

Blocco della modalità AI di Google in Secure Web Appliance

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Passi di configurazione](#)

[Verifica](#)

[Informazioni correlate](#)

Introduzione

In questo documento vengono descritti i passaggi necessari per consentire a Secure Web Appliance di essere configurata per bloccare le richieste HTTPS alla modalità AI di Google.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Amministrazione SWA
- Protocolli di rete e proxy di base
- Processo di decrittazione dell'SWA
- Espressioni regolari

Cisco consiglia di installare i seguenti strumenti:

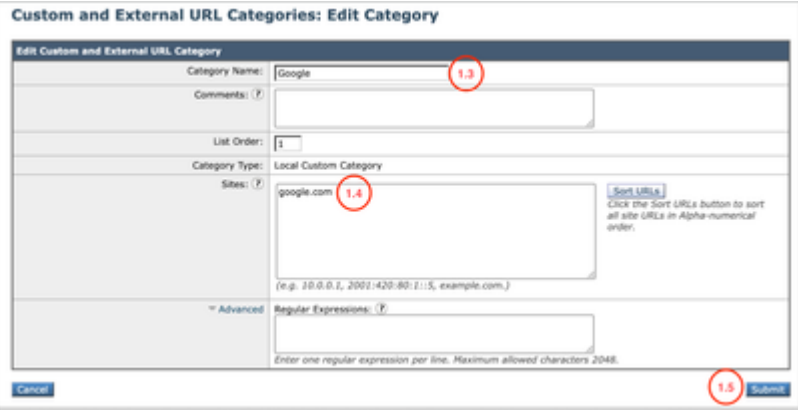
- SWA fisico o virtuale
- Accesso amministrativo all'interfaccia grafica (GUI) SWA

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.

Passi di configurazione

<p>Passaggio 1. Creare una categoria di URL personalizzati per il sito Web Google.</p>	<p>Passaggio 1.1. Dalla GUI, selezionare Web Security Manager, quindi selezionare Custom and External URL Categories (Categorie di URL esterni e personalizzati).</p> <p>Passaggio 1.2. Fare clic su Add Category (Aggiungi categoria) per creare una nuova categoria di URL personalizzati.</p> <p>Passaggio 1.3. Inserire il nome della nuova categoria.</p> <p>Passaggio 1.4. Definire gli URL nella sezione Siti: google.com</p> <p>Passaggio 1.5. Sottomettere le modifiche.</p> 
<p>Passaggio 2. Creare una categoria URL personalizzato per la modalità AI di Google.</p>	<p>Passaggio 2.1. Dalla GUI, selezionare Web Security Manager, quindi selezionare Custom and External URL Categories (Categorie di URL esterni e personalizzati).</p> <p>Passaggio 2.2. Per creare una nuova categoria di URL personalizzati, fare clic su Add Category (Aggiungi</p>

categoria).

Passaggio 2.3. Inserire il nome della nuova categoria.

Passaggio 2.4. Definire gli URL nella sezione Espressioni regolari:

google\.com.*udm=50

Passaggio 2.5. Sottomettere le modifiche.



Suggerimento: Per ulteriori informazioni su come configurare le categorie URL personalizzate, visitare: [Configure Custom URL Categories in Secure Web Appliance - Cisco](#)

Custom and External URL Categories: Edit Category

Category Name: GoogleModeA2block (2.3)
Comments: Testing
List Order: 3
Category Type: Local Custom Category
Sites:
Sort URLs: Click the Sort URLs button to sort all site URLs in Alpha-numerical order.
Regular Expressions: google\.com.*udm=50 (2.4)
Enter one regular expression per line. Maximum allowed characters 2048.
Cancel Submit (2.5)

Passaggio 3.1. Dalla GUI, selezionare Web Security Manager, quindi selezionare Decryption Policies (Criteri di decrittografia)

Passaggio 3.2. Fare clic su Aggiungi criterio.

Passaggio 3.3. Immettere il nome per il nuovo criterio.

Passaggio 3. Decrittare il traffico per Google.

Policy Settings
Enable Policy
Policy Name: Google All Block (3.3)
Description:
Insert Above Policy: 1 (gettier server access policy)
Policy Expires:
Set Expiration for Policy
On Date:
At Time: 00:00:00

Passaggio 3.4. (Facoltativo) Selezionare il profilo di identificazione a cui applicare il criterio.

Passaggio 3.5. Dalla sezione Definizione membro criterio, fare clic su URL Categories (Categorie URL) per aggiungere la categoria URL personalizzata.

Passaggio 3.6. Selezionare la categoria URL creata nel Passaggio 1.

Passaggio 3.7. Fare clic su Sottometti.

Policy Member Definition

Membership is defined by the combination of the following options. All criteria must be met for the policy to take effect.

Identification Profiles and Users:

All Identification Profiles **3.5**

All Authenticated Users

Selected Groups and Users (7)

Groups: No groups entered

Users: No users entered

Guests (users failing authentication)

All Users (authenticated and unauthenticated users)

If the "All Users" option is selected, at least one Advanced membership option must also be selected. Authentication information may not be available at HTTPS connection time. For transparent proxy traffic, user agent information is unavailable for decryption policies.

