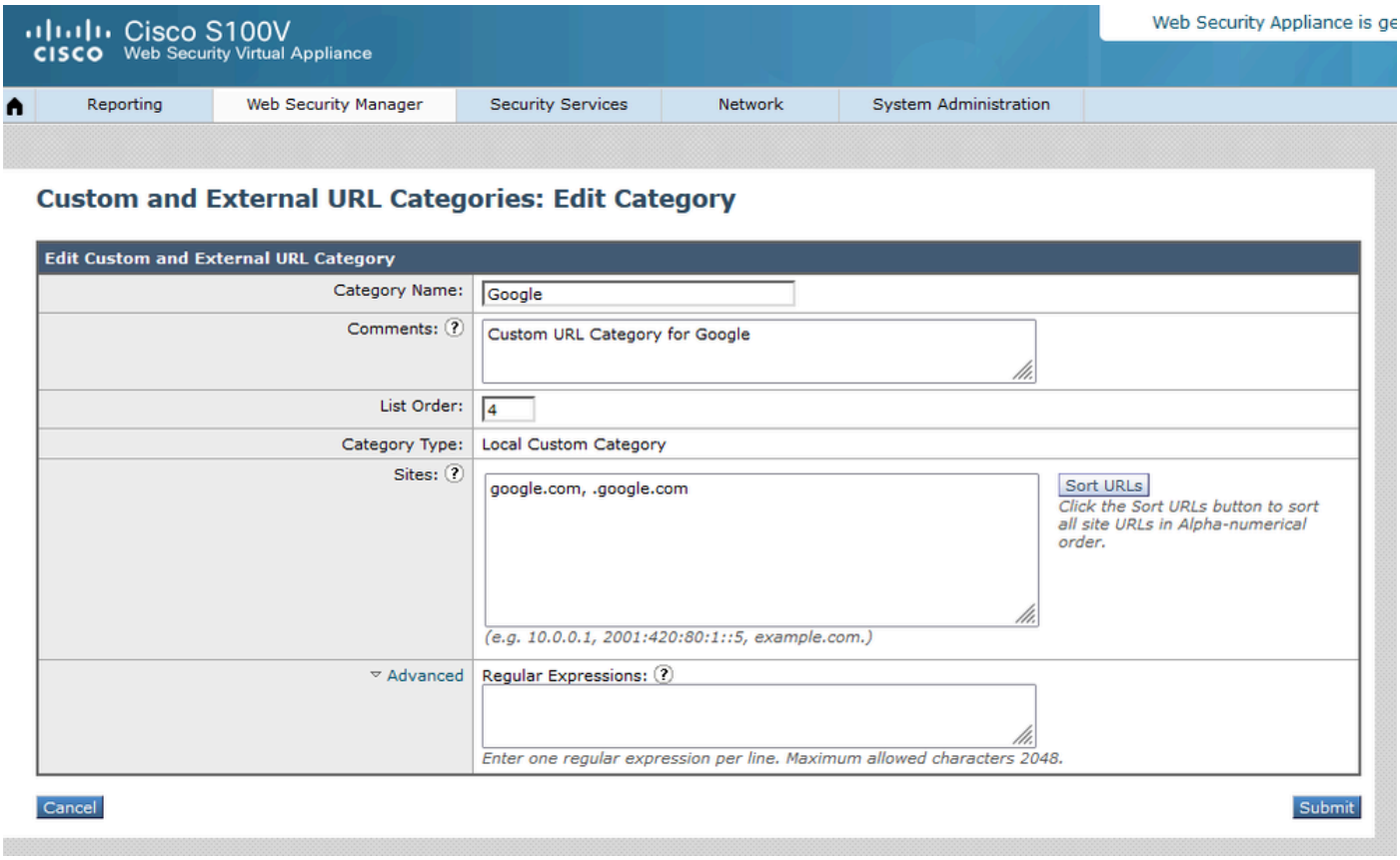
Configuratiestappen

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

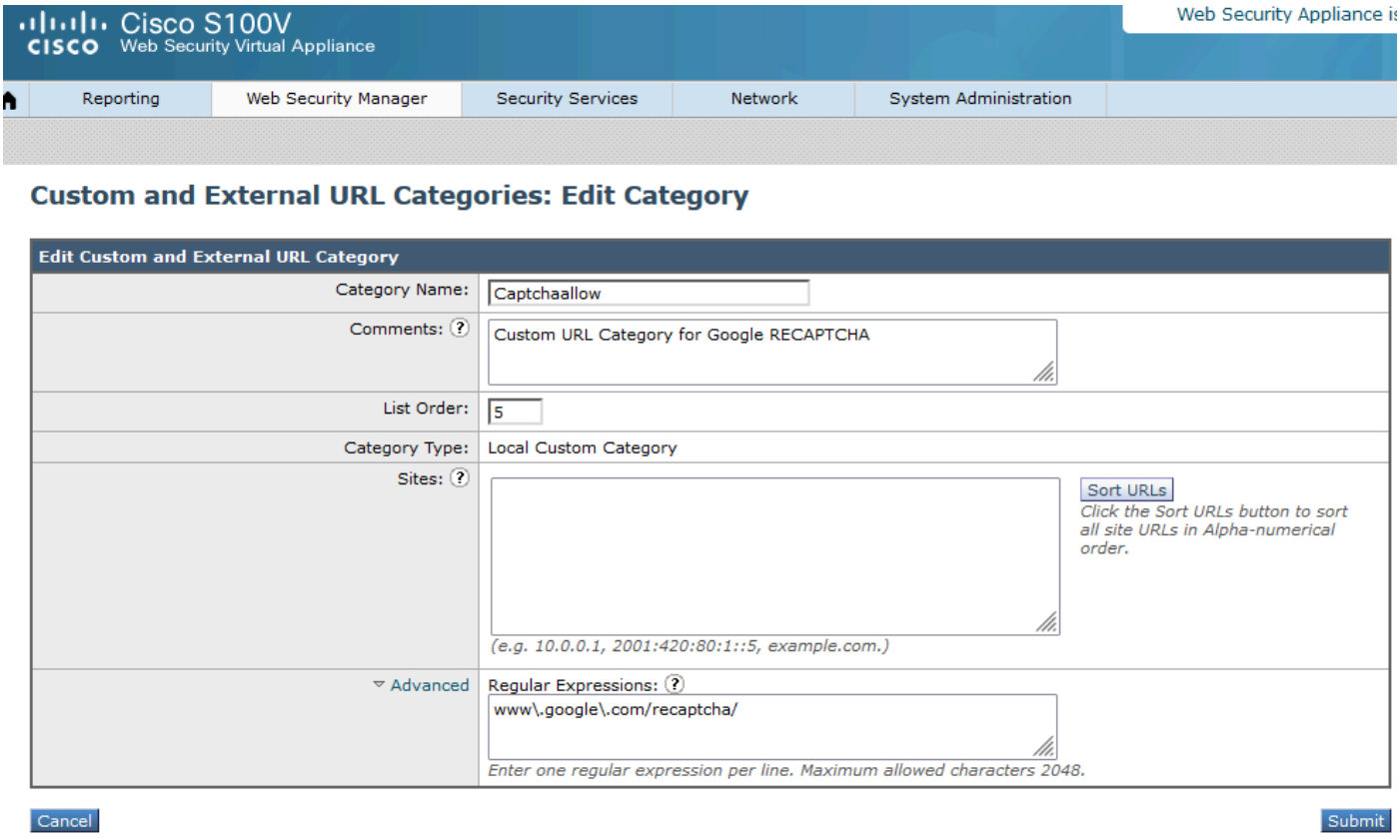


Opmerking: HTTPS-decryptie moet zijn ingeschakeld voor deze configuratie. Als het niet is ingeschakeld, raadpleegt u het artikel waarnaar verwezen wordt aan het eind van dit document.

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**.



