Google AI-modus blokkeren in de Secure Web Appliance

Inhoud

Inleiding

In dit document worden de noodzakelijke stappen beschreven die moeten worden uitgevoerd om de Secure Web Appliance zodanig te configureren dat de HTTPS-aanvragen voor de Google AI-modus worden geblokkeerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- SWA-toediening
- Basisprotocollen voor netwerken en proxy's
- Decodering van de SWA
- Reguliere expressies

Cisco raadt u aan deze hulpprogramma's te installeren:

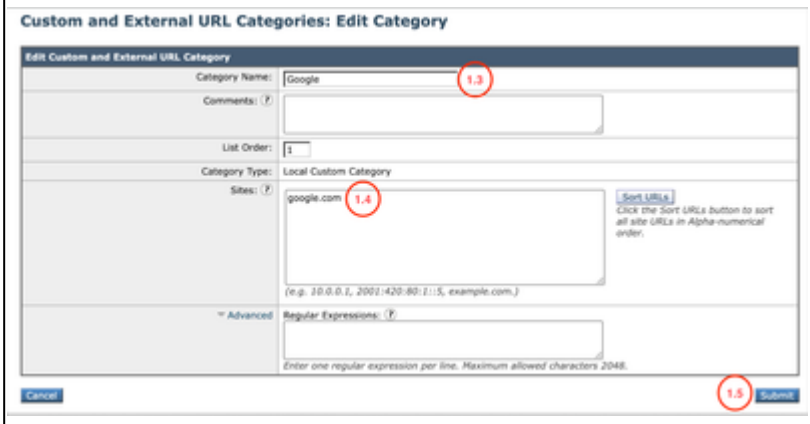
- Fysieke of virtuele SWA
- Administratieve toegang tot de grafische gebruikersinterface (GUI) van SWA

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. Maak een aangepaste URL-categorie voor de Google-website.	Stap 1.1. Navigeer vanuit de GUI naar Web Security Manager en kies Aangepaste en Externe URL-categorieën. Stap 1.2. Klik op Rubriek toevoegen om een nieuwe aangepaste URL-rubriek te maken. Stap 1.3. Voer de naam voor de nieuwe rubriek in. Stap 1.4. Definieer deze URL's in het gedeelte Sites: `google.com` Stap 1.5. Dien de wijzigingen in. 
Stap 2. Maak een aangepaste URL-categorie voor de Google AI-modus.	Stap 2.1. Navigeer vanuit de GUI naar Web Security Manager en kies Aangepaste en Externe URL-categorieën.

<table>
<tr>
<td></td>
<td>Stap 2.2. Klik op Rubriek toevoegen om een nieuwe aangepaste URL-rubriek te maken.

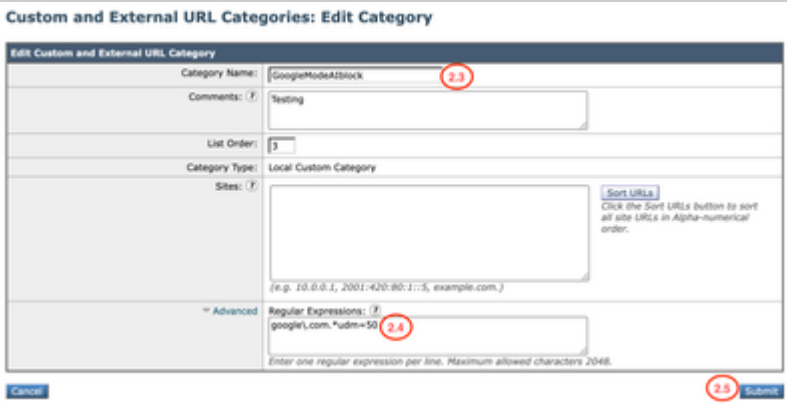
Stap 2.3. Voer de naam voor de nieuwe rubriek in.