Use the Advanced options to define or edit membership by proxy port, subnet, Time Range, destination (URL Category), or User Agents.

The following advanced membership criteria have been defined:

Proxy Ports: None Selected

Subnets: None Selected

Time Range: No Time Range Definitions Available (see Web Security Manager > Defined Time Ranges)

URL Categories: Google **3.6**

User Agents: None Selected

Cancel **3.7** Submit

Passaggio 3.8. Nella pagina Criteri di decrittografia, fare clic sul collegamento dal filtro URL per il nuovo criterio.

Passaggio 3.9. Selezionare Decrittografa come azione per Categoria URL personalizzato.

Passaggio 3.10. Fare clic su Sottometti.

Decryption Policies: URL Filtering: Decrypting Google Traffic

Custom and External URL Category Filtering

These URL Categories are defined as group membership criteria. All other categories are not applicable for this policy.

Category	Category Type	Use Global Settings	Override Global Settings					
			Pass Through	Monitor	Decrypt	Drop (F)	Quota-Based	Time-Based
Google	Custom (Local)	Select all	Select all	Select all	Select all	Select all	(Unavailable)	(Unavailable)

Cancel **3.9** **3.10** Submit

Passaggio 4.1. Dalla GUI, passare a Web Security Manager e scegliere Access Policies (Policy di accesso).

Passaggio 4.2. Fare clic su Aggiungi criterio.

Passaggio 4.3. Inserire il nome del nuovo criterio.

Passaggio 4. Bloccare il traffico in modalità AI di Google.

Policy Settings

Enable Policy

Policy Name: Google AI Block **4.3**
(e.g. my IT policy)

Description:
(Maximum allowed characters 256)

Insert Above Policy: 1 (getter server access policy)

Policy Expires: Set Expiration for Policy

On Date: MM/DD/YYYY

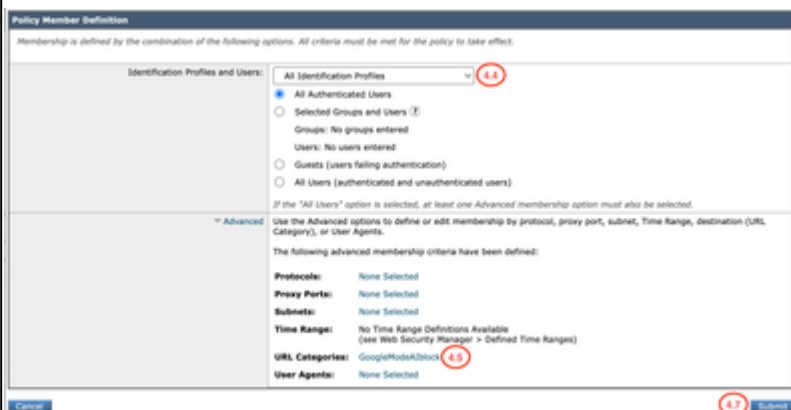
At Time: 00:00

Passaggio 4.4. (Facoltativo) Selezionare il profilo di identificazione a cui applicare il criterio.

Passaggio 4.5. Dalla sezione Definizione membro criterio, fare clic su URL Categories (Categorie URL) per aggiungere la categoria URL personalizzata.

Passaggio 4.6. Selezionare la categoria URL creata nel passaggio 2.

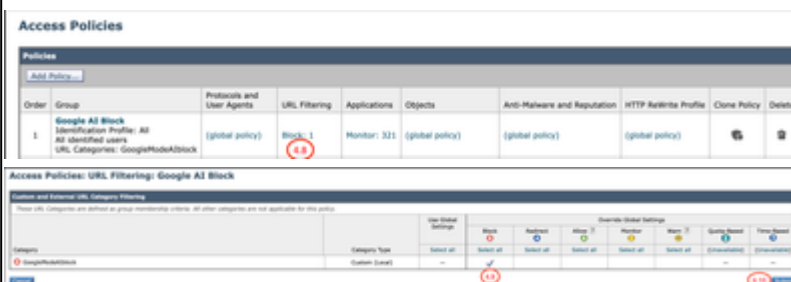
Passaggio 4.7. Fare clic su Sottometti.



Passaggio 4.8. Nella pagina Criteri di accesso, fare clic sul collegamento dal filtro URL per il nuovo criterio.

Passaggio 4.9. Selezionare Blocco come azione per Categoria URL personalizzata.

Passaggio 4.10. Fare clic su Sottometti.



Passaggio 4.11. Eseguire il commit delle modifiche.

Verifica

Una volta completate le impostazioni di configurazione, il traffico AI di Google viene elaborato nei log degli accessi come Blocco come rilevato dalla Categoria personalizzata creata per il blocco AI di Google.

<#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"

Una richiesta di query di ricerca tramite la modalità AI di Google è bloccata e visualizza questa notifica per l'utente finale.



Tutto il resto del traffico Google continua ad essere permesso.

Informazioni correlate

[Definizione di categorie URL personalizzate in WSA](#)

[Guida per l'utente di AsyncOS 15.2 per Cisco Secure Web Appliance](#)

[Configura certificato di decrittografia in Appliance Web sicura](#)

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).