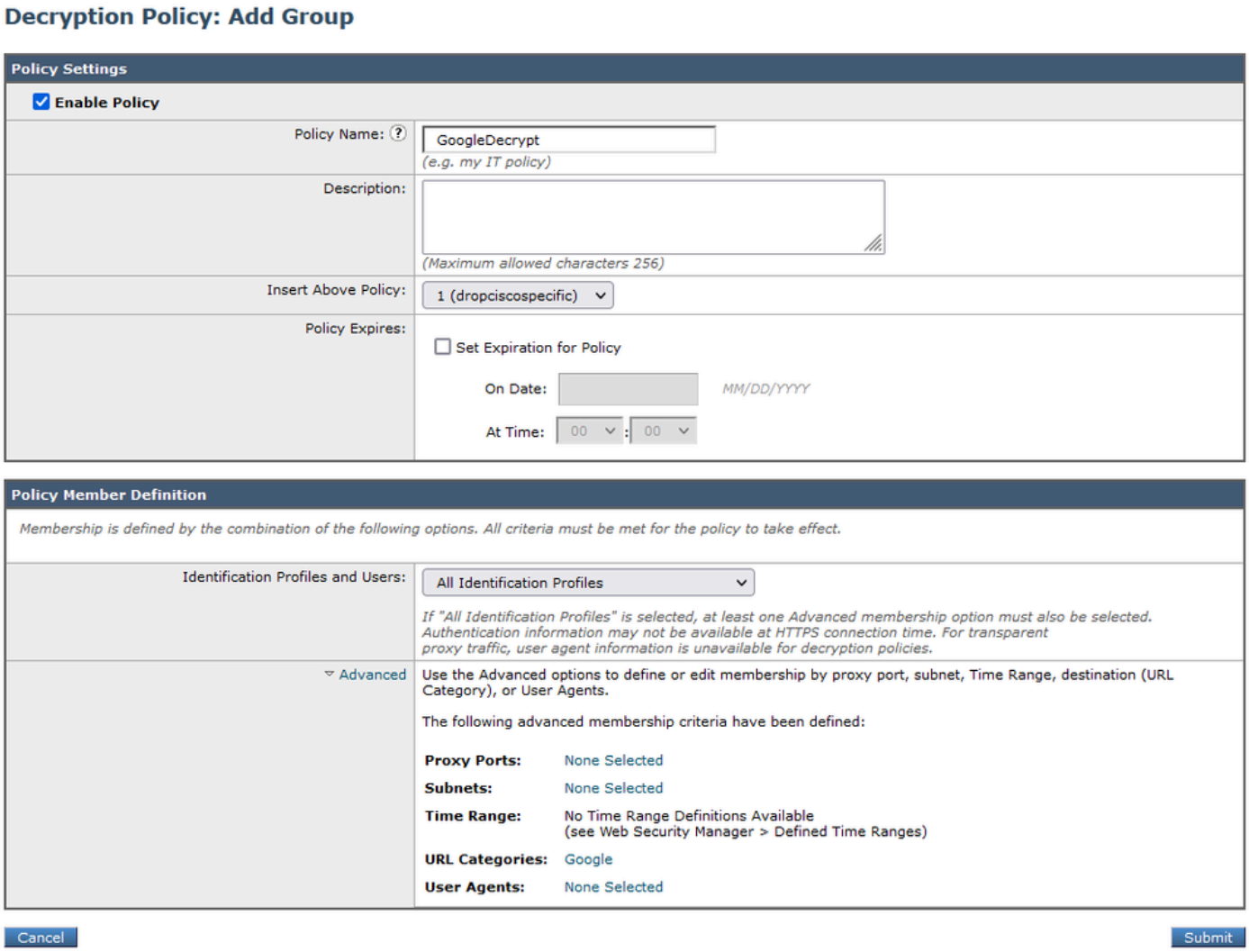
Aangepaste URL-categorie maken voor Google



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**, creeer decryptiebeleid om google.com te decrypteren. Klik op **Geen geselecteerd** naast de **URL-categorieën** en selecteer de **aangepaste Google**-URL-categorie. Klik op

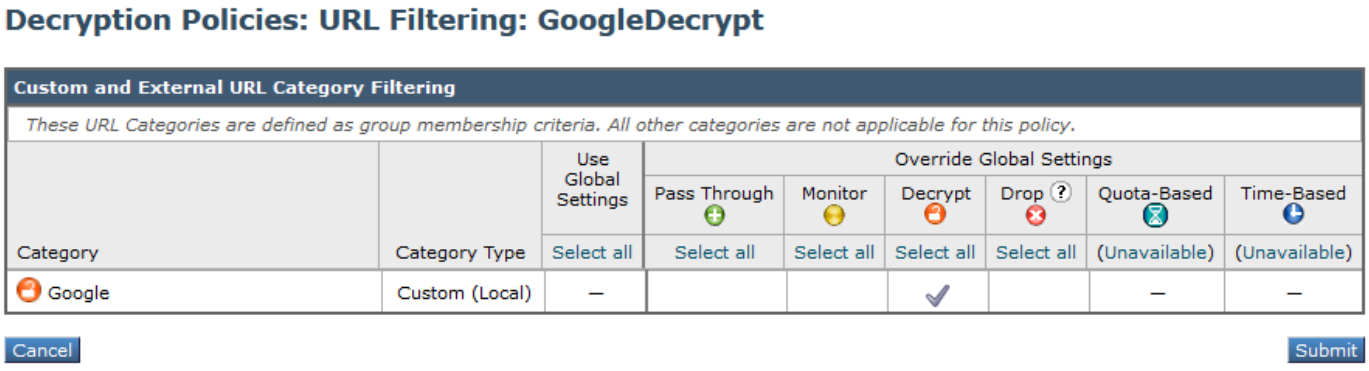
Verzenden.