Stap 2.4. Definieer deze URL's in de sectie Reguliere expressies:

<code>google\.com.*udm=50</code>

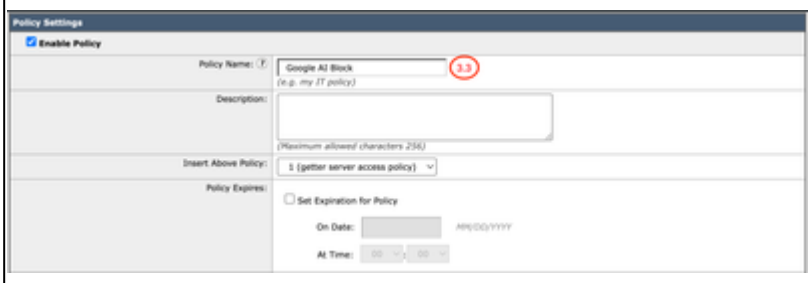
Stap 2.5. Dien de wijzigingen in.

Tip: Ga voor meer informatie over het configureren van aangepaste URL-categorieën naar: Aangepaste URL-categorieën configureren in Secure Web Appliance - Cisco

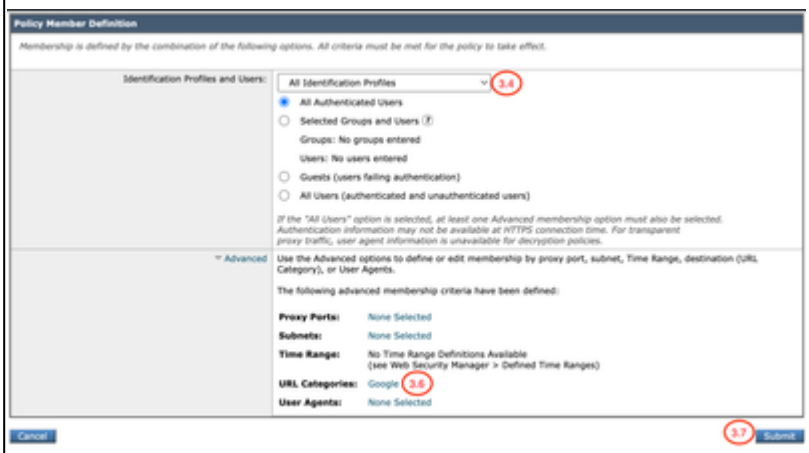
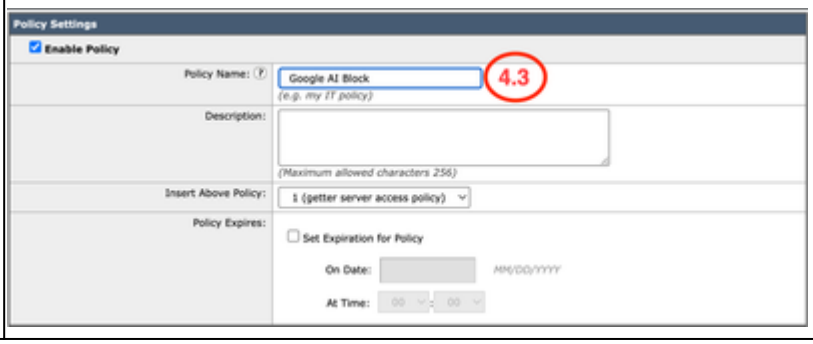
  </td>
</tr>
<tr>
<td>Stap 3. Decodeer het verkeer voor Google.</td>
<td>Stap 3.1. Navigeer vanuit de GUI naar Web Security Manager en kies Decryptiebeleid

Stap 3.2. Klik op Beleid toevoegen.

Stap 3.3. Voer een naam in voor het nieuwe beleid.

Stap 3.4. (Optioneel) Selecteer het identificatieprofiel waarop u dit beleid wilt toepassen.</td>
</tr>
</table>