Het beleid van de decryptie om Google te decrypteren

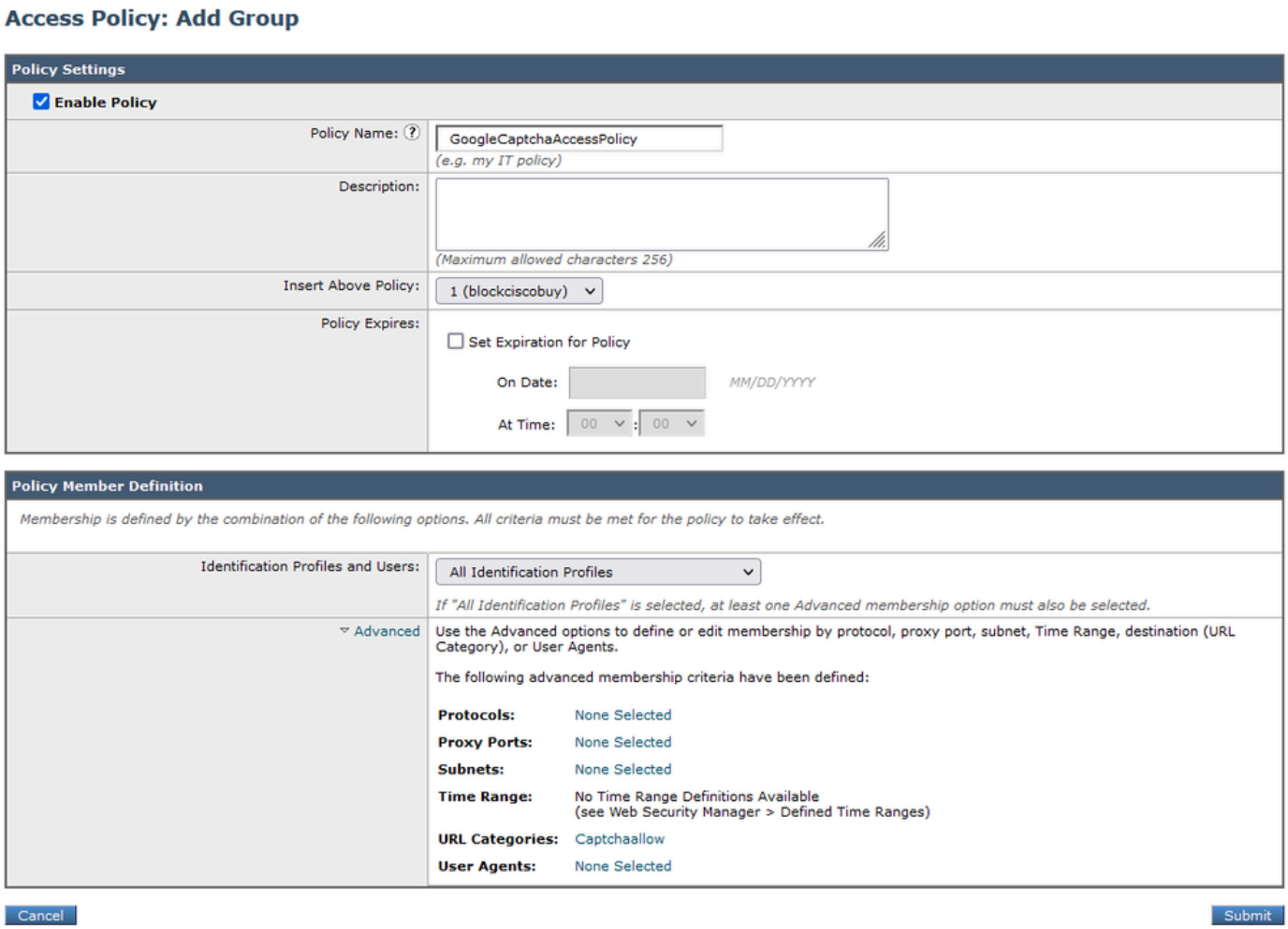
Stap 3.1. Navigeer naar **decryptie beleid** en klik op **Monitor** in lijn met het **GoogleDecrypt** beleid**.**