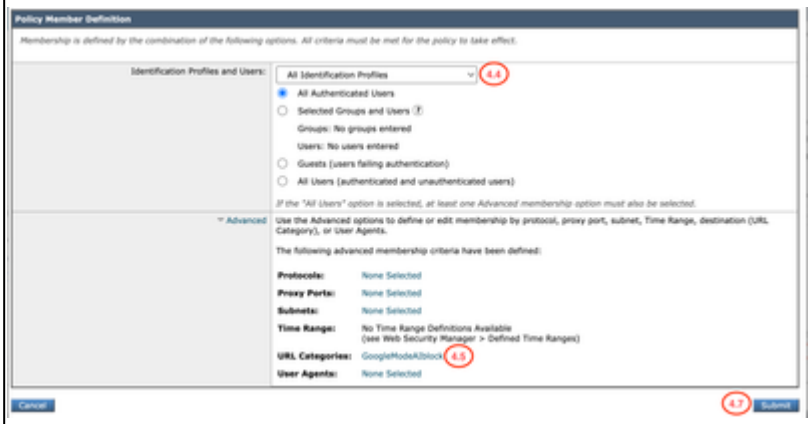
	Stap 3.5. Klik in de sectie Definitie van beleidslid op URL-categorieën links om de aangepaste URL-categorie toe te voegen. Stap 3.6. Selecteer de URL-categorie die is gemaakt in stap 1. Stap 3.7. Klik op Indienen.  Stap 3.8. Klik op de pagina Decryptiebeleid op de koppeling URL-filtering voor het nieuwe beleid. Stap 3.9. Kies Decrypt als de actie voor Aangepaste URL-rubriek. Stap 3.10. Klik op Indienen. 
Stap 4. Blokkeer de Google AI-verkeersmodus.	Stap 4.1. Navigeer vanuit de GUI naar Web Security Manager en kies Toegangsbeleid. Stap 4.2. Klik op Beleid toevoegen. Stap 4.3. Voer een naam in voor het nieuwe beleid. 

Stap 4.4. (Optioneel) Selecteer het identificatieprofiel waarop u dit beleid wilt toepassen.

Stap 4.5. Klik in de sectie Definitie van beleidslid op URL-categorieën links om de aangepaste URL-categorie toe te voegen.

Stap 4.6. Selecteer de URL-categorie die is gemaakt in stap 2.

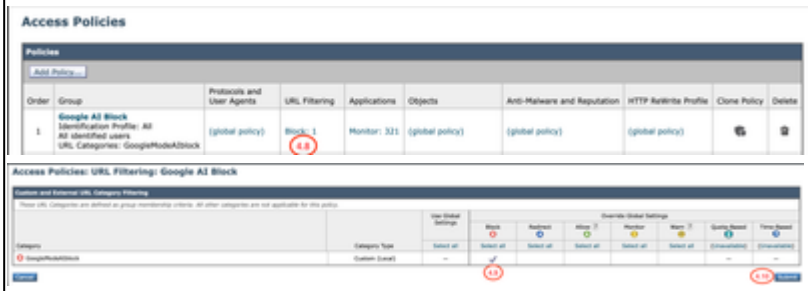
Stap 4.7. Klik op Indienen.



Stap 4.8. Klik in Access Policies op de link van URL Filtering voor het nieuwe beleid.

Stap 4.9. Kies Blokkeren als actie voor aangepaste URL-rubriek.

Stap 4.10. Klik op Indienen.



Stap 4.11. Wijzigen doorvoeren.

Verifiëren

Wanneer de configuratie-instellingen zijn voltooid, wordt Google AI-verkeer verwerkt in de toegangslogboeken als Blok, zoals wordt gedetecteerd door de aangepaste categorie die we hebben gemaakt voor Google AI Block.

<#root>

1779219170.427 101 10.184.103.26

TCP_DENIED_SSL/403

0 GET https://www.google.com:443/search?q=cisco+live+&sca_esv=afc85aa92f7b31d4&source=hp&ei=2roMatavIo

BLOCK_CUSTOMCAT_12-Google_AI_Block

-ciscotest-NONE-NONE-NONE-NONE-NONE <"C_Goo0",4.7,-,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,"IW_srch"

Een aanvraag voor een zoekopdracht via de Google AI-modus wordt geblokkeerd en geeft deze melding aan de eindgebruiker weer.

Al het andere Google-verkeer blijft toegestaan.

Gerelateerde informatie

Aangepaste URL-categorieën definiëren in WSA

Gebruikershandleiding voor AsyncOS 15.2 voor Cisco Secure Web Appliance

Decryptiecertificaat configureren in Secure Web Appliance

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.