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



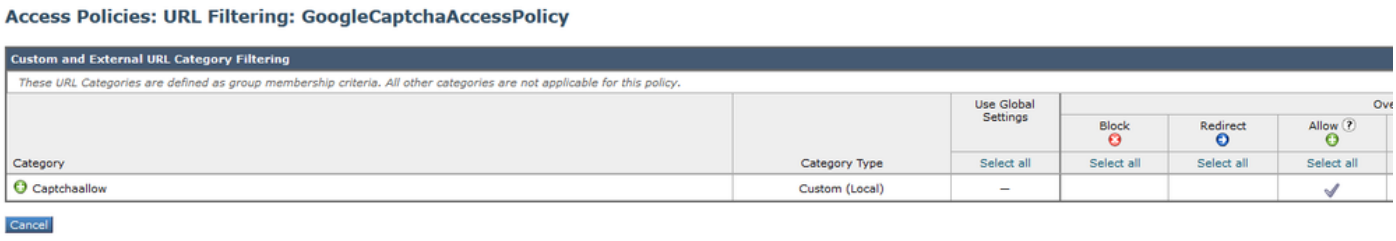
Selecteer Aangepaste URL-categorie voor Google om deze te decrypteren in het decryptie beleid

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



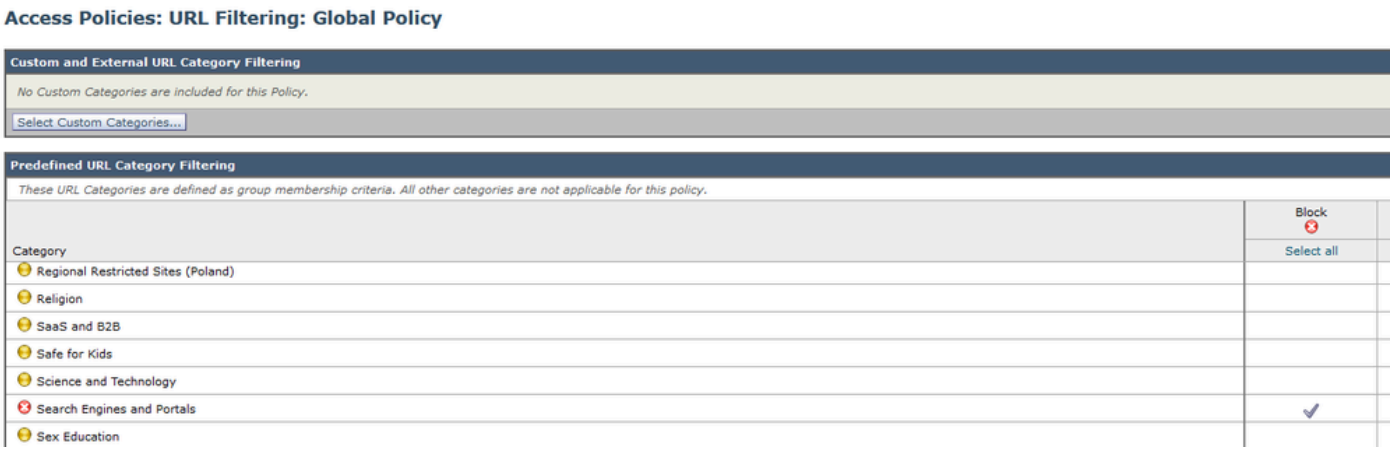
Toegangsbeleid om Google RECAPTCHA toe te staan

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



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

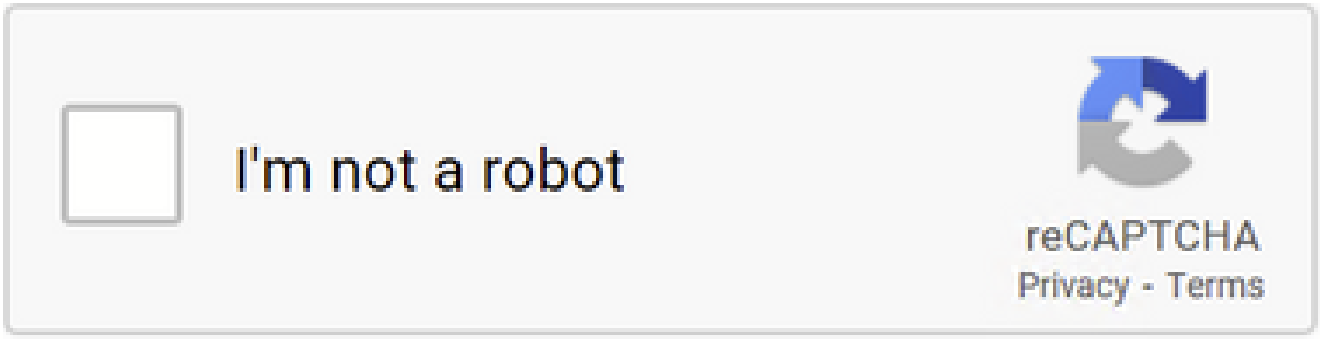
Stap 5. Zorg ervoor dat **zoekmachines en portals** in **vooraf gedefinieerde URL-categoriefiltering** worden geblokkeerd in het algemene toegangsbeleid:



Standaardbeleid om de toegang tot zoekmachines te blokkeren

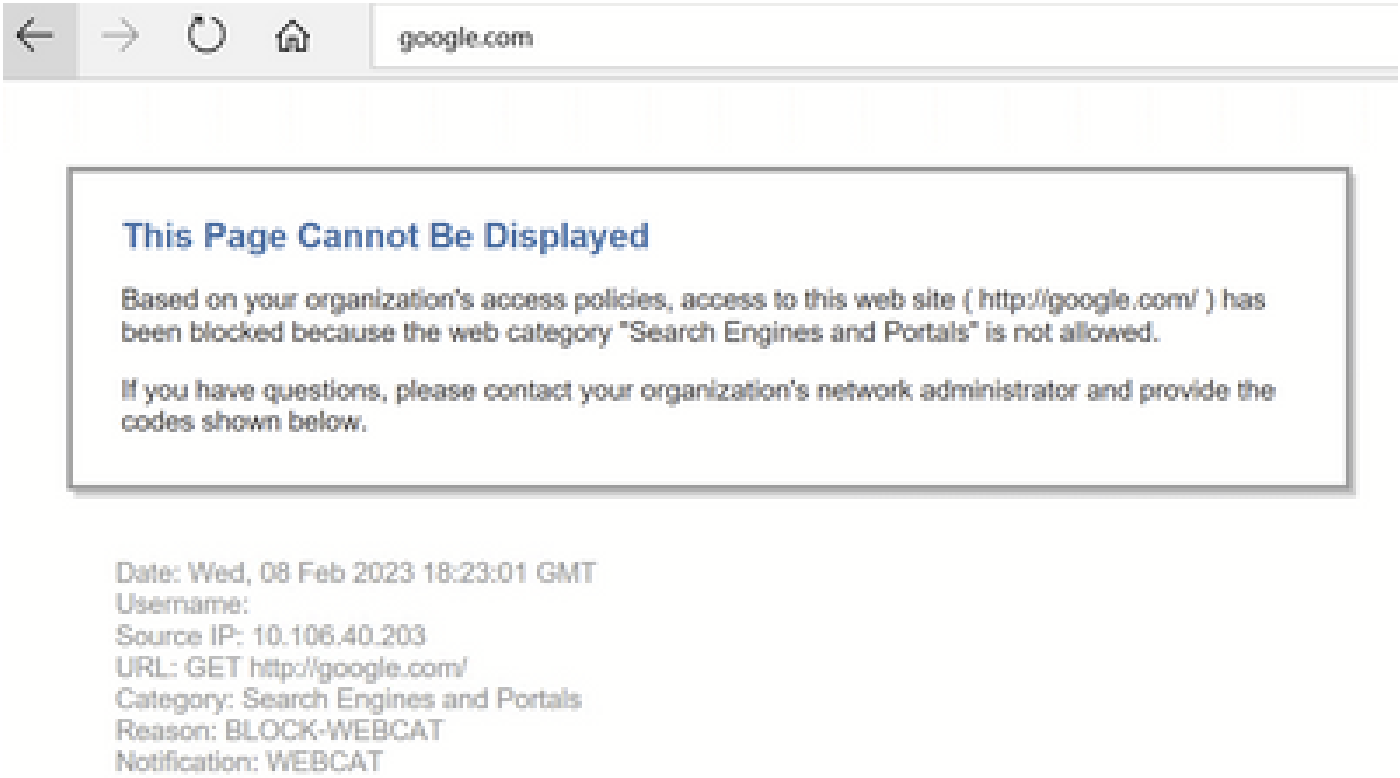
Verifiëren

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=6LdN4qUZAAAAAF



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-Fi

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.